Déploiement de Défense contre les menaces 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.

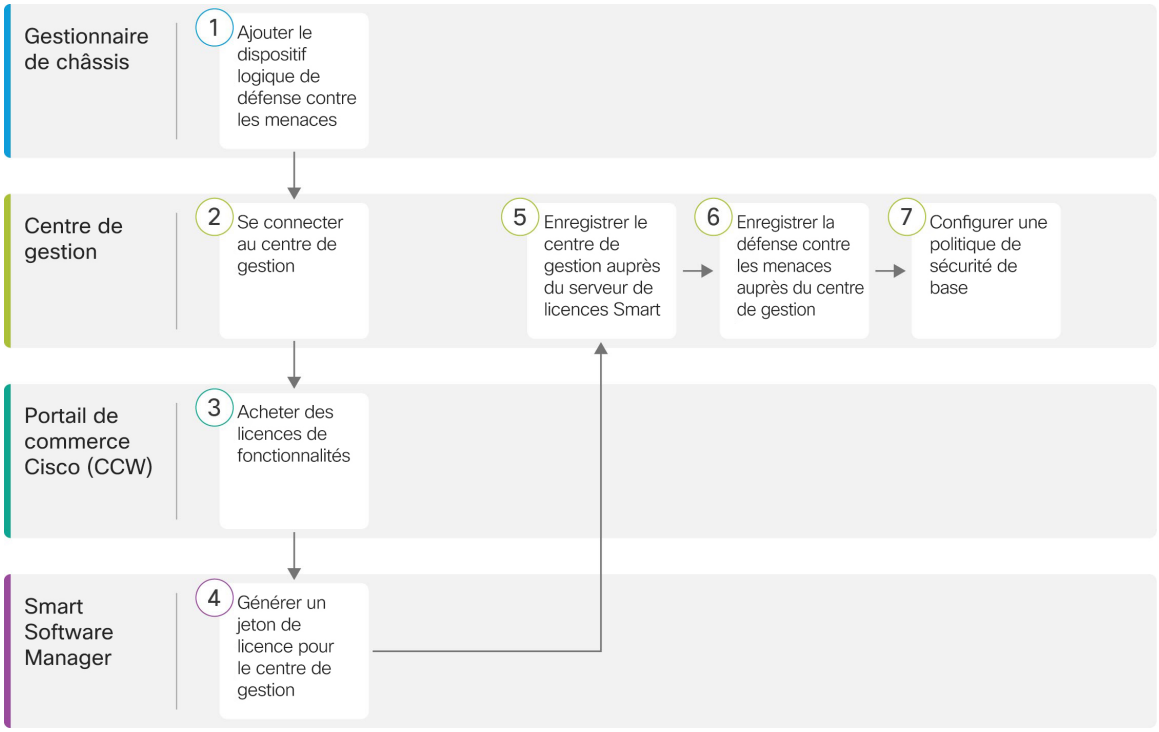
Déclaration de confidentialité : Firepower 4100 n'exige ni ne recueille de renseignements permettant d'établir l'identité de quelqu'un. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, pour créer les noms d'utilisateur. 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 3.
2	Centre de gestion	Se connecter au Centre de gestion, à la page 9.
3	Portail de commerce Cisco (CCW)	Obtenir des licences pour le Centre de gestion, à la page 9 : Achetez des licences de fonctionnalités.
4	Smart Software Manager	Obtenir des licences pour le Centre de gestion, à la page 9 : Générer un jeton de licence pour centre de gestion.
5	Centre de gestion	Obtenir des licences pour le Centre de gestion, à la page 9 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 11.
7	Centre de gestion	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 défense contre les menaces à partir du Firepower 4100 en tant qu'instance native ou conteneur. Vous pouvez déployer plusieurs instances de conteneur par security engine, mais une seule instance native. Consultez Instances d'application du dispositif logique : instance de conteneur ou instance native pour connaître le nombre maximal d'instances de conteneur par modèle.

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

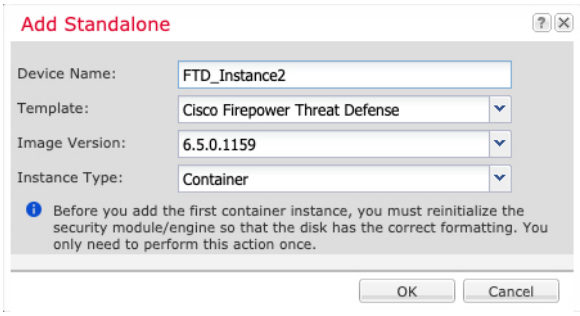
- Configurer l'interface de gestion à utiliser avec défense contre les menaces; voir Interfaces de configuration. L'interface de gestion est requise. Dans les versions 6.7 ou ultérieures, vous pouvez activer ultérieurement la gestion à partir d'une interface de données; mais vous devez affecter une interface 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 engine pour que le formatage du disque soit correct. Si cette action est requise, vous ne pourrez pas enregistrer votre dispositif logique. Cliquez sur **Security Engine**, 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
  - Adresse IP de la passerelle
  - Centre de gestion l'adresse IP et/ou l'ID NAT de votre choix

- 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**).

