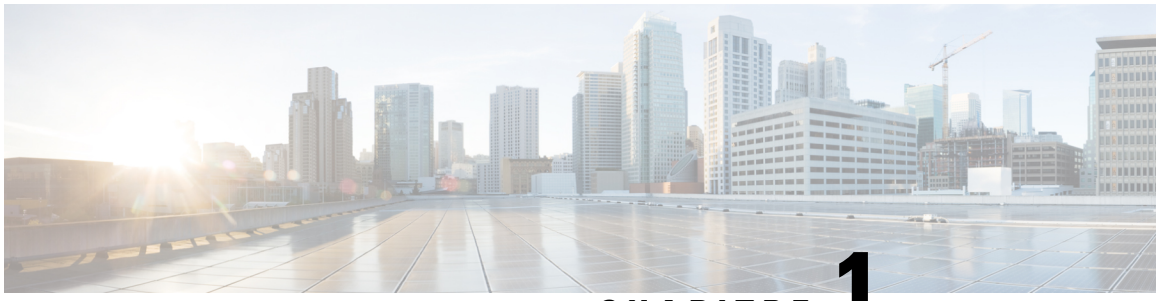
Guide de démarrage (GD) pour Cisco Firepower 9300

Dernière modification : 2025-04-25

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



CHAPITRE 1

Quels sont le système d'exploitationet le gestionnaire d'applications pour vous?

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

Systèmes d'exploitation

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

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

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

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

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

Gestionnaires

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

Défense contre les menaces Gestionnaires

Tableau 1 : Défense contre les menaces Gestionnaires

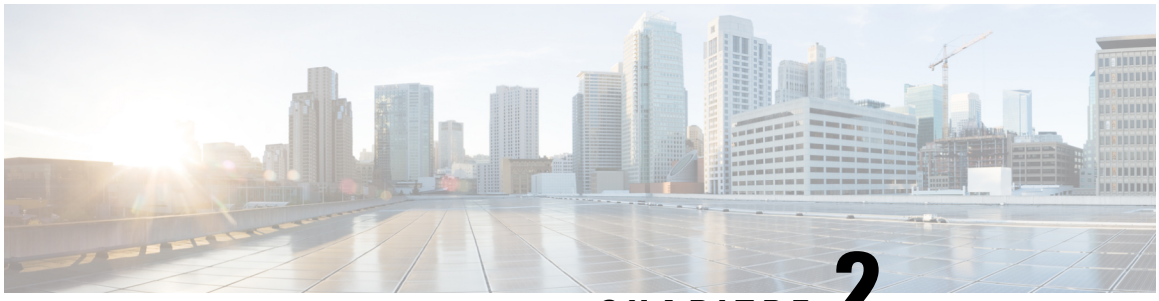
Gestionnaire	Description
Cisco Secure Firewall Management Center (anciennement Cisco Firepower Management Center)	Le centre de gestion est un puissant gestionnaire multidispositifs basé sur le Web qui fonctionne sur son propre matériel de serveur, ou comme un appareil virtuel sur un hyperviseur. Vous devriez utiliser le centre de gestion si vous voulez un gestionnaire multidispositifs, et vous avez besoin de toutes les fonctionnalités sur le dispositif de défense contre les menaces. Le centre de gestion fournit également une analyse et une surveillance puissantes du trafic et des événements. **Remarque** Le centre de gestion n'est pas compatible avec d'autres gestionnaires car le centre de gestion possède la configuration défense contre les menaces, et vous n'êtes pas autorisé à configurer le dispositif de défense contre les menaces directement, en contournant le centre de gestion. Pour commencer avec le centre de gestion, configurez d'abord le châssis conformément à Configuration initiale du châssis Firepower 9300, à la page 5, et puis voir Défense contre les menaces Déploiement avec le Centre de gestion, à la page 33.
Cisco Secure Firewall Device Manager (anciennement Cisco Firepower Device Manager)	Le gestionnaire d'appareil est un gestionnaire simplifié, basé sur le Web et sur l'appareil. Parce qu'il est simplifié, certaines fonctionnalités défense contre les menaces ne sont pas prises en charge à l'aide de gestionnaire d'appareil. Vous devriez utiliser le gestionnaire d'appareil si vous ne gérez qu'un petit nombre de appareils et n'avez pas besoin d'un gestionnaire multidispositifs. **Remarque** À la fois le gestionnaire d'appareil et le CDO en mode FDM peuvent découvrir la configuration sur le pare-feu, vous pouvez donc utiliser le gestionnaire d'appareil et le CDO pour gérer le même pare-feu. Le centre de gestion n'est pas compatible avec les autres gestionnaires. Pour commencer avec le gestionnaire d'appareil, configurez d'abord le châssis conformément à Configuration initiale du châssis Firepower 9300, à la page 5, et puis voir Défense contre les menaces Déploiement avec le Gestionnaire d'appareil, à la page 63.

Gestionnaire	Description
Cisco Defense Orchestrator (CDO)	CDO propose deux modes de gestion : • (7.2 et versions ultérieures) Mode de centre de gestion fourni dans le nuage avec toutes les fonctionnalités de configuration d'un centre de gestion sur site. Pour la fonctionnalité d'analyse, vous pouvez utiliser Secure Cloud Analytics dans le nuage ou un centre de gestion sur place. • (Utilisateurs existants de CDO uniquement) Mode gestionnaire de dispositifs avec une expérience utilisateur simplifiée. Ce mode n'est disponible que pour les utilisateurs qui utilisent déjà CDO pour gérer les défense contre les menaces dans le mode gestionnaire de dispositifs. Ce mode n'est pas couvert par ce guide. Comme CDO est basé sur le cloud, il n'y a pas de frais généraux liés à l'exécution de CDO sur vos propres serveurs. CDO gère également d'autres appareils de sécurité, comme les appareils ASA, de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos appareils de sécurité. Pour vous familiariser avec le provisionnement à faible intervention de CDO, consultez Défense contre les menaces Déploiement avec CDO, à la page 93.
Cisco Secure Firewall Threat Defense REST API	Le threat defense REST API (API REST de défense contre les menaces) vous permet d'automatiser la configuration directe de défense contre les menaces. Cette API est compatible avec l'utilisation de gestionnaire d'appareil et CDO car elles peuvent toutes deux découvrir la configuration sur la firewa Vous ne pouvez pas utiliser cette API si vous gérez le dispositif de défense contre les menaces à l'aide centre de gestion. The threat defense REST API (rEST API de défense contre les menaces) n'est pas visé par ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de Cisco Secure Firewall Threat Defense REST API.
API REST du centre de gestion du Cisco Secure Firewall	L'API REST du centre de gestion vous permet d'automatiser la configuration des politiques centre de gestion qui peuvent ensuite être appliquées aux défense contre les menaces gérés. Cette API ne gère pas le dispositif de défense contre les menaces directement. Le management center REST API (rEST API centre de gestion) n'est pas visé par ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage rapide de Cisco Secure Firewall Management Center REST API.

Gestionnaires ASA

Tableau 2 : Gestionnaires ASA

Gestionnaire	Description
Gestionnaire ASDM (Adaptive Security Device Manager)	ASDM est un gestionnaire basé sur Java qui offre une fonctionnalité ASA complète sur l'appareil. Vous devez utiliser ASDM si vous préférez une interface graphique à l'interface de ligne de commande et si vous devez seulement gérer un petit nombre d'appareils ASA. ASDM peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande, CDO ou CSM avec ASDM. Pour commencer avec ASDM, configurez d'abord le châssis en fonction de Configuration initiale du châssis Firepower 9300, à la page 5, puis consultez Déploiement d'ASA avec ASDM, à la page 123.
Interface de ligne de commande	Vous devriez utiliser l'interface de ligne de commande (CLI) de l'ASA si vous préférez ce type d'interface aux interfaces graphiques. L'interface de ligne de commande n'est toutefois pas abordée dans ce guide. Consultez les guides de configuration d'ASA pour obtenir plus d'informations.
CDO	CDO est un gestionnaire multidispositifs simplifié hébergé en nuage. Puisqu'il s'agit d'une solution simplifiée, certaines fonctionnalités ASA ne sont pas prises en charge au moyen de CDO. Vous devez utiliser CDO si vous souhaitez utiliser un gestionnaire multidispositifs offrant une expérience de gestion simplifiée. Et comme CDO est hébergé en nuage, l'exécution de CDO sur vos propres serveurs n'entraîne pas de trafic de service. Le CDO gère également d'autres appareils de sécurité, tels que les défense contre les menaces, de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos appareils de sécurité. CDO peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande ou ASDM. Le gestionnaire CDO n'est toutefois pas abordé dans ce guide. Pour commencer à utiliser CDO, consultez la page d'accueil de CDO.
Cisco Security Manager (CSM)	CSM est un puissant gestionnaire multidispositifs qui fonctionne sur son propre matériel de serveur. Vous devez utiliser CSM si vous avez besoin de gérer un grand nombre d'ASA. CSM peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande ou ASDM. Le CSM ne prend pas en charge la gestion des défense contre les menaces. Le gestionnaire CSM n'est toutefois pas abordé dans ce guide. Pour en savoir plus, consultez le guide de l'utilisateur CSM.
API REST ASA	L'API REST ASA vous permet d'automatiser la configuration d'ASA. Cependant, l'API n'inclut pas toutes les fonctionnalités de l'ASA et ne fait plus l'objet d'améliorations. L'API REST ASA n'est pas abordée dans ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage rapide de Cisco ASA REST API.



CHAPITRE 2

Configuration initiale du châssis Firepower 9300

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

Ce chapitre décrit comment effectuer la configuration initiale du Firepower 9300châssis Cisco, y compris la configuration des interfaces à utiliser avec l'ASA et les Défense contre les menacesdispositifs logiques.

Ce guide est-il pour vous?

Ce guide décrit comment configurer le châssis Firepower 9300 pour une utilisation avec l'ASA ou l'application Défense contre les menaces. Ce guide décrit les déploiements suivants :

- Défense contre les menaces autonome en tant qu'instance native ou de contenant (fonctionnalité multi-instances) à l'aide de centre de gestion
- Défense contre les menaces autonome utilisant le gestionnaire d'appareil

Remarque Le gestionnaire d'appareil ne prend pas en charge la fonctionnalité multi-instances.

- Défense contre les menaces autonome utilisant CDO

Remarque CDO ne prend pas en charge la fonctionnalité multi-instances.

- ASA autonome utilisant ASDM

Ce chapitre n'aborde pas les déploiements suivants. Pour en savoir plus à ce sujet, consultez les guides de configuration pour FXOS, ASA, FDM, CDO et FMC :

- Haute disponibilité/Basculement
- Mise en grappe (ASA ou Défense contre les menaces utilisant centre de gestion uniquement)
- Multi-instances (Défense contre les menaces utilisant centre de gestion uniquement)
- Application de décorateurs Radware DefensePro
- Configuration de l'interface de ligne de commande (ASA ou FXOS uniquement)

Ce guide vous montre la configuration d'une politique de sécurité de base; si vous avez des exigences plus avancées, consultez le guide de configuration.

À propos du châssis Firepower 9300

Le châssis Firepower 9300 est une plateforme de nouvelle génération pour les solutions de sécurité du réseau et du contenu. Le châssis Firepower 9300 comprend un superviseur et jusqu'à trois modules de sécurité sur lesquels vous pouvez installer des dispositifs logiques. Il accepte également plusieurs modules de réseau haute performance.

Fonctionnement du dispositif logique avec Firepower 4100/9300

Le Firepower 4100/9300 exécute son propre système d'exploitation sur le superviseur appelé le Firepower eXtensible Operating System (FXOS). Le gestionnaire de châssis sur la boîte offre des fonctionnalités de gestion simples et basées sur l'interface graphique utilisateur. Vous configurez les paramètres de l'interface matérielle, l'octroi de licences Smart (pour l'ASA) et d'autres paramètres opérationnels de base sur le superviseur à l'aide de l'interface de ligne de commande FXOS de . Pour utiliser l'interface de ligne de commande de FXOS, consultez le FXOS CLI configuration guide (Guide de configuration de l'interface de ligne de commande FXOS).

Un dispositif logique vous permet d'exécuter une instance d'application ainsi qu'une application de décorateurs facultative pour former une chaîne de services. Lorsque vous déployez le dispositif logique, le superviseur télécharge une image d'application de votre choix et établit une configuration par défaut. Vous pouvez ensuite configurer la politique de sécurité dans le système d'exploitation de l'application.

Les dispositifs logiques ne peuvent pas former de chaîne de service entre eux et ne peuvent pas communiquer entre eux sur le fond de panier. Tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre dispositif logique. Pour les instances de contenant, vous pouvez partager des interfaces de données; seulement dans ce cas, plusieurs dispositifs logiques peuvent communiquer sur le fond de panier.

Remarque Vous pouvez installer différents types d'applications sur des modules distincts dans le châssis. Vous pouvez également exécuter différentes versions d'un type d'application sur des modules distincts.

Applications prises en charge

Vous pouvez déployer des dispositifs logiques sur votre châssis en utilisant les types d'applications suivants.

Défense contre les menaces

Défense contre les menaces fournit des services de pare-feu de nouvelle génération, notamment le pare-feu dynamique, le routage, le VPN, le système de prévention des intrusions de nouvelle génération (NGIPS), la visibilité et le contrôle des applications (AVC), le filtrage des URL et la protection contre les logiciels malveillants.

Vous pouvez gérer Défense contre les menaces à l'aide de l'un des gestionnaires suivants :

- Centre de gestion : un gestionnaire multidispositif complet sur un serveur séparé.
- Gestionnaire d'appareil : un gestionnaire simplifié pour un seul appareil inclus sur le dispositif.
- CDO : un gestionnaire multidispositif en nuage

ASA

L'ASA offre des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN dans un seul dispositif. Vous pouvez gérer l'ASA en utilisant l'une des solutions de gestion suivantes :

- ADM : un gestionnaire simplifié pour un seul appareil inclus sur le dispositif. *Ce guide décrit comment gérer l'ASA à l'aide d'ASDM.*
- Interface de ligne de commande
- CDO : un gestionnaire multidispositif en nuage
- CSM : un gestionnaire multidispositif sur un serveur séparé.

Radware DefensePro (Décorateur)

Vous pouvez installer Radware DefensePro (vDP) pour qu'il s'exécute en premier plan sur l'ASA ou Défense contre les menaces comme application de décorateurs. vDP est une plateforme virtuelle basée sur KVM qui fournit des fonctionnalités de détection et d'atténuation des dénis de service distribués (DDoS) sur Firepower 4100/9300. Le trafic du réseau doit d'abord passer par vDP avant d'atteindre l'ASA ou Défense contre les menaces.

Pour déployez vDP, consultez le FXOS configuration guide (Guide de configuration de FXOS).

Instances d'application du dispositif logique : instance de conteneur ou instance native

Les instances d'application du dispositif logique s'exécutent dans les types de déploiement suivants :

- Instance native : Une instance native utilise toutes les ressources (CPU, RAM et espace disque) de security module. Vous ne pouvez donc installer qu'une seule instance native.
- Instance de conteneur : Une instance de conteneur utilise un sous-ensemble de ressources de security module. Vous pouvez donc installer plusieurs instances de conteneur. **Remarque :** La fonctionnalité

multi-instance n'est prise en charge que pour Défense contre les menaces; elle n’est pas prise en charge pour l’ASA ou conjointement avec vDP.

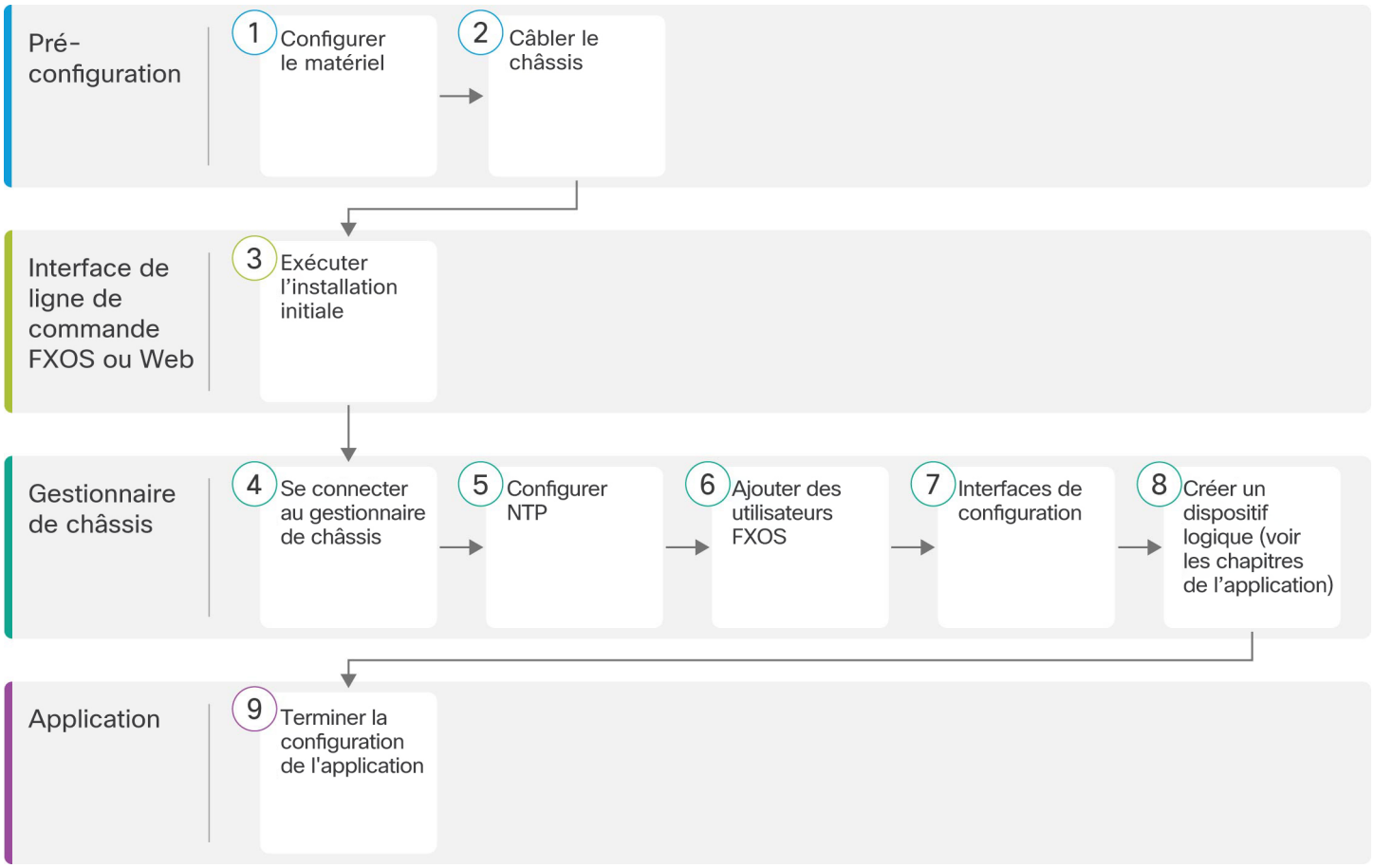
Vous pouvez utiliser une instance native sur certains modules et des instances de conteneur sur les autres modules.

Nombre maximal d’instances de conteneur par modèle

- Module de sécurité Firepower 9300 SM-24 — 7
- Module de sécurité Firepower 9300 SM-36 — 11
- Module de sécurité Firepower 9300 SM-40 — 13
- Module de sécurité Firepower 9300 SM-44 — 14
- Module de sécurité Firepower 9300 SM-48 — 15
- Module de sécurité Firepower 9300 SM-56 — 18

Procédure de bout en bout

Consultez les tâches suivantes pour configurer le châssis Firepower 9300 et déployer des dispositifs logiques sur votre châssis.



1	Pré-configuration	Configurez le matériel Firepower 9300. Consultez le Firepower 9300 hardware guide (Guide matériel Firepower 9300) et le (Guide matériel Firepower 4100).
2	Pré-configuration	Câbler le châssis, à la page 10.
3	Interface de ligne de commande FXOS ou Web	Effectuer la configuration initiale du châssis, à la page 15.
4	Gestionnaire de châssis	Se connecter à Gestionnaire de châssis, à la page 19.
5	Gestionnaire de châssis	Configurer NTP, à la page 20.
6	Gestionnaire de châssis	Ajouter des utilisateurs FXOS, à la page 22.
7	Gestionnaire de châssis	Interfaces de configuration, à la page 24.

8	Gestionnaire de châssis	Créez des dispositifs logiques : • Défense contre les menaces avec le centre de gestion : consultez Défense contre les menaces Déploiement avec le Centre de gestion, à la page 33. • Défense contre les menaces avec le gestionnaire d'appareil : consultez Défense contre les menaces Déploiement avec le Gestionnaire d'appareil, à la page 63. • Défense contre les menaces avec le CDO : consultez Défense contre les menaces Déploiement avec CDO, à la page 93. • ASA : consultez Déploiement d'ASA avec ASDM, à la page 123. **Remarque** La prise en charge de Défense contre les menaces et d'ASA sur le même châssis a été ajoutée dans FXOS 2.6.1/Défense contre les menaces 6.4/ASA 9.12(1). **Remarque** La prise en charge de Défense contre les menaces avec le gestionnaire d'appareil a été ajoutée dans FXOS 2.7.1/Défense contre les menaces 6.5
9	Application	Terminez la configuration de l'application : • Défense contre les menaces avec le centre de gestion : consultez Défense contre les menaces Déploiement avec le Centre de gestion, à la page 33. • Défense contre les menaces avec le gestionnaire d'appareil : consultez Défense contre les menaces Déploiement avec le Gestionnaire d'appareil, à la page 63. • Défense contre les menaces avec le CDO : consultez Défense contre les menaces Déploiement avec CDO, à la page 93. • ASA : consultez Déploiement d'ASA avec ASDM, à la page 123.

Câbler le châssis

Câblez les interfaces suivantes pour la configuration initiale du châssis, la surveillance continue et l'utilisation de dispositifs logiques.

- Console port (Port de console) : (facultatif.) Si vous n'effectuez pas la configuration initiale sur le port de gestion du châssis, connectez votre ordinateur de gestion au port de console pour effectuer la configuration initiale du châssis. Le Firepower 9300 comprend un câble de console de série RS-232 à RJ-45. Vous devrez peut-être utiliser un câble série tiers vers USB pour établir la connexion.
- Chassis Management port (Port de gestion du châssis) : connectez le port de gestion du châssis à votre réseau de gestion pour la configuration et la gestion continue du châssis. Vous pouvez effectuer la configuration initiale de ce port s'il reçoit une adresse IP d'un serveur DHCP.
- Logical device Management interface (Interface de gestion des dispositifs logiques) : utilisez une ou plusieurs interfaces pour gérer les dispositifs logiques. Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Vous pouvez choisir n'importe quelle interface sur le

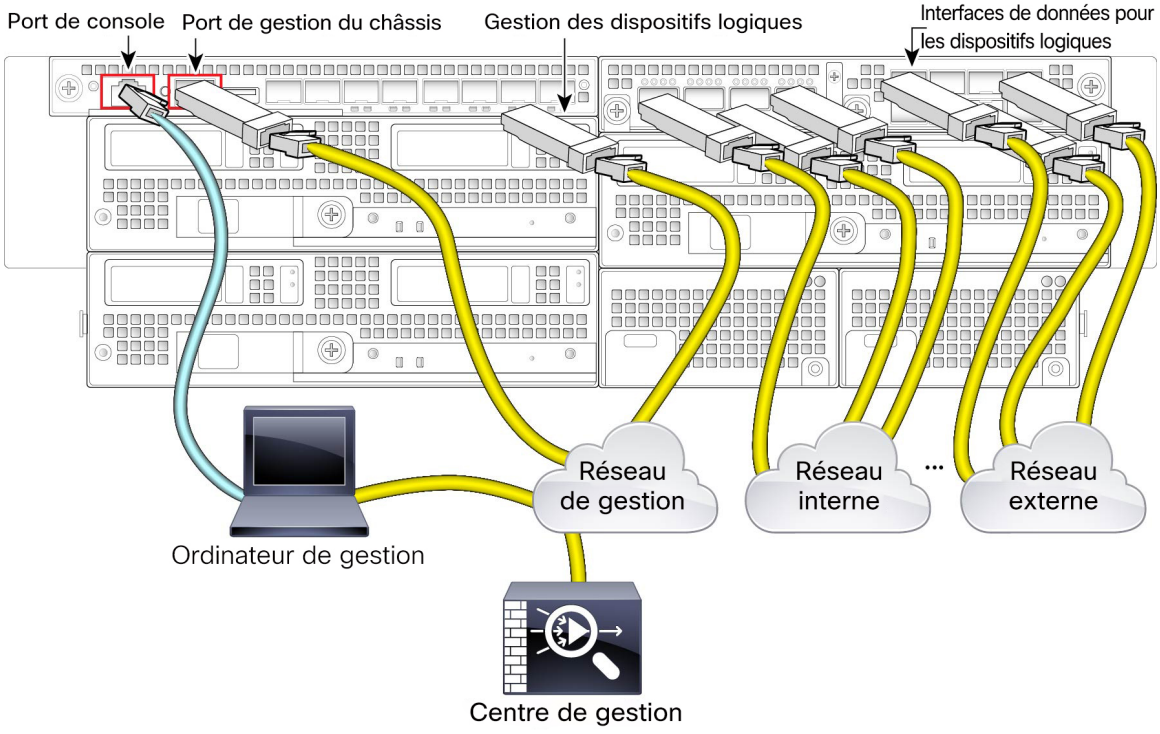
châssis à cette fin, sauf le port de gestion du châssis, qui est réservé à la gestion FXOS.les interfaces de gestion peuvent être partagées entre les dispositifs logiques, ou vous pouvez utiliser une interface distincte par dispositif logique. En règle générale, vous partagez une interface de gestion avec tous les dispositifs logiques, ou si vous utilisez des interfaces distinctes, vous pouvez les placer sur un seul réseau de gestion. Mais vos exigences précises en matière de réseau peuvent varier. Pour défense contre les menaces, l'interface de gestion est une interface distincte des interfaces de données et elle possède ses propres paramètres réseau. Dans la version 6.7 et ultérieure, vous pouvez éventuellement configurer une interface de données pour avoir l'accès gestionnaire au lieu de l'interface de gestion. Dans ce cas, vous devez toujours attribuer une interface de gestion au dispositif logique pour des raisons d'architecture interne, mais vous n'avez pas besoin de la câbler. Notez que pour centre de gestion, l'accès gestionnaire à partir d'une interface de données n'est pas pris en charge dans les déploiements à haute disponibilité ou de mise en grappe. Pour de plus amples informations, consultez la commande **configure network management-data-interface** dans la référence de commande FTD.

- Data interfaces (Interfaces de données) : connectez les interfaces de données aux réseaux de données de votre dispositif logique. Vous pouvez configurer des interfaces physiques, des EtherChannels, des sous-interfaces VLAN (pour les instances de conteneur uniquement) et des ports de séparation pour diviser les interfaces à haute capacité. vous pouvez câbler plusieurs dispositifs logiques aux mêmes réseaux ou à des réseaux différents, selon les besoins de votre réseau. Pour les instances de contenant, vous pouvez partager des interfaces de données; seulement dans ce cas, plusieurs dispositifs logiques peuvent communiquer sur le fond de panier. Autrement, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre dispositif logique. Pour en savoir plus sur les limites et les directives relatives aux interfaces partagées, consultez le FXOS configuration guide (Guide de configuration FXOS).

Remarque Toutes les interfaces, à l'exception du port de console, nécessitent des émetteurs-récepteurs SFP, SFP+ et QSFP. Consultez le Guide d'installation du matériel (GIM) pour Cisco Firepower 9300 (guide d'installation du matériel) pour connaître les émetteurs-récepteurs pris en charge.

Remarque Bien que non traité dans ce guide, pour le déploiement à haute disponibilité, utilisez une interface de données pour le lien de basculement/état. Pour la mise en grappe inter-châssis, utilisez un EtherChannel défini sur le châssis comme interface de type de grappe.

Défense contre les menaces avec le câblage du Centre de gestion

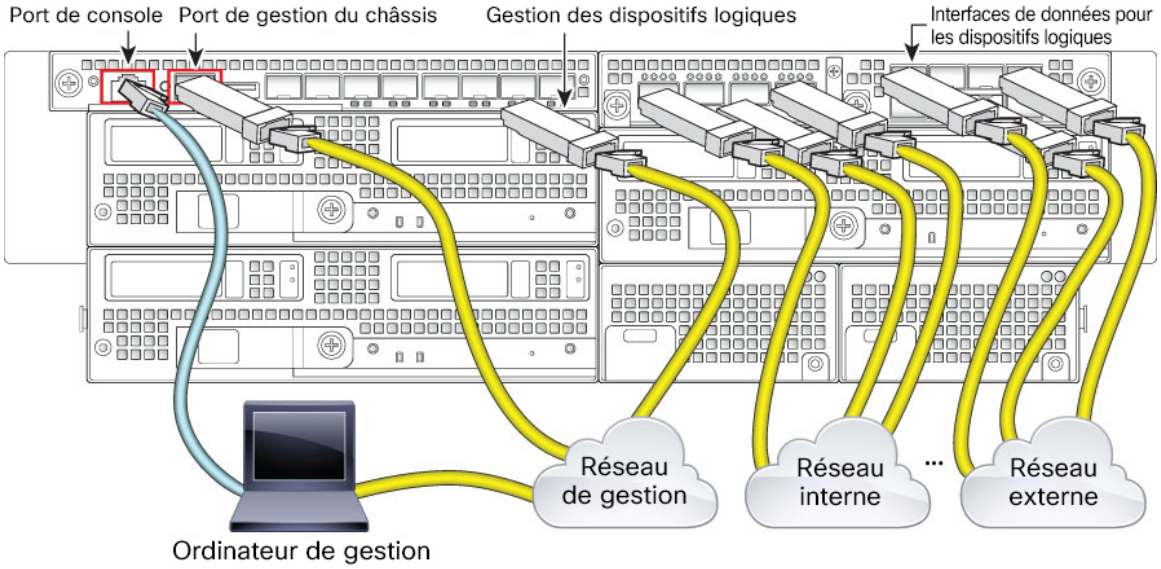


Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Placez le centre de gestion sur le réseau de gestion des dispositifs logiques (ou rendez-le accessible à partir de ce dernier). Défense contre les menaces et le centre de gestion nécessitent un accès à Internet par l'entremise du réseau de gestion pour les mises à jour et les licences. Dans la version 6.7 et ultérieure, vous pouvez éventuellement configurer une interface de données pour la gestion de centre de gestion au lieu de l'interface de gestion. Notez que l'accès centre de gestion à partir d'une interface de données n'est pas pris en charge dans les déploiements à haute disponibilité ou à mise en grappe. Pour en savoir plus sur la configuration d'une interface de données pour l'accès à centre de gestion, consultez la commande **configure network management-data-interface** dans la référence de commande FTD.

Remarque La connexion de gestion est un canal de communication sécurisé et chiffré par SSL entre elle et le dispositif. Vous n'avez pas besoin d'exécuter ce trafic sur un tunnel chiffré supplémentaire comme un VPN de site à site pour des raisons de sécurité. Si le VPN tombe en panne, par exemple, vous perdrez votre connexion de gestion. Nous vous recommandons donc un chemin de gestion simple.

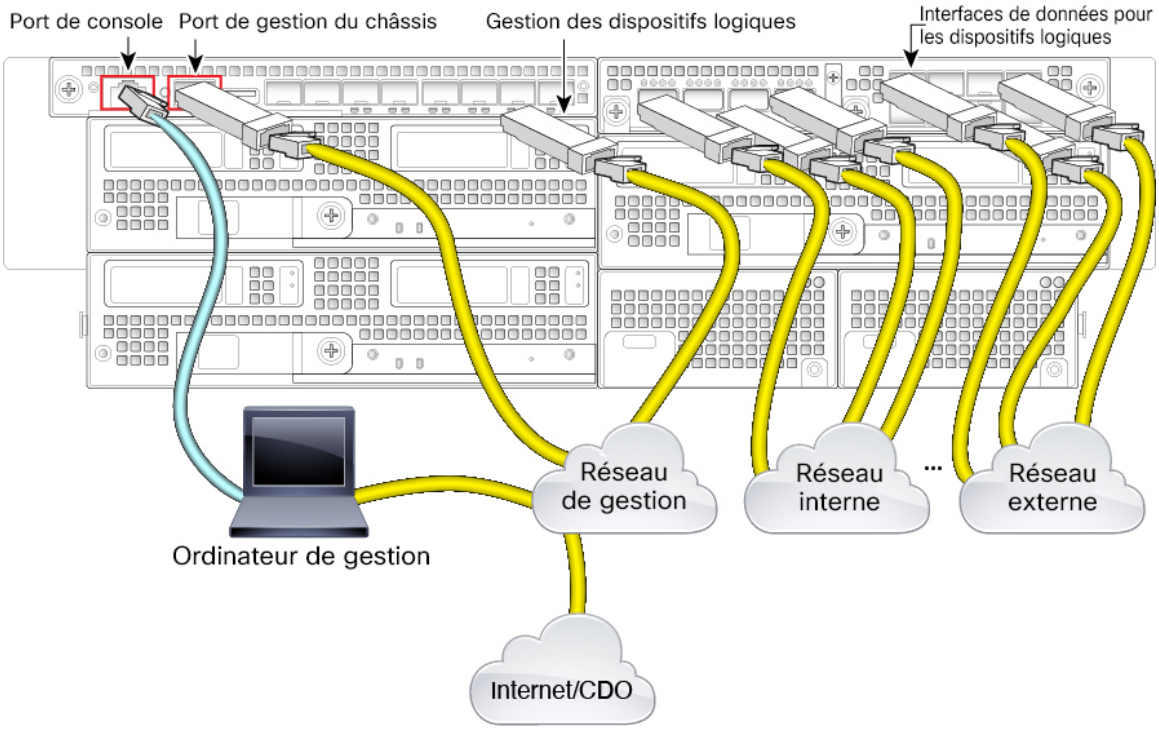
Défense contre les menaces avec le câblage du Gestionnaire d'appareil



Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Effectuez la configuration initiale de Défense contre les menaces sur l'interface de gestion du dispositif logique. Défense contre les menaces nécessite un accès Internet pour les licences, les mises à jour et la gestion des CDO, et le comportement par défaut consiste à acheminer le trafic de gestion vers l'adresse IP de la passerelle que vous avez spécifiée lors du déploiement du Défense contre les menaces. Vous pourrez activer ultérieurement la gestion de gestionnaire d'appareil à partir de n'importe quelle interface de données.

Défense contre les menaces avec le câblage CDO

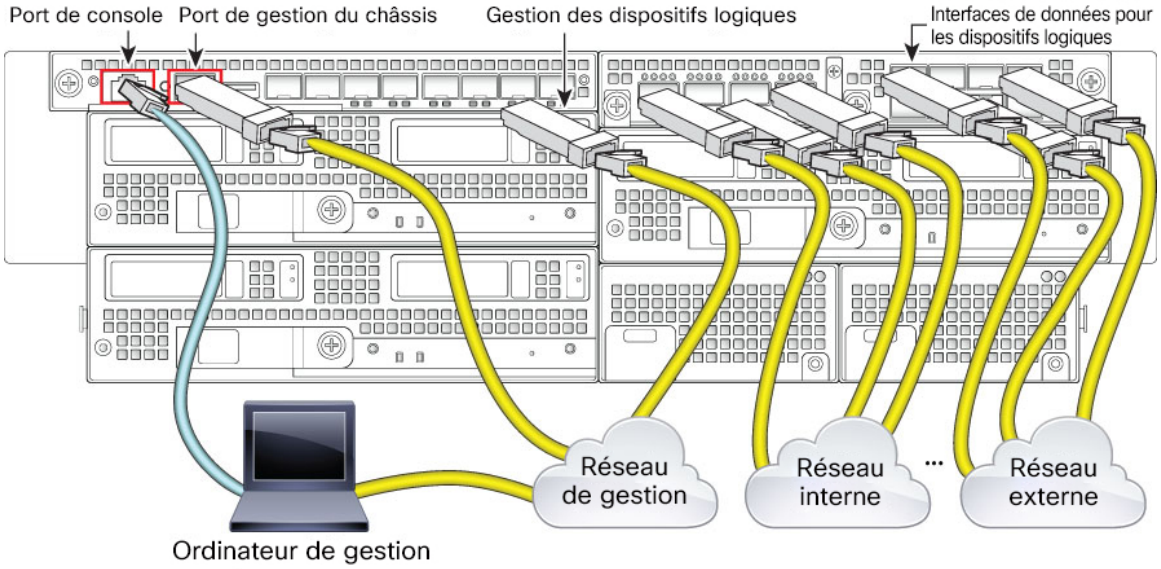


Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Assurez-vous qu'Internet soit accessible à partir du réseau de gestion des dispositifs logiques. Défense contre les menaces nécessite un accès à Internet par l'entremise du réseau de gestion du CDO, les mises à jour et les licences. Vous pouvez éventuellement configurer une interface de données pour la gestion du CDO au lieu de l'interface de gestion. Pour en savoir plus sur la configuration d'une interface de données pour l'accès du gestionnaire, consultez la commande **configure network management-data-interface** dans la référence de commande FTD.

Remarque La connexion de gestion est un canal de communication sécurisé et chiffré par SSL entre elle et le dispositif. Vous n'avez pas besoin d'exécuter ce trafic sur un tunnel chiffré supplémentaire comme un VPN de site à site pour des raisons de sécurité. Si le VPN tombe en panne, par exemple, vous perdrez votre connexion de gestion. Nous vous recommandons donc un chemin de gestion simple.

Câblage de l'ASA



Ce guide suppose que vous avez un réseau de gestion distinct avec son propre accès Internet. Par défaut, l'interface de gestion est préconfigurée lorsque vous le déployez, mais vous devez configurer les interfaces de données ultérieurement.

Effectuez la configuration initiale de l'ASA sur l'interface de gestion du dispositif logique. Vous pourrez activer ultérieurement la gestion à partir de n'importe quelle interface de données.

Effectuer la configuration initiale du châssis

Avant de pouvoir utiliser le gestionnaire de châssis pour configurer et gérer votre système, vous devez effectuer certaines tâches de configuration initiale. Vous pouvez effectuer la configuration initiale en utilisant l'interface de ligne de commande de FXOS sur le port de console ou une session SSH sur le port de gestion du châssis, ou en utilisant le protocole HTTPS sur le port de gestion du châssis.

Effectuer la configuration initiale du châssis à l'aide d'un navigateur

Le port de gestion de châssis obtient une adresse IP en utilisant DHCP. Pour la configuration initiale, vous pouvez utiliser un navigateur Web pour configurer les paramètres de base du châssis. Si vous n'avez pas de serveur DHCP, vous devez utiliser le port de console pour la configuration initiale.

