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 .

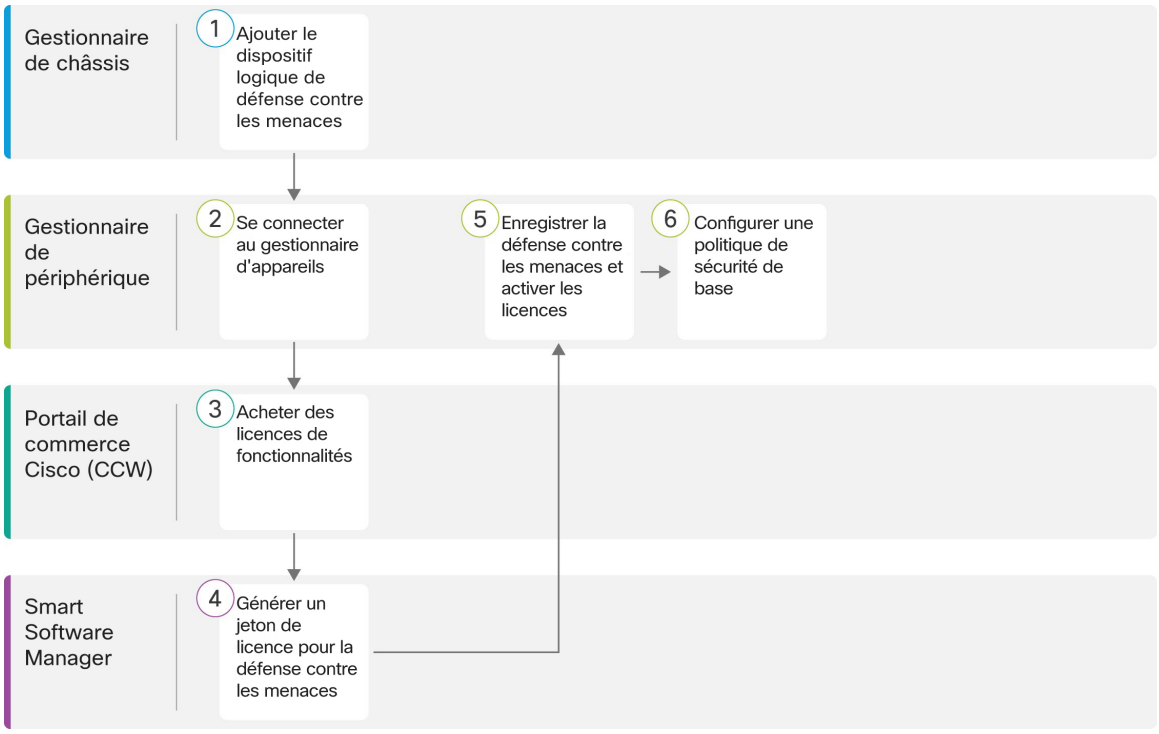
Le gestionnaire d'appareil vous permet de configurer les fonctions de base du logiciel qui sont le plus souvent utilisées pour les petits réseaux. Il est spécialement conçu pour les réseaux qui comprennent un seul dispositif ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire 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 2.
2	Gestionnaire d'appareil	Se connecter à Gestionnaire d'appareil, à la page 7.
3	Portail de commerce Cisco (CCW)	Configurer les licences, à la page 7 : Achetez des licences de fonctionnalités.
4	Smart Software Manager	Configurer les licences, à la page 7 : Générer un jeton de licence pour gestionnaire d'appareil.
5	Gestionnaire d'appareil	Configurer les licences, à la page 7 : 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 14.

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 .

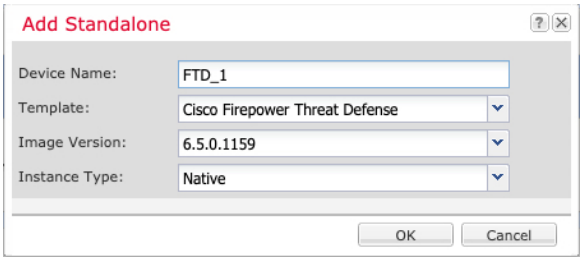
Avant de commencer

- Configurer l'interface de gestion à utiliser avec défense contre les menaces; voir Interfaces de configuration. 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.

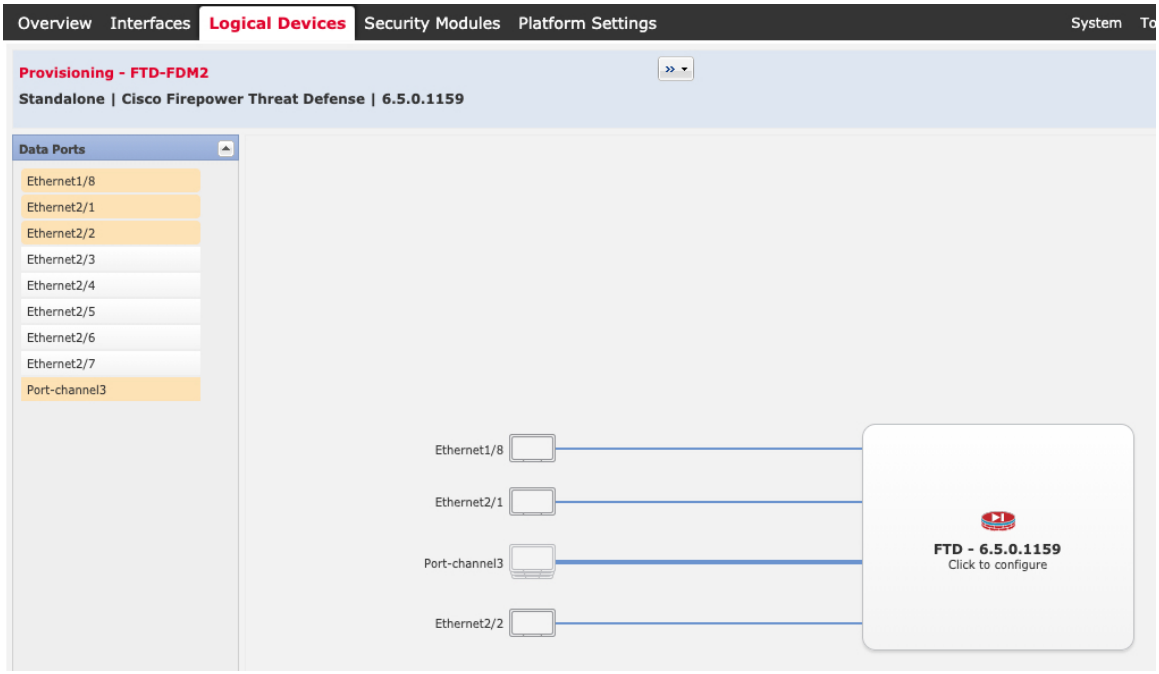
b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
c) Choisissez la version de l'image (**Image Version**).
d) Choisissez l'**Instance Type (Type d'instance)** : **Native (Instance native)**.