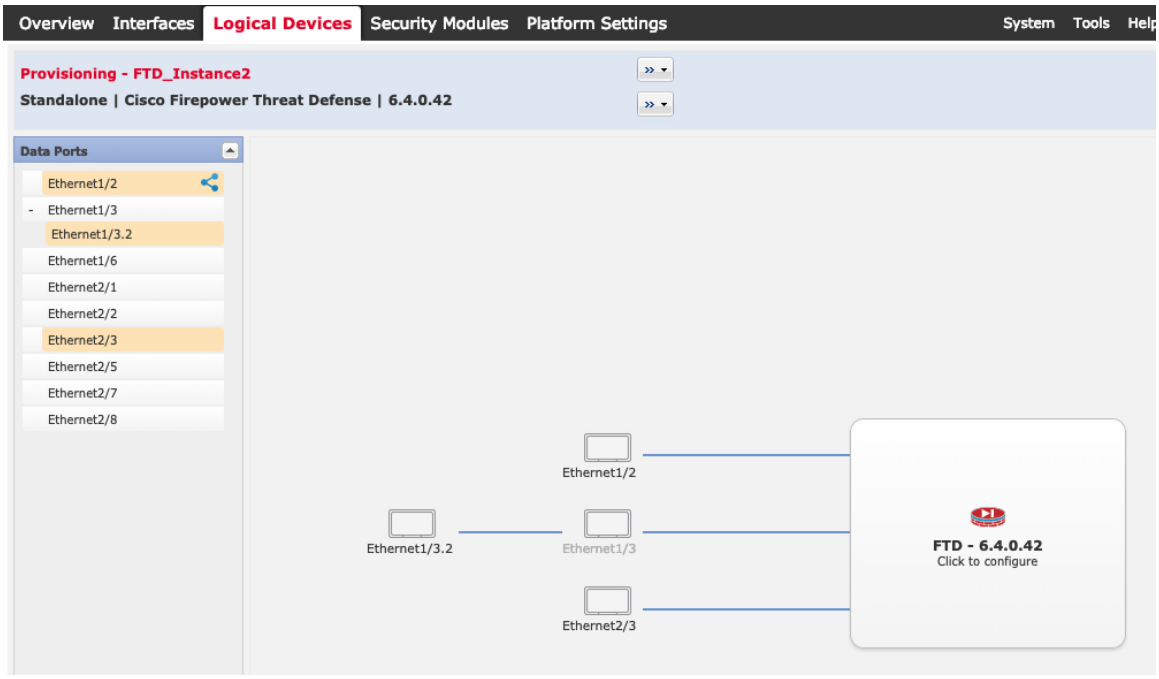
d) Choisissez le type d'instance (**Instance Type**): instance de conteneur (**Container**) ou instance native (**Native**).

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.

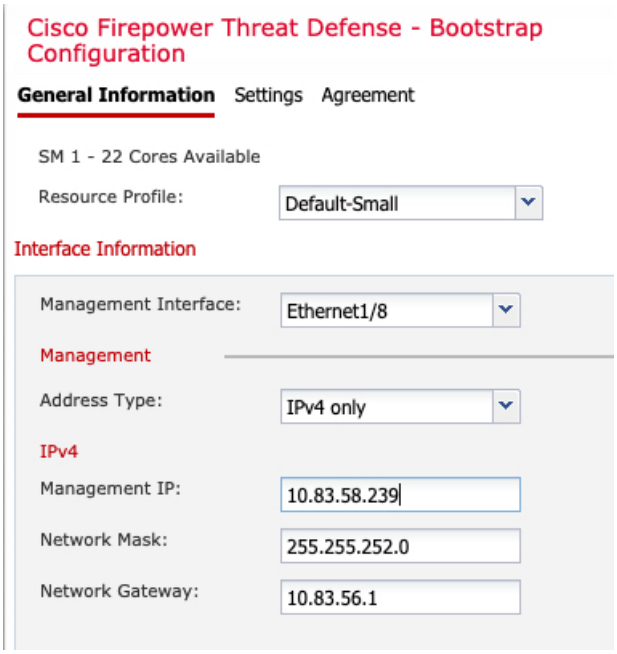
Vous pouvez affecter au maximum 10 interfaces de partage de données à une instance de conteneur. En outre, chaque interface de partage de données peut être affectée à tout au plus 14 instances de conteneur. Une interface de partage de données est indiquée par icône partage ( ).

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) 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.

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).

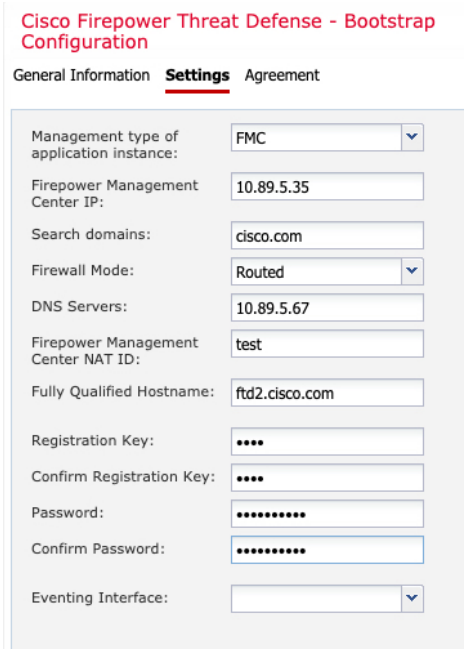
d) Configurez l'adresse IP de gestion (**Management IP**).

   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) 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**).

