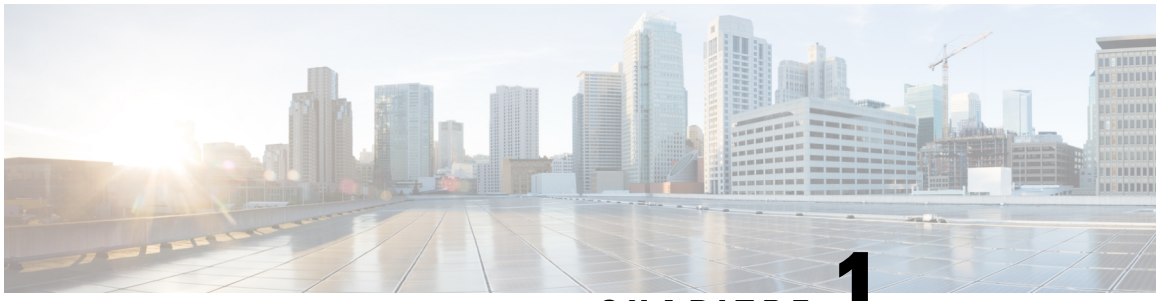
Guide de mise en route de l'appliance Cisco Firepower 1010

Première publication : 13 juin 2019

Dernière modification : 28 février 2022

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



CHAPITRE 1

Quel système d'exploitation et quel gestionnaire vous conviennent le mieux ?

Votre plateforme matérielle peut exécuter l'un des deux systèmes d'exploitation. Pour chaque système d'exploitation, vous pouvez sélectionner différents gestionnaires. Dans ce chapitre, nous décrivons les systèmes d'exploitation et gestionnaires disponibles.

Systèmes d'exploitation

Vous pouvez utiliser l'ASA Secure Firewall ou le système d'exploitation Secure Firewall Threat Defense (anciennement Firepower Threat Defense) sur votre plateforme matérielle :

- ASA : ASA est une appliance qui associe un pare-feu et un concentrateur VPN classiques et avancés.

  Vous pouvez utiliser l'ASA si vous n'avez pas l'intention d'utiliser les fonctionnalités avancées du threat defense, ou si vous souhaitez disposer d'une fonctionnalité propre à l'ASA qui n'est pas encore disponible sur le threat defense. Cisco fournit des outils de migration ASA vers threat defense pour vous aider à convertir votre ASA en pare-feu threat defense si vous commencez par utiliser ASA, puis passez au pare-feu threat defense.

- Threat Defense : Le Threat Defense est un pare-feu de nouvelle génération qui associe un pare-feu avancé avec état, un concentrateur VPN et un système de prévention des intrusions de nouvelle génération. En d'autres termes, le threat defense dispose des fonctionnalités avancées de l'ASA et les combine avec un pare-feu et un système de prévention des intrusions de nouvelle génération.

  Nous vous recommandons d'utiliser le threat defense via le système d'exploitation ASA, car il contient la plupart des fonctionnalités principales de l'ASA, ainsi que des fonctionnalités de pare-feu et de prévention des intrusions de nouvelle génération.

Pour réinstaller l'image entre l'appliance ASA et le threat defense, reportez-vous au Guide de réinstallation de Cisco Secure Firewall ASA et Threat Defense.

Gestionnaires

Le threat defense et l'ASA prennent en charge plusieurs gestionnaires.

Gestionnaires Threat Defense

Tableau 1 : Gestionnaires Threat Defense

Gestionnaire	Description
Secure Firewall Management Center (anciennement Firepower Management Center)	Le centre de gestion est un puissant gestionnaire multi-appareils basé sur le web qui s'exécute sur son propre serveur ou en tant qu'appareil virtuel sur un hyperviseur. Utilisez le centre de gestion si vous souhaitez disposer d'un gestionnaire multi-appareils et utiliser toutes les fonctionnalités du threat defense. Le centre de gestion est par ailleurs doté de puissantes fonctions d'analyse et de surveillance du trafic et des événements. Dans les versions 6.7 et ultérieures, le centre de gestion peut gérer les threat defense à partir de l'interface externe (ou d'une autre interface de données) plutôt que de l'interface de gestion standard. Cette fonctionnalité est utile pour les déploiements de succursales distantes. **Remarque** Le centre de gestion n'est pas compatible avec d'autres gestionnaires, car le centre de gestion détient la configuration du threat defense ; or, vous n'êtes pas autorisé à configurer le threat defense directement, c'est-à-dire en contournant le centre de gestion. Pour vous familiariser avec le centre de gestion sur le réseau de gestion, reportez-vous à la rubrique Déployer Threat Defense avec le Centre de gestion, à la page 5. Pour vous familiariser avec le centre de gestion sur un réseau distant, reportez-vous à la rubrique Déployer Threat Defense avec un Centre de gestion distant, à la page 49.
Gestionnaire d'appareils Secure Firewall (anciennement Firepower Device Manager)	Le gestionnaire d'appareils est un gestionnaire web simplifié et intégré sur les appareils. Dans la mesure où il s'agit d'un outil simplifié, certaines fonctionnalités du threat defense ne sont pas prises en charge dans le gestionnaire d'appareils. Vous devez utiliser le gestionnaire d'appareils si vous gérez uniquement un petit nombre d'appareils et n'avez pas besoin d'un gestionnaire multi-appareils. **Remarque** Le gestionnaire d'appareils et le CDO en mode FDM peuvent tous deux détecter la configuration sur le pare-feu. Vous pouvez donc utiliser le gestionnaire d'appareils ou le CDO pour gérer le même pare-feu. Le centre de gestion n'est pas compatible avec d'autres gestionnaires. Pour commencer avec le gestionnaire d'appareils, reportez-vous à la rubrique Déployer Threat Defense avec le Gestionnaire d'appareils, à la page 93.

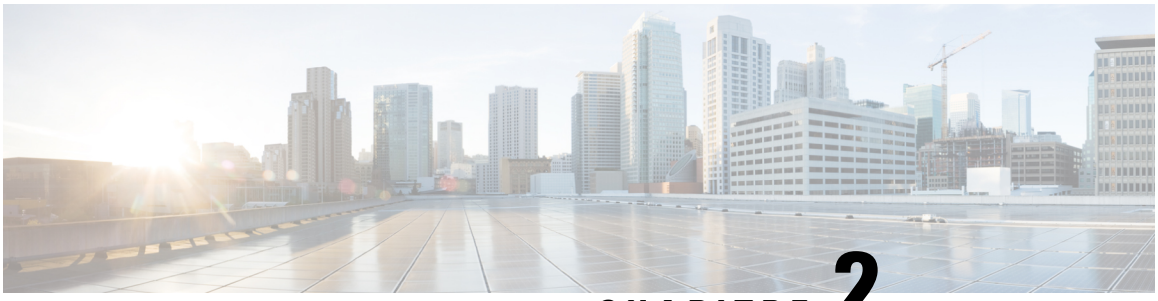
Gestionnaire	Description
Cisco Defense Orchestrator (CDO)	Le CDO propose deux modes de gestion : • (7.2 et versions ultérieures) Mode de centre de gestion fourni dans le cloud avec toutes les fonctionnalités de configuration d'un centre de gestion sur site. Pour la fonctionnalité d'analyse, vous pouvez utiliser Secure Cloud Analytics dans le cloud ou un centre de gestion sur site. • Mode de gestionnaire de périphériques avec une expérience utilisateur simplifiée. Ce mode n'est pas abordé dans ce guide. Étant donné que le CDO est basé dans le cloud, aucune surcharge ne se produit lors de l'exécution du CDO sur vos propres serveurs. Le gestionnaire CDO gère également d'autres appareils de sécurité, notamment les appliances ASA, de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos appareils de sécurité. Pour commencer à utiliser le provisionnement du gestionnaire CDO, reportez-vous à rubrique Déployer Threat Defense avec le CDO, à la page 121.
API REST de Secure Firewall Threat Defense	L'API REST Threat Defense vous permet d'automatiser la configuration directe du threat defense. Cette API est compatible avec le gestionnaire d'appareils et le CDO, car tous deux peuvent détecter la configuration sur le pare-feu. Vous ne pouvez pas utiliser cette API si vous gérez le threat defense à l'aide du centre de gestion. L'API REST Threat Defense n'est pas abordée dans ce guide. Pour obtenir plus d'informations, reportez-vous à la section Guide de l'API REST de Cisco Secure Firewall Threat Defense.
API REST de Secure Firewall Management Center	L'API REST du centre de gestion vous permet d'automatiser la configuration des politiques de centre de gestion, puis d'appliquer ces politiques aux threat defense. Cette API ne gère pas le threat defense directement. L'API REST du centre de gestion n'est pas abordée dans ce guide. Pour obtenir plus d'informations, reportez-vous à la section Guide de démarrage rapide de l'API REST de Secure Firewall Management Center.

Gestionnaires ASA

Tableau 2 : Gestionnaires ASA

Gestionnaire	Description
Adaptive Security Device Manager (ASDM)	ASDM est un gestionnaire d'appareils basé sur Java qui fournit des fonctionnalités ASA complètes. Utilisez ASDM si vous préférez recourir à une interface graphique plutôt qu'à une interface de ligne de commande, et devez gérer un petit nombre d'ASA. ASDM peut détecter la configuration sur le pare-feu, de sorte que vous pouvez également utiliser l'interface de ligne de commande, le CDO ou le CSM avec ASDM. Pour commencer à utiliser ASDM, reportez-vous à la rubrique Déployer l'ASA avec le gestionnaire ASDM, à la page 173.

Gestionnaire	Description
CLI	Vous devez utiliser l'interface de ligne de commande ASA si vous préférez les interfaces de ligne de commande aux interfaces graphiques. L'interface de ligne de commande n'est pas abordée dans ce guide. Pour en savoir plus, consultez les Guides de configuration de l'ASA.
CDO	CDO est un gestionnaire multi-appareils simplifié basé dans le cloud. Dans la mesure où il s'agit d'un outil simplifié, certaines fonctionnalités ASA ne sont pas prises en charge dans CDO. Utilisez CDO si vous souhaitez disposer d'un gestionnaire multi-appareils offrant une expérience de gestion simplifiée. Par ailleurs, étant donné que le CDO est basé dans le cloud, aucune surcharge ne se produit lors de l'exécution du CDO sur vos propres serveurs. CDO gère également d'autres périphériques de sécurité, notamment les threat defense, de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos périphériques de sécurité. CDO peut détecter la configuration sur le pare-feu, de sorte que vous pouvez également utiliser l'interface de ligne de commande ou le gestionnaire ASDM. Le gestionnaire CDO n'est pas traité dans ce guide. Pour commencer à utiliser le CDO, consultez la page d'accueil du gestionnaire CDO.
Cisco Security Manager (CSM)	CSM est un puissant gestionnaire multi-appareils qui s'exécute sur son propre serveur. Vous devez utiliser le gestionnaire CSM si vous devez gérer un grand nombre d'ASA. CSM peut détecter la configuration sur le pare-feu, de sorte que vous pouvez également utiliser l'interface de ligne de commande ou le gestionnaire ASDM. Le gestionnaire CSM ne prend pas en charge la gestion des threat defense. Le gestionnaire CSM n'est pas traité dans ce guide. Pour en savoir plus, consultez le Guide d'utilisateur du gestionnaire CSM.
API REST ASA	L'API REST ASA vous permet d'automatiser la configuration de l'ASA. Cependant, cette API n'inclut pas toutes les fonctionnalités ASA et n'est plus mise à jour. L'API REST ASA n'est pas abordée dans ce guide. Pour obtenir plus d'informations, reportez-vous à la section Guide de démarrage rapide de l'API REST Cisco ASA Secure Firewall.



CHAPITRE 2

Déployer Threat Defense avec le Centre de gestion

Ce chapitre vous concerne-t-il ?

Pour connaître tous les systèmes d'exploitation et gestionnaires disponibles, reportez-vous à la rubrique Quel système d'exploitation et quel gestionnaire vous conviennent le mieux ?, à la page 1. Ce chapitre s'applique au threat defense doté de centre de gestion.

Dans ce chapitre, nous vous expliquons comment effectuer la configuration initiale de votre threat defense et comment enregistrer le pare-feu sur le centre de gestion situé sur votre réseau de gestion. Pour le déploiement dans une succursale distante, où le gestionnaire centre de gestion se trouve sur le siège central, reportez-vous à la rubrique Déployer Threat Defense avec un Centre de gestion distant, à la page 49.

Dans un déploiement classique sur un réseau de grande envergure, vous installez plusieurs appareils gérés sur des segments de réseau. Chaque appareil contrôle, inspecte, surveille et analyse le trafic, puis envoie les informations recueillies à un gestionnaire centre de gestion. Le gestionnaire centre de gestion possède 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 afin de sécuriser votre réseau local.

À propos du pare-feu

L'appareil peut exécuter un logiciel threat defense ou un logiciel ASA. Pour basculer entre threat defense et ASA, vous devez reconfigurer l'appareil. Vous devez également recommencer l'installation si vous avez besoin d'une version logicielle différente de celle actuellement installée. Consultez la rubrique Réinstaller Cisco ASA ou Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé Système d'exploitation Secure Firewall eXtensible (FXOS). Le pare-feu ne prend pas en charge le Gestionnaire de châssis Secure Firewall FXOS ; seule une CLI limitée est prise en charge à des fins de dépannage. Pour obtenir plus d'informations, reportez-vous à la section Guide de dépannage Cisco FXOS pour la série Firepower 1000/2100 exécutant Firepower Threat Defense.

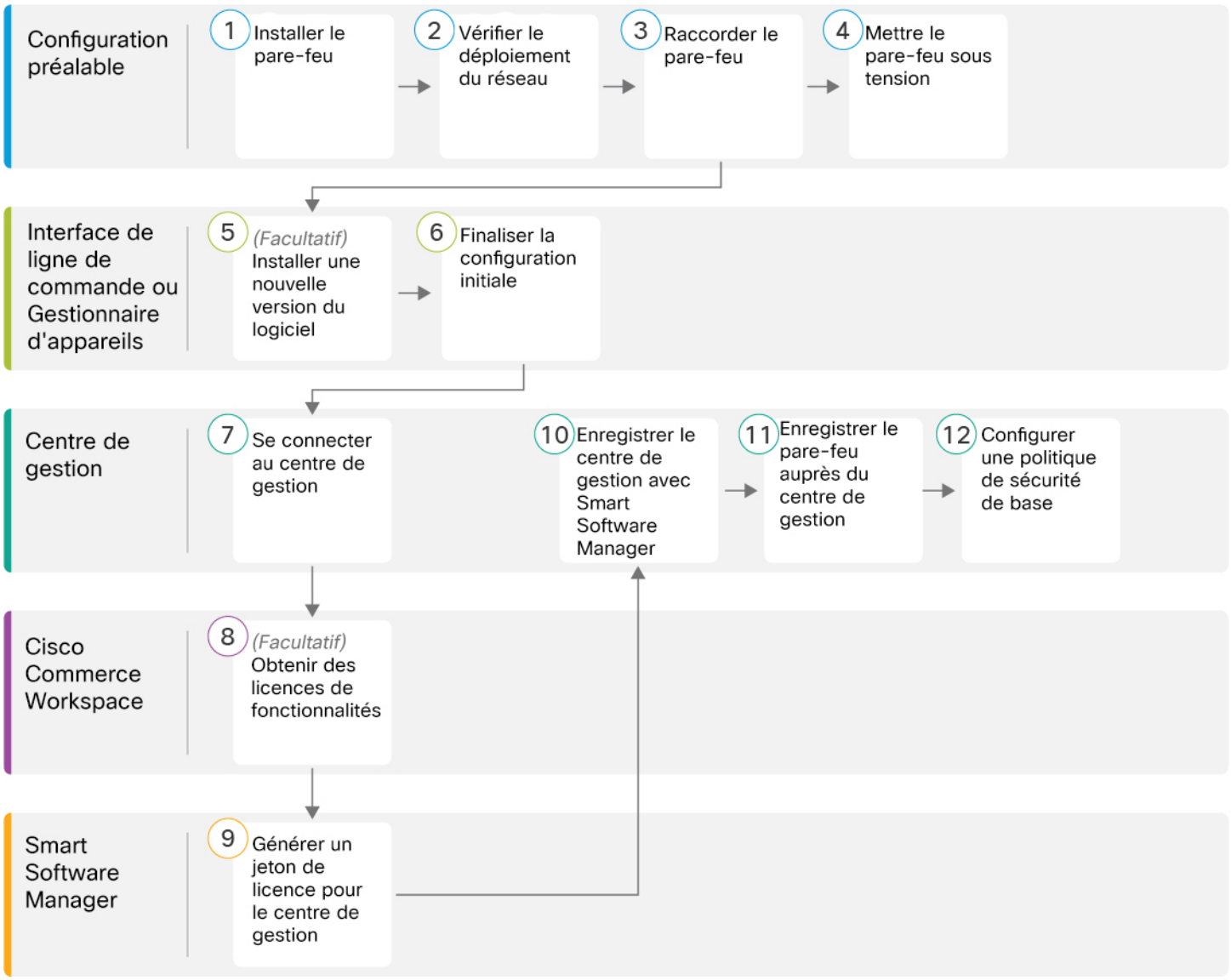
Déclaration de confidentialité—Le pare-feu ne requiert ni ne collecte activement aucune information permettant de vous identifier. Vous pouvez néanmoins utiliser des informations d'identification personnelle au cours de la configuration, notamment des noms d'utilisateur. Dans ce cas, un administrateur peut accéder à ces informations lors de l'utilisation de la configuration ou de l'utilisation du protocole SNMP.

Avant de commencer

Déployez et effectuez la configuration initiale du centre de gestion. Reportez-vous à la rubrique Guide d'installation matérielle pour Cisco Firepower Management Center 1600, 2600 et 4600 ou Guide de mise en route de Cisco Secure Firewall Management Center Virtual.

Procédure de bout en bout

Reportez-vous aux tâches suivantes pour déployer le threat defense avec le centre de gestion sur votre châssis.



1	Configuration préalable	Installez le pare-feu. Reportez-vous au guide d'installation matérielle.
2	Configuration préalable	Vérifier le déploiement du réseau, à la page 8.
3	Configuration préalable	Raccorder l'appareil (6.5 et versions ultérieures), à la page 10 Raccorder l'appareil (6.4), à la page 12.
4	Configuration préalable	Mettre le pare-feu sous tension, à la page 13.

5	Interface de ligne de commande ou Gestionnaire d'appareils	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 14
6	Interface de ligne de commande ou Gestionnaire d'appareils	Finaliser la configuration initiale de Threat Defense, à la page 15.
7	Centre de gestion	Se connecter au Centre de gestion, à la page 24.
8	Cisco Commerce Workspace	Obtenir les licences du Centre de gestion, à la page 24 : acheter des licences de fonctionnalités.
9	Smart Software Manager	Obtenir les licences du Centre de gestion, à la page 24 : générer un jeton de licence pour le centre de gestion.
10	Centre de gestion	Obtenir les licences du Centre de gestion, à la page 24 : enregistrer le centre de gestion sur Smart Licensing Server.
11	Centre de gestion	Enregistrer le Threat Defense auprès du Centre de gestion, à la page 25
12	Centre de gestion	Configurer une politique de sécurité de base, à la page 28

Vérifier le déploiement du réseau

6.5 et versions ultérieures

L'interface de gestion 1/1 dédiée est une interface spéciale qui dispose de ses propres paramètres réseau. Par défaut, l'interface de gestion 1/1 est activée et configurée en tant que client DHCP. Si votre réseau n'inclut pas de serveur DHCP, vous pouvez configurer l'interface de gestion pour qu'elle utilise une adresse IP statique lors de la configuration initiale sur le port de console. Vous pouvez configurer d'autres interfaces après avoir connecté threat defense au centre de gestion. Notez que les ports Ethernet 1/2 à 1/8 sont activés en tant que ports de commutateur par défaut.

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

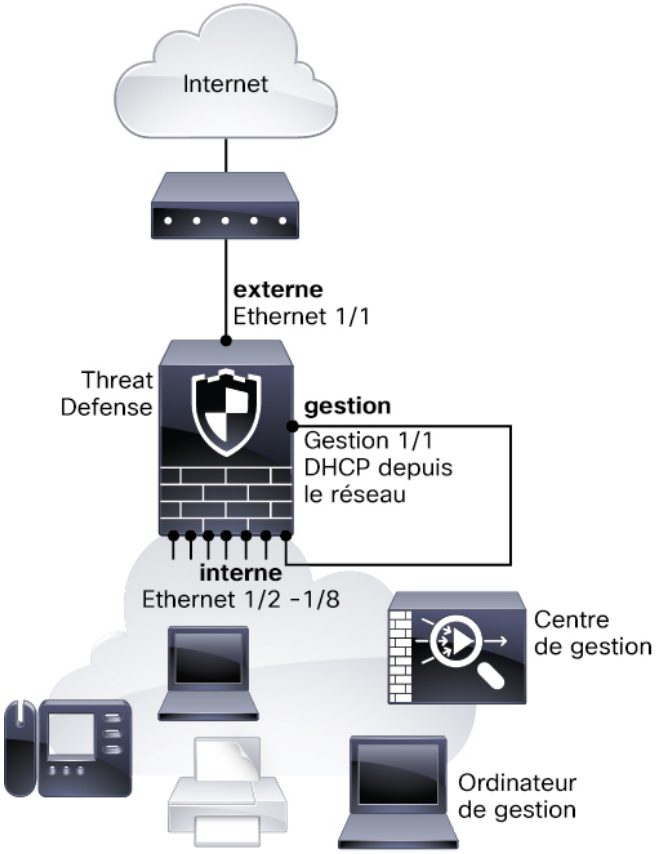
La figure suivante illustre le déploiement réseau recommandé pour le Firepower 1010.

Le centre de gestion peut communiquer uniquement avec threat defense sur l'interface de gestion. En outre, le centre de gestion et threat defense nécessitent un accès Internet via l'interface de gestion pour l'octroi de licences et les mises à jour.

Dans le schéma suivant, le Firepower 1010 fait office de passerelle Internet pour l'interface de gestion et le centre de gestion en connectant l'interface de gestion 1/1 directement à un port de commutateur interne, et en

connectant le centre de gestion et l'ordinateur de gestion à d'autres ports de commutateur internes. (Cette connexion directe est autorisée, car l'interface de gestion est séparée des autres interfaces sur threat defense.)

Illustration 1 : Déploiement réseau suggéré



Déploiement 6.4

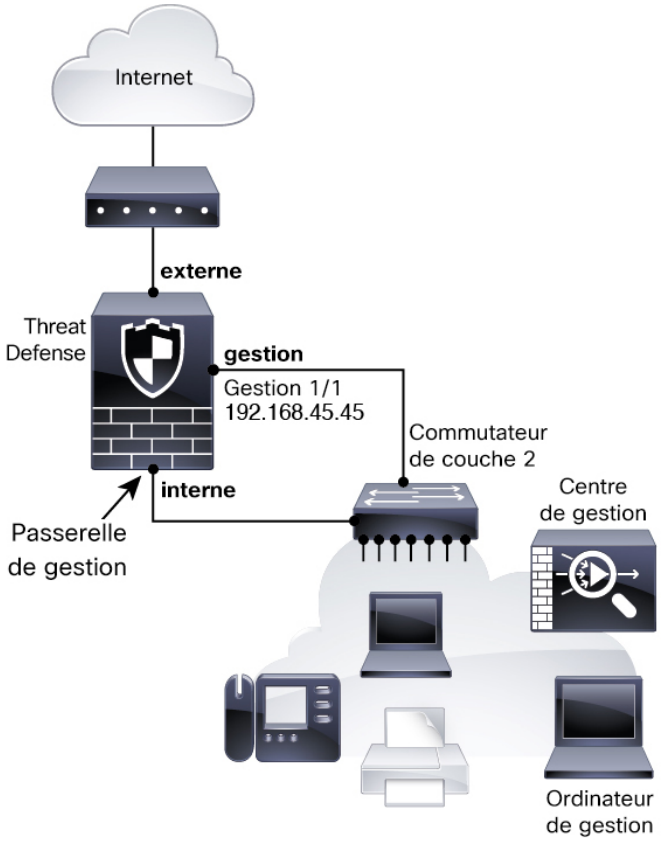
L'interface de gestion 1/1 dédiée est une interface spéciale qui dispose de ses propres paramètres réseau. Par défaut, seule l'interface de gestion 1/1 est activée et configurée avec une adresse IP (192.168.45.45). Par ailleurs, cette interface exécute initialement un serveur DHCP ; après avoir sélectionné centre de gestion comme gestionnaire lors de la configuration initiale, le serveur DHCP est désactivé. Vous pouvez configurer d'autres interfaces après avoir connecté threat defense à centre de gestion.

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

Le centre de gestion peut communiquer uniquement avec threat defense sur l'interface de gestion. En outre, le centre de gestion et threat defense nécessitent un accès Internet via l'interface de gestion pour l'octroi de licences et les mises à jour.

Dans le schéma suivant, le Firepower 1010 fait office de passerelle Internet pour l'interface de gestion et le centre de gestion en connectant l'interface de gestion 1/1 à une interface interne via un commutateur de couche 2 et en connectant le centre de gestion et l'ordinateur de gestion au commutateur. (Cette connexion directe est autorisée, car l'interface de gestion est séparée des autres interfaces sur threat defense.)

Illustration 2 : Déploiement réseau suggéré

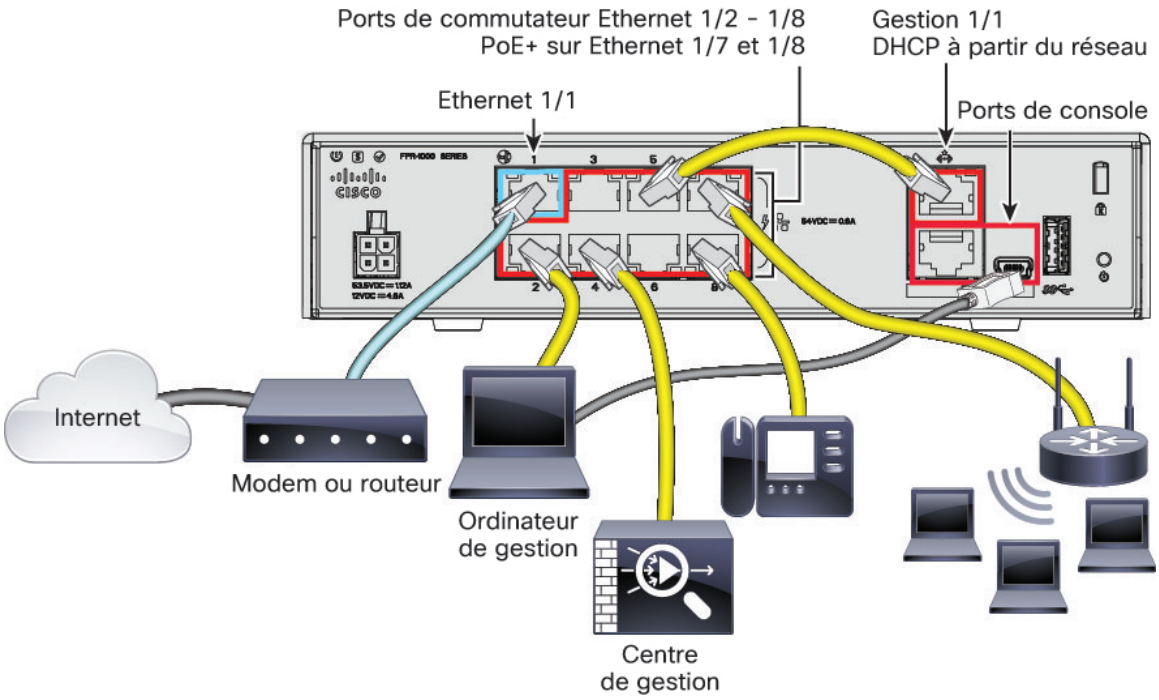


Raccorder l'appareil (6.5 et versions ultérieures)

Pour raccorder l'appareil Firepower 1010 selon le schéma recommandé, reportez-vous à l'illustration suivante, qui présente un exemple de topologie utilisant Ethernet 1/1 comme interface externe et les autres interfaces comme ports de commutateur sur le réseau interne.

Remarque Vous pouvez utiliser d'autres topologies, et votre déploiement varie en fonction de vos besoins. Par exemple, vous pouvez convertir les ports de commutateur en interfaces de pare-feu.

Illustration 3 : Raccorder le Firepower 1010



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

Procédure

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

Étape 2 Connectez directement l'interface de gestion 1/1 à l'un des ports de commutateur, Ethernet 1/2 à 1/8.

Étape 3 Raccordez les câbles suivants aux ports de commutateur, Ethernet 1/2 à 1/8 :

- Centre de gestion
- Ordinateur de gestion
- Terminaux supplémentaires

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

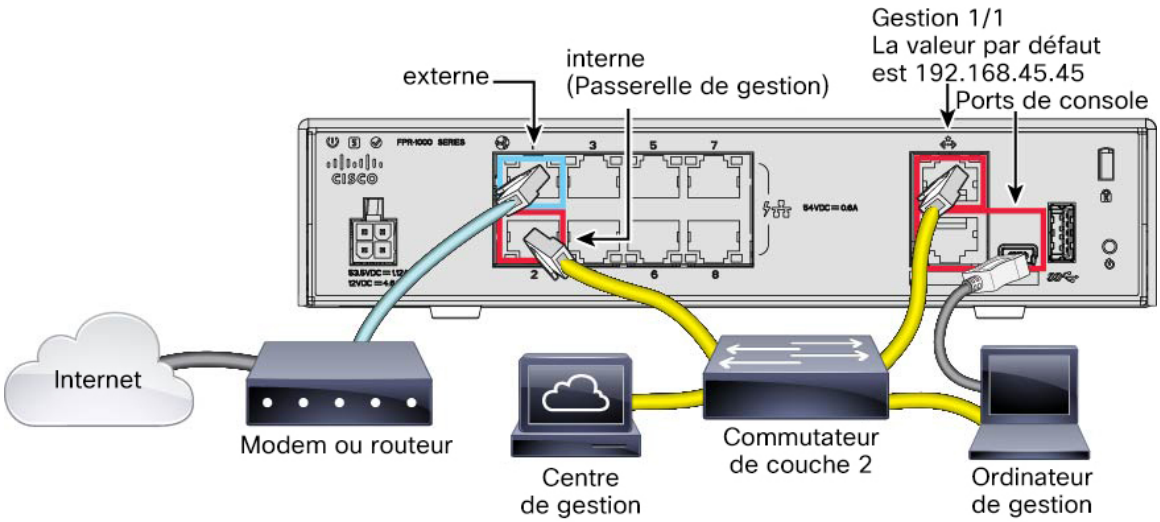
Étape 5 Connectez Ethernet 1/1 à votre routeur externe.

Raccorder l'appareil (6.4)

Pour raccorder l'appareil Firepower 1010 selon le schéma recommandé, reportez-vous à l'illustration suivante, qui présente un exemple de topologie utilisant un commutateur de couche 2.

Remarque Vous pouvez utiliser d'autres topologies, et votre déploiement varie en fonction de vos besoins.

Illustration 4 : Raccorder le Firepower 1010



Procédure

Étape 1 Installez votre matériel et apprenez à l'utiliser à l'aide du guide d'installation matérielle.

Étape 2 Raccordez les composants suivants à un commutateur Ethernet de couche 2 :

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

Remarque L'appareil Firepower 1010 et le centre de gestion possèdent tous deux la même adresse IP de gestion par défaut, à savoir 192.168.45.45. Dans ce guide, nous partons du principe que vous définissez des adresses IP différentes pour vos appareils lors de la configuration initiale. Notez que le gestionnaire centre de gestion sur les versions 6.5 et ultérieures utilise par défaut un client DHCP pour l'interface de gestion ; cependant, en l'absence de serveur DHCP, il utilise l'adresse par défaut 192.168.45.45.

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

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

Étape 5 Connectez les autres réseaux aux interfaces restantes.

Mettre le pare-feu sous tension

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

Remarque La première fois que vous démarrez le threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Avant de commencer

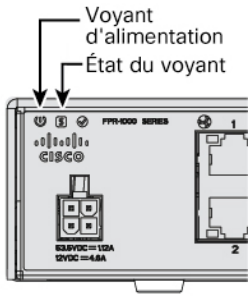
Il est important que vous utilisiez une source d'alimentation fiable pour alimenter votre appareil (à l'aide d'un système d'alimentation sans coupure, par exemple). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent en arrière-plan en permanence, et une panne de courant ne permet pas l'arrêt normal de votre système.

Procédure

Étape 1 Raccordez le câble d'alimentation à l'appareil et branchez-le à une prise électrique.

L'appareil se met automatiquement sous tension dès que vous le branchez.

Étape 2 Observez le voyant d'alimentation situé à l'arrière de l'appareil. S'il est allumé en vert, l'appareil est sous tension.



Étape 3 Observez le voyant d'état à l'arrière ou sur l'appareil. Lorsqu'il s'allume en vert, le système a terminé les diagnostics de mise sous tension.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une autre version, 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 en regard du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de publication décrite dans la rubrique 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. Pour plus d'informations, reportez-vous à la rubrique Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 44. Cette procédure illustre l'utilisation du port de console, mais vous pouvez utiliser SSH si vous le souhaitez.

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

Vous vous connectez à la CLI FXOS. Lors de la première connexion, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si vous avez modifié le mot de passe, mais que vous l'avez oublié, vous devez réinitialiser l'appareil pour rétablir le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure pour rétablir les paramètres 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 Dans l'interface de ligne de commande de la console FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

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

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

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

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, reportez-vous à la rubrique Finaliser la configuration initiale de Threat Defense à l'aide de l'interface de ligne de commande, à la page 20. Par défaut, l'interface de gestion utilise DHCP.

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

b) Suivez la procédure de réinstallation du guide de dépannage de la console FXOS.

Finaliser la configuration initiale de Threat Defense

Vous pouvez finaliser la configuration initiale de threat defense à l'aide de l'interface de ligne de commande ou du gestionnaire d'appareils.

Finaliser la configuration initiale de Threat Defense à l'aide de l'interface du Gestionnaire d'appareils

Connectez-vous au gestionnaire d'appareils pour effectuer la configuration initiale du threat defense. Lorsque vous effectuez la configuration initiale à l'aide du gestionnaire d'appareils, *toutes* les configurations d'interface effectuées dans le gestionnaire d'appareils sont conservées lorsque vous passez au centre de gestion pour la gestion, en plus des paramètres d'interface de gestion et 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 de l'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 du centre de gestion. Reportez-vous à la section Guide d'installation matérielle pour Cisco Firepower Management Center 1600, 2600 et 4600. Vous devez connaître l'adresse IP ou le nom d'hôte du centre de gestion avant de configurer le threat defense.
- Utilisez une version actuelle de Firefox, Chrome, Safari, Edge ou Internet Explorer.

Procédure

Étape 1 Connectez-vous au gestionnaire d'appareils.

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

- Interne (Ethernet1/2 à 1/8)—**https://192.168.95.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutateur interne (Ethernet 1/2 à 1/8).
- Gestion—**https://***ip_gestion*. Dans la mesure où l'interface de gestion est un client DHCP, l'adresse IP dépend de votre serveur DHCP. Vous devrez peut-être définir l'adresse IP de gestion sur une adresse statique dans le cadre de cette procédure. Nous vous recommandons donc d'utiliser l'interface interne afin de ne pas être déconnecté.

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

c) Vous êtes invité à lire et à accepter le contrat de licence de l'utilisateur final et à modifier le mot de passe admin.

Étape 2 Utilisez l'assistant de configuration lors de votre première connexion au gestionnaire d'appareils pour terminer la configuration initiale. Vous pouvez éventuellement ignorer l'assistant de configuration en cliquant sur **Ignorer la configuration de l'appareil** au bas de la page.

Une fois l'assistant de configuration terminé, outre la configuration par défaut de l'interface interne (Ethernet 1/2 à 1/8, qui sont des ports de commutateur sur le VLAN1), la configuration d'une interface externe (Ethernet 1/1) sera conservée lorsque vous passerez à la gestion du centre de gestion.

a) Configurez les options suivantes pour les interfaces externes et de gestion, puis cliquez sur **Suivant**.

1. **Adresse de l'interface externe** : 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 de l'appareil. La première interface de données est l'interface externe par défaut.

   Si vous souhaitez utiliser une interface différente depuis l'interface externe (ou interne) pour l'accès au gestionnaire, vous devez la configurer manuellement après avoir terminé l'assistant de configuration.

   Configurer IPv4 : adresse IPv4 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. Le protocole PPPoE peut être nécessaire si l'interface est connectée à un modem ADSL, un modem câble ou une autre connexion à votre FAI et que votre FAI utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE après avoir terminé l'assistant.

   Configurer IPv6 : adresse IPv6 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv6.

2. **Interface de gestion**

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

   Serveurs DNS : serveur DNS pour l'interface de gestion du pare-feu. Saisissez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. La valeur par défaut est Serveurs DNS publics

OpenDNS. Si vous modifiez les champs et souhaitez rétablir les paramètres par défaut, cliquez sur **Utiliser OpenDNS** pour recharger les adresses IP appropriées dans les champs.

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

b) Configurez les **Paramètres relatifs au temps (NTP)** et cliquez sur **Suivant**.

1. **Fuseau horaire** : sélectionnez le fuseau horaire du système.
2. **Serveur de temps NTP** : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

c) Sélectionnez **Démarrer la période d'évaluation de 90 jours sans enregistrement**.

N'enregistrez pas le threat defense auprès de Smart Software Manager ; toutes les licences sont octroyées sur le centre de gestion.

d) Cliquez sur **Terminer**.

e) Vous êtes invité à sélectionner **Gestion du cloud** ou **Autonome**. Pour la gestion du centre de gestion, sélectionnez **Autonome**, puis **J'ai compris**.

Étape 3 (Peut être obligatoire) Configurez une adresse IP statique pour l'interface de gestion. Sélectionnez **Appareil**, puis cliquez sur le lien **Paramètres système** > **Accès de gestion**.

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

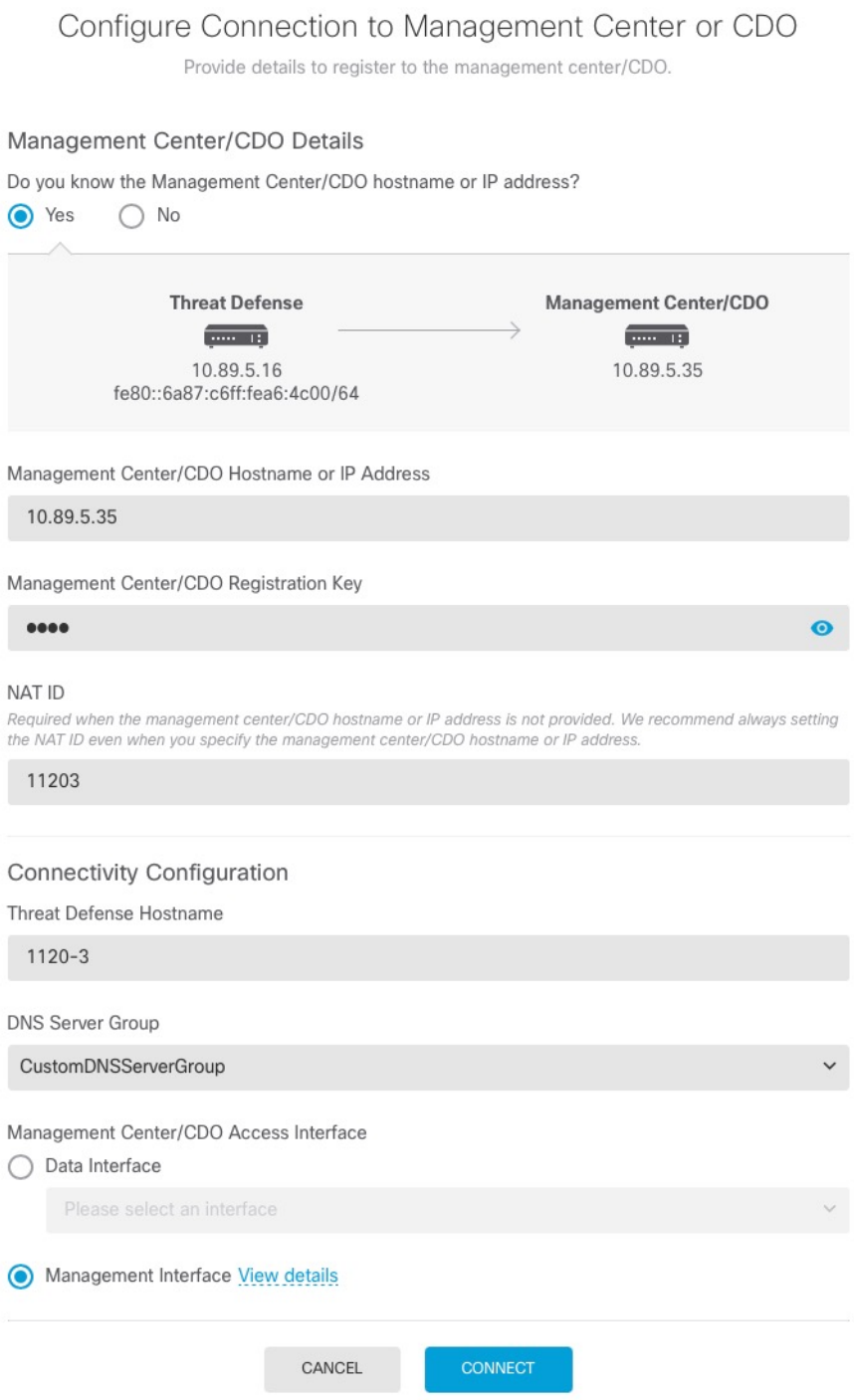
Étape 4 Si vous souhaitez configurer des interfaces supplémentaires, notamment une interface autre que l'interface externe ou interne, sélectionnez **Appareil**, puis cliquez sur le lien dans le récapitulatif **Interfaces**.

Reportez-vous à la rubrique Configurer le pare-feu dans le Gestionnaire d'appareils, à la page 113 pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareils. Les autres configurations du gestionnaire d'appareils ne sont pas conservées lorsque vous enregistrez l'appareil auprès du centre de gestion.

Étape 5 Sélectionnez **Appareil** > **Paramètres système** > **Centre de gestion**, et cliquez sur **Continuer** pour configurer la gestion du centre de gestion.

Étape 6 Configurez les **Détails du centre de gestion/CDO**.

Illustration 5 : Détails du centre de gestion/CDO



a) Pour le champ **Connaissez-vous le nom d'hôte ou l'adresse IP du Centre de gestion/CDO**, cliquez sur **Oui** si vous pouvez accéder au centre de gestion à l'aide d'une adresse IP ou d'un nom d'hôte, ou sur **Non** si le centre de gestion est derrière la NAT ou n'a pas d'adresse IP ou de nom d'hôte public.

Au moins l'un des appareils, soit le centre de gestion soit le threat defense, doit disposer d'une adresse IP accessible pour établir le canal de communication bidirectionnel chiffré SSL entre les deux appareils.

b) Si vous avez choisi **Oui**, saisissez le **Nom d'hôte/adresse IP du Centre de gestion/CDO**.

c) Spécifiez la **Clé d'enregistrement du Centre de gestion/CDO**.

Cette clé est une clé d'enregistrement unique de votre choix, que vous devez également spécifier sur le centre de gestion lorsque vous enregistrez l'appareil threat defense. La clé d'enregistrement ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le trait d'union (-). Il est possible d'utiliser cet ID pour plusieurs appareils qui s'enregistrent auprès du centre de gestion.

d) Spécifiez un **ID NAT**.

Cet ID est une chaîne unique de votre choix, que vous spécifiez également sur le centre de gestion. Ce champ est obligatoire si vous spécifiez uniquement l'adresse IP sur l'un des appareils ; nous vous recommandons cependant de spécifier l'ID NAT même si vous connaissez les adresses IP des deux appareils. L'ID NAT ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le trait d'union (-). Il est *impossible* d'utiliser cet ID pour d'autres appareils enregistrés auprès du centre de gestion. L'ID NAT est utilisé en combinaison avec l'adresse IP pour vérifier que la connexion provient de l'appareil correct ; ce n'est qu'après l'authentification de l'adresse IP/ID NAT que la clé d'enregistrement est vérifiée.

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

a) Spécifiez le **nom d'hôte du FTD**.

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

Sélectionnez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNSServerGroup** et inclut les serveurs OpenDNS.

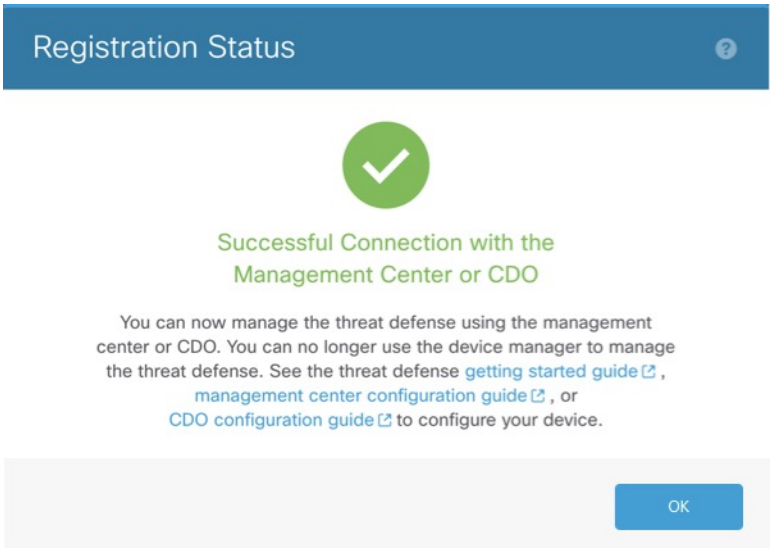
c) Pour **Centre de gestion/Interface d'accès au CDO**, choisissez **gestion**.

Étape 8 Cliquez sur **Connecter**. La boîte de dialogue **État d'enregistrement** affiche l'état actuel du commutateur sur le centre de gestion. Après l'étape **Sauvegarde des paramètres d'enregistrement du centre de gestion/CDO**, accédez au centre de gestion, et ajoutez le pare-feu.

Si vous souhaitez annuler le basculement sur centre de gestion, cliquez sur **Annuler l'enregistrement**. Sinon, ne fermez pas la fenêtre du navigateur gestionnaire d'appareils avant d'avoir terminé l'étape **Sauvegarde des paramètres d'enregistrement du centre de gestion/CDO**. Dans le cas contraire, le processus sera interrompu et ne reprendra que lorsque vous vous reconnecterez au gestionnaire d'appareils.

Si vous restez connecté au gestionnaire d'appareils après l'étape **Sauvegarde de l'enregistrement des paramètres du centre de gestion/CDO**, la boîte de dialogue **Connexion réussie avec le centre de gestion ou le CDO** finit par d'afficher, puis vous êtes déconnecté du gestionnaire d'appareils.

Illustration 6 : Connexion réussie



Finaliser la configuration initiale de Threat Defense à l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande de threat defense pour procéder à la configuration initiale, notamment à la configuration de l'adresse IP de gestion, de la passerelle et d'autres paramètres réseau de base à l'aide de l'assistant de configuration. L'interface de gestion dédiée est une interface spéciale disposant de ses propres paramètres réseau. Dans les versions 6.7 et ultérieures : si vous ne souhaitez pas utiliser l'interface de gestion pour l'accès au gestionnaire, vous pouvez utiliser l'interface de ligne de commande pour configurer une interface de données. Vous configurerez également les paramètres de communication du centre de gestion. Lorsque vous effectuez la configuration initiale à l'aide de gestionnaire d'appareils (7.1 et versions ultérieures), *toutes* les configurations d'interface effectuées dans le gestionnaire d'appareils sont conservées lorsque vous passez au centre de gestion pour la gestion, en plus des paramètres d'interface de gestion et d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès, ne sont pas conservés.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de threat defense, soit à partir du port de console soit à l'aide de SSH à l'interface de gestion, qui obtient une adresse IP d'un serveur DHCP par défaut. Si vous souhaitez modifier les paramètres réseau, nous vous recommandons d'utiliser le port de console pour éviter toute déconnexion.

Le port de console se connecte à l'interface de ligne de commande de FXOS. La session SSH se connecte directement à l'interface de ligne de commande de threat defense.

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

Sur le port de console, vous vous connectez à l'interface de ligne de commande de la console FXOS. Lors de la première connexion à FXOS, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si vous avez modifié le mot de passe, mais que vous l'avez oublié, vous devez reconfigurer l'appareil pour réinitialiser le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure de réinstallation.

Exemple :

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

[...]