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.

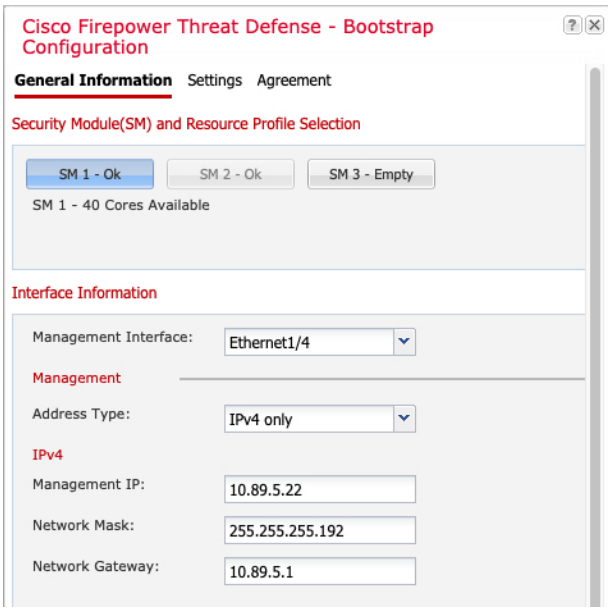


Vous ne pouvez attribuer que des interfaces de données que vous avez préalablement activées sur la page **Interfaces**. Vous activerez et configurerez plus tard ces interfaces dans le gestionnaire d'appareil, y compris la définition des adresses IP.

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).

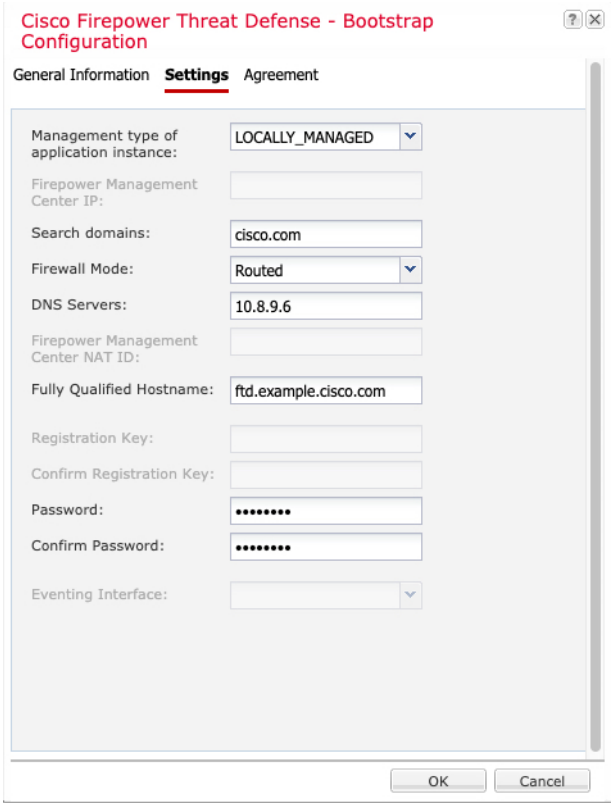
d) Configurez l'adresse IP de gestion (**Management IP**).

   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.

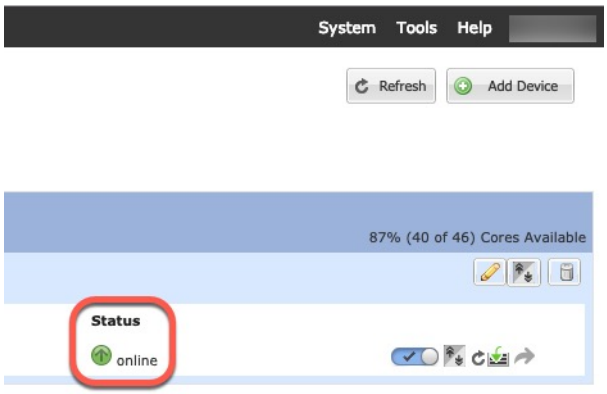
b) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.
c) Le **Firewall Mode** (Mode pare-feu) ne prend en charge que le mode **Routed** (Routé).
d) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont 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.

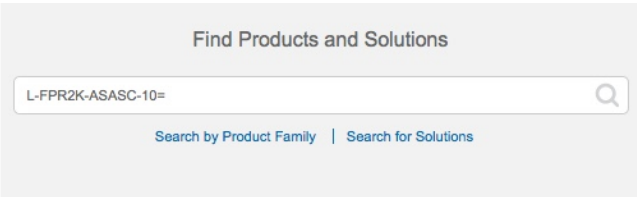
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines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

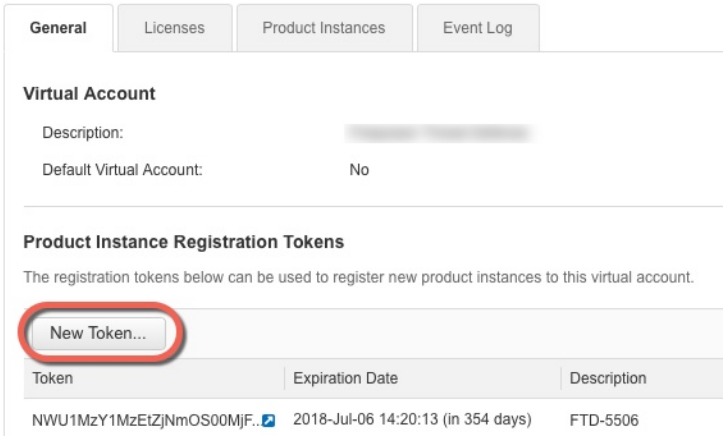
- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

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

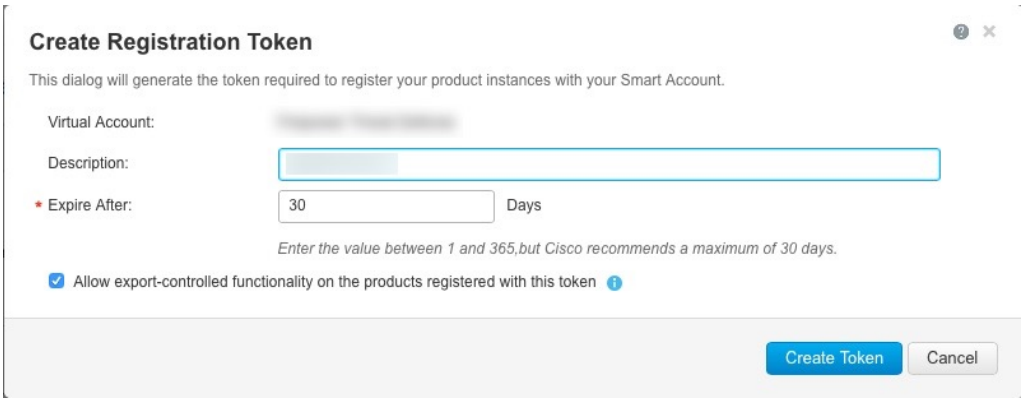
Étape 2 Dans le Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous voulez ajouter ce dispositif.