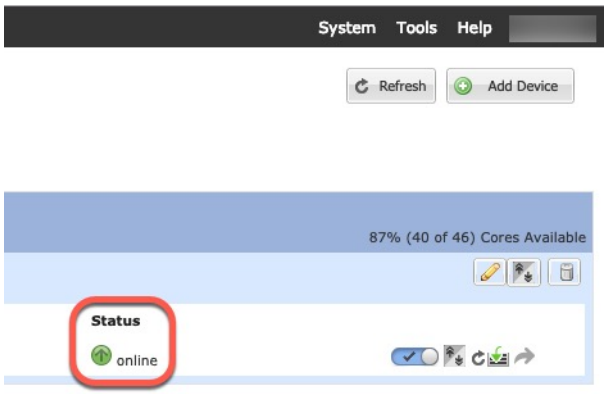
Ce paramètre active l'accélération cryptographique TLS dans le matériel et améliore les performances pour certains types de trafic. Pour obtenir plus d'informations, reportez-vous au Guide de configuration de Firepower Management Center. Cette fonctionnalité n'est pas prise en charge pour les instances 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 au 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.

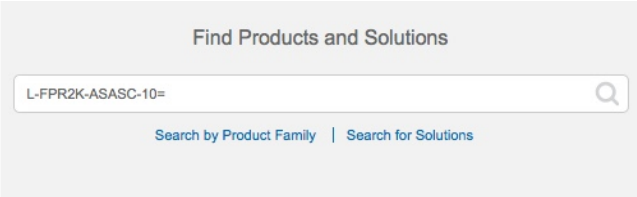
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

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-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-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-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y

- L-FPR4115T-TMC-5Y
- L-FPR4125T-TMC-1Y
- L-FPR4125T-TMC-3Y
- L-FPR4125T-TMC-5Y
- L-FPR4145T-TMC-1Y
- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y

- Cisco Secure Client : consultez le guide de commande Cisco Secure Client.
- Licence d'opérateur :
  - L-FPR4K-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.

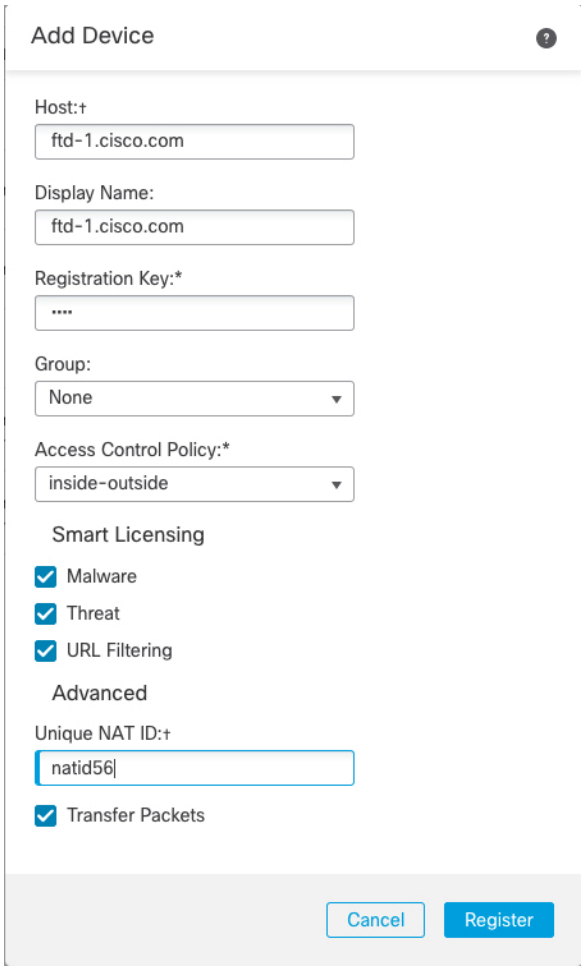
Avant de commencer

- 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 de défense contre les menaces (see Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 3) :
  - 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).



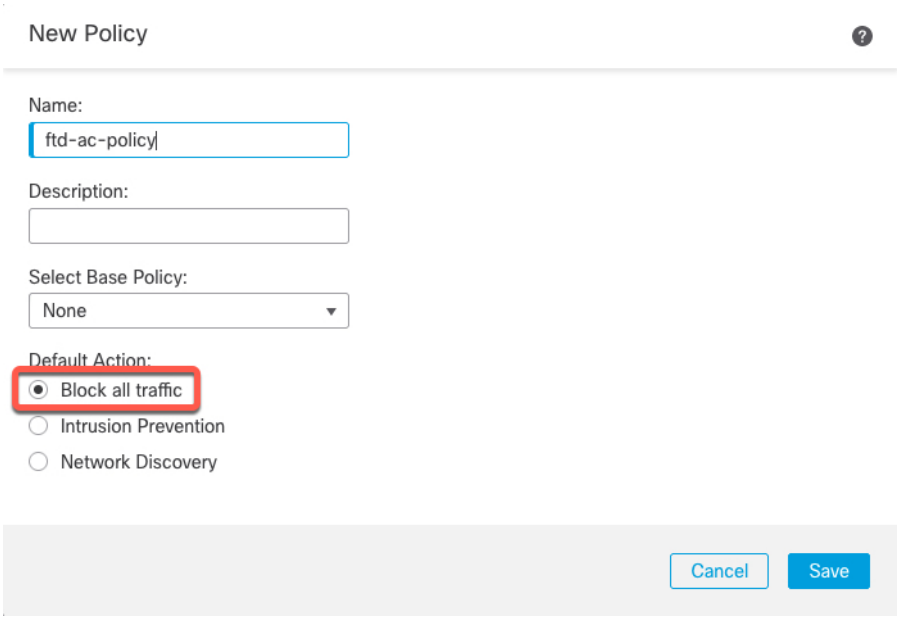
Définissez les paramètres suivants :

- **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 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 défense contre les menaces dans un centre de gestion secondaire, vous devez fournir l'adresse IP ou le nom d'hôte du dispositif de défense contre les menaces.

- **Display Name** (afficher le nom) : Saisissez le nom du dispositif de 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 24.