Remarque Pour relancer la configuration initiale, vous devez effacer toute configuration existante à l'aide des commandes suivantes à partir de l'interface de ligne de commande :

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Avant de commencer

Recueillez les informations suivantes à utiliser avec le script de configuration :

- Nouveau mot de passe de l'administrateur
- Adresse IP de gestion et filtre d'adresse locale
- l'adresse IP de la passerelle
- Sous-réseaux à partir desquels vous souhaitez autoriser l'accès HTTPS et SSH
- Nom d'hôte et le nom de domaine
- l'adresse IP du serveur DNS

Procédure

Étape 1 Configurez votre serveur DHCP pour attribuer une adresse IP au port de gestion du châssis.

La demande du client DHCP du châssis contient les informations suivantes :

- L'adresse MAC de l'interface de gestion.
- L'option DHCP 60 (vendor-class-identifier) : définie sur « FPR9300 ».
- L'option DHCP 61 (dhcp-client-identifier) : définie sur le numéro de série du châssis. Ce numéro de série se trouve sur un onglet amovible sur le châssis.

Étape 2 Démarrez le châssis.

Étape 3 Entrez l'URL suivante dans votre navigateur :

https://*adresse_ip*/**api**

Précisez l'adresse IP attribuée par le serveur DHCP au port de gestion du châssis.

Étape 4 Lorsque vous y êtes invité, connectez-vous avec le nom d'utilisateur **install** et le mot de passe *numéro_de_série_du_châssis*.

Le *numéro_de_série_du_châssis* se trouve sur un onglet amovible sur le châssis.

Étape 5 Terminez la configuration du système en suivant les invites.

- Politique de mise en application de mots de passe robustes.
- Mot de passe du compte administrateur.
- Nom du système
- Adresse IPv4 et masque de sous-réseau, ou adresse et préfixe IPv6 de gestion du superviseur.
- Adresse IPv4 ou IPv6 de la passerelle par défaut.
- Hôte/adresse de réseau et masque de réseau/préfixe à partir duquel l'accès SSH est autorisé.
- Hôte/adresse réseau et masque réseau/préfixe à partir duquel l'accès HTTPS est autorisé.
- Adresse IPv4 ou IPv6 du serveur DNS.

- Nom de domaine par défaut

Étape 6 Cliquez sur **Submit** (soumettre).

Effectuez la configuration initiale du châssis dans l'interface de ligne de commande

La première fois que vous accédez à l'interface de ligne de commande FXOS au niveau de la console ou à l'aide d'une session SSH au port de gestion du châssis, un assistant de configuration vous invite à entrer la configuration du réseau de base afin que vous puissiez accéder à gestionnaire de châssis (en utilisant le protocole HTTPS) ou à l'interface de ligne de commande FXOS (en utilisant le protocole SSH) du port de gestion du châssis.

Le port de gestion de châssis obtient une adresse IP en utilisant DHCP. Si vous n'avez pas de serveur DHCP, vous devez utiliser le port de console pour la configuration initiale.

Remarque Pour relancer la configuration initiale, vous devez effacer toute configuration existante à l'aide des commandes suivantes :

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Avant de commencer

Recueillez les informations suivantes à utiliser avec le script de configuration :

- Nouveau mot de passe de l'administrateur
- Adresse IP de gestion et filtre d'adresse locale
- l'adresse IP de la passerelle
- Sous-réseaux à partir desquels vous souhaitez autoriser l'accès HTTPS et SSH
- Nom d'hôte et le nom de domaine
- l'adresse IP du serveur DNS

Procédure

Étape 1 Démarrez le châssis.

Étape 2 Connectez-vous au port de console série à l'aide d'un émulateur de terminal ou utilisez SSH pour le port de gestion du châssis.

Le Firepower 9300 comprend un câble de console de série RS-232 à RJ-45. Vous devrez peut-être utiliser un câble série tiers vers USB pour établir la connexion. Utilisez les paramètres de série suivants :

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

Étape 3 Lorsqu'on vous y invitera, connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **cisco123**.

Étape 4 Terminez la configuration du système en suivant les invites.

Exemple :

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

  DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y
```

```
    Default domain name : cisco.com

  Following configurations will be applied:

    Switch Fabric=A
    System Name=firepower-9300
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

Étape 5 Vous pouvez vous déconnecter du port de console, le cas échéant, ou mettre fin à votre session SSH.

Se connecter à Gestionnaire de châssis

Utilisez gestionnaire de châssis pour configurer les paramètres du châssis, y compris l'activation des interfaces et le déploiement de dispositifs logiques.

Avant de commencer

- Pour en savoir plus sur les navigateurs pris en charge, consultez les notes de mise à jour pour la version que vous utilisez (http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html).
- Vous ne pouvez accéder à gestionnaire de châssis qu'à partir d'un ordinateur de gestion avec une adresse IP dans la plage que vous avez spécifiée lors de la configuration initiale du châssis.

Procédure

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

https://*adresse_ip_de_gestion_du_châssis*

- *adresse_ip_de_gestion_du_châssis* : identifie l'adresse IP ou le nom d'hôte du port de gestion de châssis que vous avez saisi lors de la configuration initiale.

Étape 2 Saisissez le nom d'utilisateur **admin** et un nouveau mot de passe.

Vous pouvez ajouter d'autres utilisateurs ultérieurement en fonction de Ajouter des utilisateurs FXOS, à la page 22.

Étape 3 Cliquez sur **Ouvrir une session**.
Vous êtes connecté, et le gestionnaire de châssis s'ouvre pour afficher la page **Overview** (Survol).

Configurer NTP

Bien que vous puissiez définir l'heure manuellement, nous vous recommandons d'utiliser un serveur NTP. Vous devez régler la bonne heure pour la licence logicielle Smart pour l'ASA et pour Défense contre les menaces avec le gestionnaire d'appareil. Pour Défense contre les menaces avec le centre de gestion, l'heure doit correspondre entre le châssis et le centre de gestion. Dans ce cas, nous vous recommandons d'utiliser le même serveur NTP sur le châssis et sur le centre de gestion. N'utilisez pas le centre de gestion lui-même comme serveur NTP; cette méthode n'est pas prise en charge.

Avant de commencer

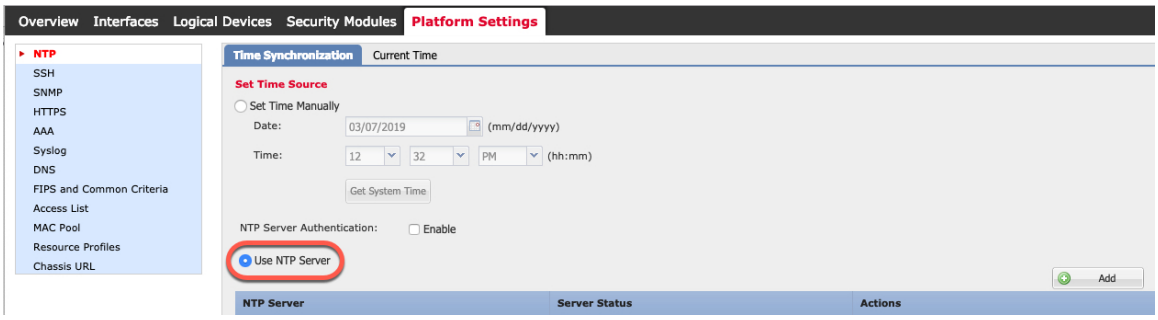
Si vous utilisez un nom d'hôte pour le serveur NTP, vous devez configurer un serveur DNS si vous ne l'avez pas déjà fait durant la configuration initiale. Consultez **Platform Settings (Configurations de plateforme)** > **DNS**.

Procédure

Étape 1 Choisissez **Platform Settings (Configurations de plateforme)** > **NTP**.

La page **Time Synchronization** (Synchronisation de l'heure) est sélectionnée par défaut.

Étape 2 Cliquez sur le bouton radio **Use NTP Server** (Utiliser le serveur NTP).

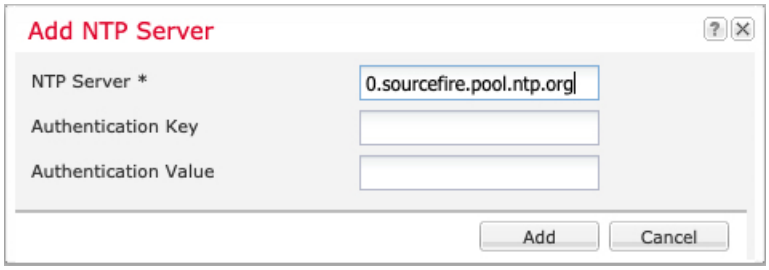


Étape 3 (Facultatif) Cochez la case **NTP Server Authentication: Enable** (Authentification du serveur NTP : activer) si vous devez authentifier le serveur NTP.

Vous serez invité à activer l'authentification NTP. Cliquez sur **Yes** (Oui) pour exiger un identifiant et une valeur de clé d'authentification pour toutes les entrées du serveur NTP.

Seul SHA1 est pris en charge pour l'authentification du serveur NTP.

Étape 4 Cliquez sur **Add** (Ajouter) et réglez les paramètres suivants :



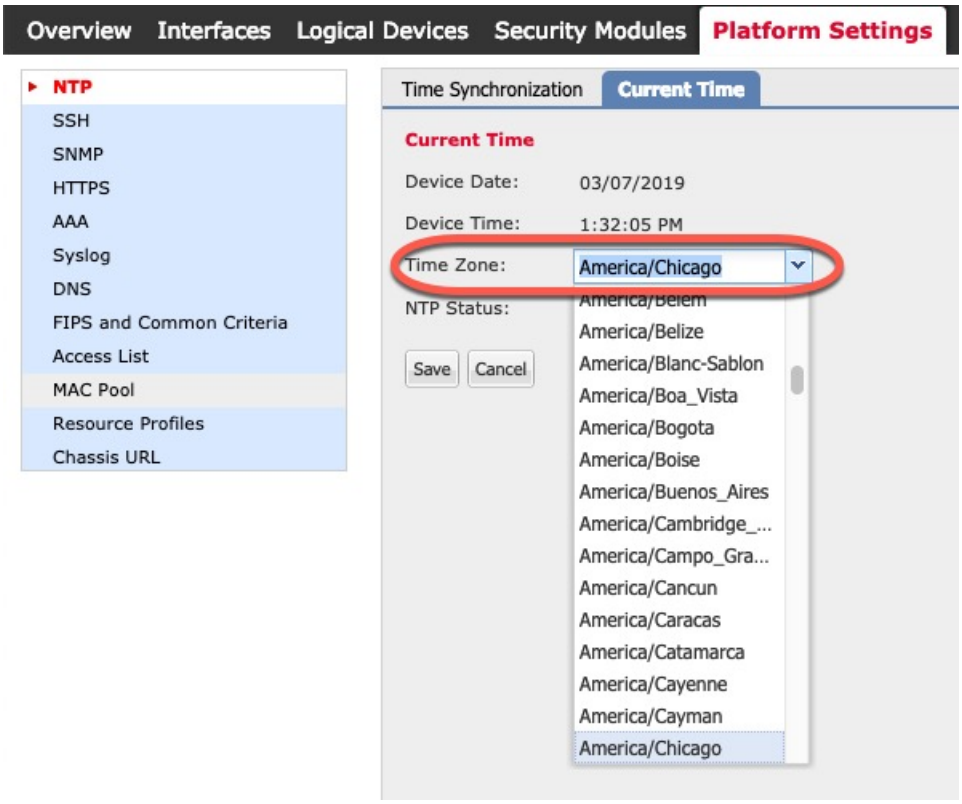
- **NTP Server** (Serveur NTP) : l'adresse IP ou le nom d'hôte du serveur NTP.
- **Authentication Key** et **Authentication Value**(clé et valeur d'authentification) : obtenez l'ID de clé et la valeur du serveur NTP. Par exemple, pour générer la clé SHA1 sur le serveur NTP version 4.2.8p8 ou ultérieure avec OpenSSL installé, saisissez la commande **ntp-keygen -M** , puis affichez l'ID de clé et la valeur dans le fichier ntp.keys. La clé est utilisée pour indiquer au client et au serveur quelle valeur utiliser lors du calcul du condensé du message.

Étape 5 Cliquez sur **Add** (Ajouter) pour ajouter le serveur distant.

Vous pouvez ajouter jusqu'à 4 serveurs NTP.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer les serveurs.

Étape 7 Cliquez sur **Current Time** (Heure actuelle) et dans la liste déroulante **Time Zone** (Fuseau horaire), choisissez le fuseau horaire approprié pour le châssis.



Étape 8 Cliquez sur **Save** (enregistrer).

Remarque
Si vous modifiez l'horloge système de plus de 10 minutes, le système vous déconnectera et vous devrez vous reconnecter au gestionnaire de châssis.

Ajouter des utilisateurs FXOS

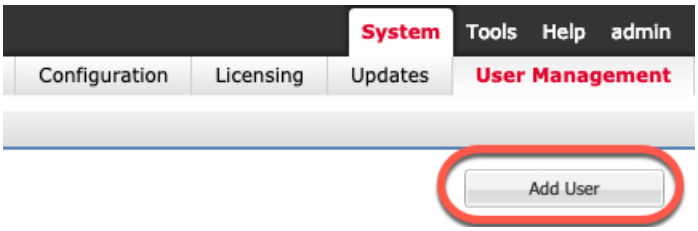
Ajoutez des utilisateurs locaux pour les connexions à gestionnaire de châssis et à l'interface de ligne de commande FXOS.

Procédure

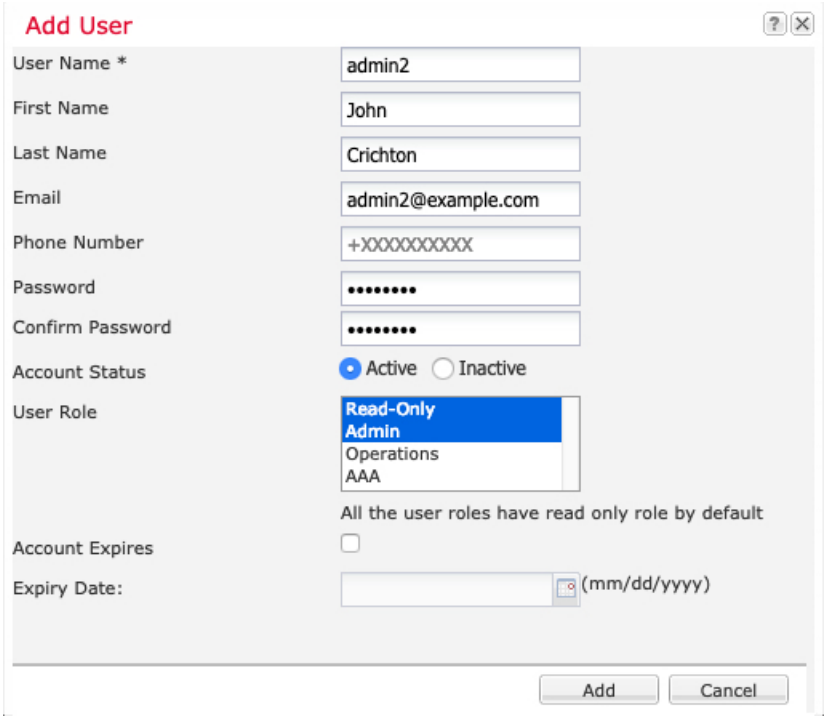
Étape 1 Choisissez **System (Système)** > **User Management (Gestion des utilisateurs)**.

Étape 2 Cliquez sur **Local Users** (Utilisateurs locaux).

Étape 3 Cliquez sur **Add User** (Ajouter un utilisateur) pour ouvrir la boîte de dialogue **Add User** (Ajouter un utilisateur).



Étape 4 Remplir les champs suivants avec les renseignements requis sur l'utilisateur :



- **User Name** (Nom d'utilisateur) : définit le nom d'utilisateur, jusqu'à 32 caractères. Après avoir enregistré l'utilisateur, l'identifiant de connexion ne peut pas être modifié. Vous devez supprimer le compte d'utilisateur et en créer un nouveau.
- (Facultatif) **First Name** (Prénom) : définit le prénom de l'utilisateur, jusqu'à 32 caractères.
- (Facultatif) **Last Name** (Nom de famille) : définit le nom de famille de l'utilisateur, jusqu'à 32 caractères.
- (Facultatif) **Email** (Adresse courriel) : définit l'adresse courriel de l'utilisateur.
- (Facultatif) **Phone Number** (Numéro de téléphone) : définit le numéro de téléphone de l'utilisateur.
- **Password** (Mot de passe) et **Confirm Password** (Confirmer le mot de passe) : définissent le mot de passe associé à ce compte. Si vous activez la vérification de la robustesse du mot de passe, le mot de passe doit être robuste. FXOS rejettera tout mot de passe qui ne répond pas aux exigences de vérification de la robustesse. Consultez le FXOS configuration guide (Guide de configuration FXOS) pour connaître les directives concernant les mots de passe sécurisés.
- **Account Status** (État du compte) : définit l'état sur **Active** (Actif) ou **Inactive** (Inactif).
- **User Role** (Rôle d'utilisateur) : définit le rôle qui représente les privilèges que vous souhaitez attribuer au compte d'utilisateur. Tous les utilisateurs se voient attribuer le rôle **Read-Only** (En lecture seule) par

défaut. Ce rôle ne peut pas être désélectionné. Pour attribuer un autre rôle, cliquez sur le nom du rôle dans la fenêtre pour qu'il soit en surbrillance. Vous pouvez utiliser l'un des rôles d'utilisateur suivants :

- **Admin** (Administrateur) : accès complet en lecture et écriture à l'ensemble du système.
- **Read-Only** (En lecture seule) : accès en lecture seule à la configuration système sans privilège de modification de l'état du système.
- **Operations** (Opérations) : accès en lecture et écriture à la configuration NTP, à la configuration de Smart Call Home pour les licences Smart et aux journaux du système, y compris aux serveurs de journalisation du système et aux défaillances. Accès en lecture au reste du système.
- **AAA Administrator** (Administrateur AAA) : accès en lecture et écriture aux utilisateurs, aux rôles et à la configuration AAA. Accès en lecture au reste du système.

- (Facultatif) **Account Expires** (Expiration du compte) : définit que ce compte expire. Le compte ne peut pas être utilisé après la date indiquée dans le champ **Expiry Date** (Date d'expiration). Après avoir configuré un compte d'utilisateur avec une date d'expiration, vous ne pouvez pas reconfigurer le compte pour qu'il n'expire pas. Vous pouvez toutefois configurer le compte avec la dernière date d'expiration disponible. Par défaut, les comptes d'utilisateur n'expirent pas.
- (Facultatif) **Expiry Date** (Date d'expiration) : date à laquelle le compte expire. La date doit être au format *aaaa-mm-jj*. Cliquez sur l'icône du calendrier à la fin de ce champ pour afficher un calendrier que vous pouvez utiliser pour sélectionner la date d'expiration.

Étape 5 Cliquez sur **Add** (Ajouter).

Interfaces de configuration

Par défaut, les interfaces physiques sont désactivées. Dans FXOS, vous pouvez activer les interfaces, ajouter des canaux EtherChannels, ajouter des sous-interfaces VLAN et modifier les propriétés de l'interface. Pour utiliser une interface, vous devez l'activer physiquement dans FXOS, puis l'activer logiquement dans l'application.

Pour configurer les ports de répartition, consultez le guide de configuration FXOS.

Types d'interface

Chaque interface est de l'un des types suivants :

- Data (Données) : à utiliser pour les données normales. Les interfaces de données ne peuvent pas être mises en commun entre les dispositifs logiques, et les dispositifs logiques ne peuvent pas communiquer avec d'autres dispositifs logiques par le fond de panier Pour le trafic sur les interfaces de données, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre dispositif logique.
- Data-sharing (Partage de données) : à utiliser pour les données normales. Pris en charge uniquement avec les instances de conteneur, ces interfaces de données peuvent être partagées par un ou plusieurs dispositifs logiques/Instances de conteneur (Défense contre les menaces-utilisant-centre de gestion seulement). Chaque instance de conteneur peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances

de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives, les grappes, ou les liens de basculement.

- Mgmt (Gestion) : permet de gérer les instances d'application. Ces interfaces peuvent être partagées par un ou plusieurs dispositifs logiques pour accéder à des hôtes externes; les dispositifs logiques ne peuvent pas communiquer sur cette interface avec d'autres dispositifs logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par dispositif logique. En fonction de votre application et de votre gestionnaire, vous pouvez ultérieurement activer la gestion à partir d'une interface de données; mais vous devez attribuer une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données.

Remarque La modification de l'interface de gestion entraînera le redémarrage du dispositif logique. Par exemple, une gestion des modifications de e1/1 à e1/2 entraînera le redémarrage du dispositif logique pour appliquer la nouvelle gestion.

- Eventing (Création d'événements) : sert d'interface de gestion secondaire pour les dispositifs Défense contre les menaces qui utilisent le centre de gestion. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres au niveau de l'interface de ligne de commande Défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Reportez-vous au guide de configuration du centre de gestion pour obtenir plus de renseignements. Les interfaces d'événements peuvent être partagées par un ou plusieurs dispositifs logiques pour accéder à des hôtes externes. Les dispositifs logiques ne peuvent pas communiquer sur cette interface avec d'autres dispositifs logiques qui partagent l'interface. Si vous configurez ultérieurement une interface de données pour la gestion, vous ne pouvez pas utiliser une interface d'événement distincte.

Remarque Une interface Ethernet virtuelle est attribuée lors de l'installation de chaque instance applicative. Si l'application n'utilise pas d'interface événementielle, l'interface virtuelle sera dans un état "admin down".

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster (grappe) : à utiliser comme liaison de commande de grappe pour un dispositif logique en grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Le type de grappe est uniquement pris en charge sur les interfaces EtherChannel. Pour la mise en grappe multi-instances, vous ne pouvez pas partager une interface de type grappe sur plusieurs appareils. Vous pouvez ajouter des sous-interfaces VLAN à la grappe EtherChannel pour fournir des liaisons de commande de grappe distinctes par grappe. Si vous ajoutez des sous-interfaces à une interface Cluster, vous ne pouvez pas utiliser cette interface pour une grappe native. Le gestionnaire d'appareil et CDO ne prend pas en charge le regroupement (clustering).

Vous devez configurer une interface de gestion et au moins une interface de données (ou de partage de données) avant de déployer un dispositif logique.

Configurer une interface physique

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, vous devez l'activer physiquement dans FXOS, puis l'activer logiquement dans l'application.

Avant de commencer

Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant d'ajouter une interface au canal EtherChannel.

Procédure

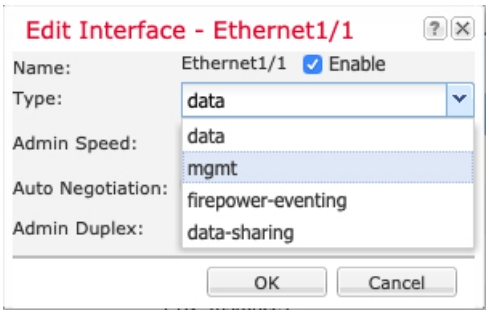
Étape 1 Cliquez sur **Interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Modifier** (✎) dans la ligne de l'interface à modifier pour ouvrir la boîte de dialogue **Edit Interface** (Modifier l'interface).

Étape 3 Cochez la case **Enable** (activer).

Étape 4 Choisissez le **Type** d'interface : **Data** (Données), **Data-sharing** (Partage de données), **Mgmt** (Gestion) ou **Firepower-eventing** (événement Firepower)



Remarque
Il y a des limites lors de l'utilisation d'interfaces de type partage de données; consultez le FXOS configuration guide (Guide de configuration de FXOS) pour de plus amples renseignements.

Pour Firepower-eventing, consultez le Guide de configuration de Firepower Management Center.

Étape 5 (Facultatif) Choisissez la **Speed** (Vitesse) de l'interface.

Étape 6 (Facultatif) Si votre interface prend en charge la négociation automatique (**Auto Negotiation**), cliquez sur le bouton radio **Yes** (oui) ou **No** (non).

Étape 7 (Facultatif) Choisissez le **Duplex** de l'interface.

Étape 8 Cliquez sur **OK**.

Ajouter un canal EtherChannel (canal de port)

Un EtherChannel (également appelé canal de port) peut inclure jusqu'à 16 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

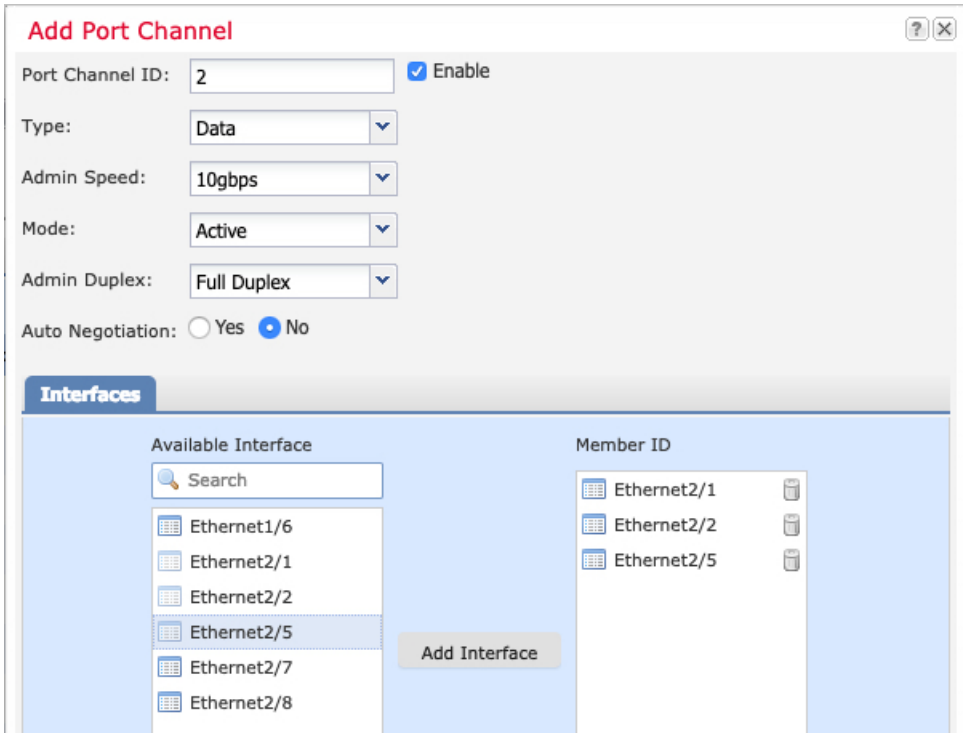
Remarque Lorsque le châssis crée un EtherChannel, l'EtherChannel reste dans un état **Suspended** (En attente) pour le mode LACP actif ou à l'arrêt pour le mode LACP activé jusqu'à ce que vous l'**affectiez** à un dispositif logique, même si la liaison physique est opérationnelle.

Procédure

Étape 1 Cliquez sur **Interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add New (Ajouter)** > **Port Channel (Canal de port)**.



Étape 3 Saisissez un **Port Channel ID** (Identifiant de canal de port), compris entre 1 et 47.

Étape 4 Cochez la case **Enable** (activer).

Étape 5 Choisissez le **Type** d'interface :

- **Data** (Données)
- **Data-sharing (Partage de données)** : pour les instances de conteneur uniquement.
- **Mgmt** (gestion)
- **Firepower-eventing** (création-d-événement-Firepower) : pour défense contre les menaces seulement.
- **Cluster** (Grappe) : pour la mise en grappe seulement.

Remarque
Il y a des limites lors de l'utilisation d'interfaces de type partage de données; consultez le FXOS configuration guide (Guide de configuration de FXOS) pour de plus amples renseignements.

Pour Firepower-eventing, consultez le Guide de configuration de Firepower Management Center.

Étape 6 Définissez l'**Admin Speed** (Vitesse d'administration) des interfaces membres dans la liste déroulante.

Étape 7 Pour les interfaces de données ou de partage de données, choisissez le **mode** du canal de port LACP : **Active** (Actif) ou **On** (Activé).

Pour les interfaces sans données ou qui ne partagent pas de données, le mode est toujours actif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.

Étape 8 Définissez **Admin Duplex** (Duplex d'administration) dans la liste déroulante.

Étape 9 Pour ajouter une interface au canal de port, sélectionnez l'interface dans la liste **Available Interface** (Interface disponible) et cliquez sur **Add Interface** (Ajouter une interface) pour la déplacer vers la liste **Member ID** (Identification de membre).

Vous pouvez ajouter jusqu'à 16 interfaces.

Astuces
Vous pouvez ajouter plusieurs interfaces en même temps. Cliquez sur les interfaces souhaitées tout en maintenant la touche **Ctrl** enfoncée. Pour sélectionner une plage d'interfaces, sélectionnez la première interface de la plage, puis, tout en maintenant la touche **Shift** (Maj) enfoncée, cliquez pour sélectionner la dernière interface de la plage.

Étape 10 Pour supprimer une interface du canal de port, cliquez sur **Supprimer** ( ) à droite de l'interface dans la liste **Member ID** (Identifiant de membre).

Étape 11 Cliquez sur **OK**.

Ajouter une sous-interface VLAN pour les instances de conteneur

Vous pouvez ajouter jusqu'à 500 sous-interfaces à votre châssis. Les sous-interfaces ne sont prises en charge que pour les instances de contenant; pour en savoir plus, consultez Instances d'application du dispositif logique : instance de conteneur ou instance native, à la page 7.

Pour la mise en grappe à instances multiples, vous ne pouvez ajouter des sous-interfaces qu'à l'interface de type grappe; les sous-interfaces des interfaces de données ne sont pas prises en charge.

Les ID de VLAN par interface doivent être uniques et, dans une instance de conteneur, les ID de VLAN doivent être uniques pour toutes les interfaces attribuées. Vous pouvez réutiliser les ID de VLAN sur des

interfaces *distinctes*, à condition qu'ils soient affectés à différentes instances de conteneur. Cependant, chaque sous-interface compte toujours dans la limite, même si elle utilise le même ID.

Vous pouvez également ajouter des sous-interfaces dans l'application. Pour plus d'informations sur le moment d'utiliser des sous-interfaces FXOS par rapport aux sous-interfaces d'application, consultez le FXOS configuration guide (Guide de configuration FXOS).

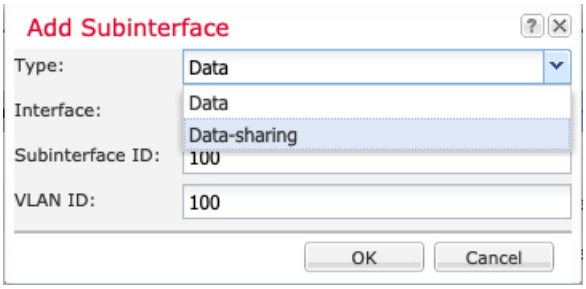
Procédure

Étape 1 Cliquez sur **Interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add New** > **Subinterface** (Ajouter une nouvelle sous-interface) pour ouvrir la boîte de dialogue Add **Subinterface (ajouter** une sous-interface).

Étape 3 Choisissez le **Type** d'interface :



- **Data** (Données)
- **Data-sharing** (Partage de données)
- **Grappe** : si vous ajoutez des sous-interfaces à une interface de grappe, vous ne pouvez pas utiliser cette interface pour une grappe native.

Pour les données et les interfaces de partage de données : le type est indépendant du type d'interface parent; vous pouvez avoir un parent de partage de données et une sous-interface de données, par exemple.

Il y a des limites lors de l'utilisation d'interfaces de type partage de données; consultez le FXOS configuration guide (Guide de configuration de FXOS) pour de plus amples renseignements.

Étape 4 Choisissez **l'interface** parente dans la liste déroulante.

Vous ne pouvez pas ajouter une sous-interface à une interface physique qui est actuellement allouée à une unité logique. Si d'autres sous-interfaces du parent sont allouées, vous pouvez ajouter une nouvelle sous-interface tant que l'interface parente elle-même n'est pas allouée.

Étape 5 Entrez **l'ID de la sous-interface** comme un nombre entier entre 1 et 4294967295.

Cet ID sera ajouté à l'ID de l'interface parente sous le nom *identifiant_d_interface.identifiant_de_sous_interface*. Par exemple, si vous ajoutez une sous-interface à Ethernet1/1 avec l'ID 100, l'ID de la sous-interface sera : Ethernet1/1.100. Cet ID est différent de l'ID VLAN, bien que vous puissiez définir ces ID pour des raisons de commodité.

Étape 6 Définissez l'**ID VLAN** entre 1 et 4095.

Étape 7 Cliquez sur **OK**.

Développez l'interface parente pour afficher toutes les sous-interfaces qu'elle contient.

Téléverser des images logicielles dans le châssis

Cette procédure décrit comment charger de nouvelles images FXOS et d'application, et comment mettre à niveau l'image FXOS. Vous devrez peut-être charger de nouvelles images si les images préinstallées ne sont pas les versions dont vous avez besoin.