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 2 : Afficher le jeton

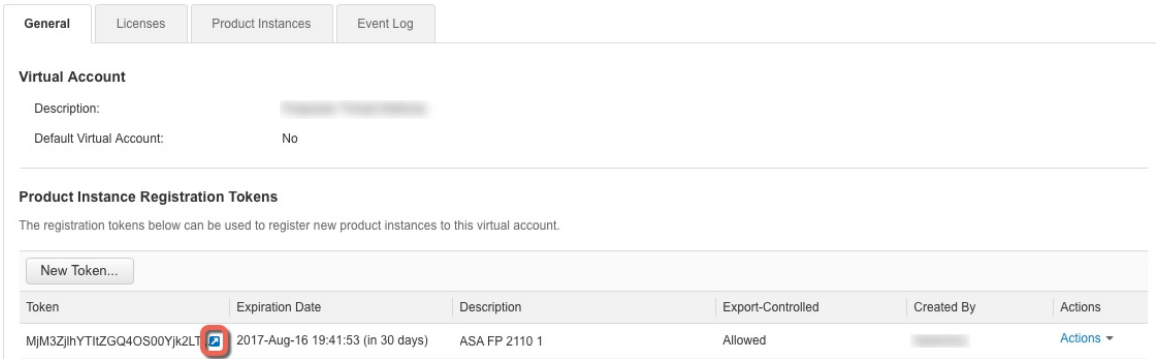
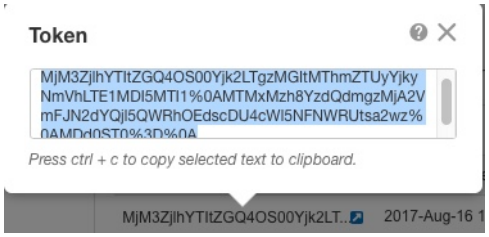


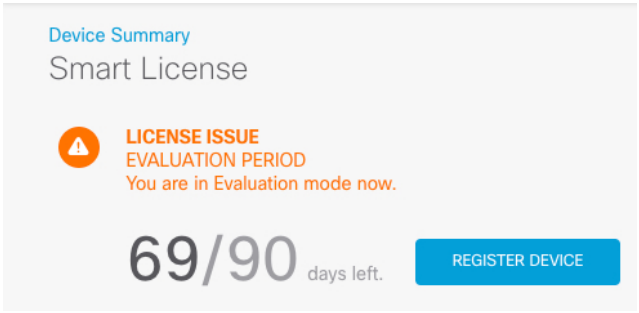
Illustration 3 : Copier le jeton



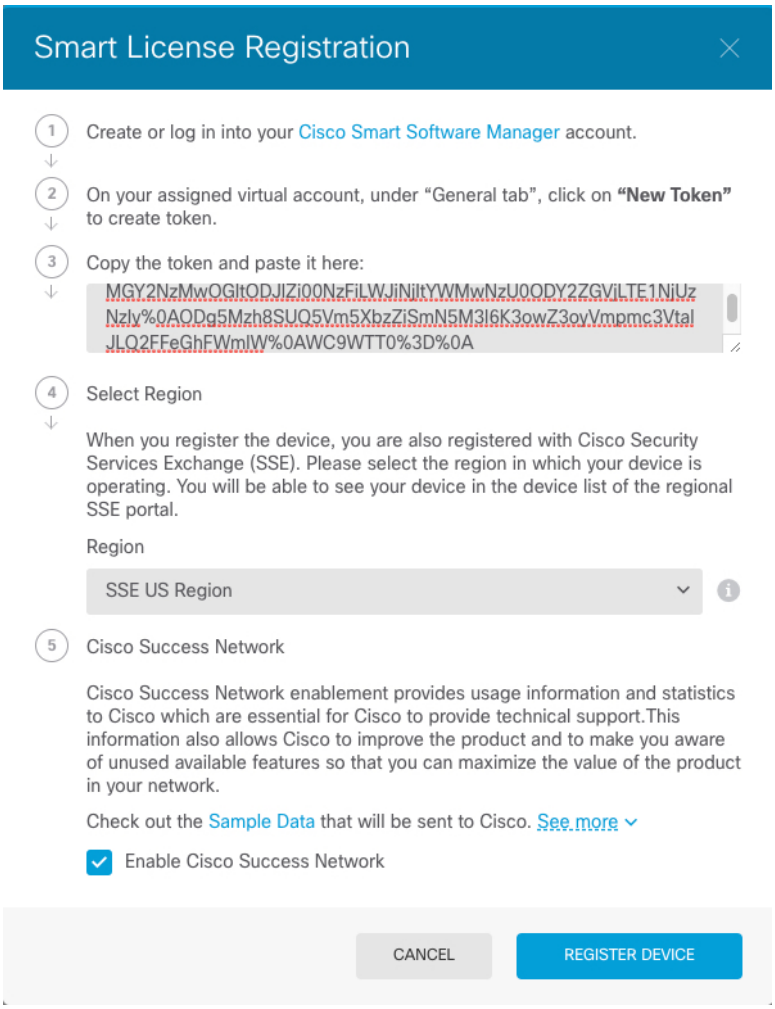
Étape 3 Dans le gestionnaire d'appareil, cliquez sur **Device (appareil)**, et puis dans le sommaire **Smart License** cliquez sur **View Configuration (voir configuration)**.