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**(transfer 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 27) 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 4100 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 15.
2	Configurer le serveur DHCP, à la page 18.

3	Ajouter la voie de routage par défaut, à la page 19.
4	Configurer NAT, à la page 21.
5	Permettre le trafic de l'intérieur vers l'extérieur, à la page 24.
6	Déployer la configuration, à la page 25.

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.

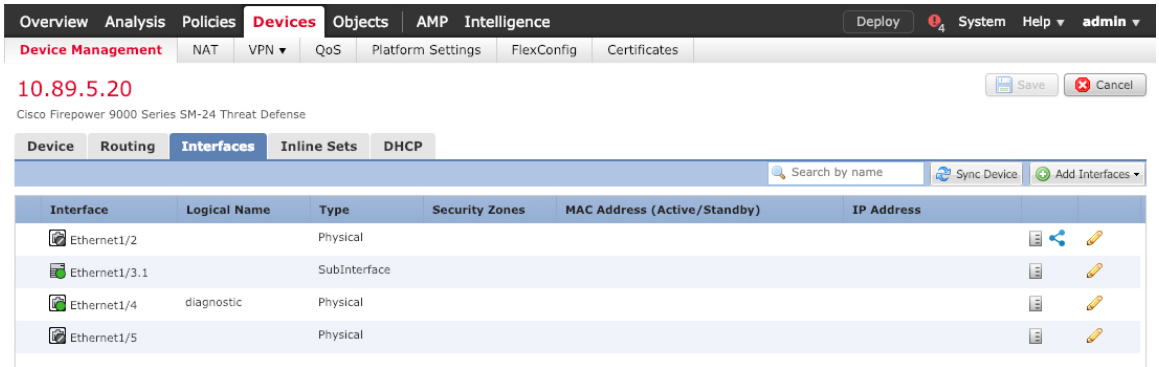
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

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

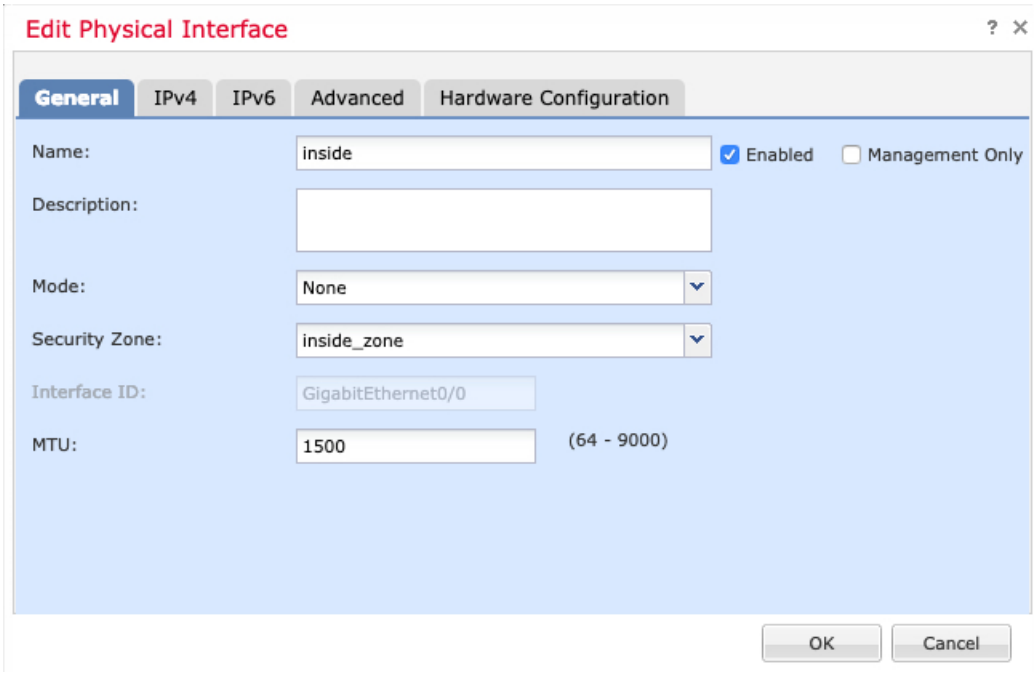
Étape 1 Choisissez **Devices (Dispositifs)** > **Device Management (Gestion du dispositif)**, et cliquez sur **Modifier** (✎) pour le pare-feu.

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).

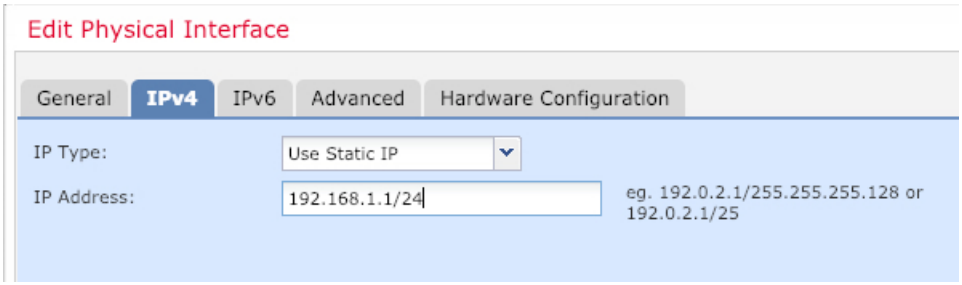
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

   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**.