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

[...]

firepower#
```

Étape 3 Si vous êtes connecté à FXOS sur le port de console, connectez-vous à l'interface de ligne de commande de threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 4 La première fois que vous vous connectez à threat defense, vous êtes invité à accepter le contrat de licence de l'utilisateur final (CLUF) et, si vous utilisez une connexion SSH, à modifier le mot de passe administrateur. Le script de configuration de la CLI vous est ensuite présenté.

Remarque Vous ne pouvez pas répéter l'assistant de configuration de la CLI à moins d'avoir effacé la configuration, par exemple, via une réinitialisation. Vous pouvez cependant modifier tous les paramètres ultérieurement dans l'interface de ligne de commande à l'aide des commandes **configure network**. Reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

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

Reportez-vous aux instructions suivantes :

- **Saisissez la passerelle IPv4 par défaut pour l'interface de gestion** : le paramètre **data-interfaces** s'applique uniquement au centre de gestion distant ou à la gestion du gestionnaire d'appareils ; vous devez définir une adresse IP de passerelle pour l'interface de gestion 1/1 lorsque vous utilisez le centre de gestion sur le réseau de gestion. Dans l'exemple de déploiement de périphérie illustré dans la section de déploiement du réseau, l'interface interne fait office de passerelle de gestion. Dans ce cas, vous devez

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

- **Si vos informations réseau ont changé, vous devrez vous reconnecter** : si vous êtes connecté à SSH, mais que vous modifiez l'adresse IP lors de la configuration initiale, vous êtes déconnecté. Reconnectez-vous en utilisant une nouvelle adresse IP et un nouveau mot de passe. Les connexions de console restent actives.
- **Gérer l'appareil localement ?** : saisissez **non** pour utiliser le centre de gestion. Si vous saisissez **oui**, vous utilisez le gestionnaire d'appareils.
- **Configurer le mode de pare-feu ?** : nous vous recommandons de définir le mode de pare-feu lors de la configuration initiale. La modification du mode de pare-feu après la configuration initiale efface la configuration en cours.

Exemple :

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

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

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

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

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

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

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

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

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

Étape 5 Identifiez le centre de gestion qui gérera ce threat defense.

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 du centre de gestion. Si le centre de gestion n'est pas directement adressable, utilisez **DONTRESOLVE** et spécifiez *nat_id*. Au moins l'un des appareils, soit le centre de gestion soit le threat defense, doit disposer d'une adresse IP accessible pour établir le canal de communication bidirectionnel chiffré SSL entre les deux appareils. Si vous spécifiez **DONTRESOLVE** dans cette commande, le threat defense doit disposer d'une adresse IP ou d'un nom d'hôte accessible.
- *reg_key* : spécifie une clé d'enregistrement unique de votre choix, que vous devez également spécifier sur le centre de gestion lors de l'enregistrement du threat defense. La clé d'enregistrement ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le trait d'union (-).
- *nat_id* : spécifie une chaîne unique de votre choix, que vous devez également spécifier sur le centre de gestion lors de l'enregistrement du threat defense lorsqu'un côté ne spécifie pas une adresse IP ou un nom d'hôte accessible. Elle est obligatoire si vous définissez le centre de gestion sur **DONTRESOLVE**. L'ID NAT ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le trait d'union (-). Il est impossible d'utiliser cet ID pour d'autres appareils enregistrés auprès du centre de gestion.

Exemple :

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

Si le centre de gestion se trouve derrière un appareil NAT, saisissez un ID NAT unique avec la clé d'enregistrement et spécifiez DONTRESOLVE au lieu du nom d'hôte, par exemple :

Exemple :

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

Si le threat defense se trouve derrière un appareil NAT, saisissez un ID NAT unique avec l'adresse IP ou le nom d'hôte du centre de gestion, par exemple :

Exemple :

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

Que faire ensuite

Enregistrez votre pare-feu sur le centre de gestion.

Se connecter au Centre de gestion

Utilisez le centre de gestion pour configurer et surveiller le threat defense.

Avant de commencer

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

Procédure

Étape 1 À l'aide d'un navigateur pris en charge, saisissez 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**.

Obtenir les licences du Centre de gestion

Toutes les licences sont fournies au threat defense via le centre de gestion. Vous pouvez acheter les licences suivantes :

- **Menace** : sécurité adaptative et système de prévention des intrusions de nouvelle génération
- **Malware** : protection contre les programmes malveillants
- **URL** : filtrage des URL
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN uniquement

Pour une présentation complète de Cisco Licensing, rendez-vous sur cisco.com/go/licensingguide.

Avant de commencer

- Veillez à disposer d'un compte principal sur 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 entreprise.

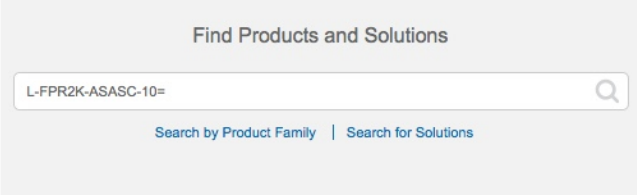
- Votre compte Smart Software Licensing doit bénéficier de la licence de chiffrement renforcé (3DES/AES) pour utiliser certaines fonctionnalités (activées à l'aide de l'indicateur de conformité d'exportation).

Procédure

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

Si vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte Smart Software License. Toutefois, si vous devez ajouter des licences vous-même, utilisez le champ de recherche **Rechercher des produits et des solutions** de Cisco Commerce Workspace. Recherchez les PID de licence suivants :

Illustration 7 : Recherche de licences



Remarque Si aucun PID n'est renvoyé, vous pouvez l'ajouter manuellement à votre commande.

- Combinaison des licences Threat, Malware et URL :
  - L-FPR1010T-TMC=

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

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

Pour cela, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Reportez-vous à au Guide d'administration de Cisco Secure Firewall Management Center pour obtenir des instructions détaillées.

Enregistrer le Threat Defense auprès du Centre de gestion

Enregistrez le threat defense auprès du centre de gestion manuellement à l'aide de l'adresse IP ou du nom d'hôte de l'appareil.

Avant de commencer

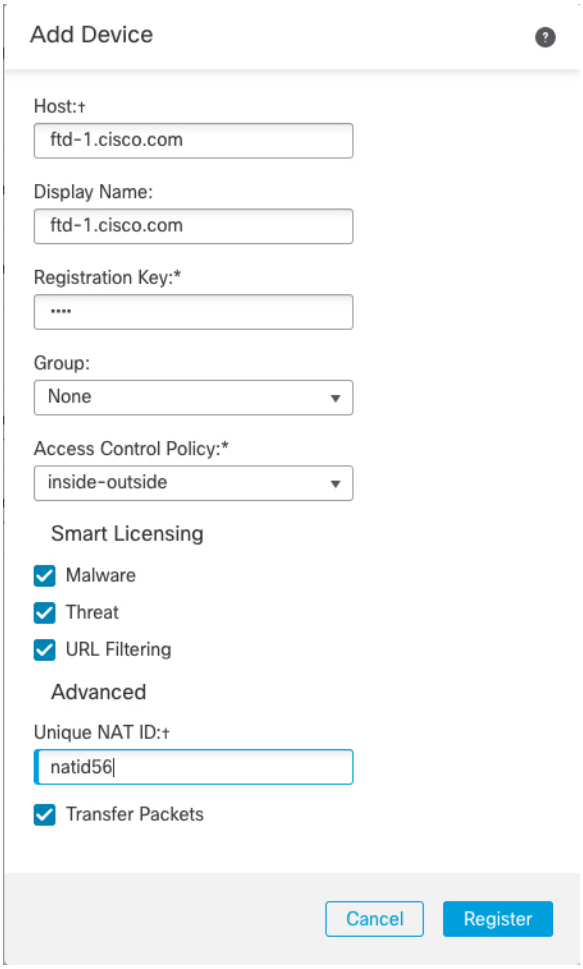
- Collectez les informations suivantes que vous avez définies dans la de démarrage :
  - Adresse IP de gestion ou nom d'hôte du threat defense, et ID NAT

- Clé d'enregistrement du centre de gestion

Procédure

Étape 1 Dans centre de gestion, sélectionnez **Appareils** > **Gestion des appareils**.

Étape 2 Dans la liste déroulante **Ajouter**, sélectionnez **Ajouter l'appareil**.



Définissez les paramètres suivants :

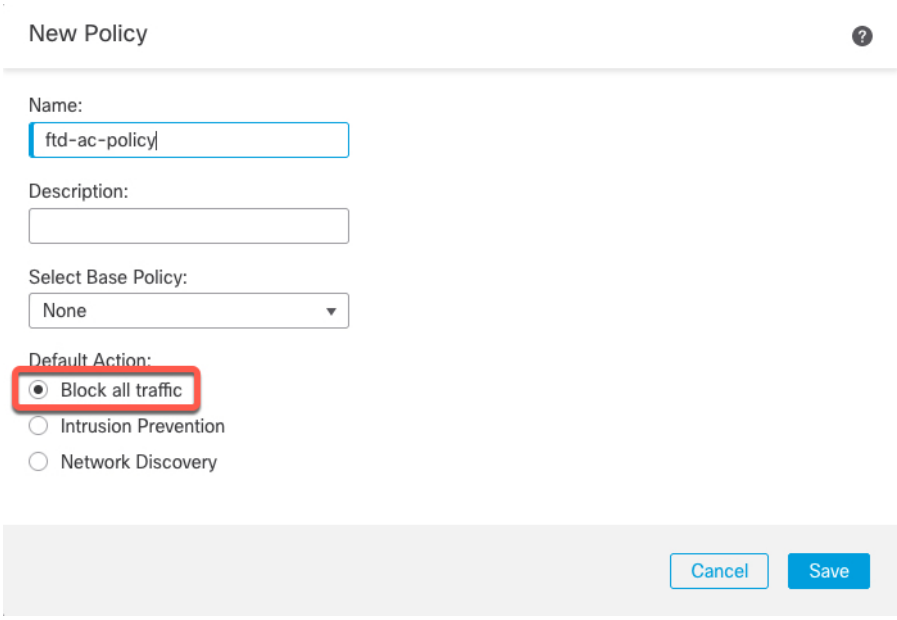
- **Hôte** : saisissez l'adresse IP ou le nom d'hôte du threat defense que vous souhaitez ajouter. Vous pouvez laisser ce champ vide si vous avez spécifié à la fois l'adresse IP du centre de gestion et un ID NAT dans la configuration de initiale du threat defense.

  Remarque Dans un environnement haute disponibilité, lorsque les deux centres de gestionse trouvent derrière un NAT, vous pouvez enregistrer le threat defense sans adresse IP ni nom d'hôte dans le centre de gestion principal. Toutefois, pour enregistrer le threat defense dans un centre de gestion secondaire, vous devez fournir l'adresse IP ou le nom d'hôte du threat defense.

- **Nom d'affichage** : saisissez le nom du threat defense tel que vous souhaitez l'afficher dans le centre de gestion.

- **Clé d'enregistrement** : saisissez la clé d'enregistrement que vous avez spécifiée dans la configuration de initiale du threat defense.
- **Domaine** : attribuez l'appareil à un domaine Leaf si vous disposez d'un environnement multidomaine.
- **Groupe** : attribuez-le à un groupe d'appareils si vous utilisez des groupes.
- **Politique de contrôle d'accès** : sélectionnez une politique initiale. Sauf si vous disposez déjà d'une politique personnalisée que vous devez utiliser, sélectionnez **Créer une nouvelle politique** et sélectionnez **Bloquer tout le trafic**. Vous pourrez la modifier ultérieurement pour autoriser le trafic ; reportez-vous à la rubrique Autoriser le trafic de l'interface interne vers l'interface externe, à la page 41.

Illustration 8 : Nouvelle politique



- **Smart Licensing**: attribuez les licences Smart dont vous avez besoin pour les fonctionnalités que vous souhaitez déployer : **Malware** (si vous souhaitez utiliser l'inspection), **Threat** (si vous prévoyez d'utiliser la prévention contre les intrusions) et **URL** (si vous avez l'intention de mettre en œuvre le filtrage d'URL basé sur les catégories). **Remarque** : vous pouvez appliquer une licence VPN d'accès distant Client sécurisé après avoir ajouté l'appareil, via la page **Système** > **Licences** > **Licences Smart**.
- **ID NAT unique** : spécifiez l'ID NAT que vous avez spécifié dans la configuration initiale du threat defense.
- **Transférer des paquets** : permet à l'appareil de transférer des paquets vers le centre de gestion. Lorsque des événements comme IPS ou Snort sont déclenchés alors que cette option est activée, l'appareil envoie des informations de métadonnées d'événement et des données de paquet au centre de gestion à des fins d'inspection. Si vous désactivez cette option, seules les informations d'événement sont envoyées au centre de gestion ; les données de paquet ne sont pas envoyées.

Étape 3 Cliquez sur **S'enregistrer** ou, si vous souhaitez ajouter un autre appareil, cliquez sur **Enregistrer et ajouter un autre appareil** et confirmez l'enregistrement.

Si l'enregistrement réussit, l'appareil est ajouté à la liste. En cas d'échec, un message d'erreur s'affiche. Si l'enregistrement du threat defense échoue, vérifiez les points suivants :

- Ping : accédez à la CLI du threat defense et envoyez une requête ping à l'adresse IP du centre de gestion à l'aide de la commande suivante :

  ping system *ip_address*

  Si la requête ping échoue, vérifiez les paramètres réseau à l'aide de la commande **show network**. Si vous devez modifier l'adresse IP de gestion du threat defense, utilisez la commande **configure network** {**ipv4** | **ipv6**} **manual**.

- Clé d'enregistrement, ID NAT et adresse IP du 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 le centre de gestion à l'aide de la commande **configure manager add**.

Pour plus d'informations sur le dépannage, consultez la page https://cisco.com/go/fmc-reg-error.

Configurer une politique de sécurité de base

Dans cette section, nous vous expliquons comment configurer une politique de sécurité de base avec les paramètres suivants :

- Interfaces internes et externes : attribuez une adresse IP statique à l'interface interne et utilisez DHCP pour l'interface externe.
- Serveur DHCP : utilisez un serveur DHCP sur l'interface interne pour les clients.
- Route par défaut : ajoutez une route par défaut via l'interface externe.
- NAT : utilisez l'interface PAT sur l'interface externe.
- Contrôle d'accès : autorisez le trafic de l'interface interne vers l'interface externe.

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

1	Configurer les interfaces (6.5 et versions ultérieures), à la page 29 Configurer les interfaces (6.4), à la page 33.
2	Configurer le serveur DHCP, à la page 36.
3	Ajouter la route par défaut, à la page 37.
4	Configuration du routage NAT, à la page 38.
5	Autoriser le trafic de l'interface interne vers l'interface externe, à la page 41.
6	Déployer la configuration, à la page 42.

Configurer les interfaces (6.5 et versions ultérieures)

Ajoutez l'interface VLAN1 pour les ports de commutateur ou convertissez les ports de commutateur 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 qu'un système transmette un trafic significatif. Habituellement, vous disposez d'une interface externe face au routeur en amont ou à Internet, et d'une ou de plusieurs interfaces internes pour les réseaux de votre entreprise. Par défaut, Ethernet1/1 est une interface de pare-feu standard que vous pouvez utiliser à l'extérieur ; les autres interfaces sont des ports de commutateur sur le VLAN 1. Après avoir ajouté l'interface VLAN1, vous pouvez la convertir en interface interne. Vous pouvez également attribuer des ports de commutateur à d'autres VLAN ou convertir des ports de commutateur en interfaces de pare-feu.

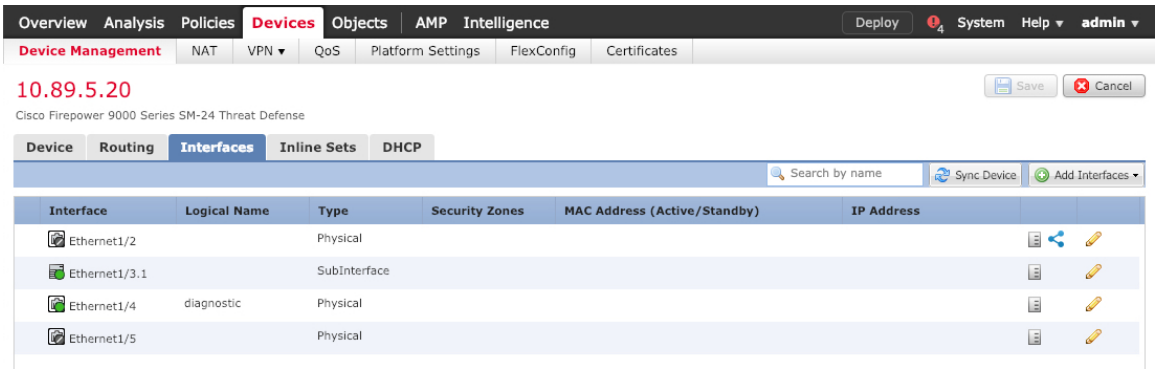
Un routage de périphérie classique consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre FAI, pendant que vous définissez des adresses statiques sur les interfaces internes.

L'exemple suivant configure une interface interne en mode routé (VLAN1) avec une adresse statique et une interface externe en mode routé à l'aide de DHCP (Ethernet1/1).

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** (✎) de l'appareil.

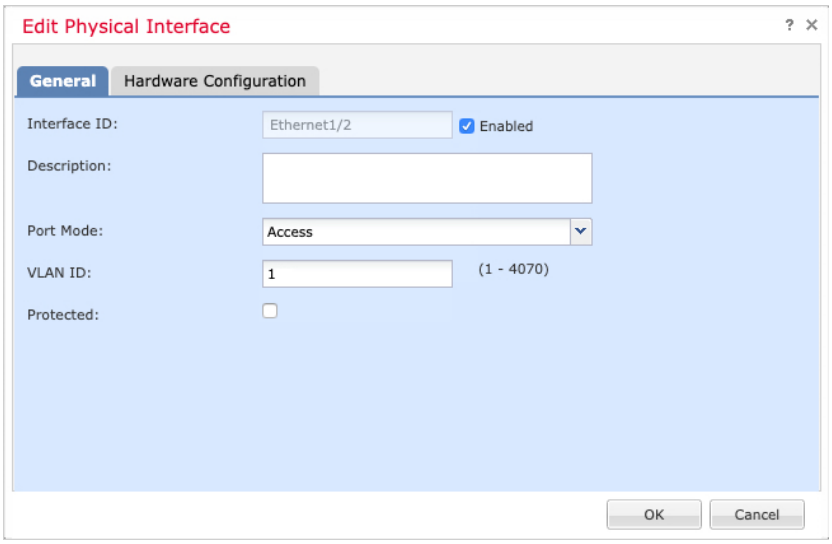
Étape 2 Cliquez sur **Interfaces**.



Étape 3 (facultatif) Désactivez le mode de port de commutateur pour l'un des ports de commutateur (Ethernet 1/2 à 1/8) en cliquant sur le curseur dans la colonne **SwitchPort** pour le désactiver ( ).

Étape 4 Activez les ports de commutateur.

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



b) Activez l'interface en cochant la case **Activé**.

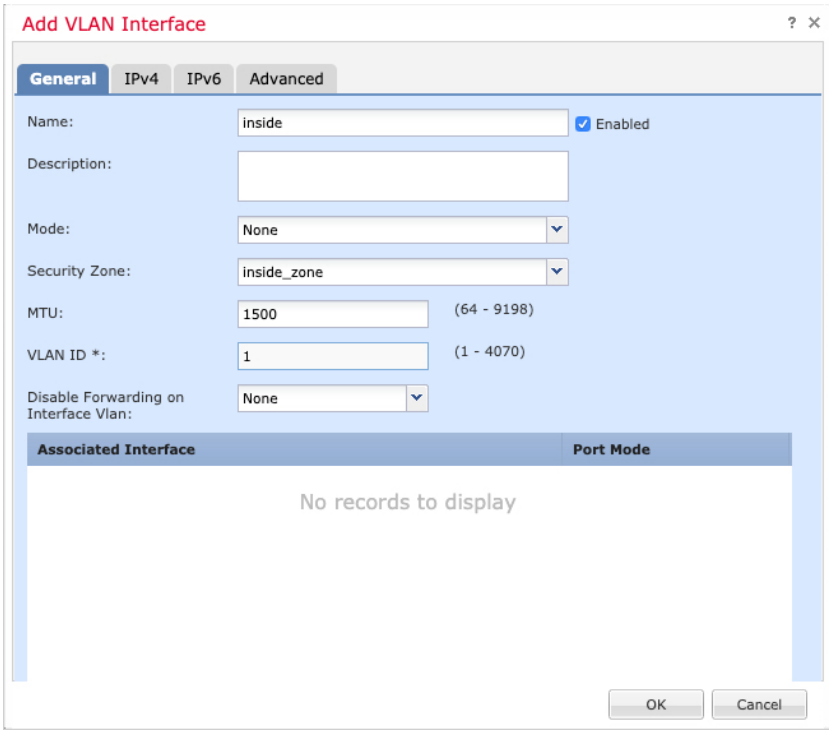
c) (facultatif) Modifiez l'ID de VLAN ; la valeur par défaut est 1. Vous devez ensuite ajouter une interface VLAN correspondant à cet ID.

d) Cliquez sur **OK**.

Étape 5 Ajoutez l'interface VLAN *interne*.

a) Cliquez sur **Ajouter des interfaces** > **Interface VLAN**.

L'onglet **Général** s'affiche.



b) Saisissez un **nom** comportant maximum 48 caractères.

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

c) Cochez la case **Activé**.

d) Laissez le champ **Mode** défini sur **Aucun**.

e) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité interne existante ou ajoutez-en une nouvelle en cliquant sur **Créer**.

Par exemple, ajoutez une zone appelée **zone_interne**. Chaque interface doit être affectée à une zone de sécurité et/ou à un groupe d'interfaces. Une interface peut appartenir 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 attribuer l'interface interne à la zone interne, et l'interface externe à la zone externe. Vous pouvez ensuite configurer votre politique de contrôle d'accès pour que le trafic transite de l'interface interne vers l'interface externe, mais pas de l'interface externe vers l'interface interne. La plupart des politiques ne prennent en charge que les zones de sécurité ; vous pouvez utiliser des zones ou des groupes d'interfaces dans les politiques NAT, les politiques de préfiltre et les politiques QoS.

f) Définissez le champ **ID de VLAN** sur **1**.

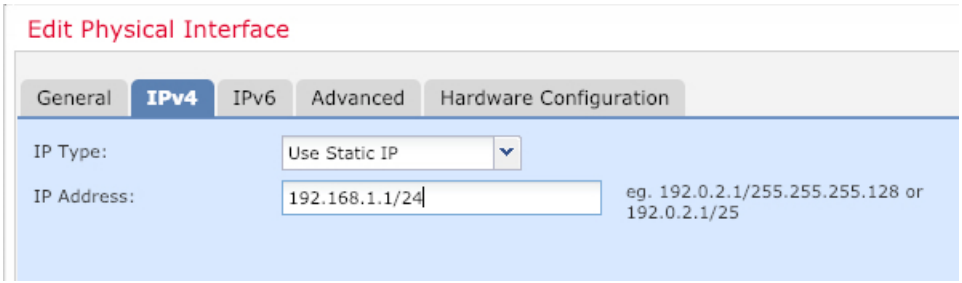
Par défaut, tous les ports de commutateur sont définis sur l'ID de VLAN 1 ; si vous choisissez un autre ID de VLAN, vous devez également modifier chaque port de commutateur pour qu'il corresponde au nouvel ID de VLAN.

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

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

- **IPv4** : sélectionnez **Utiliser l'adresse IP statique** dans la liste déroulante, et saisissez une adresse IP et un masque de sous-réseau en notation de barre oblique.

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

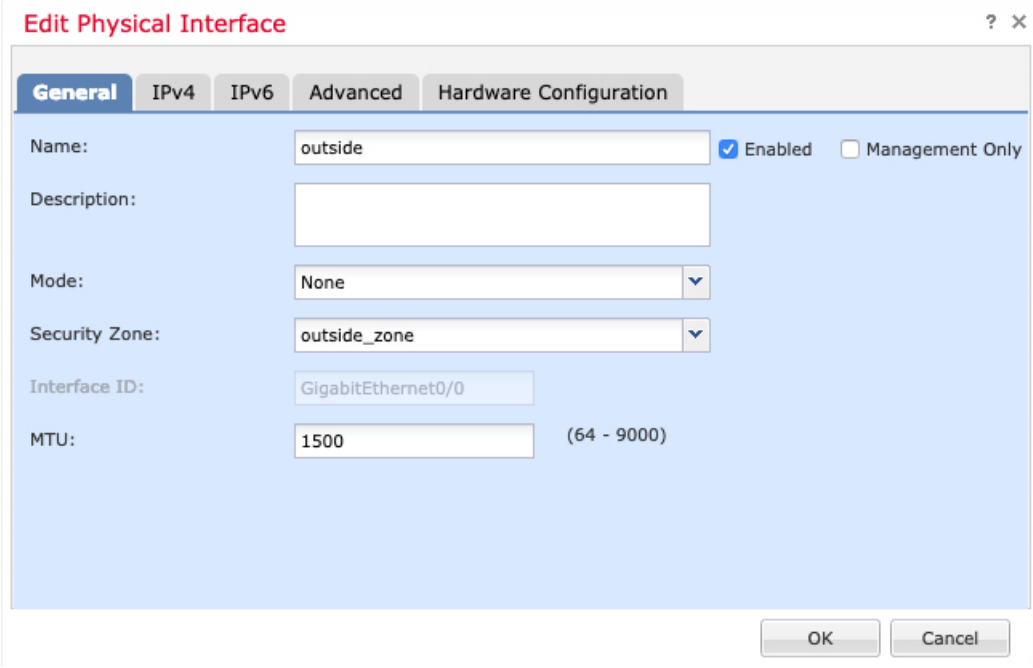


- **IPv6** : cochez la case **Configuration automatique** pour la configuration automatique sans état.

h) Cliquez sur **OK**.

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

L'onglet **Général** s'affiche.



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

a) Saisissez un **nom** comportant maximum 48 caractères.

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

b) Cochez la case **Activé**.

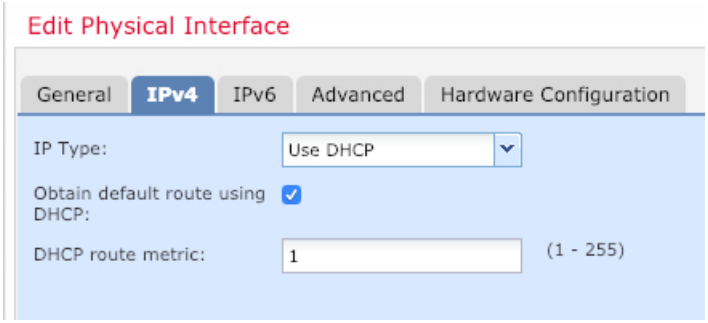
c) Laissez le champ **Mode** défini sur **Aucun**.

d) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **Créer**.

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

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

- **IPv4** : sélectionnez **Utiliser DHCP** et configurez les paramètres facultatifs suivants :
  - **Obtenir la route par défaut à l'aide de DHCP** : permet d'obtenir la route par défaut à partir du serveur DHCP.
  - **Métrique de routage DHCP** : attribue une distance administrative à la route apprise, comprise entre 1 et 255. La distance administrative par défaut pour les routes apprises est 1.



- **IPv6** : cochez la case **Configuration automatique** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

Étape 7 Cliquez sur **Enregistrer**.

Configurer les interfaces (6.4)

Activez les interfaces de threat defense, attribuez-les aux zones de sécurité et définissez les adresses IP. En règle générale, vous devez configurer au moins deux interfaces pour qu'un système transmette un trafic significatif. Habituellement, vous disposez d'une interface externe face au routeur en amont ou à Internet, et d'une ou de plusieurs interfaces internes pour les réseaux de votre entreprise. Certaines de ces interfaces peuvent être des « zones démilitarisées » (DMZ), dans lesquelles vous placez des ressources accessibles au public, comme votre serveur web.

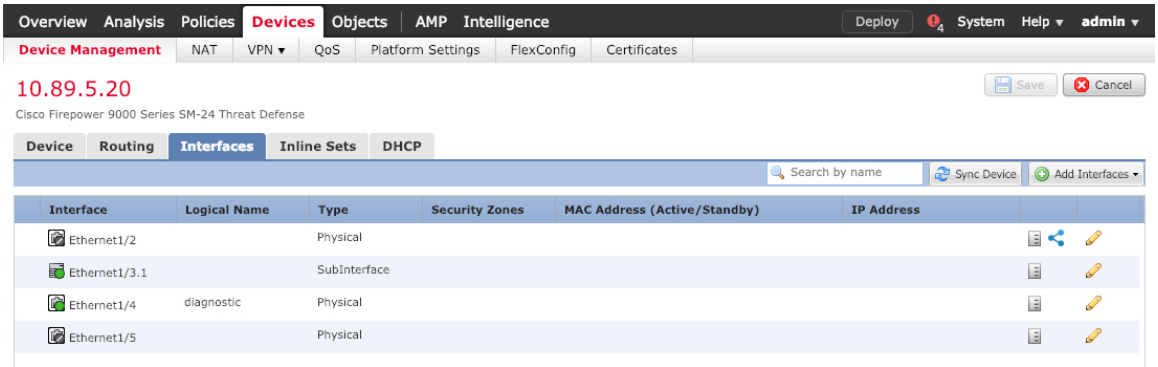
Un routage de périphérie classique consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre FAI, pendant que vous définissez des adresses statiques sur les interfaces internes.

L'exemple suivant configure une interface interne en mode routé avec une adresse statique et une interface externe en mode routé à l'aide de DHCP.

Procédure

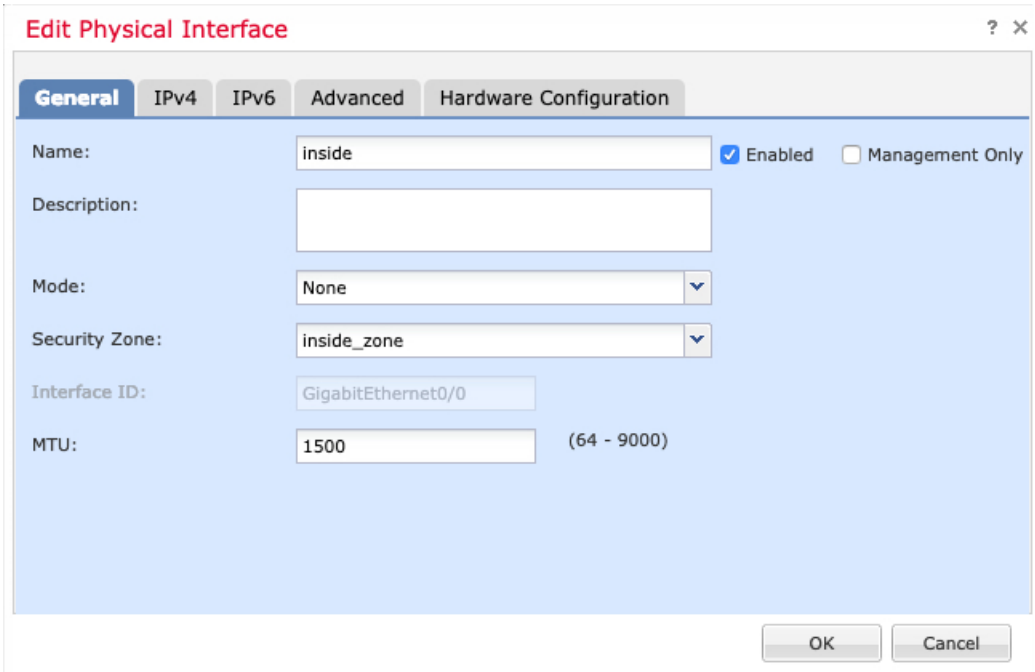
Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** ( ) du pare-feu.

Étape 2 Cliquez sur **Interfaces**.



Étape 3 Cliquez sur l'icône **Modifier** (✎) correspondant à l'interface que vous souhaitez utiliser en tant qu'interface *interne*.

L'onglet **Général** s'affiche.



a) Saisissez un **nom** comportant maximum 48 caractères.

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

b) Cochez la case **Activé**.

c) Laissez le champ **Mode** défini sur **Aucun**.

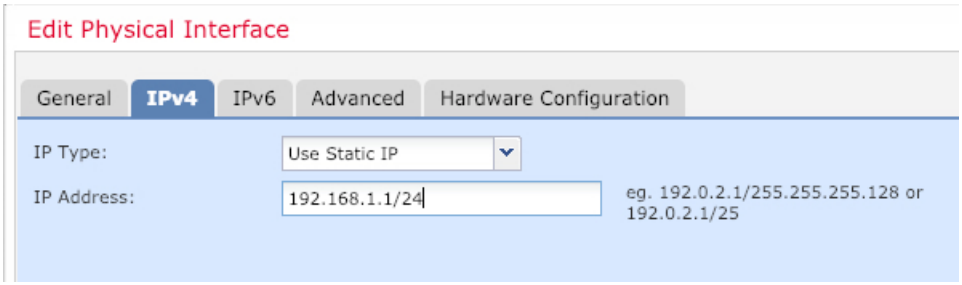
d) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité interne existante ou ajoutez-en une nouvelle en cliquant sur **Créer**.

Par exemple, ajoutez une zone appelée **zone_interne**. Chaque interface doit être affectée à une zone de sécurité et/ou à un groupe d'interfaces. Une interface peut appartenir 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 attribuer l'interface interne à la zone interne, et l'interface externe à la zone externe. Vous pouvez ensuite configurer votre politique de contrôle d'accès pour que le trafic transite de l'interface interne vers l'interface externe, mais pas de l'interface externe vers l'interface interne. La plupart des politiques ne prennent en charge que les zones de sécurité ; vous pouvez utiliser des zones ou des groupes d'interfaces dans les politiques NAT, les politiques de préfiltre et les politiques QoS.

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

- **IPv4** : sélectionnez **Utiliser l'adresse IP statique** dans la liste déroulante, et saisissez une adresse IP et un masque de sous-réseau en notation de barre oblique.

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

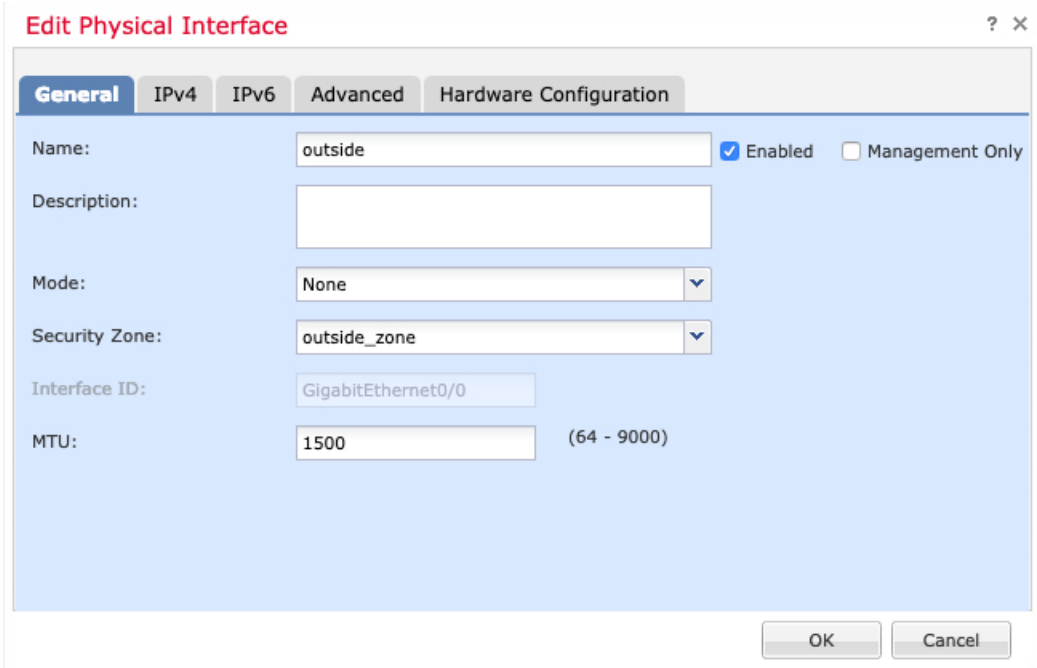


- **IPv6** : cochez la case **Configuration automatique** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

Étape 4 Cliquez sur l'icône **Modifier** (✎) correspondant à l'interface que vous souhaitez utiliser en *externe*.

L'onglet **Général** s'affiche.



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

a) Saisissez un **nom** comportant maximum 48 caractères.

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

b) Cochez la case **Activé**.

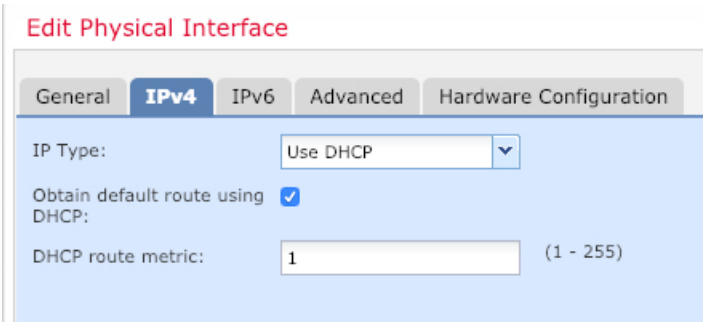
c) Laissez le champ **Mode** défini sur **Aucun**.

d) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **Créer**.

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

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

- **IPv4** : sélectionnez **Utiliser DHCP** et configurez les paramètres facultatifs suivants :
  - **Obtenir la route par défaut à l'aide de DHCP** : permet d'obtenir la route par défaut à partir du serveur DHCP.
  - **Métrique de routage DHCP** : attribue une distance administrative à la route apprise, comprise entre 1 et 255. La distance administrative par défaut pour les routes apprises est 1.



- **IPv6** : cochez la case **Configuration automatique** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

Étape 5 Cliquez sur **Enregistrer**.

Configurer le serveur DHCP

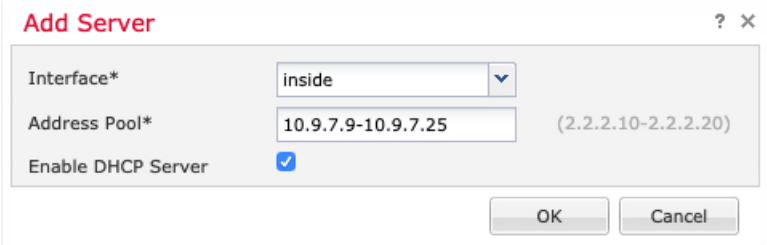
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir du threat defense.

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** (✎) de l'appareil.

Étape 2 Sélectionnez **DHCP** > **Serveur DHCP**.

Étape 3 Sur la page **Serveur**, cliquez sur **Ajouter** et configurez les options suivantes :



- **Interface** : sélectionnez l'interface dans la liste déroulante.

- **Pool d'adresses** : définissez la plage d'adresses IP (de la plus faible à la plus élevée) utilisée par le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et ne peut pas inclure l'adresse IP de l'interface proprement dite.
- **Activer le serveur DHCP** : activez le serveur DHCP sur l'interface sélectionnée.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Enregistrer**.

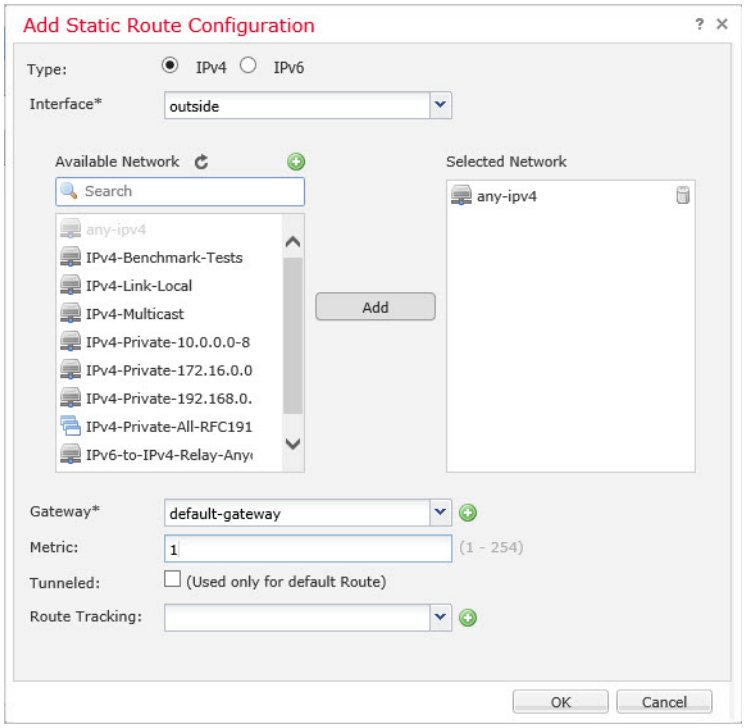
Ajouter la route par défaut

La route par défaut pointe normalement vers le routeur en amont accessible depuis l'interface externe. Si vous utilisez DHCP pour l'interface externe, votre appareil a peut-être déjà reçu une route par défaut. Si vous devez ajouter manuellement la route, procédez comme suit. Si vous avez reçu une route par défaut du serveur DHCP, elle s'affiche dans le tableau **Routes IPv4** ou **Routes IPv6** sur la page **Appareils** > **Gestion des appareils** > **Routage** > **Route statique**.

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** (✎) de l'appareil.

Étape 2 Sélectionnez **Routage** > **Route statique**, cliquez sur **Ajouter une route**, puis définissez les paramètres suivants :

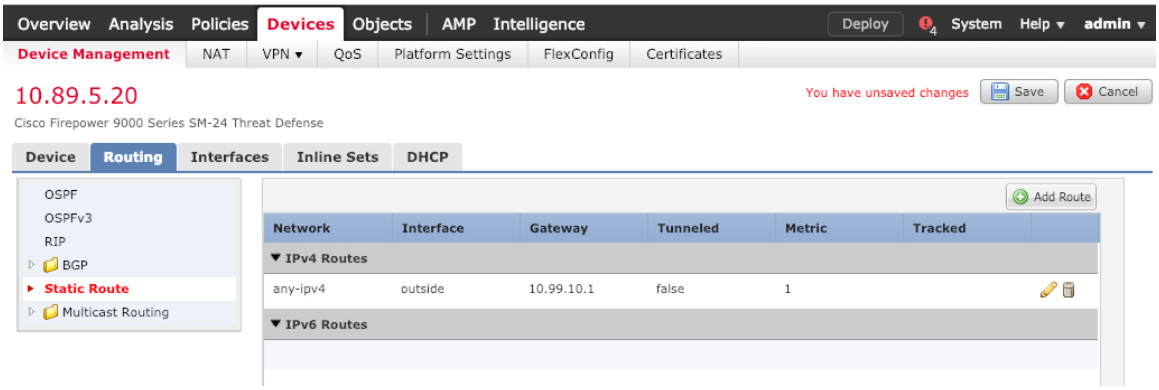


- **Type** : cliquez sur la case d'option **IPv4** ou **IPv6** en fonction du type de route statique que vous ajoutez.

- **Interface** : sélectionnez l'interface de sortie ; il s'agit généralement de l'interface externe.
- **Réseau disponible** : sélectionnez **any-ipv4** pour une route par défaut IPv4 ou **any-ipv6** pour une route par défaut IPv6, puis cliquez sur **Ajouter** pour le déplacer vers la liste **Réseau sélectionné**.
- **Passerelle** ou **Passerelle IPv6** : saisissez ou choisissez le routeur de passerelle correspondant au tronçon suivant pour cette route. Vous pouvez fournir une adresse IP ou un objet Réseaux/Hôtes.
- **Métrique** : saisissez le nombre de tronçons sur le réseau de destination. La plage valide est comprise entre 1 et 255 ; la valeur par défaut est 1.

Étape 3 Cliquez sur **OK**.

La route est ajoutée à la table des routes statiques.



Étape 4 Cliquez sur **Enregistrer**.

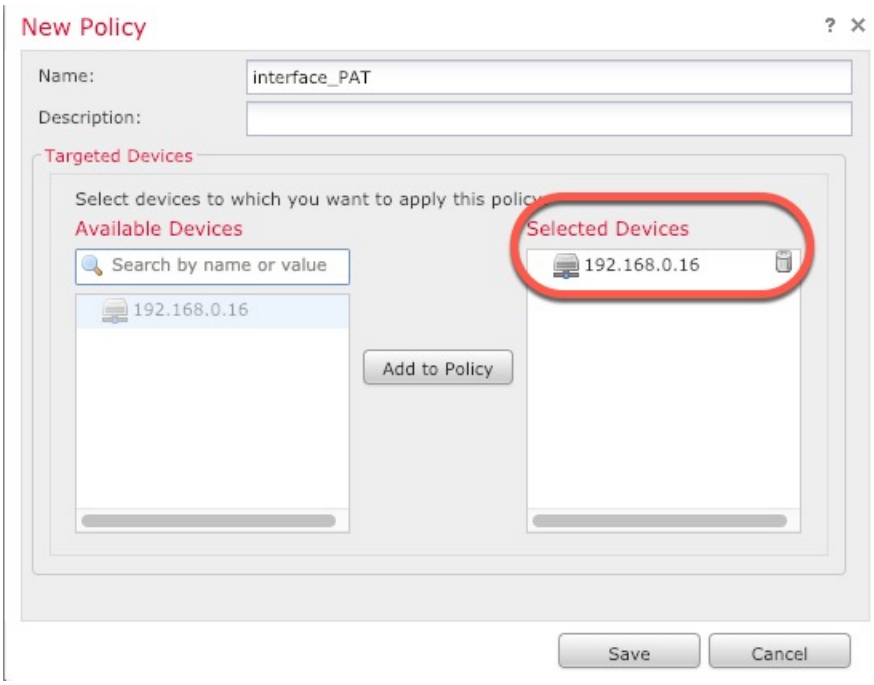
Configuration du routage NAT

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

Procédure

Étape 1 Sélectionnez **Appareils** > **NAT**, puis cliquez sur **Nouvelle politique** > **NAT de protection contre les menaces**.

Étape 2 Donnez un nom à la politique, sélectionnez le ou les appareils que vous souhaitez utiliser, puis cliquez sur **Enregistrer**.



La politique est ajoutée au centre de gestion. Vous devez quand même ajouter des règles à la politique.

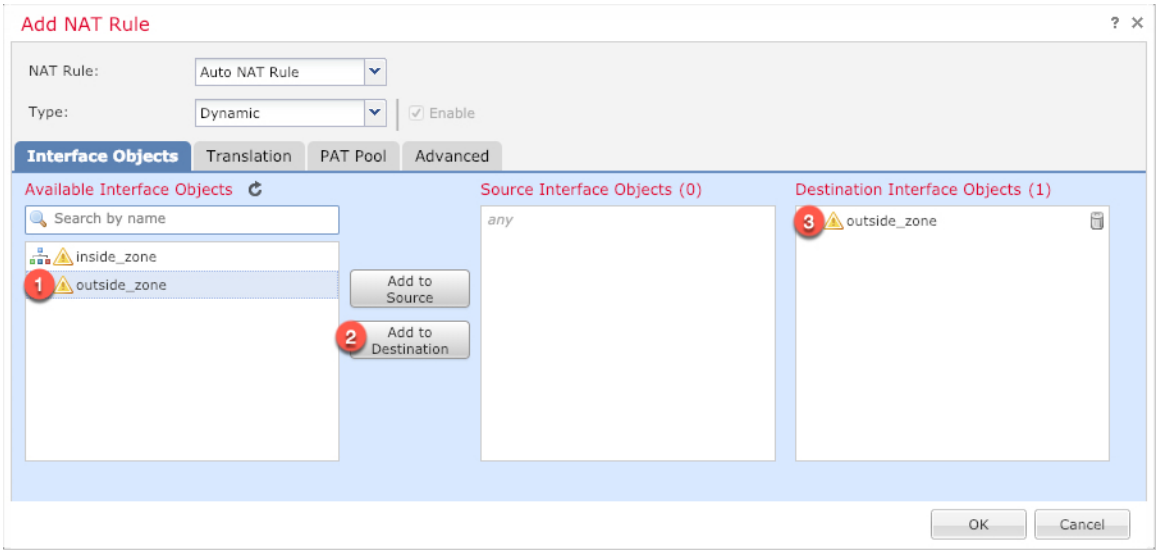
Étape 3 Cliquez sur **Ajouter une règle**.

La boîte de dialogue **Ajouter une règle NAT** apparaît.

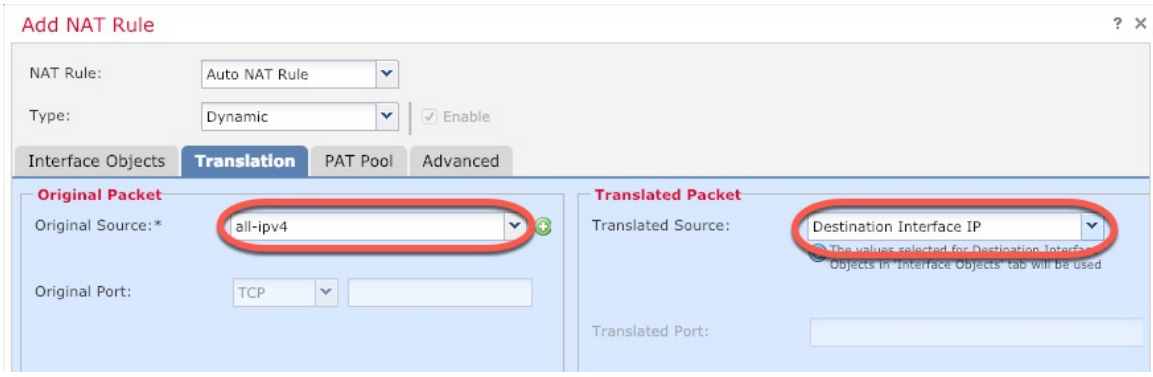
Étape 4 Configurez les options de règle de base :

- **Règle NAT** : sélectionnez **Règle NAT automatique**.
- **Type** : choisissez **Dynamique**.

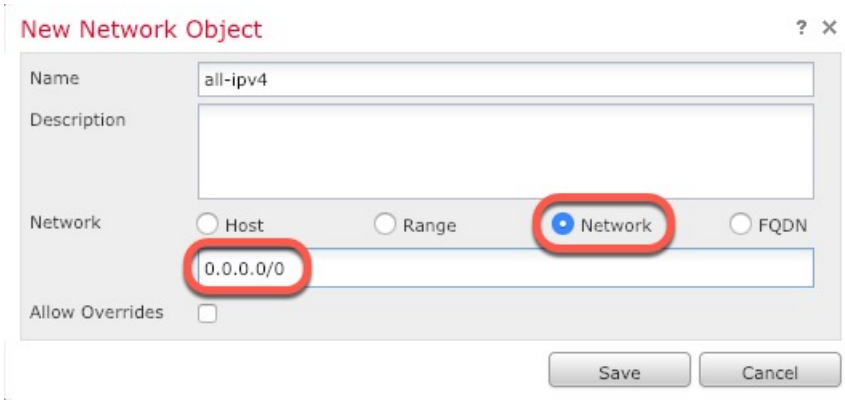
Étape 5 Sur la page **Objets d'interface**, ajoutez la zone externe de la section **Objets d'interface disponibles** à la section **Objets d'interface de destination**.



Étape 6 Sur la page **Traduction**, configurez les options suivantes :



- **Source d'origine** : cliquez sur **Ajouter** (+) pour ajouter un objet réseau pour tout le trafic IPv4 (0.0.0.0/0).

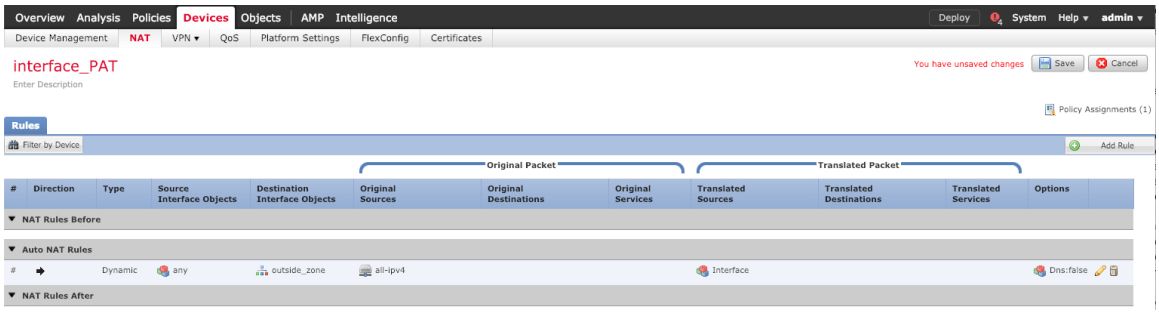


Remarque Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles NAT automatiques ajoutent la fonction NAT à la définition d'objet et vous ne pouvez pas modifier les objets définis par le système.

- **Source traduite** : sélectionnez **Adresse IP de l'interface de destination**.

Étape 7 Cliquez sur **Enregistrer** pour ajouter la règle.

La règle est enregistrée dans la table **Règles**.



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

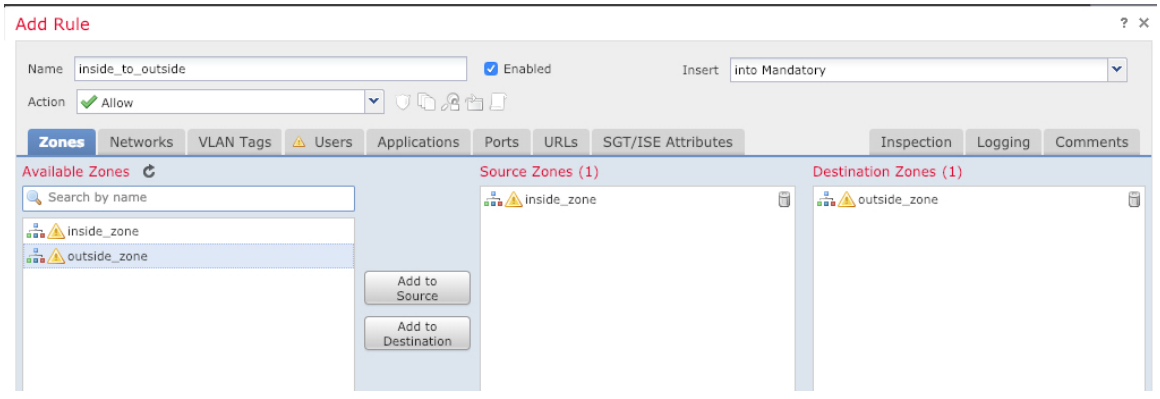
Autoriser le trafic de l'interface interne vers l'interface externe

Si vous avez créé une politique de contrôle d'accès de base **Bloquer tout le trafic** lorsque vous avez enregistré le threat defense, vous devez ajouter des règles à la politique pour autoriser le trafic via l'appareil. La procédure suivante ajoute une règle pour autoriser le trafic de la zone interne vers la zone externe. Si vous disposez d'autres zones, veillez à ajouter des règles autorisant le trafic vers les réseaux appropriés.

Procédure

Étape 1 Sélectionnez **Politique** > **Politique d'accès** > **Politique d'accès**, puis cliquez sur **Modifier** (✎) pour la politique de contrôle d'accès attribuée à threat defense.

Étape 2 Cliquez sur **Ajouter une règle**, puis définissez les paramètres suivants :



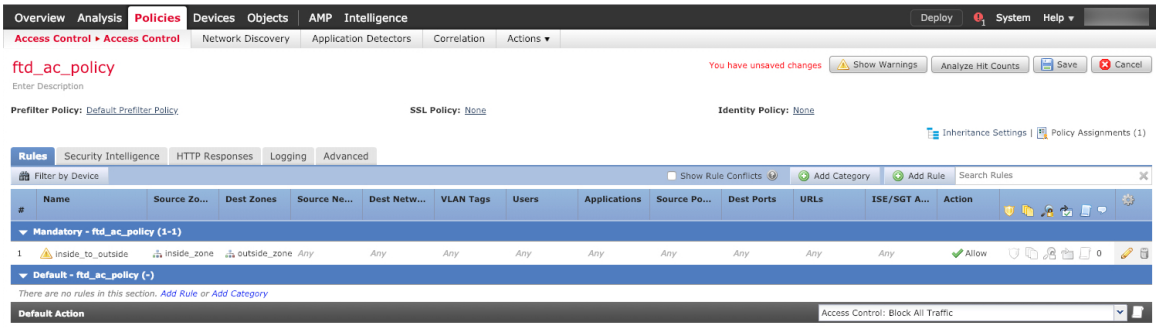
- **Nom** : donnez un nom à cette règle, par exemple **interne_vers_externe**.
- **Zones source** : sélectionnez la zone interne dans **Zones disponibles**, puis cliquez sur **Ajouter à la source**.

- **Zones de destination** : sélectionnez la zone externe dans **Zones disponibles**, puis cliquez sur **Ajouter à la destination**.

Laissez les autres paramètres tels quels.

Étape 3 Cliquez sur **Ajouter**.

La règle est ajoutée au tableau **Règles**.



Étape 4 Cliquez sur **Enregistrer**.

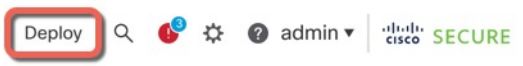
Déployer la configuration

Déployez les modifications de configuration sur le threat defense ; aucune modification n'est active sur l'appareil tant que vous ne l'avez pas déployée.

Procédure

Étape 1 Cliquez sur **Déployer** en haut à droite.

Illustration 9 : Déployer



Étape 2 Cliquez sur **Tout déployer** pour déployer sur tous les périphériques ou cliquez sur **Déploiement avancé** pour déployer sur les périphériques sélectionnés.

Illustration 10 : Tout déployer

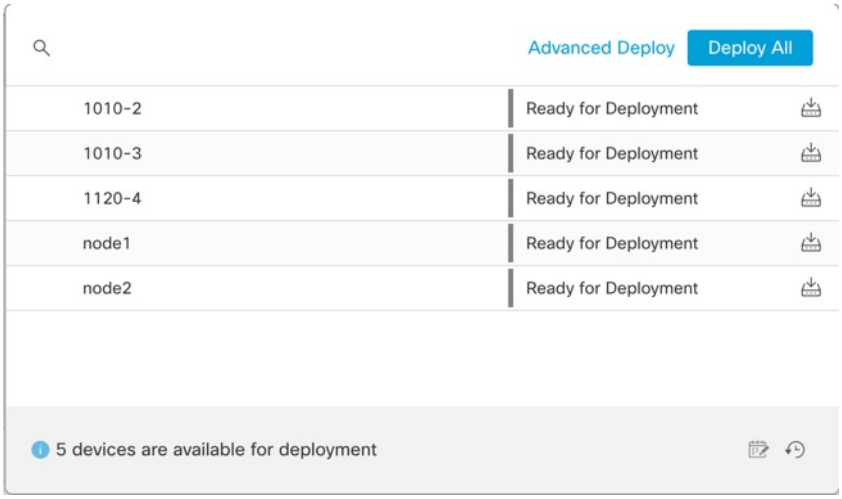
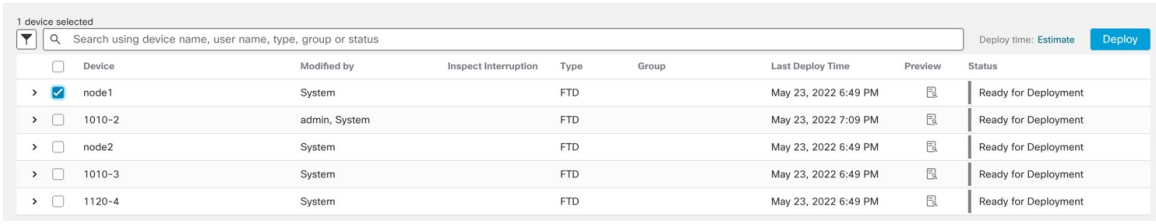
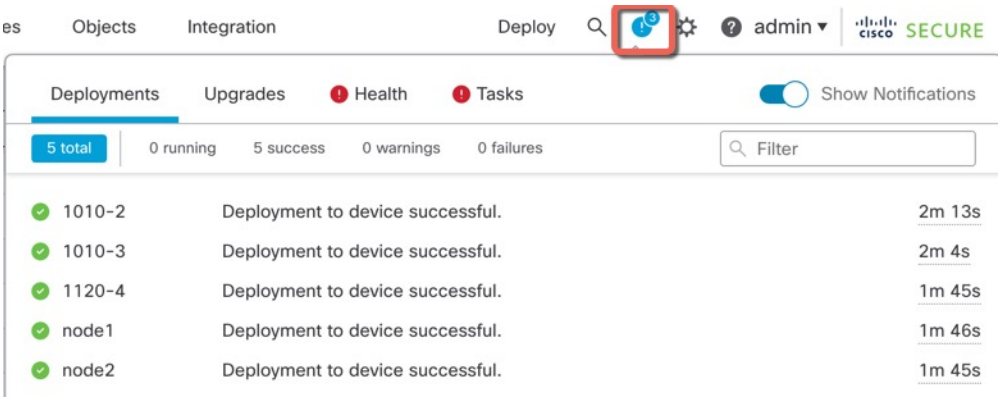


Illustration 11 : Déploiement avancé



Étape 3 Assurez-vous que le déploiement aboutit. Cliquez sur l'icône en regard du bouton **Déployer** dans la barre de menus pour afficher l'état des déploiements.

Illustration 12 : État du déploiement



Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS

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

Vous pouvez également accéder à la CLI FXOS à des fins de dépannage.

Remarque Vous pouvez également vous connecter à l'interface de gestion de l'appareil threat defense. Contrairement à une session de console, la session SSH utilise par défaut l'interface de ligne de commande du threat defense, à partir de laquelle vous pouvez vous connecter à la CLI FXOS à l'aide de la commande **connect fxos**. Vous pourrez 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 console, qui est défini par défaut sur la CLI FXOS.

Procédure

Étape 1 Pour vous connecter à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. L'appareil Firepower 1000 est livré avec un câble série USB A vers B. Veillez à installer les pilotes série USB nécessaires à votre système d'exploitation (consultez le guide matériel de l'appareil Firepower 1010). Le port de console est défini par défaut sur la CLI FXOS. Utilisez les paramètres série suivants :

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

Vous vous connectez à la CLI FXOS. Connectez-vous à l'interface de ligne de commande à l'aide du nom d'utilisateur **admin** et du 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 du threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après vous être connecté, pour obtenir des informations sur les commandes disponibles dans l'interface de ligne de commande, saisissez **help** ou **?**. Pour plus d'informations sur l'utilisation, reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande threat defense, saisissez la commande du **exit** ou **logout**.

Cette commande vous renvoie à l'invite de la CLI FXOS. Pour plus d'informations sur les commandes disponibles dans la CLI FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Mettre le pare-feu hors tension

Il est important que vous arrêtiez correctement votre système. Il ne suffit pas de débrancher le câble d'alimentation, car vous risquez d'endommager gravement le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en arrière-plan en permanence, et que débrancher ou couper l'alimentation ne permet pas un arrêt normal de votre système de pare-feu.

Le châssis initial de l'appareil Firepower 1010 ne possède pas d'interrupteur d'alimentation.Vous pouvez mettre l'appareil hors tension à l'aide de la page de gestion des appareils du centre de gestion ou de l'interface de ligne de commande FXOS.

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

Il est important que vous arrêtiez correctement votre système. Il ne suffit pas de débrancher le câble d'alimentation ou d'appuyer sur l'interrupteur d'alimentation, car vous risquez d'endommager gravement le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en arrière-plan en permanence, et que débrancher ou couper l'alimentation ne permet pas un arrêt normal de votre pare-feu.

Vous pouvez arrêter votre système correctement à l'aide du centre de gestion.

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**.

Étape 2 Cliquez sur l'icône Modifier ( ) en regard de l'appareil que vous souhaitez redémarrer.

Étape 3 Cliquez sur l'onglet **Appareils**.

Étape 4 Cliquez sur l'icône d'arrêt de l'appareil ( ) dans la section **Système**.

Étape 5 Lorsque vous y êtes invité, confirmez que vous souhaitez arrêter l'appareil.

Étape 6 Si vous disposez d'une connexion de console au pare-feu, observez les invites système lorsque le pare-feu s'arrête. L'invite suivante s'affiche :

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

Si vous ne disposez pas d'une connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Étape 7 Vous pouvez désormais débrancher ce dernier pour couper l'alimentation du châssis si nécessaire.

Mettre l'appareil hors tension à l'aide de l'interface de ligne de commande

Vous pouvez utiliser l'interface de ligne de commande FXOS pour arrêter le système en toute sécurité et mettre l'appareil hors tension. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console ; reportez-vous à la rubrique Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 44.

Procédure

Étape 1 Dans la CLI FXOS, connectez-vous à l'interface de gestion locale :

firepower # **connect local-mgmt**

Étape 2 Exécutez la commande **shutdown** :

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

Exemple :

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

Étape 3 Observez les invites du système lorsque le pare-feu s'arrête. L'invite suivante s'affiche :

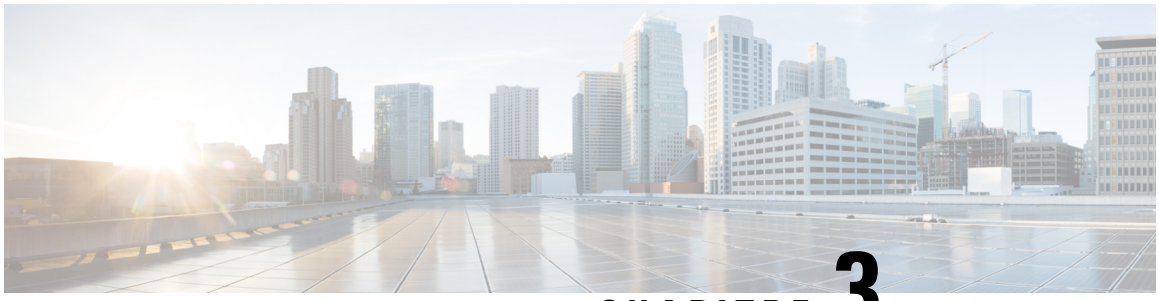
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Étape 4 Vous pouvez désormais débrancher ce dernier pour couper l'alimentation du châssis si nécessaire.

Et après ?

Pour poursuivre la configuration de votre threat defense, consultez les documents disponibles pour votre version logicielle dans Parcourir la documentation de Cisco Firepower.

Pour plus d'informations sur l'utilisation du centre de gestion, reportez-vous à la rubrique Guide de configuration de Firepower Management Center.



CHAPITRE 3

Déployer Threat Defense avec un Centre de gestion distant

Ce chapitre vous concerne-t-il ?

Pour connaître tous les systèmes d'exploitation et gestionnaires disponibles, reportez-vous à la rubrique Quel système d'exploitation et quel gestionnaire vous conviennent le mieux ?, à la page 1. Ce chapitre s'applique au threat defense situé dans une succursale distante qui utilise un centre de gestion installé au siège central.

Chaque threat defense contrôle, inspecte, surveille et analyse le trafic, puis envoie les informations recueillies à un centre de gestion central. Le gestionnaire centre de gestion possède 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 afin de sécuriser votre réseau local.

- Un administrateur du siège central préconfigure le threat defense via l'interface de ligne de commande ou à l'aide du gestionnaire d'appareils, puis envoie le threat defense à la succursale distante.
- L'administrateur de la succursale raccorde les câbles du threat defense et le met sous tension.
- L'administrateur central termine la configuration du threat defense à l'aide du centre de gestion.

Remarque Le déploiement d'une succursale à distance nécessite la version 6.7 ou une version ultérieure.

À propos du pare-feu

L'appareil peut exécuter un logiciel threat defense ou un logiciel ASA. Pour basculer entre threat defense et ASA, vous devez reconfigurer l'appareil. Vous devez également recommencer l'installation si vous avez besoin d'une version logicielle différente de celle actuellement installée. Consultez la rubrique Réinstaller Cisco ASA ou Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé Système d'exploitation Secure Firewall eXtensible (FXOS). Le pare-feu ne prend pas en charge le Gestionnaire de châssis Secure Firewall FXOS ; seule une CLI limitée est prise en charge à des fins de dépannage. Pour obtenir plus d'informations, reportez-vous à la section Guide de dépannage Cisco FXOS pour la série Firepower 1000/2100 exécutant Firepower Threat Defense.

Déclaration de confidentialité—Le pare-feu ne requiert ni ne collecte activement aucune information permettant de vous identifier. Vous pouvez néanmoins utiliser des informations d'identification personnelle

au cours de la configuration, notamment des noms d'utilisateur. Dans ce cas, un administrateur peut accéder à ces informations lors de l'utilisation de la configuration ou de l'utilisation du protocole SNMP.

Mode de fonctionnement de la gestion à distance

Pour permettre au centre de gestion de gérer le threat defense sur Internet, utilisez l'interface externe pour la gestion du centre de gestion plutôt que l'interface de gestion. Dans la mesure où la plupart des succursales distantes ne disposent que d'une seule connexion Internet, l'accès au centre de gestion externe permet une gestion centralisée.

Remarque Vous pouvez utiliser n'*importe quelle* interface de données pour l'accès FMC, par exemple l'interface interne si vous disposez d'un centre de gestion interne. Notez toutefois que ce guide couvre principalement l'accès aux interfaces externes, scénario le plus probable pour les succursales distantes.

L'interface de gestion est une interface spéciale configurée séparément des interfaces de données du threat defense, et possède ses propres paramètres réseau. Les paramètres réseau de l'interface de gestion sont utilisés même si vous activez l'accès au gestionnaire sur une interface de données. L'ensemble du trafic de gestion provient toujours de l'interface de gestion ou est toujours acheminé vers cette interface. Lorsque vous activez l'accès au gestionnaire sur une interface de données, le threat defense transfère le trafic de gestion entrant via le fond de panier à l'interface de gestion. Pour le trafic de gestion sortant, l'interface de gestion transfère le trafic via le fond de panier vers l'interface de données.

L'accès au gestionnaire à partir d'une interface de données présente les limitations suivantes :

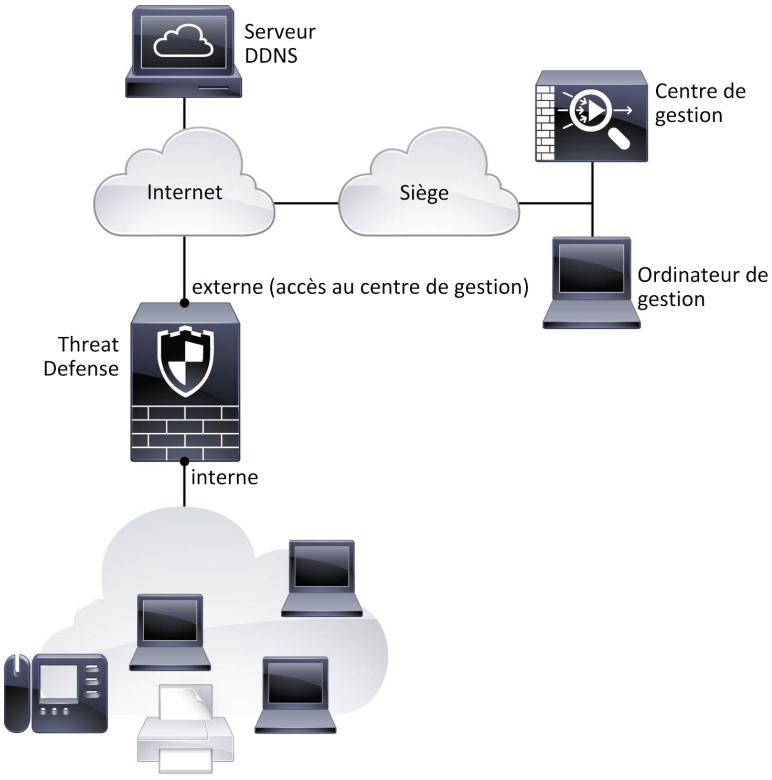
- Vous ne pouvez activer l'accès au gestionnaire que sur une seule interface de données physique. Vous ne pouvez pas utiliser de sous-interface ou EtherChannel.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, à l'aide d'une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI nécessite un protocole PPPoE, vous devrez placer un routeur prenant en charge le protocole PPPoE entre le threat defense et le modem WAN.
- L'interface doit se trouver dans le VRF global uniquement.
- SSH n'est pas activé par défaut pour les interfaces de données. Vous devrez donc activer SSH ultérieurement avec le centre de gestion. Étant donné que la passerelle de l'interface de gestion sera remplacée par les interfaces de données, vous ne pouvez pas non plus accéder à l'interface de gestion depuis 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 illustre le centre de gestion au siège central et le threat defense avec accès au gestionnaire sur l'interface externe.

Le threat defense ou le centre de gestion a besoin d'une adresse IP publique ou d'un nom d'hôte pour autoriser la connexion de gestion entrante ; il est nécessaire que vous connaissiez cette adresse IP pour la configuration initiale. Vous pouvez également configurer le DNS dynamique (DDNS) pour l'interface externe afin de pouvoir modifier les affectations d'adresses IP DHCP.

Illustration 13 :



Avant de commencer

Déployez et effectuez la configuration initiale du centre de gestion. Reportez-vous à la rubrique Guide d'installation matérielle pour Cisco Firepower Management Center 1600, 2600 et 4600 ou Guide de mise en route de Cisco Secure Firewall Management Center Virtual.

Procédure de bout en bout

Reportez-vous aux tâches suivantes pour déployer le threat defense avec le centre de gestion sur votre châssis.

Illustration 14 : Procédure de bout en bout

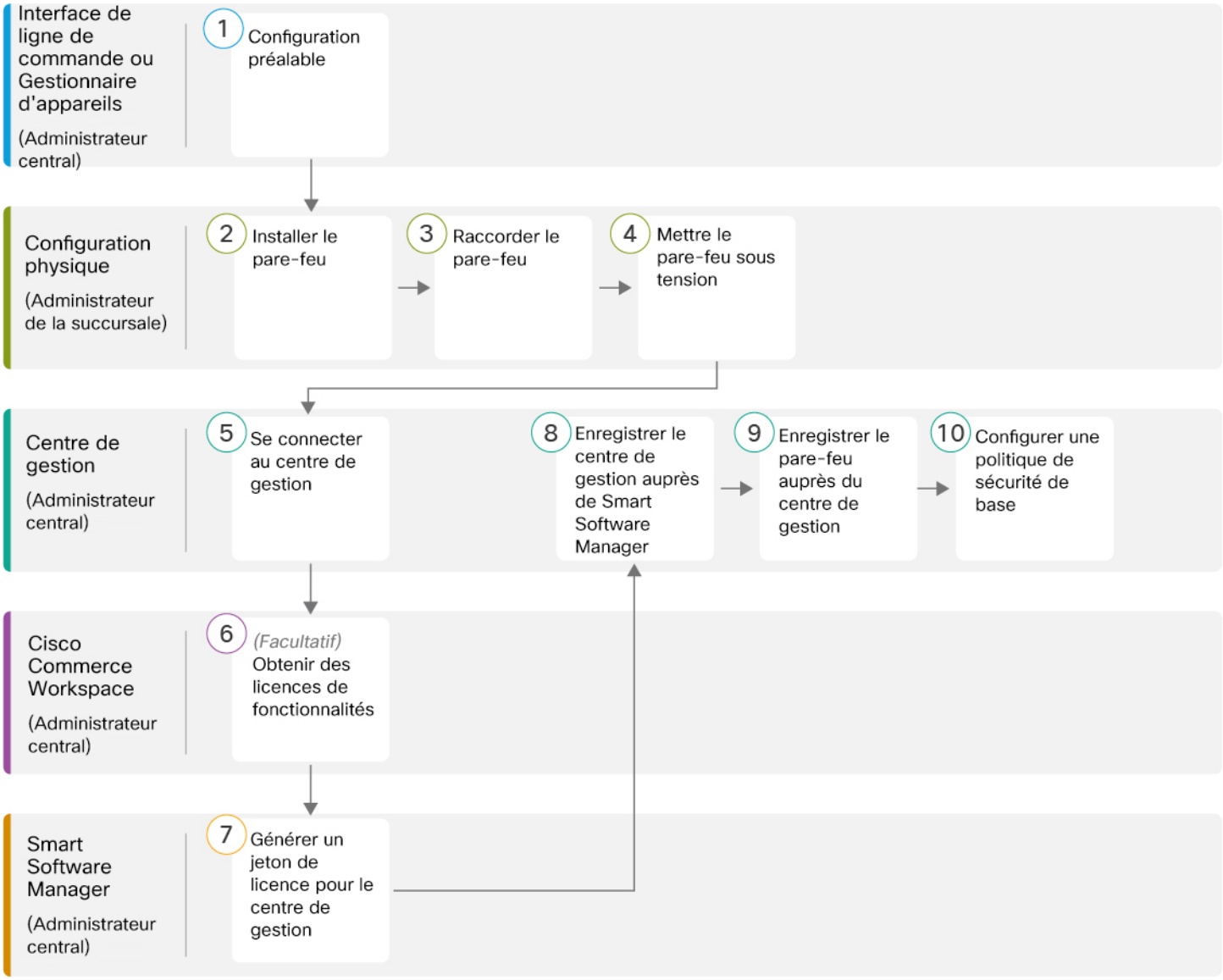


Illustration 15 : Procédure de bout en bout

1	Interface de ligne de commande ou Gestionnaire d'appareils (Administrateur central)	• (Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 54 • Effectuer la configuration préalable à l'aide de l'interface de ligne de commande, à la page 61 • Effectuer la configuration préalable à l'aide du Gestionnaire d'appareils, à la page 55

2	Configuration physique (Administrateur de la succursale)	Installez le pare-feu. Reportez-vous au guide d'installation matérielle.
3	Configuration physique (Administrateur de la succursale)	Raccorder le pare-feu, à la page 66.
4	Configuration physique (Administrateur de la succursale)	Mettre l'appareil sous tension, à la page 67
5	Centre de gestion (Administrateur central)	Administrateur central : Se connecter au Centre de gestion, à la page 24.
6	Cisco Commerce Workspace (Administrateur central)	Obtenir les licences pour le Centre de gestion, à la page 69 : acheter des licences de fonctionnalités.
7	Smart Software Manager (Administrateur central)	Obtenir les licences pour le Centre de gestion, à la page 69 : générer un jeton de licence pour le centre de gestion.
8	Centre de gestion (Administrateur central)	Obtenir les licences pour le Centre de gestion, à la page 69 : enregistrer le centre de gestion sur Smart Licensing Server.
9	Centre de gestion (Administrateur central)	Enregistrer le Threat Defense auprès du Centre de gestion, à la page 70.
10	Centre de gestion (Administrateur central)	Configurer une politique de sécurité de base, à la page 73.

Configuration préalable de l'administrateur central

Vous devez préconfigurer manuellement le threat defense 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 autre version, 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 en regard du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de publication décrite dans la rubrique 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. Pour plus d'informations, reportez-vous à la rubrique Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 84. Cette procédure illustre l'utilisation du port de console, mais vous pouvez utiliser SSH si vous le souhaitez.

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

Vous vous connectez à la CLI FXOS. Lors de la première connexion, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si vous avez modifié le mot de passe, mais que vous l'avez oublié, vous devez réinitialiser l'appareil pour rétablir le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure pour rétablir les paramètres 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 Dans l'interface de ligne de commande de la console FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

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

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

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

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, reportez-vous à la rubrique Effectuer la configuration préalable à l'aide de l'interface de ligne de commande, à la page 61. Par défaut, l'interface de gestion utilise DHCP.

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

b) Suivez la procédure de réinstallation du guide de dépannage de la console FXOS.

Effectuer la configuration préalable à l'aide du Gestionnaire d'appareils

Connectez-vous au gestionnaire d'appareils pour effectuer la configuration initiale du threat defense. Lorsque vous effectuez la configuration initiale à l'aide du gestionnaire d'appareils, *toutes* les configurations d'interface effectuées dans le gestionnaire d'appareils sont conservées lorsque vous passez au centre de gestion pour la gestion, en plus des paramètres d'interface de gestion et 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 de l'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 du centre de gestion. Reportez-vous à la section Guide d'installation matérielle pour Cisco Firepower Management Center 1600, 2600 et 4600. Vous devez connaître l'adresse IP ou le nom d'hôte du centre de gestion avant de configurer le threat defense.
- Utilisez une version actuelle de Firefox, Chrome, Safari, Edge ou Internet Explorer.

Procédure

Étape 1 Connectez votre ordinateur de gestion à l'interface interne (Ethernet1/2 à 1/8) interne.

Étape 2 Mettez le pare-feu sous tension.

Remarque La première fois que vous démarrez le threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Étape 3 Connectez-vous au gestionnaire d'appareils.

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 êtes invité à lire et à accepter le contrat de licence de l'utilisateur final et à modifier le mot de passe admin.

Étape 4 Utilisez l'assistant de configuration lors de votre première connexion au gestionnaire d'appareils pour terminer la configuration initiale. Vous pouvez éventuellement ignorer l'assistant de configuration en cliquant sur **Ignorer la configuration de l'appareil** au bas de la page.

Une fois l'assistant de configuration terminé, outre la configuration par défaut de l'interface interne (Ethernet 1/2 à 1/8, qui sont des ports de commutateur sur le VLAN1), la configuration d'une interface externe (Ethernet 1/1) sera conservée lorsque vous passerez à la gestion du centre de gestion.

a) Configurez les options suivantes pour les interfaces externes et de gestion, puis cliquez sur **Suivant**.

1. **Adresse de l'interface externe** : 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 de l'appareil. La première interface de données est l'interface externe par défaut.

   Si vous souhaitez utiliser une interface différente depuis l'interface externe (ou interne) pour l'accès au gestionnaire, vous devez la configurer manuellement après avoir terminé l'assistant de configuration.