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

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



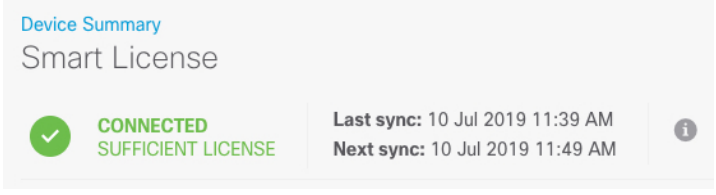
Suivez ensuite les instructions de la boîte de dialogue **Smart License Registration** pour coller votre jeton :



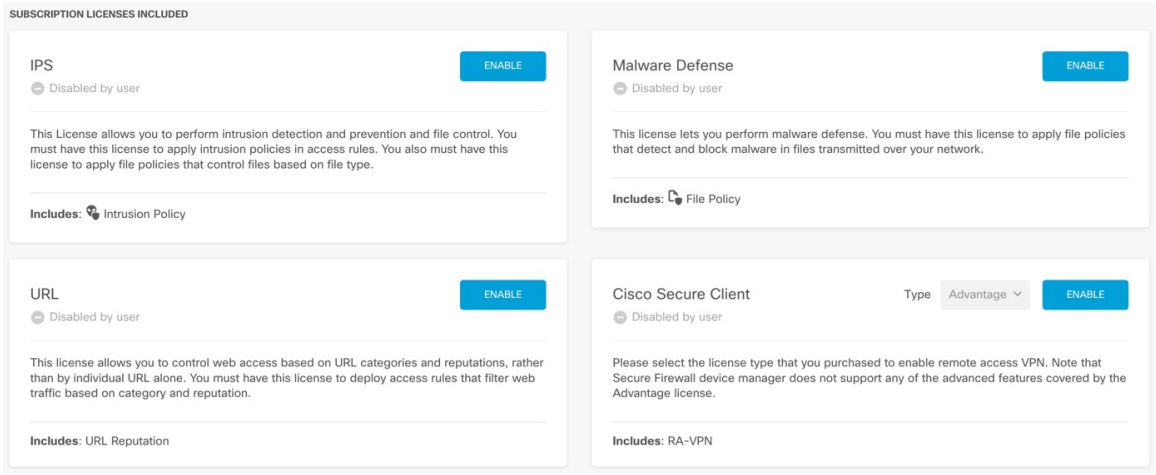
Étape 5 Cliquez sur **Register Device** (enregistrer l'appareil).

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

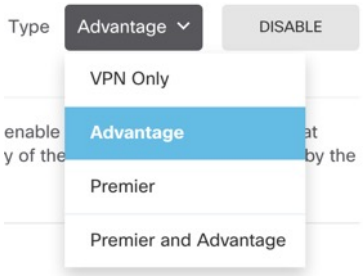
Une fois que l'appareil a été enregistré et que vous avez actualisé la page, les éléments suivants apparaissent :



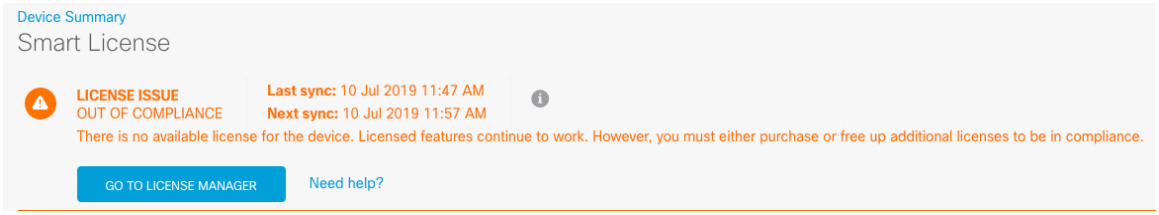
Étape 6 Cliquez sur **Enable/Disable** (activer/désactiver) pour chaque licence facultative, au besoin.



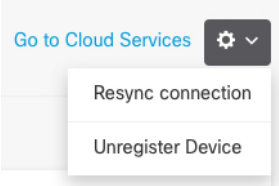
- **Enable** (activer) : Enregistre la licence avec votre compte Cisco Smart Software Manager et active les fonctionnalités contrôlées. Vous pouvez maintenant configurer et déployer les politiques contrôlées par la licence.
- **Disable** (désactiver) : Désinscrit la licence de votre compte Cisco Smart 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 14. 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 17. 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 19. Si vous ne recevez pas la route par défaut du serveur DHCP externe, vous devez l'ajouter manuellement.
4	Configurer NAT, à la page 21. Utilisez l'interface PAT sur l'interface externe.
5	Permettre le trafic de l'intérieur vers l'extérieur, à la page 23. Permettez le trafic de l'intérieur vers l'extérieur
6	(Facultatif) Configurer le serveur DHCP, à la page 24. 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 25. Modifiez la passerelle de gestion et/ou autorisez la gestion à partir d'une interface de données.
8	Déployer la configuration, à la page 27.

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.