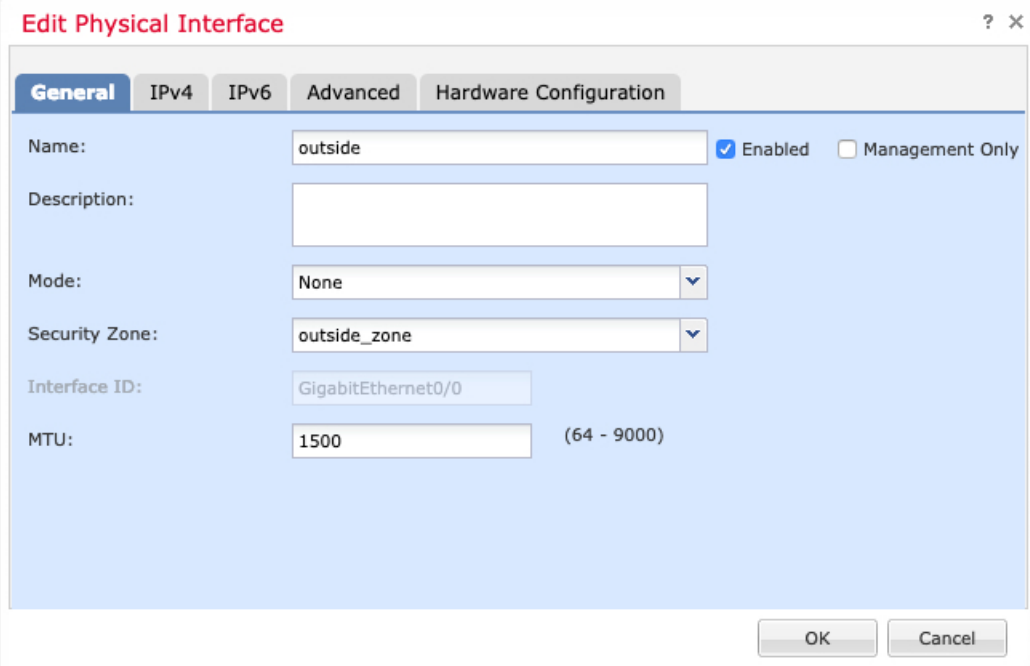


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

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.

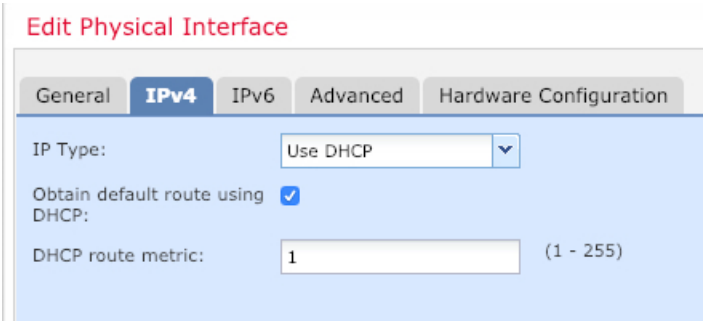
Par exemple, nommez l'interface **externe**.

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

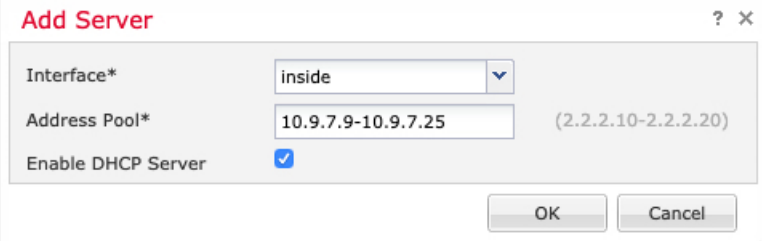
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de Défense contre les menaces.

Procédure

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

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).

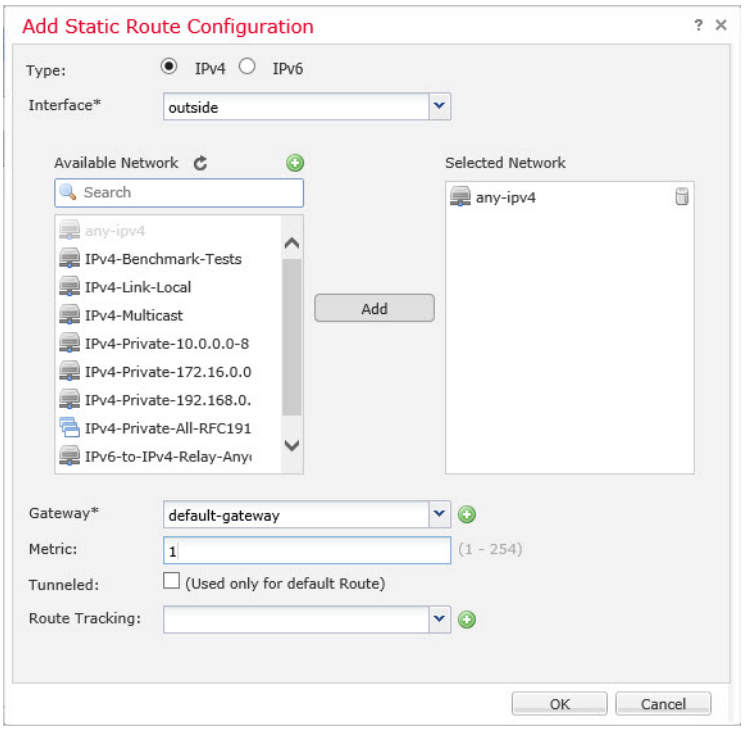
Ajouter la voie de routage par défaut

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 le dispositif.