   Configurer IPv4 : adresse IPv4 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. Le protocole PPPoE peut être nécessaire si l'interface est connectée à un modem ADSL, un modem câble ou une autre connexion à votre FAI et que votre FAI utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE après avoir terminé l'assistant.

   Configurer IPv6 : adresse IPv6 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv6.

2. **Interface de gestion**

   Les paramètres de l'interface de gestion ne sont pas visibles si vous avez effectué la configuration initiale dans l'interface de ligne de commande.

   Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès au gestionnaire sur une interface de données. Par exemple, le trafic de gestion acheminé vers le fond de panier via l'interface de données résout les noms de domaine complets à l'aide des serveurs DNS de l'interface de gestion, et non des serveurs DNS de l'interface de données.

   Serveurs DNS : serveur DNS pour l'adresse de gestion du système. Saisissez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. La valeur par défaut est Serveurs DNS publics OpenDNS. Si vous modifiez les champs et souhaitez rétablir les paramètres par défaut, cliquez sur **Utiliser OpenDNS** pour recharger les adresses IP appropriées dans les champs.

   Nom d'hôte du pare-feu : nom d'hôte de l'adresse de gestion du système.

b) Configurez les **Paramètres relatifs au temps (NTP)** et cliquez sur **Suivant**.

1. **Fuseau horaire** : sélectionnez le fuseau horaire du système.
2. **Serveur de temps NTP** : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

c) Sélectionnez **Démarrer la période d'évaluation de 90 jours sans enregistrement**.

N'enregistrez pas le threat defense auprès de Smart Software Manager ; toutes les licences sont octroyées sur le centre de gestion.

d) Cliquez sur **Terminer**.
e) Vous êtes invité à sélectionner **Gestion du cloud** ou **Autonome**. Pour la gestion du centre de gestion, sélectionnez **Autonome**, puis **J'ai compris**.

Étape 5 (Peut être obligatoire) Configurez l'interface de gestion. Reportez-vous à l'interface de gestion sur **Appareil** > **Interfaces**.

La passerelle doit être définie sur les interfaces de données de l'interface de gestion. 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 utilise par défaut les interfaces de données et vous n'avez rien à configurer. Si vous avez reçu une passerelle de DHCP, vous devez configurer cette interface avec une adresse IP statique et définir la passerelle sur les interfaces de données.

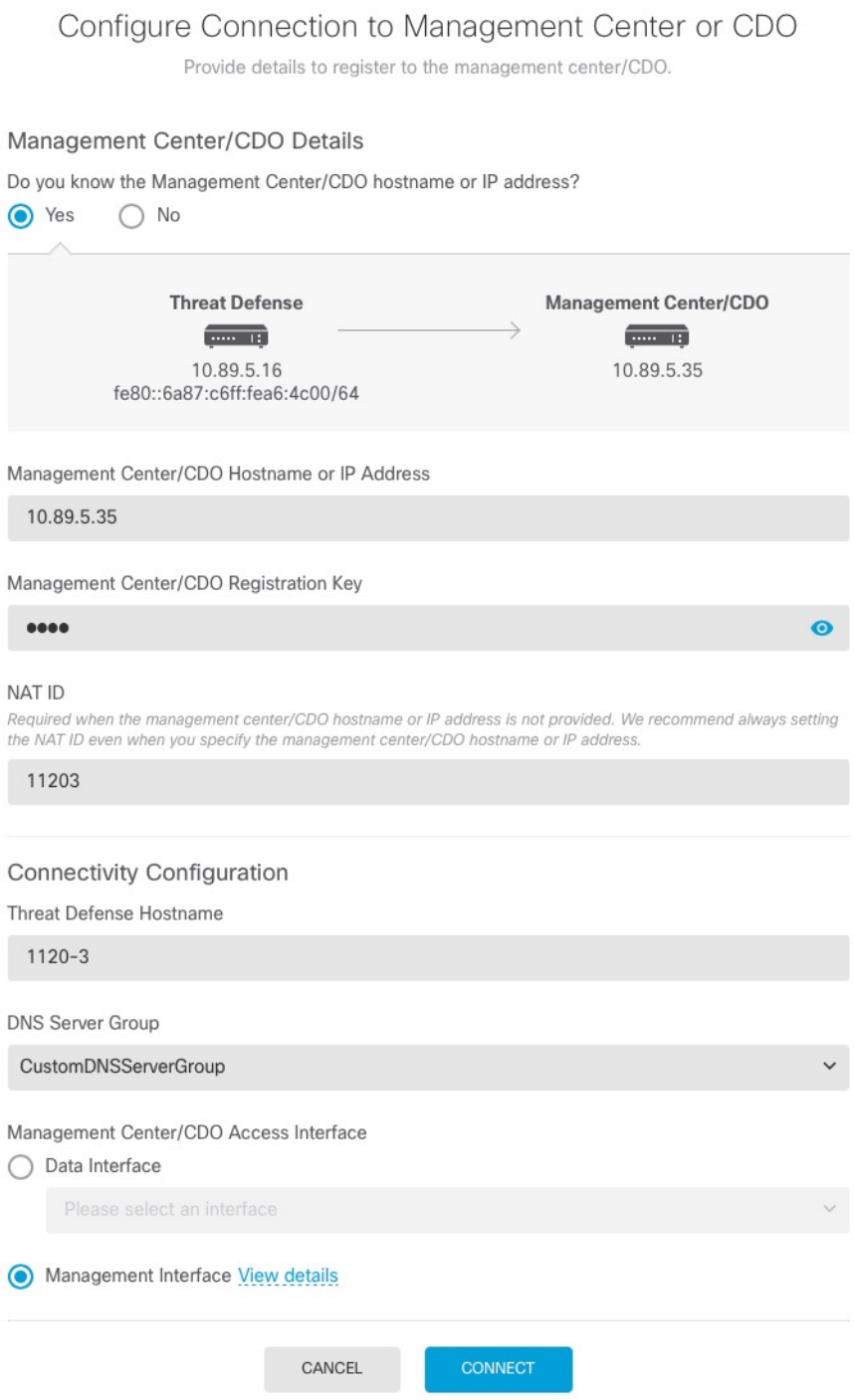
Étape 6 Si vous souhaitez configurer des interfaces supplémentaires, notamment une interface autre que l'interface externe ou interne que vous souhaitez utiliser pour l'accès au gestionnaire sélectionnez **Appareil**, puis cliquez sur le lien dans le récapitulatif **Interfaces**.

Reportez-vous à la rubrique Configurer le pare-feu dans le Gestionnaire d'appareils, à la page 113 pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareils. Les autres configurations du gestionnaire d'appareils ne sont pas conservées lorsque vous enregistrez l'appareil auprès du centre de gestion.

Étape 7 Sélectionnez **Appareil** > **Paramètres système** > **Centre de gestion**, et cliquez sur **Continuer** pour configurer la gestion du centre de gestion.

Étape 8 Configurer le **Centre de gestion/Détails du CDO**.

Illustration 16 : Détails du centre de gestion/CDO



a) Pour le champ **Connaissez-vous le nom d'hôte ou l'adresse IP du Centre de gestion/CDO**, cliquez sur **Oui** si vous pouvez accéder au centre de gestion à l'aide d'une adresse IP ou d'un nom d'hôte, ou sur **Non** si le centre de gestion est derrière la NAT ou n'a pas d'adresse IP ou de nom d'hôte public.

Au moins l'un des appareils, soit le centre de gestion soit le threat defense, doit disposer d'une adresse IP accessible pour établir le canal de communication bidirectionnel chiffré SSL entre les deux appareils.

b) Si vous avez choisi **Oui**, saisissez le **Nom d'hôte/adresse IP du Centre de gestion/CDO**.

c) Spécifiez la **Clé d'enregistrement du Centre de gestion/CDO**.

Cette clé est une clé d'enregistrement unique de votre choix, que vous devez également spécifier sur le centre de gestion lorsque vous enregistrez l'appareil threat defense. La clé d'enregistrement ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le trait d'union (-). Il est possible d'utiliser cet ID pour plusieurs appareils qui s'enregistrent auprès du centre de gestion.

d) Spécifiez un **ID NAT**.

Cet ID est une chaîne unique de votre choix, que vous spécifiez également sur le centre de gestion. Ce champ est obligatoire si vous spécifiez uniquement l'adresse IP sur l'un des appareils ; nous vous recommandons cependant de spécifier l'ID NAT même si vous connaissez les adresses IP des deux appareils. L'ID NAT ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le trait d'union (-). Il est *impossible* d'utiliser cet ID pour d'autres appareils enregistrés auprès du centre de gestion. L'ID NAT est utilisé en combinaison avec l'adresse IP pour vérifier que la connexion provient de l'appareil correct ; ce n'est qu'après l'authentification de l'adresse IP/ID NAT que la clé d'enregistrement est vérifiée.

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

a) Spécifiez le **nom d'hôte du FTD**.

Ce nom de domaine complet sera utilisé pour l'interface externe ou l'interface choisie pour l'**interface d'accès au centre de gestion/CDO**.

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

Sélectionnez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNSServerGroup** et inclut 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 DNS de données est utilisé pour le DDNS (s'il est configuré) ou pour les politiques de sécurité appliquées à cette interface. Vous devrez probablement 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 via 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 attribuez à ce threat defense. Lorsque vous ajoutez le threat defense au centre de gestion, le paramètre local est conservé et les serveurs DNS ne sont *pas* ajoutés à une politique Paramètres de la plateforme. Toutefois, si vous attribuez ultérieurement une politique Paramètres de la plateforme au threat defense qui inclut une configuration DNS, cette configuration remplace 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 threat defense.

En outre, les serveurs DNS locaux ne sont conservés par le centre de gestion que si les serveurs DNS ont été détectés lors de l'enregistrement initial.

c) Pour l'**interface d'accès au centre de gestion/CDO**, choisissez **externe**.

Bien que vous puissiez choisir n'importe quelle interface configurée, dans ce guide nous supposons que vous utilisez une interface externe.

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

Un message s'affiche vous demandant de vérifier que vous disposez d'une route par défaut via l'interface. Si vous avez choisi une interface extérieure, 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 la rubrique Configurer le pare-feu dans le Gestionnaire d'appareils, à la page 113 pour plus d'informations sur la configuration des routes statiques dans le gestionnaire d'appareils.

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

DDNS garantit que le centre de gestion peut atteindre le threat defense à son nom de domaine complet (FQDN) si l'adresse IP du threat defense change. Accédez à **Appareil** > **Paramètres système** > **Service DDNS** pour configurer DDNS.

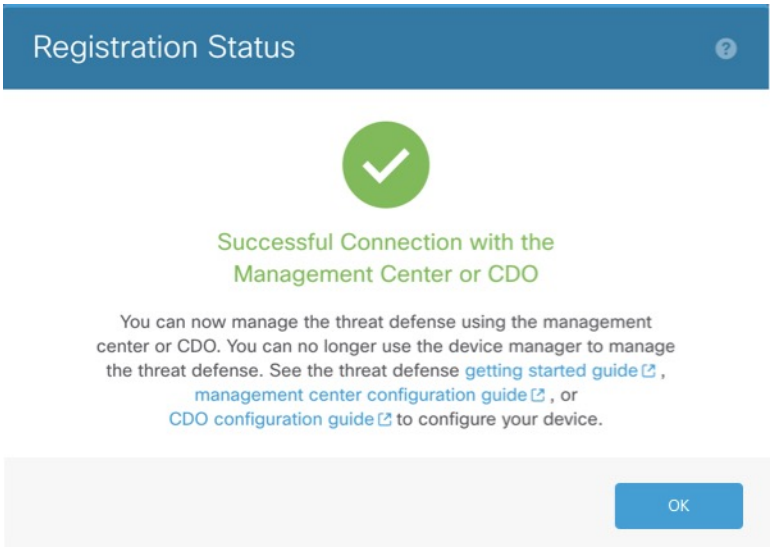
Si vous configurez DDNS avant d'ajouter le threat defense au centre de gestion, le threat defense ajoute automatiquement des certificats pour toutes les autorités de certification principales du bundle Autorités de certification racines approuvées par Cisco afin que le threat defense puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le threat defense FTD prend en charge tout serveur DDNS qui utilise la spécification de l'API distante DynDNS (https://help.dyn.com/remote-access-api/).

Étape 12 Cliquez sur **Connecter**. La boîte de dialogue **État d'enregistrement** affiche l'état actuel du commutateur sur le centre de gestion. Après l'étape **Sauvegarde des paramètres d'enregistrement du centre de gestion/CDO**, accédez au centre de gestion, et ajoutez le pare-feu.

Si vous souhaitez annuler le basculement sur centre de gestion, cliquez sur **Annuler l'enregistrement**. Sinon, ne fermez pas la fenêtre du navigateur gestionnaire d'appareils avant d'avoir terminé l'étape **Sauvegarde des paramètres d'enregistrement du centre de gestion/CDO**. Dans le cas contraire, le processus sera interrompu et ne reprendra que lorsque vous vous reconnecterez au gestionnaire d'appareils.

Si vous restez connecté au gestionnaire d'appareils après l'étape **Sauvegarde de l'enregistrement des paramètres du centre de gestion/CDO**, la boîte de dialogue **Connexion réussie avec le centre de gestion ou le CDO** finit par d'afficher, puis vous êtes déconnecté du gestionnaire d'appareils.

Illustration 17 : Connexion réussie



Effectuer la configuration préalable à l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande du threat defense 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'appareils (7.1 et versions ultérieures), *toutes* les configurations d'interface effectuées dans le gestionnaire d'appareils sont conservées lorsque vous passez au centre de gestion pour la gestion, en plus des paramètres d'interface de gestion et d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès, ne sont pas conservés.

Avant de commencer

Déployez et effectuez la configuration initiale du centre de gestion. Reportez-vous à la section Guide d'installation matérielle pour Cisco Firepower Management Center 1600, 2600 et 4600. Vous devez connaître l'adresse IP ou le nom d'hôte du centre de gestion avant de configurer le threat defense.

Procédure

Étape 1 Mettez le pare-feu sous tension.

Remarque La première fois que vous démarrez le threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Étape 2 Connectez-vous à l'interface de ligne de commande du threat defense sur le port de console.

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

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

Lors de la première connexion au FXOS, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez reconfigurer l'appareil pour réinitialiser le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure de réinstallation.

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 du threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 5 La première fois que vous vous connectez à threat defense, vous êtes invité à accepter le contrat de licence de l'utilisateur final (CLUF) et, si vous utilisez une connexion SSH, à modifier le mot de passe administrateur. Vous accédez ensuite au script de configuration de l'interface de ligne de commande pour les paramètres de l'interface de gestion.

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

Remarque Vous ne pouvez pas répéter l'assistant de configuration de la CLI à moins d'avoir effacé la configuration, par exemple, via une réinitialisation. Vous pouvez cependant modifier tous les paramètres ultérieurement dans l'interface de ligne de commande à l'aide des commandes **configure network**. Reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

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

Reportez-vous aux instructions suivantes :

- **Configurer IPv4 via DHCP ou manuellement ?**—Sélectionnez **manuel**. Même si vous n'avez pas l'intention d'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 route par défaut, qui doit être **data-interfaces** (reportez-vous au point suivant), peut être remplacée par une autre envoyée par le serveur DHCP.
- **Saisissez la passerelle IPv4 par défaut pour l'interface de gestion** : définissez la passerelle sur **data-interfaces**. Ce paramètre transfère le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé via l'interface de données d'accès au gestionnaire.
- **Si vos informations réseau ont changé, vous devrez vous reconnecter** : si vous êtes connecté à 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 suite à la modification de la route par défaut (via les interfaces de données). Les connexions de console restent actives.
- **Gérer l'appareil localement ?** : saisissez **non** pour utiliser le centre de gestion. Si vous saisissez **oui**, vous utilisez le gestionnaire d'appareils.
- **Configurer le mode pare-feu ?** : saisissez **routé**. L'accès au gestionnaire externe est uniquement pris en charge 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 externe pour l'accès au gestionnaire.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base de l'interface externe. Consultez les informations suivantes 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 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**, cette commande la définit maintenant.

- Lorsque vous ajoutez le threat defense au centre de gestion, le centre de gestion détecte et conserve la configuration de l'interface, notamment les paramètres suivants : nom et adresse IP de l'interface, route statique vers la passerelle, serveurs DNS et serveur DDNS. Pour en savoir plus sur la configuration du serveur DNS, reportez-vous à la rubrique ci-dessous. Dans le centre de gestion, vous pouvez modifier ultérieurement la configuration de l'interface d'accès FMC, mais assurez-vous de ne pas apporter de modifications susceptibles d'empêcher le threat defense ou le centre de gestion de rétablir la connexion de gestion. Si la connexion de gestion est interrompue, le threat defense inclut la commande **configure policy rollback** permettant de restaurer le déploiement précédent.
- Si vous configurez une URL de mise à jour du serveur DDNS, le threat defense ajoute automatiquement des certificats pour toutes les autorités de certification principales du bundle Autorités de certification racines approuvées par Cisco afin que le threat defense puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le threat defense FTD prend en charge tout serveur DDNS qui utilise la spécification de l'API distante DynDNS (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 avez défini avec le script de configuration (ou à l'aide de la commande **configure network dns servers**) est utilisé pour le trafic de gestion. Le serveur DNS de données est utilisé pour le DDNS (s'il est configuré) ou pour les politiques de sécurité appliquées 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 attribuez à ce threat defense. Lorsque vous ajoutez le threat defense au centre de gestion, le paramètre local est conservé et les serveurs DNS ne sont *pas* ajoutés à une politique Paramètres de la plateforme. Toutefois, si vous attribuez ultérieurement une politique Paramètres de la plateforme au threat defense qui inclut une configuration DNS, cette configuration remplace 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 threat defense.

  En outre, les serveurs DNS locaux ne sont conservés par le centre de gestion que si les serveurs DNS ont été détectés lors de l'enregistrement initial. Par exemple, si vous avez enregistré l'appareil à l'aide de l'interface de gestion, mais que vous avez ensuite configuré une interface de données à l'aide de la commande **configure network management-data-interface**, vous devez configurer manuellement tous ces paramètres dans le centre de gestion y compris les serveurs DNS, pour qu'ils correspondent à la configuration du threat defense.
- Vous pouvez modifier l'interface de gestion après avoir enregistré le threat defense auprès du centre de gestion, soit en tant qu'interface de gestion, soit en tant qu'interface de données.
- Le nom de domaine complet que vous avez défini dans l'assistant de configuration est utilisé pour cette interface.
- Vous pouvez effacer la totalité de la configuration de l'appareil via cette commande ; vous pouvez utiliser cette option dans un scénario de récupération, mais nous vous déconseillons de l'utiliser pour la configuration initiale ou le fonctionnement normal.
- Pour désactiver la gestion des données, saisissez 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 de l'interface de données au centre de gestion sur un réseau spécifique.

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

Par défaut, tous les réseaux sont autorisés.

Étape 8 Identifiez le centre de gestion qui gérera ce threat defense.

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 du centre de gestion. Si le centre de gestion n'est pas directement adressable, utilisez **DONTRESOLVE**. Au moins l'un des appareils, soit le centre de gestion soit le threat defense, doit disposer d'une adresse IP accessible pour établir le canal de communication bidirectionnel chiffré SSL entre les deux appareils. Si vous spécifiez **DONTRESOLVE** dans cette commande, le threat defense doit disposer d'une adresse IP ou d'un nom d'hôte accessible.
- *reg_key* : spécifie une clé d'enregistrement unique de votre choix, que vous devez également spécifier sur le centre de gestion lors de l'enregistrement du threat defense. La clé d'enregistrement ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le trait d'union (-).
- *nat_id* : spécifie la chaîne unique de votre choix, que vous spécifiez également sur le centre de gestion. Lorsque vous utilisez une interface de données pour la gestion, vous devez spécifier l'ID NAT sur *le threat defense et le centre de gestion* pour l'enregistrement. L'ID NAT ne doit pas comporter plus de 37 caractères. Les caractères valides incluent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le

trait d'union (-). Il est impossible d'utiliser cet ID pour d'autres appareils enregistrés auprès du centre de gestion.

Exemple :

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

Étape 9 Arrêtez le threat defense pour pouvoir envoyer l'appareil à la succursale distante.

Il est important que vous arrêtiez correctement votre système. Il ne suffit pas de débrancher le câble d'alimentation ou d'appuyer sur l'interrupteur d'alimentation, car vous risquez d'endommager gravement le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en arrière-plan en permanence, et que débrancher ou couper l'alimentation ne permet pas un arrêt normal de votre système.

a) Saisissez la commande **shutdown**.
b) Observez les voyants d'alimentation et d'état pour vérifier que le châssis est hors tension (ils doivent être éteints).
c) Une fois le châssis hors tension, vous pouvez le débrancher pour couper l'alimentation si nécessaire.

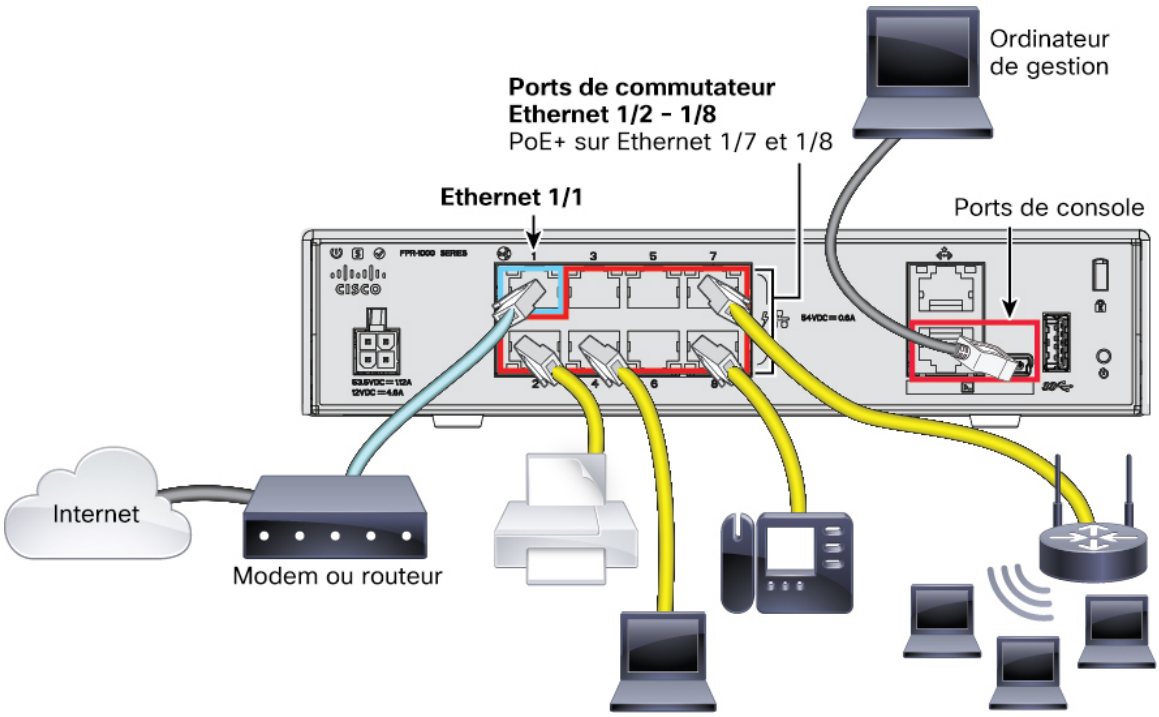
Installation dans une succursale

Une fois que vous avez reçu le pare-feu threat defense du siège social, il vous suffit de le raccorder et de le mettre sous tension en vue de le connecter à Internet depuis l'interface externe. L'administrateur central peut alors terminer la configuration.

Raccorder le pare-feu

Le centre de gestion et votre ordinateur de gestion se trouvent sur un site distant et peuvent accéder au threat defense via Internet. Pour raccorder l'appareil Firepower 1010, procédez comme suit.

Illustration 18 : Raccorder un déploiement de gestion à distance



Procédure

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

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

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

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

Dans la succursale, la connexion à la console n'est pas nécessaire pour une utilisation quotidienne ; elle peut cependant être nécessaire à des fins de 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 threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Avant de commencer

Il est important que vous utilisiez une source d'alimentation fiable pour alimenter votre appareil (à l'aide d'un système d'alimentation sans coupure, par exemple). Une panne de courant sans arrêt préalable peut endommager

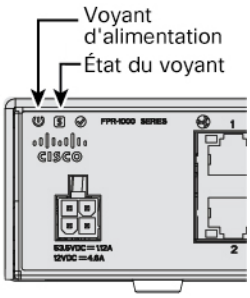
gravement le système de fichiers. De nombreux processus s'exécutent en arrière-plan en permanence, et une panne de courant ne permet pas l'arrêt normal de votre système.

Procédure

Étape 1 Raccordez le câble d'alimentation à l'appareil et branchez-le à une prise électrique.

L'appareil se met automatiquement sous tension dès que vous le branchez.

Étape 2 Observez le voyant d'alimentation situé à l'arrière de l'appareil. S'il est allumé en vert, l'appareil est sous tension.



Étape 3 Observez le voyant d'état à l'arrière ou sur l'appareil. Lorsqu'il s'allume en vert, le système a terminé les diagnostics de mise sous tension.

Configuration postérieure de l'administrateur central

Dès que l'administrateur de la succursale distante a câblé le threat defense pour qu'il dispose d'un accès Internet depuis l'interface externe, vous pouvez enregistrer le threat defense sur le centre de gestion et terminer la configuration de l'appareil.

Se connecter au Centre de gestion

Utilisez le centre de gestion pour configurer et surveiller le threat defense.

Avant de commencer

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

Procédure

Étape 1 À l'aide d'un navigateur pris en charge, saisissez 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**.

Obtenir les licences pour le Centre de gestion

Toutes les licences sont fournies au threat defense via le centre de gestion. Vous pouvez éventuellement acheter les licences de fonctionnalités suivantes :

- **Menace** : sécurité adaptative et système de prévention des intrusions de nouvelle génération
- **Malware** : protection contre les programmes malveillants
- **URL** : filtrage des URL
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN uniquement

Pour une présentation complète de Cisco Licensing, rendez-vous sur cisco.com/go/licensingguide.

Avant de commencer

- Veillez à disposer d'un compte principal sur Smart Software Manager.

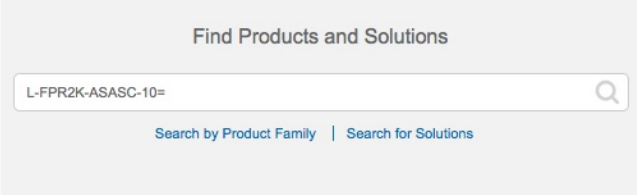
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre entreprise.
- Votre compte Smart Software Licensing doit bénéficier de la licence de chiffrement renforcé (3DES/AES) pour utiliser certaines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

Procédure

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

Si vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte Smart Software License. Toutefois, si vous devez ajouter des licences vous-même, utilisez le champ de recherche **Rechercher des produits et des solutions** de Cisco Commerce Workspace. Recherchez les PID de licence suivants :

Illustration 19 : Recherche de licences



Remarque Si aucun PID n'est renvoyé, vous pouvez l'ajouter manuellement à votre commande.

- Combinaison des licences Threat, Malware et URL :
  - L-FPR1010T-TMC=

Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée limitée correspondant à l'un des PID suivants :

- L-FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

- VPN RA : consultez le Guide d'aide à la commande Cisco AnyConnect.

Étape 2 Si cela n'est pas déjà fait, enregistrez le centre de gestion auprès du gestionnaire Smart Software Manager.

Pour cela, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Consultez le Guide de configuration de centre de gestion pour obtenir des instructions supplémentaires. Pour utiliser la fonction LTP, vous devez activer l'option **Assistance cloud pour LTP**, pendant ou après l'enregistrement auprès de Smart Software Manager. Consultez la page **Système** > **Licences** > **Licences Smart**.

Enregistrer le Threat Defense auprès du Centre de gestion

Enregistrez le threat defense auprès du centre de gestion.

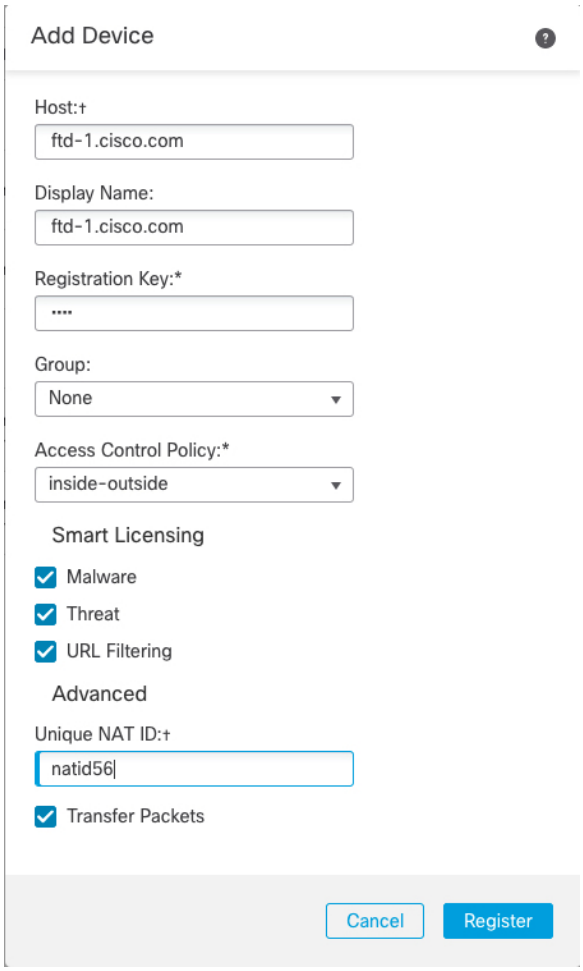
Avant de commencer

- Collectez les informations suivantes que vous avez définies dans la configuration initiale du threat defense :
  - Adresse IP de gestion ou nom d'hôte du threat defense, et ID NAT
  - Clé d'enregistrement du centre de gestion

Procédure

Étape 1 Dans centre de gestion, sélectionnez **Appareils** > **Gestion des appareils**.

Étape 2 Dans la liste déroulante **Ajouter**, sélectionnez **Ajouter l'appareil**.



Définissez les paramètres suivants :

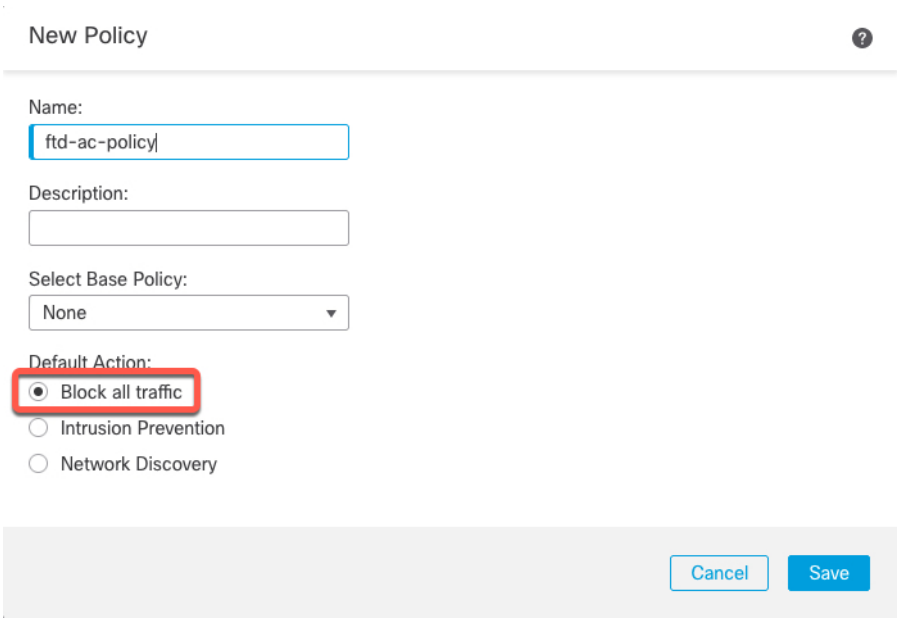
- **Hôte** : saisissez l'adresse IP ou le nom d'hôte du threat defense que vous souhaitez ajouter. Vous pouvez laisser ce champ vide si vous avez spécifié à la fois l'adresse IP du centre de gestion et un ID NAT dans la configuration de initiale du threat defense.

  Remarque Dans un environnement haute disponibilité, lorsque les deux centres de gestionse trouvent derrière un NAT, vous pouvez enregistrer le threat defense sans adresse IP ni nom d'hôte dans le centre de gestion principal. Toutefois, pour enregistrer le threat defense dans un centre de gestion secondaire, vous devez fournir l'adresse IP ou le nom d'hôte du threat defense.

- **Nom d'affichage** : saisissez le nom du threat defense tel que vous souhaitez l'afficher dans le centre de gestion.
- **Clé d'enregistrement** : saisissez la clé d'enregistrement que vous avez spécifiée dans la configuration de initiale du threat defense.
- **Domaine** : attribuez l'appareil à un domaine Leaf si vous disposez d'un environnement multidomaine.
- **Groupe** : attribuez-le à un groupe d'appareils si vous utilisez des groupes.
- **Politique de contrôle d'accès** : sélectionnez une politique initiale. Sauf si vous disposez déjà d'une politique personnalisée que vous devez utiliser, sélectionnez **Créer une nouvelle politique** et sélectionnez

Bloquer tout le trafic. Vous pourrez la modifier ultérieurement pour autoriser le trafic ; reportez-vous à la rubrique Autoriser le trafic de l'interface interne vers l'interface externe, à la page 41.

Illustration 20 : Nouvelle politique



- **Smart Licensing**: attribuez les licences Smart dont vous avez besoin pour les fonctionnalités que vous souhaitez déployer : **Malware** (si vous souhaitez utiliser l'inspection), **Threat** (si vous prévoyez d'utiliser la prévention contre les intrusions) et **URL** (si vous avez l'intention de mettre en œuvre le filtrage d'URL basé sur les catégories). **Remarque** : vous pouvez appliquer une licence VPN d'accès distant Client sécurisé après avoir ajouté l'appareil, via la page **Système** > **Licences** > **Licences Smart**.
- **ID NAT unique** : spécifiez l'ID NAT que vous avez spécifié dans la configuration initiale du threat defense.
- **Transférer des paquets** : permet à l'appareil de transférer des paquets vers le centre de gestion. Lorsque des événements comme IPS ou Snort sont déclenchés alors que cette option est activée, l'appareil envoie des informations de métadonnées d'événement et des données de paquet au centre de gestion à des fins d'inspection. Si vous désactivez cette option, seules les informations d'événement sont envoyées au centre de gestion ; les données de paquet ne sont pas envoyées.

Étape 3 Cliquez sur **S'enregistrer** ou, et confirmez l'enregistrement.

Si l'enregistrement réussit, l'appareil est ajouté à la liste. En cas d'échec, un message d'erreur s'affiche. Si l'enregistrement du threat defense échoue, vérifiez les points suivants :

- Ping : accédez à l'interface de ligne de commande du threat defense et envoyez une requête ping à l'adresse IP centre de gestion à l'aide de la commande suivante :

  ping system *ip_address*

  Si la requête ping échoue, vérifiez les paramètres réseau à l'aide de la commande **show network**. Si vous devez modifier l'adresse IP de gestion du threat defense, utilisez la commande **configure network management-data-interface**.

- Clé d'enregistrement, ID NAT et adresse IP du 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 le threat defense à l'aide de la commande **configure manager add**.

Pour plus d'informations sur le dépannage, consultez la page https://cisco.com/go/fmc-reg-error.

Configurer une politique de sécurité de base

Dans cette section, nous vous expliquons comment configurer une politique de sécurité de base avec les paramètres suivants :

- Interfaces internes et externes : attribuez une adresse IP statique à l'interface interne. 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.
- Serveur DHCP : utilisez un serveur DHCP sur l'interface interne pour les clients.
- NAT : utilisez l'interface PAT sur l'interface externe.
- Contrôle d'accès : autorisez le trafic de l'interface interne vers l'interface externe.
- SSH : activez SSH sur l'interface d'accès du gestionnaire.

Configurer les interfaces

Ajoutez l'interface VLAN1 pour les ports de commutateur ou convertissez les ports de commutateur 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 qu'un système transmette un trafic significatif. Habituellement, vous disposez d'une interface externe face au routeur en amont ou à Internet, et d'une ou de plusieurs interfaces internes pour les réseaux de votre entreprise. Par défaut, Ethernet1/1 est une interface de pare-feu standard que vous pouvez utiliser à l'extérieur ; les autres interfaces sont des ports de commutateur sur le VLAN 1. Après avoir ajouté l'interface VLAN1, vous pouvez la convertir en interface interne. Vous pouvez également attribuer des ports de commutateur à d'autres VLAN ou convertir des ports de commutateur en interfaces de pare-feu.

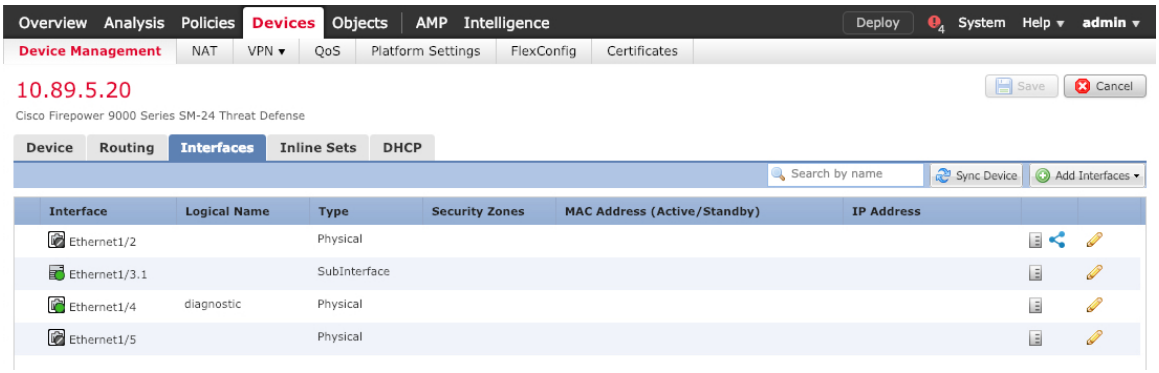
Un routage de périphérie classique consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre FAI, pendant que vous définissez des adresses statiques sur les interfaces internes.

L'exemple suivant configure une interface interne en mode routé (VLAN1) avec une adresse statique et une interface externe en mode routé à l'aide de DHCP (Ethernet1/1).

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** (✎) de l'appareil.

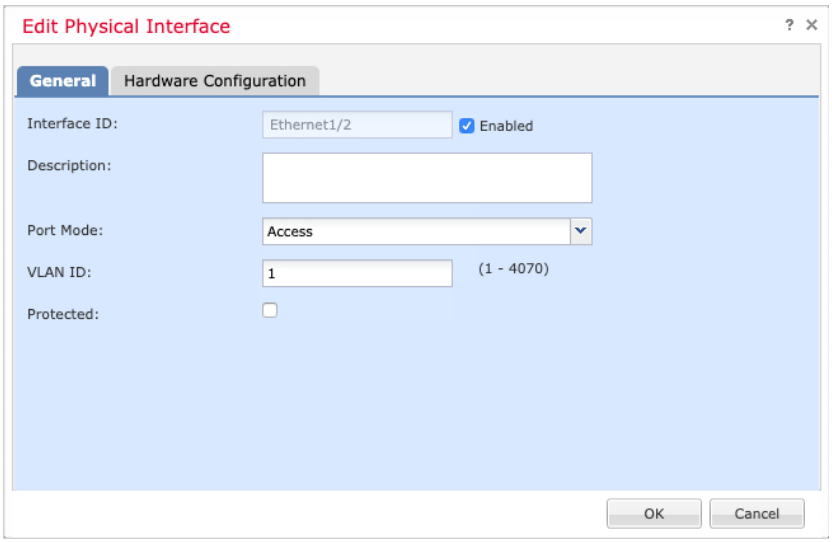
Étape 2 Cliquez sur **Interfaces**.



Étape 3 (facultatif) Désactivez le mode de port de commutateur pour l'un des ports de commutateur (Ethernet 1/2 à 1/8) en cliquant sur le curseur dans la colonne **SwitchPort** pour le désactiver ( ).

Étape 4 Activez les ports de commutateur.

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



b) Activez l'interface en cochant la case **Activé**.

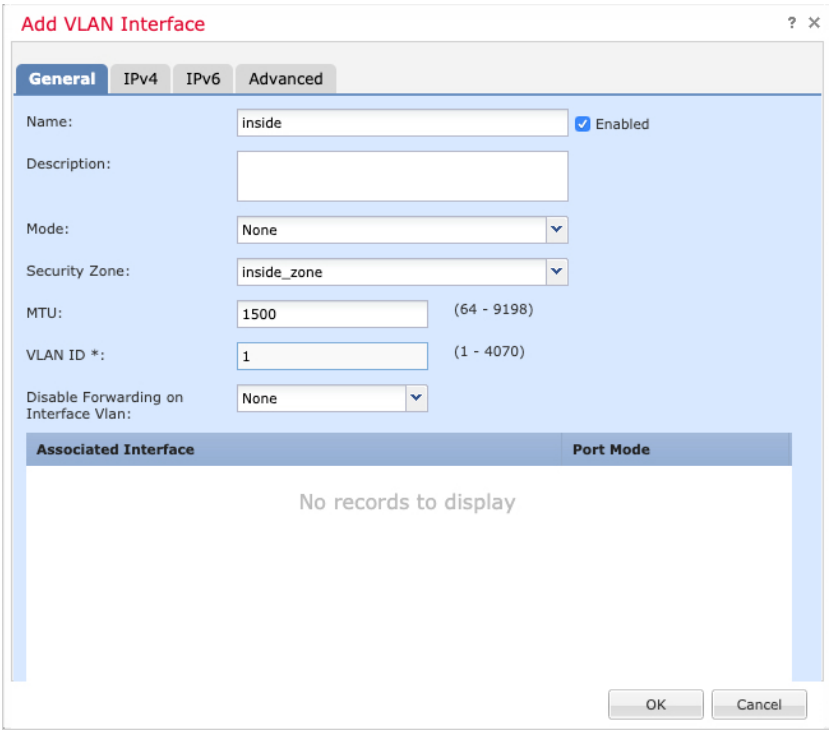
c) (facultatif) Modifiez l'ID de VLAN ; la valeur par défaut est 1. Vous devez ensuite ajouter une interface VLAN correspondant à cet ID.

d) Cliquez sur **OK**.

Étape 5 Ajoutez l'interface VLAN *interne*.

a) Cliquez sur **Ajouter des interfaces** > **Interface VLAN**.

L'onglet **Général** s'affiche.



b) Saisissez un **nom** comportant maximum 48 caractères.

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

c) Cochez la case **Activé**.

d) Laissez le champ **Mode** défini sur **Aucun**.

e) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité interne existante ou ajoutez-en une nouvelle en cliquant sur **Créer**.

Par exemple, ajoutez une zone appelée **zone_interne**. Chaque interface doit être affectée à une zone de sécurité et/ou à un groupe d'interfaces. Une interface peut appartenir 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 attribuer l'interface interne à la zone interne, et l'interface externe à la zone externe. Vous pouvez ensuite configurer votre politique de contrôle d'accès pour que le trafic transite de l'interface interne vers l'interface externe, mais pas de l'interface externe vers l'interface interne. La plupart des politiques ne prennent en charge que les zones de sécurité ; vous pouvez utiliser des zones ou des groupes d'interfaces dans les politiques NAT, les politiques de préfiltre et les politiques QoS.

f) Définissez le champ **ID de VLAN** sur **1**.

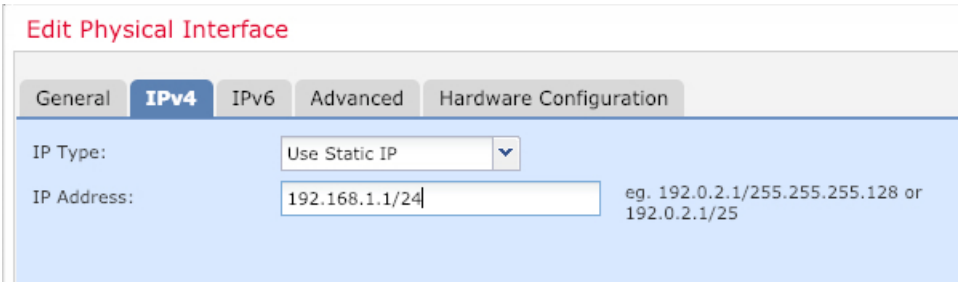
Par défaut, tous les ports de commutateur sont définis sur l'ID de VLAN 1 ; si vous choisissez un autre ID de VLAN, vous devez également modifier chaque port de commutateur pour qu'il corresponde au nouvel ID de VLAN.

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

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

- **IPv4** : sélectionnez **Utiliser l'adresse IP statique** dans la liste déroulante, et saisissez une adresse IP et un masque de sous-réseau en notation de barre oblique.

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

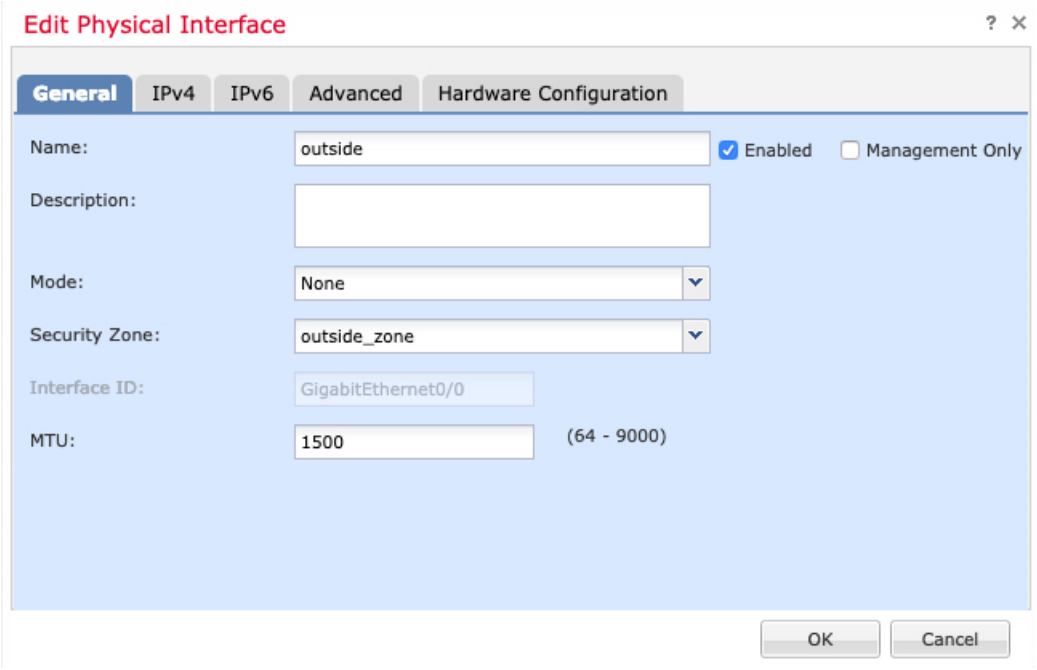


- **IPv6** : cochez la case **Configuration automatique** pour la configuration automatique sans état.

h) Cliquez sur **OK**.

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

L'onglet **Général** s'affiche.



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

a) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **Créer**.

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

b) Cliquez sur **OK**.

Étape 7 Cliquez sur **Enregistrer**.

Configurer le serveur DHCP

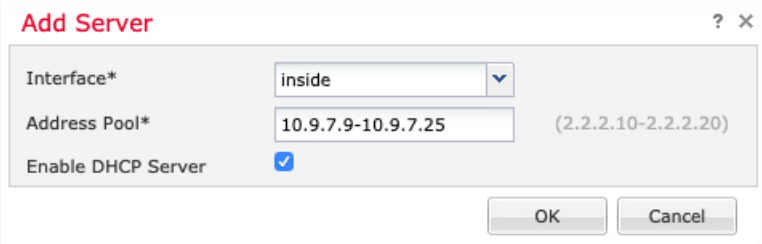
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir du threat defense.

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** (✎) de l'appareil.

Étape 2 Sélectionnez **DHCP** > **Serveur DHCP**.

Étape 3 Sur la page **Serveur**, cliquez sur **Ajouter** et configurez les options suivantes :



- **Interface** : sélectionnez l'interface dans la liste déroulante.
- **Pool d'adresses** : définissez la plage d'adresses IP (de la plus faible à la plus élevée) utilisée par le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et ne peut pas inclure l'adresse IP de l'interface proprement dite.
- **Activer le serveur DHCP** : activez le serveur DHCP sur l'interface sélectionnée.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Enregistrer**.

Configuration du routage NAT

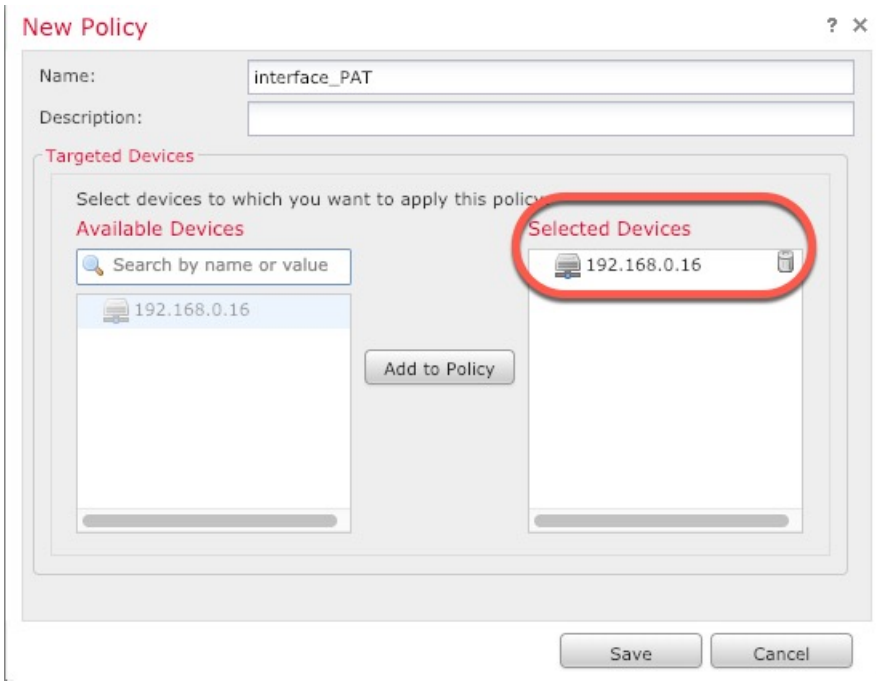
Configuration du routage NAT

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

Procédure

Étape 1 Sélectionnez **Appareils** > **NAT**, puis cliquez sur **Nouvelle politique** > **NAT de protection contre les menaces**.

Étape 2 Donnez un nom à la politique, sélectionnez le ou les appareils que vous souhaitez utiliser, puis cliquez sur **Enregistrer**.



La politique est ajoutée au centre de gestion. Vous devez quand même ajouter des règles à la politique.

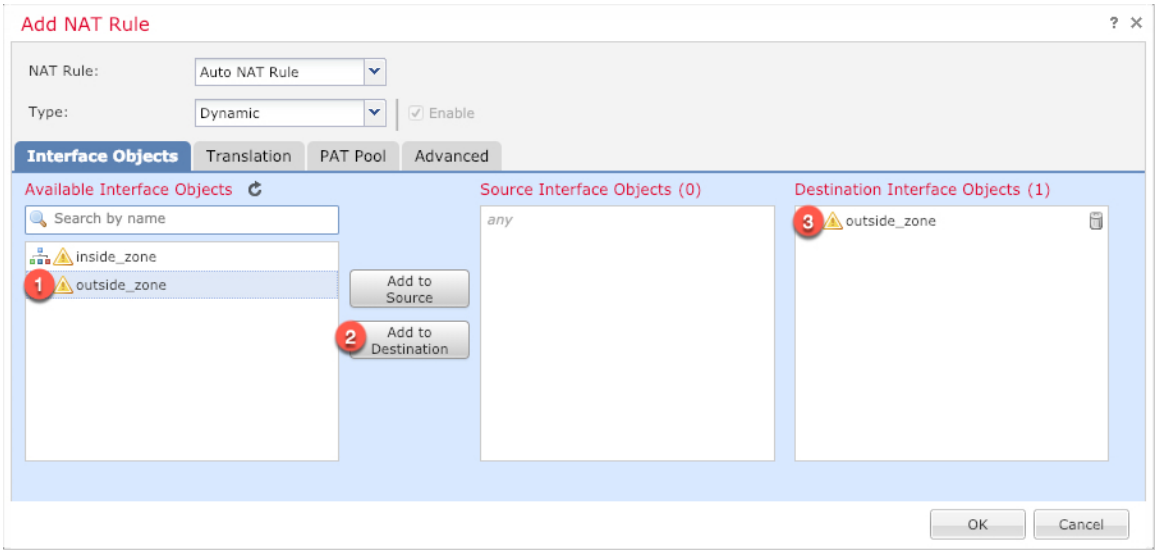
Étape 3 Cliquez sur **Ajouter une règle**.

La boîte de dialogue **Ajouter une règle NAT** apparaît.

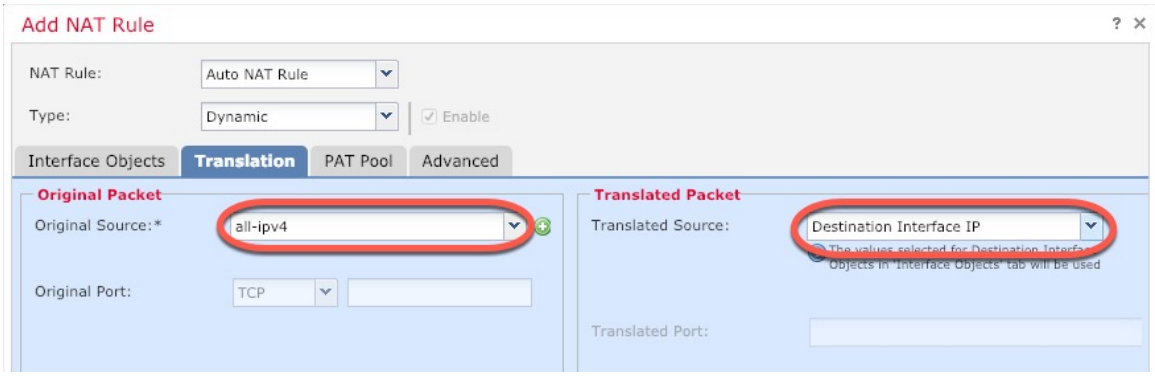
Étape 4 Configurez les options de règle de base :

- **Règle NAT** : sélectionnez **Règle NAT automatique**.
- **Type** : choisissez **Dynamique**.

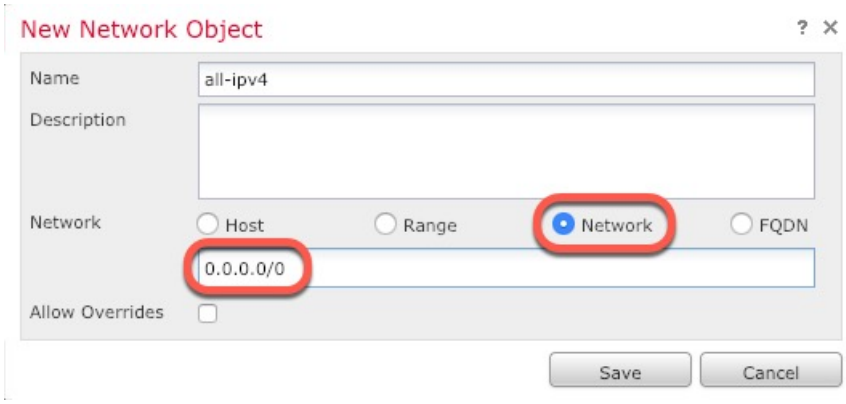
Étape 5 Sur la page **Objets d'interface**, ajoutez la zone externe de la section **Objets d'interface disponibles** à la section **Objets d'interface de destination**.



Étape 6 Sur la page **Traduction**, configurez les options suivantes :



- **Source d'origine** : cliquez sur **Ajouter** (+) pour ajouter un objet réseau pour tout le trafic IPv4 (0.0.0.0/0).

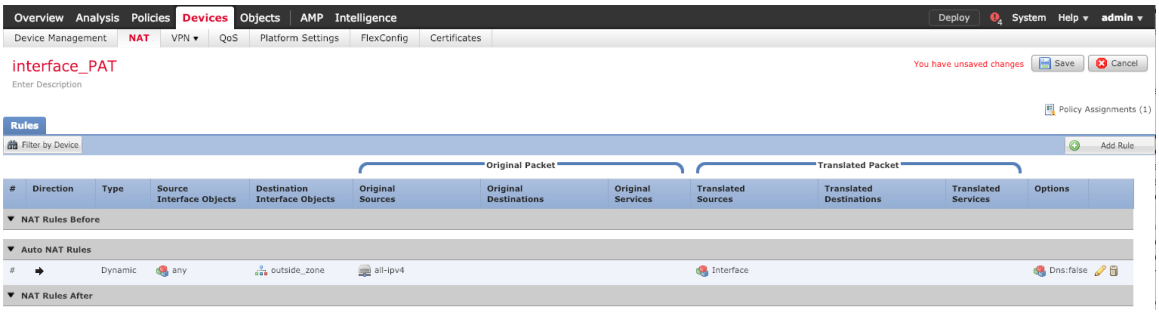


Remarque Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles NAT automatiques ajoutent la fonction NAT à la définition d'objet et vous ne pouvez pas modifier les objets définis par le système.

- **Source traduite** : sélectionnez **Adresse IP de l'interface de destination**.

Étape 7 Cliquez sur **Enregistrer** pour ajouter la règle.

La règle est enregistrée dans la table **Règles**.



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

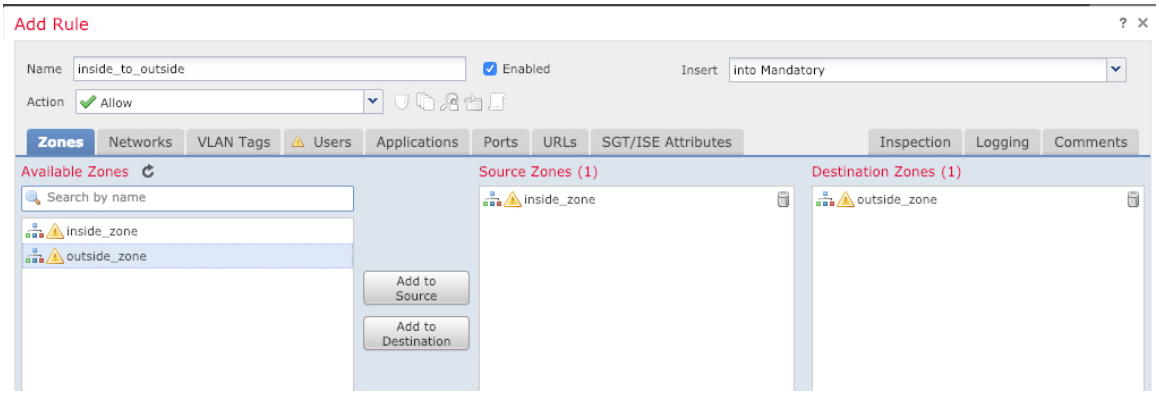
Autoriser le trafic de l'interface interne vers l'interface externe

Si vous avez créé une politique de contrôle d'accès de base **Bloquer tout le trafic** lorsque vous avez enregistré le threat defense, vous devez ajouter des règles à la politique pour autoriser le trafic via l'appareil. La procédure suivante ajoute une règle pour autoriser le trafic de la zone interne vers la zone externe. Si vous disposez d'autres zones, veillez à ajouter des règles autorisant le trafic vers les réseaux appropriés.

Procédure

Étape 1 Sélectionnez **Politique** > **Politique d'accès** > **Politique d'accès**, puis cliquez sur **Modifier** (✎) pour la politique de contrôle d'accès attribuée à threat defense.

Étape 2 Cliquez sur **Ajouter une règle**, puis définissez les paramètres suivants :



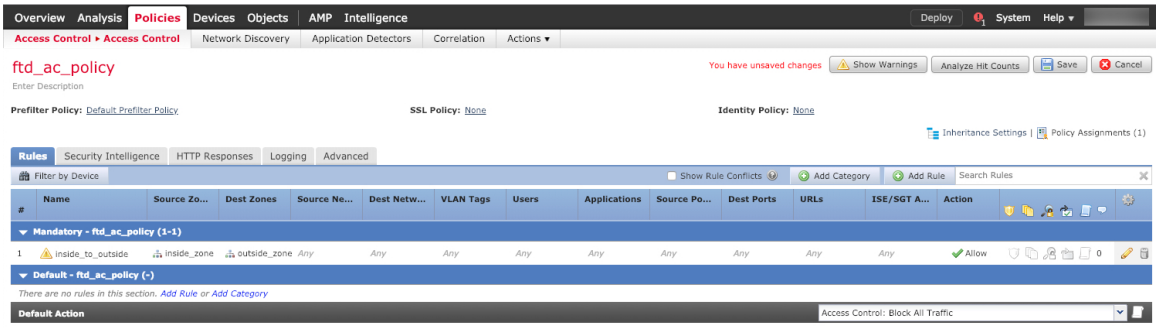
- **Nom** : donnez un nom à cette règle, par exemple **interne_vers_externe**.
- **Zones source** : sélectionnez la zone interne dans **Zones disponibles**, puis cliquez sur **Ajouter à la source**.

- **Zones de destination** : sélectionnez la zone externe dans **Zones disponibles**, puis cliquez sur **Ajouter à la destination**.

Laissez les autres paramètres tels quels.

Étape 3 Cliquez sur **Ajouter**.

La règle est ajoutée au tableau **Règles**.



Étape 4 Cliquez sur **Enregistrer**.

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

Si vous avez activé l'accès au centre de gestion sur une interface de données, par exemple externe, vous devez activer SSH sur cette interface en suivant cette procédure. Dans cette section, nous vous expliquons comment activer les connexions SSH sur une ou plusieurs interfaces de *données* sur le threat defense. SSH n'est pas pris en charge par l'interface logique de diagnostic.

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

L'interface de gestion est distincte des autres interfaces sur l'appareil. Elle permet de configurer et d'enregistrer l'appareil sur le gestionnaire du centre de gestion. SSH pour les interfaces de données partage la liste des utilisateurs internes et externes avec SSH pour l'interface de gestion. D'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 standard, et non les routes statiques définies lors de la configuration ou sur l'interface de ligne de commande.

Sur l'interface de gestion, pour configurer une liste d'accès SSH, reportez-vous à la commande **configure ssh-access-list** de la rubrique Référence des commandes pour Secure Firewall Threat Defense. Pour configurer une route statique, consultez la commande **configure network static-routes**. Par défaut, vous configurez la route par défaut via l'interface de gestion lors de la configuration initiale.

Pour utiliser SSH, il n'est pas nécessaire de disposer d'une règle d'accès autorisant l'adresse IP de l'hôte. Vous devez uniquement configurer l'accès SSH conformément à cette section.

Vous pouvez uniquement utiliser le protocole SSH pour accéder à une interface accessible ; si votre hôte SSH se trouve sur l'interface externe, vous pouvez uniquement établir une connexion de gestion directement vers l'interface externe.

L'appareil autorise un maximum de 5 connexions SSH simultanées.

Remarque Après trois tentatives infructueuses de connexion à l'interface de ligne de commande via SSH, l'appareil interrompt la connexion SSH.

Avant de commencer

- Vous pouvez configurer les utilisateurs internes SSH dans l'interface de ligne de commande à l'aide de la commande **configure user add**. Par défaut, il existe un utilisateur **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** dans les paramètres de la plateforme.
- Vous devez disposer d'objets réseau qui définissent les hôtes ou les réseaux autorisés à établir des connexions SSH à l'appareil. Vous pouvez ajouter des objets dans le cadre de cette 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 **Objets** > **Gestion des objets** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser l'objet réseau **any** fourni par le système. Utilisez plutôt **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Appareils** > **Paramètres de la plateforme** et créez ou modifiez la politique threat defense.

Étape 2 Sélectionnez **Secure Shell**.

Étape 3 Identifiez les interfaces et les adresses IP qui autorisent les connexions SSH.

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

a) Cliquez sur **Ajouter** pour ajouter une nouvelle règle ou sur **Modifier** pour modifier une règle.

b) Configurez les propriétés de la règle :

- **Adresse IP** : objet ou groupe réseau qui identifie les hôtes ou les réseaux autorisés à établir des connexions SSH. Sélectionnez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur +.
- **Zones de sécurité** : ajoutez les zones contenant les interfaces sur lesquelles vous autorisez les connexions SSH. Pour les interfaces ne faisant pas partie d'une zone, vous pouvez saisir le nom de l'interface dans le champ situé sous la liste Zone de sécurité sélectionnée, puis cliquer sur **Ajouter**. Ces règles seront appliquées à un appareil uniquement si celui-ci inclut les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 Cliquez sur **Enregistrer**.

Vous pouvez maintenant accéder à la page **Déployer** > **Déploiement** et déployer la politique sur les appareils affectés. Les modifications ne sont pas actives tant que vous ne les avez pas déployées.

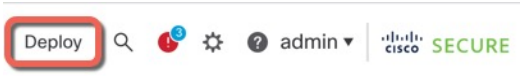
Déployer la configuration

Déployez les modifications de configuration sur le threat defense ; aucune modification n'est active sur l'appareil tant que vous ne l'avez pas déployée.

Procédure

Étape 1 Cliquez sur **Déployer** en haut à droite.

Illustration 21 : Déployer



Étape 2 Cliquez sur **Tout déployer** pour déployer sur tous les périphériques ou cliquez sur **Déploiement avancé** pour déployer sur les périphériques sélectionnés.

Illustration 22 : Tout déployer

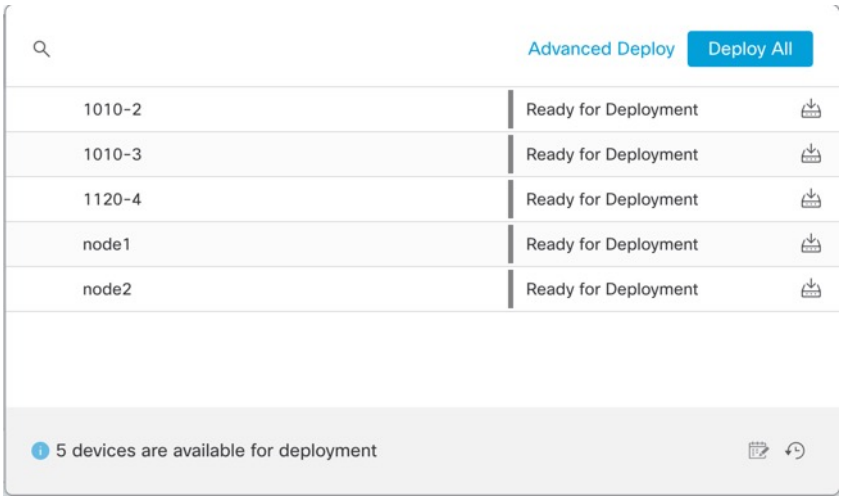
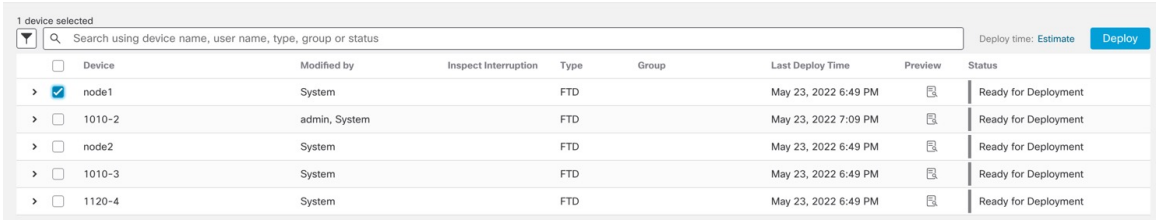
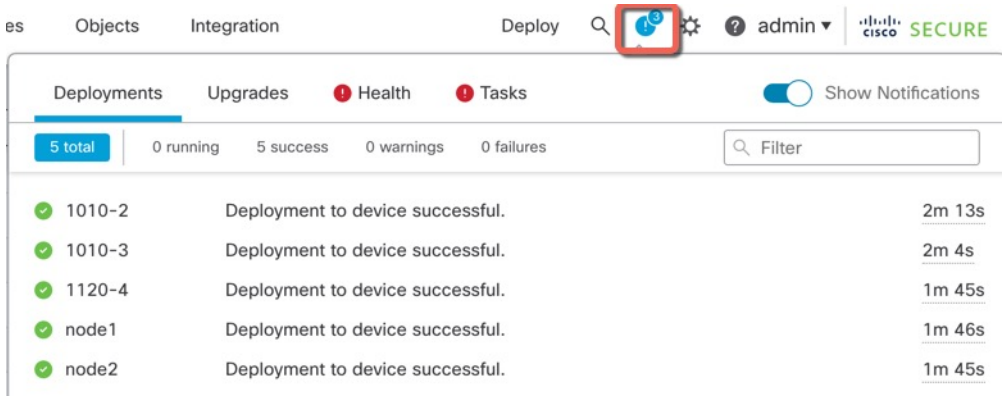


Illustration 23 : Déploiement avancé



Étape 3 Assurez-vous que le déploiement aboutit. Cliquez sur l'icône en regard du bouton **Déployer** dans la barre de menus pour afficher l'état des déploiements.

Illustration 24 : État du déploiement



Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS

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

Vous pouvez également accéder à la CLI FXOS à des fins de dépannage.

Remarque Vous pouvez également vous connecter à l'interface de gestion de l'appareil threat defense. Contrairement à une session de console, la session SSH utilise par défaut l'interface de ligne de commande du threat defense, à partir de laquelle vous pouvez vous connecter à la CLI FXOS à l'aide de la commande **connect fxos**. Vous pourrez 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 console, qui est défini par défaut sur la CLI FXOS.

Procédure

Étape 1 Pour vous connecter à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. L'appareil Firepower 1000 est livré avec un câble série USB A vers B. Veillez à installer les pilotes série USB nécessaires à votre système d'exploitation (consultez le guide matériel de l'appareil Firepower 1010). Le port de console est défini par défaut sur la CLI FXOS. Utilisez les paramètres série suivants :

- 9 600 bauds
- 8 bits de données
- Aucune parité

- 1 bit d'arrêt

Vous vous connectez à la CLI FXOS. Connectez-vous à l'interface de ligne de commande à l'aide du nom d'utilisateur **admin** et du 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 du threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après vous être connecté, pour obtenir des informations sur les commandes disponibles dans l'interface de ligne de commande, saisissez **help** ou **?**. Pour plus d'informations sur l'utilisation, reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande threat defense, saisissez la commande du **exit** ou **logout**.

Cette commande vous renvoie à l'invite de la CLI FXOS. Pour plus d'informations sur les commandes disponibles dans la CLI FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Résoudre les problèmes de connectivité de gestion sur une interface de données

Prise en charge des modèles—Threat Defense

Lorsque vous utilisez une interface de données pour l'accès au centre de gestion au lieu d'utiliser l'interface de gestion dédiée, veillez à modifier les paramètres d'interface et de réseau du threat defense dans le centre de gestion afin de ne pas interrompre la connexion. Si vous modifiez le type d'interface de gestion après avoir ajouté le threat defense au centre de gestion (c'est-à-dire, remplacez l'interface de données par l'interface de gestion, ou vice versa), si les interfaces et les paramètres réseau ne sont pas configurés correctement, vous risquez de perdre la connectivité à l'interface de gestion.

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

Afficher l'état de connexion de l'interface de gestion

Dans le centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Appareils** > **Gestion des appareils** > **Appareil** > **Gestion** > **Détails de l'accès au FMC** > **État de connexion**.

Dans l'interface de ligne de commande du threat defense, saisissez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion. Vous pouvez également utiliser **sftunnel-status** pour afficher des informations plus complètes.

Reportez-vous à l'exemple de résultat suivant pour une connexion interrompue ; aucune information de connexion de canal homologue et aucune information de pulsation n'est disponible :