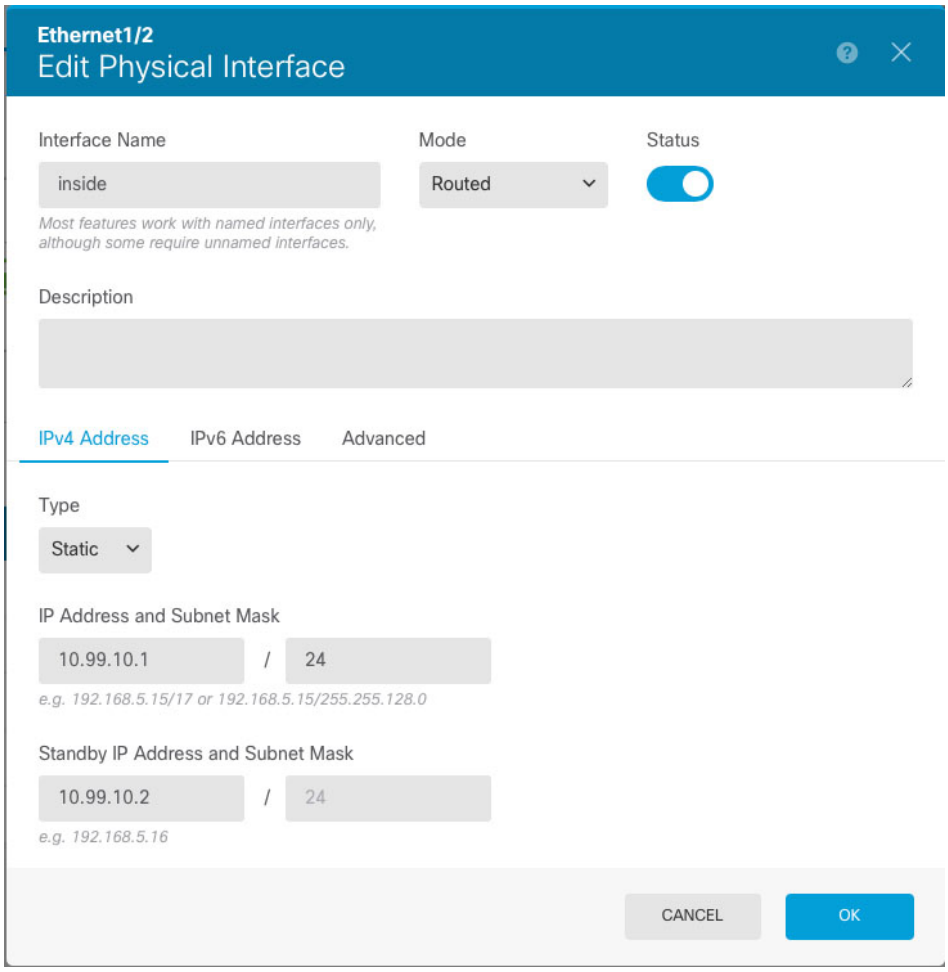
Procédure

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.

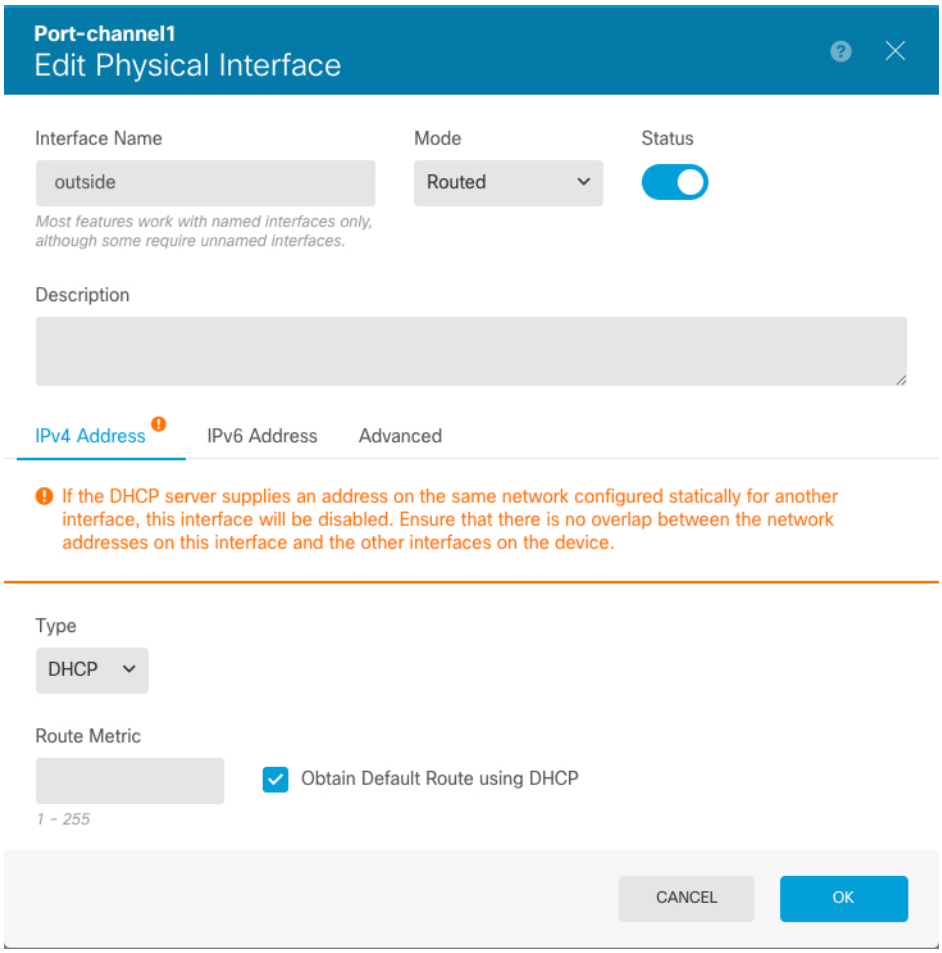
d) (Facultatif) Définissez la **Description**.

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.

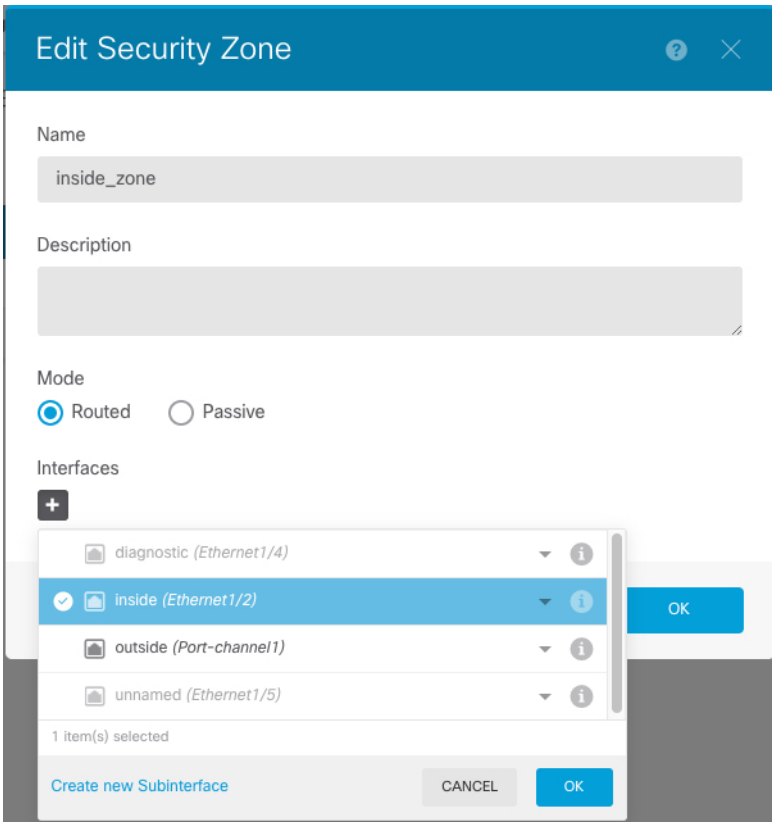
Cette procédure vous explique comment ajouter des interfaces aux zones préconfigurées suivantes :

- **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.