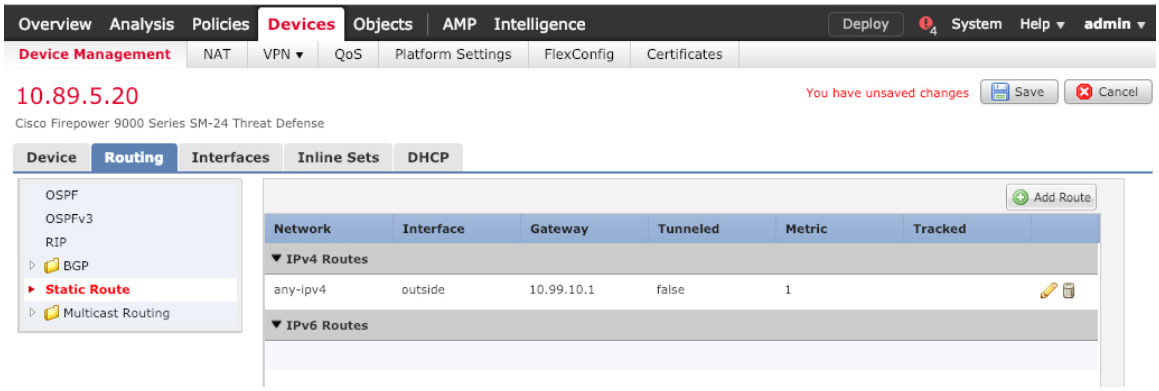
Étape 2 Sélectionnez **Routing (routage)** > **Static Route (route statique)**, cliquez sur **Add Route (ajouter route)**, et définissez ce qui suit :



- **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).

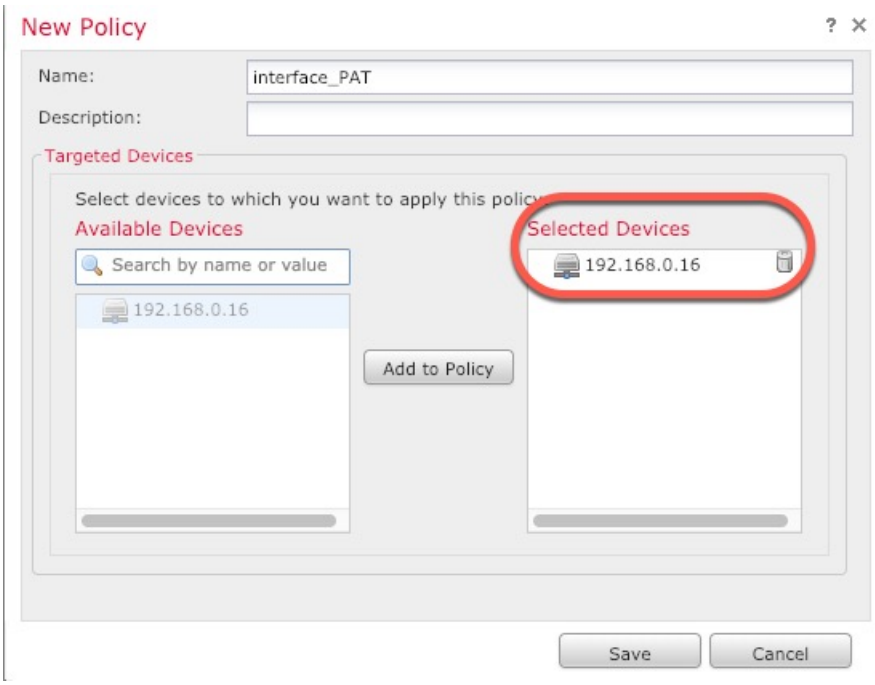
Configurer NAT

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.

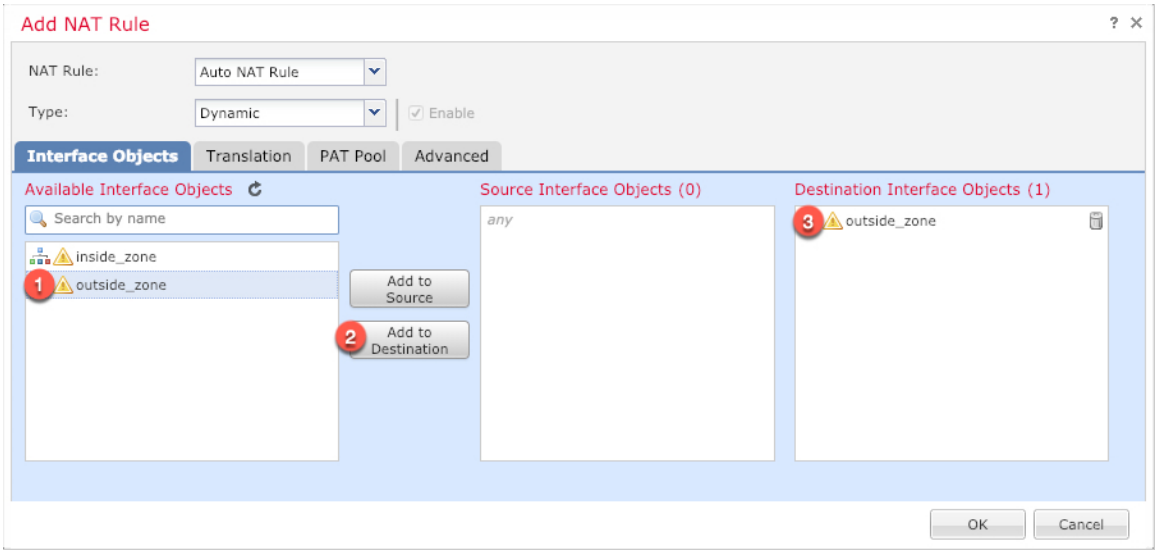
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