```
> 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
```

Reportez-vous à l'exemple de résultat suivant pour une connexion active comprenant des informations de canal homologue et de 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
```

Afficher les informations relatives au réseau du Threat Defense

Dans l'interface de ligne de commande du threat defense, affichez les paramètres réseau de l'interface de gestion et d'accès aux données du centre de gestion :

show network

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

=====================[ br1 ]======================
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
```

```
Configuration            : Manual
Address                  : 10.99.10.4
Netmask                  : 255.255.255.0
Gateway                  : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration            : Disabled

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

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

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

Vérifier que le Threat Defense est enregistré auprès du Centre de gestion

Dans l'interface de ligne de commande du threat defense, vérifiez que le centre de gestion a bien été enregistré. Notez que cette commande n'affiche pas l'état *actuel* de la connexion de gestion.

show managers

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

>
```

Envoyer une requête ping au Centre de gestion

Dans l'interface de ligne de commande du threat defense, utilisez la commande suivante pour envoyer une requête ping au centre de gestion à partir des interfaces de données :

ping *fmc_ip*

Dans l'interface de ligne de commande du threat defense, utilisez la commande suivante pour envoyer une requête ping au centre de gestion à partir de l'interface de gestion, afin de l'acheminer via le fond de panier aux interfaces de données :

ping system *fmc_ip*

Capturer les paquets sur l'interface interne du Threat Defense

Dans l'interface de ligne de commande du threat defense, capturez les paquets sur l'interface de fond de panier interne (nlp_int_tap) pour déterminer 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 du threat defense, consultez les informations relatives à l'interface de fond de panier interne, 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
```

Vérifier le routage et la NAT

Dans l'interface de ligne de commande du threat defense, vérifiez que la route par défaut (S*) a bien été ajoutée et qu'il existe des règles NAT internes 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

Reportez-vous aux commandes suivantes pour vérifier que tous les autres paramètres sont présents. Vous pouvez également consulter la plupart de ces commandes sur la page **Appareils** > **Gestion des appareils** > **Appareil** > **Gestion** > **Détails de l'accès au FMC** > **Résultat de la CLI** du centre de gestion.

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
>
```

Rechercher une mise à jour DDNS réussie

Dans l'interface de ligne de commande du threat defense, vérifiez que la mise à jour DDNS a réussi :

debug ddns

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

Si la mise à jour échoue, utilisez les commandes **debug http** et **debug ssl**. Pour les échecs de validation du certificat, vérifiez que les certificats racines sont installés sur l'appareil :

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
```

Consulter les fichiers journaux du Centre de gestion

Consultez la page https://cisco.com/go/fmc-reg-error.

Rétablir la configuration en cas de déconnexion du Centre de gestion

Si vous utilisez une interface de données sur le threat defense pour le centre de gestion, et que vous déployez une modification de configuration depuis le centre de gestion ayant une incidence sur la connectivité réseau, vous pouvez rétablir la dernière configuration déployée sur le threat defense afin de restaurer la connectivité de gestion. Vous pouvez ensuite ajuster les paramètres de configuration dans le centre de gestion afin de maintenir et de redéployer la connectivité réseau. Vous pouvez utiliser la fonction de restauration même si aucune perte de connectivité ne se produit, car elle ne se limite pas à cette situation de dépannage.

Reportez-vous aux instructions suivantes :

- Seul le déploiement précédent est disponible localement sur le threat defense ; vous ne pouvez pas rétablir les déploiements antérieurs.
- La fonction de restauration n'est pas prise en charge pour les déploiements haute disponibilité ou en cluster.
- La restauration s'applique uniquement aux configurations que vous pouvez définir dans le centre de gestion. Par exemple, la restauration ne s'applique à aucune configuration locale liée à l'interface de gestion dédiée, que vous pouvez configurer uniquement sur l'interface de ligne de commande de threat defense. Notez que si vous avez modifié les paramètres de l'interface de données après le dernier déploiement du centre de gestion à l'aide de la commande **configure network management-data-interface**, puis que vous utilisez la commande de restauration, ces paramètres ne sont pas conservés ; les derniers paramètres déployés sur le centre de gestion sont rétablis.

- Il est impossible de restaurer le mode UCAPL/CC.
- Il est impossible de restaurer les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent.
- Pendant la restauration, les connexions sont interrompues, car la configuration en cours est supprimée.

Avant de commencer

Prise en charge des modèles—Threat Defense

Procédure

Étape 1 Sur l'interface de ligne de commande de threat defense, restaurez la configuration précédente.

configure policy rollback

Après la restauration, le système threat defense informe le centre de gestion que la restauration a réussi. Dans le centre de gestion, l'écran de déploiement affiche une bannière indiquant que la configuration a été restaurée.

Si la restauration échoue, reportez-vous à la rubrique https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html pour connaître les problèmes de déploiement courants. Dans certains cas, la restauration peut échouer après le rétablissement de l'accès du centre de gestion ; dans ce cas, vous pouvez résoudre les problèmes de configuration du centre de gestion et renouveler le déploiement depuis le 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 le centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Appareils** > **Gestion des appareils** > **Appareil** > **Gestion** > **Détails de l'accès au FMC** > **État de connexion**.

Dans l'interface de ligne de commande du threat defense, saisissez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

Si le rétablissement de la connexion prend plus de 10 minutes, vous devez dépanner la connexion. Reportez-vous à la rubrique Résoudre les problèmes de connectivité de gestion sur une interface de données, à la page 85.

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

Il est important que vous arrêtiez correctement votre système. Il ne suffit pas de débrancher le câble d'alimentation ou d'appuyer sur l'interrupteur d'alimentation, car vous risquez d'endommager gravement le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en arrière-plan en permanence, et que débrancher ou couper l'alimentation ne permet pas un arrêt normal de votre pare-feu.

Vous pouvez arrêter votre système correctement à l'aide du centre de gestion.

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**.

Étape 2 Cliquez sur l'icône Modifier ( ) en regard de l'appareil que vous souhaitez redémarrer.

Étape 3 Cliquez sur l'onglet **Appareils**.

Étape 4 Cliquez sur l'icône d'arrêt de l'appareil ( ) dans la section **Système**.

Étape 5 Lorsque vous y êtes invité, confirmez que vous souhaitez arrêter l'appareil.

Étape 6 Si vous disposez d'une connexion de console au pare-feu, observez les invites système lorsque le pare-feu s'arrête. L'invite suivante s'affiche :

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

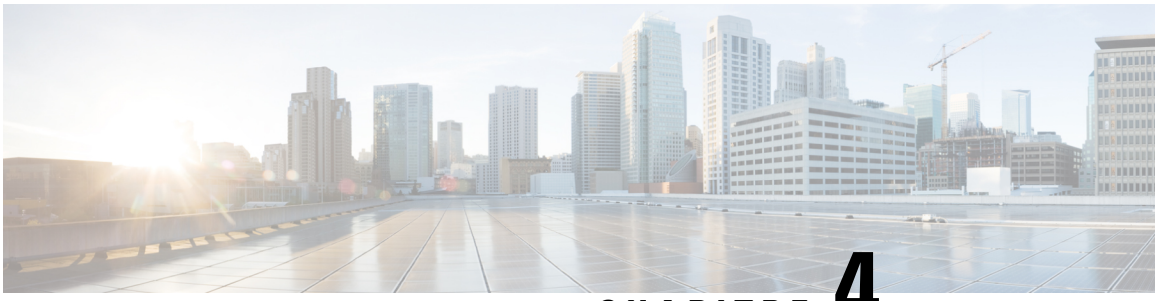
Si vous ne disposez pas d'une connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Étape 7 Vous pouvez désormais débrancher ce dernier pour couper l'alimentation du châssis si nécessaire.

Et après ?

Pour poursuivre la configuration de votre threat defense, consultez les documents disponibles pour votre version logicielle dans Parcourir la documentation de Cisco Firepower.

Pour plus d'informations sur l'utilisation du centre de gestion, reportez-vous à la rubrique Guide de configuration de Firepower Management Center.



CHAPITRE 4

Déployer Threat Defense avec le Gestionnaire d'appareils

Ce chapitre vous concerne-t-il ?

Pour connaître tous les systèmes d'exploitation et gestionnaires disponibles, reportez-vous à la rubrique Quel système d'exploitation et quel gestionnaire vous conviennent le mieux ?, à la page 1. Ce chapitre s'applique au threat defense doté de gestionnaire d'appareils.

Dans ce chapitre, nous vous expliquons comment effectuer la configuration initiale de votre threat defense à l'aide de l'assistant de configuration d'appareils web.

Le gestionnaire d'appareils vous permet de configurer les fonctionnalités de base des logiciels les plus couramment utilisés pour les réseaux de faible envergure. Il est spécialement conçu pour les réseaux qui incluent uniquement quelques appareils, voire un seul, sur lesquels il est inutile d'utiliser un gestionnaire multi-appareils haute puissance capable de contrôler un réseau de grande envergure contenant de nombreux appareils gestionnaire d'appareils.

À propos du pare-feu

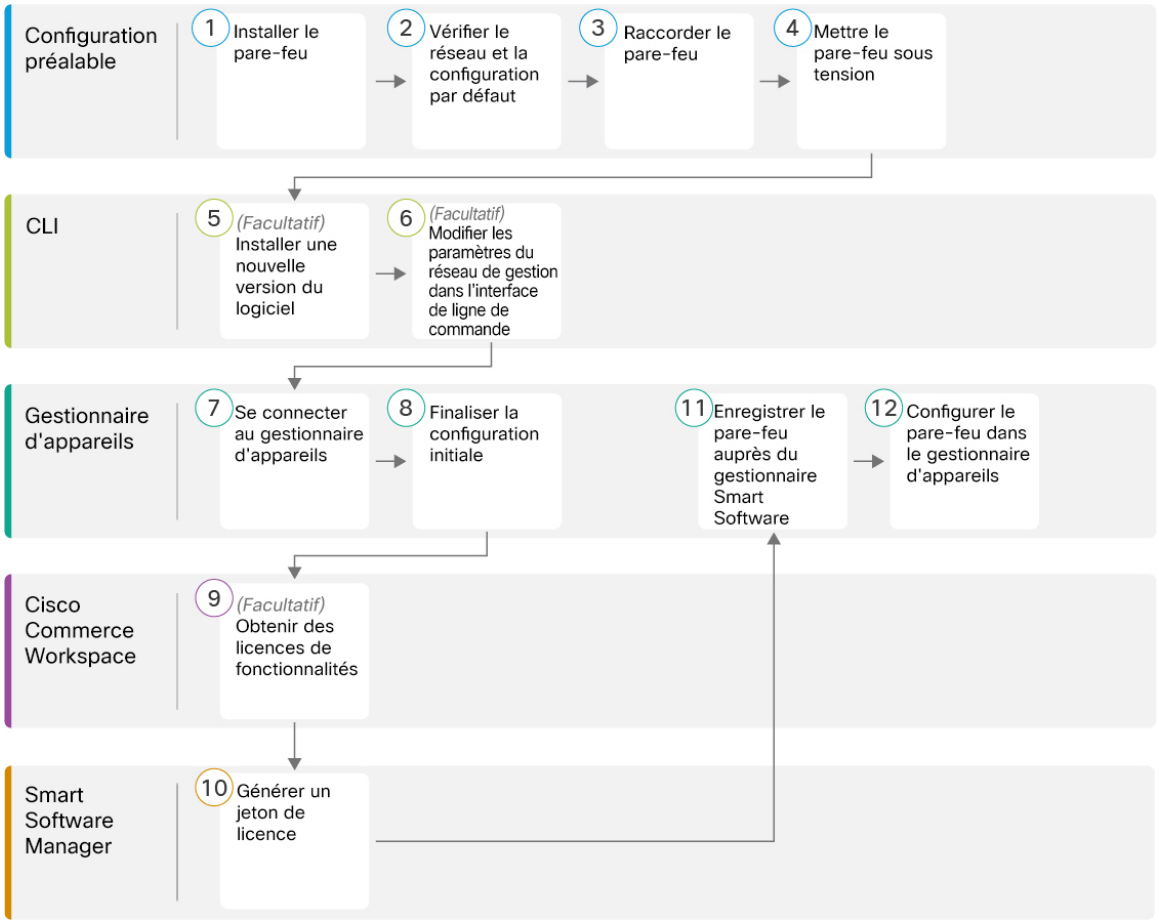
L'appareil peut exécuter un logiciel threat defense ou un logiciel ASA. Pour basculer entre threat defense et ASA, vous devez reconfigurer l'appareil. Vous devez également recommencer l'installation si vous avez besoin d'une version logicielle différente de celle actuellement installée. Consultez la rubrique Réinstaller Cisco ASA ou Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé Système d'exploitation Secure Firewall eXtensible (FXOS). Le pare-feu ne prend pas en charge le Gestionnaire de châssis Secure Firewall FXOS ; seule une CLI limitée est prise en charge à des fins de dépannage. Pour obtenir plus d'informations, reportez-vous à la section Guide de dépannage Cisco FXOS pour la série Firepower 1000/2100 exécutant Firepower Threat Defense.