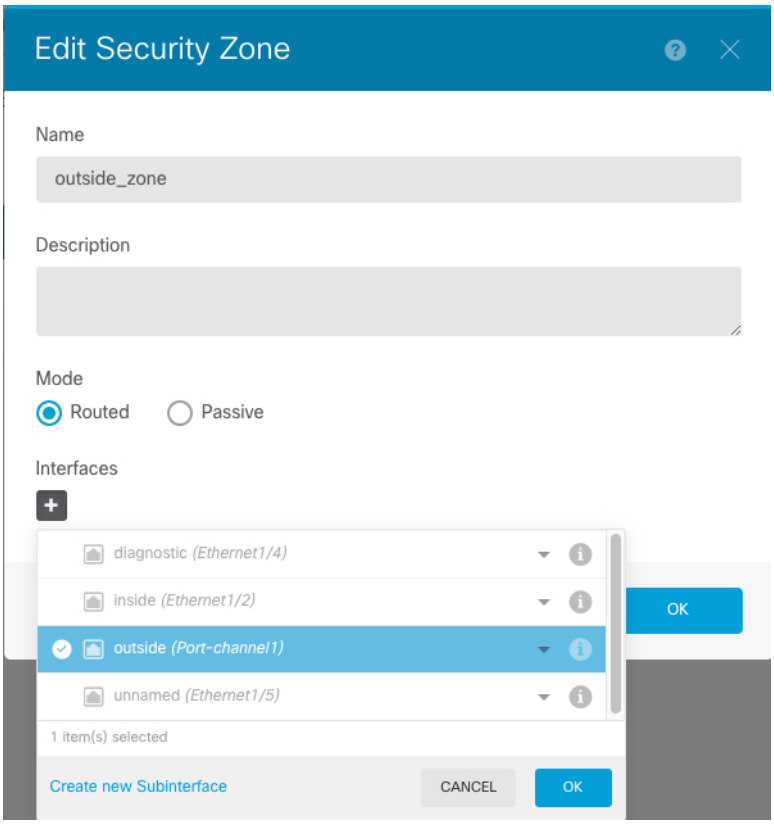
Étape 2 Cliquez sur l'icône de modification ( ) pour **inside_zone** (zone_interne).



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)**.

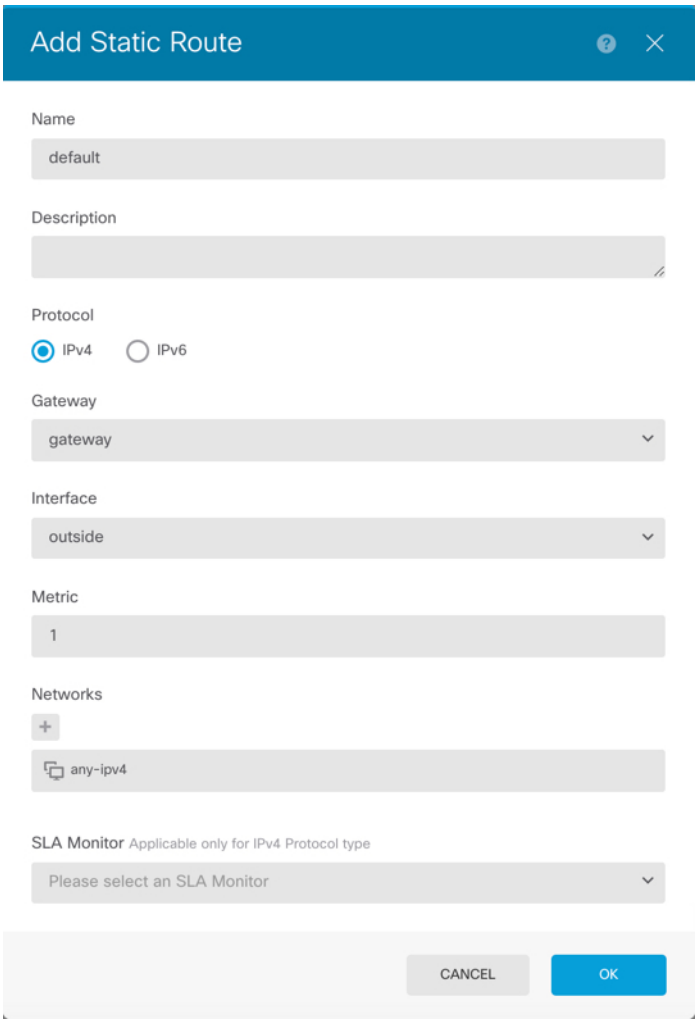
Procédure

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).

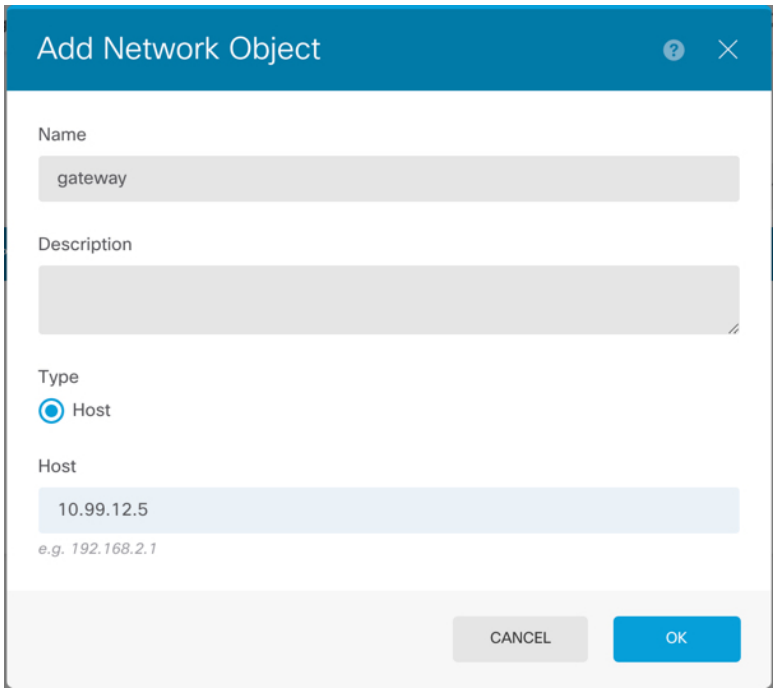
Étape 3 Configurez les propriétés des voies de routage par défaut.