Avant de commencer

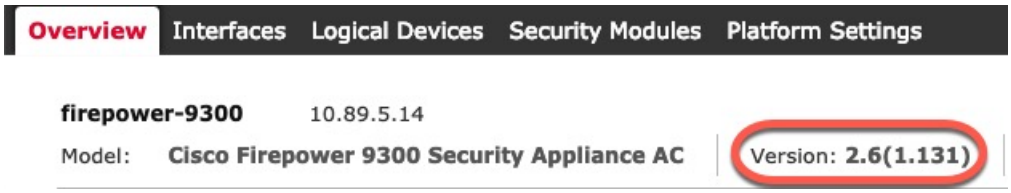
- Vérifiez la compatibilité entre FXOS, l'ASA et les versions Défense contre les menaces dans le FXOS compatibility guide (Guide de compatibilité FXOS).
- Assurez-vous que l'image que vous souhaitez télécharger est disponible sur votre ordinateur local. Pour obtenir FXOS et les logiciels d'application pour Firepower 9300, consultez :

  http://www.cisco.com/go/firepower9300-software
- Pour vous assurer la réussite de votre chargement pendant votre session HTTPS, vous devrez peut-être modifier le délai d'expiration absolu au niveau de l'interface de ligne de commande de FXOS. Le délai d'expiration absolu est de 60 minutes (le maximum), et les téléversements volumineux peuvent prendre plus de 60 minutes. Pour désactiver le délai d'expiration absolu, saisissez :