Déclaration de confidentialité—Le pare-feu ne requiert ni ne collecte activement aucune information permettant de vous identifier. Vous pouvez néanmoins utiliser des informations d'identification personnelle au cours de la configuration, notamment des noms d'utilisateur. Dans ce cas, un administrateur peut accéder à ces informations lors de l'utilisation de la configuration ou de l'utilisation du protocole SNMP.

Procédure de bout en bout

Reportez-vous aux tâches suivantes pour déployer le threat defense avec le gestionnaire d'appareils sur votre châssis.



1	Configuration préalable	Installez le pare-feu. Reportez-vous au guide d'installation matérielle.

2	Configuration préalable	Vérifier le déploiement et la configuration par défaut du réseau, à la page 95.
3	Configuration préalable	Raccorder l'appareil, à la page 99.
4	Configuration préalable	Mettre le pare-feu sous tension, à la page 13.
5	CLI	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 101
6	CLI	(Facultatif) Modifier les paramètres du réseau de gestion dans l'interface de ligne de commande, à la page 102.
7	Gestionnaire d'appareils	Se connecter au Gestionnaire d'appareils, à la page 105.
8	Gestionnaire d'appareils	Terminer la configuration initiale, à la page 105.
9	Cisco Commerce Workspace	(Facultatif) Configurer l'octroi de licences, à la page 107 : obtenez des licences de fonction.
10	Smart Software Manager	Configurer l'octroi de licences, à la page 107 : générez un jeton de licence.
11	Gestionnaire d'appareils	Configurer l'octroi de licences, à la page 107 : enregistrez l'appareil auprès de Smart Licensing Server.
12	Gestionnaire d'appareils	Configurer le pare-feu dans le Gestionnaire d'appareils, à la page 113.

Vérifier le déploiement et la configuration par défaut du réseau

Vous pouvez gérer le threat defense à l'aide du gestionnaire d'appareils à partir de l'interface de gestion 1/1 ou de l'interface interne. L'interface de gestion dédiée est une interface spéciale disposant de ses propres paramètres réseau.

La figure suivante illustre le déploiement réseau recommandé. Si vous connectez l'interface externe directement à un modem câble ou ADSL, nous vous recommandons de mettre le modem en mode pont pour que le threat defense effectue tout le routage et la NAT pour vos réseaux internes. Si vous devez configurer le protocole PPPoE de sorte que l'interface externe se connecte à votre FAI, faites-le une fois la configuration initiale terminée dans gestionnaire d'appareils.

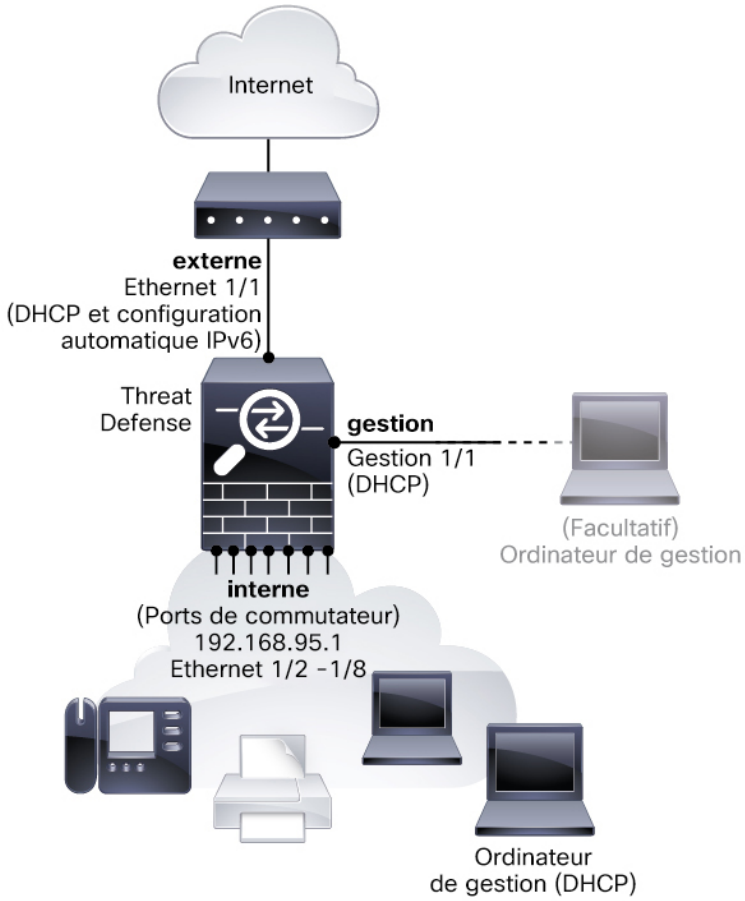
Remarque Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut (par exemple, votre réseau de gestion n'inclut pas de serveur DHCP), vous pouvez vous connecter au port de console et effectuer la configuration initiale sur l'interface de ligne de commande, notamment configurer l'adresse IP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

Si vous devez modifier l'adresse IP interne, faites-le une fois la configuration initiale terminée dans le gestionnaire d'appareils. Par exemple, il est possible que vous deviez modifier l'adresse IP interne dans les cas suivants :

- (7.0 et versions ultérieures) L'adresse IP interne est 192.168.95.1. (Version 6.7 et versions antérieures) L'adresse IP interne est 192.168.1.1. Si l'interface externe tente d'obtenir une adresse IP sur le réseau 192.168.1.0, qui est un réseau par défaut courant, le bail DHCP échouera et l'interface externe n'obtiendra aucune adresse IP. Ce problème se produit, car threat defense ne peut pas disposer de deux interfaces sur le même réseau. Dans ce cas, vous devez modifier l'adresse IP interne de façon à la placer sur un nouveau réseau.
- Si vous ajoutez threat defense à un réseau interne, vous devrez modifier l'adresse IP interne de façon à ce qu'elle corresponde au réseau.

La figure suivante illustre le déploiement réseau par défaut à utiliser pour threat defense à l'aide du gestionnaire d'appareils avec la configuration par défaut.

Illustration 25 : Déploiement réseau suggéré



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

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

Configuration par défaut

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

- **interne**—adresse IP (7.0 et versions ultérieures) 192.168.95.1 ; (versions antérieures à 7.0) 192.168.1.1.
  - (6.5 et versions ultérieures) **Commutateur matériel** : Ethernet 1/2 à 1/8 appartiennent au VLAN 1
  - (6.4) **Commutateur logiciel** (routage et pontage intégrés) : Ethernet 1/2 à 1/8 appartiennent à l'interface de groupe de ponts (BVI) 1
- **externe** : Ethernet 1/1, adresse IP du DHCP IPv4 et configuration automatique IPv6
- Flux de trafic **interne→externe**

- **gestion** : gestion 1/1 (gestion)
  - (6.6 et versions ultérieures) Adresse IP de DHCP
  - (6.5 et versions antérieures) Adresse IP 192.168.45.45

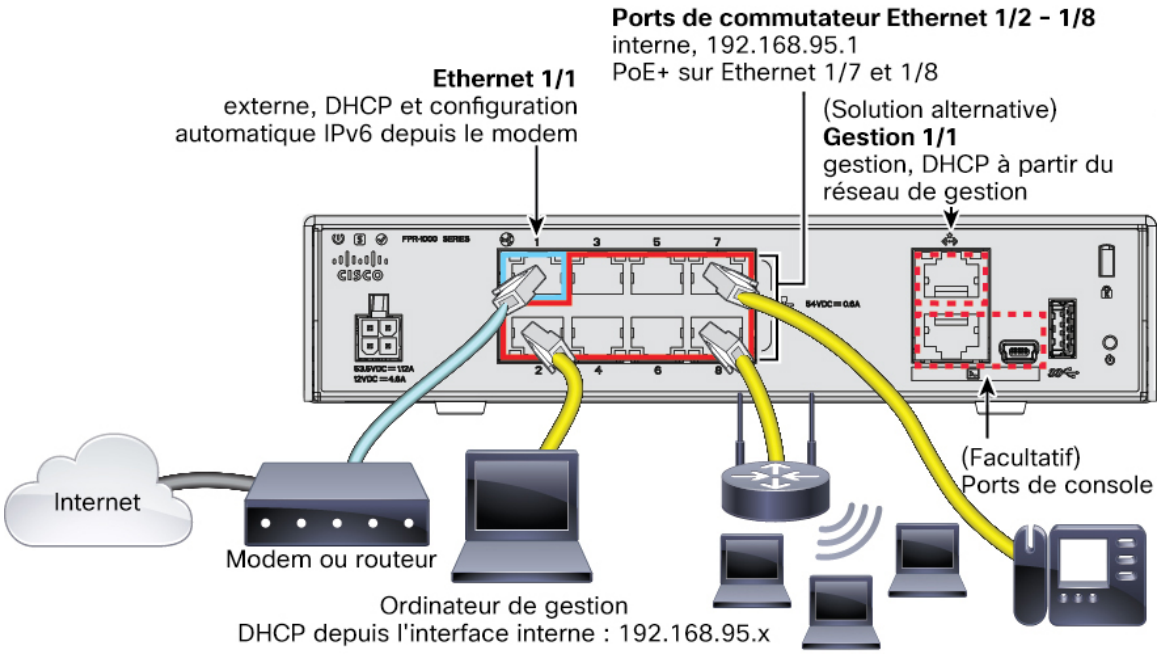
Remarque L'interface de gestion 1/1 est une interface spéciale distincte des interfaces de données, qui est utilisée pour la gestion, l'octroi de licences Smart et les mises à jour de la base de données.L'interface physique est partagée avec une deuxième interface logique, l'interface de diagnostic. L'interface de diagnostic est une interface de données, mais elle est limitée à d'autres types de trafics de gestion (vers l'appareil et depuis l'appareil), tels que syslog ou SNMP. L'interface de diagnostic n'est généralement pas utilisée. Pour obtenir plus d'informations, reportez-vous à la section Guide de configuration de Cisco Secure Firewall Device Manager.

- **Serveur DNS pour la gestion** : OpenDNS : (IPv4) 208.67.222.222, 208.67.220.220 ; (IPv6) 2620:119:35::35 ou serveurs spécifiés lors de la configuration. Les serveurs DNS obtenus auprès de DHCP ne sont jamais utilisés.
- **NTP** : serveurs Cisco NTP : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org ou serveurs spécifiés lors de la configuration
- **Routes par défaut**
  - **Interfaces de données** : obtenues à partir d'un DHCP externe ou d'une adresse IP de passerelle spécifiée lors de la configuration
  - **Interface de gestion** :(6.6 et versions ultérieures) obtenue auprès du serveur de gestion DHCP. Si vous ne recevez pas de passerelle, la route par défaut passe par le fond de panier et via les interfaces de données (6.5 et versions antérieures). Par le fond de panier et via les interfaces de données

    Notez que l'interface de gestion nécessite un accès Internet pour l'octroi de licences et les mises à jour, via le fond de panier ou à l'aide d'une passerelle Internet distincte. Notez que seul le trafic provenant de l'interface de gestion peut transiter par le fond de panier ; sinon, la gestion n'autorise pas le trafic de transit pour le trafic entrant dans la gestion depuis le réseau.
- **Serveur DHCP** : activé sur l'interface interne et (6.5 et versions antérieures uniquement) l'interface de gestion.
- **Accès au Gestionnaire d'appareils** : tous les hôtes sont autorisés sur l'interface de gestion et l'interface interne.
- **NAT** : interface PAT pour l'ensemble du trafic de l'interface interne vers l'interface externe.

Raccorder l'appareil

Illustration 26 : Raccorder le Firepower 1010



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

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

Remarque Dans les versions 6.5 et ultérieures, les interfaces Ethernet 1/2 à 1/8 sont configurées en tant que ports de commutateur matériels ; PoE+ est également disponible sur Ethernet 1/7 et 1/8. Dans la version 6.4, les interfaces Ethernet 1/2 à 1/8 sont configurées en tant que membres du groupe de ponts (ports de commutateur logiciels) ; PoE+ n'est pas disponible. Le câblage initial est le même pour les deux versions.

Gérez le pare-feu Firepower 1010 sur l'interface de gestion 1/1 ou sur l'interface Ethernet 1/2 à 1/8. La configuration par défaut configure également Ethernet 1/1 comme interface externe.

Procédure

Étape 1 Installez votre matériel et apprenez à l'utiliser à l'aide du guide d'installation matérielle.

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

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

gestion). Par conséquent, assurez-vous que ces paramètres n'entrent pas en conflit avec les paramètres existants du réseau interne (reportez-vous à la rubrique Configuration par défaut, à la page 97).

- Gestion 1/1 (appelée MGMT) : connectez l'interface de gestion 1/1 à votre réseau de gestion et assurez-vous que votre ordinateur de gestion est connecté (ou a accès) au réseau de gestion. L'interface de gestion 1/1 obtient une adresse IP auprès d'un serveur DHCP sur votre réseau de gestion ; si vous utilisez cette interface, vous devez déterminer l'adresse IP attribuée au threat defense pour pouvoir vous connecter à l'adresse IP à partir de votre ordinateur de gestion.

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

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

Par défaut, l'adresse IP est obtenue via la configuration automatique des adresses IPv4 DHCP et IPv6, mais vous pouvez définir une adresse statique lors de la configuration initiale.

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

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

Mettre le pare-feu sous tension

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

Remarque La première fois que vous démarrez le threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Avant de commencer

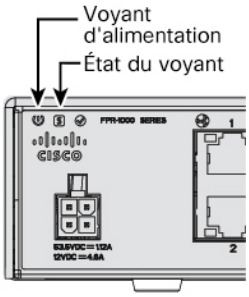
Il est important que vous utilisiez une source d'alimentation fiable pour alimenter votre appareil (à l'aide d'un système d'alimentation sans coupure, par exemple). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent en arrière-plan en permanence, et une panne de courant ne permet pas l'arrêt normal de votre système.

Procédure

Étape 1 Raccordez le câble d'alimentation à l'appareil et branchez-le à une prise électrique.

L'appareil se met automatiquement sous tension dès que vous le branchez.

Étape 2 Observez le voyant d'alimentation situé à l'arrière de l'appareil. S'il est allumé en vert, l'appareil est sous tension.



Étape 3 Observez le voyant d'état à l'arrière ou sur l'appareil. Lorsqu'il s'allume en vert, le système a terminé les diagnostics de mise sous tension.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une autre version, 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 en regard du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de publication décrite dans la rubrique 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. Pour plus d'informations, reportez-vous à la rubrique Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 117. Cette procédure illustre l'utilisation du port de console, mais vous pouvez utiliser SSH si vous le souhaitez.

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

Vous vous connectez à la CLI FXOS. Lors de la première connexion, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si vous avez modifié le mot de passe, mais que vous l'avez oublié, vous devez réinitialiser l'appareil pour rétablir le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure pour rétablir les paramètres 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 Dans l'interface de ligne de commande de la console FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

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

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

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

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

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

b) Suivez la procédure de réinstallation du guide de dépannage de la console FXOS.

(Facultatif) Modifier les paramètres du réseau de gestion dans l'interface de ligne de commande

Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut, vous pouvez vous connecter au port de console et effectuer la configuration initiale à partir de l'interface de ligne de commande, notamment la configuration de l'adresse IP de gestion, de la passerelle et d'autres paramètres réseau de base. Vous pouvez uniquement configurer les paramètres de l'interface de gestion ; vous ne pouvez pas configurer des interfaces internes ou externes (vous pourrez les configurer ultérieurement dans l'interface graphique utilisateur).

Remarque Vous ne pouvez pas répéter le script de configuration de l'interface de ligne de commande si vous ne supprimez pas la configuration, par exemple, via une réinitialisation. Vous pouvez cependant modifier tous les paramètres ultérieurement dans l'interface de ligne de commande à l'aide des commandes **configure network**. Reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

Procédure

Étape 1 Connectez-vous au port de console du threat defense. Pour plus d'informations, reportez-vous à la rubrique Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 117.

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

Vous vous connectez à l'interface de ligne de commande de la console FXOS. Lors de la première connexion, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si vous avez modifié le mot de passe, mais que vous l'avez oublié, vous devez reconfigurer l'appareil pour réinitialiser le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure de réinstallation.

Exemple :

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

[...]

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

[...]

firepower#
```

Étape 2 Connectez-vous à l'interface de ligne de commande du threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 3 La première fois que vous vous connectez au threat defense, vous êtes invité à accepter le contrat de licence utilisateur final (CLUF) Le script de configuration de la CLI vous est ensuite présenté.

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

Reportez-vous aux instructions suivantes :

- **Saisissez la passerelle IPv4 par défaut pour l'interface de gestion** : si vous définissez une adresse IP manuelle, spécifiez le paramètre **data-interfaces** ou l'adresse IP du routeur de passerelle. Le paramètre **data-interfaces** envoie le trafic de gestion sortant via le fond de panier pour quitter une interface de données. Ce paramètre est utile si vous ne disposez pas d'un réseau de gestion distinct pouvant accéder à Internet. Le trafic provenant de l'interface de gestion inclut l'enregistrement des licences et les mises à jour de la base de données qui nécessitent un accès Internet. Si vous utilisez le paramètre **data-interfaces**, vous pouvez toujours utiliser le gestionnaire d'appareils (ou SSH) sur l'interface de gestion si vous êtes directement connecté au réseau de gestion, mais pour la gestion à distance de réseaux ou d'hôtes spécifiques, vous devez ajouter une route statique à l'aide de la commande **configure network static-routes**. Notez que ce paramètre n'a pas d'incidence sur la gestion du gestionnaire d'appareils sur les interfaces de données. Si vous utilisez DHCP, le système utilise la passerelle fournie par DHCP et utilise le paramètre **data-interfaces** comme méthode de secours si DHCP ne fournit pas de passerelle.
- **Si vos informations réseau ont changé, vous devrez vous reconnecter** : si vous êtes connecté à SSH avec l'adresse IP par défaut, mais que vous modifiez l'adresse IP lors de la configuration initiale, vous êtes déconnecté. Reconnectez-vous en utilisant une nouvelle adresse IP et un nouveau mot de passe. Les connexions de console restent actives.
- **Gérer l'appareil localement ?** : saisissez **oui** pour utiliser le gestionnaire d'appareils ou le CDO/gestionnaire d'appareils. Une réponse **négative** signifie que vous avez l'intention d'utiliser le centre de gestion pour gérer l'appareil.

Exemple :

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

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

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

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

>
```

Étape 4 Connectez-vous au gestionnaire d'appareils avec la nouvelle adresse IP de gestion.

Se connecter au Gestionnaire d'appareils

Connectez-vous au gestionnaire d'appareils pour configurer votre threat defense.

Avant de commencer

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

Procédure

Étape 1 Saisissez l'URL suivante dans votre navigateur.

- (7.0 et versions ultérieures) Interne (Ethernet1/2 à 1/8)—**https://192.168.95.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutateur interne (Ethernet 1/2 à 1/8).
- (6.7 et versions antérieures) Interne (Ethernet1/2 à 1/8)—**https://192.168.1.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutateur interne (Ethernet 1/2 à 1/8).
- (6.6 et versions ultérieures) Gestion—**https://***ip_gestion*. Dans la mesure où l'interface de gestion est un client DHCP, l'adresse IP dépend de votre serveur DHCP. Si vous avez modifié l'adresse IP de gestion lors de la configuration de l'interface de ligne de commande, saisissez cette adresse.
- (6.5 et versions antérieures) Gestion—**https://192.168.45.45**. Si vous avez modifié l'adresse IP de gestion lors de la configuration de l'interface de ligne de commande, saisissez cette adresse.

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

Que faire ensuite

- exécutez l'assistant de configuration de gestionnaire d'appareils ; consultez la rubrique Terminer la configuration initiale, à la page 105.

Terminer la configuration initiale

Utilisez l'assistant de configuration lors de votre première connexion au gestionnaire d'appareils pour terminer la configuration initiale. Une fois l'assistant de configuration terminé, l'appareil doit être opérationnel et les politiques de base suivantes doivent être en place :

- Une interface externe (Ethernet1/1) et une interface interne. Les ports Ethernet 1/2 à 1/8 sont des ports de commutateur sur l'interface VLAN1 interne (6.5 et versions ultérieures) ou des membres du groupe de ponts interne sur BVI1 (6.4).
- Des zones de sécurité pour les interfaces internes et externes.
- Une règle d'accès approuvant tout le trafic interne vers le trafic externe.
- Une règle NAT d'interface qui traduit tout le trafic interne vers le trafic externe en ports uniques sur l'adresse IP de l'interface externe.

- Un serveur DHCP exécuté sur l'interface interne.

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

Procédure

Étape 1 Vous êtes invité à lire et à accepter le contrat de licence de l'utilisateur final et à modifier le mot de passe admin.

Vous devez suivre ces étapes pour continuer.

Étape 2 Configurez les options suivantes pour les interfaces externes et de gestion, puis cliquez sur **Suivant**.

Remarque Vos paramètres sont déployés sur l'appareil lorsque vous cliquez sur **Suivant**. L'interface est nommée « externe » et est ajoutée à la zone de sécurité « zone_externe ». Vérifiez que vos paramètres sont corrects.

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

Configurer IPv4 : adresse IPv4 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. Le protocole PPPoE peut être nécessaire si l'interface est connectée à un modem ADSL, un modem câble ou une autre connexion à votre FAI et que votre FAI utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE après avoir terminé l'assistant.

Configurer IPv6 : adresse IPv6 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv6.

b) **Interface de gestion**

Serveurs DNS : serveur DNS pour l'adresse de gestion du système. Saisissez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. La valeur par défaut est Serveurs DNS publics OpenDNS. Si vous modifiez les champs et souhaitez rétablir les paramètres par défaut, cliquez sur **Utiliser OpenDNS** pour recharger les adresses IP appropriées dans les champs.

Nom d'hôte du pare-feu : nom d'hôte de l'adresse de gestion du système.

Étape 3 Configurez les paramètres d'heure système et cliquez sur **Suivant**.

a) **Fuseau horaire** : sélectionnez le fuseau horaire du système.
b) **Serveur de temps NTP** : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

Étape 4 (facultatif) Configurez les licences Smart du système.

L'achat d'un appareil threat defense inclut automatiquement une licence de base. Toutes les licences supplémentaires sont facultatives.

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

Pour enregistrer l'appareil immédiatement, cliquez sur le lien pour vous connecter à votre compte Smart Software Manager et consultez la rubrique Configurer l'octroi de licences, à la page 107.

Pour utiliser la licence d'évaluation, sélectionnez **Démarrer la période d'évaluation de 90 jours sans inscription**.

Étape 5 Cliquez sur **Terminer**.

Que faire ensuite

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

Configurer l'octroi de licences

Le threat defense utilise l'outil Cisco Smart Software Licensing, qui vous permet d'acheter et de gérer un pool de licences de manière centralisée.

Lorsque vous enregistrez le châssis, l'outil Smart Software Manager délivre un certificat d'identification pour établir la communication entre le châssis et Smart Software Manager. Il attribue également le châssis au compte virtuel approprié.

Pour une présentation complète de Cisco Licensing, rendez-vous sur cisco.com/go/licensingguide.

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

- **Menace** : sécurité adaptative et système de prévention des intrusions de nouvelle génération
- **Malware** : protection contre les programmes malveillants
- **URL** : filtrage des URL
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN uniquement

Avant de commencer

- Veillez à disposer d'un compte principal sur 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 entreprise.

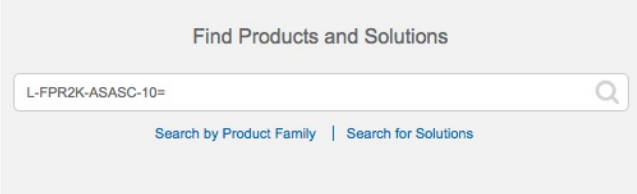
- Votre compte Smart Software Licensing doit bénéficier de la licence de chiffrement renforcé (3DES/AES) pour utiliser certaines fonctionnalités (activées à l'aide de l'indicateur de conformité d'exportation).

Procédure

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

Si vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte Smart Software License. Toutefois, si vous devez ajouter des licences vous-même, utilisez le champ de recherche **Rechercher des produits et des solutions** de Cisco Commerce Workspace. Recherchez les PID de licence suivants :

Illustration 27 : Recherche de licences



Remarque Si aucun PID n'est renvoyé, vous pouvez l'ajouter manuellement à votre commande.

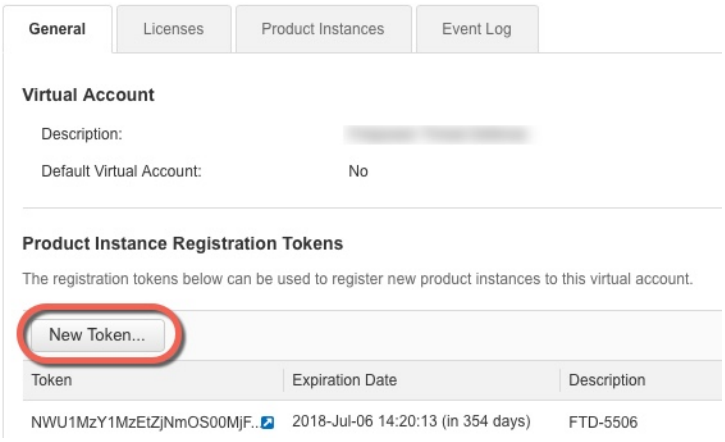
- Combinaison des licences Threat, Malware et URL :
  - L-FPR1010T-TMC=

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

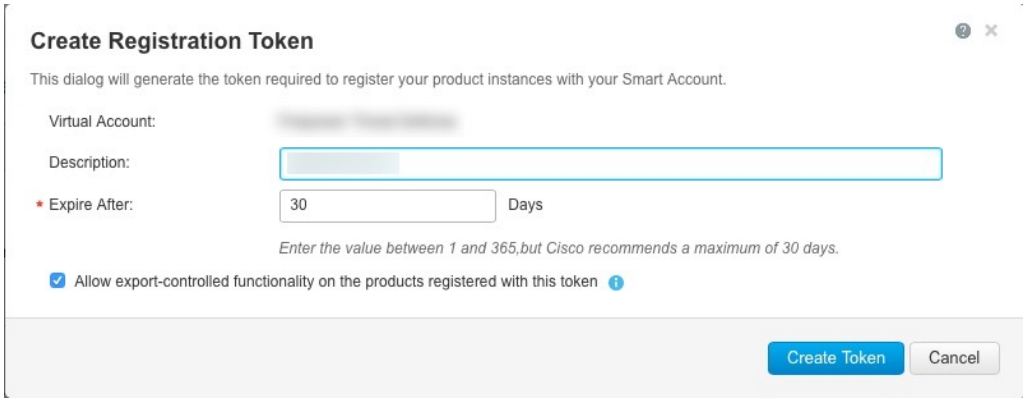
Étape 2 Dans Smart Software Manager, demandez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter cet appareil, et copiez-le.

a) Cliquez sur **Inventaire**.

b) Dans l'onglet **Général**, cliquez sur **Nouveau jeton**.



c) Dans la boîte de dialogue **Créer un jeton d'enregistrement**, saisissez les paramètres suivants, puis cliquez sur **Créer un jeton** :



- **Description**
- **Délai d'expiration** : Cisco recommande de définir un délai de 30 jours.
- **Autoriser la fonctionnalité de contrôle d'exportation sur les produits enregistrés avec ce jeton** : active l'indicateur de conformité d'exportation si vous êtes dans un pays qui autorise un chiffrement renforcé. Vous devez sélectionner cette option maintenant si vous prévoyez d'utiliser cette fonctionnalité. Si vous activez cette fonctionnalité ultérieurement, vous devrez réenregistrer votre appareil avec une nouvelle clé de produit et recharger l'appareil. Si cette option n'est pas disponible, votre compte ne prend pas en charge la fonctionnalité de contrôle d'exportation.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône représentant une flèche à droite du jeton pour ouvrir la boîte de dialogue **Jeton** afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour l'utiliser plus tard dans la procédure d'enregistrement du threat defense.

Illustration 28 : Afficher le jeton

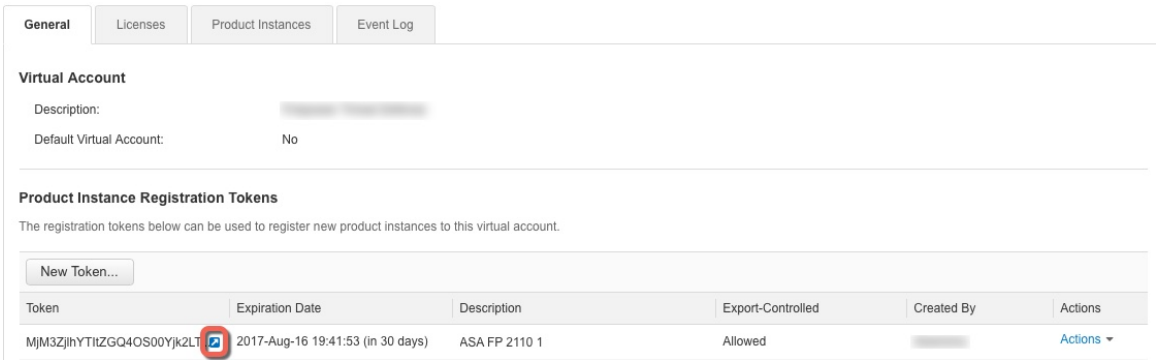
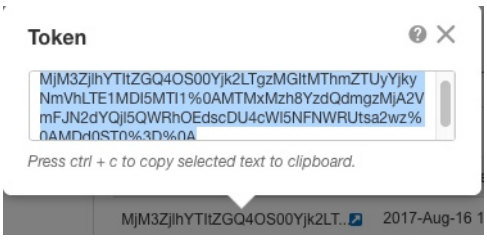


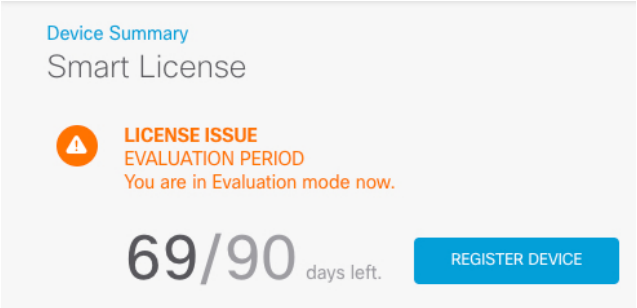
Illustration 29 : Copier le jeton



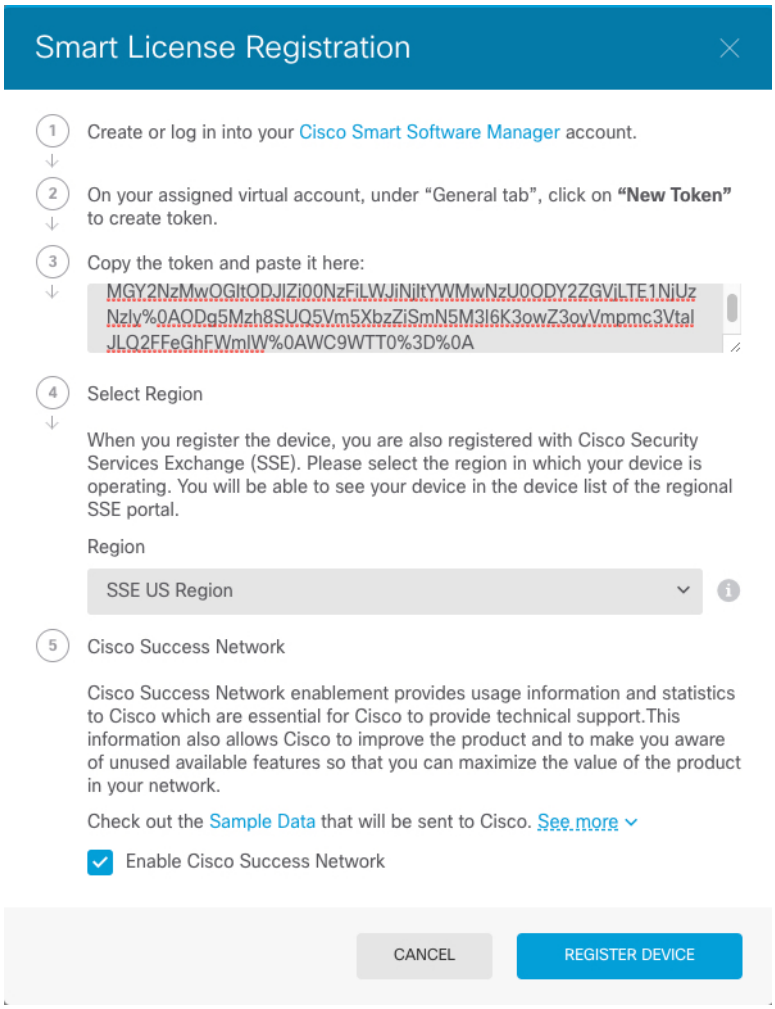
Étape 3 Dans le gestionnaire d'appareils, cliquez sur **Appareil**, puis, dans le récapitulatif **Licence Smart**, cliquez sur **Afficher la configuration**.

La page **Licence Smart** s'affiche.

Étape 4 Cliquez sur **Enregistrer l'appareil**.



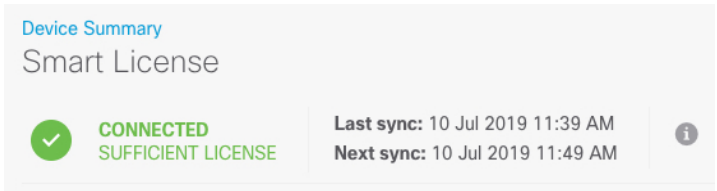
Suivez ensuite les instructions de la boîte de dialogue **Enregistrement de la licence Smart** pour coller votre jeton :



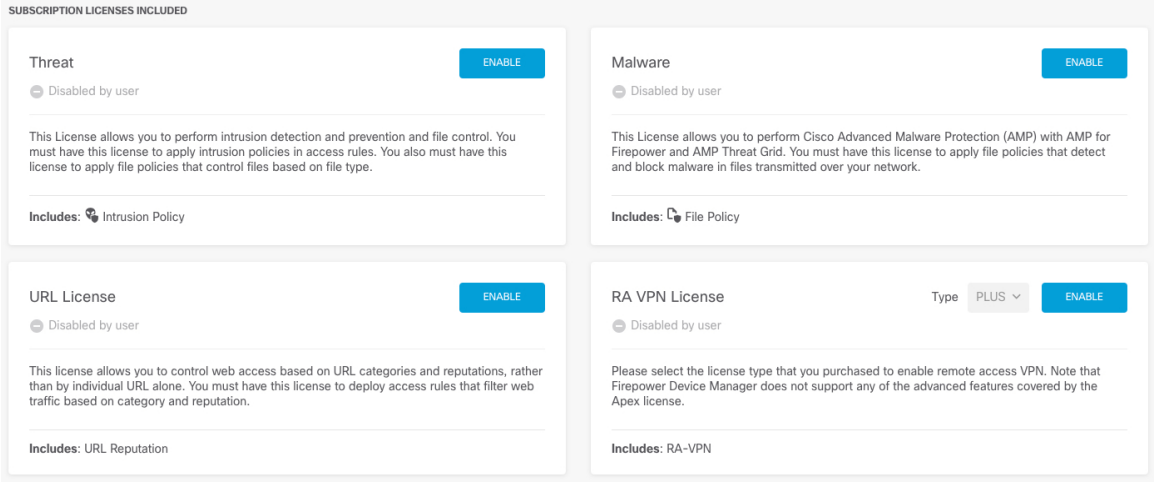
Étape 5 Cliquez sur **Enregistrer l'appareil**.

Vous revenez à la page **Licence Smart**. Pendant l'enregistrement de l'appareil, le message suivant s'affiche :

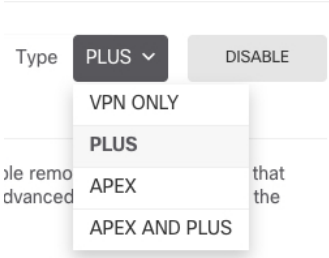
Une fois l'appareil enregistré et la page actualisée, les informations suivantes s'affichent :



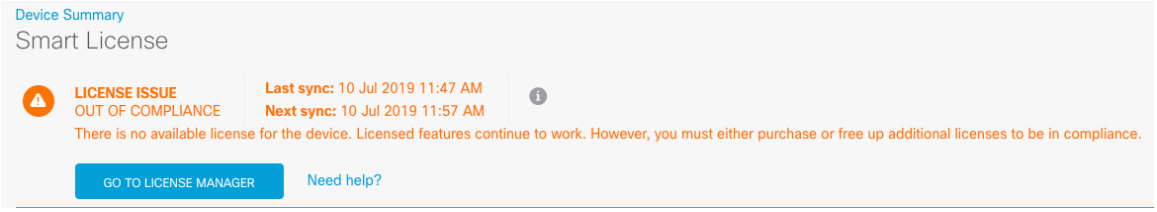
Étape 6 Cliquez sur la commande **Activer/Désactiver** en regard de chaque licence facultative.



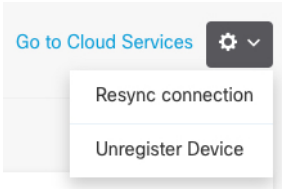
- **Activer** : enregistre la licence avec votre compte Cisco Smart Software Manager et active les fonctionnalités contrôlées. Vous pouvez maintenant configurer et déployer des politiques contrôlées par la licence.
- **Désactiver** : annule l'enregistrement de la licence avec votre compte Cisco Smart Software Manager et désactive les fonctionnalités contrôlées. Vous ne pouvez pas configurer les fonctionnalités dans de nouvelles politiques, ni déployer des politiques qui utilisent cette fonctionnalité.
- Si vous avez activé la licence **VPN RA**, sélectionnez le type de licence que vous souhaitez utiliser : **Plus**, **Apex**, **VPN uniquement** ou **Plus et Apex**.



Après avoir activé les fonctionnalités, si vous ne disposez pas des licences dans votre compte, le message de non-conformité suivant s'affiche après l'actualisation de la page :



Étape 7 Sélectionnez **Synchroniser de nouveau la connexion** dans la liste déroulante de l'icône d'engrenage pour synchroniser les informations de licence avec Cisco Smart Software Manager.



Configurer le pare-feu dans le Gestionnaire d'appareils

Consultez les étapes suivantes pour connaître les fonctionnalités supplémentaires que vous souhaitez configurer. Cliquez sur le bouton d'aide (**?**) sur une page pour obtenir des informations détaillées sur chaque étape.

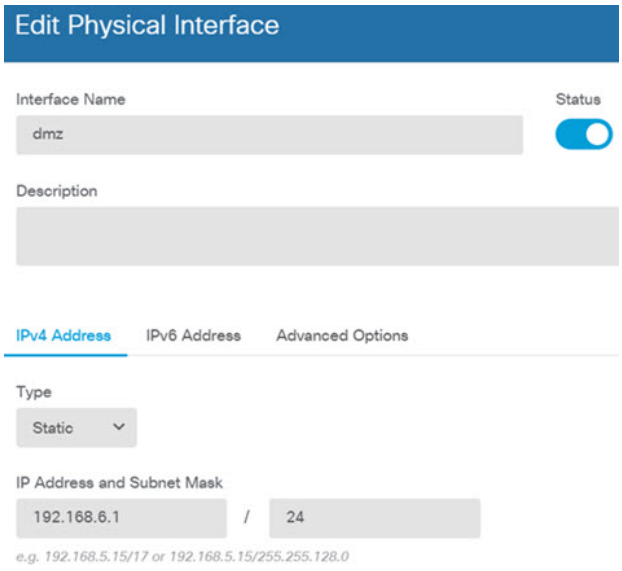
Procédure

Étape 1 Si vous souhaitez convertir une interface de groupe de ponts (6.4) ou souhaitez convertir un port de commutateur en interface de pare-feu (6.5 et versions ultérieures), sélectionnez **Appareil**, puis cliquez sur le lien dans le récapitulatif **Interfaces**.

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

L'exemple suivant configure une interface à utiliser en tant que « zone démilitarisée » (DMZ), dans laquelle vous placez des ressources accessibles au public, par exemple votre serveur web. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Illustration 30 : Modifier l'interface



Étape 2 Si vous avez configuré de nouvelles interfaces, sélectionnez **Objets**, puis sélectionnez **Zones de sécurité** dans la table des matières.

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

Dans l'exemple suivant, nous vous expliquons comment créer une nouvelle zone DMZ pour l'interface DMZ.

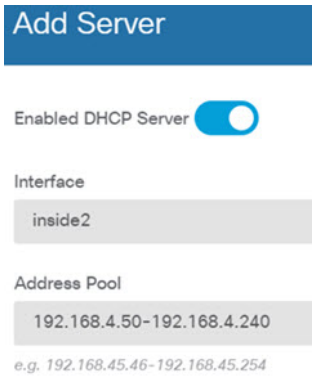
Illustration 31 : Objet de la zone de sécurité

Étape 3 Si vous souhaitez que les clients internes utilisent DHCP pour obtenir une adresse IP de l'appareil, sélectionnez **Appareil** > **Paramètres système** > **Serveur DHCP**, puis sélectionnez l'onglet **Serveurs DHCP**.

Un serveur DHCP est déjà configuré pour l'interface interne, mais vous pouvez modifier le pool d'adresses, voire le supprimer. Si vous avez configuré d'autres interfaces internes, il est très fréquent d'installer un serveur DHCP sur ces interfaces. Cliquez sur + pour configurer le serveur et le pool d'adresses pour chaque interface interne.

Vous pouvez également ajuster la liste WINS et DNS fournie aux clients dans l'onglet **Configuration**. Dans l'exemple suivant, nous vous expliquons comment configurer un serveur DHCP sur l'interface interne2 avec le pool d'adresses 192.168.4.50-192.168.4.240.

Illustration 32 : Serveur DHCP



Étape 4 Sélectionnez **Appareil**, puis cliquez sur **Afficher la configuration** (ou sur **Créer la première route statique**) dans le groupe **Routage** et configurez une route par défaut.

La route par défaut pointe généralement vers le routeur en amont ou le routeur du FAI qui se trouve hors de l'interface externe. Une route IPv4 par défaut est any-ipv4 (0.0.0.0/0), tandis qu'une route IPv6 par défaut est

any-ipv6 (::0/0). Créez des routes pour chaque version IP que vous utilisez. Si vous utilisez DHCP pour obtenir une adresse pour l'interface externe, vous disposez peut-être déjà des routes par défaut dont vous avez besoin.

Remarque Les routes que vous définissez sur cette page concernent uniquement les interfaces de données. Elles n'ont pas d'impact sur l'interface de gestion. Définissez la passerelle de gestion sur **Appareil** > **Paramètres système** > **Interface de gestion**.

L'exemple suivant présente une route par défaut pour IPv4. Dans cet exemple, isp-gateway est un objet réseau qui identifie l'adresse IP de la passerelle du FAI (vous devez obtenir l'adresse de auprès de votre FAI). Vous pouvez créer cet objet en cliquant sur **Créer un réseau** en bas de la liste déroulante **Passerelle**.

Illustration 33 : Route par défaut

Étape 5 Sélectionnez **Politiques** et configurez les politiques de sécurité du réseau.

L'assistant de configuration d'appareils active le flux de trafic entre la zone interne et la zone externe, et la NAT d'interface pour toutes les interfaces lorsqu'elles accèdent à l'interface externe. Même si vous configurez de nouvelles interfaces, si vous les ajoutez à l'objet de la zone interne, la règle de contrôle d'accès les applique automatiquement.

Cependant, si vous possédez plusieurs interfaces internes, vous devez disposer d'une règle de contrôle d'accès pour autoriser le flux de trafic d'une zone interne à l'autre. Si vous ajoutez d'autres zones de sécurité, vous devez disposer de règles pour autoriser le trafic vers et depuis ces zones. Il s'agit de vos modifications minimales.

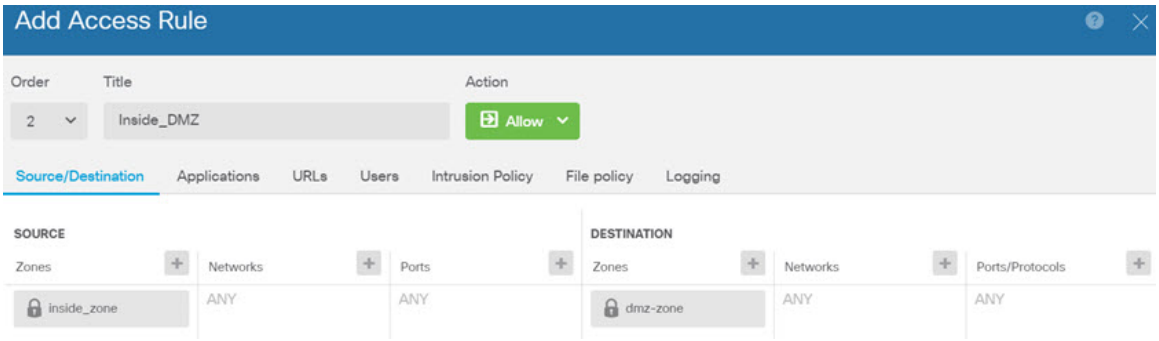
En outre, vous pouvez configurer d'autres politiques pour fournir des services supplémentaires et affiner la NAT et les règles d'accès pour obtenir les résultats dont votre organisation a besoin. Vous pouvez configurer les politiques suivantes :

- **Déchiffrement SSL** : si vous souhaitez inspecter les connexions chiffrées (telles que HTTPS) pour détecter les intrusions, les programmes malveillants, etc., vous devez les déchiffrer. Utilisez la politique de décodage SSL pour déterminer les connexions à déchiffrer. Le système chiffre à nouveau la connexion après l'avoir inspectée.
- **Identité** : si vous souhaitez mettre en corrélation l'activité du réseau avec des utilisateurs individuels ou contrôler l'accès au réseau en fonction de l'utilisateur ou du groupe d'utilisateurs, utilisez la politique d'identité pour déterminer l'utilisateur associé à une adresse IP source donnée.

- **Sécurité adaptative** : utilisez la politique Sécurité adaptative pour supprimer rapidement les connexions depuis ou vers les adresses IP ou les URL de la liste noire. Lorsque vous mettez en liste noire les sites malveillants connus, il est inutile de les prendre en compte dans votre politique de contrôle d'accès. Cisco fournit régulièrement des mises à jour des adresses et des URL malveillantes afin que la liste noire Sécurité adaptative se mette à jour dynamiquement. Utilisez des flux pour éviter de modifier la politique en vue d'ajouter ou de supprimer des éléments dans la liste noire.
- **NAT (traduction d'adresses réseau)** : utilisez la politique NAT pour convertir les adresses IP internes en adresses routables externes.
- **Contrôle d'accès** : utilisez la politique de contrôle d'accès pour déterminer les connexions autorisées sur le réseau. Vous pouvez filtrer par zone de sécurité, adresse IP, protocole, port, application, URL, utilisateur ou groupe d'utilisateurs. Vous appliquez également des politiques d'intrusion et de fichiers (programmes malveillants) à l'aide de règles de contrôle d'accès. Utilisez cette politique pour mettre en œuvre le filtrage des URL.
- **Intrusion** : utilisez les politiques d'intrusion pour détecter les menaces connues. Même si vous appliquez des politiques d'intrusion à l'aide de règles de contrôle d'accès, vous pouvez modifier les politiques d'intrusion pour activer ou désactiver sélectivement des règles d'intrusion spécifiques.

Dans l'exemple suivant, nous vous expliquons comment autoriser le trafic entre la zone interne et la zone DMZ dans la politique de contrôle d'accès. Dans cet exemple, aucune option n'est définie dans les autres onglets, à l'exception de **Journalisation**, où l'option **À la fin de la connexion** est sélectionnée.

Illustration 34 : Politique de contrôle d'accès



Étape 6 Sélectionnez **Appareil**, puis cliquez sur **Afficher la configuration** dans le groupe **Mises à jour** et configurez les planifications de mises à jour pour les bases de données système.

Si vous utilisez des politiques d'intrusion, configurez des mises à jour régulières pour les règles et les bases de données VDB. Si vous utilisez des flux de sécurité adaptative, planifiez la mise à jour de ces flux. Si vous utilisez la géolocalisation dans des politiques de sécurité comme critères de correspondance, planifiez la mise à jour de cette base de données.

Étape 7 Cliquez sur le bouton **Déployer** dans le menu, puis sur le bouton Déployer maintenant ( ) pour déployer vos modifications sur l'appareil.

Les modifications ne sont pas appliquées sur l'appareil tant que vous ne les déployez pas.

Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS

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

Vous pouvez également accéder à la CLI FXOS à des fins de dépannage.

Remarque Vous pouvez également vous connecter à l'interface de gestion de l'appareil threat defense. Contrairement à une session de console, la session SSH utilise par défaut l'interface de ligne de commande du threat defense, à partir de laquelle vous pouvez vous connecter à la CLI FXOS à l'aide de la commande **connect fxos**. Vous pourrez 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 console, qui est défini par défaut sur la CLI FXOS.

Procédure

Étape 1 Pour vous connecter à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. L'appareil Firepower 1000 est livré avec un câble série USB A vers B. Veillez à installer les pilotes série USB nécessaires à votre système d'exploitation (consultez le guide matériel de l'appareil Firepower 1010). Le port de console est défini par défaut sur la CLI FXOS. Utilisez les paramètres série suivants :

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

Vous vous connectez à la CLI FXOS. Connectez-vous à l'interface de ligne de commande à l'aide du nom d'utilisateur **admin** et du 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 du threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après vous être connecté, pour obtenir des informations sur les commandes disponibles dans l'interface de ligne de commande, saisissez **help** ou **?**. Pour plus d'informations sur l'utilisation, reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande threat defense, saisissez la commande du **exit** ou **logout**.

Cette commande vous renvoie à l'invite de la CLI FXOS. Pour plus d'informations sur les commandes disponibles dans la CLI FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Afficher les informations sur le matériel

Utilisez l'interface de ligne de commande (CLI) pour afficher des informations sur votre matériel, notamment le modèle de l'appareil, la version du matériel, le numéro de série et les composants du châssis, y compris les modules d'alimentation et les modules réseau. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console ; reportez-vous à la rubrique Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 117.

Procédure

Étape 1 Pour afficher le modèle matériel de l'appareil, utilisez la commande **show model**.

>**show model**

Exemple :

```
> show model
Cisco Firepower 1010 Threat Defense
```

Étape 2 Pour afficher le numéro de série du châssis, utilisez la commande **show serial-number**.

>**show serial-number**

Exemple :

```
> show serial-number
JMX19434085
```

Ces informations figurent également dans le résultat des commandes **show version system**, **show running-config** et **show inventory**.

Étape 3 Pour afficher des informations sur tous les produits Cisco installés sur l'appareil réseau auxquels sont attribués un identifiant de produit (PID), un identifiant de version (VID) et un numéro de série (SN), utilisez la commande **show inventory**.

>**show inventory**

a) À partir de l'interface de ligne de commande du threat defense :

Exemple :

```
> show inventory
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010          , VID: V00     , SN: JMX1943408S
```

b) À partir de l'interface de ligne de commande de FXOS :

Exemple :

```
firepower /chassis # show inventory
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-1010        Cisco Systems, In JMX1943408S 0.3
```

Mettre le pare-feu hors tension

Il est important que vous arrêtiez correctement votre système. Il ne suffit pas de débrancher le câble d'alimentation, car vous risquez d'endommager gravement le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en arrière-plan en permanence, et que débrancher ou couper l'alimentation ne permet pas un arrêt normal de votre système de pare-feu.

Le châssis initial de l'appareil Firepower 1010 ne possède pas d'interrupteur d'alimentation.Vous pouvez mettre le pare-feu hors tension à l'aide de gestionnaire d'appareils ou utiliser l'interface de ligne de commande de FXOS.

Mettre le pare-feu hors tension à l'aide du Gestionnaire d'appareils

Vous pouvez arrêter votre système correctement à l'aide du gestionnaire d'appareils.

Procédure

Étape 1 Utilisez le gestionnaire d'appareils pour arrêter le pare-feu.

Remarque Pour les versions 6.4 et antérieures, saisissez la commande **shutdown** dans l'interface de ligne de commande du gestionnaire d'appareils.

a) Cliquez sur **Appareil**, puis cliquez sur le lien **Paramètres système** > **Redémarrage/Arrêt**.
b) Cliquez sur **Arrêter**.

Étape 2 Si vous disposez d'une connexion de console au pare-feu, observez les invites système lorsque le pare-feu s'arrête. L'invite suivante s'affiche :

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

Si vous ne disposez pas d'une connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Étape 3 Vous pouvez désormais débrancher ce dernier pour couper l'alimentation du châssis si nécessaire.

Mettre l'appareil hors tension à l'aide de l'interface de ligne de commande

Vous pouvez utiliser l'interface de ligne de commande FXOS pour arrêter le système en toute sécurité et mettre l'appareil hors tension. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console ; reportez-vous à la rubrique Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 117.