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

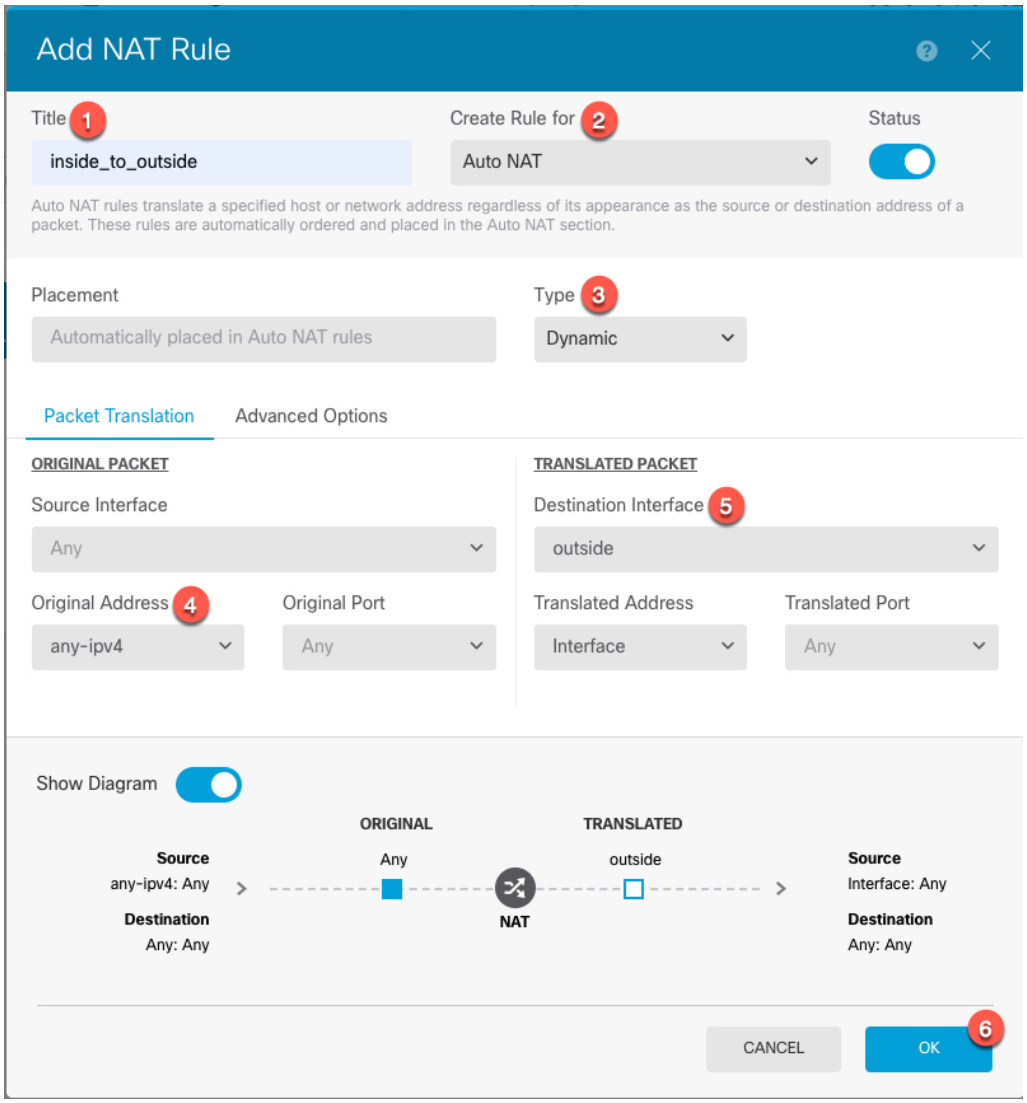
Une règle NAT typique convertit les adresses internes en un port sur l'adresse IP de l'interface externe. Ce type de règle NAT est appelé *interface Port Address Translation (PAT)*. Vous ne pouvez pas utiliser l'interface PAT pour IPv6.

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

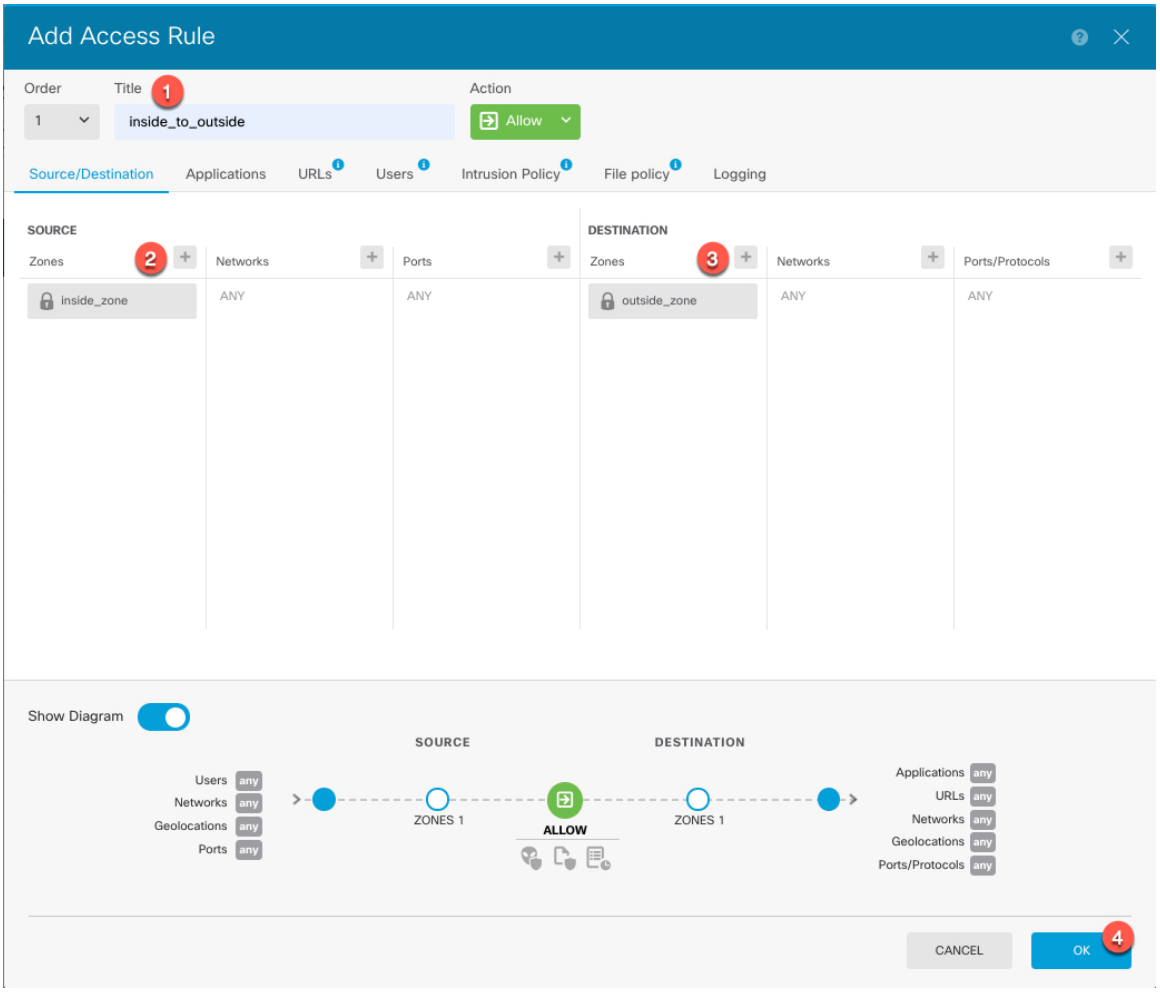
Par défaut, le trafic est bloqué entre les zones de sécurité. Cette procédure montre comment autoriser le trafic de l'intérieur vers l'extérieur.