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set absolute-session-timeout 0
Firepower-chassis /security/default-auth* # commit-buffer
```

Procédure

Étape 1 Vérifiez votre version FXOS actuelle en consultant la page **Overview** (Survol).



Vous pourrez afficher les images des applications actuellement disponibles sur le châssis à l'étape suivante.

Étape 2 Sélectionnez **System** > **Updates**.

La page **Available Updates** (Mises à jour disponibles) affiche une liste des images de l'ensemble de la plateforme FXOS et des applications.

Étape 3 Cliquez sur **Upload Image**(Charger une image) pour ouvrir la boîte de dialogue **Upload Image** (Charger une image).

Étape 4 Cliquez sur **Browse** (Naviguer) pour accéder à l'image à charger et la sélectionner.

Étape 5 Cliquez sur **Upload** (charger). L'image sélectionnée est téléversée sur le châssis.

La boîte de dialogue **Upload Image** (Téléverser une image) affiche une barre de progression, puis une boîte de dialogue **Success** (Réussite) à la fin du chargement de l'image.

Étape 6 Pour mettre à niveau l'image FXOS :

a) Cliquez sur le Icône mise à niveau ( ) de l'offre groupée de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

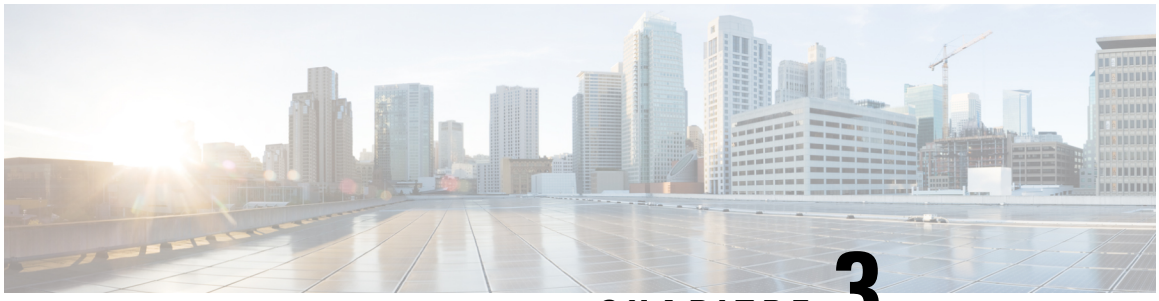
b) Cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez poursuivre l'installation.

Le châssis se recharge. Le processus de mise à niveau prend généralement entre 20 et 30 minutes.

Historique de FXOS

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Sous-interfaces VLAN à utiliser avec des instances de conteneur	2.4.1	Pour fournir une utilisation flexible de l'interface physique, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces entre plusieurs instances. **Remarque** Nécessite la version 6.3 ou une version ultérieure de défense contre les menaces. Écrans Nouveaux ou modifiés : Menu déroulant **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Add New (Ajouter) > Subinterface (Sous-interface)** Écrans Nouveaux ou modifiés de centre de gestion : **Devices (Dispositifs)** > **Device Management (Gestion des dispositifs)** > **icône Edit (Modifier) > Interfaces**
Interfaces de partage de données pour les instances de conteneurs	2.4.1	Pour fournir une utilisation de l'interface physique flexible, vous pouvez partager des interfaces entre plusieurs instances. **Remarque** Nécessite la version 6.3 ou une version ultérieure de défense contre les menaces. Écrans Nouveaux ou modifiés : **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Type**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge des données EtherChannels en mode activé	2.4.1	Vous pouvez maintenant définir les données et les EtherChannels de partage de données en mode LACP actif ou en mode Activé. Les autres types d'EtherChannels ne prennent en charge que le mode actif. Écrans Nouveaux ou modifiés : **Interfaces** > **All Interfaces(Toutes les interfaces)** > **Edit Port Channel (Modifier le canal de port)** > **Mode**
Prise en charge des EtherChannels dans les ensembles en ligne défense contre les menaces	2.1.1	Vous pouvez désormais utiliser les EtherChannels dans l'ensemble en ligne défense contre les menaces.
Prise en charge de la propagation de l'état de la liaison défini en ligne pour défense contre les menaces	2.0.1	Lorsque vous configurez un ensemble en ligne dans l'application défense contre les menaces et activez la propagation de l'état de la liaison, défense contre les menaces envoie l'appartenance à l'ensemble en ligne au châssis FXOS. La propagation de l'état de la liaison signifie que le châssis met automatiquement hors service la deuxième interface de la paire d'interfaces en ligne lorsque l'une des interfaces d'un ensemble en ligne tombe en panne. Commandes FXOS nouvelles ou modifiées : **show fall |grep link-down**, **show interface detail**
Prise en charge des modules de réseau de contournement du matériel pour défense contre les menaces	2.0.1	Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Écrans Nouveaux ou modifiés de centre de gestion : **Devices (Dispositifs)** > **Device Management (Gestion des dispositifs)** > **Interfaces** > **Edit Physical Interface (Modifier les interfaces physiques)**
Interface de type Firepower-eventing pour défense contre les menaces	1.1.4	Vous pouvez spécifier une interface comme événement Firepower-Eventing à utiliser avec défense contre les menaces. Cette interface est une interface de gestion secondaire pour les dispositifs défense contre les menaces. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez la section « Management Interfaces » (Interfaces de gestion) dans le chapitre *System Configuration* (Configuration système) du guide de configuration centre de gestion. Écrans Nouveaux ou modifiés de gestionnaire de châssis : **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Type**



CHAPITRE 3

Défense contre les menaces Déploiement avec le Centre de gestion

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

Ce chapitre décrit comment déployer un dispositif logique autonome Défense contre les menaces avec le centre de gestion. Pour déployer une paire de haute disponibilité ou un cluster, consultez la section Guide de configuration de Firepower Management Center.

Dans un déploiement type sur un grand réseau, vous installez plusieurs dispositifs gérés sur des segments de réseau. Chaque dispositif contrôle, inspecte, surveille et analyse le trafic, puis signale à un gestionnaire le centre de gestion. centre de gestion fournit une console de gestion centralisée avec une interface Web que vous pouvez utiliser pour effectuer des tâches d'administration, de gestion, d'analyse et de création de rapports en cours de services pour sécuriser votre réseau local.

Pour les réseaux qui ne comprennent qu'un seul appareil ou quelques-uns, où vous n'avez pas besoin d'utiliser un gestionnaire d'appareils multiples très puissant comme le centre de gestion, vous pouvez utiliser le gestionnaire intégré gestionnaire d'appareil. Utilisez l'assistant de configuration de dispositif Web gestionnaire d'appareil pour configurer les fonctionnalités de base du logiciel qui sont le plus souvent utilisées pour les déploiements sur de petits réseaux.

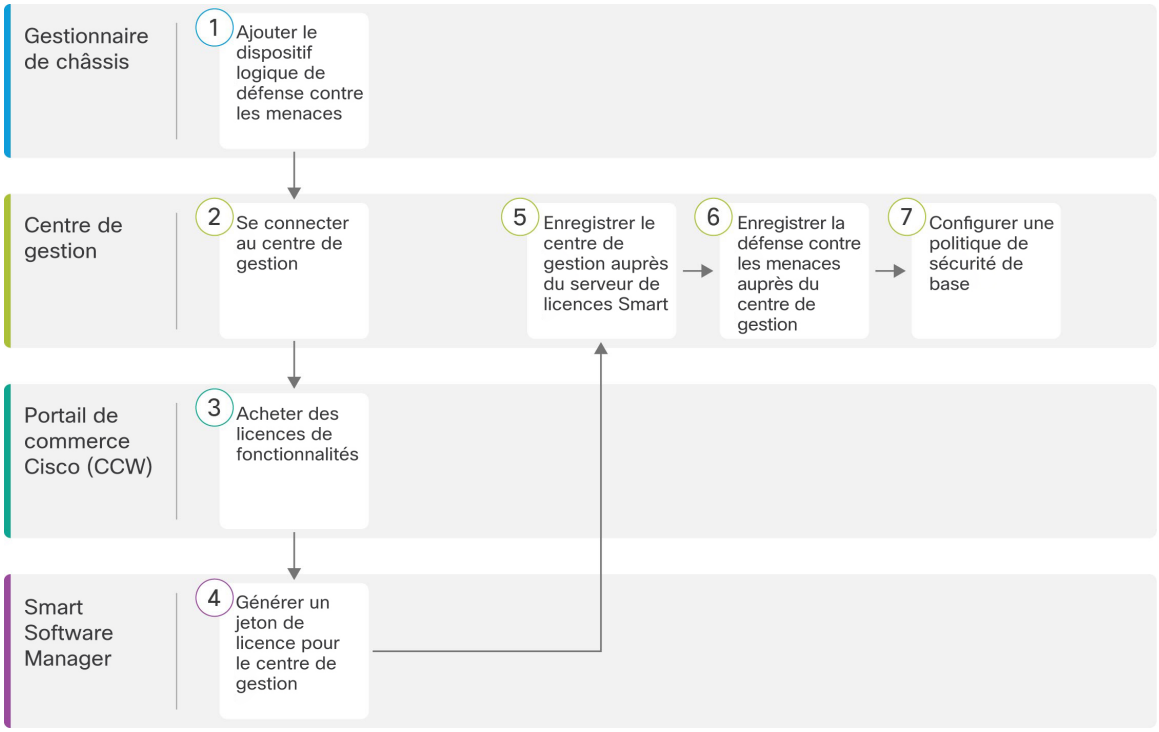
Déclaration de confidentialité : Firepower 9300 n'exige ni ne recueille de renseignements permettant d'établir l'identité de quelqu'un. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, pour créer les noms d'utilisateur. Si c'est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu'il travaille à la configuration ou qu'il utilise SNMP.

Avant de commencer

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

Procédure de bout en bout

Consultez les tâches suivantes pour déployer et configurer Défense contre les menaces sur votre châssis.



	Espace de travail	Étapes
1	Gestionnaire de châssis	Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 35.
2	Centre de gestion	Se connecter à Centre de gestion, à la page 41.
3	Portail de commerce Cisco (CCW)	Obtenir des licences pour le Centre de gestion, à la page 41 : Achetez des licences de fonctionnalités.
4	Smart Software Manager	Obtenir des licences pour le Centre de gestion, à la page 41 : Générer un jeton de licence pour centre de gestion.
5	Centre de gestion	Obtenir des licences pour le Centre de gestion, à la page 41 Enregistrez centre de gestion auprès du serveur de licences Smart.

	Espace de travail	Étapes
6	Centre de gestion	Enregistrer Défense contre les menaces avec le Centre de gestion, à la page 43.
7	Centre de gestion	Configurer une politique de sécurité de base, à la page 46.

Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces

Vous pouvez déployer le dispositif de défense contre les menaces à partir du Firepower 9300 en tant qu'instance native ou conteneur. Vous pouvez déployer plusieurs instances de conteneur par security module, mais une seule instance native. Consultez Instances d'application du dispositif logique : instance de conteneur ou instance native, à la page 7 pour connaître le nombre maximal d'instances de conteneur par modèle. Vous pouvez utiliser une instance native sur certains modules et des instances de conteneur sur les autres modules.

Pour ajouter une paire de haute disponibilité ou une grappe, consultez la rubrique Guide de configuration de Firepower Management Center.

Cette procédure vous permet de configurer les caractéristiques logiques du dispositif, y compris la configuration de démarrage utilisée par l'application.

Avant de commencer

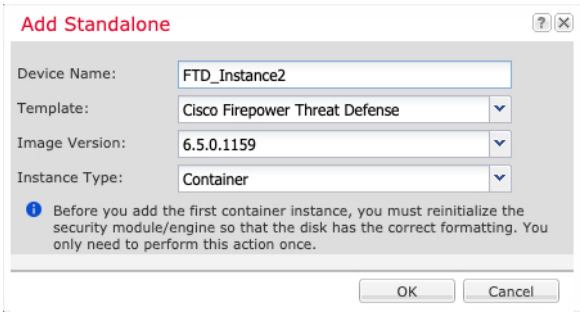
- Configurer l'interface de gestion à utiliser avec défense contre les menaces; voir Interfaces de configuration, à la page 24. L'interface de gestion est requise. Dans les versions 6.7 ou ultérieures, vous pouvez activer ultérieurement la gestion à partir d'une interface de données; mais vous devez affecter une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données. Il convient de souligner que cette interface de gestion est différente du port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**).
- Vous devez également configurer au moins une interface de données.
- Pour les instances de conteneur, si vous ne souhaitez pas utiliser le profil par défaut, qui utilise le minimum de ressources, ajoutez un profil de ressource sur **Platform Settings (paramètres de plateforme)** > **Resource Profiles (profils de ressources)**.
- Pour les instances de conteneur, avant de pouvoir installer une instance de conteneur pour la première fois, vous devrez peut-être réinitialiser security module pour que le formatage du disque soit correct. Si cette action est requise, vous ne pourrez pas enregistrer votre dispositif logique. Cliquez sur **Security Modules**, puis sur Icône réinitialiser ( ).
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce dispositif
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - Centre de gestion l'adresse IP et/ou l'ID NAT de votre choix

- l'adresse IP du serveur DNS

Procédure

Étape 1 Dans gestionnaire de châssis, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur **Add** > **Standalone**, puis définissez les paramètres suivants :



a) Indiquez un nom de dispositif (**Device Name**).

Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de dispositif utilisé dans la configuration de l'application.

Remarque
Vous ne pouvez pas modifier ce nom après avoir ajouté le dispositif logique.

b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.

c) Choisissez la version de l'image (**Image Version**).

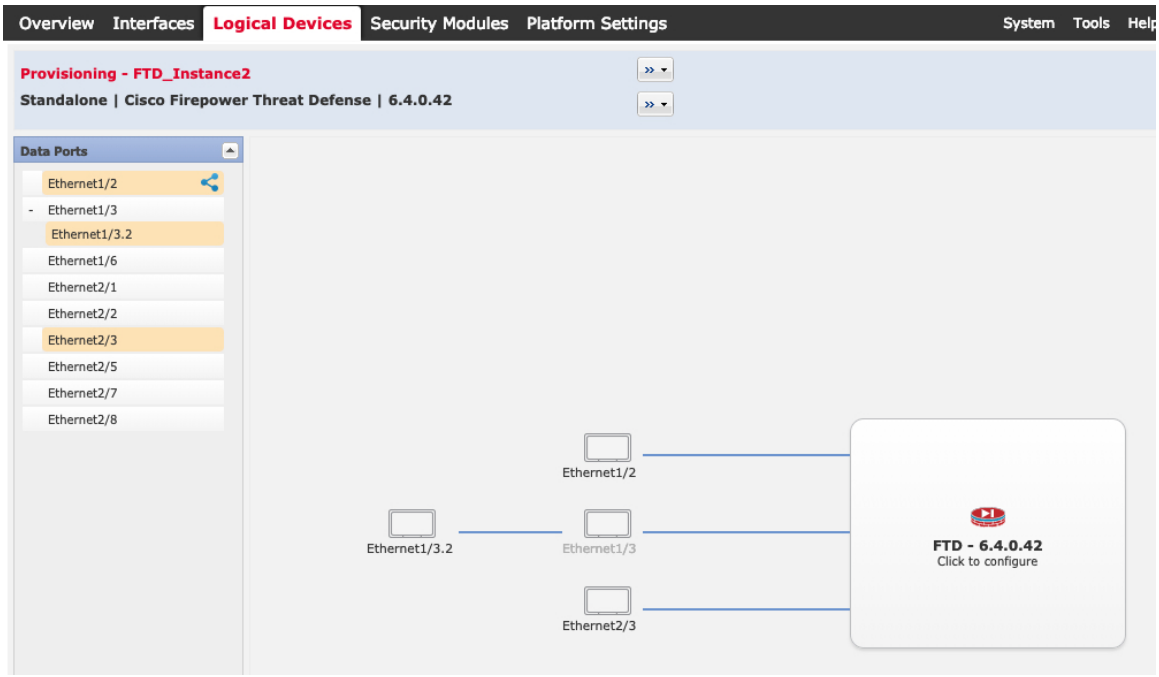
d) Choisissez le type d'instance (**Instance Type**): instance de conteneur (**Container**) ou instance native (**Native**).

Une instance native utilise toutes les ressources (CPU, RAM et espace disque) de security module/engine. Vous ne pouvez donc installer qu'une seule instance native. Une instance de conteneur utilise un sous-ensemble de ressources de security module/engine. Vous pouvez donc installer plusieurs instances de conteneur.

e) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du dispositif).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au dispositif.



Vous pouvez uniquement affecter des données et des interfaces de partage de données que vous avez précédemment activées dans la page **Interfaces**. Vous activerez et configurerez plus tard ces interfaces dans le centre de gestion, y compris la définition des adresses IP.

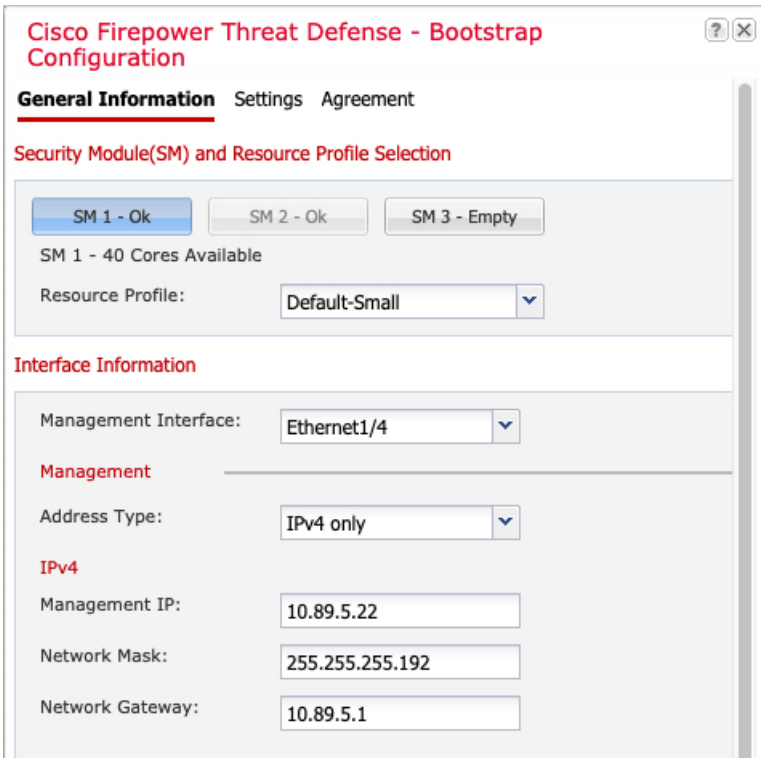
Vous pouvez affecter au maximum 10 interfaces de partage de données à une instance de conteneur. En outre, chaque interface de partage de données peut être affectée à tout au plus 14 instances de conteneur. Une interface de partage de données est indiquée par icône partage ( ).

Hardware Bypass : Les ports compatibles sont représentés par l'icône suivante : . Pour certains modules d'interface, vous pouvez activer la fonction de contournement matériel pour les interfaces en ensemble en ligne uniquement (voir le Guide de configuration de Firepower Management Center pour obtenir plus de renseignements sur les ensembles en ligne). Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Si vous n'affectez pas les deux interfaces dans une paire de Hardware Bypass, un message d'avertissement s'affiche pour vous assurer que votre affectation est intentionnelle. Vous n'avez pas besoin d'utiliser la fonctionnalité Hardware Bypass, vous pouvez donc affecter des interfaces uniques si vous préférez.

Étape 4 Cliquez sur l'icône de dispositif au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce dispositif logique.

b) Pour une instance de conteneur, spécifiez le profil des ressources (**Resource Profile**).

   Si vous affectez ultérieurement un profil de ressource différent, l'instance sera rechargée, ce qui peut prendre environ 5 minutes. Remarque : En ce qui concerne les grappes ou les paires à haute disponibilité établies, si vous affectez un profil de ressource de taille différente, faites le nécessaire pour que tous les membres aient la même taille dès que possible.

c) Choisissez l'interface de gestion (**Management Interface**).

   Cette interface est utilisée pour gérer le dispositif logique. Cette interface est distincte du port de gestion du châssis.

d) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).

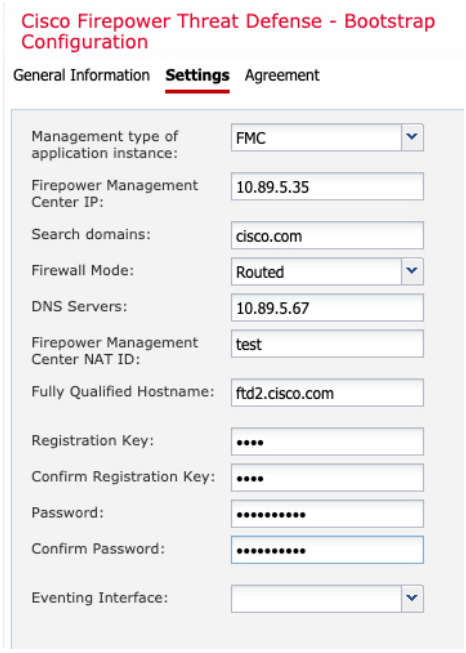
e) Configurez l'adresse IP de gestion (**Management IP**).

   Définissez une adresse IP unique pour cette interface.

f) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).

g) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Sous l'onglet **Settings** (paramètres), procédez comme suit :



a) Pour une instance native, dans la liste déroulante **Management type of application instance** (type de gestion de l'instance d'application), choisissez **FMC**.

   Les instances natives prennent également en charge le gestionnaire d'appareilcomme gestionnaire. Après avoir déployé le dispositif logique, vous ne pouvez pas modifier le type de gestionnaire.

b) Entrez **l'adresse IP du Cisco Firepower Management Center** ou le nom d'hôte du gestionnaire de centre de gestion. Si vous ne connaissez pas l'adresse IP de centre de gestion, laissez ce champ vide et saisissez une phrase d'accès dans le champ **Firepower Management Center NAT ID**.

c) Pour une instance de conteneur, à la question sur l'autorisation du mode expert à partir de sessions SSD FTD (**Permit Expert mode from FTD SSH sessions**): répondez oui (**Yes**) ou non (**No**). Le mode expert fournit l'accès à shell défense contre les menaces pour un dépannage avancé.

   Si vous choisissez **Yes (oui)** pour cette option, les utilisateurs qui accèdent à l'instance de conteneur directement à partir d'une séance SSH peuvent passer en mode expert. Si vous choisissez **No** (non), seuls les utilisateurs qui accèdent à l'instance de conteneur à partir de l'interface de ligne de commande de FXOS peuvent passer en mode expert. Nous vous recommandons de choisir **No** (non) pour augmenter l'isolement entre les instances.

   Utilisez le mode expert uniquement si une procédure documentée vous indique que c'est nécessaire ou si le Centre d'assistance technique (TAC) de Cisco vous demande de l'utiliser. Pour entrer dans ce mode, utilisez la commande **expert** dans l'interface de ligne de commande de défense contre les menaces.

d) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.

e) Choisissez le mode du pare-feu (**Firewall Mode**) : **Transparent** ou **Routed** (routage).

   En mode routage, l'défense contre les menaces est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

f) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont séparés par des virgules.

Par exemple, défense contre les menaces utilise DNS si vous spécifiez un nom d'hôte pour centre de gestion.

g) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour défense contre les menaces.

h) Saisissez une clé d'enregistrement (**Registration Key**) à partager entre centre de gestion et l'appareil lors de l'enregistrement.

Vous pouvez choisir n'importe quelle chaîne de texte pour cette clé entre 1 et 37 caractères; vous entrez la même clé sur centre de gestion lorsque vous ajoutez défense contre les menaces.

i) Saisissez un mot de passe (**Password**) pour l'utilisateur admin défense contre les menaces pour l'accès à l'interface de ligne de commande.

j) Choisissez **l'interface d'événements** sur laquelle les événements doivent être envoyés. Si aucune interface d'événement n'est pas spécifiée, l'interface de gestion sera utilisée.

Cette interface doit être définie comme une interface pour événements Firepower.

k) Pour une instance de conteneur, définissez **Hardware Crypto** sur activé (**Enabled**) ou désactivé (**Disabled**).

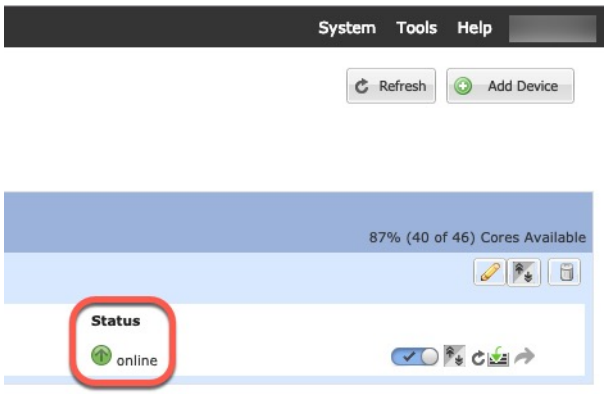
Ce paramètre active l'accélération cryptographique TLS dans le matériel et améliore les performances pour certains types de trafic. Pour obtenir plus d'informations, reportez-vous à la Guide de configuration de Firepower Management Center. Cette fonctionnalité n'est pas prise en charge pour les instances natives. Pour afficher le pourcentage de ressources matérielles de chiffrement allouées à cette instance, entrez la commande **show hw-crypto**.

Étape 7 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.

Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (enregistrer).

Le châssis déploie le dispositif logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau dispositif logique dans la page **Logical Devices**. Lorsque le dispositif logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Se connecter à Centre de gestion

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

Avant de commencer

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

Procédure

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

https://*adresse_ip_de_fmc*

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

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

Obtenir des licences pour le Centre de gestion

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

- **Threat (menace)** : Renseignements sur la sécurité et IPS de nouvelle génération
- **Défense contre les programmes malveillants** : défense contre les Programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **Cisco Secure Client** :Secure Client Advantage, Secure Client Premier, ou Secure Client VPN Only
- **Opérateur** : Diamètre, GTP/GPRS, M3UA, SCTP

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

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

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

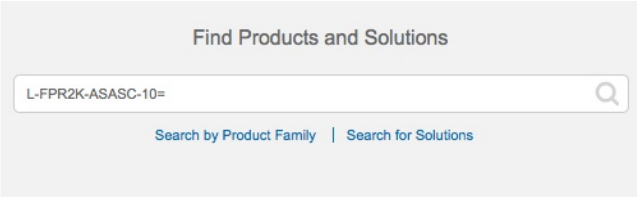
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

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

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

Illustration 1 : Recherche de licences



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

- Combinaison de licences englobant IPS, les , la défense contre les programmes malveillants et les URL :
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y

- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.
- Licence d'opérateur :
  - L-FPR9K-FTD-CAR=

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

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

Enregistrer Défense contre les menaces avec le Centre de gestion

Enregistrez chaque dispositif logique individuellement sur le même centre de gestion.

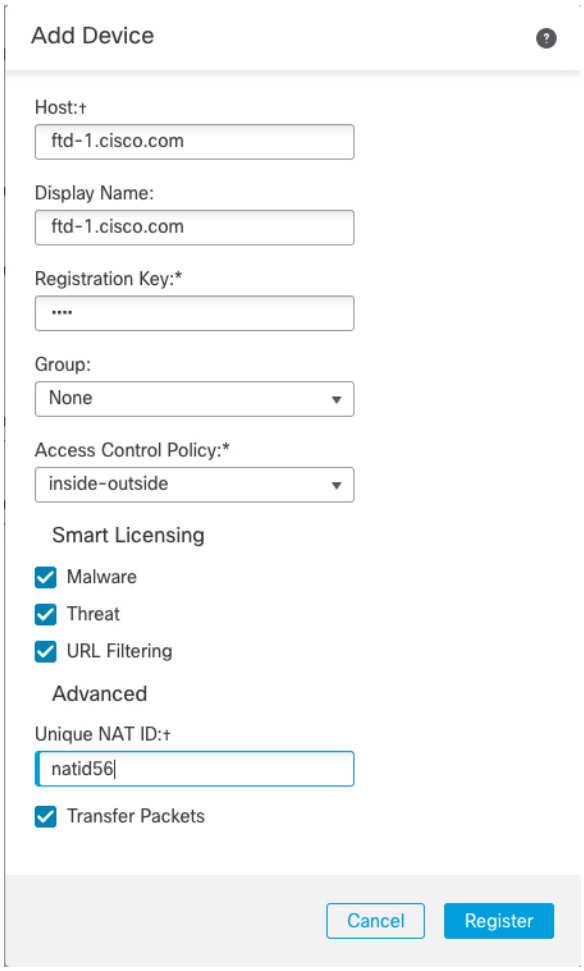
Avant de commencer

- Assurez-vous que **l'état** du dispositif logique défense contre les menaces est **en ligne** sur gestionnaire de châssis la page **Dispositifs logiques**.
- Rassemblez les informations suivantes que vous avez définies dans la configuration initiale du démarrage du dispositif de défense contre les menaces (see Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 35) :
  - L'adresse IP ou le nom d'hôte du gestionnaire défense contre les menaces, et l'ID NAT.
  - La clé d'enregistrement centre de gestion
- Dans les versions 6.7 et ultérieures, si vous souhaitez utiliser une interface de données pour la gestion, utilisez la commande **configure network management-data-interface** à l'interface de ligne de commande défense contre les menaces. Consultez la section Référence des commandes de défense contre les menaces de Cisco Secure Firewall pour obtenir plus de renseignements.

Procédure

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

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



Définissez les paramètres suivants :

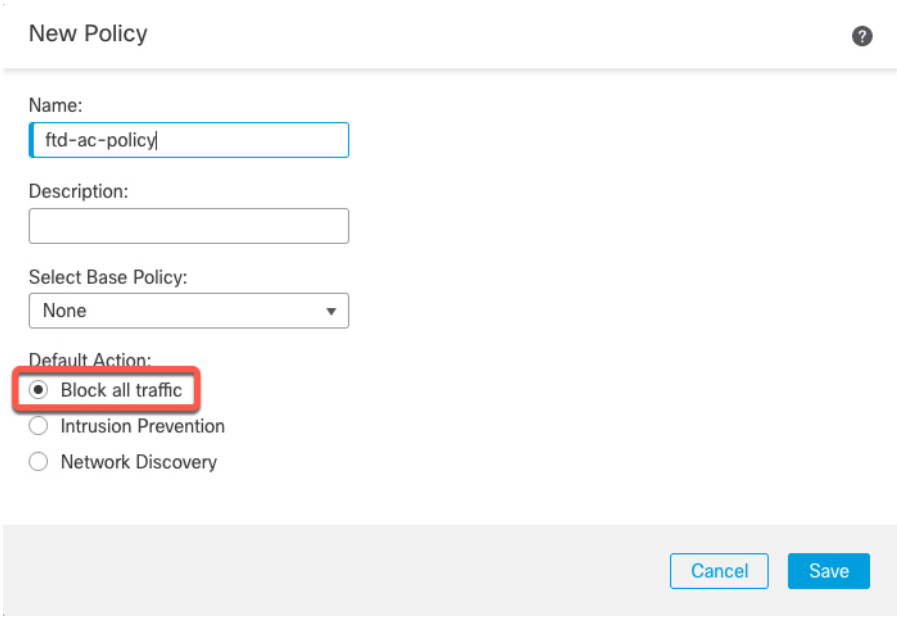
- **Host (Hôte)** : saisissez l'adresse IP ou le nom d'hôte de défense contre les menacesque vous souhaitez ajouter. Vous pouvez laisser ce champ vide si vous avez spécifié à la fois l'adresse IP centre de gestion et un ID NAT dans la configuration initiale de démarrage du dispositif de défense contre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

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

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

- **Group** (groupe) : attribuez-le à un groupe de dispositifs si vous utilisez des groupes.
- **Access Control Policy** (politique de contrôle d'accès) : choisissez une politique initiale. Sauf si vous avez déjà une politique personnalisée que vous savez que vous devez utiliser, choisissez **Create new policy** (créer une nouvelle politique) et **Block all traffic** (bloquer tout le trafic). Vous pourrez modifier ce réglage ultérieurement pour autoriser le trafic; voir Permettre le trafic de l'intérieur vers l'extérieur, à la page 56.

Illustration 2 : Nouvelle politique



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

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

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