Procédure

Étape 1 Dans la CLI FXOS, connectez-vous à l'interface de gestion locale :

firepower # **connect local-mgmt**

Étape 2 Exécutez la commande **shutdown** :

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

Exemple :

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

Étape 3 Observez les invites du système lorsque le pare-feu s'arrête. L'invite suivante s'affiche :

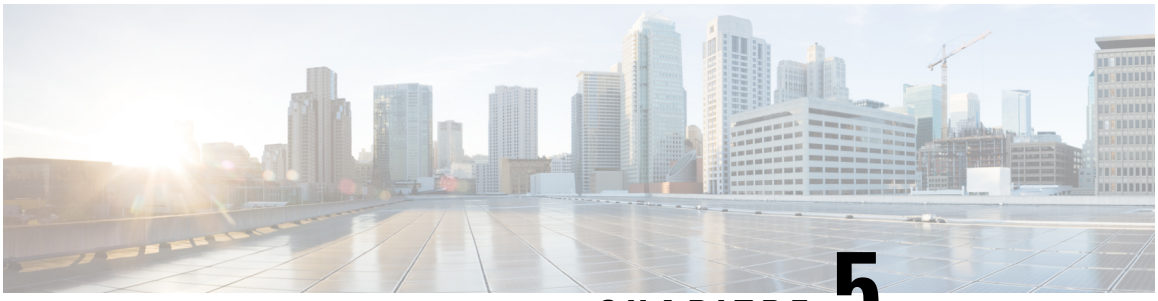
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Étape 4 Vous pouvez désormais débrancher ce dernier pour couper l'alimentation du châssis si nécessaire.

Et après ?

Pour poursuivre la configuration de votre threat defense, consultez les documents disponibles pour votre version logicielle dans Parcourir la documentation de Cisco Firepower.

Pour plus d'informations sur l'utilisation du gestionnaire d'appareils, reportez-vous à la rubrique Guide de configuration de Cisco Firepower Threat Defense pour le gestionnaire de périphériques Firepower.



CHAPITRE 5

Déployer Threat Defense avec le CDO

Ce chapitre vous concerne-t-il ?

Pour connaître tous les systèmes d'exploitation et gestionnaires disponibles, reportez-vous à la rubrique Quel système d'exploitation et quel gestionnaire vous conviennent le mieux ?, à la page 1. Ce chapitre s'adresse aux threat defense qui utilisent le Secure Firewall Management Center cloud de Cisco Defense Orchestrator (CDO). Pour utiliser le CDO avec la fonctionnalité gestionnaire d'appareils, consultez la documentation du CDO.

Remarque Le centre de gestion cloud prend en charge threat defense versions 7.2 et ultérieures. Pour les versions antérieures, vous pouvez utiliser la fonctionnalité gestionnaire d'appareils du CDO.

Chaque threat defense contrôle, inspecte, surveille et analyse le trafic. Le CDO possède une console de gestion centralisée avec une interface web que vous pouvez utiliser pour effectuer des tâches d'administration et de gestion afin de sécuriser votre réseau local.

À propos du pare-feu

L'appareil peut exécuter un logiciel threat defense ou un logiciel ASA. Pour basculer entre threat defense et ASA, vous devez reconfigurer l'appareil. Vous devez également recommencer l'installation si vous avez besoin d'une version logicielle différente de celle actuellement installée. Consultez la rubrique Réinstaller Cisco ASA ou Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé Système d'exploitation Secure Firewall eXtensible (FXOS). Le pare-feu ne prend pas en charge le Gestionnaire de châssis Secure Firewall FXOS ; seule une CLI limitée est prise en charge à des fins de dépannage. Pour obtenir plus d'informations, reportez-vous à la section Guide de dépannage Cisco FXOS pour la série Firepower 1000/2100 exécutant Firepower Threat Defense.

Déclaration de confidentialité—Le pare-feu ne requiert ni ne collecte activement aucune information permettant de vous identifier. Vous pouvez néanmoins utiliser des informations d'identification personnelle au cours de la configuration, notamment des noms d'utilisateur. Dans ce cas, un administrateur peut accéder à ces informations lors de l'utilisation de la configuration ou de l'utilisation du protocole SNMP.

À propos de la gestion du Threat Defense via le CDO

Secure Firewall Management Center sur le cloud

Le centre de gestion sur le cloud offre de nombreuses fonctions, à l'instar du centre de gestion sur site. Lorsque vous utilisez le CDO en tant que gestionnaire principal, vous ne pouvez utiliser un centre de gestion sur site qu'à des fins d'analyse. Le centre de gestion sur site ne prend pas en charge la configuration ou la mise à niveau des politiques.

Méthodes d'intégration du CDO

Vous pouvez intégrer un appareil de l'une des manières suivantes :

- Exécution de la fonction Low-touch provisioning à l'aide du numéro de série :
  - Un administrateur du siège central envoie le threat defense à la succursale distante. Aucune configuration préalable n'est requise. Aucune configuration n'est requise sur l'appareil, car la fonction LTP n'est pas disponible sur les appareils préconfigurés.

Remarque L'administrateur central peut préenregistrer le threat defense sur le CDO en utilisant le numéro de série du threat defense avant d'envoyer l'appareil à la succursale.

  - L'administrateur de la succursale raccorde les câbles du threat defense et le met sous tension.
  - L'administrateur central termine la configuration du threat defense à l'aide du CDO.

  Vous pouvez également utiliser un numéro de série si vous avez déjà commencé à configurer l'appareil dans le gestionnaire d'appareils, bien que cette méthode ne soit pas abordée dans ce guide.

- Assistant d'intégration à l'aide de l'enregistrement de la CLI : utilisez cette méthode manuelle si vous devez effectuer une préconfiguration ou si vous utilisez l'interface d'un gestionnaire que la fonction Low-Touch Provisioning ne prend pas en charge.

Interface d'accès du gestionnaire Threat Defense

Vous pouvez utiliser l'interface de gestion ou l'interface externe pour accéder au gestionnaire. Toutefois, ce guide couvre uniquement l'accès à l'interface externe. La fonction LTP prend en charge uniquement l'interface externe.

L'interface de gestion est une interface spéciale configurée séparément des interfaces de données du threat defense, et possède ses propres paramètres réseau. Les paramètres réseau de l'interface de gestion sont utilisés même si vous activez l'accès au gestionnaire sur une interface de données. L'ensemble du trafic de gestion provient toujours de l'interface de gestion ou est toujours acheminé vers cette interface. Lorsque vous activez l'accès au gestionnaire sur une interface de données, le threat defense transfère le trafic de gestion entrant via

le fond de panier à l'interface de gestion. Pour le trafic de gestion sortant, l'interface de gestion transfère le trafic via le fond de panier vers l'interface de données.

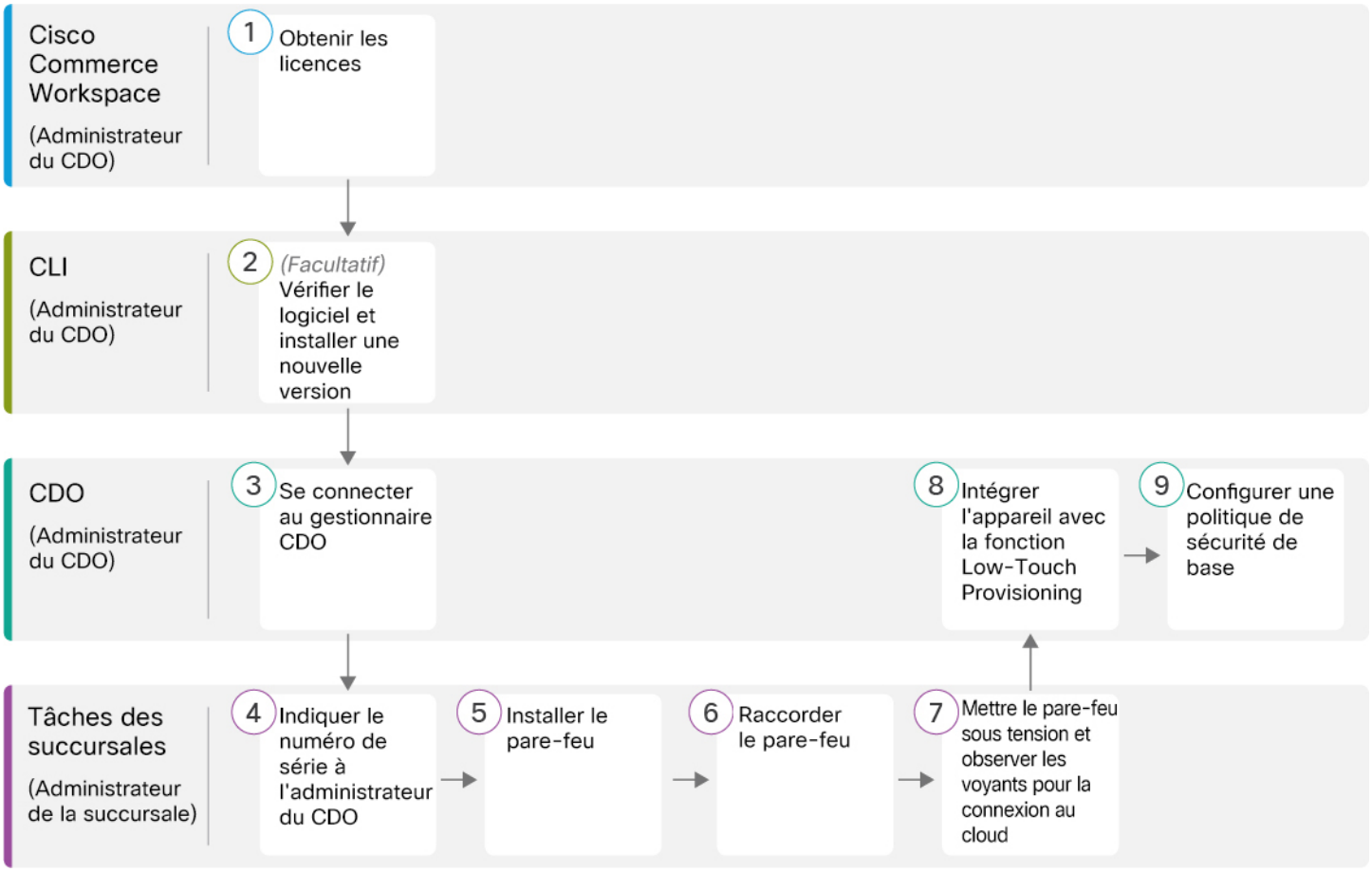
L'accès au gestionnaire à partir d'une interface de données présente les limitations suivantes :

- Vous ne pouvez activer l'accès au gestionnaire que sur une seule interface de données physique. Vous ne pouvez pas utiliser de sous-interface ou EtherChannel.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, à l'aide d'une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI nécessite un protocole PPPoE, vous devrez placer un routeur prenant en charge le protocole PPPoE entre le threat defense et le modem WAN.
- L'interface doit se trouver dans le VRF global uniquement.
- SSH n'est pas activé par défaut pour les interfaces de données. Vous devrez donc activer SSH ultérieurement avec le centre de gestion. Étant donné que la passerelle de l'interface de gestion sera remplacée par les interfaces de données, vous ne pouvez pas non plus accéder à l'interface de gestion depuis un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**.

Procédure de bout en bout : LTP (Low-Touch Provisioning)

Reportez-vous aux tâches suivantes pour déployer le threat defense avec le CDO sur votre châssis à l'aide du provisionnement presque entièrement automatisé.

Illustration 35 : Procédure de bout en bout : LTP (Low-Touch Provisioning)



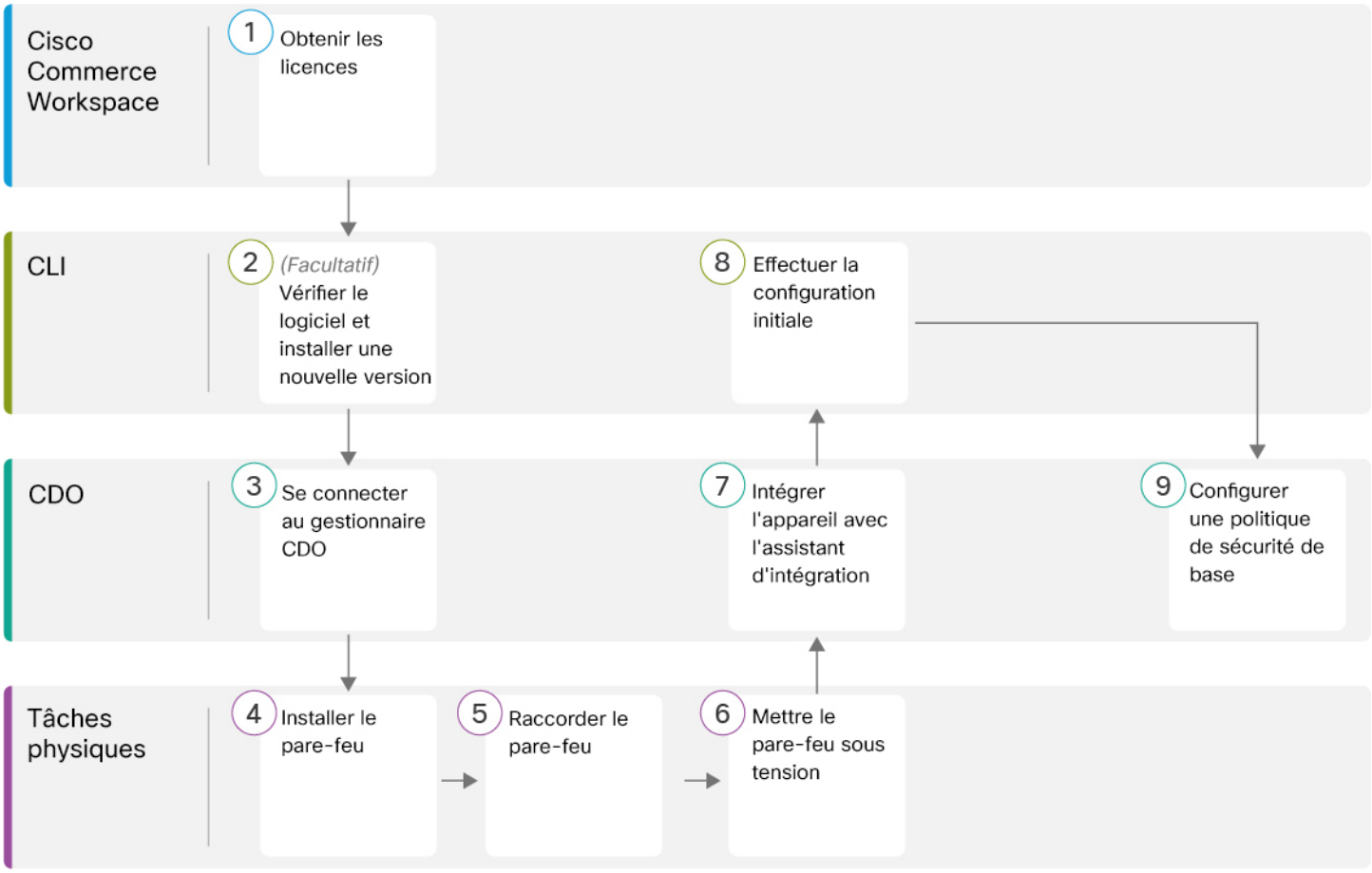
1	Cisco Commerce Workspace (Administrateur du CDO)	Obtenir les licences, à la page 127.
2	CLI (Administrateur du CDO)	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 128.
3	CDO (Administrateur du CDO)	Se connecter au gestionnaire CDO, à la page 130.
4	Tâches des succursales (Administrateur de la succursale)	Indiquer le numéro de série du pare-feu à l'administrateur central, à la page 134.

5	Tâches des succursales (Administrateur de la succursale)	Installez le pare-feu. Reportez-vous au guide d'installation matérielle.
6	Tâches des succursales (Administrateur de la succursale)	Raccorder le pare-feu, à la page 135.
7	Tâches des succursales (Administrateur de la succursale)	Mettre le pare-feu sous tension, à la page 136.
8	CDO (Administrateur du CDO)	Intégrer un appareil avec la fonction Low-Touch Provisioning, à la page 137.
9	CDO (Administrateur du CDO)	Configurer une politique de sécurité de base, à la page 152.

Procédure de bout en bout : assistant d'intégration

Reportez-vous aux tâches suivantes pour intégrer le threat defense au CDO à l'aide de l'assistant d'intégration.

Illustration 36 : Procédure de bout en bout : assistant d'intégration



1	Cisco Commerce Workspace	Obtenir les licences, à la page 127.
2	CLI	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 128.
3	CDO	Se connecter au gestionnaire CDO, à la page 130.
4	Tâches physiques	Installez le pare-feu. Reportez-vous au guide d'installation matérielle.
5	Tâches physiques	Raccorder le pare-feu, à la page 138.
6	Tâches physiques	Mettre le pare-feu sous tension, à la page 140.
7	CDO	Intégrer un appareil avec l'assistant d'intégration, à la page 140.

8	Interface de ligne de commande ou Gestionnaire d'appareils	• Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 142. • Effectuer la configuration initiale à l'aide du Gestionnaire d'appareils, à la page 146.
9	CDO	Configurer une politique de sécurité de base, à la page 152.

Configuration préalable de l'administrateur central

Dans cette section, nous vous expliquons comment obtenir des licences de fonctionnalités pour votre pare-feu, comment installer une nouvelle version logicielle avant le déploiement et comment se connecter au CDO.

Obtenir les licences

Toutes les licences sont fournies au threat defense via le CDO. Vous pouvez éventuellement acheter les licences de fonctionnalités suivantes :

- **Menace** : sécurité adaptative et système de prévention des intrusions de nouvelle génération
- **Malware** : protection contre les programmes malveillants
- **URL** : filtrage des URL
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN uniquement

Pour une présentation complète de Cisco Licensing, rendez-vous sur cisco.com/go/licensingguide.

Avant de commencer

- Veillez à disposer d'un compte principal sur Smart Software Manager.

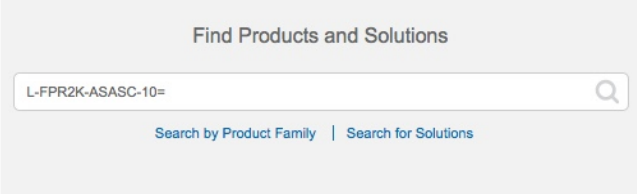
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre entreprise.
- Votre compte Smart Software Licensing doit bénéficier de la licence de chiffrement renforcé (3DES/AES) pour utiliser certaines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

Procédure

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

Si vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte Smart Software License. Toutefois, si vous devez ajouter des licences vous-même, utilisez le champ de recherche **Rechercher des produits et des solutions** de Cisco Commerce Workspace. Recherchez les PID de licence suivants :

Illustration 37 : Recherche de licences



Remarque Si aucun PID n'est renvoyé, vous pouvez l'ajouter manuellement à votre commande.

- Combinaison des licences Threat, Malware et URL :
  - L-FPR1010T-TMC=

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

Étape 2 Si cela n'est pas déjà fait, enregistrez le CDO auprès du gestionnaire Smart Software Manager.

Pour cela, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Reportez-vous à la documentation du CDO pour obtenir des instructions détaillées.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une autre version, 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 en regard du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de publication décrite dans la rubrique 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).

Avant de commencer

Pour la fonction LTP, si vous vous connectez et modifiez le mot de passe, vous désactivez le processus de LTP (Low-Touch Provisioning). Vous ne devez vous connecter et effectuer une réinstallation que si vous

savez déjà que vous devez modifier la version du logiciel. Si vous êtes connecté et souhaitez restaurer la fonctionnalité de LTP sans installer le logiciel, vous pouvez rétablir les paramètres d'usine. Consultez le Guide de dépannage de la console FXOS.

Procédure

Étape 1 Mettez le pare-feu sous tension et connectez-vous au port de console. Pour plus d'informations, consultez Mettre le pare-feu sous tension, à la page 140 et Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS, à la page 163.

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

Vous vous connectez à la CLI FXOS. Lors de la première connexion, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si vous avez modifié le mot de passe, mais que vous l'avez oublié, vous devez réinitialiser l'appareil pour rétablir le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure pour rétablir les paramètres 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 Dans l'interface de ligne de commande de la console FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

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

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

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

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, reportez-vous à la rubrique Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 142. Par défaut, l'interface de gestion utilise DHCP.

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

b) Suivez la procédure de réinstallation du guide de dépannage de la console FXOS.

Étape 4 Pour la fonction LTP, *ne vous connectez pas au pare-feu* après la réinstallation ; la connexion démarre la configuration initiale. La fonction LTP est disponible uniquement sur les pare-feu avec de nouvelles installations qui n'ont pas été configurées.

Se connecter au gestionnaire CDO

Le gestionnaire CDO utilise Cisco Secure Sign-On comme fournisseur d'identité et Duo Security pour l'authentification multifacteur (MFA). Le gestionnaire CDO nécessite une MFA qui fournit une couche de sécurité supplémentaire pour protéger l'identité de vos utilisateurs. L'authentification à deux facteurs, un type de MFA, nécessite deux composants (ou facteurs) pour garantir l'identité des utilisateurs qui se connectent au gestionnaire CDO.

Le premier facteur est un nom d'utilisateur et un mot de passe, et le second est un mot de passe à usage unique, qui est généré à la demande par Duo Security.

Après avoir établi vos informations d'identification Cisco Secure Sign-On, vous pouvez vous connecter au gestionnaire CDO à partir de votre tableau de bord Cisco Secure Sign-On. Le tableau de bord Cisco Secure Sign-On vous permet également de vous connecter à tous les autres produits Cisco pris en charge.

- Si vous disposez d'un compte Cisco Secure Sign-On, passez directement à la rubrique Se connecter au gestionnaire CDO avec Cisco Secure Sign-On, à la page 133.
- Si vous ne disposez pas d'un compte Cisco Secure Sign-On, passez à la rubrique Créer un nouveau compte Cisco Secure Sign-On, à la page 130.

Créer un nouveau compte Cisco Secure Sign-On

Le processus de connexion initiale comprend quatre étapes. Les quatre étapes sont obligatoires.

Avant de commencer

- **Installer Duo Security** : nous vous recommandons d'installer l'application Duo Security sur un terminal mobile. Consultez le Guide Duo pour l'authentification à deux facteurs : guide d'inscription si vous avez des questions sur l'installation de Duo.
- **Synchronisation de l'heure** : vous allez utiliser votre terminal mobile pour générer un mot de passe unique. Il est important que l'horloge de votre terminal soit synchronisée avec l'heure réelle, car l'OTP est basé sur le temps. Assurez-vous que l'horloge de votre terminal est correctement réglée.
- Utilisez une version actuelle de Firefox ou de Chrome.

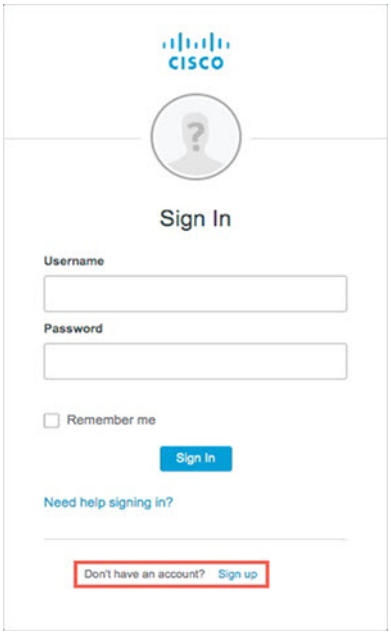
Procédure

Étape 1 **Inscrivez-vous pour un nouveau compte Cisco Secure Sign-On.**

a) Accédez à la page https://sign-on.security.cisco.com.

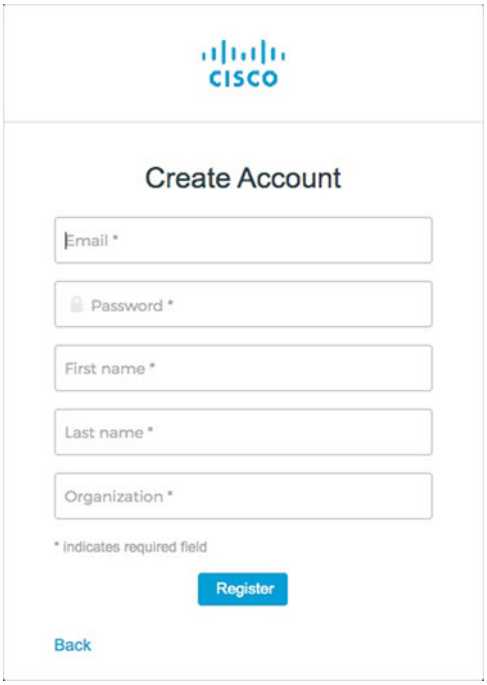
b) En bas de l'écran de connexion, cliquez sur **Inscription**.

Illustration 38 : Inscription à Cisco SSO



c) Renseignez les champs de la boîte de dialogue **Créer un compte** et cliquez sur **Enregistrer**.

Illustration 39 : Créer le compte



Conseil Saisissez l'adresse e-mail que vous prévoyez d'utiliser pour vous connecter à CDO et ajoutez un nom d'organisation correspondant à votre entreprise.

d) Après avoir cliqué sur **Enregistrer**, Cisco vous envoie un e-mail de vérification à l'adresse avec laquelle vous vous êtes enregistré. Ouvrez l'e-mail et cliquez sur **Activer le compte**.

Étape 2 **Configurez l'authentification multifacteur à l'aide de Duo.**

a) Dans l'écran **Configurer l'authentification multifacteur**, cliquez sur **Configurer**.
b) Cliquez sur **Démarrer la configuration** et suivez les instructions pour sélectionner un appareil et vérifier s'il est associé à votre compte.

Pour en savoir plus, consultez le Guide Duo pour l'authentification à deux facteurs : guide d'inscription. Si l'application Duo est déjà installée sur votre appareil, vous recevrez un code d'activation pour ce compte. Duo prend en charge plusieurs comptes sur un seul appareil.

c) Au terme de l'assistant, cliquez sur **Continuer pour vous connecter**.
d) Connectez-vous à Cisco Secure Sign-On avec l'authentification à deux facteurs.

Étape 3 (facultatif) **Configurez Google Authenticator en tant qu'authentificateur supplémentaire.**

a) Sélectionnez le terminal mobile que vous associez à Google Authenticator, puis cliquez sur **Suivant**.
b) Suivez les instructions de l'assistant de configuration pour configurer Google Authenticator.

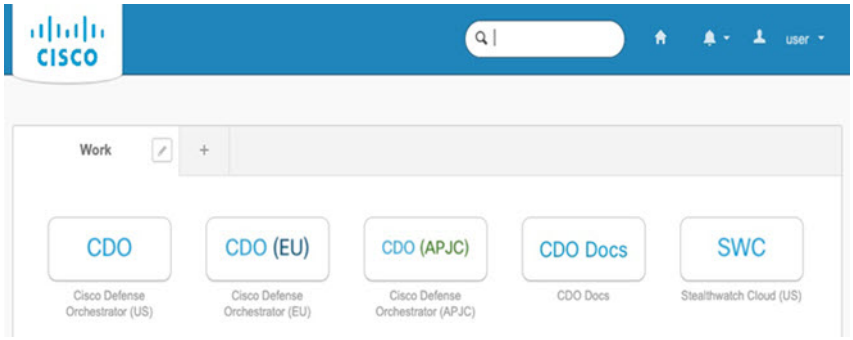
Étape 4 **Configurez les options de récupération du compte pour votre compte Cisco Secure Sign-On.**

a) Choisissez une question et une réponse en cas de « mot de passe oublié ».
b) Choisissez un numéro de téléphone de récupération pour réinitialiser votre compte par SMS.
c) Sélectionnez une image de sécurité.
d) Cliquez sur **Créer mon compte**.

Le tableau de bord Cisco Security Sign-On s'affiche avec les vignettes de l'application CDO. Les vignettes d'autres applications s'affichent également.

Conseil Vous pouvez déplacer les vignettes vers le tableau de bord pour les classer dans l'ordre de votre choix, créer des onglets pour regrouper les vignettes et les renommer.

Illustration 40 : Tableau de bord Cisco SSO



Se connecter au gestionnaire CDO avec Cisco Secure Sign-On

Connectez-vous au gestionnaire CDO pour intégrer et gérer votre appareil.

Avant de commencer

Cisco Defense Orchestrator (CDO) utilise Cisco Secure Sign-On comme fournisseur d'identité et Duo Security pour l'authentification multifacteur.

- Pour vous connecter à CDO, vous devez tout d'abord créer votre compte dans Cisco Secure Sign-On et configurer l'authentification multifacteur à l'aide de Duo ; consultez la rubrique Créer un nouveau compte Cisco Secure Sign-On, à la page 130.
- Utilisez une version actuelle de Firefox ou de Chrome.

Procédure

Étape 1 Dans un navigateur web, accédez à https://sign-on.security.cisco.com/.

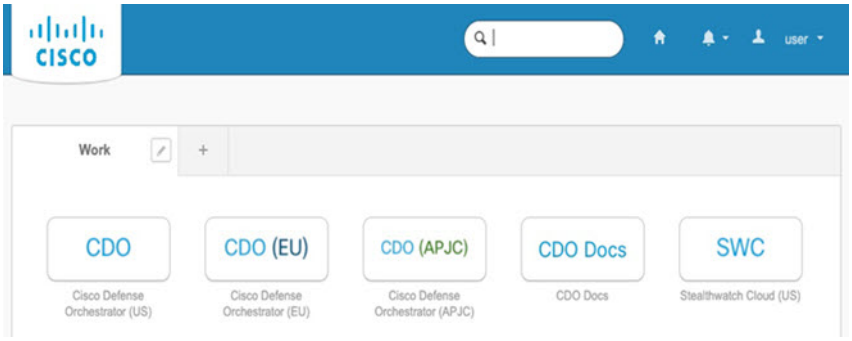
Étape 2 Saisissez votre **nom d'utilisateur** et votre **mot de passe**.

Étape 3 Cliquez sur **Log in**.

Étape 4 Recevez un autre facteur d'authentification avec Duo Security et confirmez votre connexion. Le système confirme votre connexion et affiche le tableau de bord Cisco Secure Sign-On.

Étape 5 Cliquez sur la vignette CDO appropriée dans le tableau de bord Cisco Secure Sign-on. La vignette **CDO** vous dirige vers https://defenseorchestrator.com, la vignette **CDO (UE)** vers https://defenseorchestrator.eu et la vignette **CDO (APJC)** vers https://www.apj.cdo.cisco.com.

Illustration 41 : Tableau de bord Cisco SSO



Étape 6 Cliquez sur le logo de l'authentificateur pour sélectionner **Duo Security** ou **Google Authenticator**, si vous avez configuré les deux authentificateurs.

- Si vous possédez déjà un enregistrement utilisateur sur un locataire existant, vous êtes connecté à ce locataire.
- Si vous possédez déjà un enregistrement utilisateur sur plusieurs locataires, vous pouvez choisir le locataire CDO auquel vous connecter.
- Si vous ne disposez pas déjà d'un enregistrement utilisateur sur un locataire existant, vous pouvez en savoir plus sur le gestionnaire CDO ou solliciter un compte d'essai.

Déployer le pare-feu avec la fonction Low-Touch Provisioning

Une fois que vous avez reçu le pare-feu threat defense du siège social, il vous suffit de le raccorder et de le mettre sous tension en vue de le connecter à Internet depuis l'interface externe. L'administrateur central peut alors terminer la configuration.

Indiquer le numéro de série du pare-feu à l'administrateur central

Avant de monter en rack le pare-feu ou de jeter l'emballage, notez le numéro de série afin de pouvoir vous coordonner avec l'administrateur central.

Procédure

Étape 1 Déballez le châssis et ses composants.

Faites l'inventaire de votre pare-feu et de son emballage avant de raccorder les câbles ou de mettre le pare-feu sous tension. Vous devez également vous familiariser avec la disposition du châssis, les composants et les voyants.

Étape 2 Notez le numéro de série du pare-feu.

Il se trouve sur le coffret de livraison. Il se trouve également sur un autocollant sur la partie inférieure du châssis du pare-feu.

Étape 3 Envoyez le numéro de série du pare-feu à l'administrateur réseau du CDO de votre service informatique/siège.

Votre administrateur réseau doit disposer du numéro de série de votre pare-feu pour activer la fonction LTP (Low-Touch Provisioning), se connecter au pare-feu et le configurer à distance.

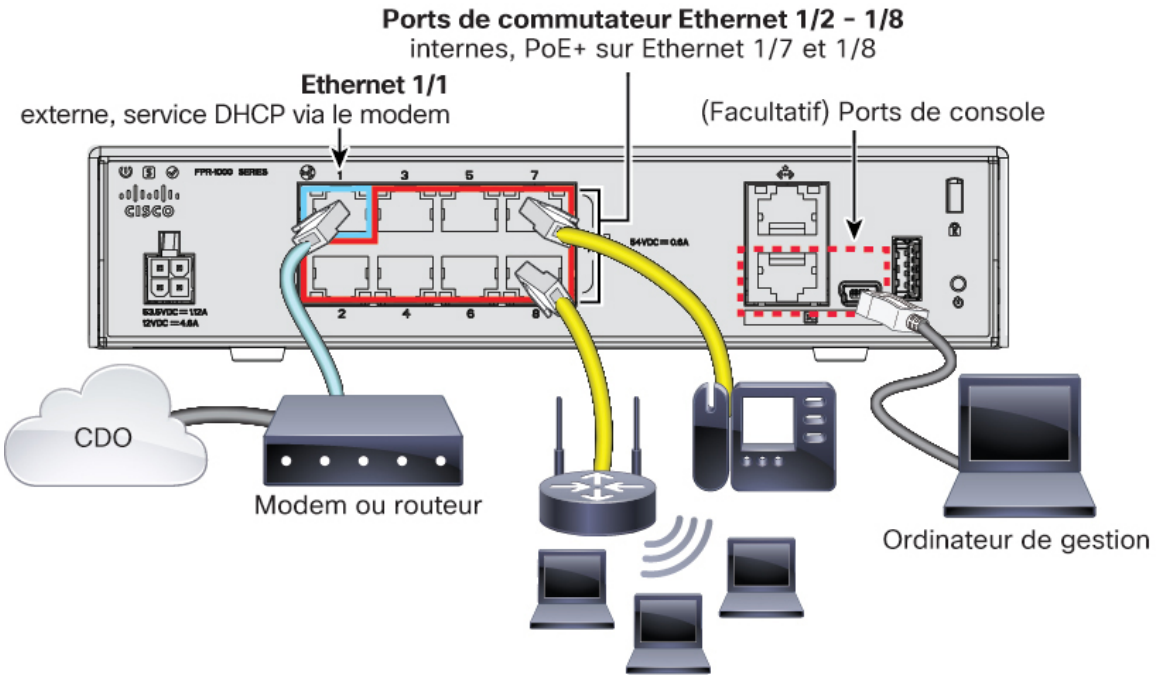
Contactez l'administrateur du CDO pour établir un calendrier d'intégration.

Raccorder le pare-feu

Dans cette rubrique, nous vous expliquons comment connecter l'appareil Firepower 1010 à votre réseau afin qu'un CDO puisse le gérer à distance.

Si vous avez reçu un pare-feu dans votre succursale et que vous devez le brancher sur votre réseau, regardez cette vidéo. Elle décrit votre pare-feu, ainsi que les séquences de voyants qui indiquent l'état du pare-feu. Si nécessaire, vous pouvez vérifier l'état du pare-feu auprès de votre service informatique en observant les voyants.

Illustration 42 : Raccorder le Firepower 1010



La fonction LTP prend en charge la connexion au CDO via Ethernet 1/1 (externe).

Remarque Les interfaces Ethernet 1/2 à 1/8 sont configurées en tant que ports de commutateur matériels ; PoE+ est également disponible sur Ethernet 1/7 et 1/8.

Procédure

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

Étape 2 Connectez le câble réseau de l'interface Ethernet 1/1 à votre modem de réseau étendu (WAN). Votre modem WAN établit la connexion Internet dans votre succursale et sert également de route vers Internet à votre pare-feu.

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

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

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

Dans la succursale, la connexion à la console n'est pas nécessaire pour une utilisation quotidienne ; elle peut cependant être nécessaire à des fins de dépannage.

Mettre le pare-feu sous tension

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

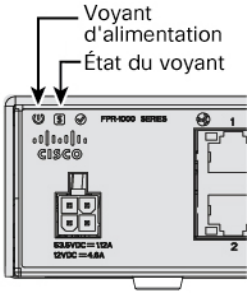
Remarque La première fois que vous démarrez le threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Procédure

Étape 1 Raccordez le câble d'alimentation à l'appareil et branchez-le à une prise électrique.

L'appareil se met automatiquement sous tension dès que vous le branchez.

Étape 2 Observez le voyant d'alimentation situé à l'arrière de l'appareil. S'il est allumé en vert, l'appareil est sous tension.



Étape 3 Observez le voyant d'état à l'arrière ou sur l'appareil. Lorsqu'il s'allume en vert, le système a terminé les diagnostics de mise sous tension.

Étape 4 Observez le voyant d'état à l'arrière ou en haut de l'appareil ; lorsque l'appareil démarre correctement, le voyant d'état clignote rapidement en vert.

En cas de problème, le voyant d'état clignote rapidement en orange. Le cas échéant, contactez votre service informatique.

Étape 5 Observez le voyant d'état à l'arrière ou en haut de l'appareil ; lorsque l'appareil se connecte au cloud Cisco, le voyant d'état clignote lentement en vert.

En cas de problème, le voyant d'état clignote en orange et en vert, ce qui signifie que l'appareil ne s'est pas connecté au cloud Cisco. Le cas échéant, assurez-vous que votre câble réseau est connecté à l'interface Ethernet 1/1 et à votre modem WAN. Si, après avoir ajusté le câble réseau, l'appareil ne se connecte toujours pas au cloud Cisco après environ 10 minutes supplémentaires, contactez votre service informatique.

Que faire ensuite

- Contactez votre service informatique pour confirmer votre calendrier d'intégration et vos activités. Vous devez mettre en place un plan de communication avec l'administrateur du CDO de votre siège central.
- Une fois cette tâche terminée, l'administrateur du CDO pourra configurer et gérer l'appareil à distance. Vous avez terminé.

Intégrer un appareil avec la fonction Low-Touch Provisioning

Intégrez le threat defense à l'aide de la fonction LTP (Low-Touch Provisioning) et du numéro de série.

Procédure

Étape 1 Dans le volet de navigation CDO, cliquez sur **Inventaires**, cliquez sur le bouton Plus bleu ( ) pour **intégrer** l'appareil.

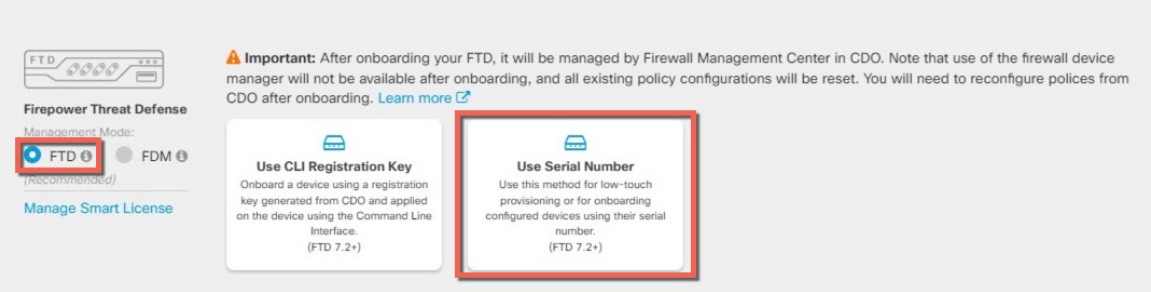
Étape 2 Sélectionnez la vignette **FTD**.

Étape 3 Sous **Mode de gestion**, assurez-vous que **FTD** est sélectionné.

À tout moment après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Gérer la licence Smart** pour enregistrer ou modifier les licences Smart existantes disponibles pour votre périphérique. Reportez-vous à la rubrique Obtenir les licences, à la page 127 pour connaître les licences disponibles.

Étape 4 Sélectionnez **Utiliser le numéro de série** comme méthode d'intégration.

Illustration 43 : Utiliser le numéro de série



Étape 5 Dans la zone **Connexion**, saisissez le **numéro de série** et le **nom de l'appareil**, puis cliquez sur **Suivant**.

Étape 6 Dans la zone **Réinitialisation du mot de passe**, cliquez sur la case d'option **Oui, ce nouvel appareil n'a jamais été connecté ou configuré pour un gestionnaire**, puis cliquez sur **Suivant**.

Étape 7 Utilisez le menu déroulant de la zone **Affectation de politique** pour choisir une politique de contrôle d'accès pour l'appareil. Si aucune politique n'est configurée, choisissez la **politique de contrôle d'accès par défaut**.

Étape 8 Pour la **Licence d'abonnement**, cochez la case en regard de chaque fonctionnalité que vous souhaitez activer. Cliquez sur **Next (Suivant)**.

Étape 9 (facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **Inventaire**. Saisissez une étiquette et cliquez sur le bouton bleu Plus (). Les étiquettes sont appliquées à l'appareil après son intégration au CDO.

Que faire ensuite

Sur la page **Inventaire**, sélectionnez l'appareil que vous venez d'intégrer et sélectionnez l'une des options répertoriées sous le volet **Gestion** situé à droite.

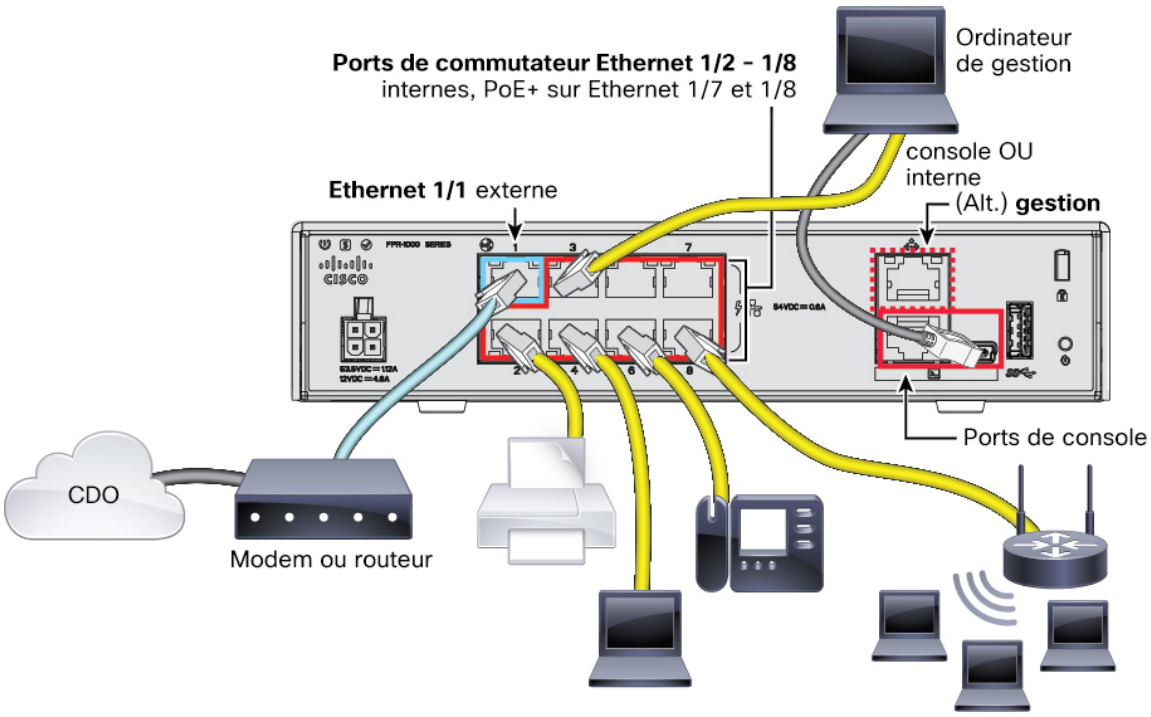
Déployer le pare-feu avec l'assistant d'intégration

Dans cette section, nous vous expliquons comment configurer le pare-feu en vue de l'intégrer à l'aide de l'assistant d'intégration du CDO.

Raccorder le pare-feu

Dans cette rubrique, nous vous expliquons comment connecter l'appareil Firepower 1010 à votre réseau afin qu'un CDO puisse le gérer à distance.

Illustration 44 : Raccorder le Firepower 1010



Vous pouvez vous connecter au CDO sur l'interface externe ou l'interface de gestion, selon l'interface que vous avez configurée pour l'accès du gestionnaire lors de la configuration initiale. Ce guide présente l'interface externe.

Remarque Les interfaces Ethernet 1/2 à 1/8 sont configurées en tant que ports de commutateur matériels ; PoE+ est également disponible sur Ethernet 1/7 et 1/8.

Procédure

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

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

Vous pouvez également utiliser l'interface de gestion pour l'accès au gestionnaire. Notez toutefois que ce guide couvre principalement l'accès aux interfaces externes, scénario le plus probable pour les succursales distantes.

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

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

Étape 4 Connectez l'ordinateur de gestion au port de console ou à une interface interne.

Si vous effectuez la configuration initiale à l'aide de l'interface de ligne de commande, vous devrez vous connecter au port de console. Le port de console peut également être requis à des fins de dépannage. Si vous effectuez la configuration initiale à l'aide du gestionnaire d'appareils, connectez-vous à une interface interne.

Mettre le pare-feu sous tension

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

Remarque La première fois que vous démarrez le threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Avant de commencer

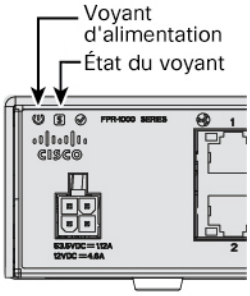
Il est important que vous utilisiez une source d'alimentation fiable pour alimenter votre appareil (à l'aide d'un système d'alimentation sans coupure, par exemple). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent en arrière-plan en permanence, et une panne de courant ne permet pas l'arrêt normal de votre système.

Procédure

Étape 1 Raccordez le câble d'alimentation à l'appareil et branchez-le à une prise électrique.

L'appareil se met automatiquement sous tension dès que vous le branchez.

Étape 2 Observez le voyant d'alimentation situé à l'arrière de l'appareil. S'il est allumé en vert, l'appareil est sous tension.



Étape 3 Observez le voyant d'état à l'arrière ou sur l'appareil. Lorsqu'il s'allume en vert, le système a terminé les diagnostics de mise sous tension.

Intégrer un appareil avec l'assistant d'intégration

Intégrez le threat defense à l'aide de l'assistant d'intégration du CDO avec une clé d'enregistrement de la CLI.

Procédure

Étape 1 Dans le volet de navigation CDO, cliquez sur **Inventaires**, cliquez sur le bouton Plus bleu ( ) pour **intégrer** l'appareil.

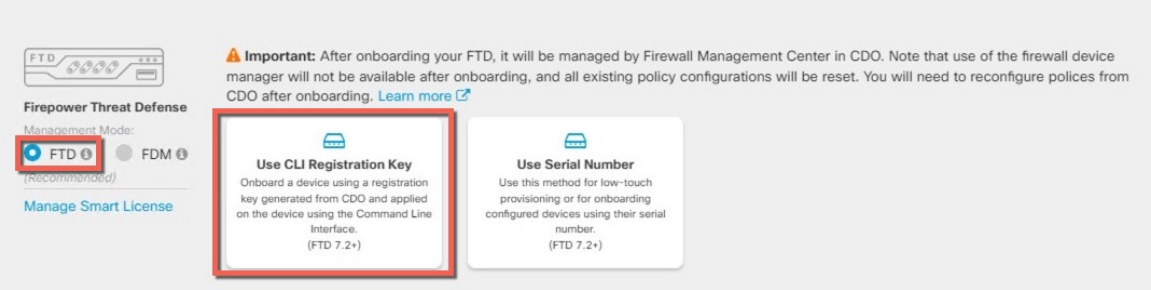
Étape 2 Sélectionnez la vignette **FTD**.

Étape 3 Sous **Mode de gestion**, assurez-vous que **FTD** est sélectionné.

À tout moment après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Gérer la licence Smart** pour enregistrer ou modifier les licences Smart existantes disponibles pour votre périphérique. Reportez-vous à la rubrique Obtenir les licences, à la page 127 pour connaître les licences disponibles.

Étape 4 Sélectionnez **Utiliser la clé d'enregistrement de la CLI** comme méthode d'intégration.

Illustration 45 : Utiliser la clé d'enregistrement de la CLI



Étape 5 Saisissez le **nom de l'appareil** et cliquez sur **Suivant**.

Étape 6 Utilisez le menu déroulant de la zone **Affectation de politique** pour choisir une politique de contrôle d'accès pour l'appareil. Si aucune politique n'est configurée, choisissez la **politique de contrôle d'accès par défaut**.

Étape 7 Pour la **licence d'abonnement**, cliquez sur la case d'option **Appareil FTD physique**, puis cochez chaque licence de fonctionnalité que vous souhaitez activer. Cliquez sur **Next (Suivant)**.

Étape 8 Pour la **clé d'enregistrement de la CLI**, le CDO génère une commande avec la clé d'enregistrement et d'autres paramètres. Vous devez copier cette commande et l'utiliser dans la configuration initiale du threat defense.

configure manager add *cdo_hostname registration_key nat_id display_name*

Finalisez la configuration initiale sur l'interface de ligne de commande ou à l'aide du gestionnaire d'appareils :

- Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 142 : copiez cette commande dans l'interface de ligne de commande du FTD après avoir terminé le script de démarrage.
- Effectuer la configuration initiale à l'aide du Gestionnaire d'appareils, à la page 146 : copiez les parties *cdo_hostname*, *registration_key* et *nat_id* de la commande dans les champs **Nom d'hôte/adresse IP du centre de gestion/CDO**, **Clé d'enregistrement du centre de gestion/CDO** et **ID NAT**.

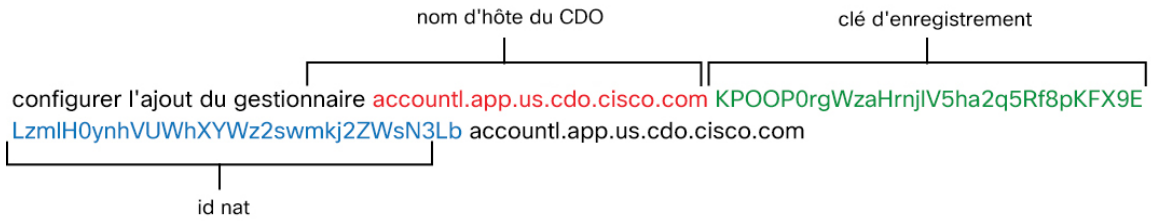
Exemple :

Exemple de commande pour la configuration de la CLI :

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

Exemples de composants de commande pour la configuration de l'interface graphique utilisateur :

Illustration 46 : configurer l'ajout de composants de commande du gestionnaire



Étape 9 Cliquez sur **Suivant** dans l'assistant d'intégration pour commencer à enregistrer l'appareil.

Étape 10 (facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **Inventaire**. Saisissez une étiquette et cliquez sur le bouton bleu Plus (+). Les étiquettes sont appliquées à l'appareil après son intégration au CDO.

Que faire ensuite

Sur la page **Inventaire**, sélectionnez l'appareil que vous venez d'intégrer et sélectionnez l'une des options répertoriées sous le volet **Gestion** situé à droite.

Effectuer la configuration initiale

Effectuez la configuration initiale du threat defense à l'aide de l'interface de ligne de commande ou du gestionnaire d'appareils.

Effectuer la configuration initiale à l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande du threat defense pour effectuer la configuration initiale. Lorsque vous utilisez l'interface de ligne de commande pour procéder à la configuration initiale, seuls les paramètres de l'interface de gestion ou de l'interface d'accès au gestionnaire sont conservés. Lorsque vous procédez à la configuration initiale à l'aide du gestionnaire d'appareils, *toutes* les configurations d'interface effectuées dans le gestionnaire d'appareils sont conservées lorsque vous passez au CDO pour la gestion, en plus des paramètres d'interface de gestion et d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès, ne sont pas conservés.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du threat defense sur le port de console.

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

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

Lors de la première connexion à FXOS, vous êtes invité à modifier le mot de passe par défaut. Ce mot de passe est également utilisé pour la connexion au threat defense pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez reconfigurer l'appareil pour réinitialiser le mot de passe par défaut. Consultez le Guide de dépannage de la console FXOS pour connaître la procédure de réinstallation.

Exemple :

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

[...]