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

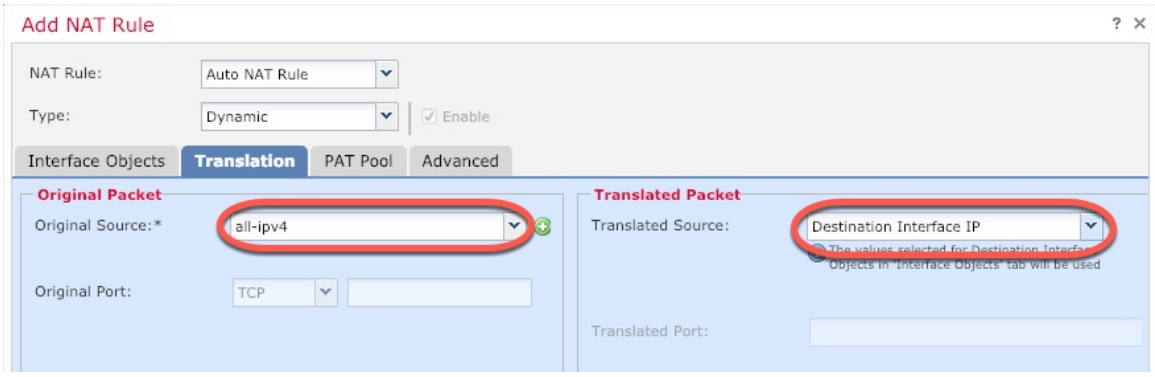
Étape 4 Configurez les options des règles de base :

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

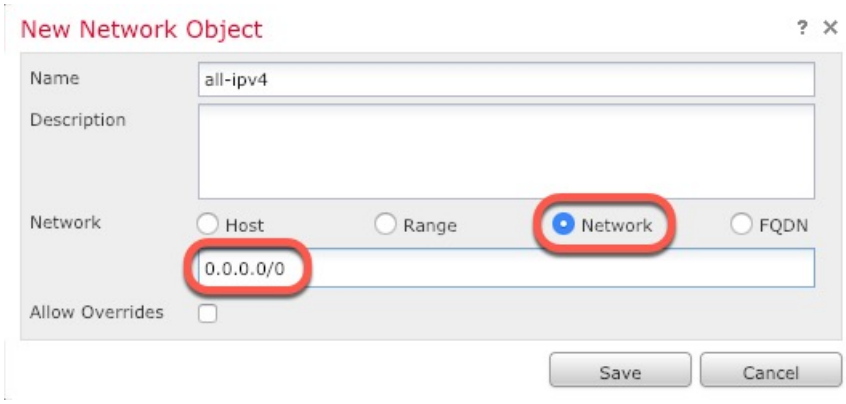
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



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).

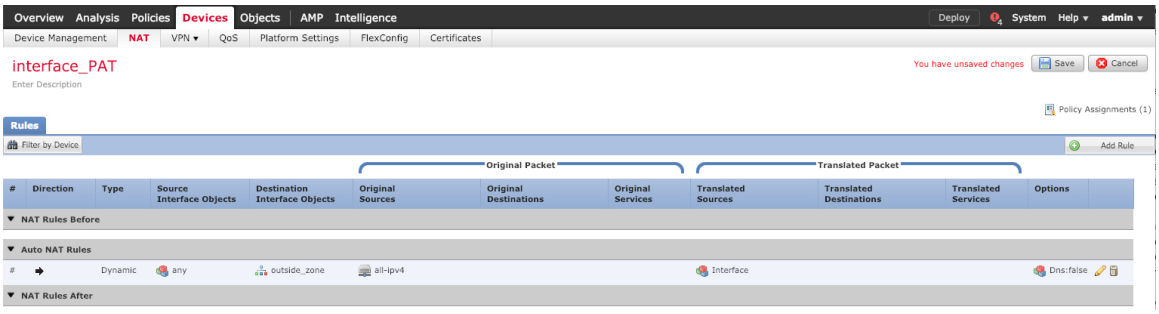


Remarque
Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **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**.

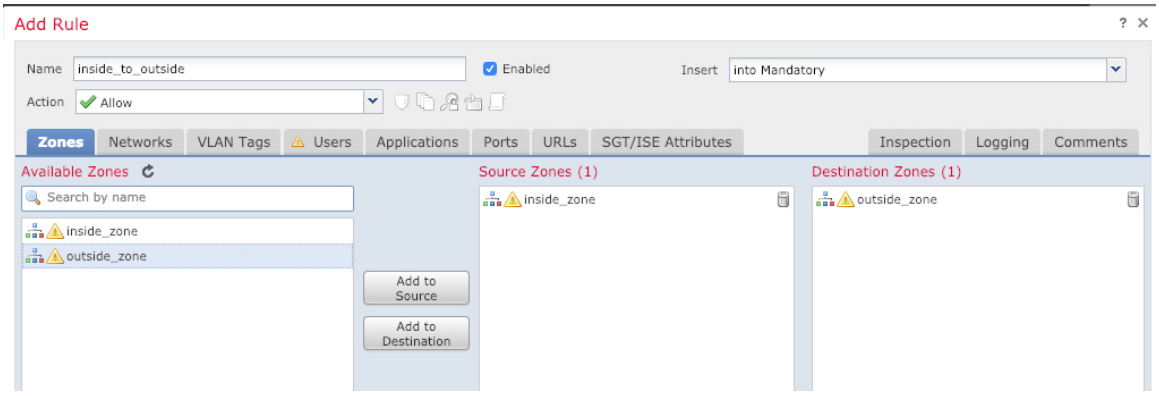
Permettre le trafic de l'intérieur vers l'extérieur