- Ping : accédez à l'interface de ligne de commande de défense contre les menaces (Accéder à l'interface de ligne de commande Défense contre les menaces, à la page 59) et envoyez un ping à l'adresse IP centre de gestion à l'aide de la commande suivante :

  ping system *adresse_ip*

  Si le message ping échoue, vérifiez vos paramètres réseau à l'aide de la commande **show network**. Si vous devez modifier l'adresse IP de gestion de défense contre les menaces, utilisez la commande **configure network** {**ipv4** | **ipv6**} **manual**. Si vous avez configuré une interface de données pour l'accès centre de gestion, utilisez la commande **configure network management-data-interface**.

- NTP : assurez-vous que le serveur NTP Firepower 9300 correspond au serveur centre de gestion défini sur la page **System (système)** > **Configuration** > **Time Synchronization (synchronisation du temps)**.

- Clé d'enregistrement, ID NAT et adresse IP centre de gestion : assurez-vous que vous utilisez la même clé d'enregistrement et, le cas échéant, le même ID NAT, sur les deux appareils. Vous pouvez définir la clé d'enregistrement et l'ID NAT sur centre de gestion à l'aide de la commande **configure manager add**.

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

Configurer une politique de sécurité de base

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

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

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

1	Configurer les interfaces, à la page 47.
2	Configurer le serveur DHCP, à la page 50.
3	Ajouter la voie de routage par défaut, à la page 51.
4	Configurer NAT, à la page 53.
5	Permettre le trafic de l'intérieur vers l'extérieur, à la page 56.

6	Déployer la configuration, à la page 57.

Configurer les interfaces

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

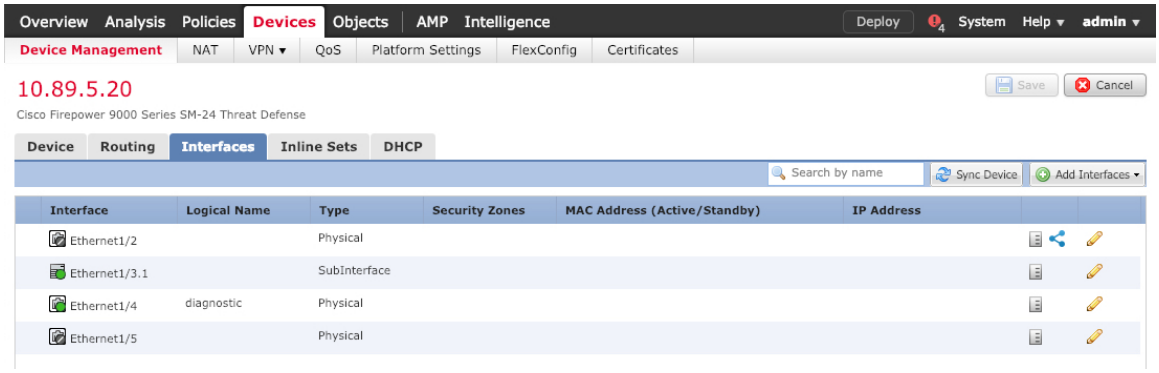
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

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

Procédure

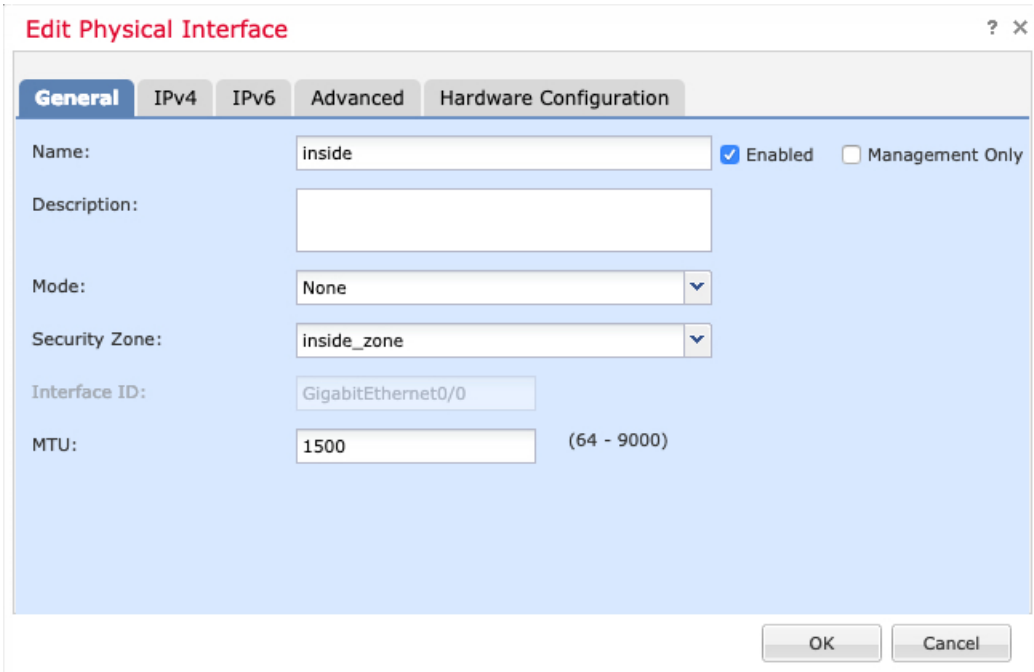
Étape 1 Choisissez **Devices (dispositifs)** > **Device Management (gestion du dispositif)**, et cliquez sur **Modifier** (✎) pour le pare-feu.

Étape 2 Cliquez sur **Interfaces**.



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

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



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

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

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

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

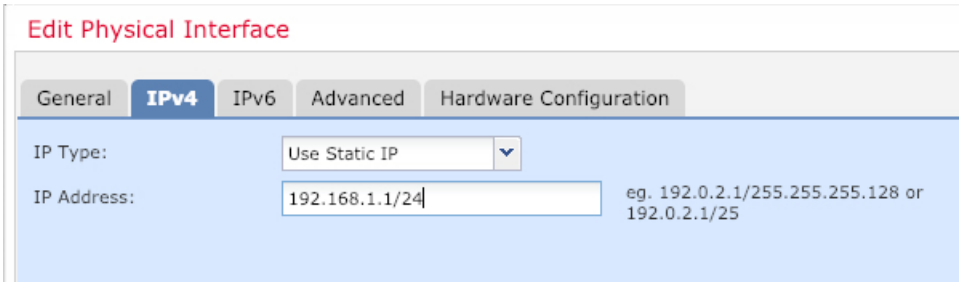
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

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

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

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

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

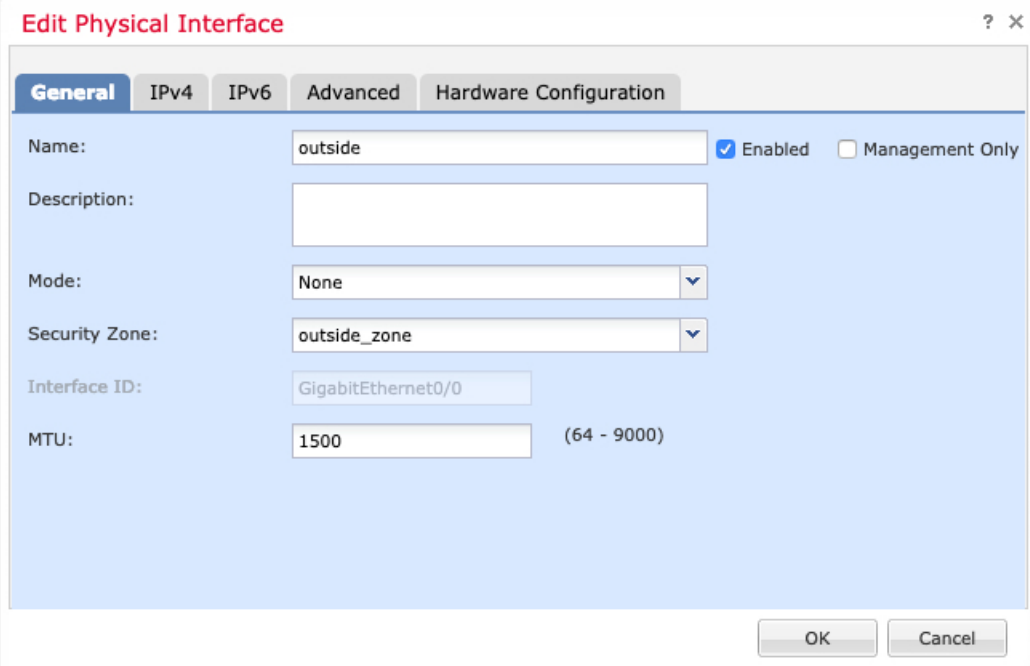


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

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

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



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

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

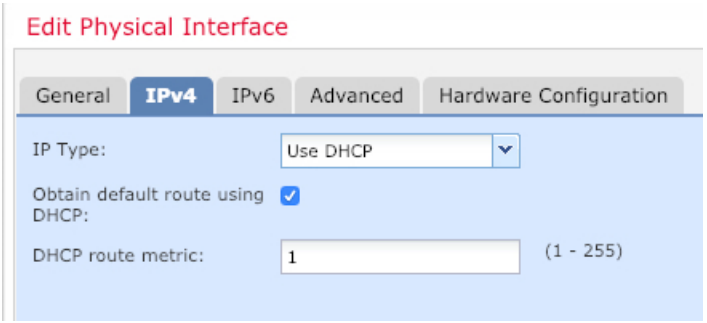
Par exemple, nommez l'interface **externe**.

b) Cochez la case **Enabled** (activer).
c) Laissez le **Mode** défini sur **None** (aucun).
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **New** (nouveau).

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

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

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



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

f) Cliquez sur **OK**.

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

Configurer le serveur DHCP

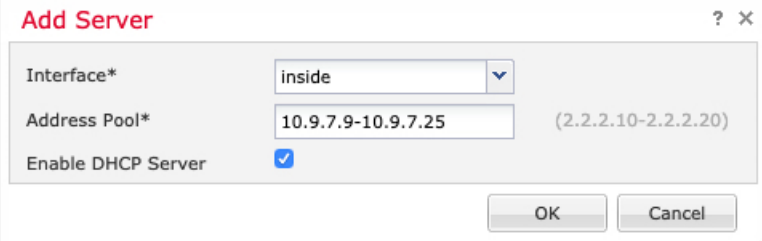
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de Défense contre les menaces.

Procédure

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

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

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



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

Étape 4 Cliquez sur **OK**.

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

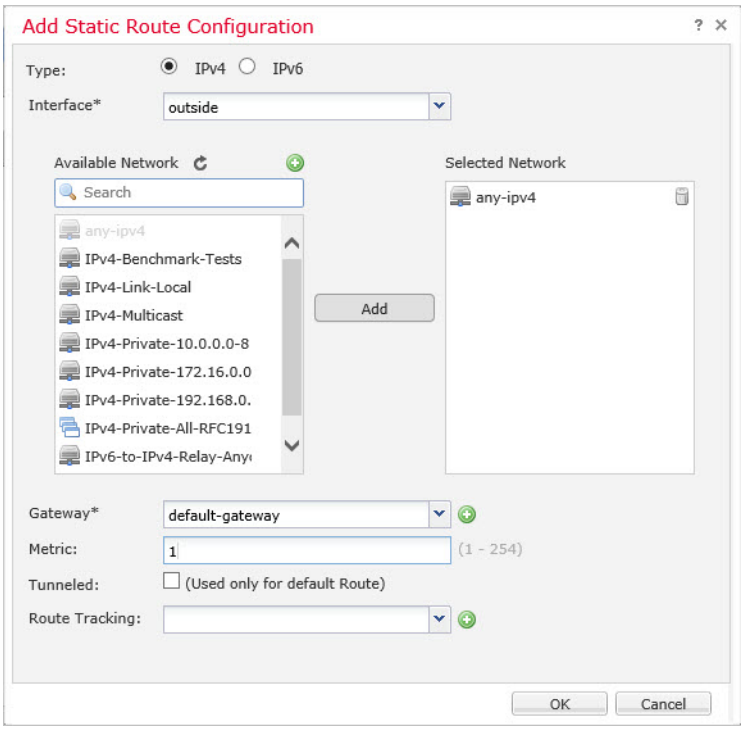
Ajouter la voie de routage par défaut

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

Procédure

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

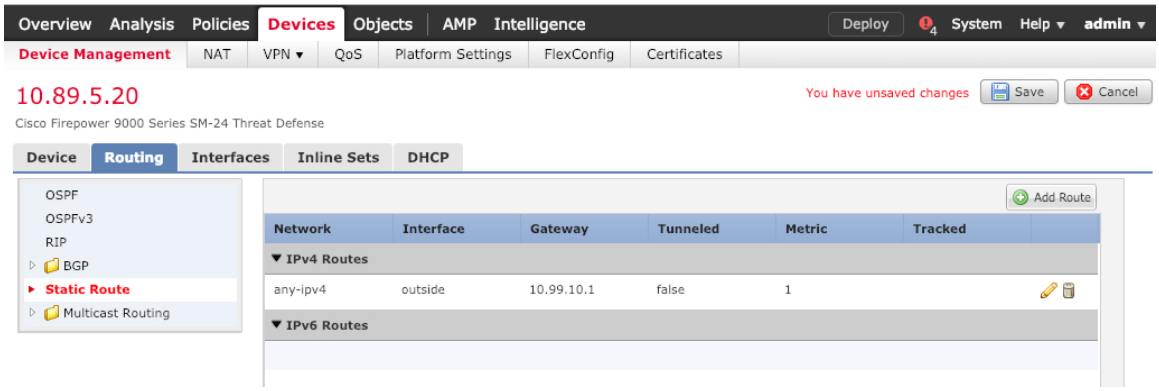
Étape 2 Sélectionnez **Routing (routage)** > **Static Route (route statique)**, cliquez sur **Add Route (ajouter route)**, et définissez ce qui suit :



- **Type** : Cliquez sur le bouton radio **IPv4** ou **IPv6** selon le type de routage statique que vous ajoutez.
- **Interface** : Sélectionnez l'interface de sortie; il s'agit généralement de l'interface externe.
- **Available Network** (réseau disponible) : Choisissez **any-ipv4** pour une voie de routage par défaut IPv4 ou **any-ipv6** pour une voie de routage par défaut IPv6, puis cliquez sur **Add** (ajouter) pour la déplacer vers la liste **Selected Network** (réseau sélectionné).
- **Gateway (passerelle)** ou **IPv6 Gateway (passerelle iPv6)** : Saisissez ou choisissez le routeur de passerelle qui est le prochain saut sur cette voie de routage. Vous pouvez fournir une adresse IP ou un objet réseaux/hôtes.
- **Metric** (nombre) : Saisissez le nombre de sauts sur le réseau de destination. Les valeurs valides vont de 1 à 255; la valeur par défaut est 1.

Étape 3 Cliquez sur **OK**.

La voie est ajoutée à la table de routage statique.



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

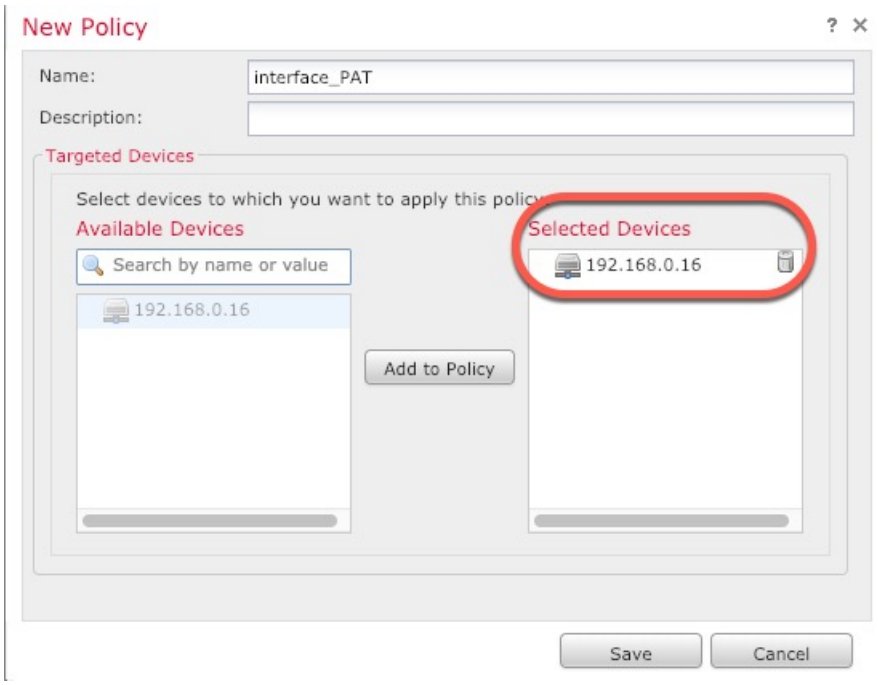
Configurer NAT

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

Procédure

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

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



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

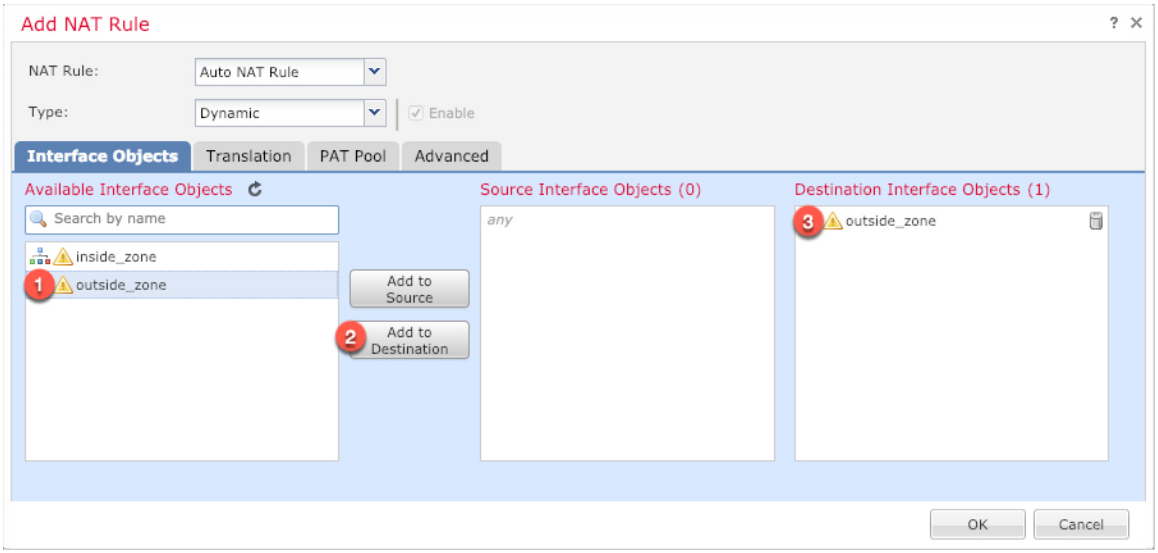
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

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

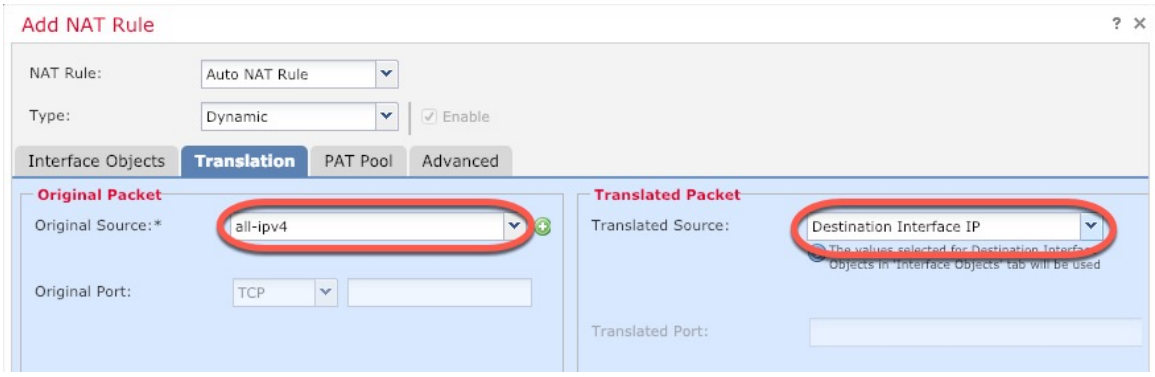
Étape 4 Configurez les options des règles de base :

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

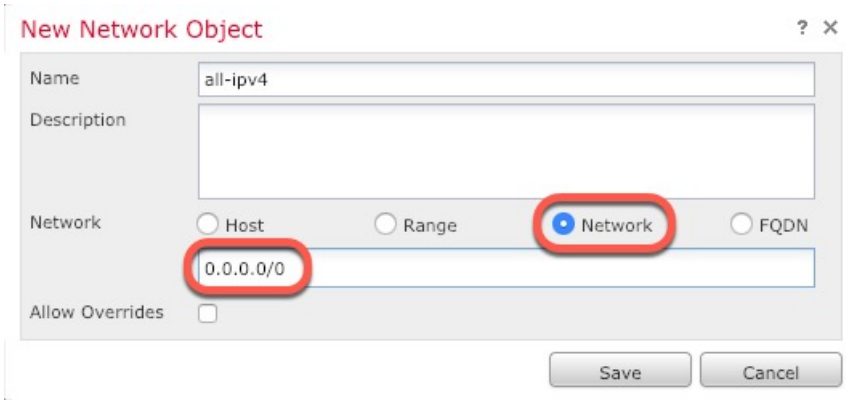
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



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



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

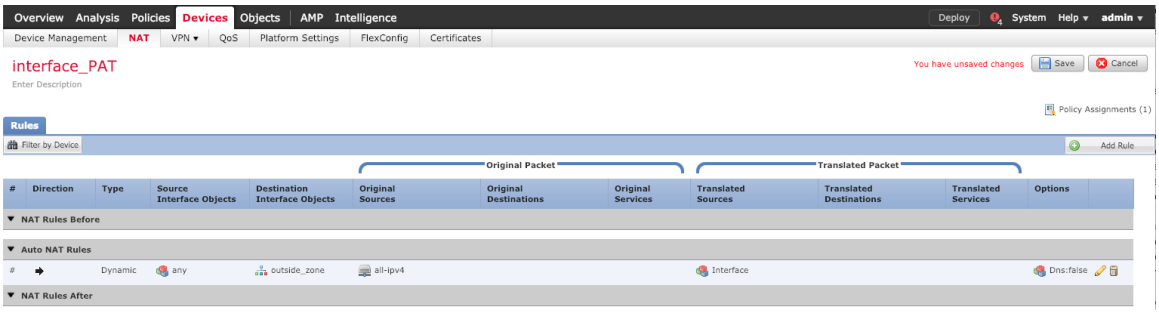


Remarque
Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

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

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

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



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

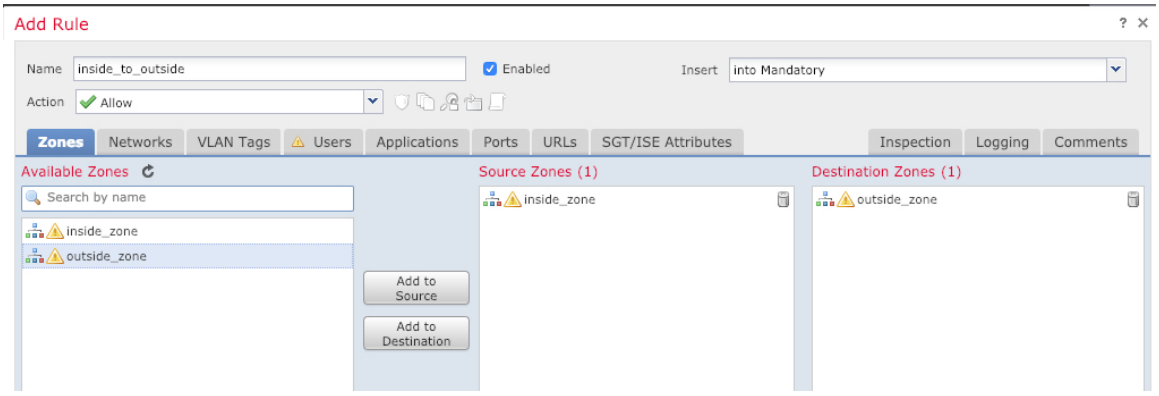
Permettre le trafic de l'intérieur vers l'extérieur

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

Procédure

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

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



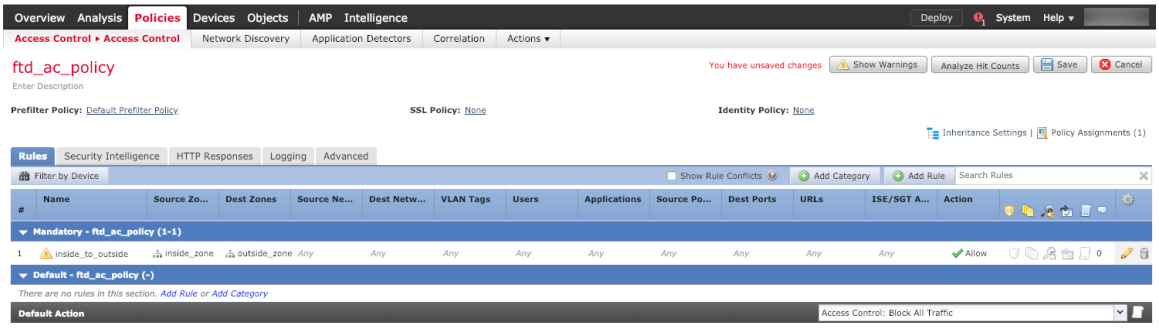
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

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

Laissez les autres paramètres tels quels.

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

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



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

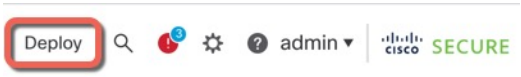
Déployer la configuration

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

Procédure

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

Illustration 3 : Déployer



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

Illustration 4 : Déployer tout

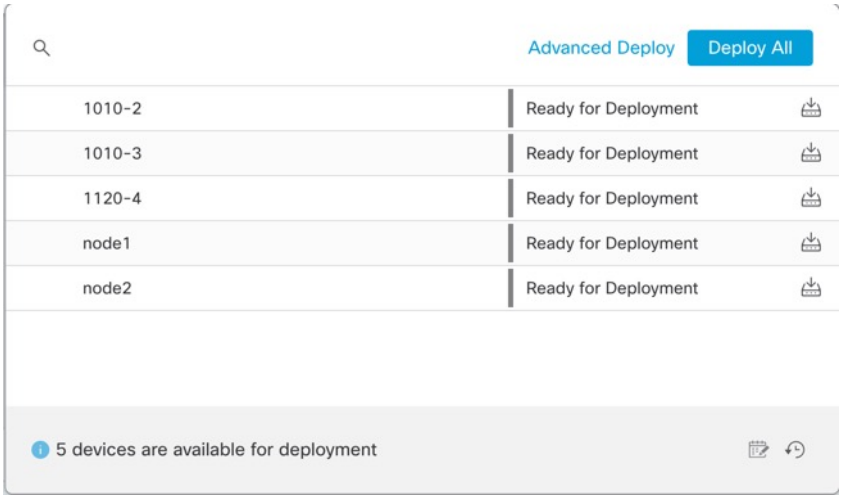
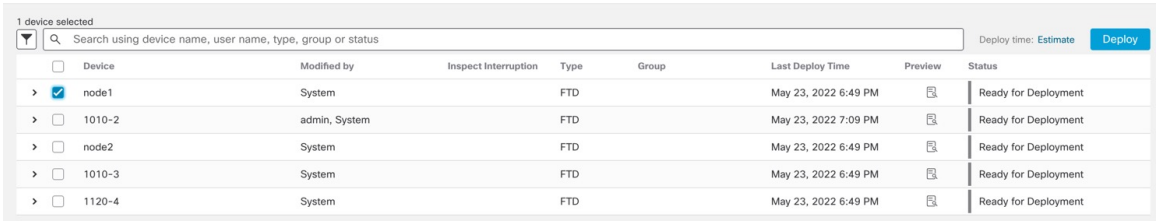
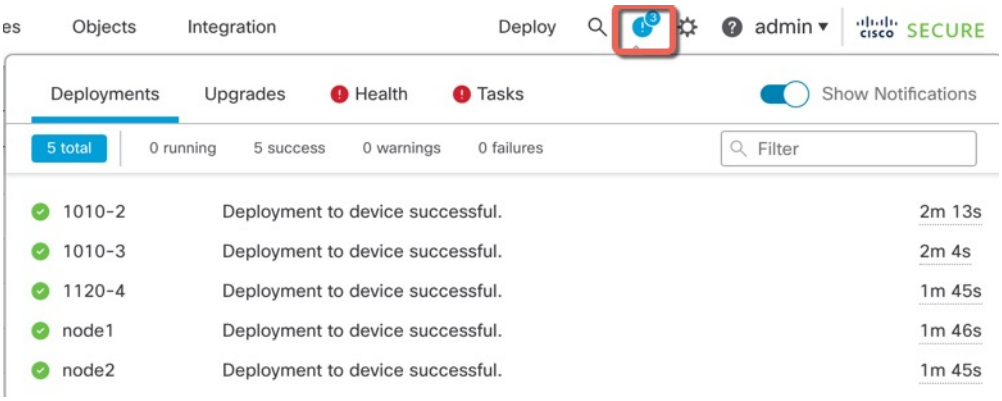


Illustration 5 : Déploiement avancé



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

Illustration 6 : État du déploiement



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

Vous pouvez utiliser l'interface de ligne de commande de Défense contre les menaces pour modifier les paramètres de l'interface de gestion et à des fins de dépannage. Vous pouvez accéder à l'interface de ligne de commande en utilisant SSH sur l'interface de gestion, ou en vous connectant à partir de l'interface de ligne de commande FXOS.

Procédure

Étape 1 (Option 1) SSH directement lié à l'adresse IP de l'interface de gestion de Défense contre les menaces.

Vous avez défini l'adresse IP de gestion lorsque vous avez déployé le dispositif logique. Connectez-vous à Défense contre les menaces avec le compte administrateur et le mot de passe que vous avez définis lors du déploiement initial.

Si vous avez oublié le mot de passe, vous pouvez le modifier en modifiant le dispositif logique dans le dossier de l'entreprise gestionnaire de châssis.

Étape 2 (Option 2) À partir de l'interface de ligne de commande de FXOS, connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

a) Connectez-vous au security module.

connect module *numéro_de_logement* {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connectez-vous à la console de Défense contre les menaces.

connect ftd *nom*

Si vous avez plusieurs instances d'application, vous devez préciser le nom de l'instance. Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
```

```
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
==========================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **exit**.

Remarque
Pour les versions antérieures à la version 6.3, entrez **Ctrl-a, d**.

d) Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Pour quitter la console :

1. Entrez **~**

   Vous quittez l'application Telnet.

2. Pour quitter l'application Telnet, entrez :

   telnet>**quit**

Pour quitter la session Telnet :

Entrez **Ctrl-], .**

Exemple

L'exemple suivant se connecte à Défense contre les menaces sur le module de sécurité 1 et repart au niveau superviseur de Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
```

```
'connect module <slot> telnet' to connect to the security module.
==================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

Quelle est l'étape suivante?

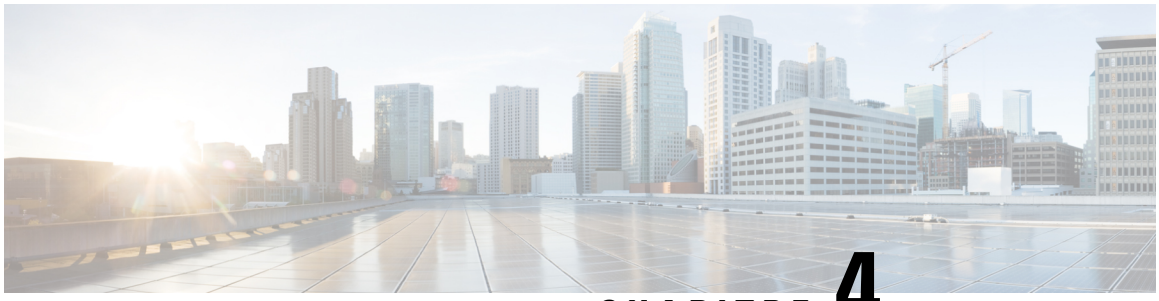
Pour continuer à configurer votre défense contre les menaces, consultez les documents disponibles pour votre version de logiciel à Orientation dans la documentation Cisco Firepower.

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

Historique pour Défense contre les menaces avec le Centre de gestion

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge d'ASA et de Défense contre les menaces sur des modules distincts du même Firepower 9300	6.4	Vous pouvez maintenant déployer l'ASA et les dispositifs logiques Défense contre les menaces sur le même Firepower 9300. **Remarque** FXOS 2.6.1 est nécessaire.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Capacité multi-instance pour le dispositif de défense contre les menaces sur le Firepower 4100/9300	6.3.0	Vous pouvez désormais déployer plusieurs dispositifs logiques, chacun avec l'instance de conteneur défense contre les menaces, sur un moteur ou module de sécurité. Auparavant, vous ne pouviez déployer qu'une seule instance d'application native. Pour fournir une utilisation flexible de l'interface physique, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces entre plusieurs instances. La gestion des ressources vous permet de personnaliser les capacités de performance de chaque instance. Vous pouvez utiliser la haute disponibilité en utilisant une instance de conteneur sur deux châssis distincts. La mise en grappe n'est pas prise en charge. **Remarque** La capacité multi-instance est similaire au mode à contexte multiple ASA, bien que son implémentation soit différente. Le mode contexte multiple n'est pas disponible sur défense contre les menaces. Écrans Nouveaux ou modifiés de centre de gestion : • Icône **Devices (Dispositifs)** > **Device Management (Gestion des dispositifs)** > **Edit (Modifier)** Onglet **> Interfaces** Écrans Nouveaux ou modifiés de gestionnaire de châssis : • **Overview (Survol)** > **Devices (Dispositifs)** • Menu déroulant **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Add New (Ajouter) > Subinterface (Sous-interface)** • **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Type** • **Logical Devices (Dispositifs logiques)** > **Add Device (Ajouter un dispositif)** • **Platform Settings (Paramètres de la plateforme)** > **Mac Pool (Bassin Mac** • **Platform Settings (Paramètres de la plateforme)** > **Resource Profiles (Profils des ressources)**



CHAPITRE 4

Défense contre les menaces Déploiement avec le Gestionnaire d'appareil

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

Ce chapitre décrit comment déployer un dispositif logique autonome Défense contre les menaces avec le gestionnaire d'appareil. Pour déployer une paire de haute disponibilité, voir le Guide Cisco Secure Firewall Device Manager Configuration .

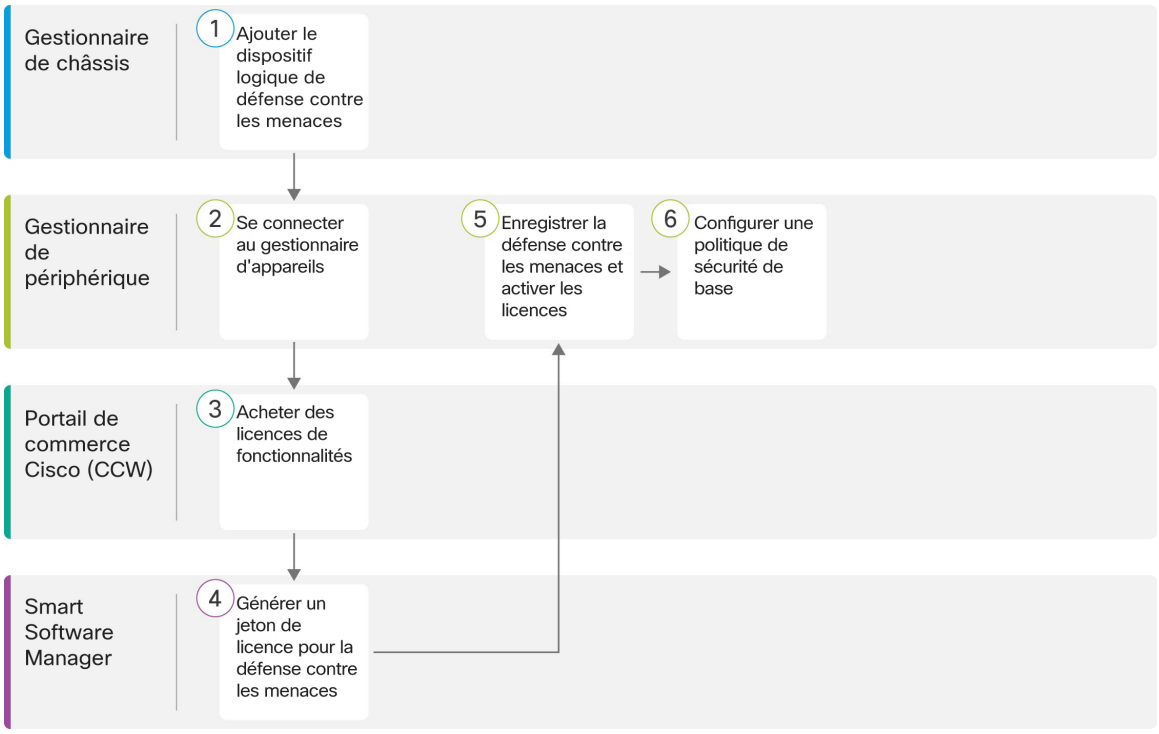
Le gestionnaire d'appareil vous permet de configurer les fonctions de base du logiciel qui sont le plus souvent utilisées pour les petits réseaux. Il est spécialement conçu pour les réseaux qui comprennent un seul dispositif ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire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

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet Défense contre les menaces, utilisez plutôt le centre de gestion.

Déclaration de confidentialité : Firepower 9300 n'exige ni ne recueille de renseignements permettant d'établir l'identité de quelqu'un. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, pour créer les noms d'utilisateur. Si c'est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu'il travaille à la configuration ou qu'il utilise SNMP.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer et configurer Défense contre les menaces sur votre châssis.



	Espace de travail	Étapes
1	Gestionnaire de châssis	Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 64.
2	Gestionnaire d'appareil	Se connecter à Gestionnaire d'appareil, à la page 69.
3	Portail de commerce Cisco (CCW)	Configurer les licences, à la page 69 : Achetez des licences de fonctionnalités.
4	Smart Software Manager	Configurer les licences, à la page 69 : Générer un jeton de licence pour gestionnaire d'appareil.
5	Gestionnaire d'appareil	Configurer les licences, à la page 69 : enregistrer gestionnaire d'appareil auprès du serveur de licences Smart et activez les licences de fonctionnalités.
6	Gestionnaire d'appareil	Configurer une politique de sécurité de base, à la page 76.

Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces

Vous pouvez déployer le dispositif de défense contre les menaces à partir du Firepower 9300 en tant qu'instance native. Les instances de conteneur ne sont pas prises en charge.

Pour ajouter une paire de haute disponibilité, consultez la rubrique Guide Cisco Secure Firewall Device Manager Configuration .

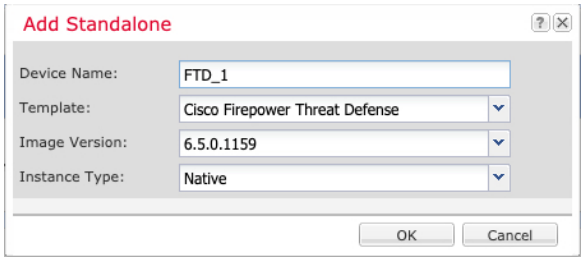
Avant de commencer

- Configurer l'interface de gestion à utiliser avec défense contre les menaces; voir Interfaces de configuration, à la page 24. L'interface de gestion est requise. Il convient de souligner que cette interface de gestion est différente du port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**).
- Vous devez également configurer au moins une interface de données.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce dispositif
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - l'adresse IP du serveur DNS
  - Nom d'hôte et le nom de domaine Défense contre les menaces

Procédure

Étape 1 Dans Gestionnaire de châssis, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur **Add** > **Standalone**, puis définissez les paramètres suivants :



a) Indiquez un nom de dispositif (**Device Name**).

Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de dispositif utilisé dans la configuration de l'application.

Remarque
Vous ne pouvez pas modifier ce nom après avoir ajouté le dispositif logique.

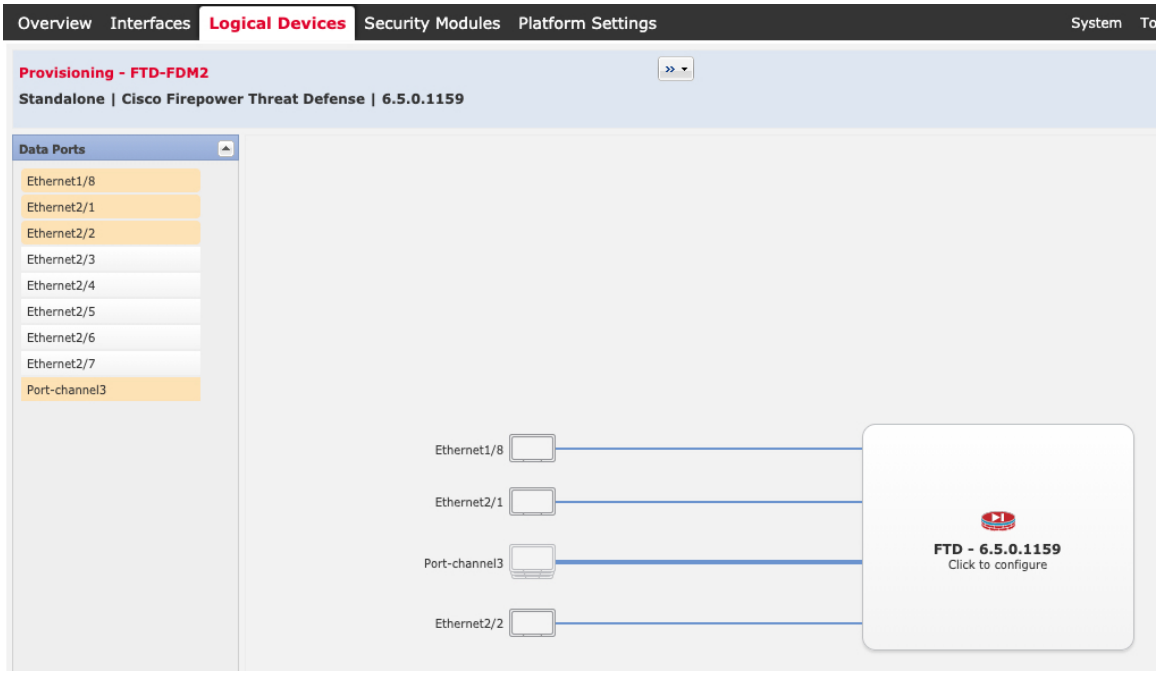
b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
c) Choisissez la version de l'image (**Image Version**).
d) Choisissez l'**Instance Type (Type d'instance)** : **Native (Instance native)**.

Les instances de conteneur ne sont pas prises en charge avec le gestionnaire d'appareil.

e) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du dispositif).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au dispositif.

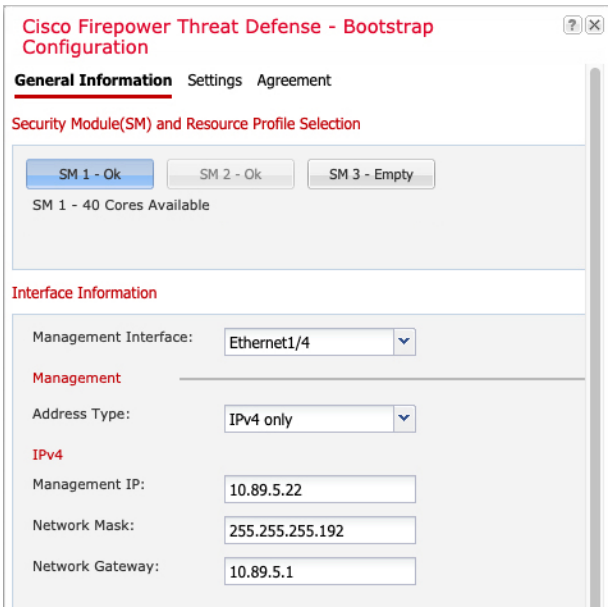


Vous ne pouvez attribuer que des interfaces de données que vous avez préalablement activées sur la page **Interfaces**. Vous activerez et configurerez plus tard ces interfaces dans le gestionnaire d'appareil, y compris la définition des adresses IP.

Étape 4 Cliquez sur l'icône de dispositif au centre de l'écran.

Une boîte de dialogue s’affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l’interface de ligne de commande de l’application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) (Pour Firepower 9300) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce dispositif logique.
b) Choisissez l'interface de gestion (**Management Interface**).

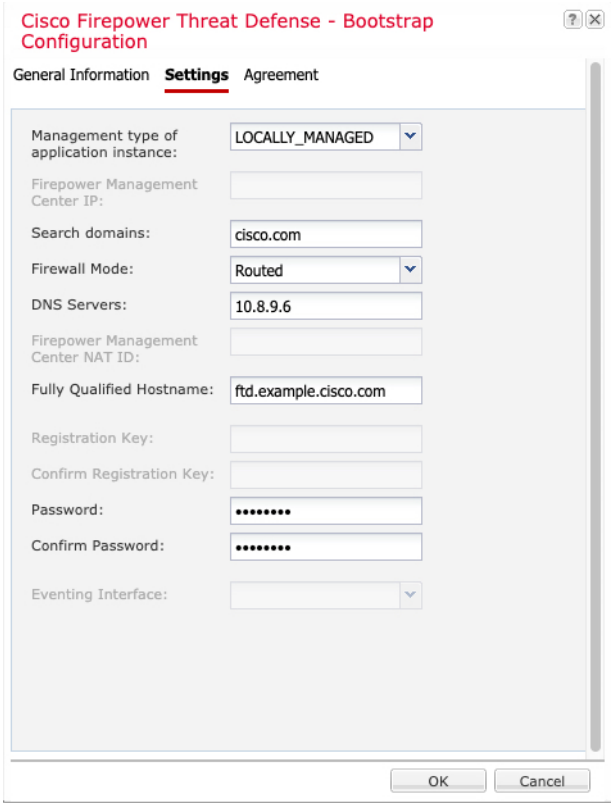
   Cette interface est utilisée pour gérer le dispositif logique. Cette interface est distincte du port de gestion du châssis.

c) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).
d) Configurez l'adresse IP de gestion (**Management IP**).

   Définissez une adresse IP unique pour cette interface.

e) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).
f) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Sous l'onglet **Settings** (paramètres), procédez comme suit :



a) Dans la liste déroulante **Management type of application instance** (Type de gestion de l'instance d'application), choisissez **LOCALLY_MANAGED**.

   Les instances natives prennent également en charge le centre de gestioncomme gestionnaire. Si vous changez le gestionnaire après avoir déployé le dispositif logique, votre configuration est effacée et le dispositif est réinitialisé.

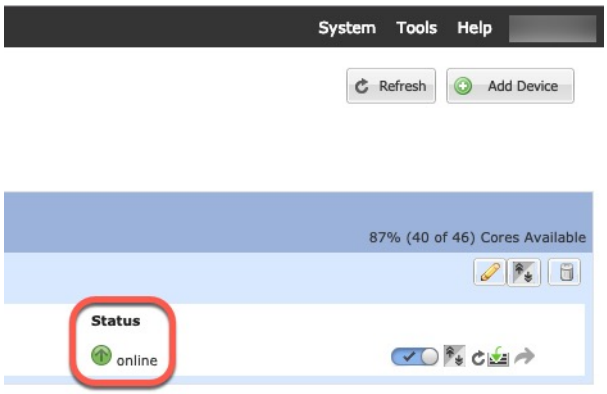
b) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.
c) Le **Firewall Mode** (Mode pare-feu) ne prend en charge que le mode **Routed** (Routé).
d) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont séparés par des virgules.
e) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour Défense contre les menaces.
f) Saisissez un mot de passe (**Password**) pour l'utilisateur admin Défense contre les menaces pour l'accès à l'interface de ligne de commande.

Étape 7 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.

Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (enregistrer).

Le châssis déploie le dispositif logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau dispositif logique dans la page **Logical Devices**. Lorsque le dispositif logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Se connecter à Gestionnaire d'appareil

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

Avant de commencer

- Utilisez une version actuelle de Firefox, Chrome, Safari, Edge ou Internet Explorer.
- Assurez-vous que **l'état** du dispositif logique défense contre les menaces est **en ligne** sur gestionnaire de châssis la page **Dispositifs logiques**.

Procédure

Étape 1 Entrez l'URL suivante dans votre navigateur.

- Management (gestion) : **https://***management_ip*. Entrez l'adresse IP de l'interface que vous avez entrée dans la configuration de démarrage.

Étape 2 Connectez-vous avec le nom d'utilisateur **admin**, et le mot de passe que vous avez défini lorsque vous avez déployé le mot de passe par défaut défense contre les menaces.

Étape 3 Vous êtes invité à accepter la licence d'évaluation de 90 jours.

Configurer les licences

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

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

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

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

- **Threat (menace)** : Renseignements sur la sécurité et IPS de nouvelle génération
- **Défense contre les programmes malveillants** : défense contre les Programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **Cisco Secure Client** :Secure Client Advantage, Secure Client Premier, ou Secure Client VPN Only

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

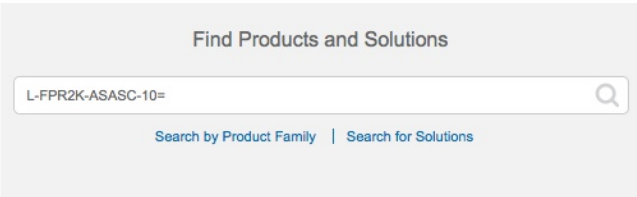
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines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

Procédure

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

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

Illustration 7 : Recherche de licences



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

- Combinaison de licences englobant IPS, les , la défense contre les programmes malveillants et les URL :
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

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

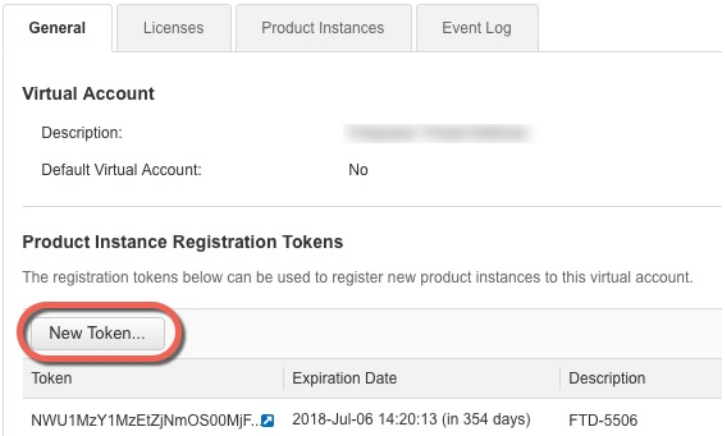
- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

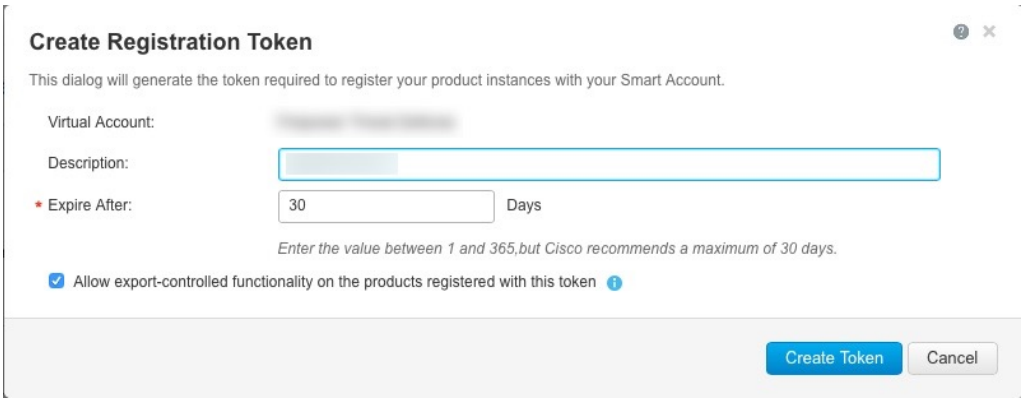
Étape 2 Dans le Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous voulez ajouter ce dispositif.

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

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



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



- **Description**
- **Expire After** (expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token** (autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton : active l'indicateur de conformité à l'exportation si vous êtes dans un pays qui autorise un 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 vous ne voyez pas cette option, votre compte ne prend pas en charge la fonctionnalité d'exportation contrôlée.