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

[...]

firepower#
```

Étape 3 Connectez-vous à l'interface de ligne de commande du threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 4 La première fois que vous vous connectez au threat defense, vous êtes invité à accepter le contrat de licence utilisateur final (CLUF). Vous accédez ensuite au script de configuration de l'interface de ligne de commande pour les paramètres de l'interface de gestion.

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

Remarque Vous ne pouvez pas répéter l'assistant de configuration de la CLI à moins d'avoir effacé la configuration, par exemple, via une réinitialisation. Vous pouvez cependant modifier tous les paramètres ultérieurement dans l'interface de ligne de commande à l'aide des commandes **configure network**. Reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

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

Reportez-vous aux instructions suivantes :

- **Configurer IPv4 via DHCP ou manuellement ?**—Sélectionnez **manuel**. Même si vous n'avez pas l'intention d'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 route par défaut, qui doit être **data-interfaces** (reportez-vous au point suivant), peut être remplacée par une autre envoyée par le serveur DHCP.
- **Saisissez la passerelle IPv4 par défaut pour l'interface de gestion** : définissez la passerelle sur **data-interfaces**. Ce paramètre transfère le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé via l'interface de données d'accès au gestionnaire.
- **Gérer l'appareil localement ?** : saisissez **non** pour utiliser le CDO. Si vous saisissez **oui**, vous utilisez le gestionnaire d'appareils.

- **Configurer le mode pare-feu ?** : saisissez **routé**. L'accès au gestionnaire externe est uniquement pris en charge en mode pare-feu routé.

Exemple :

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

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

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

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

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

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

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

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

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

Étape 5 Configurez l'interface externe pour l'accès au gestionnaire.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base de l'interface externe. Consultez les informations suivantes 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 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**, cette commande la définit maintenant.
- Lorsque vous ajoutez le threat defense au CDO, celui-ci détecte et conserve la configuration de l'interface, notamment les paramètres suivants : nom et adresse IP de l'interface, route statique vers la passerelle, serveurs DNS et serveur DDNS. Pour en savoir plus sur la configuration du serveur DNS, reportez-vous à la rubrique ci-dessous. Dans le CDO, vous pouvez modifier ultérieurement la configuration de l'interface d'accès FMC, mais assurez-vous de ne pas apporter de modifications susceptibles d'empêcher le threat defense ou le CDO de rétablir la connexion de gestion. Si la connexion de gestion est interrompue, le threat defense inclut la commande **configure policy rollback** permettant de restaurer le déploiement précédent.
- Si vous configurez une URL de mise à jour du serveur DDNS, le threat defense ajoute automatiquement des certificats pour toutes les autorités de certification principales du bundle Autorités de certification racines approuvées par Cisco afin que le threat defense puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le threat defense FTD prend en charge tout serveur DDNS qui utilise la spécification de l'API distante DynDNS (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 avez défini avec le script de configuration (ou à l'aide de la commande **configure network dns servers**) est utilisé pour le trafic de gestion. Le serveur DNS de données est utilisé pour le DDNS (s'il est configuré) ou pour les politiques de sécurité appliquées à cette interface.

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

  En outre, les serveurs DNS locaux ne sont conservés par le CDO que si les serveurs DNS ont été détectés lors de l'enregistrement initial. Par exemple, si vous avez enregistré l'appareil à l'aide de l'interface de gestion, mais que vous avez ensuite configuré une interface de données à l'aide de la commande **configure network management-data-interface**, vous devez configurer manuellement tous ces paramètres dans le CDO, y compris les serveurs DNS, pour qu'ils correspondent à la configuration du threat defense.
- Vous pouvez modifier l'interface de gestion après avoir enregistré le threat defense auprès du CDO, soit en tant qu'interface de gestion, soit en tant qu'interface de données.
- Le nom de domaine complet que vous avez défini dans l'assistant de configuration est utilisé pour cette interface.
- Vous pouvez effacer la totalité de la configuration de l'appareil via cette commande ; vous pouvez utiliser cette option dans un scénario de récupération, mais nous vous déconseillons de l'utiliser pour la configuration initiale ou le fonctionnement normal.
- Pour désactiver la gestion des données, saisissez la commande **configure network management-data-interface disable**.

Exemple :

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

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

Setting IPv4 network configuration.
Network settings changed.

>
```

Exemple :

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

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

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 6 Identifiez le CDO qui va gérer ce threat defense à l'aide de la commande **configure manager add** que le CDO a générée. Reportez-vous à la section Intégrer un appareil avec l'assistant d'intégration, à la page 140 pour générer la commande.

Exemple :

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

Effectuer la configuration initiale à l'aide du Gestionnaire d'appareils

Connectez-vous au gestionnaire d'appareils pour effectuer la configuration initiale du threat defense. Lorsque vous effectuez la configuration initiale à l'aide du gestionnaire d'appareils, *toutes* les configurations d'interface effectuées dans le gestionnaire d'appareils sont conservées lorsque vous passez au CDO pour la gestion, en plus des paramètres d'interface de gestion et 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 de l'interface de gestion et d'accès au gestionnaire sont conservés (par exemple, la configuration par défaut de l'interface interne n'est pas conservée).

Procédure

Étape 1 Connectez votre ordinateur de gestion à l'une des interfaces suivantes : Ethernet1/2 à 1/8.

Étape 2 Connectez-vous au gestionnaire d'appareils.

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 êtes invité à lire et à accepter le contrat de licence de l'utilisateur final et à modifier le mot de passe admin.

Étape 3 Utilisez l'assistant de configuration lors de votre première connexion au gestionnaire d'appareils pour terminer la configuration initiale. Vous pouvez éventuellement ignorer l'assistant de configuration en cliquant sur **Ignorer la configuration de l'appareil** au bas de la page.

Une fois l'assistant de configuration terminé, outre la configuration par défaut de l'interface interne (Ethernet 1/2 à 1/8, qui sont des ports de commutateur sur le VLAN1), la configuration d'une interface externe (Ethernet 1/1) sera conservée lorsque vous passerez à la gestion du CDO.

a) Configurez les options suivantes pour les interfaces externes et de gestion, puis cliquez sur **Suivant**.

1. **Adresse de l'interface externe** : 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 de l'appareil. La première interface de données est l'interface externe par défaut.

   Si vous souhaitez utiliser une interface différente depuis l'interface externe (ou interne) pour l'accès au gestionnaire, vous devez la configurer manuellement après avoir terminé l'assistant de configuration.

   Configurer IPv4 : adresse IPv4 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. Le protocole PPPoE peut être nécessaire si l'interface est connectée à un modem ADSL, un modem câble ou une autre connexion à votre FAI et que votre FAI utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE après avoir terminé l'assistant.

   Configurer IPv6 : adresse IPv6 de l'interface externe. Vous pouvez utiliser DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Désactivé** pour ne pas configurer d'adresse IPv6.

2. **Interface de gestion**

   Les paramètres de l'interface de gestion ne sont pas visibles si vous avez effectué la configuration initiale dans l'interface de ligne de commande.

   Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès au gestionnaire sur une interface de données. Par exemple, le trafic de gestion acheminé vers le fond de panier via l'interface de données résout les noms de domaine complets à l'aide des serveurs DNS de l'interface de gestion, et non des serveurs DNS de l'interface de données.

Serveurs DNS : serveur DNS pour l'adresse de gestion du système. Saisissez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. La valeur par défaut est Serveurs DNS publics OpenDNS. Si vous modifiez les champs et souhaitez rétablir les paramètres par défaut, cliquez sur **Utiliser OpenDNS** pour recharger les adresses IP appropriées dans les champs.

Nom d'hôte du pare-feu : nom d'hôte de l'adresse de gestion du système.

b) Configurez les **Paramètres relatifs au temps (NTP)** et cliquez sur **Suivant**.

1. **Fuseau horaire** : sélectionnez le fuseau horaire du système.
2. **Serveur de temps NTP** : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

c) Sélectionnez **Démarrer la période d'évaluation de 90 jours sans enregistrement**.

N'enregistrez pas le threat defense auprès de Smart Software Manager ; toutes les licences sont octroyées sur le CDO.

d) Cliquez sur **Terminer**.

e) Vous êtes invité à sélectionner **Gestion du cloud** ou **Autonome**. Pour le CDO fourni dans le cloud centre de gestion, sélectionnez **Autonome**, puis **J'ai compris**.

L'option **Gestion du cloud** concerne les fonctionnalités CDO/FDM existantes.

Étape 4 (Peut être obligatoire) Configurez l'interface de gestion. Reportez-vous à l'interface de gestion sur **Appareil** > **Interfaces**.

La passerelle doit être définie sur les interfaces de données de l'interface de gestion. 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 utilise par défaut les interfaces de données et vous n'avez rien à configurer. Si vous avez reçu une passerelle de DHCP, vous devez configurer cette interface avec une adresse IP statique et définir la passerelle sur les interfaces de données.

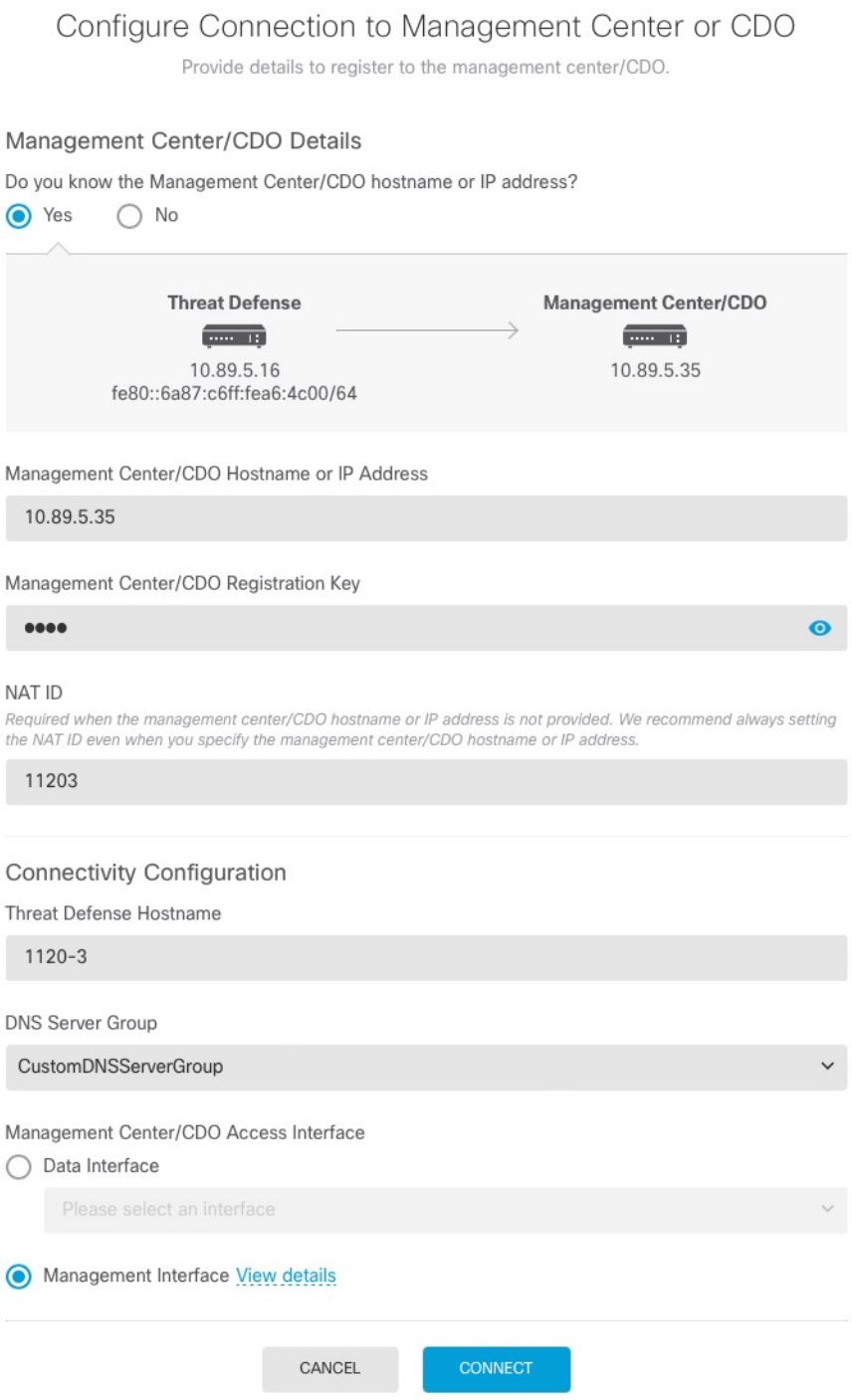
Étape 5 Si vous souhaitez configurer des interfaces supplémentaires, notamment une interface autre que l'interface externe ou interne que vous souhaitez utiliser pour l'accès au gestionnaire sélectionnez **Appareil**, puis cliquez sur le lien dans le récapitulatif **Interfaces**.

Reportez-vous à la rubrique Configurer le pare-feu dans le Gestionnaire d'appareils, à la page 113 pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareils. Les autres configurations du gestionnaire d'appareils ne sont pas conservées lorsque vous enregistrez l'appareil auprès du CDO.

Étape 6 Sélectionnez **Appareil** > **Paramètres système** > **Centre de gestion**, et cliquez sur **Continuer** pour configurer la gestion du centre de gestion.

Étape 7 Configurez les **détails du centre de gestion/CDO**.

Illustration 47 : Détails du centre de gestion/CDO



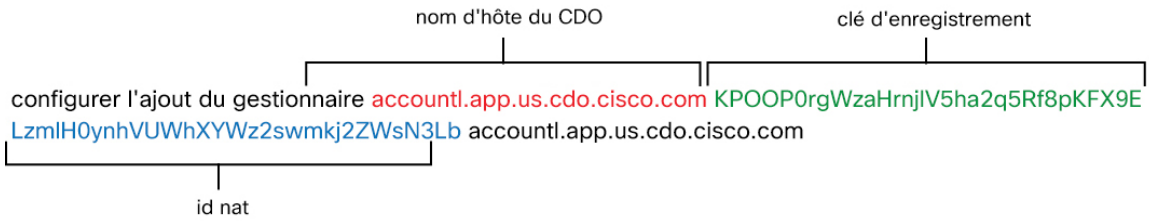
a) Pour **Connaissez-vous le nom d'hôte ou l'adresse IP du centre de gestion/CDO**, cliquez sur **Oui**.

CDO génère la commande **configure manager add**. Reportez-vous à la section Intégrer un appareil avec l'assistant d'intégration, à la page 140 pour générer la commande.

configure manager add *cdo_hostname registration_key nat_id display_name*

Exemple :

Illustration 48 : configurer l'ajout de composants de commande du gestionnaire



b) Copiez les parties *cdo_hostname*, *registration_key* et *nat_id* de la commande dans les champs **Nom d'hôte/adresse IP du Centre de gestion/CDO**, **Clé d'enregistrement du Centre de gestion/CDO** et **ID NAT**.

Étape 8 Configurez la **configuration de connectivité**.

a) Spécifiez le **nom d'hôte du FTD**.

Ce nom de domaine complet sera utilisé pour l'interface externe ou l'interface choisie pour l'**interface d'accès au centre de gestion/CDO**.

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

Sélectionnez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNSServerGroup** et inclut 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 DNS de données est utilisé pour le DDNS (s'il est configuré) ou pour les politiques de sécurité appliquées à cette interface. Vous devrez probablement 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 via l'interface externe.

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

En outre, les serveurs DNS locaux ne sont conservés par le CDO que si les serveurs DNS ont été détectés lors de l'enregistrement initial.

c) Pour **Interface d'accès au Centre de gestion/CDO**, sélectionnez **externe**.

Bien que vous puissiez choisir n'importe quelle interface configurée, dans ce guide nous supposons que vous utilisez une interface externe.

Étape 9 Si vous avez choisi une interface de données externe différente, ajoutez une route par défaut.

Un message s'affiche vous demandant de vérifier que vous disposez d'une route par défaut via l'interface. Si vous avez choisi une interface extérieure, 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 CDO. Reportez-vous à la rubrique Configurer le pare-feu dans le Gestionnaire

d'appareils, à la page 113 pour plus d'informations sur la configuration des routes statiques dans le gestionnaire d'appareils.

Étape 10 Cliquez sur **Ajouter une méthode DNS dynamique (DDNS)**.

DDNS garantit que le CDO peut atteindre le threat defense à son nom de domaine complet (FQDN) si l'adresse IP du threat defense change. Accédez à **Appareil** > **Paramètres système** > **Service DDNS** pour configurer DDNS.

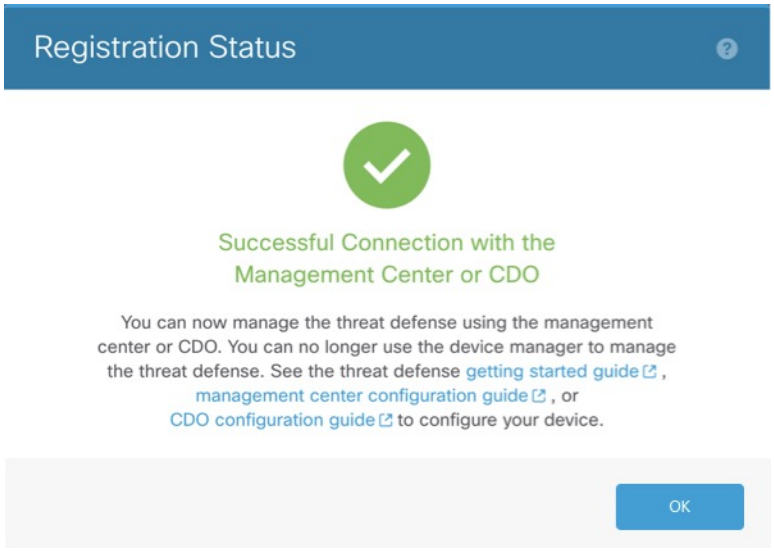
Si vous configurez DDNS avant d'ajouter le threat defense au CDO, le threat defense ajoute automatiquement des certificats pour toutes les autorités de certification principales du bundle Autorités de certification racines approuvées par Cisco afin que le threat defense puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le threat defense FTD prend en charge tout serveur DDNS qui utilise la spécification de l'API distante DynDNS (https://help.dyn.com/remote-access-api/).

Étape 11 Cliquez sur **Connecter**. La boîte de dialogue **État de l'enregistrement** affiche l'état actuel du commutateur vers le CDO. Après l'étape **Sauvegarde des paramètres d'enregistrement du centre de gestion/CDO**, accédez au CDO et ajoutez le pare-feu.

Si vous souhaitez annuler le basculement vers le CDO, cliquez sur **Annuler l'enregistrement**. Sinon, ne fermez pas la fenêtre du navigateur gestionnaire d'appareils avant d'avoir terminé l'étape de **sauvegarde des paramètres d'enregistrement du centre de gestion/CDO**. Dans le cas contraire, le processus sera interrompu et ne reprendra que lorsque vous vous reconnecterez au gestionnaire d'appareils.

Si vous restez connecté au gestionnaire d'appareils après l'étape de **sauvegarde des paramètres d'enregistrement du centre de gestion/CDO**, la boîte de dialogue **Connexion réussie avec le centre de gestion ou le CDO** s'affiche, après quoi vous êtes déconnecté du gestionnaire d'appareils.

Illustration 49 : Connexion réussie



Configurer une politique de sécurité de base

Dans cette section, nous vous expliquons comment configurer une politique de sécurité de base avec les paramètres suivants :

- Interfaces internes et externes : attribuez une adresse IP statique à l'interface interne. 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.
- Serveur DHCP : utilisez un serveur DHCP sur l'interface interne pour les clients.
- NAT : utilisez l'interface PAT sur l'interface externe.
- Contrôle d'accès : autorisez le trafic de l'interface interne vers l'interface externe.
- SSH : activez SSH sur l'interface d'accès du gestionnaire.

Configurer les interfaces

Ajoutez l'interface VLAN1 pour les ports de commutateur ou convertissez les ports de commutateur 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 qu'un système transmette un trafic significatif. Habituellement, vous disposez d'une interface externe face au routeur en amont ou à Internet, et d'une ou de plusieurs interfaces internes pour les réseaux de votre entreprise. Par défaut, Ethernet1/1 est une interface de pare-feu standard que vous pouvez utiliser à l'extérieur ; les autres interfaces sont des ports de commutateur sur le VLAN 1. Après avoir ajouté l'interface VLAN1, vous pouvez la convertir en interface interne. Vous pouvez également attribuer des ports de commutateur à d'autres VLAN ou convertir des ports de commutateur en interfaces de pare-feu.

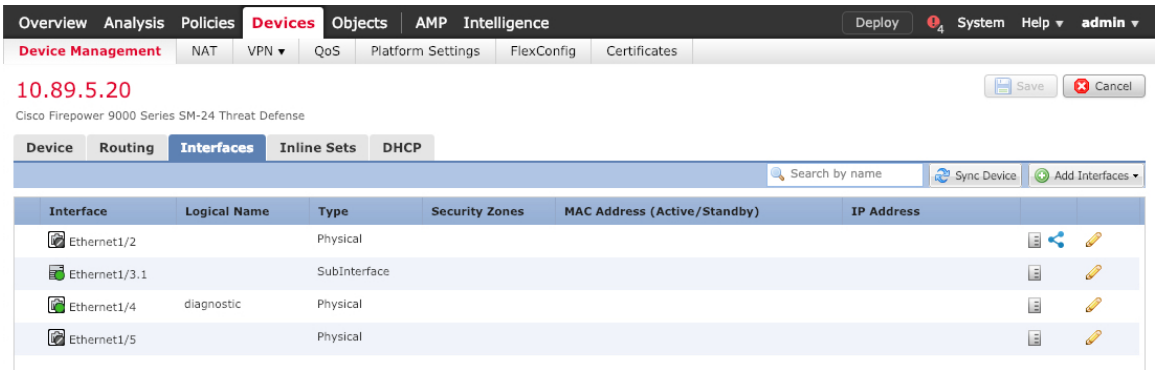
Un routage de périphérie classique consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre FAI, pendant que vous définissez des adresses statiques sur les interfaces internes.

L'exemple suivant configure une interface interne en mode routé (VLAN1) avec une adresse statique et une interface externe en mode routé à l'aide de DHCP (Ethernet1/1).

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** (✎) de l'appareil.

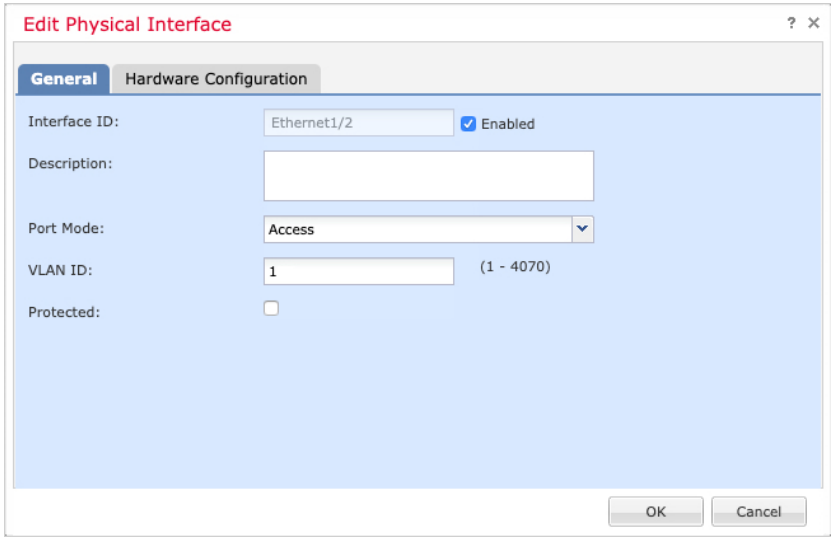
Étape 2 Cliquez sur **Interfaces**.



Étape 3 (facultatif) Désactivez le mode de port de commutateur pour l'un des ports de commutateur (Ethernet 1/2 à 1/8) en cliquant sur le curseur dans la colonne **SwitchPort** pour le désactiver ( ).

Étape 4 Activez les ports de commutateur.

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



b) Activez l'interface en cochant la case **Activé**.

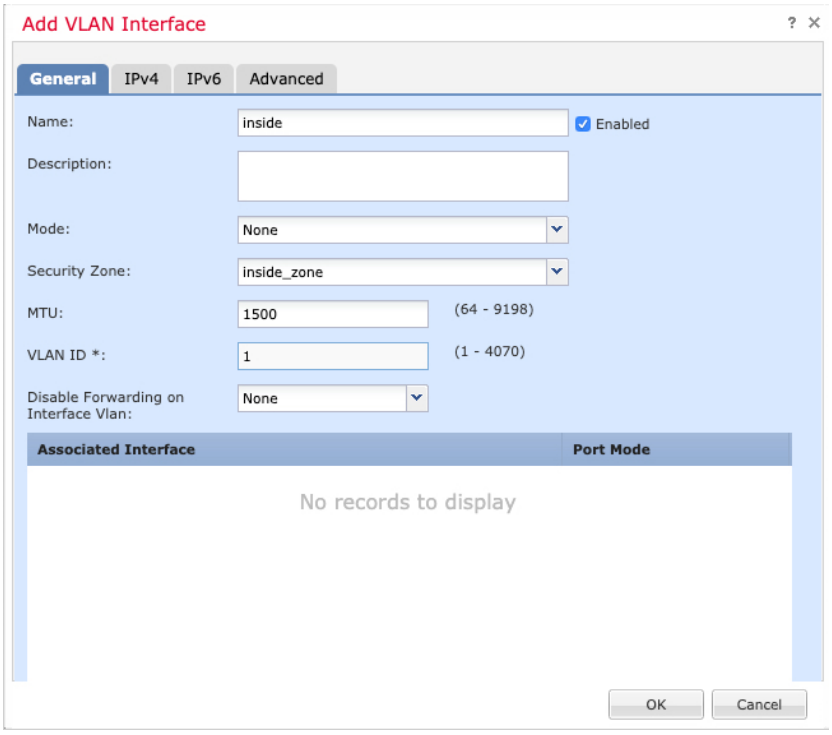
c) (facultatif) Modifiez l'ID de VLAN ; la valeur par défaut est 1. Vous devez ensuite ajouter une interface VLAN correspondant à cet ID.

d) Cliquez sur **OK**.

Étape 5 Ajoutez l'interface VLAN *interne*.

a) Cliquez sur **Ajouter des interfaces** > **Interface VLAN**.

L'onglet **Général** s'affiche.



b) Saisissez un **nom** comportant maximum 48 caractères.

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

c) Cochez la case **Activé**.

d) Laissez le champ **Mode** défini sur **Aucun**.

e) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité interne existante ou ajoutez-en une nouvelle en cliquant sur **Créer**.

Par exemple, ajoutez une zone appelée **zone_interne**. Chaque interface doit être affectée à une zone de sécurité et/ou à un groupe d'interfaces. Une interface peut appartenir 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 attribuer l'interface interne à la zone interne, et l'interface externe à la zone externe. Vous pouvez ensuite configurer votre politique de contrôle d'accès pour que le trafic transite de l'interface interne vers l'interface externe, mais pas de l'interface externe vers l'interface interne. La plupart des politiques ne prennent en charge que les zones de sécurité ; vous pouvez utiliser des zones ou des groupes d'interfaces dans les politiques NAT, les politiques de préfiltre et les politiques QoS.

f) Définissez le champ **ID de VLAN** sur **1**.

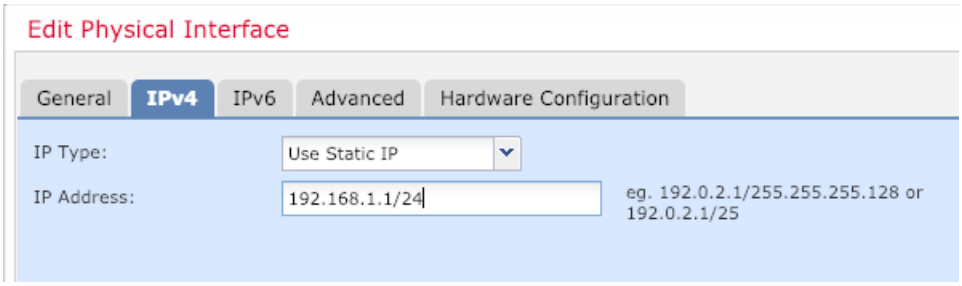
Par défaut, tous les ports de commutateur sont définis sur l'ID de VLAN 1 ; si vous choisissez un autre ID de VLAN, vous devez également modifier chaque port de commutateur pour qu'il corresponde au nouvel ID de VLAN.

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

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

- **IPv4** : sélectionnez **Utiliser l'adresse IP statique** dans la liste déroulante, et saisissez une adresse IP et un masque de sous-réseau en notation de barre oblique.

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

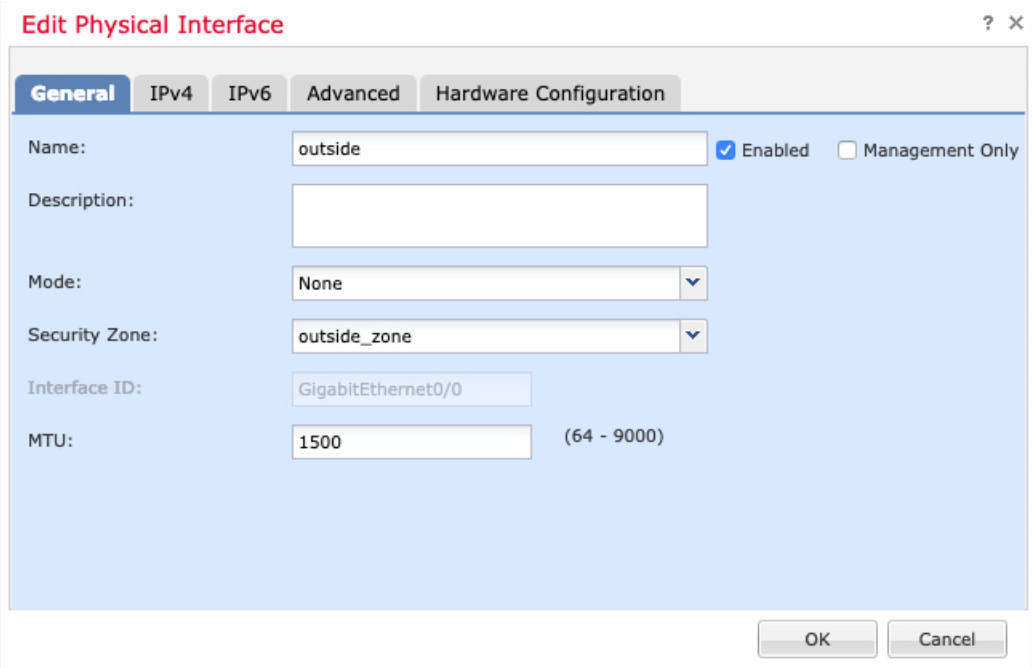


- **IPv6** : cochez la case **Configuration automatique** pour la configuration automatique sans état.

h) Cliquez sur **OK**.

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

L'onglet **Général** s'affiche.



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

a) Dans la liste déroulante **Zone de sécurité**, sélectionnez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **Créer**.

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

b) Cliquez sur **OK**.

Étape 7 Cliquez sur **Enregistrer**.

Configurer le serveur DHCP

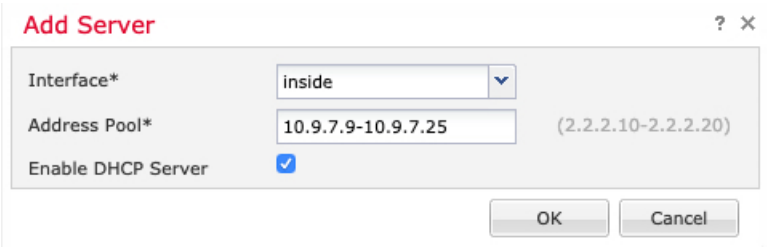
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir du threat defense.

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**, puis cliquez sur l'icône **Modifier** (✎) de l'appareil.

Étape 2 Sélectionnez **DHCP** > **Serveur DHCP**.

Étape 3 Sur la page **Serveur**, cliquez sur **Ajouter** et configurez les options suivantes :



- **Interface** : sélectionnez l'interface dans la liste déroulante.
- **Pool d'adresses** : définissez la plage d'adresses IP (de la plus faible à la plus élevée) utilisée par le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et ne peut pas inclure l'adresse IP de l'interface proprement dite.
- **Activer le serveur DHCP** : activez le serveur DHCP sur l'interface sélectionnée.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Enregistrer**.

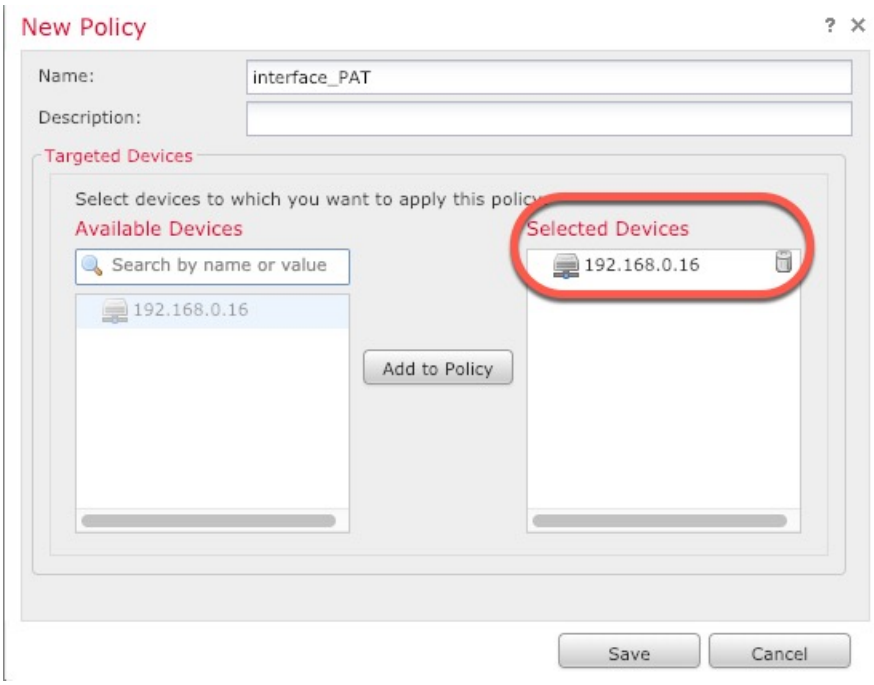
Configuration du routage NAT

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

Procédure

Étape 1 Sélectionnez **Appareils** > **NAT**, puis cliquez sur **Nouvelle politique** > **NAT de protection contre les menaces**.

Étape 2 Donnez un nom à la politique, sélectionnez le ou les appareils que vous souhaitez utiliser, puis cliquez sur **Enregistrer**.



La politique est ajoutée au centre de gestion. Vous devez quand même ajouter des règles à la politique.

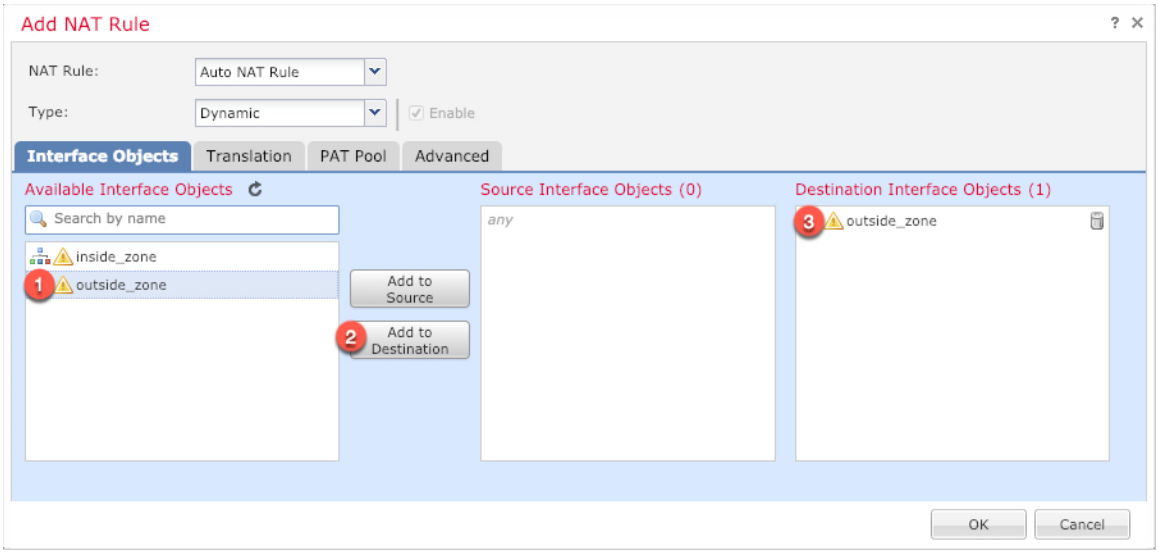
Étape 3 Cliquez sur **Ajouter une règle**.

La boîte de dialogue **Ajouter une règle NAT** apparaît.

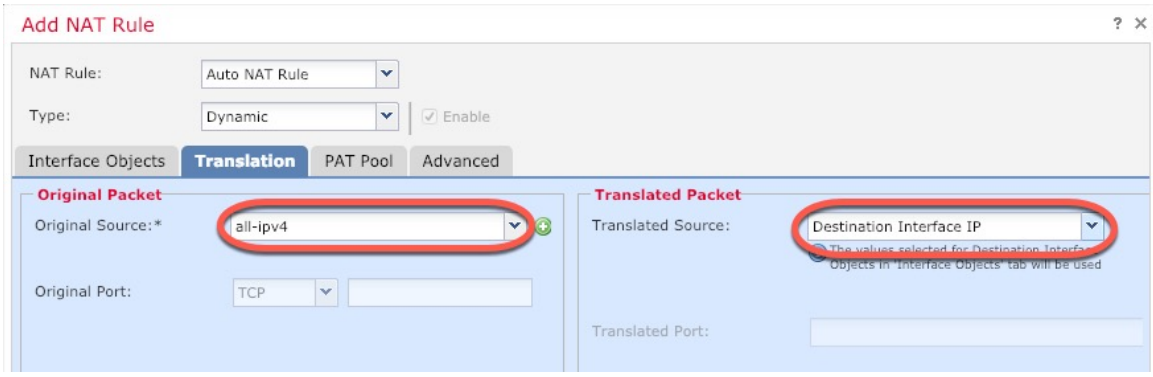
Étape 4 Configurez les options de règle de base :

- **Règle NAT** : sélectionnez **Règle NAT automatique**.
- **Type** : choisissez **Dynamique**.

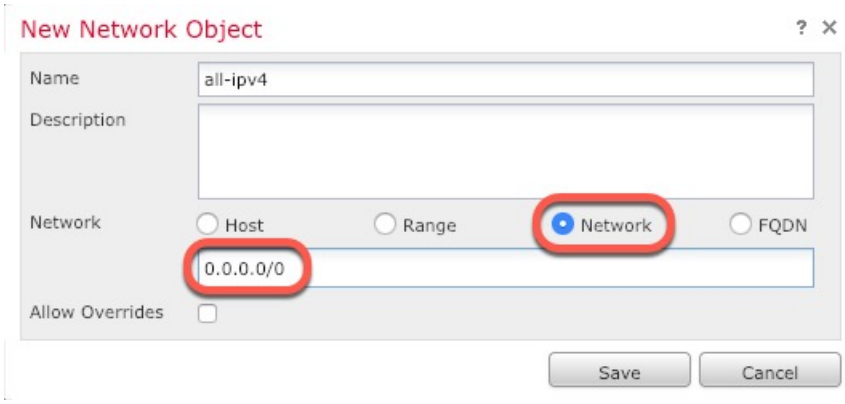
Étape 5 Sur la page **Objets d'interface**, ajoutez la zone externe de la section **Objets d'interface disponibles** à la section **Objets d'interface de destination**.



Étape 6 Sur la page **Traduction**, configurez les options suivantes :



- **Source d'origine** : cliquez sur **Ajouter** (+) pour ajouter un objet réseau pour tout le trafic IPv4 (0.0.0.0/0).

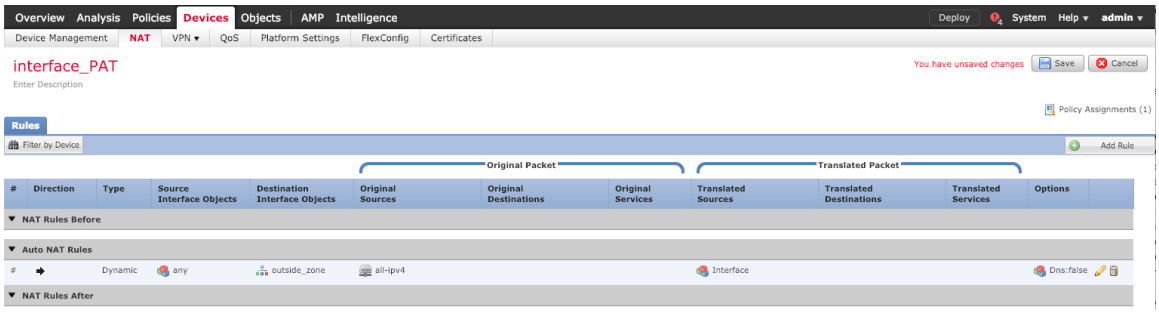


Remarque Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles NAT automatiques ajoutent la fonction NAT à la définition d'objet et vous ne pouvez pas modifier les objets définis par le système.

- **Source traduite** : sélectionnez **Adresse IP de l'interface de destination**.

Étape 7 Cliquez sur **Enregistrer** pour ajouter la règle.

La règle est enregistrée dans la table **Règles**.



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

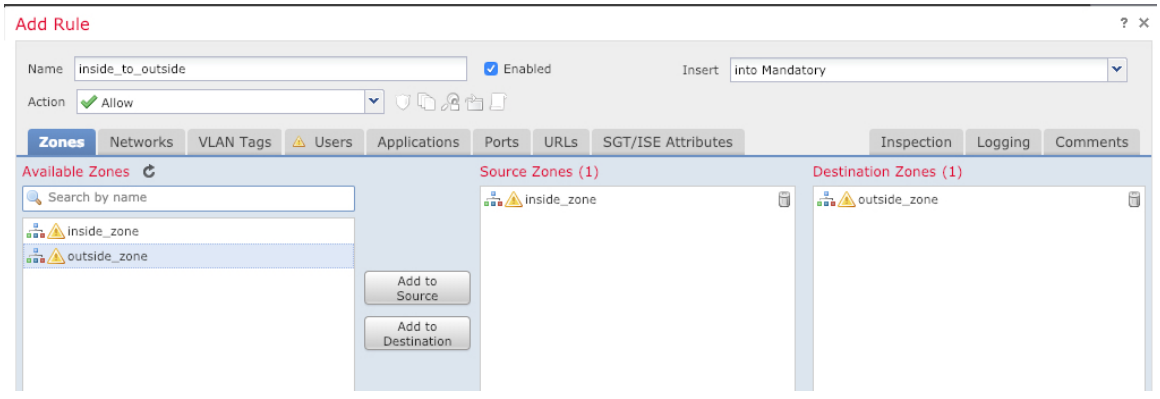
Autoriser le trafic de l'interface interne vers l'interface externe

Si vous avez créé une politique de contrôle d'accès de base **Bloquer tout le trafic** lorsque vous avez enregistré le threat defense, vous devez ajouter des règles à la politique pour autoriser le trafic via l'appareil. La procédure suivante ajoute une règle pour autoriser le trafic de la zone interne vers la zone externe. Si vous disposez d'autres zones, veillez à ajouter des règles autorisant le trafic vers les réseaux appropriés.

Procédure

Étape 1 Sélectionnez **Politique** > **Politique d'accès** > **Politique d'accès**, puis cliquez sur **Modifier** (✎) pour la politique de contrôle d'accès attribuée à threat defense.

Étape 2 Cliquez sur **Ajouter une règle**, puis définissez les paramètres suivants :



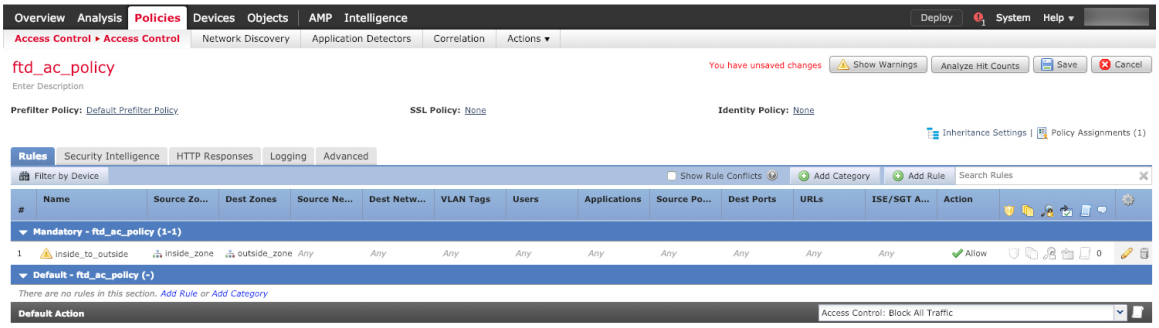
- **Nom** : donnez un nom à cette règle, par exemple **interne_vers_externe**.
- **Zones source** : sélectionnez la zone interne dans **Zones disponibles**, puis cliquez sur **Ajouter à la source**.

- **Zones de destination** : sélectionnez la zone externe dans **Zones disponibles**, puis cliquez sur **Ajouter à la destination**.

Laissez les autres paramètres tels quels.

Étape 3 Cliquez sur **Ajouter**.

La règle est ajoutée au tableau **Règles**.



Étape 4 Cliquez sur **Enregistrer**.

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

Si vous avez activé l'accès au centre de gestion sur une interface de données, par exemple externe, vous devez activer SSH sur cette interface en suivant cette procédure. Dans cette section, nous vous expliquons comment activer les connexions SSH sur une ou plusieurs interfaces de *données* sur le threat defense. SSH n'est pas pris en charge par l'interface logique de diagnostic.

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

L'interface de gestion est distincte des autres interfaces sur l'appareil. Elle permet de configurer et d'enregistrer l'appareil sur le gestionnaire du centre de gestion. SSH pour les interfaces de données partage la liste des utilisateurs internes et externes avec SSH pour l'interface de gestion. D'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 standard, et non les routes statiques définies lors de la configuration ou sur l'interface de ligne de commande.

Sur l'interface de gestion, pour configurer une liste d'accès SSH, reportez-vous à la commande **configure ssh-access-list** de la rubrique Référence des commandes pour Secure Firewall Threat Defense. Pour configurer une route statique, consultez la commande **configure network static-routes**. Par défaut, vous configurez la route par défaut via l'interface de gestion lors de la configuration initiale.

Pour utiliser SSH, il n'est pas nécessaire de disposer d'une règle d'accès autorisant l'adresse IP de l'hôte. Vous devez uniquement configurer l'accès SSH conformément à cette section.

Vous pouvez uniquement utiliser le protocole SSH pour accéder à une interface accessible ; si votre hôte SSH se trouve sur l'interface externe, vous pouvez uniquement établir une connexion de gestion directement vers l'interface externe.

L'appareil autorise un maximum de 5 connexions SSH simultanées.

Remarque Après trois tentatives infructueuses de connexion à l'interface de ligne de commande via SSH, l'appareil interrompt la connexion SSH.

Avant de commencer

- Vous pouvez configurer les utilisateurs internes SSH dans l'interface de ligne de commande à l'aide de la commande **configure user add**. Par défaut, il existe un utilisateur **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** dans les paramètres de la plateforme.
- Vous devez disposer d'objets réseau qui définissent les hôtes ou les réseaux autorisés à établir des connexions SSH à l'appareil. Vous pouvez ajouter des objets dans le cadre de cette 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 **Objets** > **Gestion des objets** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser l'objet réseau **any** fourni par le système. Utilisez plutôt **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Appareils** > **Paramètres de la plateforme** et créez ou modifiez la politique threat defense.

Étape 2 Sélectionnez **Secure Shell**.

Étape 3 Identifiez les interfaces et les adresses IP qui autorisent les connexions SSH.

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

a) Cliquez sur **Ajouter** pour ajouter une nouvelle règle ou sur **Modifier** pour modifier une règle.

b) Configurez les propriétés de la règle :

- **Adresse IP** : objet ou groupe réseau qui identifie les hôtes ou les réseaux autorisés à établir des connexions SSH. Sélectionnez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur +.
- **Zones de sécurité** : ajoutez les zones contenant les interfaces sur lesquelles vous autorisez les connexions SSH. Pour les interfaces ne faisant pas partie d'une zone, vous pouvez saisir le nom de l'interface dans le champ situé sous la liste Zone de sécurité sélectionnée, puis cliquer sur **Ajouter**. Ces règles seront appliquées à un appareil uniquement si celui-ci inclut les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 Cliquez sur **Enregistrer**.

Vous pouvez maintenant accéder à la page **Déployer** > **Déploiement** et déployer la politique sur les appareils affectés. Les modifications ne sont pas actives tant que vous ne les avez pas déployées.

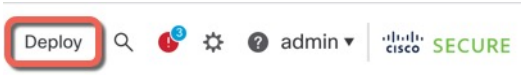
Déployer la configuration

Déployez les modifications de configuration sur le threat defense ; aucune modification n'est active sur l'appareil tant que vous ne l'avez pas déployée.

Procédure

Étape 1 Cliquez sur **Déployer** en haut à droite.

Illustration 50 : Déployer



Étape 2 Cliquez sur **Tout déployer** pour déployer sur tous les périphériques ou cliquez sur **Déploiement avancé** pour déployer sur les périphériques sélectionnés.

Illustration 51 : Tout déployer

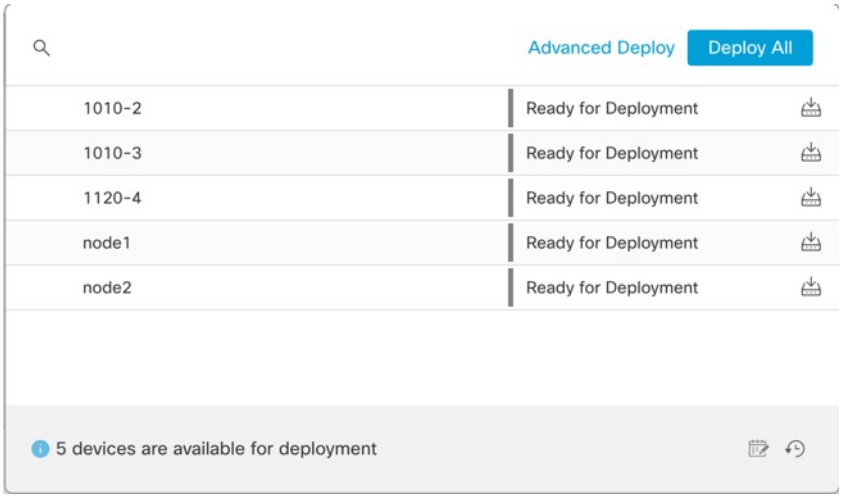
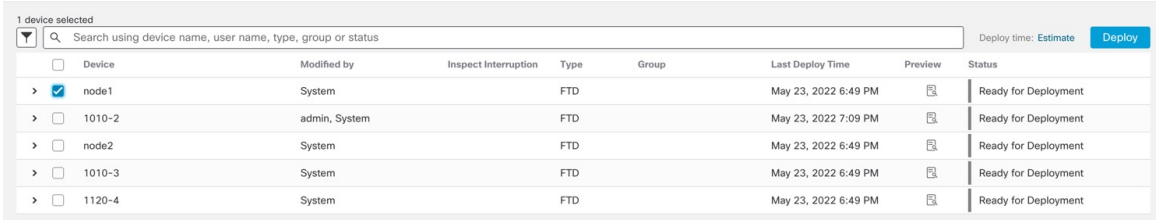
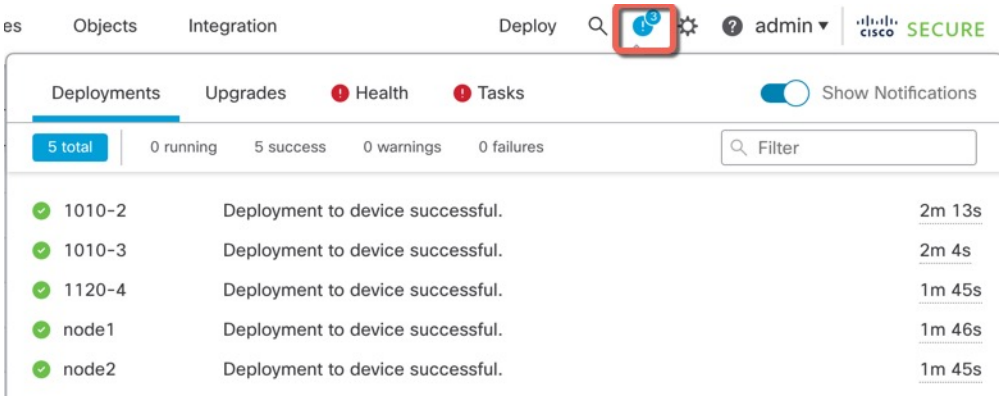


Illustration 52 : Déploiement avancé



Étape 3 Assurez-vous que le déploiement aboutit. Cliquez sur l'icône en regard du bouton **Déployer** dans la barre de menus pour afficher l'état des déploiements.

Illustration 53 : État du déploiement



Dépannage et maintenance

Accéder à l'interface de ligne de commande du Threat Defense et de la console FXOS

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

Vous pouvez également accéder à la CLI FXOS à des fins de dépannage.

Remarque Vous pouvez également vous connecter à l'interface de gestion de l'appareil threat defense. Contrairement à une session de console, la session SSH utilise par défaut l'interface de ligne de commande du threat defense, à partir de laquelle vous pouvez vous connecter à la CLI FXOS à l'aide de la commande **connect fxos**. Vous pourrez 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 console, qui est défini par défaut sur la CLI FXOS.

Procédure

Étape 1 Pour vous connecter à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. L'appareil Firepower 1000 est livré avec un câble série USB A vers B. Veillez à installer les pilotes série USB nécessaires à votre système d'exploitation (consultez le guide matériel de l'appareil Firepower 1010). Le port de console est défini par défaut sur la CLI FXOS. Utilisez les paramètres série suivants :

- 9 600 bauds

- 8 bits de données
- Aucune parité
- 1 bit d'arrêt

Vous vous connectez à la CLI FXOS. Connectez-vous à l'interface de ligne de commande à l'aide du nom d'utilisateur **admin** et du 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 du threat defense.

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après vous être connecté, pour obtenir des informations sur les commandes disponibles dans l'interface de ligne de commande, saisissez **help** ou **?**. Pour plus d'informations sur l'utilisation, reportez-vous à la rubrique Référence des commandes pour Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande threat defense, saisissez la commande du **exit** ou **logout**.