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

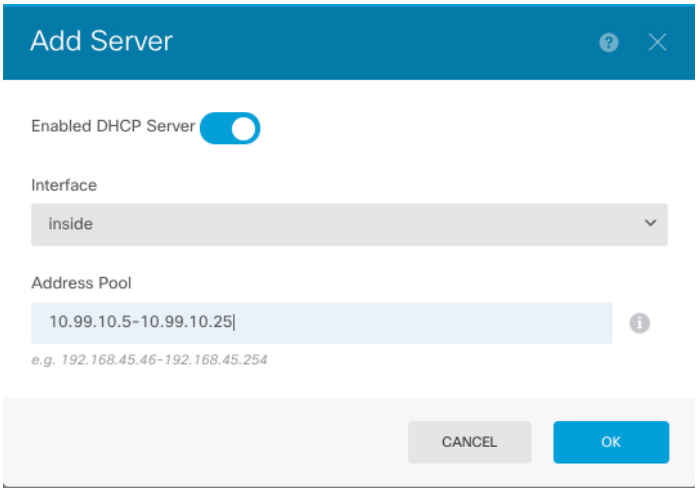
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de Défense contre les menaces.

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.

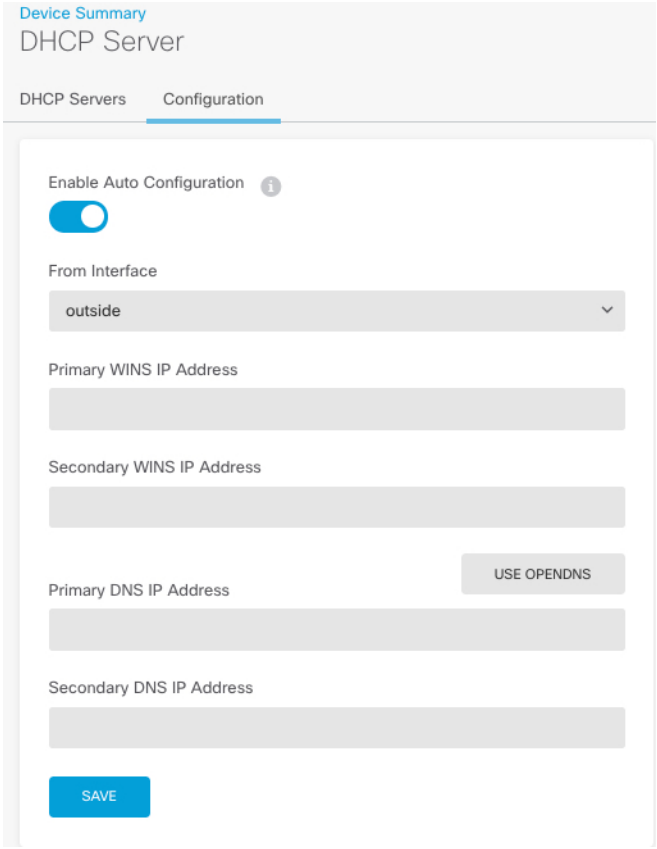
L'interface doit avoir une adresse IP statique; vous ne pouvez pas utiliser DHCP pour obtenir l'adresse de l'interface si vous souhaitez exécuter un serveur DHCP sur l'interface.

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 14.

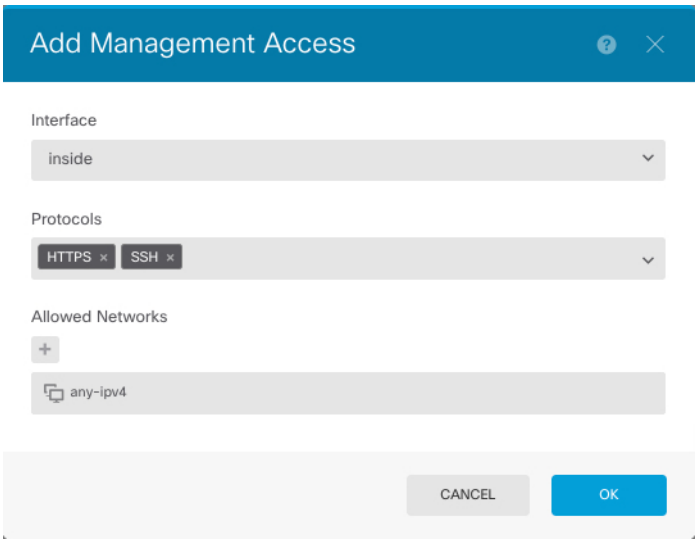
Procédure

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 :



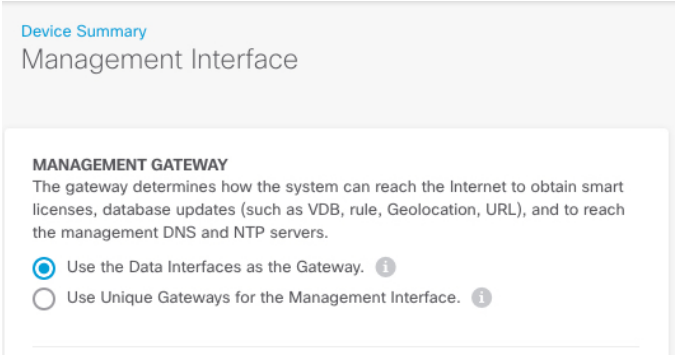
- **Interface** : sélectionnez l'interface sur laquelle vous souhaitez autoriser l'accès de gestion.
- **Protocols** (Protocoles) : indiquez si la règle est pour HTTPS (port 443), pour SSH (port 22) ou les deux.
- **Allowed Networks** (Réseaux permis) : sélectionnez les objets réseau qui définissent 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.

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.