Le jeton est ajouté à votre inventaire.

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

Illustration 8 : Afficher le jeton

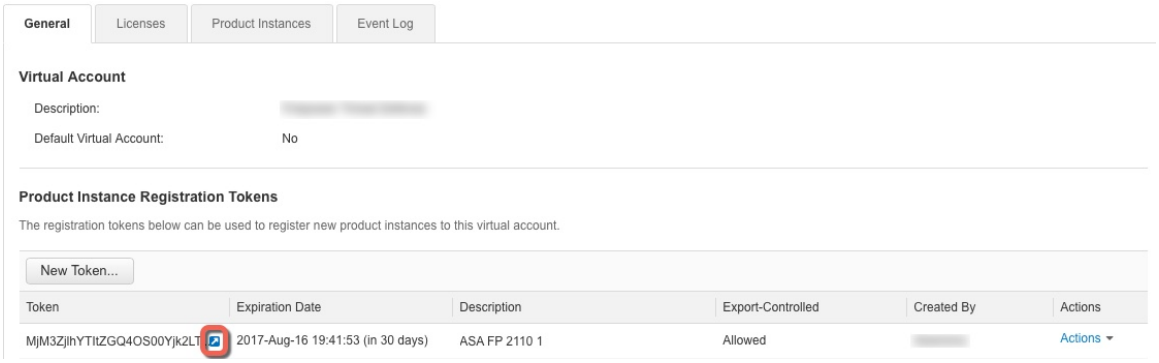
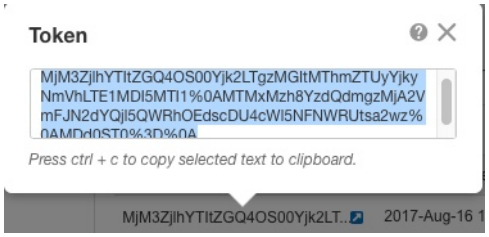


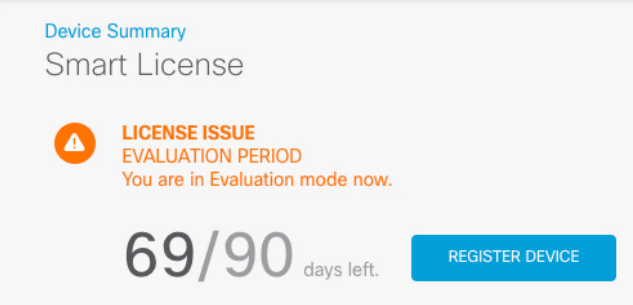
Illustration 9 : Copier le jeton



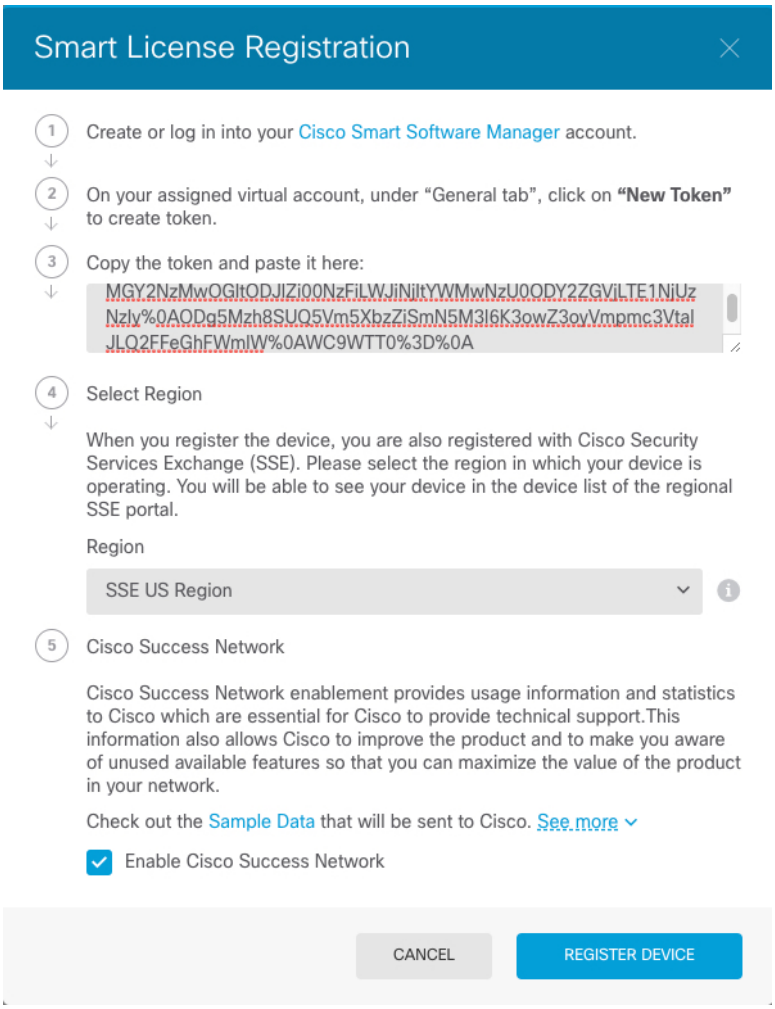
Étape 3 Dans le gestionnaire d'appareil, cliquez sur **Device (appareil)**, et puis dans le sommaire **Smart License** cliquez sur **View Configuration (voir configuration)**.

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

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



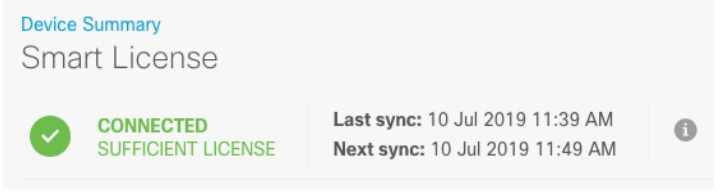
Suivez ensuite les instructions de la boîte de dialogue **Smart License Registration** pour coller votre jeton :



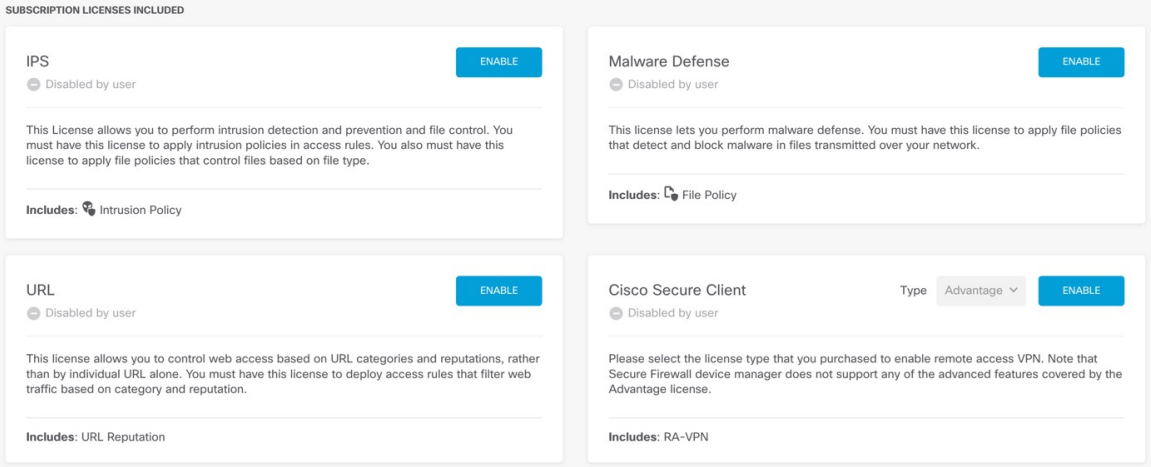
Étape 5 Cliquez sur **Register Device** (enregistrer l'appareil).

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

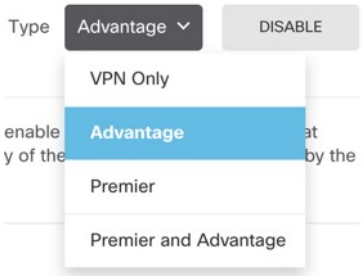
Une fois que l'appareil a été enregistré et que vous avez actualisé la page, les éléments suivants apparaissent :



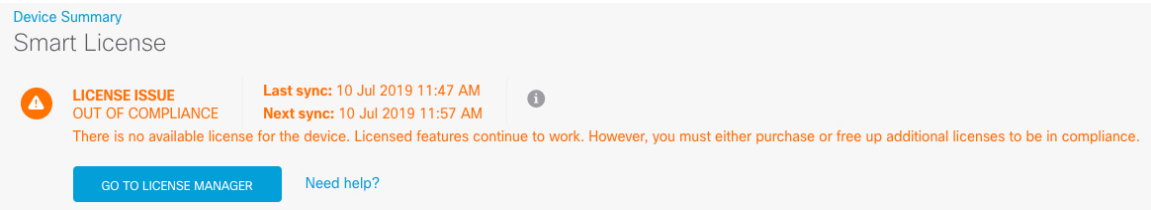
Étape 6 Cliquez sur **Enable/Disable** (activer/désactiver) pour chaque licence facultative, au besoin.



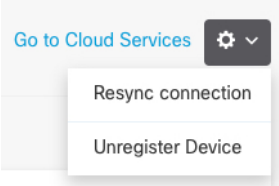
- **Enable** (activer) : Enregistre la licence avec votre compte Cisco Smart Software Manager et active les fonctionnalités contrôlées. Vous pouvez maintenant configurer et déployer les politiques contrôlées par la licence.
- **Disable** (désactiver) : Désinscrit la licence de votre compte Cisco Smart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



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



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



Configurer une politique de sécurité de base

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

1	Interfaces de configuration, à la page 76. Attribuez une adresse IP statique à l'interface interne et utilisez DHCP pour l'interface externe.
2	Ajouter des interfaces aux zones de sécurité, à la page 79. Ajoutez les interfaces interne et externe aux zones de sécurité interne et externe, qui sont requises pour le contrôle d'accès.
3	Ajouter la voie de routage par défaut, à la page 81. Si vous ne recevez pas la route par défaut du serveur DHCP externe, vous devez l'ajouter manuellement.
4	Configurer NAT, à la page 83. Utilisez l'interface PAT sur l'interface externe.
5	Permettre le trafic de l'intérieur vers l'extérieur, à la page 85. Permettez le trafic de l'intérieur vers l'extérieur
6	(Facultatif) Configurer le serveur DHCP, à la page 86. Utilisez un serveur DHCP sur l'interface interne pour les clients.
7	(Facultatif) Configurer la passerelle de gestion et autoriser la gestion sur les interfaces de données, à la page 87. Modifiez la passerelle de gestion et/ou autorisez la gestion à partir d'une interface de données.
8	Déployer la configuration, à la page 89.

Interfaces de configuration

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

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

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

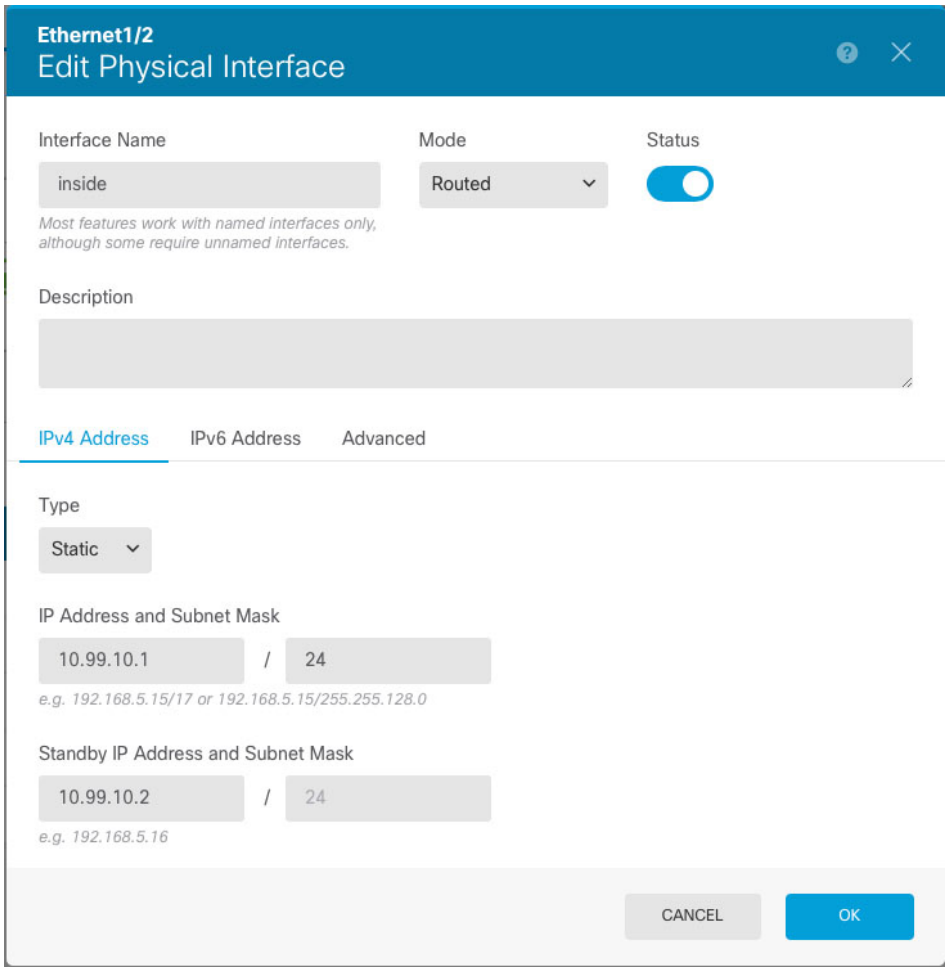
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification pour l'interface que vous souhaitez utiliser pour la valeur *inside* (intérieur)

Étape 3 Définissez les paramètres suivants :



a) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom de l'interface en utilisant au maximum 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe). Sans nom, le reste de la configuration de l'interface est ignoré. Sauf si vous configurez des sous-interfaces, l'interface doit avoir un nom.

b) Réglez le **Mode** sur **Routed** (routé).

Si vous souhaitez utiliser des interfaces passives, consultez le Guide Cisco Secure Firewall Device Manager Configuration .

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

Important
Vous devez également activer l'interface dans FXOS.

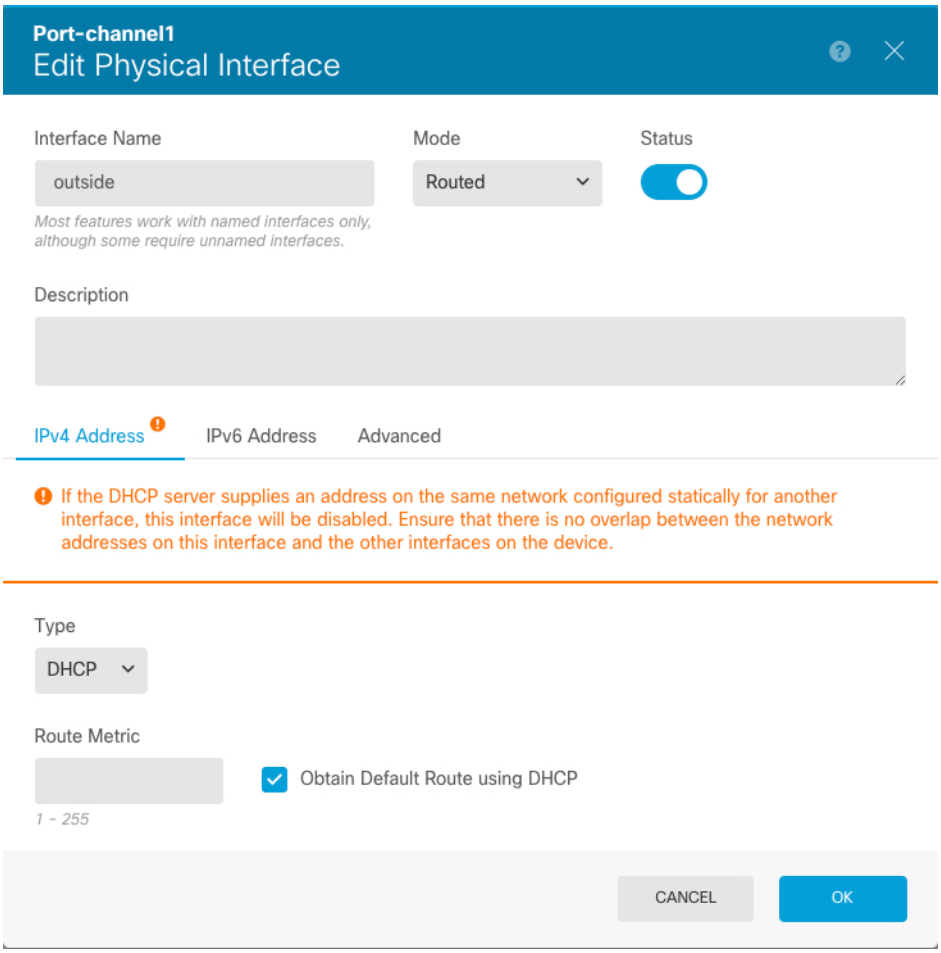
d) (Facultatif) Définissez la **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

e) Sur la page **IPv4 Address** (Adresse IPv4), configurez une adresse IP statique.
f) (Facultatif) Cliquez sur **IPv6 Address** (Adresse IPv6) et configurez l'adresse IPv6.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur l'icône de modification ( ) de l'interface que vous souhaitez utiliser pour la partie *outside* (externe) et définissez les mêmes champs que pour la partie interne; pour cette interface, choisissez **DHCP** pour l'adresse IPv4.



Remarque
Si vous utilisez une adresse IP statique ou si vous ne recevez pas de route par défaut de DHCP, vous devrez définir manuellement une route par défaut. consultez le Guide Cisco Secure Firewall Device Manager Configuration .

Ajouter des interfaces aux zones de sécurité

Une zone de sécurité est un regroupement d'interfaces. Les zones divisent le réseau en segments pour vous aider à gérer et à classer le trafic. Vous pouvez définir plusieurs zones, mais une interface donnée ne peut se trouver que dans une seule zone.

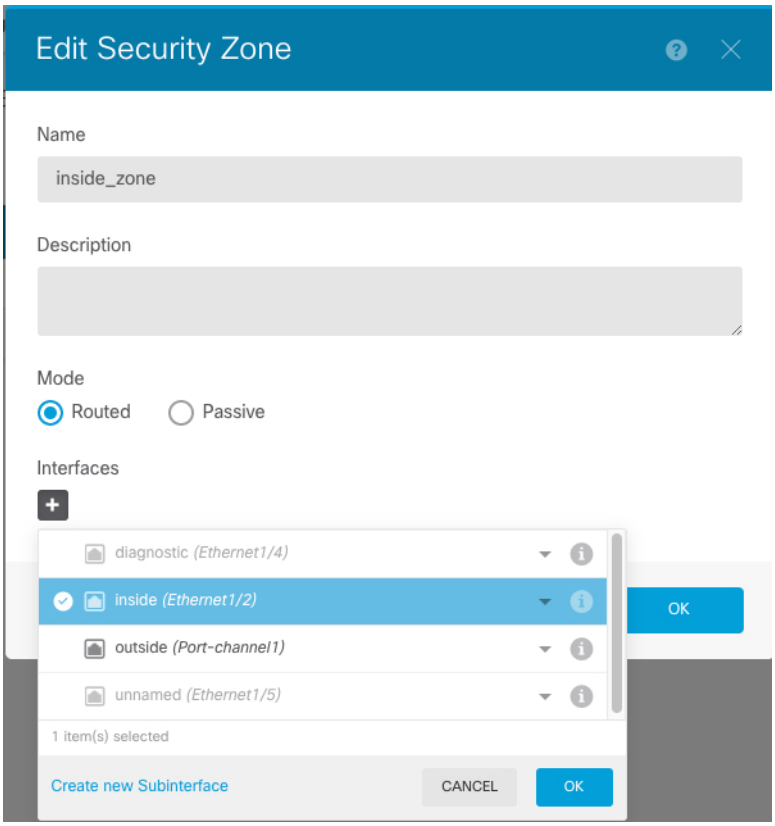
Cette procédure vous explique comment ajouter des interfaces aux zones préconfigurées suivantes :

- **inside_zone** (zone_interne) : cette zone est destinée à représenter les réseaux internes.
- **outside_zone** (zone_externe) : cette zone est destinée à représenter les réseaux en dehors de votre contrôle, comme Internet.

Procédure

Étape 1 Sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

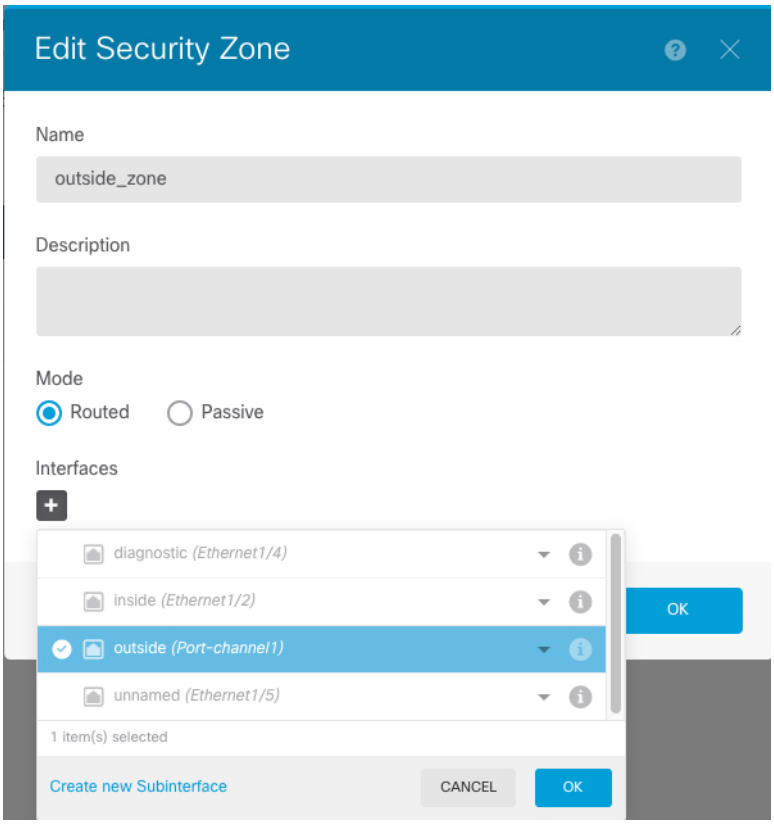
Étape 2 Cliquez sur l'icône de modification ( ) pour **inside_zone** (zone_interne).



Étape 3 Dans la liste des **Interfaces** , cliquez sur + et sélectionnez l'interface interne à ajouter à la zone.

Étape 4 Cliquez sur **OK** pour enregistrer les modifications.

Étape 5 Répétez ces étapes pour ajouter l'interface externe à l'**outside_zone** (zone_externe).



Ajouter la voie de routage par défaut

La voie de routage par défaut s'oriente normalement vers le routeur en amont accessible de l'interface externe. Si vous utilisez DHCP pour l'interface externe, votre appareil a peut-être déjà reçu une voie de routage par défaut. Si vous devez ajouter la route manuellement, procédez comme suit. Si vous avez reçu une route par défaut du serveur DHCP, elle apparaîtra à la page **Device Summary (Récapitulatif du dispositif)** > **Static Routing (Route statique)**.

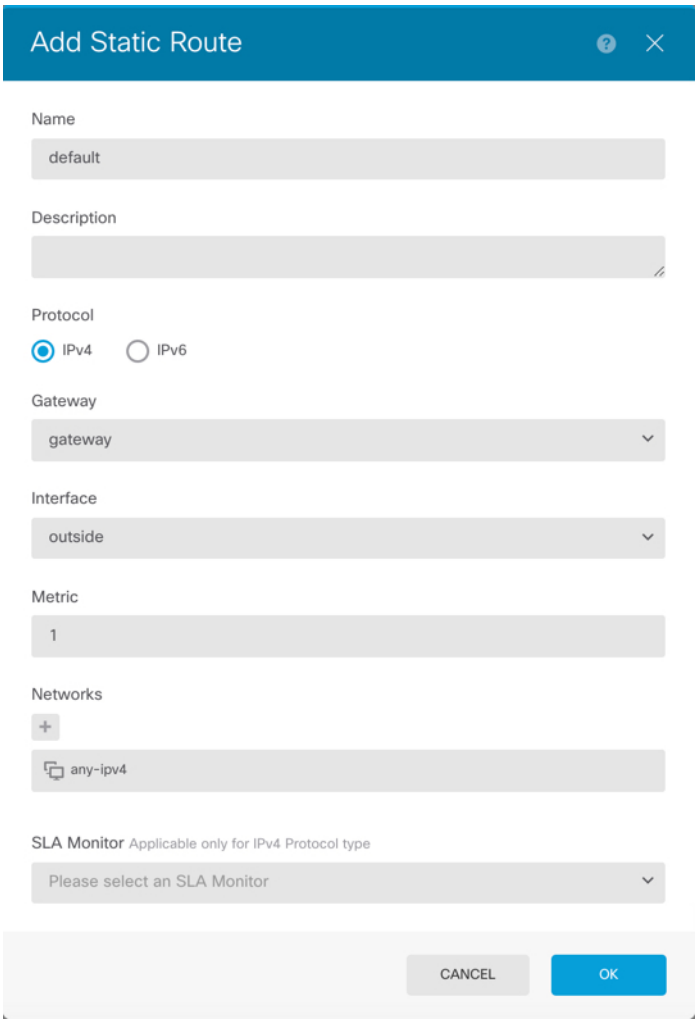
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé du routage (**Routing**).

La page **Static Routing** (routage statique) s'ouvre.

Étape 2 Cliquez sur + ou sur **Create Static Route** (créer une voie de routage statique).

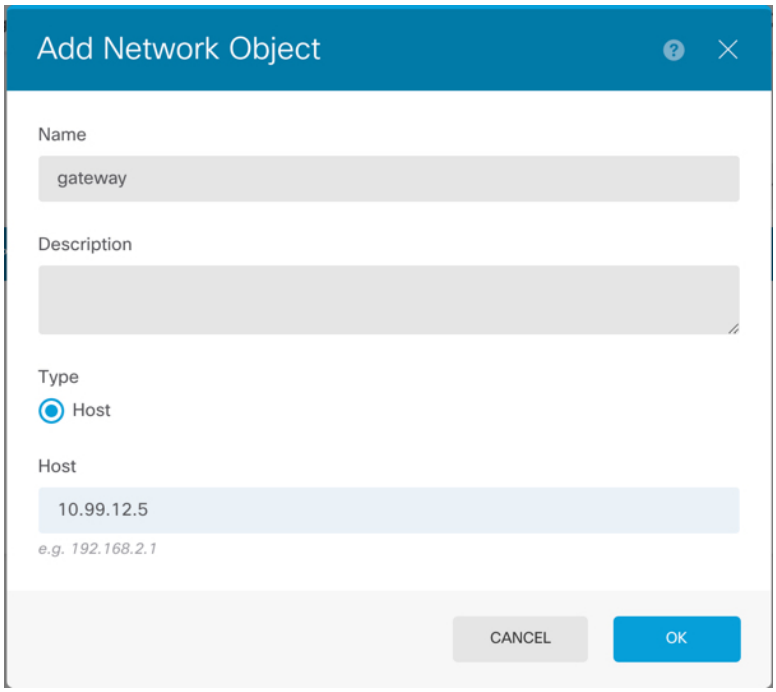
Étape 3 Configurez les propriétés des voies de routage par défaut.



a) Saisissez un nom (**Name**), par exemple, **default**.
b) Cliquez sur le bouton radio **IPv4** ou **IPv6**.

   Vous devez créer des voies de routage par défaut distinctes pour IPv4 et IPv6.

c) Cliquez sur **Gateway** (passerelle), puis sur **Create New Network** (créer un nouveau réseau) pour ajouter l'adresse IP de la passerelle en tant qu'objet hôte.



d) Choisissez l'**Interface** de passerelle, par exemple **outside** (externe).

e) Cliquez sur l'icône **Networks (réseaux)** +, puis choisissez **any-ipv4** pour une voie de routage IPv4 par défaut ou **any-ipv6** pour une voie de routage IPv6 par défaut.

Étape 4 Cliquez sur **OK**.

Configurer NAT

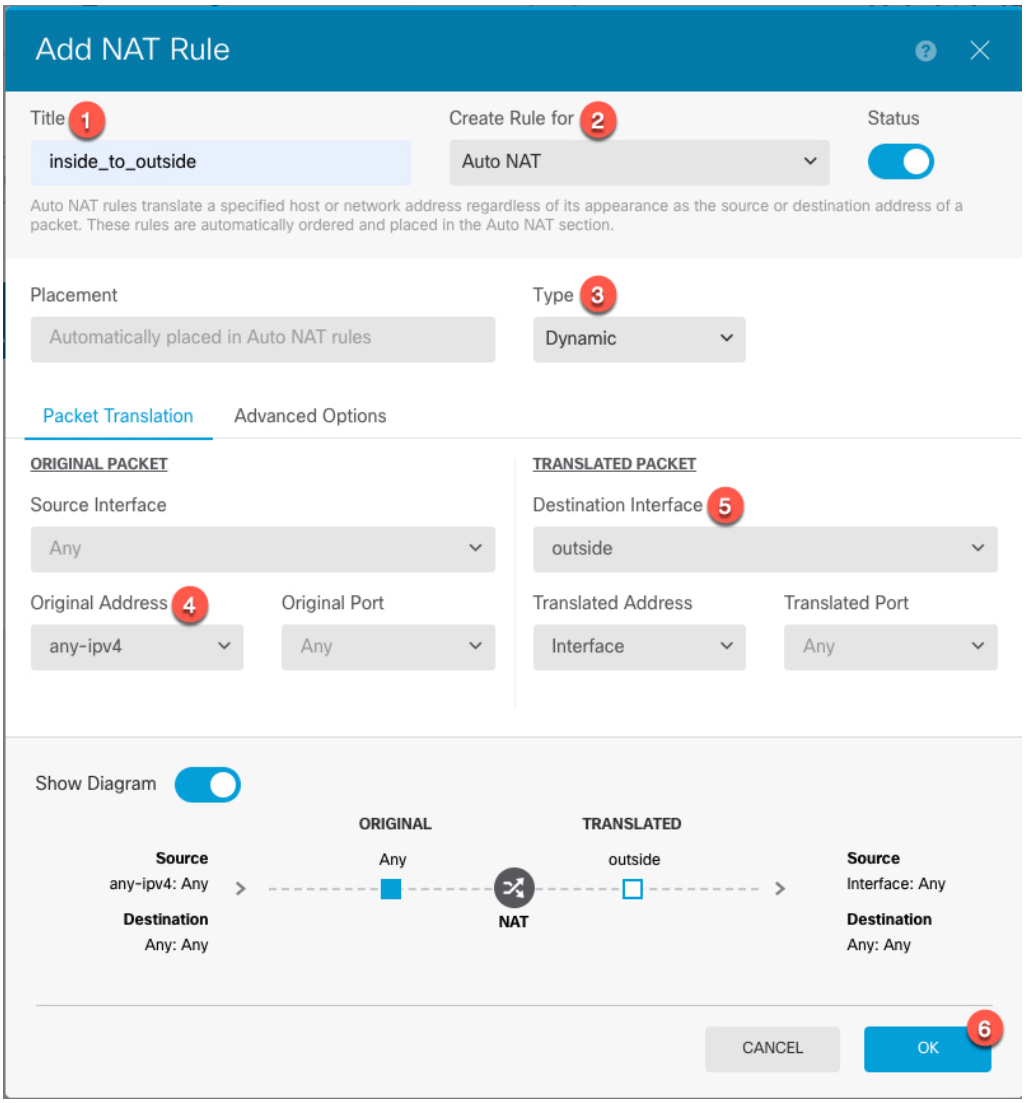
Une règle NAT typique convertit les adresses internes en un port sur l'adresse IP de l'interface externe. Ce type de règle NAT est appelé *interface Port Address Translation (PAT)*. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.

Procédure

Étape 1 Cliquez sur **Policies** (Politiques), puis sur **NAT**.

Étape 2 Cliquez sur + ou **Create NAT Rule** (Créer une règle NAT).

Étape 3 Configurez les options des règles de base :



a) Définissez le **Title** (Titre).
b) Choisissez **Create Rule For (Créer une règle pour)** > **Auto NAT (NAT automatique)**.
c) Choisissez **Type** > **Dynamic (Dynamique)**.

Étape 4 Configurez les options de paquets de traduction suivantes :

a) Pour l'**Original Packet** (Paquet original), définissez l'**Original Address** (Adresse d'origine) sur **any-ipv4**.

Cette règle traduira tout le trafic IPv4 provenant de n'importe quelle interface. Si vous souhaitez restreindre les interfaces ou les adresses, vous pouvez choisir une **Source Interface** (Interface source) spécifique et préciser les adresses IP pour l'**Original Address** (Adresse d'origine).

b) Pour le **Translated Packet** (Paquet traduit), définissez la **Destination Interface** (Interface de destination) sur l'interface externe.

Par défaut, l'adresse IP de l'interface est utilisée pour l'adresse traduite.

Étape 5 (Facultatif) Cliquez sur **Show Diagram** (Afficher le diagramme) pour afficher une représentation visuelle de la règle.

Étape 6 Cliquez sur **OK**.

Permettre le trafic de l'intérieur vers l'extérieur

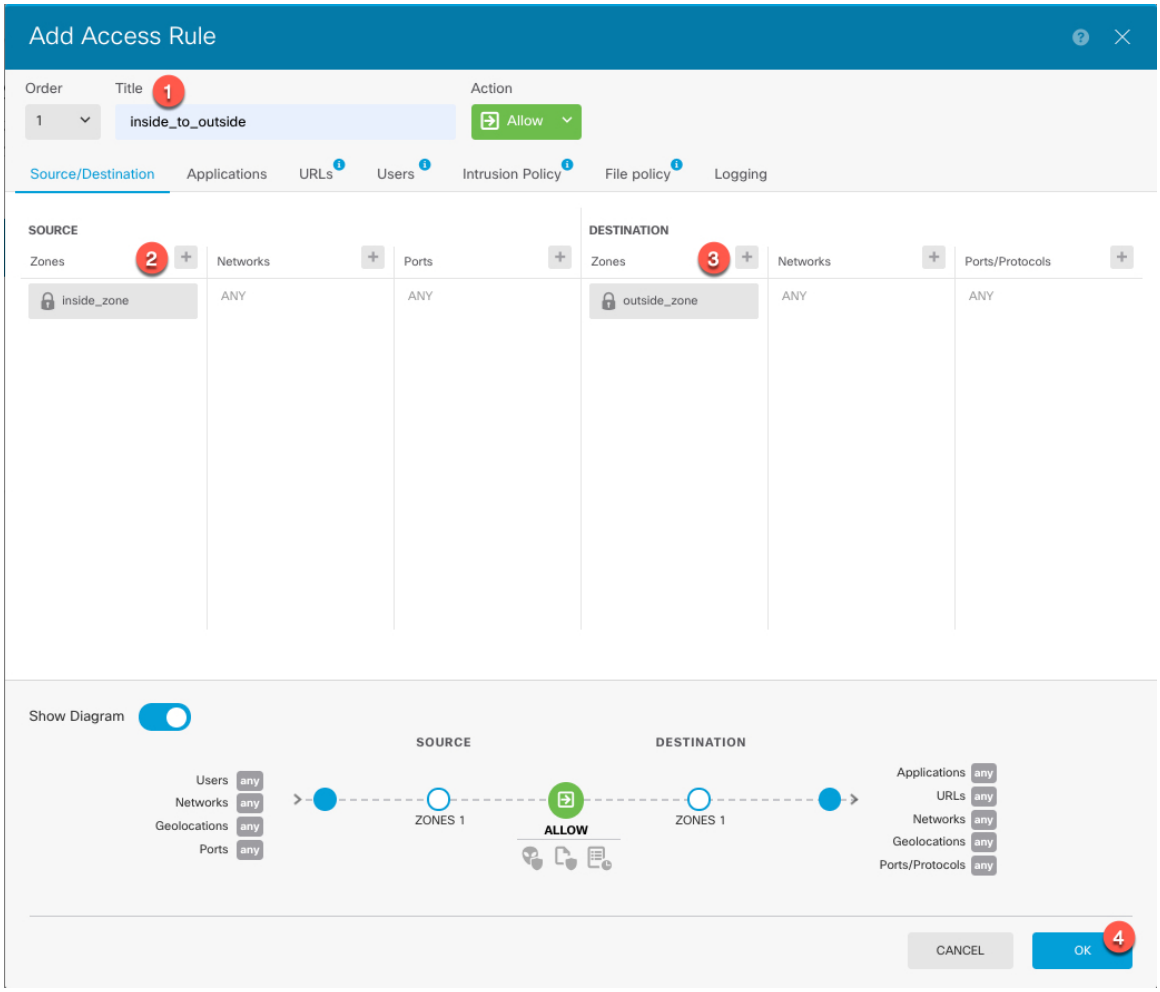
Par défaut, le trafic est bloqué entre les zones de sécurité. Cette procédure montre comment autoriser le trafic de l'intérieur vers l'extérieur.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.

Étape 2 Cliquez sur + ou **Créer une règle d'accès**.

Étape 3 Configurez les options des règles de base :



a) Définissez le **Title** (Titre).

b) Pour **Source**, cliquez sur l'icône **Zones** + et choisissez la zone interne.

c) Pour la **Destination**, cliquez sur l'icône **Zones** + et choisissez la zone externe.
d) (Facultatif) Cliquez sur **Show Diagram** (Afficher le diagramme) pour afficher une représentation visuelle de la règle.
e) Cliquez sur **OK**.

(Facultatif) Configurer le serveur DHCP

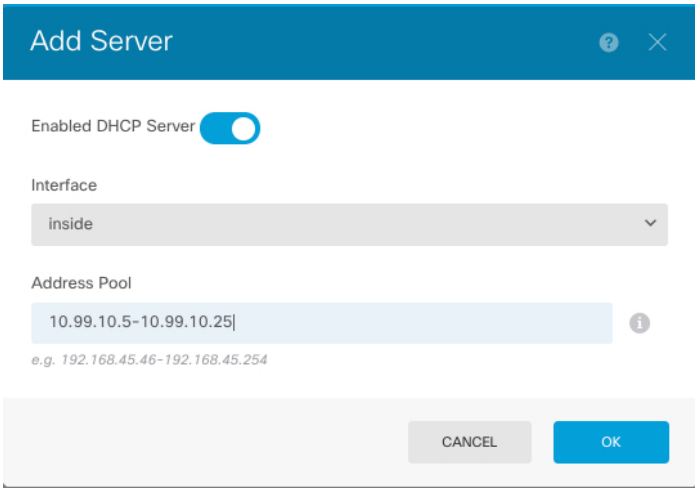
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de Défense contre les menaces.

Procédure

Étape 1 Cliquez sur **Device** (Dispositif), puis sur le lien **System Settings (Paramètres système)** > **DHCP Server (Serveur DHCP)**.

Étape 2 Cliquez sur + ou **Create DHCP Server** (Créer un serveur DHCP).

Étape 3 Configurez les propriétés du serveur.



a) Cliquez sur le curseur **Enable DHCP Server** (Activer le serveur DHCP) pour qu'il affiche activé ( ).
b) Choisissez l'**Interface** sur laquelle vous souhaitez activer le serveur DHCP.

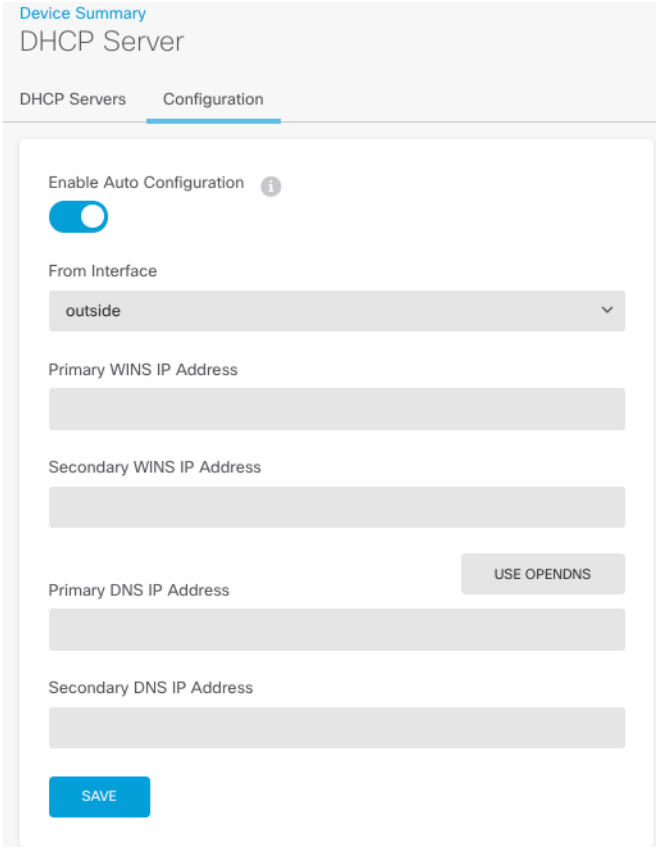
L'interface doit avoir une adresse IP statique; vous ne pouvez pas utiliser DHCP pour obtenir l'adresse de l'interface si vous souhaitez exécuter un serveur DHCP sur l'interface.

c) Saisissez le **Address Pool** (Bassin d'adresses).

La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure : l'adresse IP de l'interface elle-même, l'adresse de diffusion ou l'adresse réseau du sous-réseau.

d) Cliquez sur **OK**.

Étape 4 (Facultatif) Cliquez sur **Configuration**, réglez la configuration automatique et les paramètres globaux.



La configuration automatique DHCP permet au serveur DHCP de fournir aux clients DHCP des informations sur le serveur DNS, le nom de domaine et le serveur WINS obtenues d'un client DHCP qui s'exécute sur l'interface précisée. Généralement, vous utiliseriez la configuration automatique si vous obtenez une adresse en utilisant DHCP sur l'interface externe, mais vous pouvez choisir n'importe quelle interface qui obtient son adresse par le biais de DHCP. Si vous ne pouvez pas utiliser la configuration automatique, vous pouvez définir manuellement les options requises.

a) Cliquez sur le curseur **Enable Auto Configuration** (Activer la configuration automatique) pour qu'il s'affiche comme étant activé ( ).
b) Choisissez l'interface à partir de laquelle vous souhaitez que les clients héritent des paramètres du serveur dans le menu déroulant **From Interface** (Interface d'origine).
c) Si vous n'activez pas la configuration automatique ou si vous souhaitez remplacer l'un des paramètres configurés automatiquement, configurez une ou plusieurs des options globales. Ces paramètres seront envoyés aux clients DHCP sur toutes les interfaces qui fonctionnent sur un serveur DHCP.
d) Cliquez sur **Save** (enregistrer).

(Facultatif) Configurer la passerelle de gestion et autoriser la gestion sur les interfaces de données

Lorsque vous avez déployé défense contre les menaces, vous avez configuré l'adresse de gestion et une passerelle externe. La procédure suivante vous permet de configurer le dispositif de défense contre les menaces

pour envoyer le trafic de gestion sur le fond de panier par l'entremise des interfaces de données plutôt que par l'entremise de l'interface de gestion. Dans ce cas, vous pouvez toujours gérer le dispositif de défense contre les menaces si vous êtes sur un réseau de gestion directement connecté, mais le trafic de gestion destiné à tout autre réseau sera acheminé par l'entremise des interfaces de données plutôt que par l'entremise de la gestion.

De plus, par défaut, vous ne pouvez gérer le dispositif de défense contre les menaces que par l'entremise de l'interface de gestion (gestionnaire d'appareil ou accès à l'interface de ligne de commande). La procédure suivante vous permet également d'activer la gestion sur une ou plusieurs interfaces de données. Notez que la passerelle de l'interface de gestion n'affecte pas le trafic de gestion gestionnaire d'appareil sur les interfaces de données; dans ce cas, le dispositif de défense contre les menaces utilise la table de routage normale.

Avant de commencer

Configurer les interfaces de données conformément à Interfaces de configuration, à la page 76.

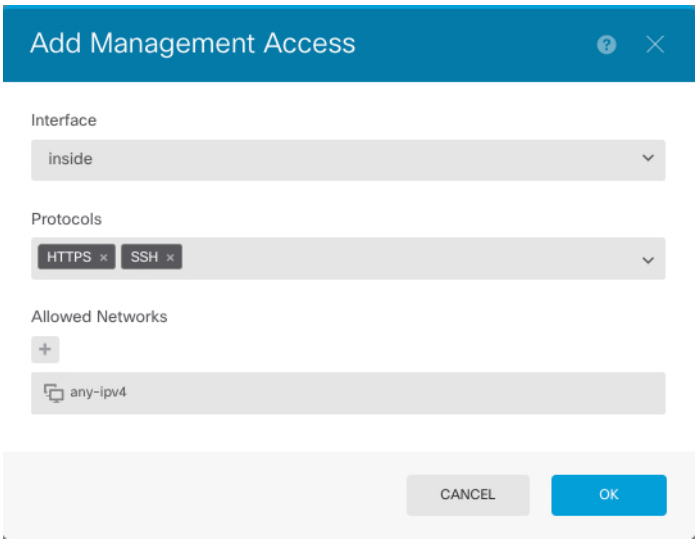
Procédure

Étape 1 Autoriser la gestion à partir d'une interface de données.

a) Cliquez sur **Device** (dispositif), puis cliquez sur le lien**System Settings** > **Management Access**.

b) Cliquez sur **Data Interfaces** (Interfaces de données).

c) Cliquez sur + ou **Create Data Interface** (Créer une interface de données), et créez une règle pour chaque interface :



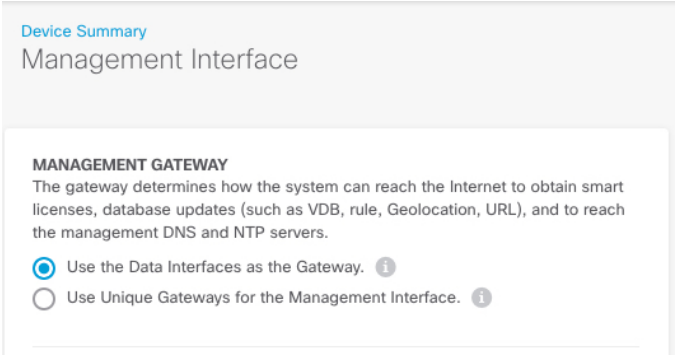
- **Interface** : sélectionnez l'interface sur laquelle vous souhaitez autoriser l'accès de gestion.
- **Protocols** (Protocoles) : indiquez si la règle est pour HTTPS (port 443), pour SSH (port 22) ou les deux.
- **Allowed Networks** (Réseaux permis) : sélectionnez les objets réseau qui définissent le réseau ou l'hôte IPv4 ou IPv6 qui devrait pouvoir accéder au système. Pour spécifier la sélection de « toute » adresse, sélectionnez **any-ipv4** (0.0.0.0/0) et **any-ipv6** (::/0).

d) Cliquez sur **OK**.

Étape 2 Définissez la passerelle de gestion sur les interfaces de données.

a) Cliquer sur **l'appareil**, puis cliquez sur **Systems Settings (paramètres systèmes) du lien de** > **l'interface de gestion**.

b) Sélectionnez **Use the Data Interfaces as the Gateway** (Utilisez les interfaces de données comme passerelle).



c) Cliquez sur **Save (Enregistrer)**, lisez l'avertissement, puis cliquez sur **OK**.

Déployer la configuration

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

Procédure

Étape 1 Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

L'icône est mise en évidence avec un point lorsqu'il y a des modifications non déployées.

La fenêtre Pending Changes (modifications en attente) affiche une comparaison de la version déployée de la configuration avec les modifications en attente. Ces modifications sont codées par couleur pour indiquer les éléments supprimés, ajoutés ou modifiés. Consultez la légende dans la fenêtre pour obtenir une explication des couleurs.

Étape 2 Si vous êtes satisfait des modifications, vous pouvez cliquer sur **Deploy Now** (déployer maintenant) pour lancer le travail immédiatement.

La fenêtre montrera que le déploiement est en cours. Vous pouvez fermer la fenêtre ou attendre la fin du déploiement. Si vous fermez la fenêtre alors que le déploiement est en cours, le travail ne s'arrête pas. Vous pouvez voir les résultats dans la liste des tâches ou dans le journal d'audit. Si vous laissez la fenêtre ouverte, cliquez sur le lien **Deployment History** (historique de déploiement) pour afficher les résultats.

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

Vous pouvez utiliser l'interface de ligne de commande de Défense contre les menaces pour modifier les paramètres de l'interface de gestion et à des fins de dépannage. Vous pouvez accéder à l'interface de ligne de commande en utilisant SSH sur l'interface de gestion, ou en vous connectant à partir de l'interface de ligne de commande FXOS.

Procédure

Étape 1 (Option 1) SSH directement lié à l'adresse IP de l'interface de gestion de Défense contre les menaces.

Vous avez défini l'adresse IP de gestion lorsque vous avez déployé le dispositif logique. Connectez-vous à Défense contre les menaces avec le compte administrateur et le mot de passe que vous avez définis lors du déploiement initial.

Si vous avez oublié le mot de passe, vous pouvez le modifier en modifiant le dispositif logique dans le dossier de l'entreprise gestionnaire de châssis.

Étape 2 (Option 2) À partir de l'interface de ligne de commande de FXOS, connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

a) Connectez-vous au security module.

connect module *numéro_de_logement* {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connectez-vous à la console de Défense contre les menaces.

connect ftd *nom*

Si vous avez plusieurs instances d'application, vous devez préciser le nom de l'instance. Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
```

```
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
==========================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **exit**.

Remarque
Pour les versions antérieures à la version 6.3, entrez **Ctrl-a, d**.

d) Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Pour quitter la console :

1. Entrez **~**

   Vous quittez l'application Telnet.

2. Pour quitter l'application Telnet, entrez :

   telnet>**quit**

Pour quitter la session Telnet :

Entrez **Ctrl-], .**

Exemple

L'exemple suivant se connecte à Défense contre les menaces sur le module de sécurité 1 et repart au niveau superviseur de Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
```

```
'connect module <slot> telnet' to connect to the security module.
==================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

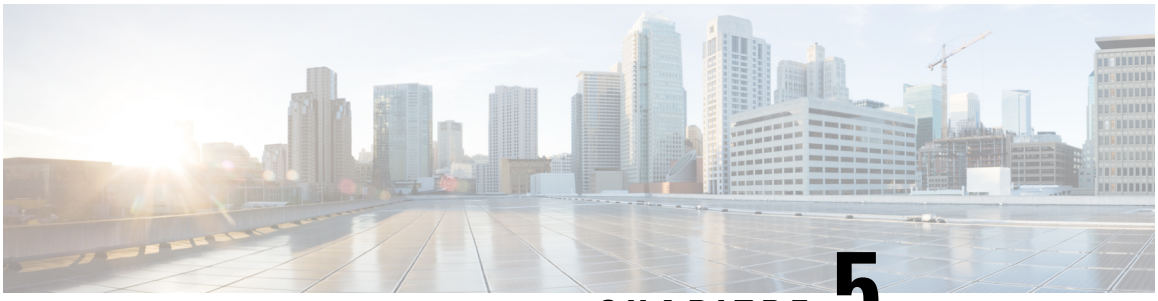
Quelle est l'étape suivante?

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

Pour des informations relatives à l'utilisation de gestionnaire d'appareil, consultez Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager.

Historique pour Défense contre les menaces avec le Gestionnaire d'appareil

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge de gestionnaire d'appareil avec les instances natives	6.5.0	Vous pouvez maintenant déployer une instance native à l'aide du gestionnaire d'appareil. Écrans Nouveaux ou modifiés : **Logical Devices (Dispositifs logiques)** > **Add Device (Ajouter un dispositif)** **Remarque** Nécessite FXOS 2.7.1.



CHAPITRE 5

Défense contre les menaces Déploiement avec CDO

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

Pour voir tous les systèmes d'exploitation et gestionnaires disponibles, consultez Quels sont le système d'exploitationet le gestionnaire d'applications pour vous?, à la page 1. Ce chapitre s'applique à Défense contre les menaces utilisant Cisco Defense Orchestrator fournis dans le nuage (cDO) Cisco Secure Firewall Management Center. Pour utiliser CDO à l'aide de fonctionnalités gestionnaire d'appareil, consultez la documentation de CDO.

Remarque La version infonuagique centre de gestionprend en chargeDéfense contre les menaces la version 7.2 et les versions ultérieures. Pour les versions antérieures, vous pouvez utiliser les fonctionnalités de CDO gestionnaire d'appareil. Toutefois, le mode gestionnaire de dispositifs n'est disponible que pour les utilisateurs existants de CDO qui gèrent déjà les Défense contre les menaces qui utilisent ce mode.

Chaque Défense contre les menaces contrôle, inspecte, surveille et analyse le trafic. CDO fournit une console de gestion centralisée avec une interface Web que vous pouvez utiliser pour effectuer des tâches d'administration et de gestion au service de la sécurisation de votre réseau local.

À propos du pare-feu

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

Le pare-feu exécute un système d'exploitation sous-jacent appelé le Cisco Secure Firewall eXtensible Operating System (FXOS). Le pare-feu ne prend pas en charge le Cisco Secure Firewall chassis manager FXOS; seule une interface de ligne de commande limitée est prise en charge à des fins de dépannage. Consultez la section Guide de dépannage Cisco FXOS pour Firepower 1000/2100 et Secure Firewall 3100 avec Firepower Threat Defense pour obtenir plus de renseignements.

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

À propos de la gestion par CDODéfense contre les menaces

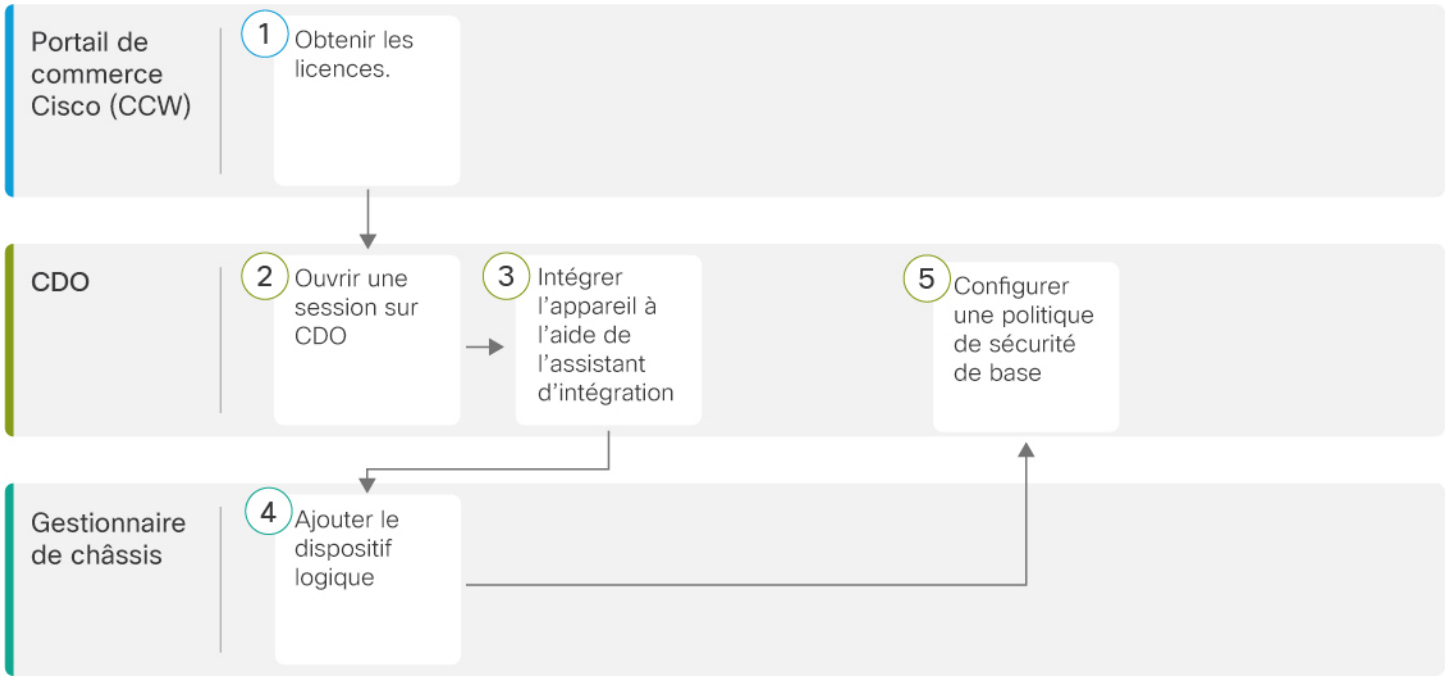
La solution infonuagique centre de gestion centre de gestion offre bon nombre des mêmes fonctions qu'une solution centre de gestion locale et présente la même apparence. Lorsque vous utilisez CDO en tant que gestionnaire principal, vous pouvez utiliser un centre de gestion local à des fins d'analyse uniquement. Le centre de gestion local ne prend pas en charge la configuration ou la mise à niveau des politiques.

Remarque CDO ne prend pas en charge les instances ou les grappes de contenant.

Procédure de bout en bout

Consultez les tâches suivantes pour préparer le dispositif de défense contre les menaces au CDO à l'aide de l'assistant de préparation.

Illustration 10 : Procédure de bout en bout



1	Portail de commerce Cisco (CCW)	Obtenir des licences, à la page 95.