Cette commande vous renvoie à l'invite de la CLI FXOS. Pour plus d'informations sur les commandes disponibles dans la CLI FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Résoudre les problèmes de connectivité de gestion sur une interface de données

Lorsque vous utilisez une interface de données pour l'accès au gestionnaire au lieu d'utiliser l'interface de gestion dédiée, veillez à modifier les paramètres d'interface et de réseau du threat defense dans le CDO afin de ne pas interrompre la connexion. Si vous modifiez le type d'interface de gestion après avoir ajouté le threat defense au CDO (c'est-à-dire, remplacez l'interface de données par l'interface de gestion, ou vice versa), si les interfaces et les paramètres réseau ne sont pas configurés correctement, vous risquez de perdre la connectivité à l'interface de gestion.

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

Afficher l'état de connexion de l'interface de gestion

Dans le CDO, vérifiez l'état de la connexion de gestion sur la page **Appareils** > **Gestion des appareils** > **Appareil** > **Gestion** > **Détails de l'accès - Détails de configuration** > **État de connexion**.

Dans l'interface de ligne de commande du threat defense, saisissez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion. Vous pouvez également utiliser **sftunnel-status** pour afficher des informations plus complètes.

Reportez-vous à l'exemple de résultat suivant pour une connexion interrompue ; aucune information de connexion de canal homologue et aucune information de pulsation n'est disponible :

```
> 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
```

Reportez-vous à l'exemple de résultat suivant pour une connexion active comprenant des informations de canal homologue et de 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
```

Afficher les informations relatives au réseau du threat defense

Dans l'interface de ligne de commande du threat defense, affichez les paramètres réseau de l'interface de gestion et d'accès aux données du gestionnaire :

show network

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

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

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

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

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

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

Vérifier que le threat defense est enregistré auprès du CDO

Dans l'interface de ligne de commande du threat defense, vérifiez que le CDO a bien été enregistré. Notez que cette commande n'affiche pas l'état *actuel* de la connexion de gestion.

show managers

```
> show managers
Type                      : Manager
Host                      : account1.app.us.cdo.cisco.com
Display name              : account1.app.us.cdo.cisco.com
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

Envoyer une requête ping au CDO

Dans l'interface de ligne de commande du threat defense, utilisez la commande suivante pour envoyer une requête ping au CDO à partir des interfaces de données :

ping *cdo_hostname*

Dans l'interface de ligne de commande du threat defense, utilisez la commande suivante pour envoyer une requête ping au CDO à partir de l'interface de gestion, afin de l'acheminer via le fond de panier aux interfaces de données :

ping system *cdo_hostname*

Capturer les paquets sur l'interface interne du threat defense

Dans l'interface de ligne de commande du threat defense, capturez les paquets sur l'interface de fond de panier interne (nlp_int_tap) pour déterminer 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 du threat defense, consultez les informations relatives à l'interface de fond de panier interne, 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
```

Vérifier le routage et la NAT

Dans l'interface de ligne de commande du threat defense, vérifiez que la route par défaut (S*) a bien été ajoutée et qu'il existe des règles NAT internes 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

Reportez-vous aux commandes suivantes pour vérifier que tous les autres paramètres sont présents. Vous pouvez également consulter la plupart de ces commandes sur la page **Appareils** > **Gestion des appareils** > **Appareil** > **Gestion** > **Accès au gestionnaire - Détails de configuration** > **Résultat de la CLI** du CDO.

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
>
```

Rechercher une mise à jour DDNS réussie

Dans l'interface de ligne de commande du threat defense, vérifiez que la mise à jour DDNS a réussi :

debug ddns

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

Si la mise à jour échoue, utilisez les commandes **debug http** et **debug ssl**. Pour les échecs de validation du certificat, vérifiez que les certificats racines sont installés sur l'appareil :

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
```

Consulter les fichiers journaux du CDO

Consultez la page https://cisco.com/go/fmc-reg-error.

Rétablir la configuration en cas de déconnexion du CDO

Si vous utilisez une interface de données sur le threat defense pour l'accès au gestionnaire, et que vous déployez une modification de configuration depuis le CDO ayant une incidence sur la connectivité réseau, vous pouvez rétablir la dernière configuration déployée sur le threat defense afin de restaurer la connectivité de gestion. Vous pouvez ensuite ajuster les paramètres de configuration dans le CDO afin de maintenir et de redéployer la connectivité réseau. Vous pouvez utiliser la fonction de restauration même si aucune perte de connectivité ne se produit, car elle ne se limite pas à cette situation de dépannage.

Reportez-vous aux instructions suivantes :

- Seul le déploiement précédent est disponible localement sur le threat defense ; vous ne pouvez pas rétablir les déploiements antérieurs.
- La restauration s'applique uniquement aux configurations que vous pouvez définir dans le CDO. Par exemple, la restauration ne s'applique à aucune configuration locale liée à l'interface de gestion dédiée, que vous pouvez configurer uniquement sur l'interface de ligne de commande de threat defense. Notez que si vous avez modifié les paramètres de l'interface de données après le dernier déploiement du CDO

à l'aide de la commande **configure network management-data-interface**, puis que vous utilisez la commande de restauration, ces paramètres ne seront pas conservés ; les derniers paramètres déployés sur le CDO seront rétablis.

- Il est impossible de restaurer les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent.
- Pendant la restauration, les connexions sont interrompues, car la configuration en cours est supprimée.

Procédure

Étape 1 Sur l'interface de ligne de commande de threat defense, restaurez la configuration précédente.

configure policy rollback

Après la restauration, le threat defense informe le CDO que la restauration a réussi. Dans le CDO, l'écran de déploiement affiche une bannière indiquant que la configuration a été restaurée.

Remarque Si la restauration échoue et que l'interface de gestion du CDO est restaurée, reportez-vous à la rubrique https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html pour connaître les problèmes de déploiement courants. Dans certains cas, la restauration peut échouer après le rétablissement de l'accès de gestion du CDO ; dans ce cas, vous pouvez résoudre les problèmes de configuration du CDO et renouveler le déploiement depuis le CDO.

Exemple :

Pour le threat defense qui utilise une interface de données pour l'accès du gestionnaire :

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

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

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

Dans le CDO, vérifiez l'état de la connexion de gestion sur la page **Appareils** > **Gestion des appareils** > **Appareil** > **Gestion** > **Détails de l'accès - Détails de configuration** > **État de connexion**.

Dans l'interface de ligne de commande du threat defense, saisissez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

Si le rétablissement de la connexion prend plus de 10 minutes, vous devez dépanner la connexion. Reportez-vous à la rubrique Résoudre les problèmes de connectivité de gestion sur une interface de données, à la page 164.

Mettre le pare-feu hors tension à l'aide du CDO

Il est important que vous arrêtiez correctement votre système. Il ne suffit pas de débrancher le câble d'alimentation ou d'appuyer sur l'interrupteur d'alimentation, car vous risquez d'endommager gravement le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en arrière-plan en permanence, et que débrancher ou couper l'alimentation ne permet pas un arrêt normal de votre pare-feu.

Vous pouvez arrêter votre système correctement à l'aide du CDO.

Procédure

Étape 1 Sélectionnez **Appareils** > **Gestion des appareils**.

Étape 2 Cliquez sur l'icône Modifier () en regard de l'appareil que vous souhaitez redémarrer.

Étape 3 Cliquez sur l'onglet **Appareils**.

Étape 4 Cliquez sur l'icône d'arrêt de l'appareil () dans la section **Système**.

Étape 5 Lorsque vous y êtes invité, confirmez que vous souhaitez arrêter l'appareil.

Étape 6 Si vous disposez d'une connexion de console au pare-feu, observez les invites système lorsque le pare-feu s'arrête. L'invite suivante s'affiche :

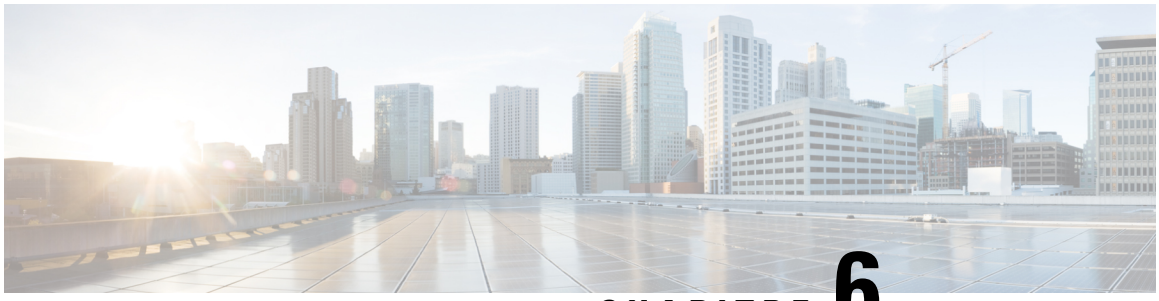
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Si vous ne disposez pas d'une connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Étape 7 Vous pouvez désormais débrancher ce dernier pour couper l'alimentation du châssis si nécessaire.

Et après ?

Pour poursuivre la configuration de votre threat defense avec CDO, reportez-vous à la page d'accueil Cisco Defense Orchestrator.



CHAPITRE 6

Déployer l'ASA avec le gestionnaire ASDM

Ce chapitre vous concerne-t-il ?

Pour connaître tous les systèmes d'exploitation et gestionnaires disponibles, reportez-vous à la rubrique Quel système d'exploitation et quel gestionnaire vous conviennent le mieux ?, à la page 1. Ce chapitre s'applique à l'ASA utilisant ASDM.

Ce chapitre ne couvre pas les déploiements suivants, pour lesquels vous devez consulter le Guide de configuration de l'ASA :

- Basculement
- Configurer l'interface de ligne de commande

Dans ce chapitre, nous vous expliquons également comment configurer une politique de sécurité de base. Si vous avez des exigences plus avancées, consultez le guide de configuration.

À propos du pare-feu

L'appareil peut exécuter un logiciel threat defense ou un logiciel ASA. Pour basculer entre threat defense et ASA, vous devez reconfigurer l'appareil. Vous devez également recommencer l'installation si vous avez besoin d'une version logicielle différente de celle actuellement installée. Consultez la rubrique Réinstaller Cisco ASA ou Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé Système d'exploitation Secure Firewall eXtensible (FXOS). Le pare-feu ne prend pas en charge le Gestionnaire de châssis Secure Firewall FXOS ; seule une CLI limitée est prise en charge à des fins de dépannage. Pour obtenir plus d'informations, reportez-vous à la section Guide de dépannage Cisco FXOS pour la série Firepower 1000/2100 exécutant Firepower Threat Defense.

Déclaration de confidentialité—Le pare-feu ne requiert ni ne collecte activement aucune information permettant de vous identifier. Vous pouvez néanmoins utiliser des informations d'identification personnelle au cours de la configuration, notamment des noms d'utilisateur. Dans ce cas, un administrateur peut accéder à ces informations lors de l'utilisation de la configuration ou de l'utilisation du protocole SNMP.

À propos de l'ASA

L'ASA fournit des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN au sein d'un seul appareil.

Vous pouvez gérer l'ASA à l'aide de l'un des gestionnaires suivants :

- ASDM (abordé dans ce guide) : un gestionnaire d'appareil unique est inclus sur l'appareil.
- CLI
- CDO est un gestionnaire multi-appareils simplifié basé dans le cloud.
- Cisco Security Manager : gestionnaire multi-appareils sur un serveur distinct.

Vous pouvez également accéder à l'interface de ligne de commande de la console FXOS à des fins de dépannage.

Fonctionnalités non prises en charge

Fonctionnalités ASA générales non prises en charge

Les fonctionnalités ASA suivantes ne sont pas prises en charge sur le pare-feu Firepower 1010 :

- Mode multicontextuel
- Basculement actif/actif
- Interfaces redondantes
- Clustering
- API REST ASA
- Module ASA FirePOWER
- Filtre du trafic de botnets
- Les inspections suivantes :
  - Mappages d'inspection SCTP (l'inspection avec état SCTP à l'aide de listes de contrôle d'accès est prise en charge)
  - de la tête
  - GTP/GPRS

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutateur

Les interfaces VLAN et les ports de commutateur ne prennent pas en charge les fonctionnalités suivantes :

- Routage dynamique
- Routage multidiffusion
- Routage fondé sur les politiques
- Protocole ECMP (Equal-Cost Multi-Path routing)
- Ensembles intégrés ou interfaces passives
- VXLAN
- EtherChannel
- Basculement et liaison d'état
- Zones de trafic
- Balisage du groupe de sécurité (SGT)

Migrer la configuration d'une appliance ASA 5500-X

Vous pouvez copier et coller la configuration d'une console ASA 5500-X dans Firepower 1010. Vous devrez cependant modifier votre configuration. Notez également qu'il existe certaines différences de comportement entre les plateformes.

1. Pour copier la configuration, saisissez la commande **more system:running-config** sur l'ASA 5500-X.
2. Modifiez la configuration si nécessaire (voir ci-dessous).
3. Connectez-vous au port de console de Firepower 1010 et passez en mode de configuration globale :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. Effacez la configuration actuelle à l'aide de la commande **clear configure all**.
5. Collez la configuration modifiée dans l'interface de ligne de commande ASA.

Les procédures de ce guide sont basées sur une configuration par défaut définie en usine. Par conséquent, si vous collez une configuration existante, certaines procédures de ce guide ne s'appliqueront pas à votre console ASA.

Configurer l'appliance ASA 5500-X	Configuration du Firepower 1010

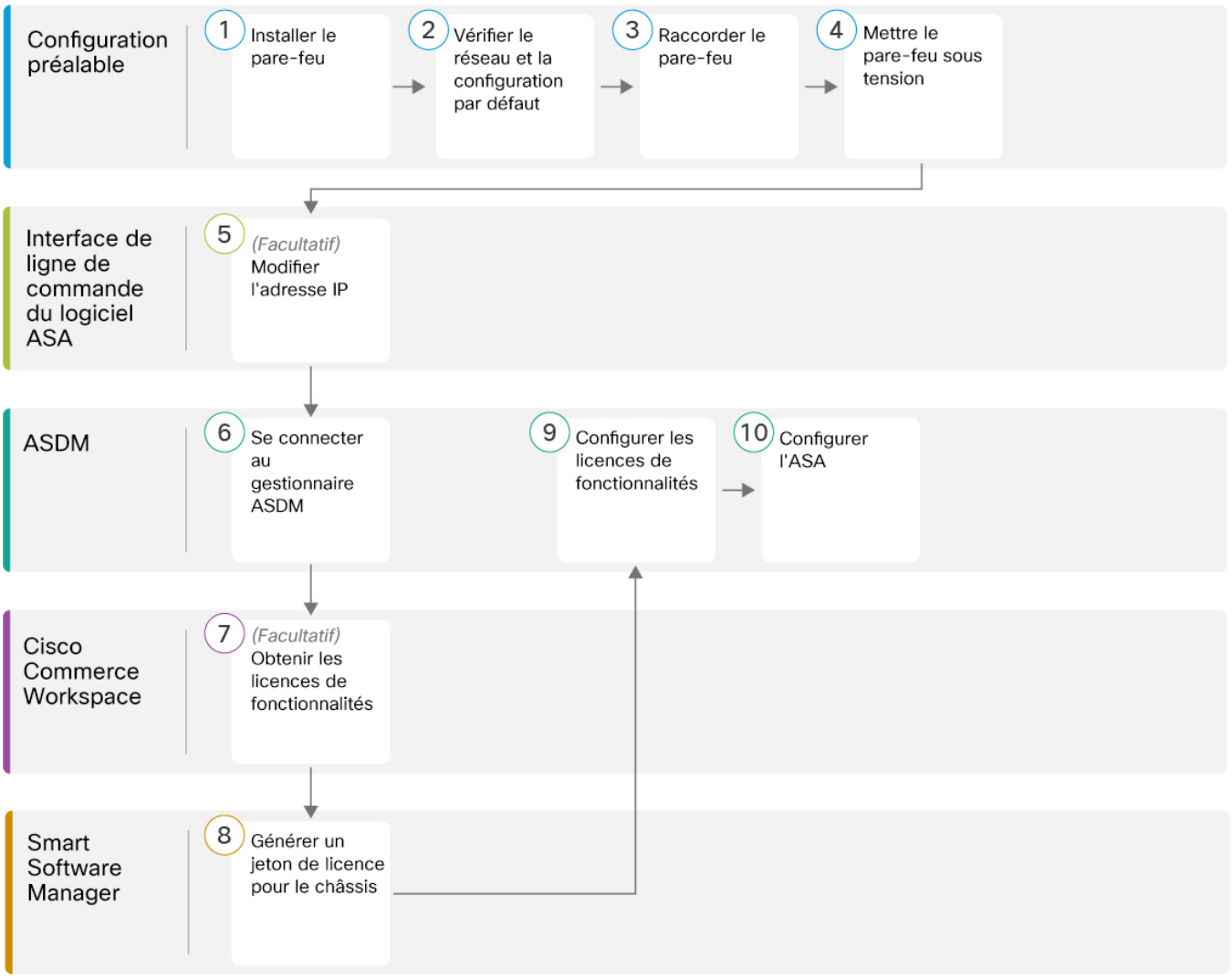
Interfaces de pare-feu Ethernet 1/2 à 1/8	Ports de commutateur Ethernet 1/2 à 1/8
	Ces ports Ethernet sont configurés en tant que ports de commutateur par défaut. Pour chaque interface de votre configuration, ajoutez la commande **no switchport** pour les convertir en interfaces de pare-feu standard. Par exemple :
	`interface ethernet 1/2`
	`  no switchport`
	`  ip address 10.8.7.2 255.255.255.0`
	`  nameif inside`

Licence PAK	Licence Smart Les licences PAK ne sont pas appliquées lorsque vous copiez et collez votre configuration. Aucune licence n'est installée par défaut. L'octroi de licences Smart nécessite que vous vous connectiez au serveur Smart Licensing pour obtenir vos licences. L'octroi de licences Smart a également une incidence sur l'accès ASDM ou SSH (voir ci-dessous).
Accès ASDM initial	Supprimez tout VPN ou toute autre configuration de fonction de chiffrement renforcé (même si vous vous êtes limité à configurer un chiffrement faible) si vous ne pouvez pas vous connecter à ASDM ni vous enregistrer auprès de Smart Licensing Server. Vous pouvez réactiver ces fonctionnalités après avoir obtenu la licence de chiffrement renforcé (3DES). La raison de ce problème est que l'ASA inclut la fonctionnalité 3DES par défaut pour l'accès de gestion uniquement. Si vous activez une fonction de chiffrement renforcé, le trafic ASDM et HTTPS (notamment celui vers et depuis Smart Licensing Server) est bloqué. Il existe toutefois une exception à cette règle : vous êtes connecté à une interface de gestion uniquement, telle que l'interface de gestion 1/1. Cela n'a aucune incidence sur SSH.
ID d'interface	Veillez à modifier les ID d'interface pour qu'ils correspondent aux nouveaux ID de matériel. Par exemple, l'ASA 5525-X inclut l'interface de gestion 0/0, ainsi que GigabitEthernet 0/0 à 0/5. Firepower 1120 intègre les interfaces de gestion 1/1 et Ethernet 1/1 à 1/8.

Configurer l'appliance ASA 5500-X	Configuration du Firepower 1010
boot system commandes L'ASA 5500-X autorise jusqu'à quatre commandes **boot system** pour spécifier l'image de démarrage à utiliser.	L'appareil Firepower 1010 n'autorise qu'une seule commande **boot system**. Vous devez donc supprimer toutes les commandes sauf une. Vous n'avez besoin d'*aucune* commande **boot system** dans votre configuration, car celle-ci n'est pas lue au démarrage pour déterminer l'image de démarrage. C'est l'image de démarrage chargée en dernier qui est toujours exécutée lors du rechargement. La commande **boot system** exécute une action lorsque vous la saisissez : le système valide et décompresse l'image, puis la copie dans l'emplacement de démarrage (un emplacement interne sur disk0 géré par FXOS). La nouvelle image se charge lorsque vous rechargez l'ASA.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer et configurer ASA sur votre châssis.



1	Configuration préalable	Installez le pare-feu. Reportez-vous au guide d'installation matérielle.
2	Configuration préalable	Vérifier le déploiement et la configuration par défaut du réseau, à la page 179.
3	Configuration préalable	Raccorder l'appareil, à la page 182.
4	Configuration préalable	Mettre le pare-feu sous tension, à la page 13
5	Interface de ligne de commande du logiciel ASA	(Facultatif) Modifier l'adresse IP, à la page 184.
6	ASDM	Se connecter au gestionnaire ASDM, à la page 185.

7	Cisco Commerce Workspace	Configurer l'octroi de licences, à la page 186 : Obtenir les licences de fonctionnalité.
8	Smart Software Manager	Configurer l'octroi de licences, à la page 186 : Générer un jeton de licence pour le châssis.
9	ASDM	Configurer l'octroi de licences, à la page 186 : Configurer les licences de fonction.
10	ASDM	Configurer l'ASA, à la page 190.

Vérifier le déploiement et la configuration par défaut du réseau

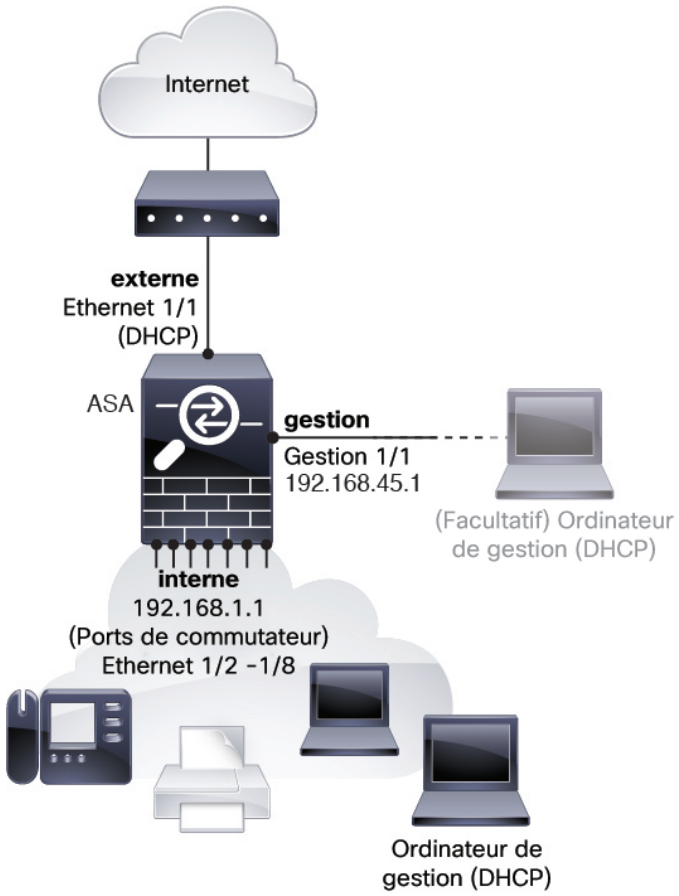
La figure suivante illustre le déploiement réseau par défaut du pare-feu Firepower 1010 à l'aide de la configuration par défaut.

Si vous connectez l'interface externe directement à un modem câble ou ADSL, nous vous recommandons de mettre le modem en mode pont pour que le logiciel ASA effectue tout le routage et la NAT pour vos réseaux internes. Si vous devez configurer PPPoE pour que l'interface externe se connecte à votre FAI, faites-le dans le cadre de l'assistant de démarrage du gestionnaire ASDM.

Remarque Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut pour l'accès au gestionnaire ASDM, vous pouvez définir l'adresse IP de gestion dans l'interface de ligne de commande ASA. Reportez-vous à la rubrique (Facultatif) Modifier l'adresse IP, à la page 184.

Si vous devez modifier l'adresse IP interne, utilisez l'assistant de démarrage du gestionnaire ASDM. Par exemple, il est possible que vous deviez modifier l'adresse IP interne dans les cas suivants :

- Si l'interface externe tente d'obtenir une adresse IP sur le réseau 192.168.1.0, qui est un réseau par défaut courant, le bail DHCP échouera et l'interface externe n'obtiendra aucune adresse IP. Ce problème se produit, car le logiciel ASA ne peut pas avoir deux interfaces sur le même réseau. Dans ce cas, vous devez modifier l'adresse IP interne de façon à la placer sur un nouveau réseau.
- Si vous ajoutez l'ASA à un réseau interne existant, vous devrez modifier l'adresse IP interne pour qu'elle se trouve sur le réseau existant.



Configuration par défaut de l'appliance Firepower 1010

La configuration par défaut de l'appareil Firepower 1010 concerne les éléments suivants :

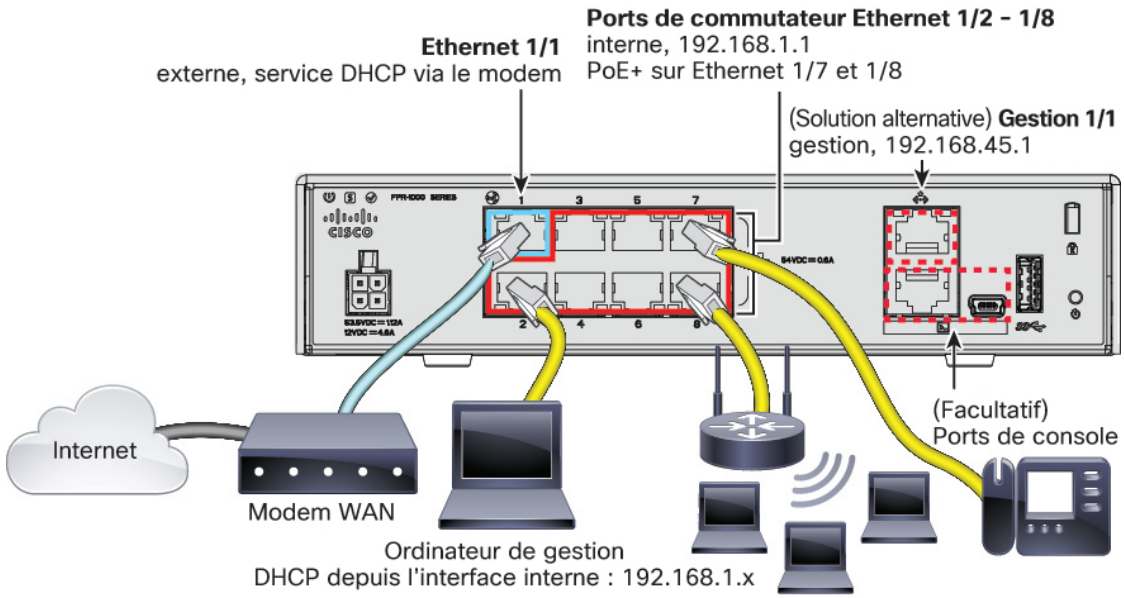
- **Commutateur matériel** : réseaux Ethernet 1/2 à 1/8 appartenant au VLAN 1
- Flux de trafic **interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **Gestion** : gestion 1/1 (gestion), adresse IP 192.168.45.1
- **Adresse IP externe** provenant de DHCP, adresse IP interne : 192.168.1.1
- **Serveur DHCP** sur l'interface interne, interface de gestion
- **Route par défaut** depuis DHCP externe
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes de gestion sont limités au réseau 192.168.45.0/24 et les hôtes internes au réseau 192.168.1.0/24.
- **NAT** : interface PAT pour l'ensemble du trafic de l'interface interne vers l'interface externe.
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration inclut les commandes suivantes :

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
```

```
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Raccorder l'appareil



Gérez l'appareil Firepower 1010 sur l'interface de gestion 1/1 ou sur l'interface Ethernet 1/2 à 1/8 (ports de commutateur internes). La configuration par défaut configure également Ethernet 1/1 comme port externe.

Procédure

Étape 1 Installez votre matériel et apprenez à l'utiliser à l'aide du guide d'installation matérielle.

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

- Ethernet 1/2 à 1/8 : connectez votre ordinateur de gestion directement à l'un des ports de commutateur internes (Ethernet 1/2 à 1/8). L'interface interne possède une adresse IP par défaut (192.168.1.1) et exécute un serveur DHCP pour fournir des adresses IP aux clients (y compris l'ordinateur de gestion). Par conséquent, assurez-vous que ces paramètres n'entrent pas en conflit avec les paramètres existants du

réseau interne (reportez-vous à la rubrique Configuration par défaut de l'appliance Firepower 1010, à la page 180).

- Gestion 1/1 : connectez votre ordinateur de gestion directement à l'interface de gestion 1/1. Vous pouvez également connecter l'interface de gestion 1/1 à votre réseau de gestion ; assurez-vous que votre ordinateur de gestion se trouve sur le réseau de gestion, car seuls les clients de ce réseau peuvent accéder à l'ASA. L'interface de gestion 1/1 possède une adresse IP par défaut (192.168.45.1) et exécute un serveur DHCP pour fournir des adresses IP aux clients (y compris l'ordinateur de gestion). Par conséquent, assurez-vous que ces paramètres n'entrent pas en conflit avec les paramètres existants du réseau de gestion (reportez-vous à la rubrique Configuration par défaut de l'appliance Firepower 1010, à la page 180).

  Si vous devez modifier l'adresse IP de l'interface de gestion 1/1 par défaut, vous devez également connecter votre ordinateur de gestion au port de console. Reportez-vous à la rubrique (Facultatif) Modifier l'adresse IP, à la page 184.

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

Pour Smart Software Licensing, ASA nécessite un accès à Internet pour pouvoir accéder à l'autorité de licence.

Étape 4 Connectez les appareils internes aux ports internes restants du commutateur, à savoir Ethernet 1/2 à 1/8.

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

Mettre le pare-feu sous tension

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

Remarque La première fois que vous démarrez le threat defense, l'initialisation peut prendre entre 15 et 30 minutes.

Avant de commencer

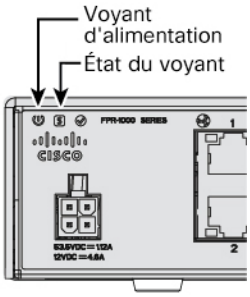
Il est important que vous utilisiez une source d'alimentation fiable pour alimenter votre appareil (à l'aide d'un système d'alimentation sans coupure, par exemple). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent en arrière-plan en permanence, et une panne de courant ne permet pas l'arrêt normal de votre système.

Procédure

Étape 1 Raccordez le câble d'alimentation à l'appareil et branchez-le à une prise électrique.

L'appareil se met automatiquement sous tension dès que vous le branchez.

Étape 2 Observez le voyant d'alimentation situé à l'arrière de l'appareil. S'il est allumé en vert, l'appareil est sous tension.



Étape 3 Observez le voyant d'état à l'arrière ou sur l'appareil. Lorsqu'il s'allume en vert, le système a terminé les diagnostics de mise sous tension.

(Facultatif) Modifier l'adresse IP

Si vous ne pouvez pas utiliser l'adresse IP par défaut pour l'accès ASDM, vous pouvez définir l'adresse IP de l'interface internede dans l'interface de ligne de commande ASA.

Remarque Cette procédure rétablit la configuration par défaut et définit également l'adresse IP que vous avez choisie. Par conséquent, si vous avez modifié la configuration ASA que vous souhaitez conserver, n'utilisez pas cette procédure.

Procédure

Étape 1 Connectez-vous au port de console ASA et accédez au mode de configuration globale. Pour plus d'informations, reportez-vous à la rubrique Accéder au ASA et au CLI FXOS, à la page 192.

Étape 2 Restaurez la configuration par défaut avec l'adresse IP choisie.

configure factory-default [*ip_address* [*mask*]]

Exemple :

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
```

```
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Étape 3 Enregistrez la configuration par défaut dans la mémoire Flash.

write memory

Se connecter au gestionnaire ASDM

Lancez le gestionnaire ASDM pour pouvoir configurer l'ASA.

ASA inclut la fonctionnalité 3DES par défaut pour l'accès de gestion uniquement. Vous pouvez donc vous connecter à Smart Software Manager et utiliser immédiatement le gestionnaire ASDM. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur l'ASA. Le chiffrement renforcé doit être activé pour les autres fonctionnalités nécessitant un chiffrement renforcé (comme le VPN). Vous devez donc vous enregistrer auprès de Smart Software Manager.

Remarque Si vous tentez de configurer des fonctionnalités susceptibles d'utiliser le chiffrement renforcé avant de vous enregistrer, même si vous configurez uniquement le chiffrement faible, votre connexion HTTPS est abandonnée sur cette interface et vous ne pouvez plus vous reconnecter. Il existe toutefois une exception à cette règle : vous êtes connecté à une interface de gestion uniquement, telle que l'interface de gestion 1/1. Cela n'a aucune incidence sur SSH. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer l'ASA, vous connecter à une interface de gestion uniquement ou vous connecter à une interface non configurée pour une fonction de chiffrement renforcé.

Avant de commencer

- Reportez-vous aux Notes de version de l'application ASDM sur Cisco.com pour plus d'informations sur les conditions requises pour exécuter l'application ASDM.

Procédure

Étape 1 Saisissez l'URL suivante dans votre navigateur.

- **https://192.168.1.1** : adresse IP de l'interface interne .Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutateur interne (Ethernet 1/2 à 1/8).
- **https://192.168.45.1** : adresse IP de l'interface de gestion.

Remarque Veillez à spécifier **https://** et non **http://** ou simplement l'adresse IP (par défaut, HTTP) ; ASA ne transfère pas automatiquement une demande HTTP à HTTPS.

La page web **Cisco ASDM** s'affiche. Des avertissements de sécurité du navigateur peuvent s'afficher, car le certificat ASA n'est pas installé ; vous pouvez ignorer ces avertissements en toute sécurité et consulter la page web.

Étape 2 Cliquez sur l'une des options disponibles : **Installer le lanceur de l'application ASDM** ou **Exécuter ASDM**.

Étape 3 Suivez les instructions à l'écran pour démarrer l'application ASDM selon l'option sélectionnée.

La page **Lanceur de l'application Cisco ASDM-IDM** s'affiche.

Étape 4 Laissez les champs de nom d'utilisateur et de mot de passe vides, puis cliquez sur **OK**.

La fenêtre principale de l'ASDM apparaît.

Configurer l'octroi de licences

Le ASA utilise Smart Licensing. Vous pouvez utiliser la version standard de Smart Licensing, qui nécessite un accès Internet ; pour la gestion hors ligne, vous pouvez configurer la réservation de licence permanente ou un logiciel Smart Software Manager sur site (anciennement, serveur satellite). Pour plus d'informations sur ces méthodes d'octroi de licences hors ligne, reportez-vous au guide Licences de fonctionnalités Cisco ASA , qui s'applique à la version standard de Smart Licensing.

Pour une présentation complète de Cisco Licensing, rendez-vous sur cisco.com/go/licensingguide.

Lorsque vous enregistrez le châssis, l'outil Smart Software Manager délivre un certificat d'identification pour établir la communication entre le pare-feu et Smart Software Manager. Il attribue également le pare-feu au compte virtuel approprié. Tant que vous ne vous êtes pas enregistré auprès de Smart Software Manager, vous ne serez pas en mesure de modifier la configuration aux fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'est pas affecté. Les fonctionnalités sous licence sont les suivantes :

- Standard
- Security Plus : pour le basculement entre l'unité active et l'unité de secours
- Chiffrement fort (3DES/AES) : si votre compte Smart n'est pas autorisé pour le chiffrement renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le chiffrement renforcé, vous pouvez ajouter manuellement une licence de chiffrement renforcé à votre compte.
- AnyConnect : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN uniquement.

ASA inclut la fonctionnalité 3DES par défaut pour l'accès de gestion uniquement. Vous pouvez donc vous connecter à Smart Software Manager et utiliser immédiatement le gestionnaire ASDM. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur l'ASA. Le chiffrement renforcé doit être activé pour les autres fonctionnalités nécessitant un chiffrement renforcé (comme le VPN). Vous devez donc vous enregistrer auprès de Smart Software Manager.

Remarque Si vous tentez de configurer des fonctionnalités susceptibles d'utiliser le chiffrement renforcé avant de vous enregistrer, même si vous configurez uniquement le chiffrement faible, votre connexion HTTPS est abandonnée sur cette interface et vous ne pouvez plus vous reconnecter. Il existe toutefois une exception à cette règle : vous êtes connecté à une interface de gestion uniquement, telle que l'interface de gestion 1/1. Cela n'a aucune incidence sur SSH. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer l'ASA, vous connecter à une interface de gestion uniquement ou vous connecter à une interface non configurée pour une fonction de chiffrement renforcé.

Lorsque vous demandez le jeton d'enregistrement de l'ASA à partir de votre compte Smart Software Manager, cochez la case **Autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton** afin que la licence Chiffrement renforcé soit appliquée (votre compte doit prendre en charge son utilisation). La licence Chiffrement renforcé est automatiquement activée pour les clients qui la prennent en charge lorsque vous appliquez le jeton d'enregistrement sur le châssis. Aucune action supplémentaire n'est requise. Si votre compte Smart n'est pas autorisé pour le chiffrement renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le chiffrement renforcé, vous pouvez ajouter manuellement une licence de chiffrement renforcé à votre compte.

Avant de commencer

- Veillez à disposer d'un compte principal sur 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 entreprise.

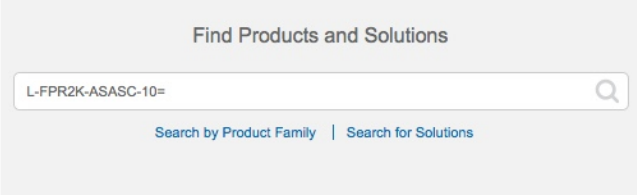
- Votre compte Smart Software Manager doit bénéficier de la licence de chiffrement renforcé (3DES/AES) pour utiliser certaines fonctionnalités (activées à l'aide de l'indicateur de conformité d'exportation).

Procédure

Étape 1 Assurez-vous que votre compte Smart Licensing contient les licences disponibles dont vous avez besoin, à savoir au minimum la licence Standard.

Si vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte Smart Software Manager. Toutefois, si vous devez ajouter des licences vous-même, utilisez le champ de recherche **Rechercher des produits et des solutions** de Cisco Commerce Workspace. Recherchez les PID de licence suivants :

Illustration 54 : Recherche de licences



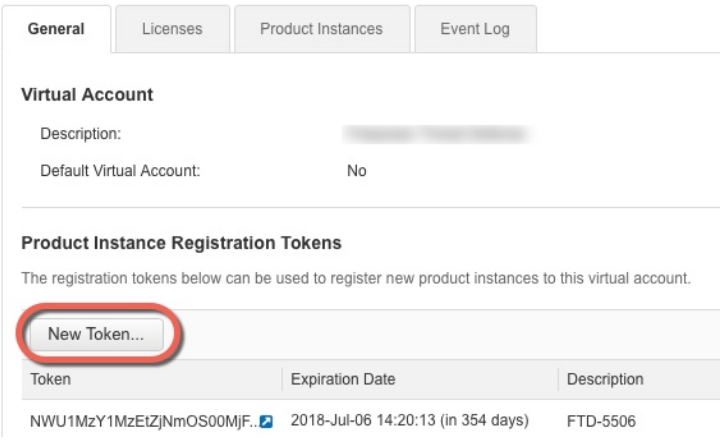
- Licence standard : L-FPR1000-ASA=. La licence Standard est gratuite, mais vous devez systématiquement l'ajouter à votre compte Smart Software Licensing.
- Licence Security Plus : L-FPR1010-SEC-PL=. La licence Security Plus permet le basculement.

- Licence Chiffrement renforcé (3DES/AES) : L-FPR1K-ENC-K9=. Requise uniquement si votre compte n'est pas autorisé pour le chiffrement fort.
- AnyConnect : consultez le Guide d'aide à la commande Cisco AnyConnect. Vous n'activez pas cette licence directement dans l'ASA.

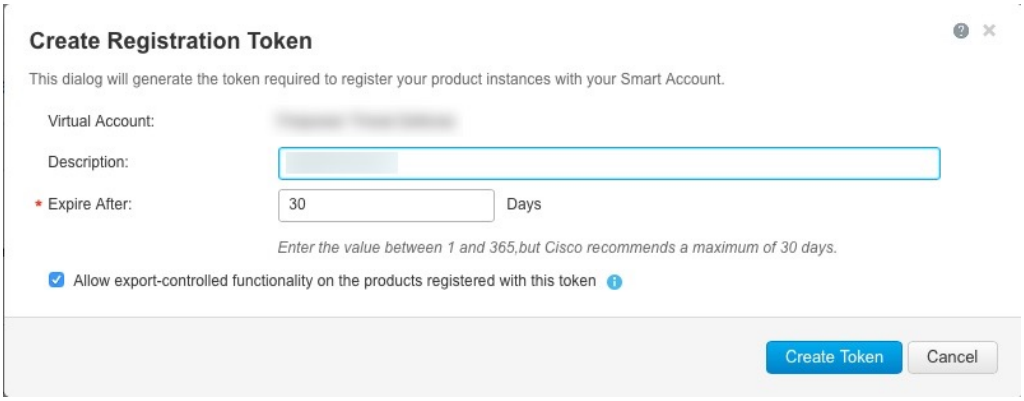
Étape 2 Dans Cisco Smart Software Manager, demandez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter cet appareil, et copiez-le.

a) Cliquez sur **Inventaire**.

b) Dans l'onglet **Général**, cliquez sur **Nouveau jeton**.



c) Dans la boîte de dialogue **Créer un jeton d'enregistrement**, saisissez les paramètres suivants, puis cliquez sur **Créer un jeton** :



- **Description**
- **Délai d'expiration** : Cisco recommande de définir un délai de 30 jours.

- **Autoriser la fonctionnalité de contrôle d'exportation sur les produits enregistrés avec ce jeton** : active l'indicateur de conformité d'exportation.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône représentant une flèche à droite du jeton pour ouvrir la boîte de dialogue **Jeton** afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour l'utiliser plus tard dans la procédure d'enregistrement du ASA.

Illustration 55 : Afficher le jeton

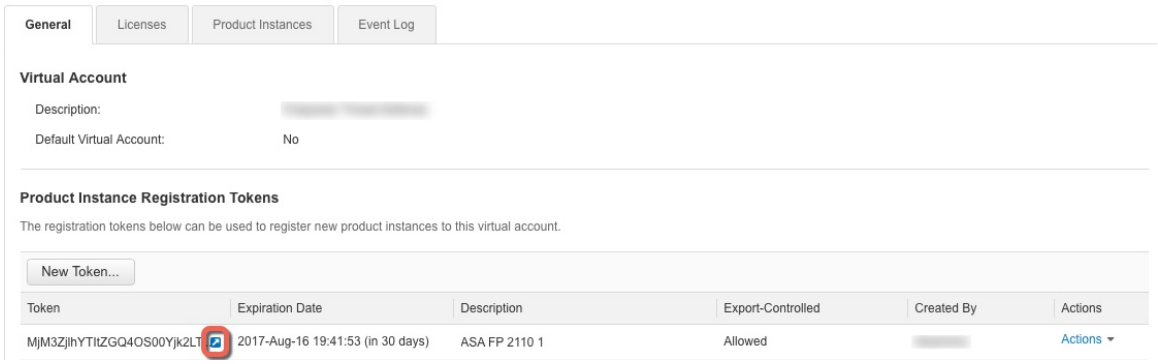
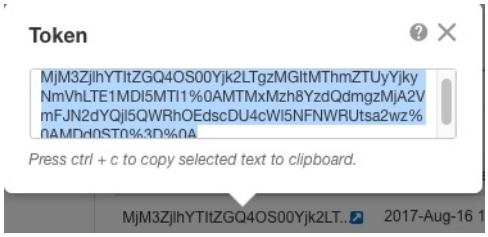


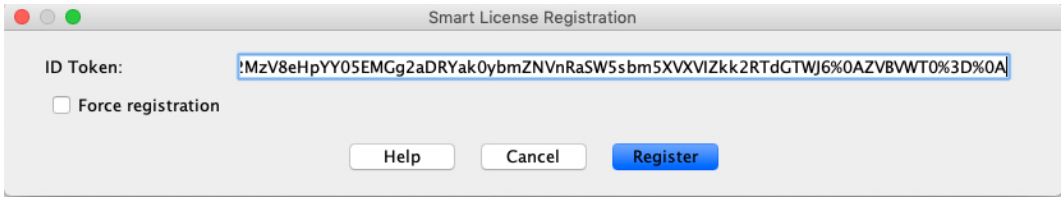
Illustration 56 : Copier le jeton



Étape 3 Dans le gestionnaire ASDM, sélectionnez **Configuration** > **Gestion des appareils** > **Octroi de licences** > **Smart Licensing**.

Étape 4 Cliquez sur **Enregistrer**.

Étape 5 Saisissez le jeton d'enregistrement dans le champ **Jeton d'ID**.

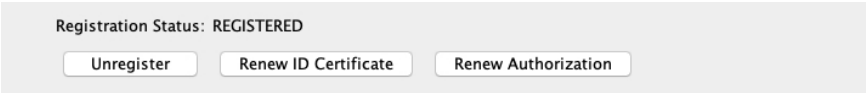


Vous pouvez également cocher la case **Forcer l'enregistrement** pour enregistrer un ASA déjà enregistré, mais qui peut ne pas être synchronisé avec Smart Software Manager. Par exemple, utilisez l'option **Forcer l'enregistrement** si l'ASA a été accidentellement supprimé de Smart Software Manager.

Étape 6 Cliquez sur **Enregistrer**.

L'ASA s'enregistre auprès de Smart Software Manager à l'aide de l'interface externe préconfigurée et demande l'autorisation d'utiliser les droits de licence configurés. Smart Software Manager applique également la licence

Chiffrement renforcé (3DES/AES) si votre compte le permet. Le gestionnaire ASDM actualise la page lorsque l'état de la licence est mis à jour. Vous pouvez également sélectionner **Surveillance** > **Propriétés** > **Licence Smart** pour vérifier l'état de la licence, en particulier si l'enregistrement échoue.



Étape 7 Définissez les paramètres suivants :

a) Cochez la case **Activer la configuration de licence Smart**.

b) Dans la liste déroulante **Niveau de fonctionnalité**, sélectionnez **Standard**.

Seul le niveau Standard est disponible.

c) (facultatif) Cochez la case **Activer Security Plus**.

Le niveau Security Plus permet le basculement entre l'unité active et l'unité de secours.

Étape 8 Cliquez sur **Apply** (Appliquer).

Étape 9 Cliquez sur l'icône **Enregistrer** dans la barre d'outils.

Étape 10 Quittez le gestionnaire ASDM et redémarrez-le.

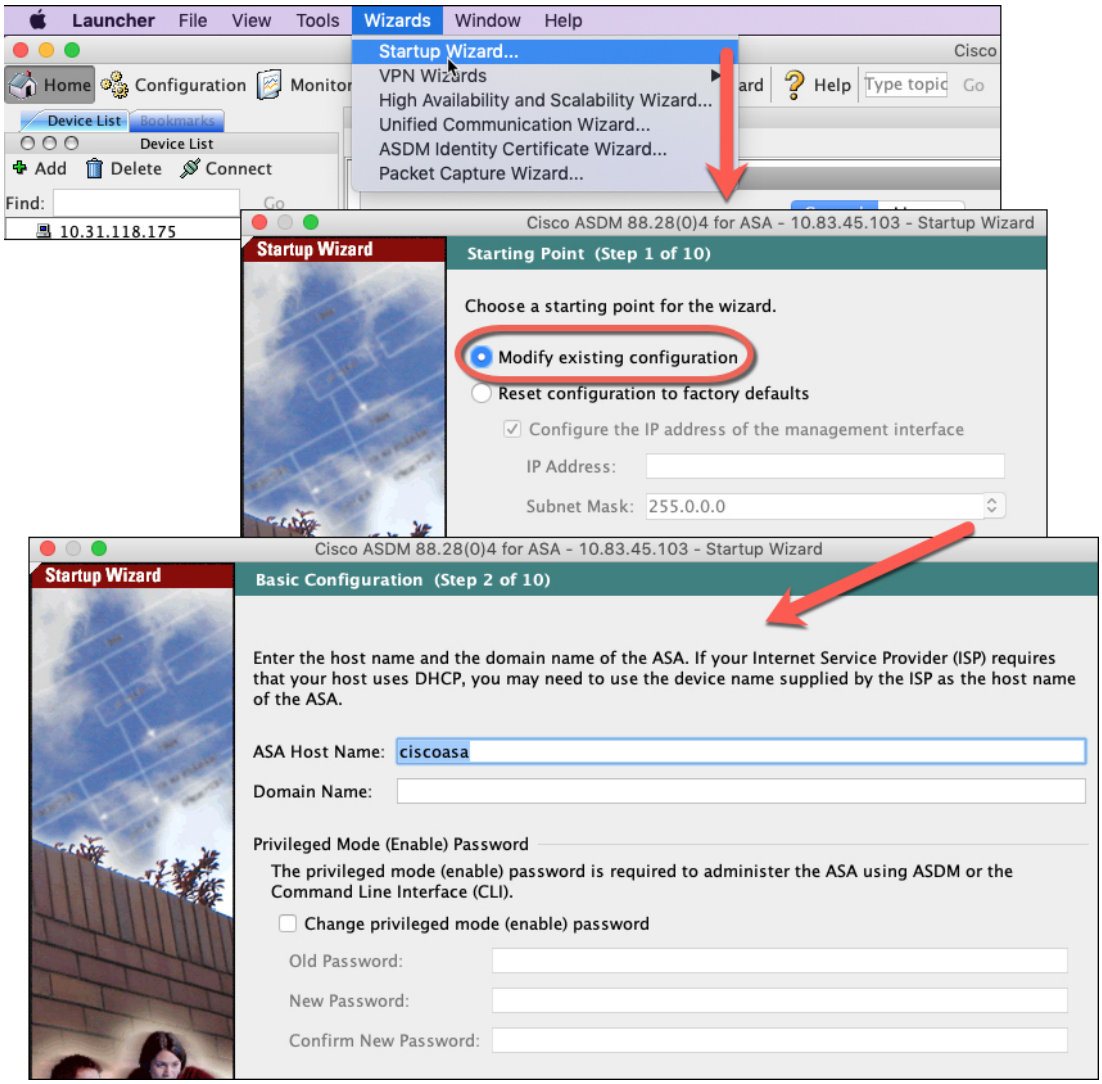
Lorsque vous modifiez des licences, vous devez redémarrer le gestionnaire ASDM pour afficher les écrans mis à jour.

Configurer l'ASA

ASDM vous permet d'utiliser des assistants pour configurer les fonctionnalités de base et avancées. Vous pouvez également configurer manuellement les fonctionnalités non incluses dans les assistants.

Procédure

Étape 1 Sélectionnez **Assistants > Assistant de démarrage**, puis cliquez sur la case d'option **Modifier la configuration existante**.



Étape 2 L'**assistant de démarrage** vous guide tout au long de la configuration :

- Mot de passe d'activation
- Interfaces, notamment la définition des adresses IP des interfaces internes et externes et l'activation des interfaces.
- Routes statiques
- Serveur DHCP
- Etc.

Étape 3 (facultatif) Dans le menu **Assistants**, exécutez d'autres assistants.

Étape 4 Pour poursuivre la configuration de votre ASA, consultez les documents disponibles pour votre version logicielle dans le document Consultation de la documentation des solutions Cisco ASA.

Accéder au ASA et au CLI FXOS

Vous pouvez utiliser l'interface de ligne de commande de ASApour dépanner ou configurer le ASA au lieu d'utiliser le gestionnaire ASDM. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console. Vous pouvez ensuite configurer l'accès SSH à l'ASA sur n'importe quelle interface ; l'accès SSH est désactivé par défaut. Consultez le Guide de configuration des opérations générales de l'ASA pour en savoir plus.

Vous pouvez également accéder au CLI FXOS à partir de la CLI de l'ASA à des fins de dépannage.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. L'appareil Firepower 1000 est livré avec un câble série USB A vers B. Veillez à installer les pilotes série USB nécessaires à votre système d'exploitation (consultez le guide matériel de l'appareil Firepower 1010) Utilisez les paramètres série suivants :

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

Vous vous connectez à l'interface de ligne de commande ASA. Par défaut, aucune information d'identification d'utilisateur n'est requise pour l'accès à la console.

Étape 2 Accédez au mode d'exécution privilégié.

enable

Vous êtes invité à modifier le mot de passe la première fois que vous saisissez la commande **enable**.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Le mot de passe d'activation que vous avez défini sur l'ASA est également le mot de passe de l'utilisateur **admin** de la FXOS si l'ASA ne démarre pas et que vous passez en mode Protégé en cas de défaillance sur la FXOS.

Toutes les commandes (à l'exception des commandes de configuration) sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode d'exécution privilégié, saisissez la commande **disable**, **exit** ou **quit**.

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, saisissez la commande **exit**, **quit** ou **end**.

Étape 4 (facultatif) Connectez-vous au CLI FXOS.

connect fxos [**admin**]

- **admin** : fournit un accès de niveau administrateur. Sans cette option, les utilisateurs disposent d'un accès en lecture seule. Notez qu'aucune commande de configuration n'est disponible, même en mode administrateur.

Vous n'êtes pas invité à saisir les informations d'identification de l'utilisateur. Le nom d'utilisateur ASA actuel est transmis à la FXOS, et aucune connexion supplémentaire n'est requise. Pour revenir à l'interface de ligne de commande ASA, saisissez **exit** ou appuyez sur **Ctrl-Maj-6**, **x**.

Dans FXOS, vous pouvez afficher l'activité des utilisateurs à l'aide de la commande **scope security/show audit-logs**.

Exemple :

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Et après ?

- Pour poursuivre la configuration de votre ASA, consultez les documents disponibles pour votre version logicielle dans le document Consulter la documentation des solutions Cisco ASA.
- Pour le dépannage, consultez le Guide de dépannage de la console FXOS.

Et après ?