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 :



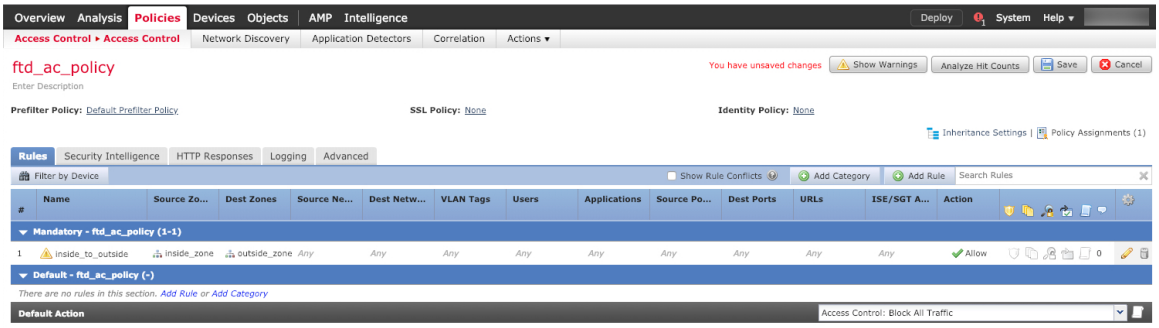
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

- **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).

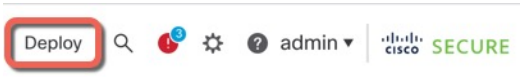
Déployer la configuration

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

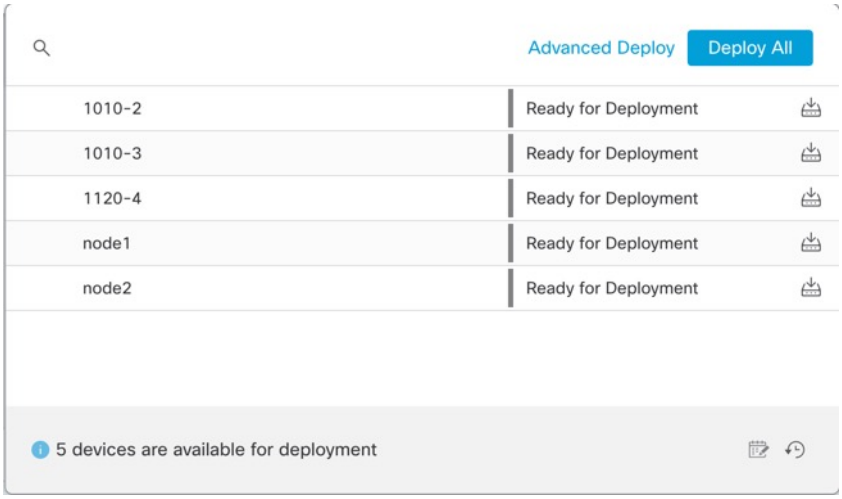
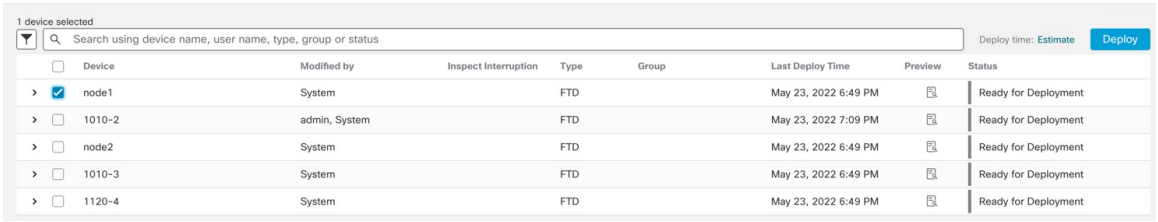
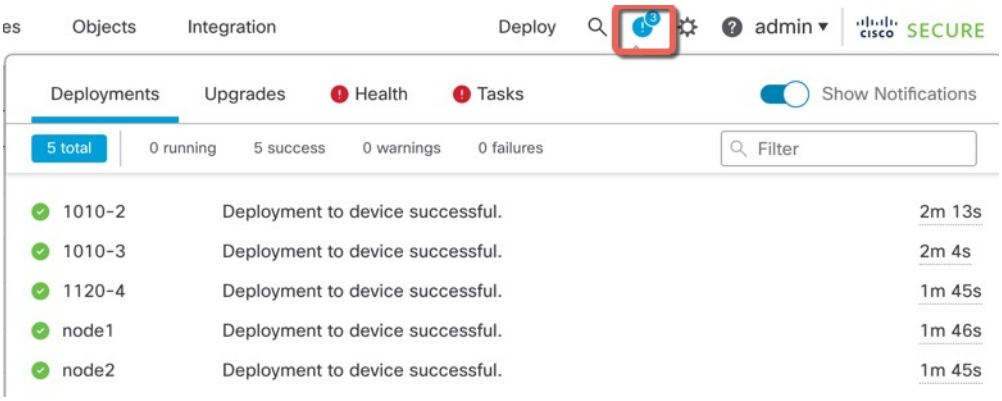


Illustration 5 : Déploiement avancé



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 engine.

connect module 1 {**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 deDéfense contre les menaces.

connect ftd *name*

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 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.
Défense contre les menaces pour les Firepower 4115, 4125 et 4145	6.4	Nous avons lancé les Firepower 4115, 4125 et 4145. **Remarque** FXOS 2.6.1 est nécessaire.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Capacité multi-instance pour 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 (Aperçu)** > **Devices (Dispositifs)** • **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Add New (Ajouter)** menu déroulant **> 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)**

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.