2	CDO	Ouvrez une session sur CDO, à la page 97.
3	CDO	Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 101.
4	Gestionnaire de châssis	Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 103.
5	CDO	Configurer une politique de sécurité de base, à la page 46.

Obtenir des licences

Toutes les licences sont fournies au Défense contre les menaces par le CDO. Vous pouvez également acheter les licences de fonctionnalités suivantes :

- **Threat (menace)** : Renseignements sur la sécurité et IPS de nouvelle génération
- **Défense contre les programmes malveillants** : défense contre les Programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **Cisco Secure Client** :Secure Client Advantage, Secure Client Premier, ou Secure Client VPN Only

- **Opérateur** : Diamètre, GTP/GPRS, M3UA, SCTP

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

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

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

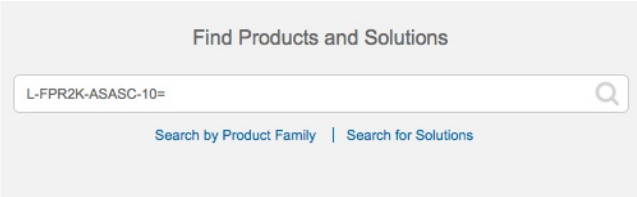
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

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

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

Illustration 11 : Recherche de licences



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

- Combinaison de licences englobant IPS, les , la défense contre les programmes malveillants et les URL :
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

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

  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y

- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.
- Licence d'opérateur :
  - L-FPR9K-FTD-CAR=

Étape 2 Si vous ne l'avez pas encore fait, enregistrez le CDO auprès du gestionnaire de logiciels intelligent.

Pour vous enregistrer, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Consultez la documentation de CDO pour des instructions détaillées.

Ouvrez une session sur CDO

CDO utilise Cisco Secure Sign-On comme fournisseur d'identité et Duo Security pour l'authentification multi-facteurs (MFA). CDO nécessite l'authentification multi-facteurs (MFA), qui offre une couche de sécurité supplémentaire pour protéger votre identité d'utilisateur. L'authentification à deux facteurs, un type de MFA, requiert deux composants, ou facteurs, pour confirmer l'identité de l'utilisateur qui se connecte à CDO.

Le premier facteur est un nom d'utilisateur et un mot de passe, et le second est un mot de passe à usage unique (OTP), qui est généré à la demande par Duo Security.

Après avoir établi vos identifiants Cisco Secure Sign-On, vous pouvez vous connecter à CDO à partir de votre tableau de bord Cisco Secure Sign-On. Depuis le tableau de bord Cisco Secure Sign-On, vous pouvez également vous connecter à n'importe quel autre produit Cisco pris en charge.

- Si vous avez un compte Cisco Secure Sign-On, passez directement à Ouvrez une session sur CDO avec la connexion sécurisée Cisco Secure Sign-On., à la page 100.
- Si vous n'avez pas un compte Cisco Secure Sign-On, passez à Créer un nouveau compte de connexion Cisco Secure, à la page 97.

Créer un nouveau compte de connexion Cisco Secure

Le flux de travail de connexion initiale est un processus en quatre étapes. Vous devez effectuer les quatre étapes.

Avant de commencer

- **Install DUO Security** (installer la sécurité DUO) Nous vous recommandons d'installer l'application Duo Security sur un téléphone mobile. Consultez le guide Duo d'authentification à deux facteurs (guide d'inscription) (Duo Guide to Two Factor Authentication: Enrollment Guide) si vous avez des questions sur l'installation de Duo.

- **Time Synchronization** (synchronisation de l'heure) : Vous allez utiliser votre appareil mobile pour générer un mot de passe à usage unique. Il est important que l'horloge de votre appareil soit synchronisée avec le temps réel, car l'OTP est basé sur le temps. Faites en sorte que l'horloge de votre appareil soit réglée à l'heure exacte.
- Utilisez une version actuelle de Firefox ou de Chrome.

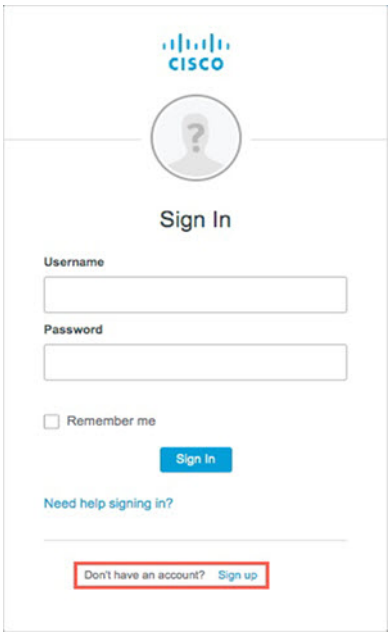
Procédure

Étape 1 **Inscrivez-vous pour un nouveau compte Cisco Secure Sign-On.**

a) Rendez-vous sur https://sign-on.security.cisco.com.

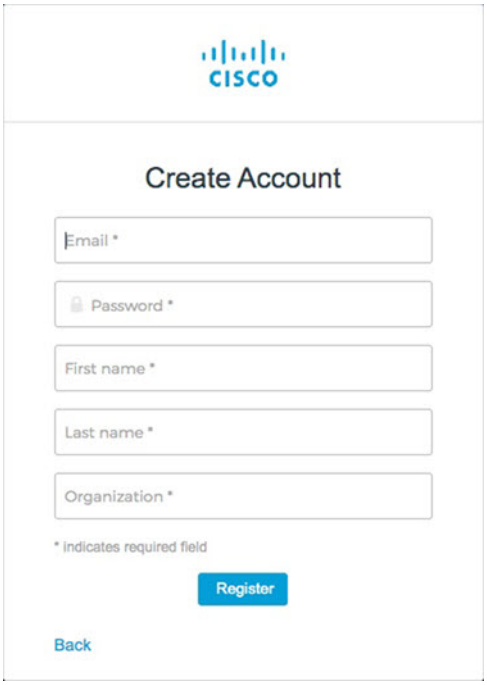
b) Au bas de l'écran de connexion, cliquez sur **Sign up** (s'inscrire).

Illustration 12 : Inscription à Cisco SSO



c) Remplissez les champs de la boîte de dialogue **Create Account** (créer un compte) et cliquez sur **Register** (enregistrer).

Illustration 13 : Créer un compte



Astuces
Entrez l'adresse électronique que vous prévoyez d'utiliser pour vous connecter à CDO et ajoutez un nom d'organisation pour représenter votre entreprise.

d) Après avoir cliqué sur **Register** (enregistrer), Cisco vous envoie un courriel de vérification à l'adresse avec laquelle vous vous êtes inscrit. Ouvrez le courriel et cliquez sur **Activate Account** (activer le compte).

Étape 2 **Configurez l'authentification multifacteurs à l'aide de Duo.**

a) Dans l'écran **Set up multi-factor authentication** (configurer l'authentification multifacteur), cliquez sur **Configure** (configurer).
b) Cliquez sur **Start setup** (démarrer la configuration) et suivez les invites pour choisir un appareil et vérifier l'appariement de cet appareil avec votre compte.

Pour en savoir plus, consultez le Guide to Two Factor Authentication: Enrollment Guide. Si vous avez déjà l'application Duo sur votre appareil, vous recevrez un code d'activation pour ce compte. Duo prend en charge plusieurs comptes sur un seul appareil.

c) À la fin de la configuration avec l'assistant, cliquez sur **Continue to Login** (continuer la connexion).
d) Connectez-vous à Cisco Secure Sign-On avec l'authentification à deux facteurs.

Étape 3 (Facultatif) **Configurez Google Authenticator comme authentificateur supplémentaire.**

a) Choisissez l'appareil mobile que vous jumelez avec Google Authenticator, puis cliquez sur **Next** (suivant).
b) Suivez les invites de l'assistant de configuration pour configurer Google Authenticator.

Étape 4 **Configurez les options de récupération de compte pour votre compte Cisco Secure Sign-On.**

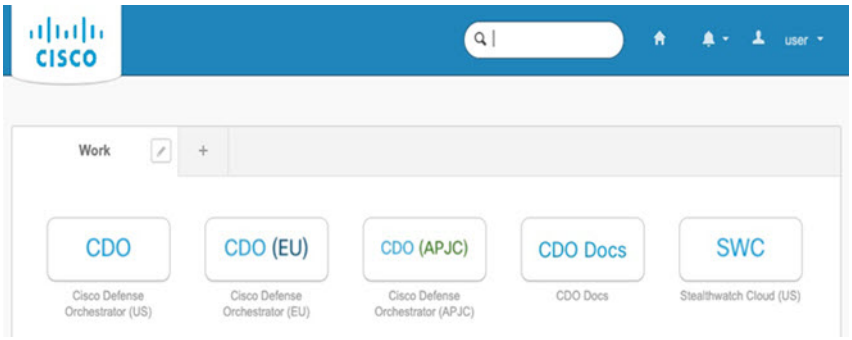
a) Choisissez une question et un mot de passe en cas d'oubli de mot de passe.
b) Choisissez un numéro de téléphone de récupération pour réinitialiser votre compte par SMS.
c) Choisissez une image de sécurité.

d) Cliquez sur **Create My Account** (créer mon compte).

Vous voyez maintenant le tableau de bord Cisco Security Sign-On avec les vignettes de l'application CDO. Vous pouvez également voir d'autres tuiles d'applications.

Astuces
Vous pouvez faire glisser les vignettes sur le tableau de bord pour les classer à votre guise, créer des onglets pour regrouper les vignettes et renommer les onglets.

Illustration 14 : Tableau de bord Cisco SSO



Ouvrez une session sur CDO avec la connexion sécurisée Cisco Secure Sign-On.

Connectez-vous à CDO pour la préparation et la gestion de votre appareil.

Avant de commencer

Cisco Defense Orchestrator (CDO) utilise Cisco Secure Sign-On comme fournisseur d'identité et Duo Security pour l'authentification multi-facteurs (MFA).

- Pour vous connecter à CDO, vous devez d'abord créer votre compte dans Cisco Secure Sign-On et configurer MFA à l'aide de Duo; voir Créer un nouveau compte de connexion Cisco Secure, à la page 97.
- Utilisez une version actuelle de Firefox ou de Chrome.

Procédure

Étape 1 Dans un navigateur Web, accédez à https://sign-on.security.cisco.com/.

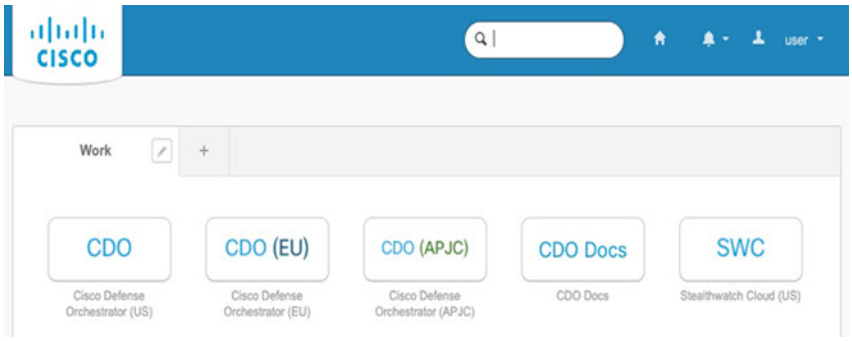
Étape 2 Saisissez votre nom d'utilisateur (**Username**) et votre mot de passe Cisco **Password**.

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

Étape 4 Recevez un autre facteur d'authentification avec Duo Security et confirmez votre connexion. Le système confirme votre connexion et affiche le tableau de bord Cisco Secure Sign-On.

Étape 5 Cliquez sur la vignette CDO appropriée sur le tableau de bord Cisco Secure Sign-on. La tuile **CDO** vous dirige vers https://defenseorchestrator.com, la tuile **CDO (UE)** vous dirige vers https://defenseorchestrator.eu et la tuile **CDO (APJC)** vous dirige vers https://www.apj.cdo.cisco.com.

Illustration 15 : Tableau de bord Cisco SSO



Étape 6 Cliquez sur le logo de l'authentificateur pour sélectionner **Duo Security** ou **Google Authenticator**, si vous avez configuré les deux authentifiants.

- Si vous avez déjà un enregistrement utilisateur sur un locataire existant, vous êtes connecté à ce locataire.
- Si vous avez déjà un enregistrement utilisateur sur plusieurs locataires, vous pourrez choisir le locataire CDO avec lequel la connexion doit s'établir.
- Si vous n'avez pas encore d'enregistrement utilisateur sur un locataire existant, vous pourrez en savoir plus sur CDO ou demander un compte d'essai.

Préparation d'un appareil avec Onboarding Wizard (assistant de préparation)

Intégrez le à l'aide de l'assistant de préparation de CDO à l'aide d'une clé d'enregistrement CLI.défense contre les menaces

Procédure

Étape 1 Dans le volet de navigation de CDO, cliquez sur **Inventory inventory)** , puis sur le bouton bleu plus ( ) pour la **Préparation** d'un appareil.

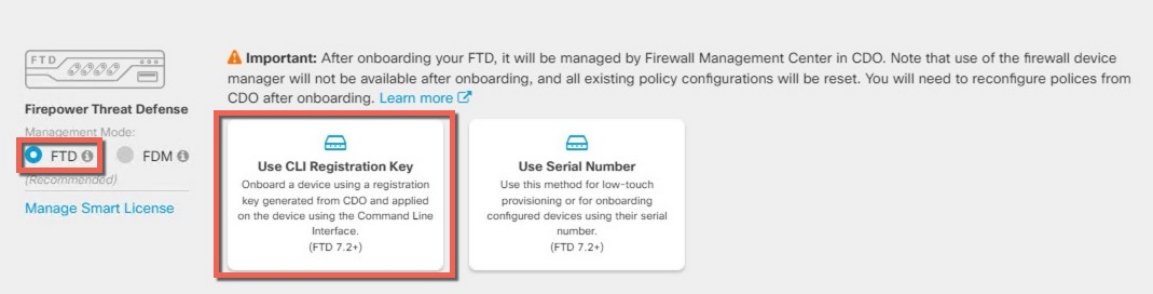
Étape 2 Sélectionnez la vignette **FTD**.

Étape 3 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné.

À tout moment, après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Manage Smart License (gérer la licence Smart)** pour inscrire ou modifier les licences Smart existantes disponibles pour votre appareil. Consultez pour savoir quelles licences sont disponibles.Obtenir des licences, à la page 95

Étape 4 Sélectionnez **Use CLI Registration Key (Utiliser la clé d'enregistrement de l'interface de ligne de commande)** comme méthode de préparation.

Illustration 16 : Utiliser la clé d'enregistrement de l'interface de ligne de commande



Étape 5 Saisissez le **nom du dispositif**, puis cliquez sur **Next (suivant)**.

Étape 6 Pour **l'affectation de politique**, utilisez le menu déroulant pour choisir une politique de contrôle d'accès pour le dispositif. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 7 Pour la **licence par abonnement**, cliquez sur le bouton radio **Physical FTD Device (appareil physique FTD)**, puis cochez chacune des licences de fonctionnalité que vous souhaitez activer. Cliquez sur **Next** (suivant).

Étape 8 Pour la **clé d'enregistrement de l'interface de ligne de commande**, CDO génère une commande avec la clé d'enregistrement et d'autres paramètres. Vous devez copier cette commande et l'utiliser dans la configuration initiale du.défense contre les menaces

configure manager add *cdo_hostname registration_key nat_id display_name*

Dans le gestionnaire de châssis lorsque vous déployez le dispositif logique (consultez Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 103), copiez ceci

Exemple :

Exemple de commande :

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

Étape 9 Cliquez sur **Next (suivant)** dans l'assistant de préparation pour commencer l'enregistrement de l'appareil.

Étape 10 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu plus (+). Les étiquettes sont appliquées au dispositif après son intégration à CDO.

Prochaine étape

Sur la page **d'inventaire**, sélectionnez le dispositif que vous venez d'intégrer et sélectionnez l'une des options répertoriées sous le volet de **gestion** situé à droite.

Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces

Vous pouvez déployer le dispositif de défense contre les menaces à partir du Firepower 9300 en tant qu'instance native autonome. CDO ne prend pas en charge les instances ou les grappes de contenant.

Cette procédure vous permet de configurer les caractéristiques logiques du dispositif, y compris la configuration de démarrage utilisée par l'application.

Avant de commencer

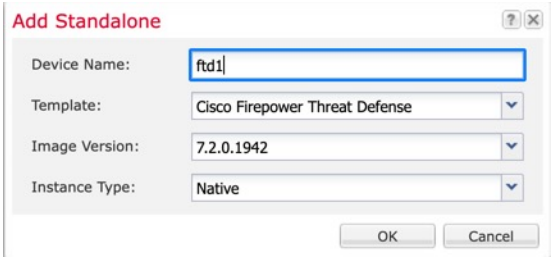
- Configurer l'interface de gestion à utiliser avec défense contre les menaces; voir Interfaces de configuration, à la page 24. L'interface de gestion est requise. Vous pouvez activer ultérieurement la gestion à partir d'une interface de données; mais vous devez affecter une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données. Il convient de souligner que cette interface de gestion est différente du port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**).
- Vous devez également configurer au moins une interface de données.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce dispositif
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - Nom d'hôte de CDO, clé d'enregistrement et ID de NAT généré par CDO. Consultez Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 101.
  - l'adresse IP du serveur DNS

Procédure

Étape 1 Dans gestionnaire de châssis, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur **Add** > **Standalone**, puis définissez les paramètres suivants :

Illustration 17 : Ajouter un dispositif autonome



a) Indiquez un nom de dispositif (**Device Name**).

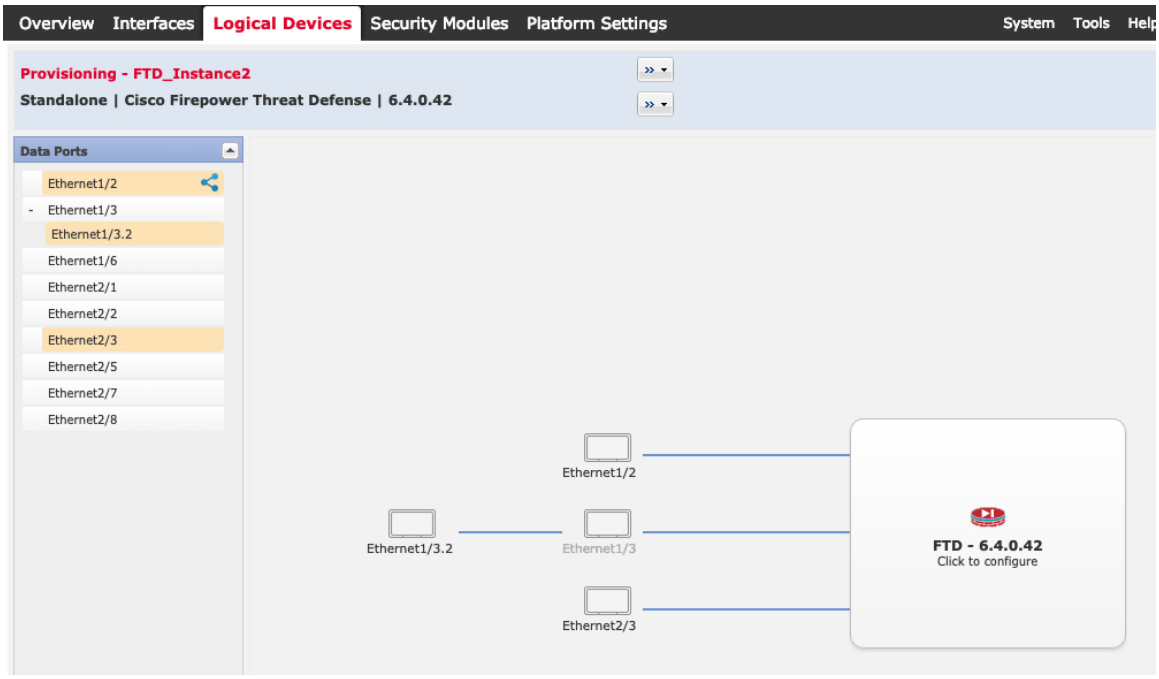
Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de dispositif utilisé dans la configuration de l'application.

Remarque
Vous ne pouvez pas modifier ce nom après avoir ajouté le dispositif logique.

b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
c) Choisissez la version de l'image (**Image Version**).
d) Choisissez l'**Instance Type (Type d'instance)** : **Native (Instance native)**.
e) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du dispositif).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au dispositif.



Vous ne pouvez attribuer que des interfaces de données que vous avez préalablement activées sur la page **Interfaces**. Vous pourrez ensuite activer et configurer ces interfaces dans CDO, y compris pour ce qui concerne la définition des adresses IP.

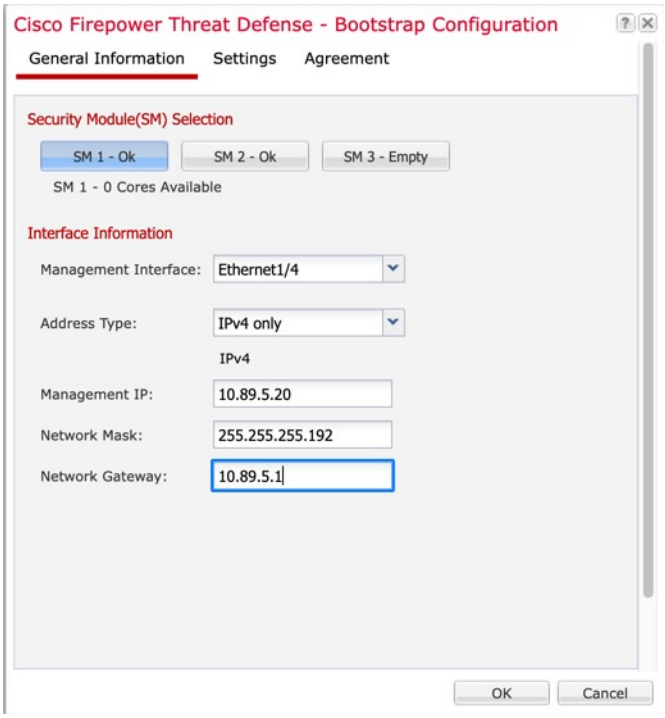
Hardware Bypass : Les ports compatibles sont représentés par l'icône suivante : . Pour certains modules d'interface, vous pouvez activer la fonction de contournement matériel pour les interfaces d'ensemble en ligne uniquement. Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Si vous n'affectez pas les deux interfaces dans une paire de Hardware Bypass, un message d'avertissement s'affiche pour vous assurer que votre affectation est intentionnelle. Vous n'avez pas besoin d'utiliser la fonctionnalité Hardware Bypass, vous pouvez donc affecter des interfaces uniques si vous préférez.

Étape 4 Cliquez sur l'icône de dispositif au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :

Illustration 18 : Renseignements généraux



a) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce dispositif logique.
b) Choisissez l'interface de gestion (**Management Interface**).

   Cette interface est utilisée pour gérer le dispositif logique. Cette interface est distincte du port de gestion du châssis.

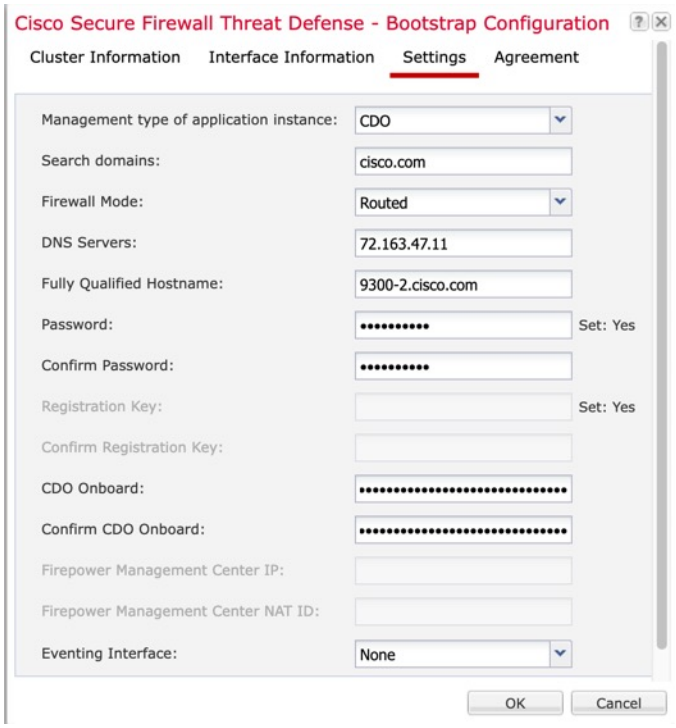
c) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).
d) Configurez l'adresse IP de gestion (**Management IP**).

   Définissez une adresse IP unique pour cette interface.

e) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).
f) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Sous l'onglet **Settings** (paramètres), procédez comme suit :

Illustration 19 : Paramètres



a) Dans la liste déroulante **Management type of application instance** (Type de gestion de l'instance d'application), choisissez **CDO**.
b) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.
c) Choisissez le mode du pare-feu (**Firewall Mode**) : **Transparent** ou **Routed** (routage).

   En mode routage, l'défense contre les menaces est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

   Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

d) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont séparés par des virgules.

   Par exemple, défense contre les menaces utilise DNS si vous spécifiez un nom d'hôte pour centre de gestion.

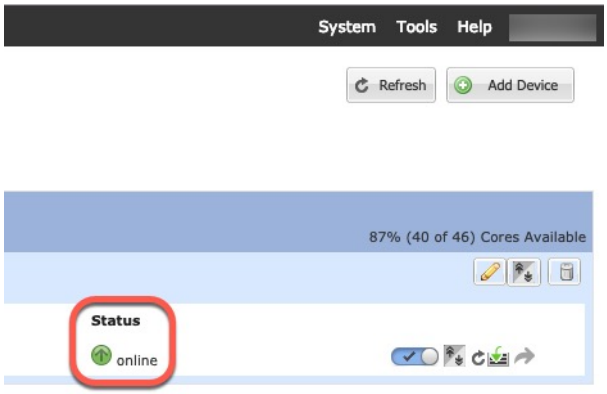
e) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour défense contre les menaces.
f) Saisissez un mot de passe (**Password**) pour l'utilisateur admin défense contre les menaces pour l'accès à l'interface de ligne de commande.
g) Copiez la commande générée par CDO dans les champs **CDO Onboard** (Intégration dans CDO) et **Confirm CDO Onboard** (Confirmer l'intégration dans CDO).
h) Une interface d'événement **Eventing Interface** distincte n'est pas prise en charge pour CDO, donc ce paramètre sera ignoré.

Étape 7 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.

Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (enregistrer).

Le châssis déploie le dispositif logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau dispositif logique dans la page **Logical Devices**. Lorsque le dispositif logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Configurer une politique de sécurité de base

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

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

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

1	Configurer les interfaces, à la page 47.
2	Configurer le serveur DHCP, à la page 50.
3	Ajouter la voie de routage par défaut, à la page 51.

4	Configurer NAT, à la page 53.
5	Permettre le trafic de l'intérieur vers l'extérieur, à la page 56.
6	Déployer la configuration, à la page 57.

Configurer les interfaces

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

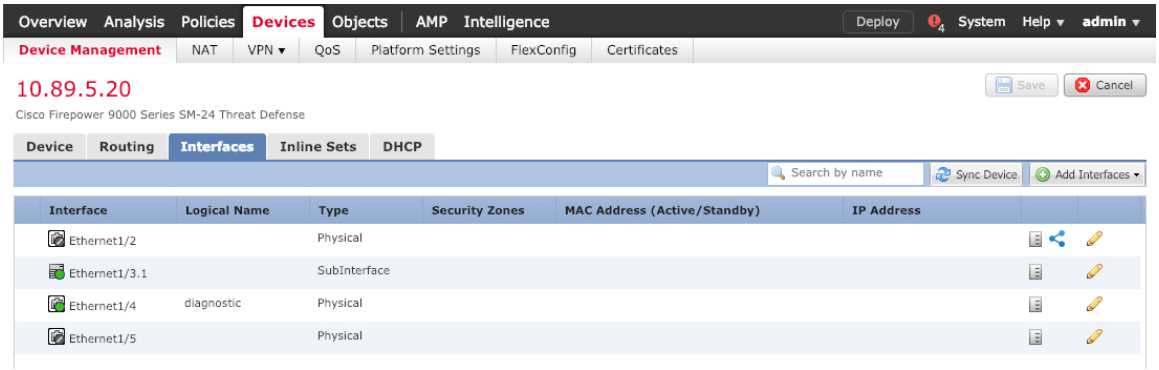
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

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

Procédure

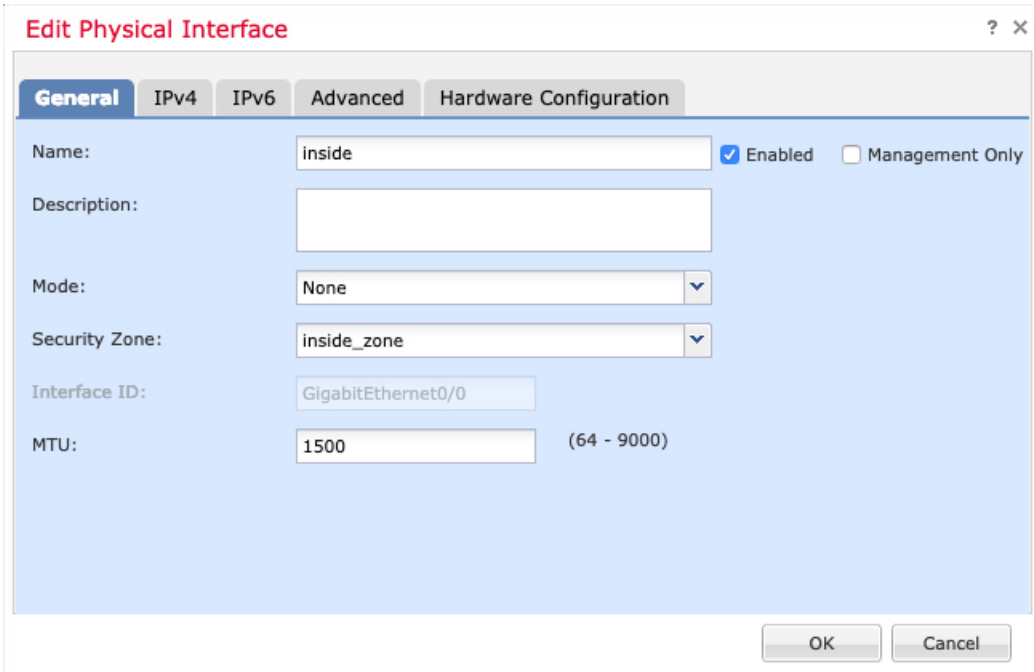
Étape 1 Choisissez **Devices (dispositifs)** > **Device Management (gestion du dispositif)**, et cliquez sur **Modifier** (✎) pour le pare-feu.

Étape 2 Cliquez sur **Interfaces**.



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

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



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

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

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

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

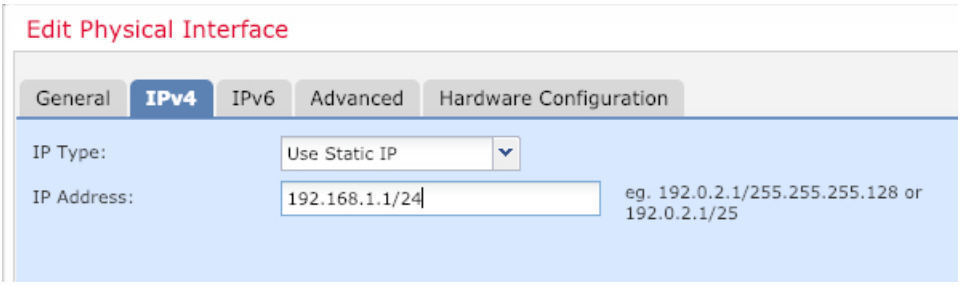
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

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

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

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

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

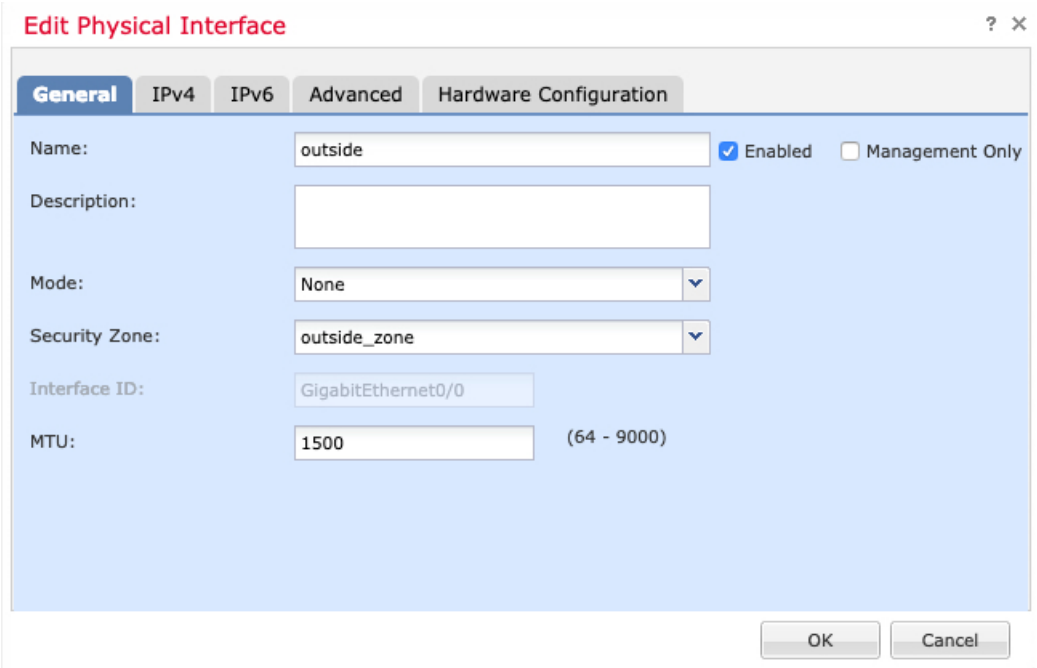


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

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

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



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

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

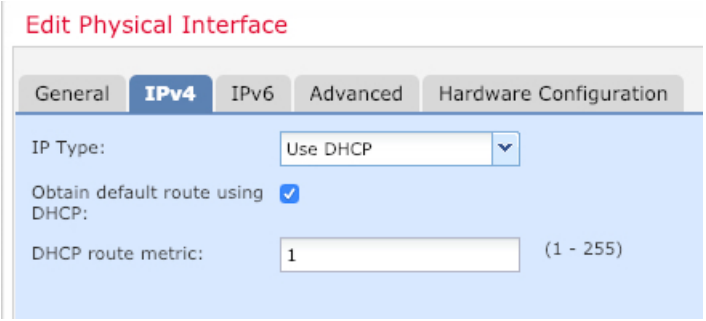
Par exemple, nommez l'interface **externe**.

b) Cochez la case **Enabled** (activer).
c) Laissez le **Mode** défini sur **None** (aucun).
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **New** (nouveau).

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

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

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



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

f) Cliquez sur **OK**.

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

Configurer le serveur DHCP

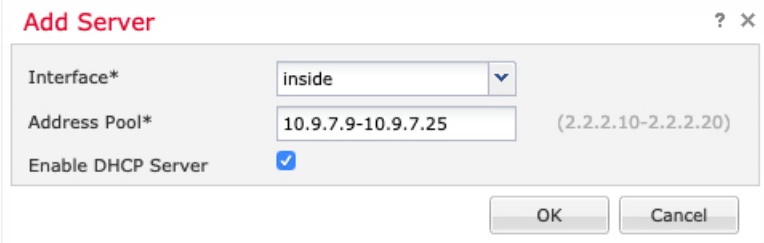
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de Défense contre les menaces.

Procédure

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

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

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



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

Étape 4 Cliquez sur **OK**.

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

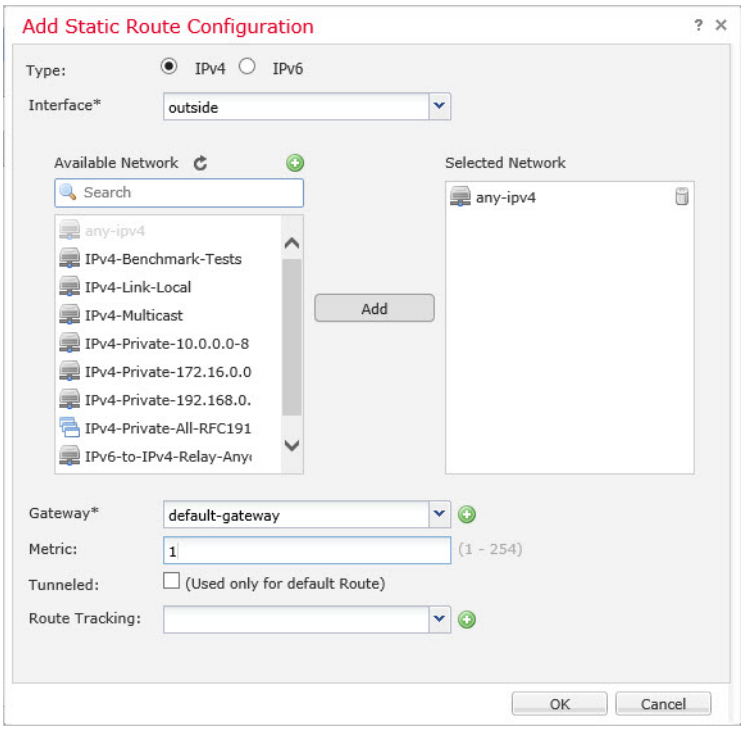
Ajouter la voie de routage par défaut

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

Procédure

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

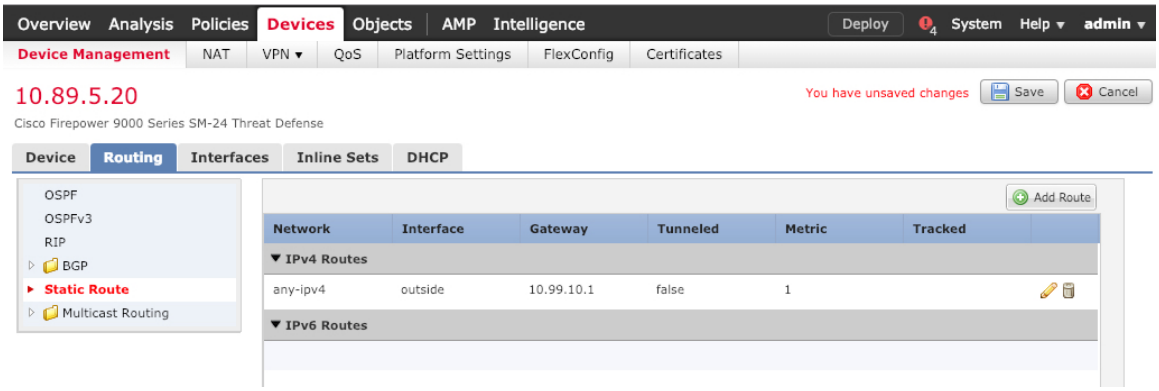
Étape 2 Sélectionnez **Routing (routage)** > **Static Route (route statique)**, cliquez sur **Add Route (ajouter route)**, et définissez ce qui suit :



- **Type** : Cliquez sur le bouton radio **IPv4** ou **IPv6** selon le type de routage statique que vous ajoutez.
- **Interface** : Sélectionnez l'interface de sortie; il s'agit généralement de l'interface externe.
- **Available Network** (réseau disponible) : Choisissez **any-ipv4** pour une voie de routage par défaut IPv4 ou **any-ipv6** pour une voie de routage par défaut IPv6, puis cliquez sur **Add** (ajouter) pour la déplacer vers la liste **Selected Network** (réseau sélectionné).
- **Gateway (passerelle)** ou **IPv6 Gateway (passerelle iPv6)** : Saisissez ou choisissez le routeur de passerelle qui est le prochain saut sur cette voie de routage. Vous pouvez fournir une adresse IP ou un objet réseaux/hôtes.
- **Metric** (nombre) : Saisissez le nombre de sauts sur le réseau de destination. Les valeurs valides vont de 1 à 255; la valeur par défaut est 1.

Étape 3 Cliquez sur **OK**.

La voie est ajoutée à la table de routage statique.



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

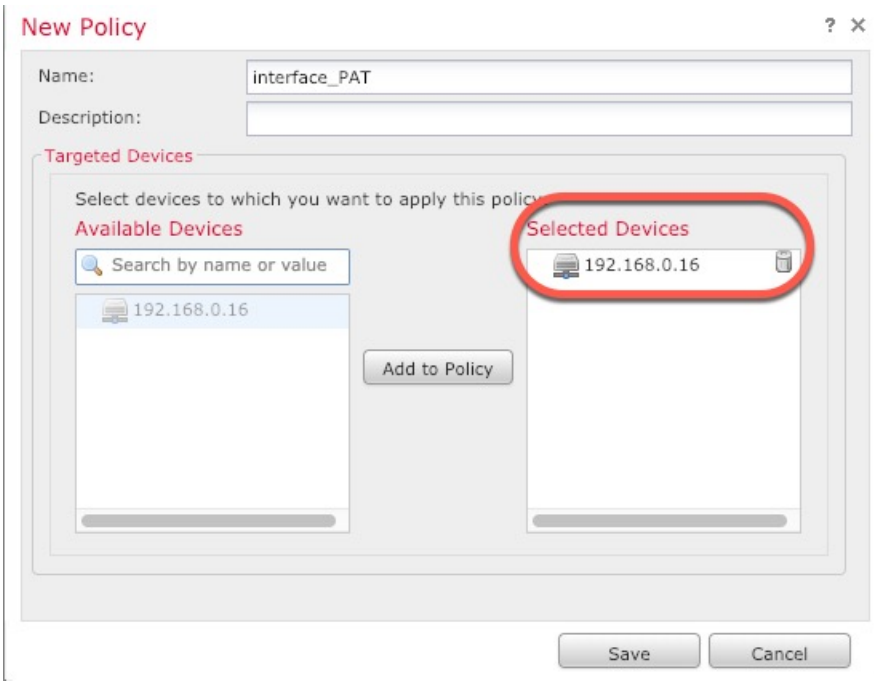
Configurer NAT

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

Procédure

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

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



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

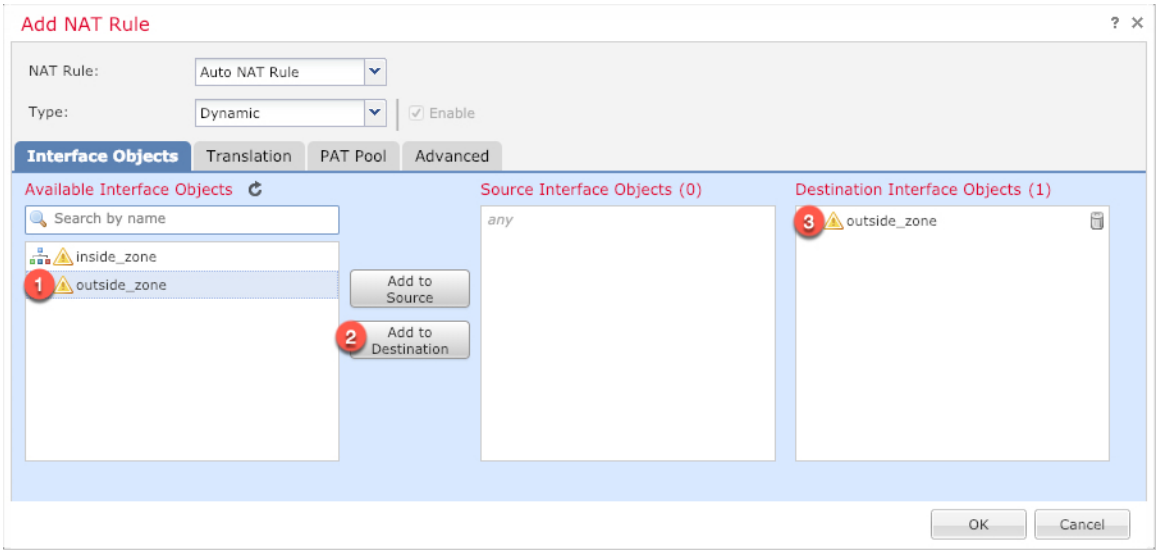
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

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

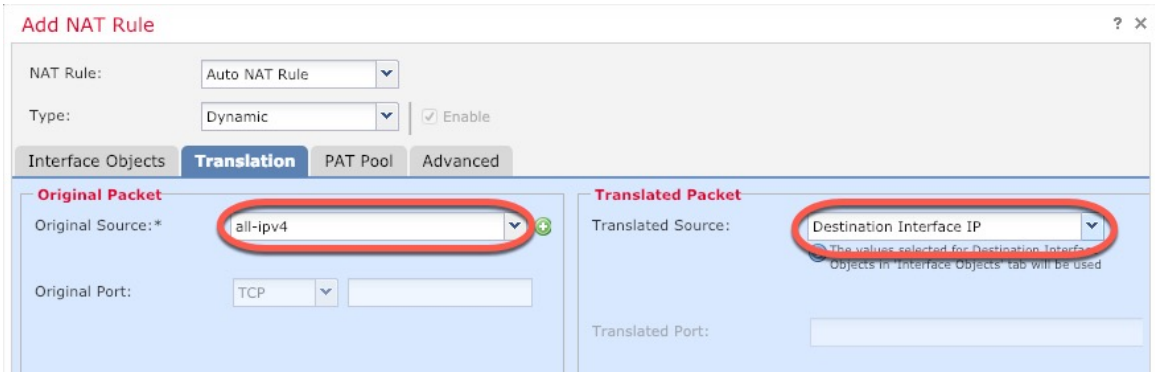
Étape 4 Configurez les options des règles de base :

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

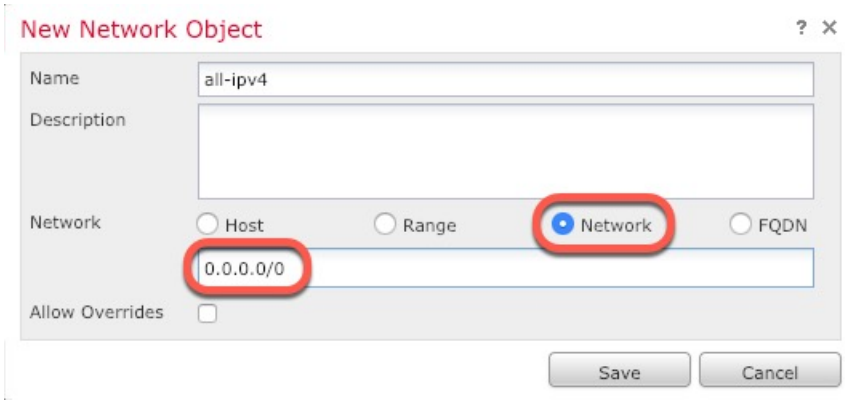
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



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



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

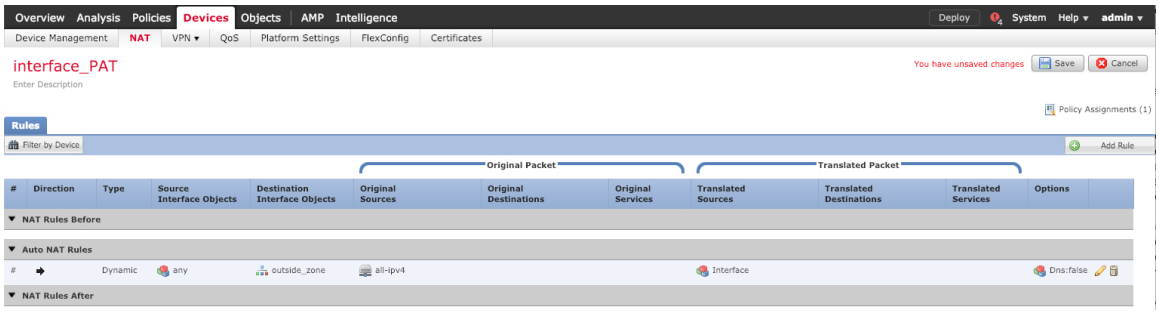


Remarque
Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

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

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

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



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

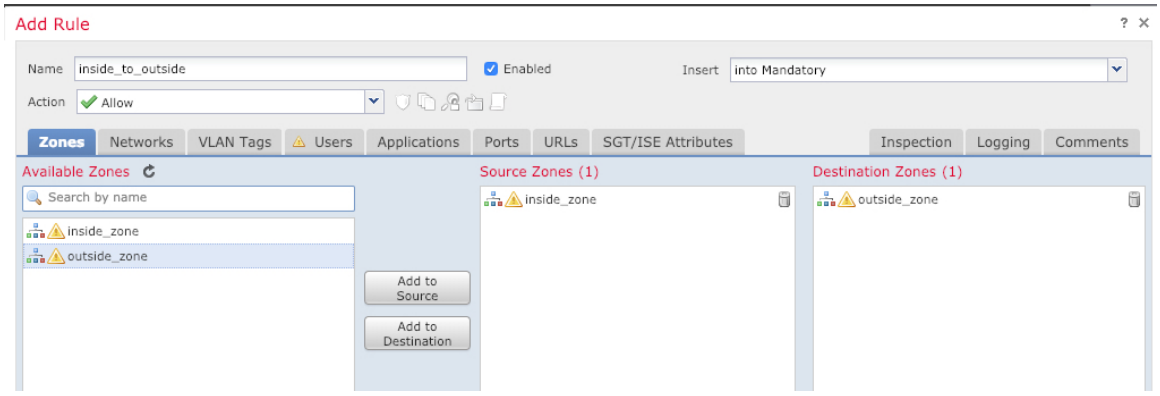
Permettre le trafic de l'intérieur vers l'extérieur

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

Procédure

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

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



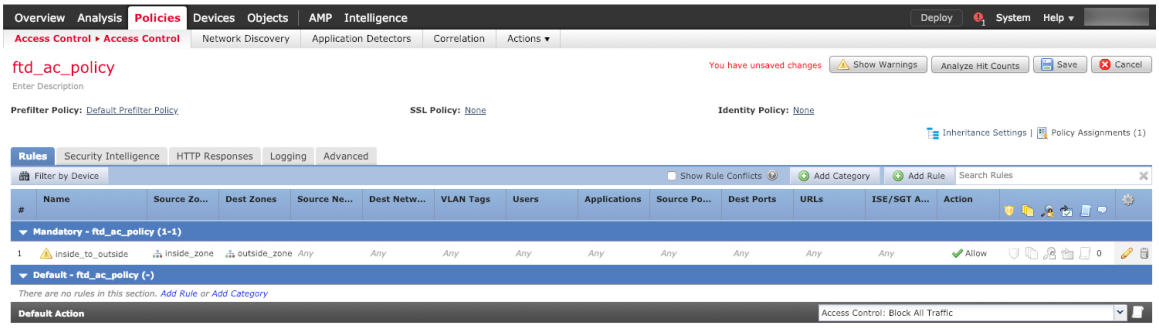
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

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

Laissez les autres paramètres tels quels.

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

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



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

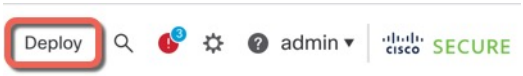
Déployer la configuration

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

Procédure

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

Illustration 20 : Déployer



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

Illustration 21 : Déployer tout

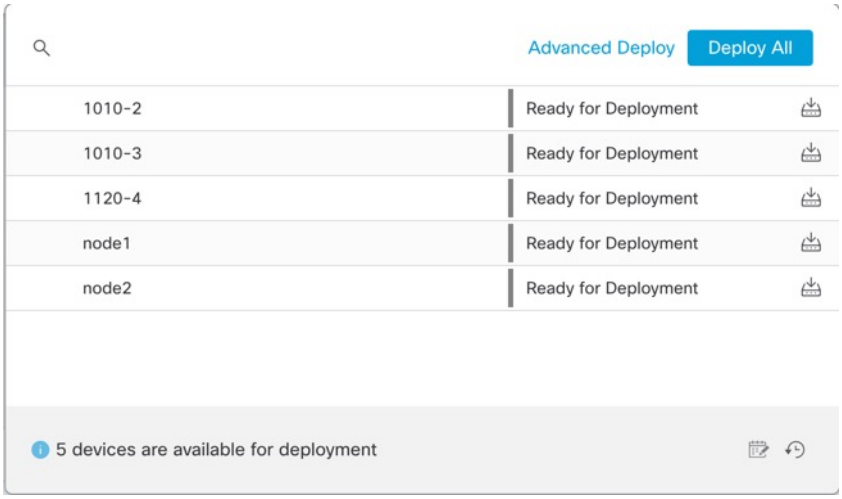
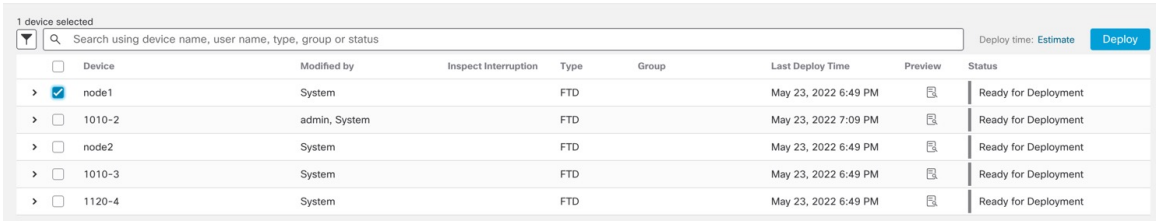
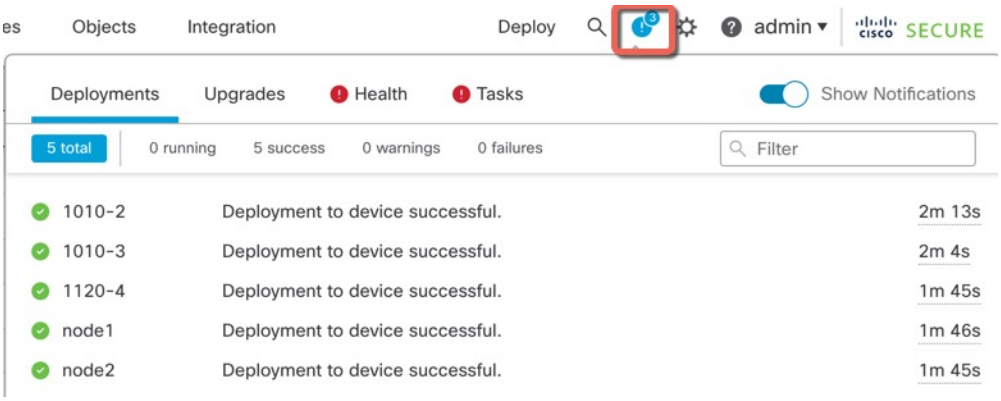


Illustration 22 : Déploiement avancé



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

Illustration 23 : État du déploiement



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

Vous pouvez utiliser l'interface de ligne de commande de Défense contre les menaces pour modifier les paramètres de l'interface de gestion et à des fins de dépannage. Vous pouvez accéder à l'interface de ligne de commande en utilisant SSH sur l'interface de gestion, ou en vous connectant à partir de l'interface de ligne de commande FXOS.

Procédure

Étape 1 (Option 1) SSH directement lié à l'adresse IP de l'interface de gestion de Défense contre les menaces.

Vous avez défini l'adresse IP de gestion lorsque vous avez déployé le dispositif logique. Connectez-vous à Défense contre les menaces avec le compte administrateur et le mot de passe que vous avez définis lors du déploiement initial.

Si vous avez oublié le mot de passe, vous pouvez le modifier en modifiant le dispositif logique dans le dossier de l'entreprise gestionnaire de châssis.

Étape 2 (Option 2) À partir de l'interface de ligne de commande de FXOS, connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

a) Connectez-vous au security module.

connect module *numéro_de_logement* {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connectez-vous à la console de Défense contre les menaces.

connect ftd *nom*

Si vous avez plusieurs instances d'application, vous devez préciser le nom de l'instance. Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
```

```
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
==========================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **exit**.

Remarque
Pour les versions antérieures à la version 6.3, entrez **Ctrl-a, d**.

d) Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Pour quitter la console :

1. Entrez **~**

   Vous quittez l'application Telnet.

2. Pour quitter l'application Telnet, entrez :

   telnet>**quit**

Pour quitter la session Telnet :

Entrez **Ctrl-], .**

Exemple

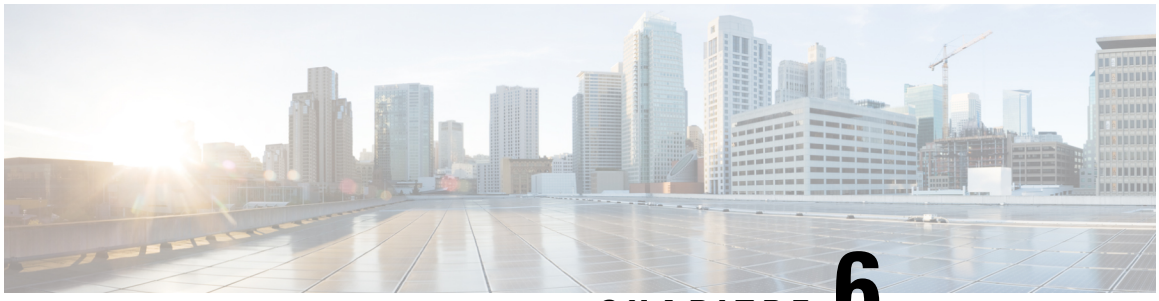
L'exemple suivant se connecte à Défense contre les menaces sur le module de sécurité 1 et repart au niveau superviseur de Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
```

```
'connect module <slot> telnet' to connect to the security module.
======================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

Prochaines étapes

Pour continuer la configuration de défense contre les menaces en utilisant CDO, consultez la page d'accueil Cisco Defense Orchestrator.



CHAPITRE 6

Déploiement d'ASA avec ASDM

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

Ce chapitre explique comment déployer un dispositif logique ASA autonome, notamment comment configurer l'octroi de licences Smart. Ce chapitre n'aborde pas les déploiements suivants. Pour en savoir plus à ce sujet, consultez le guide de configuration ASA :

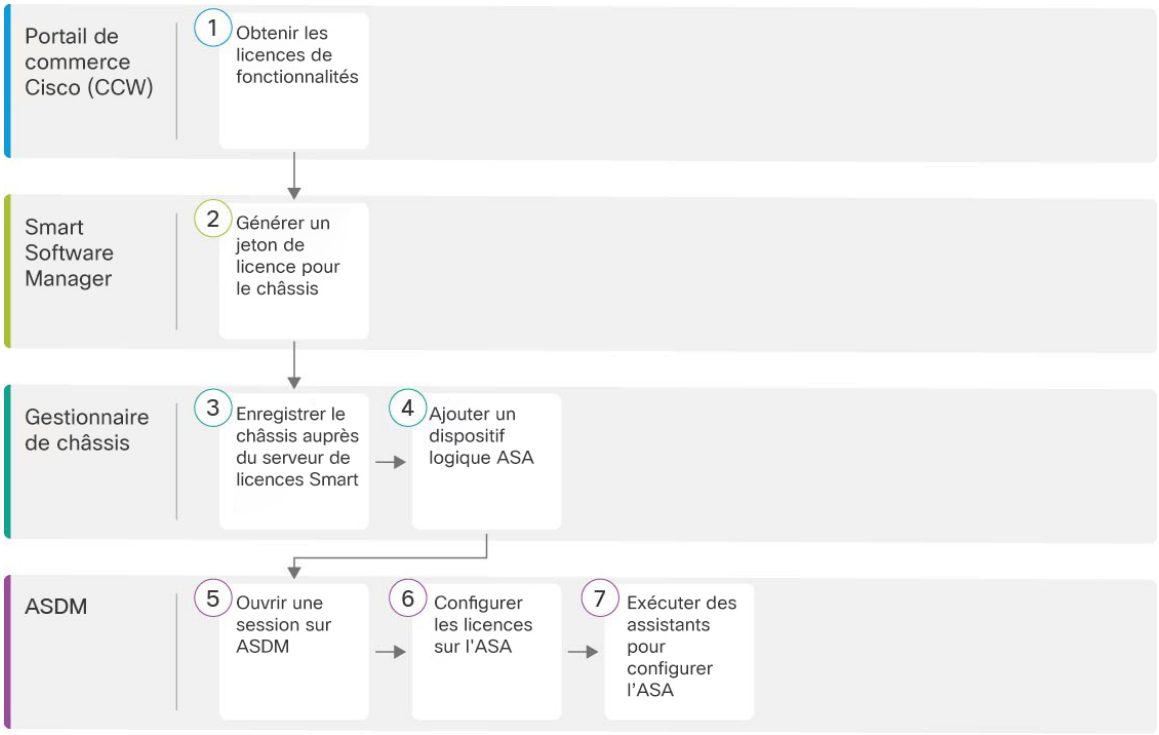
- Mise en grappes
- Basculement
- Configuration de l'interface de ligne de commande

Ce chapitre vous guide dans la configuration d'une politique de sécurité de base; si vous avez des exigences plus avancées, consultez le guide de configuration.

Déclaration de confidentialité : Firepower 9300 n'exige ni ne recueille de renseignements permettant d'établir l'identité de quelqu'un. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, pour créer les noms d'utilisateur. Si c'est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu'il travaille à la configuration ou qu'il utilise SNMP.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer et configurer l'ASA sur votre châssis.



1	Portail de commerce Cisco (CCW)	Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 124 : Obtenir les licences de fonctionnalités.
2	Smart Software Manager	Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 124 : Générer un jeton de licence pour le châssis.
3	Gestionnaire de châssis	Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 124 : Enregistrer le châssis auprès du serveur de licences Smart
4	Gestionnaire de châssis	Gestionnaire de châssis : ajouter un ASA logique, à la page 129.
5	ASDM	Connectez-vous à l'ASDM, à la page 133.
6	ASDM	Configurer les droits de licence sur l'ASA, à la page 133.
7	ASDM	Configurer un ASA, à la page 134.

Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences

Le ASA utilise les licences intelligentes. Vous pouvez utiliser le système habituel de licences intelligentes, qui nécessite un accès à Internet ; ou pour une gestion hors ligne, vous pouvez configurer la réservation

permanente de licences ou Smart Software Manager sur site (anciennement connu sous le nom de serveur satellite). Pour plus d'informations sur ces méthodes d'octroi de licences hors ligne, consultez Cisco ASA Series Feature Licenses; ce guide s'applique aux licences Smart habituelles.

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

Pour l'ASA sur le Firepower 9300, la configuration de la licence logicielle Smart est partagée entre FXOS sur le châssis et l'ASA.

- Firepower 9300 : configurez toute l'infrastructure de licences logicielles Smart dans FXOS, y compris les paramètres de communication avec l'autorité de licence. Le Firepower 9300 lui-même ne nécessite aucune licence pour fonctionner.
- ASA : configurez tous les droits de licence de l'ASA.

Lorsque vous enregistrez le châssis, Smart Software Manager émet un certificat d'ID pour la communication entre le pare-feu et Smart Software Manager. Il assigne également le pare-feu au compte virtuel approprié. jusqu'à ce que vous vous inscriviez à Smart Software Manager, vous ne pourrez pas modifier la configurationaux fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'en sera pas affecté autrement. Voici les fonctionnalités de licences :

- Essentials
- Security Contexts (contextes de sécurité)
- Opérateur—Diamètre, GTP/GPRS, M3UA, SCTP
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.
- Cisco Secure Client : Secure Client Advantage, Secure Client Premier ou Secure Client VPN Only

Lorsque vous demandez le jeton d'enregistrement pour le ASA à partir de Smart Software Manager, cochez la case **Allow export-controlled functionality on the products registered with this token (autoriser la fonctionnalité d'exportation contrôlée sur les produits enregistrés avec ce jeton)** afin que la licence complète de cryptage renforcé soit appliquée (votre compte doit être qualifié pour son utilisation). La licence de chiffrement renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement sur le châssis. Dans ce cas-là, aucune action supplémentaire n'est requise. Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Un chiffrement renforcé est requis pour l'accès à ASDM.

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

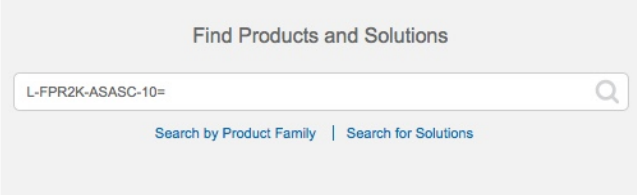
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Manager doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).
- Si vous ne l'avez pas encore fait, Configurer NTP, à la page 20.
- Si vous n'avez pas configuré le DNS lors de la configuration initiale, ajoutez un serveur DNS sur la page **Platform Settings (Paramètres de la plateforme)** > **DNS**.

Procédure

Étape 1 Assurez-vous que votre compte Smart Licensing contient les licences disponibles dont vous avez besoin, y compris au minimum la licence Essentials.

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

Illustration 24 : Recherche de licences

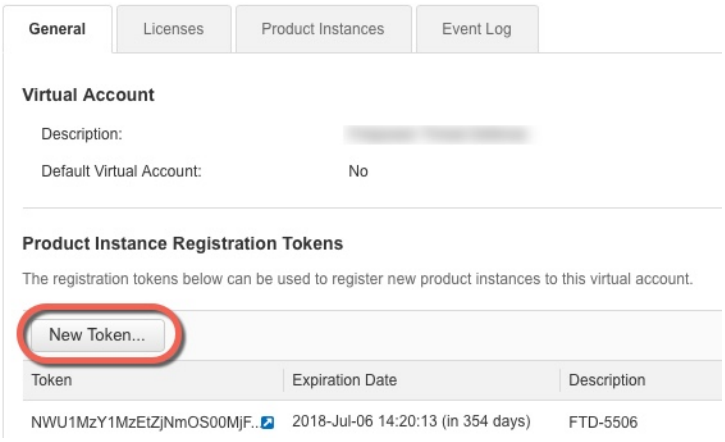


- Licence Essentials—L-F9K-ASA=. La licence Essentialsgratuite, mais vous devez toujours l'ajouter à votre compte de licences Smart.
- 10 licences de contexte — L-F9K-ASA-SC-10=. Les licences de contexte sont cumulatives; achetez plusieurs licences pour répondre à vos besoins.
- Exploitant (diamètre GTP/GPRS, M3UA, SCTP)— L-F9K-ASA-CAR=
- Chiffrement renforcé (3DES/AES) — L-F9K-ASA-ENCR-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.
- Cisco Secure Client—Voir le guide de commande Cisco Secure Client. Vous n'activez pas cette licence directement dans le ASA.

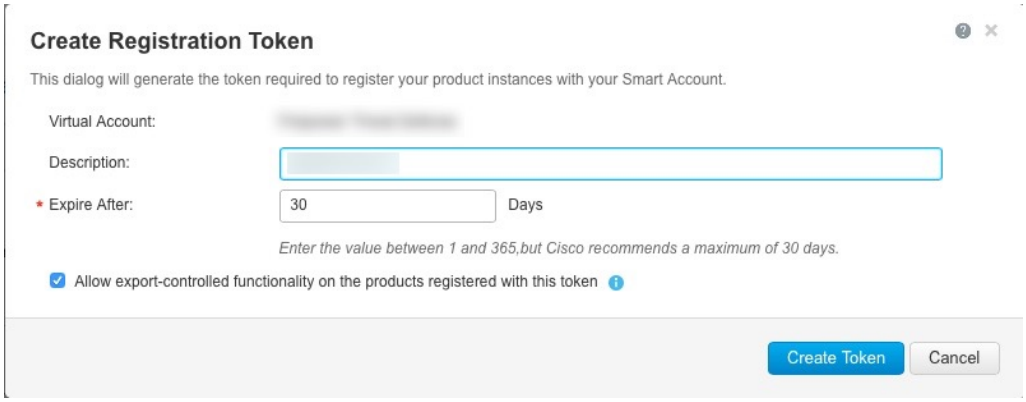
Étape 2 Dans Cisco Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce dispositif.

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

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



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



- **Description**
- **Expire After** (expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token (autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton)** : Active l'indicateur de conformité à l'exportation.

Le jeton est ajouté à votre inventaire.

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

Illustration 25 : Afficher le jeton

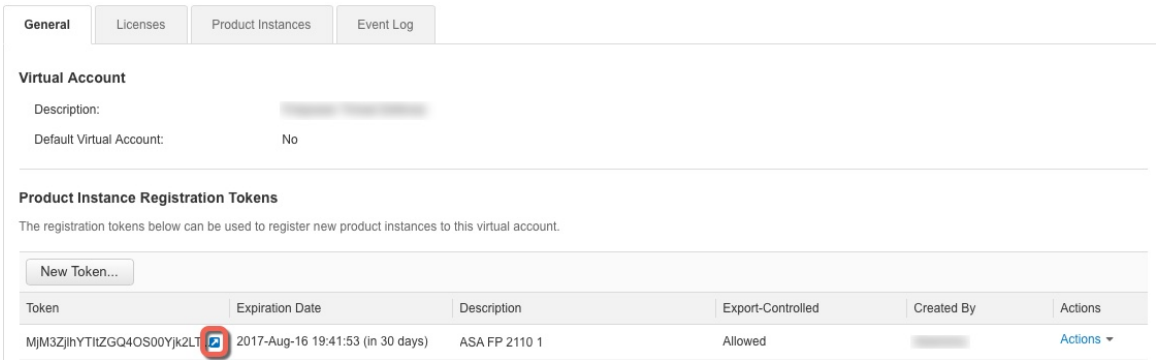
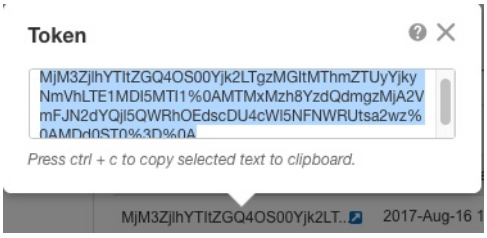
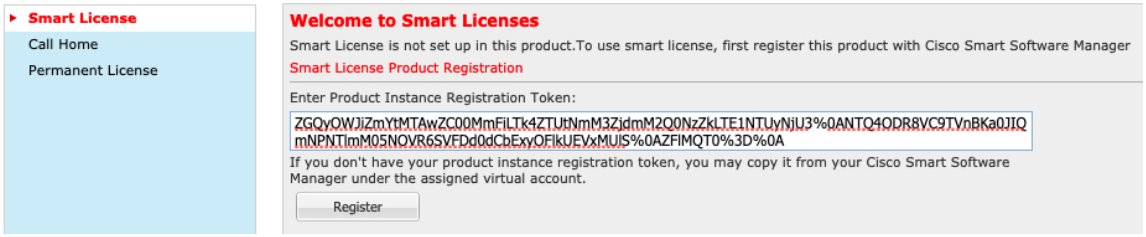


Illustration 26 : Copier le jeton



Étape 3 Dans le gestionnaire de châssis, choisissez **System (Système)** > **Licensing (Licence)** > **Smart License (Licence Smart)**.

Étape 4 Saisissez le jeton d'enregistrement dans le champ **Enter Product Instance Registration Token** (Saisir le jeton d'enregistrement de l'instance du produit).



Étape 5 Cliquez sur **Register** (Inscrire).

Le Firepower 9300 s'enregistre auprès de l'autorité de licence. Une inscription réussie peut prendre plusieurs minutes. Actualisez cette page pour voir l'état.

Illustration 27 : Enregistrement en cours

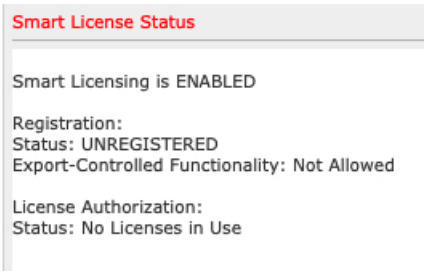
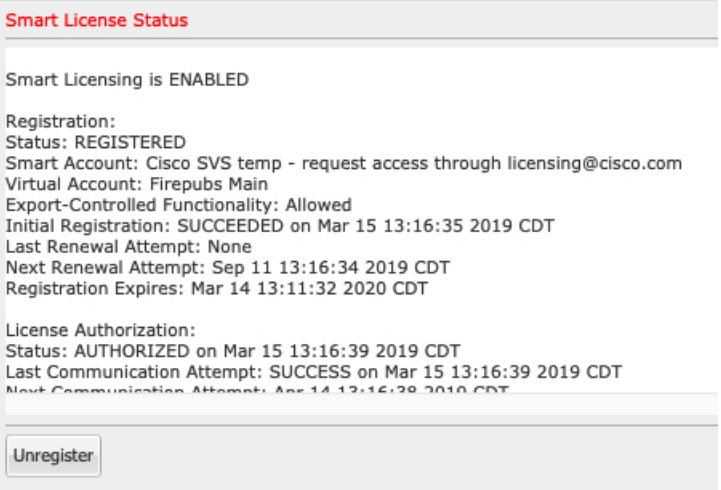


Illustration 28 : Inscription réussie



Gestionnaire de châssis : ajouter un ASA logique

Vous pouvez déployer un ASA à partir de Firepower 9300 en tant qu'instance native.

Pour ajouter une paire de basculement ou une grappe, consultez le guide de configuration des opérations générales de l'ASA.

Cette procédure vous permet de configurer les caractéristiques logiques du dispositif, y compris la configuration de démarrage utilisée par l'application.

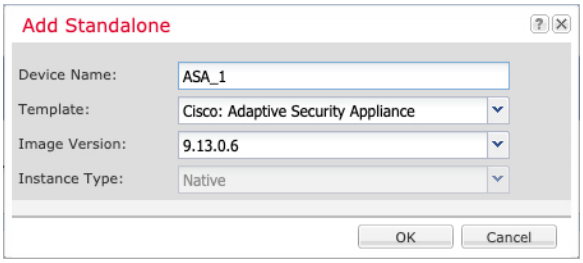
Avant de commencer

- Configurez une interface de gestion à utiliser avec l'ASA; consultez Interfaces de configuration, à la page 24. L'interface de gestion est requise. Il convient de souligner que cette interface de gestion est différente du port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**).
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce dispositif
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - Nouveau mot de passe d'administrateur/mot de passe d'activation

Procédure

Étape 1 Dans gestionnaire de châssis, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur **Add** > **Standalone**, puis définissez les paramètres suivants :



a) Indiquez un nom de dispositif (**Device Name**).

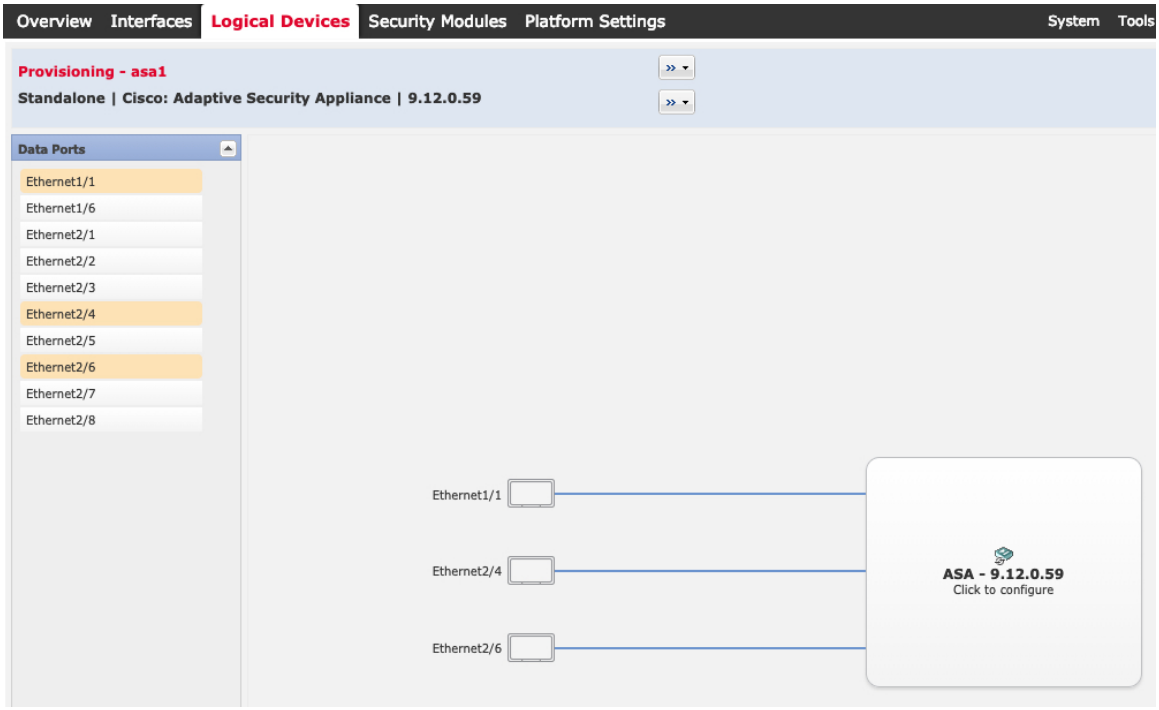
Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de dispositif utilisé dans la configuration de l'application.

Remarque
Vous ne pouvez pas modifier ce nom après avoir ajouté le dispositif logique.

b) pour le **Template** (modèle), choisissez **Cisco: Adaptive Security Appliance** (Cisco : Appareil de sécurité adaptable).
c) Choisissez la version de l'image (**Image Version**).
d) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du dispositif).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au dispositif.

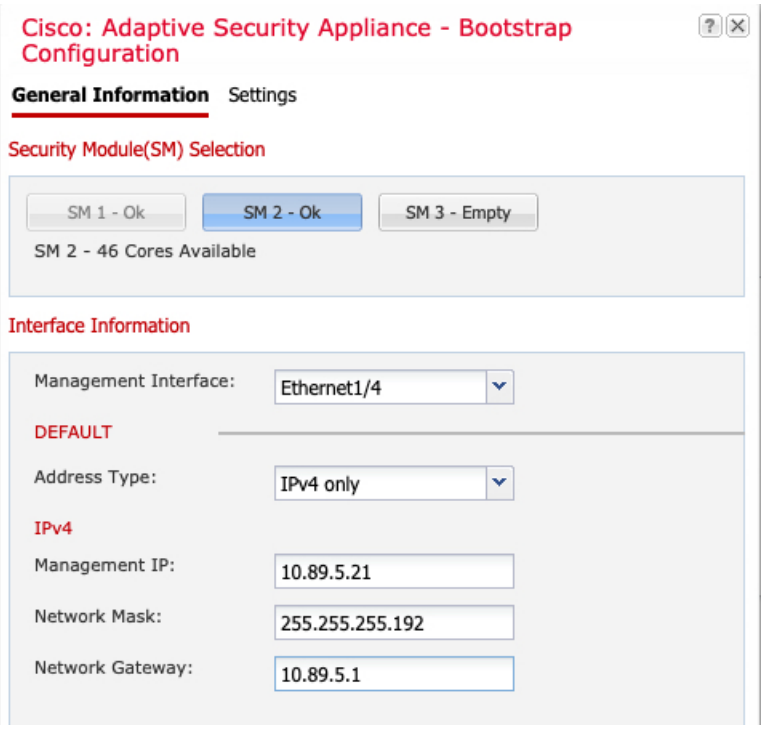


Vous ne pouvez attribuer que des interfaces de données que vous avez préalablement activées sur la page **Interfaces**. Vous pourrez ensuite activer et configurer ces interfaces dans ASDM, y compris pour ce qui concerne la définition des adresses IP.

Étape 4 Cliquez sur l'icône de dispositif au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce dispositif logique.

b) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le dispositif logique. Cette interface est distincte du port de gestion du châssis.

c) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).

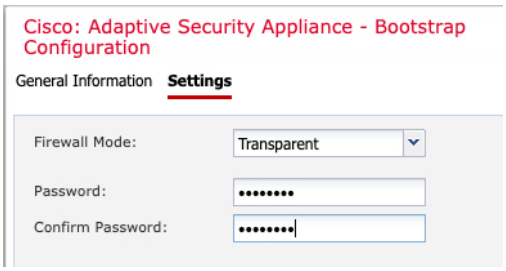
d) Configurez l'adresse IP de gestion (**Management IP**).

Définissez une adresse IP unique pour cette interface.

e) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).

f) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Cliquez sur **Settings** (Paramètres).



a) Choisissez le mode du pare-feu (**Firewall Mode**) : **Transparent** ou **Routed** (routage).

   En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

   Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

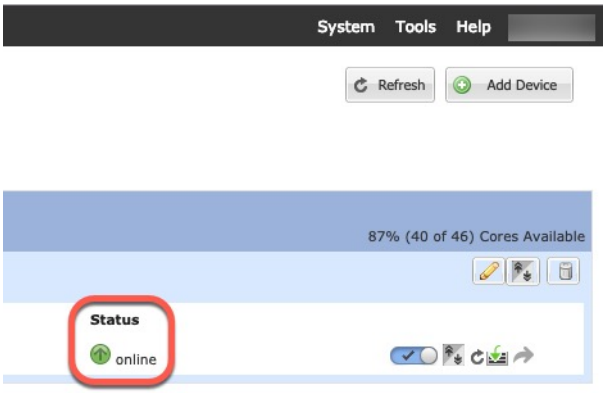
b) Saisissez et confirmez un **Password** (Mot de passe) pour l'utilisateur admin et pour le mot de passe d'activation.

   L'utilisateur/mot de passe administrateur ASA préconfigurés et le mot de passe d'activation sont utiles pour la récupération du mot de passe. si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin et le mot de passe d'activation si vous l'oubliez.

Étape 7 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 8 Cliquez sur **Save** (enregistrer).

Le châssis déploie le dispositif logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau dispositif logique dans la page **Logical Devices**. Lorsque le dispositif logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Connectez-vous à l'ASDM

Lancez l'ASDM pour pouvoir configurer l'ASA.

Avant de commencer

- Consultez les notes de version d'ASDM sur Cisco.com pour connaître les exigences d'exécution d'ASDM.
- Assurez-vous que **l'état** de le dispositif logique ASA est **en ligne** sur gestionnaire de châssis la page **Logical devices (dispositifs logiques)**.

Procédure

Étape 1 Entrez l'URL suivante dans votre navigateur.

- **https://***management_ip* : Adresse IP de l'interface que vous avez entrée dans la configuration de démarrage.

Remarque
Assurez-vous de spécifier **https://**, et non **http://** ou simplement l'adresse IP (qui est par défaut HTTP); le ASA ne transmet pas automatiquement une requête HTTP à HTTPS.

La page Web **Cisco ASDM** s'affiche. Il est possible que des avertissements de sécurité s'affichent dans votre navigateur parce que le certificat n'est pas installé sur ASA; vous pouvez ignorer ces avertissements et visiter la page Web en toute sécurité.

Étape 2 Cliquez sur l'une des options suivantes : **Installer le lanceur ASDM** ou **Exécuter ASDM**.

Étape 3 Suivez les instructions à l'écran pour lancer ASDM selon l'option que vous avez choisie.

Le lanceur **Cisco ASDM-IDM** apparaît.

Étape 4 LLaissez le nom d'utilisateur vide, entrez le mot de passe d'activation que vous avez défini lorsque vous avez déployé ASA, et cliquez **OK**.

La principale fenêtre ASDM s'ouvre.

Configurer les droits de licence sur l'ASA

Attribuez des licences à l'ASA. Vous devez au minimum attribuer la licence standard.

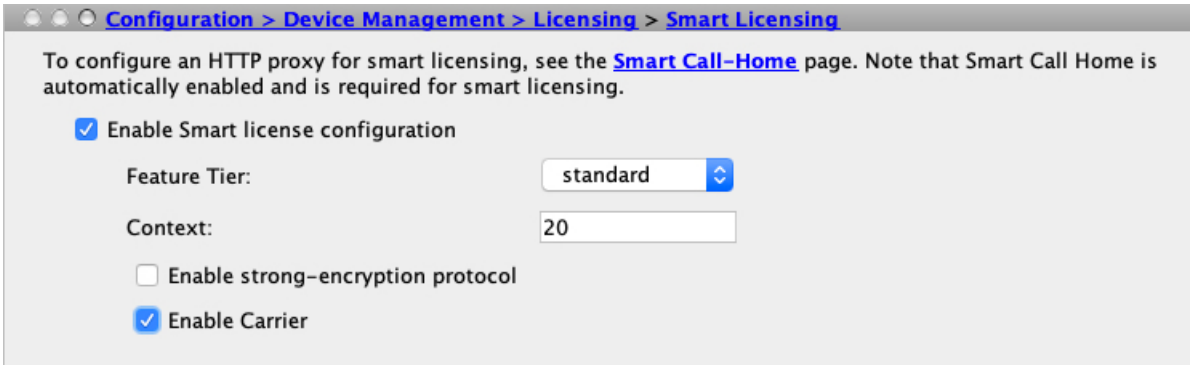
Avant de commencer

- Gestionnaire de châssis : enregistrez le châssis auprès du serveur de licences, à la page 124.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Device Management (gestion d'appareils)** > **Licensing (licences)** > **Smart Licensing (licences Smart)**.

Étape 2 Définissez les paramètres suivants :



a) Cochez la case **Enable Smart license configuration** (activer la configuration de licence Smart).

b) Dans la liste déroulante **Niveaux de fonctionnalités**, choisissez **Essentials**.

Seul le niveau Essentials est disponible.

c) (Facultatif) Pour la licence de **contexte**, entrez le nombre de contextes.

Vous pouvez utiliser 10 contextes sans licence. Le nombre maximal de contextes est établi à 250. Par exemple, pour utiliser le maximum, entrez 240 pour le nombre de contextes; cette valeur est ajoutée à la valeur par défaut de 10.

d) (Facultatif) Vérifiez le **Carrier** (Transporteur).

Étape 3 Cliquez sur **Apply** (appliquer).

Si vous ne disposez pas des licences appropriées dans votre compte, vous ne pouvez pas appliquer vos modifications de licence.

Étape 4 Cliquez sur l'icône **Save** (enregistrer) dans la barre d'outils.

Étape 5 Quittez ASDM, puis relancez-le.

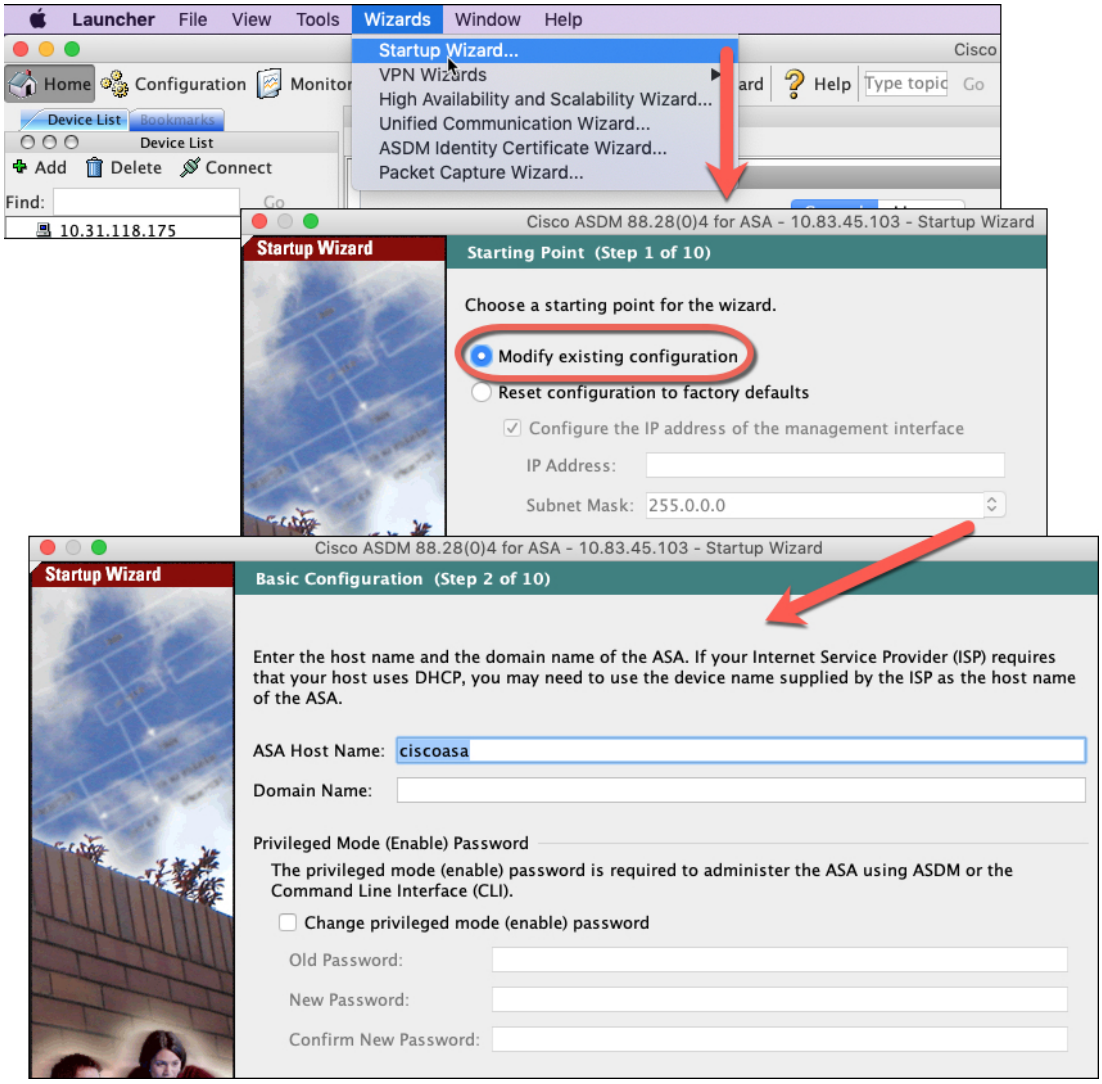
Lorsque vous modifiez les licences, vous devez relancer ASDM pour afficher les écrans mis à jour.

Configurer un ASA

Grâce à ASDM, vous pouvez utiliser des assistants pour configurer les fonctionnalités de base et les fonctionnalités avancées. Vous pouvez également configurer manuellement les fonctionnalités non visées par les assistants de configuration.

Procédure

Étape 1 Sélectionnez **Wizards (assistants) > Startup Wizard (assistants de démarrage)**, puis cliquez sur la touche radio **Modify existing configuration** (modifier la configuration existante).



Étape 2 L'assistant de démarrage (**Startup Wizard**) vous guide tout au long de la configuration :

- des interfaces pour activer
- Interfaces, y compris la définition des adresses IP d'interface intérieure et extérieure et l'activation des interfaces.
- du routage statique;
- Le serveur DHCP
- et plus encore...

Étape 3 (Facultatif) Dans le menu **Wizards** (assistants), exécutez d'autres assistants.

Étape 4 Pour continuer à configurer votre ASA, consultez les documents disponibles pour votre version de logiciel à la page d'orientation dans la documentation de la gamme Cisco ASA.

Accéder à l'interface de ligne de commande d'ASA

Vous pouvez utiliser l'interface de ligne de commande d'ASA pour dépanner ou configurer l'ASA au lieu d'utiliser l'ASDM. Vous pouvez accéder à l'interface de ligne de commande en vous connectant à partir de l'interface de ligne de commande FXOS. Vous pourrez configurer ultérieurement l'accès SSH à l'ASA à partir de n'importe quelle interface. Consultez le guide de configuration sur les opérations générales ASA pour obtenir plus d'informations.

Procédure

Étape 1 À partir de l'interface de ligne de commande de FXOS, connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *numéro_de_logement* {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Étape 2 Connectez-vous à la console de l'ASA.

connect asa

Exemple :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

Étape 3 Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **Ctrl-a, d**.

Étape 4 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Exemple

Dans l'exemple suivant, une connexion est établie à un ASA sur le module de sécurité 1, puis retourne au niveau de superviseur du Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

Quelle est l'étape suivante?

- Pour continuer de configurer votre ASA, reportez-vous aux documents disponibles pour votre version du logiciel dans la navigation de la documentation Cisco de la série ASA.

Historique de l'ASA

Fonctionnalités	Version	Détails
Prise en charge d'ASA et de Défense contre les menaces sur des modules distincts du même Firepower 9300	9.12(1)	Vous pouvez maintenant déployer l'ASA et les dispositifs logiques Défense contre les menaces sur le même Firepower 9300. **Remarque** FXOS 2.6.1 est nécessaire.

Fonctionnalités	Version	Détails
Prise en charge du déploiement en mode transparent pour un dispositif logique ASA	9.10(1)	Vous pouvez désormais spécifier le mode transparent ou routé lorsque vous déployez l'ASA. **Remarque** FXOS 2.4.1 est nécessaire. Écrans Nouveaux ou modifiés de gestionnaire de châssis : Liste déroulante **Logical Devices (Dispositifs logiques)** > **Add Device (Ajouter un dispositif)** > **Settings (Paramètres) > Firewall Mode (Mode de pare-feu)**
Mise à niveau de Smart Agent vers la version 1.6	9.6(2)	Smart Agent a été mis à niveau de la version 1.1 à la version 1.6. Cette mise à niveau prend en charge la réservation de licences permanentes et prend également en charge la définition du droit de licence de cryptage renforcé (3DES/AES) en fonction de l'autorisation définie dans votre compte de licence.
Licence de transporteur	9.5(2)	La nouvelle licence de transporteur remplace la licence GTP/GPRS existante et comprend également la prise en charge de l'inspection SCTP et Diameter. Pour l'ASA sur le châssis Firepower 9300, la commande **feature mobile-sp** passera automatiquement à la commande **feature carrier**. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des dispositifs)** > **Licensing (Licence)** > **Smart License (Licence Smart)**

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.