Défense contre les menaces Déploiement avec CDO

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

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

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

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

À propos du pare-feu

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

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

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

- À propos de la gestion par CDODéfense contre les menaces, à la page 2

À propos de la gestion par CDODéfense contre les menaces

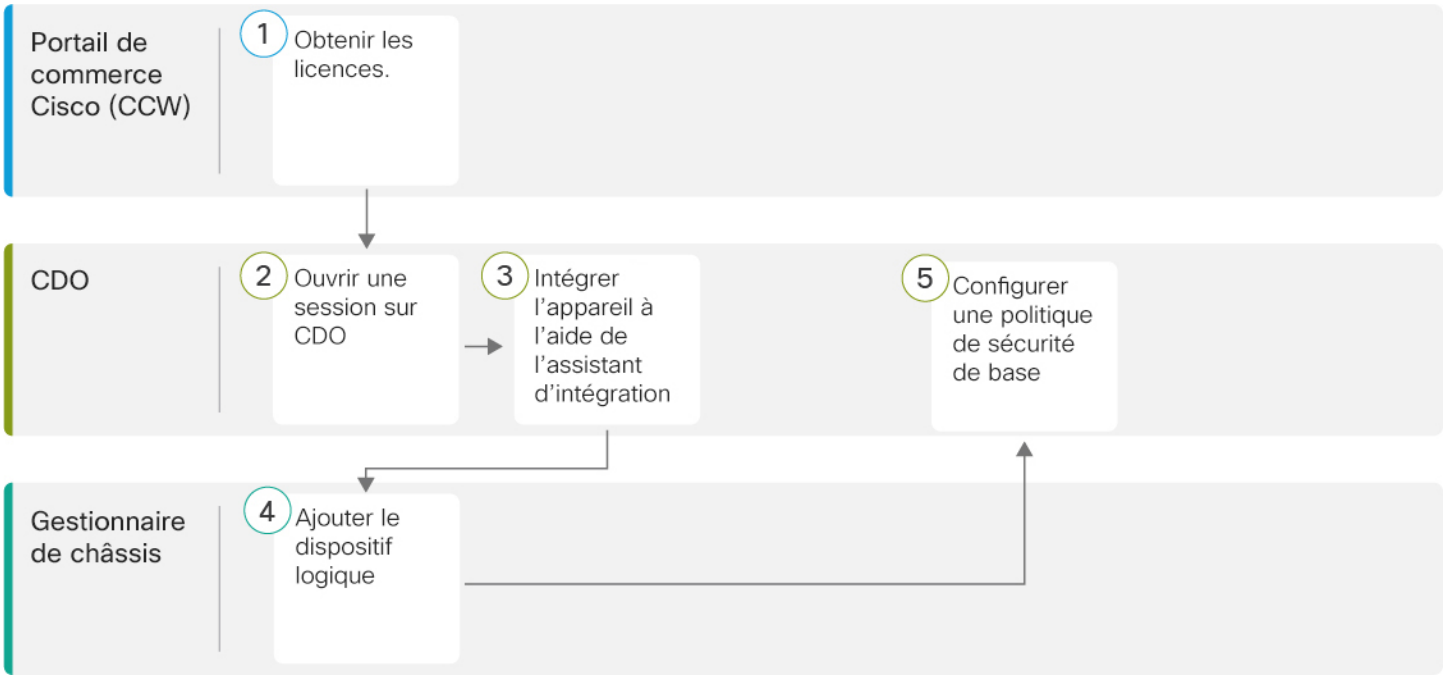
La solution infonuagique centre de gestion centre de gestion offre bon nombre des mêmes fonctions qu'une solution centre de gestion locale et présente la même apparence. Lorsque vous utilisez CDO en tant que gestionnaire principal, vous pouvez utiliser un centre de gestion local à des fins d'analyse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

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

Procédure de bout en bout

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

Illustration 1 : Procédure de bout en bout



1	Portail de commerce Cisco (CCW)	Obtenir des licences, à la page 3.
2	CDO	Ouvrez une session sur CDO, à la page 5.
3	CDO	Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 9.
4	Gestionnaire de châssis	Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 10.
5	CDO	Configurer une politique de sécurité de base.

Obtenir des licences

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

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

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

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

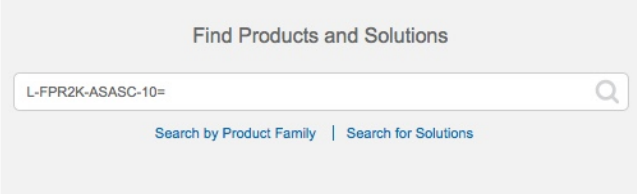
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines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

Procédure

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

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

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

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

Ouvrez une session sur CDO

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

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

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

- Si vous avez un compte Cisco Secure Sign-On, passez directement à Ouvrez une session sur CDO avec la connexion sécurisée Cisco Secure Sign-On., à la page 8.
- Si vous n'avez pas un compte Cisco Secure Sign-On, passez à Créer un nouveau compte de connexion Cisco Secure, à la page 5.

Créer un nouveau compte de connexion Cisco Secure

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

Avant de commencer

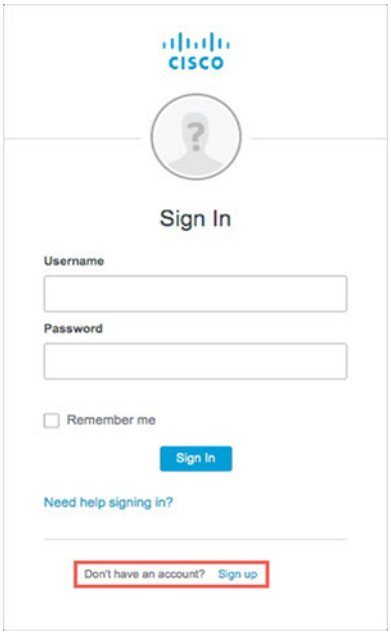
- **Install DUO Security** (installer la sécurité DUO) Nous vous recommandons d'installer l'application Duo Security sur un téléphone mobile. Consultez le guide Duo d'authentification à deux facteurs (guide d'inscription) (Duo Guide to Two Factor Authentication: Enrollment Guide) si vous avez des questions sur l'installation de Duo.
- **Time Synchronization** (synchronisation de l'heure) : Vous allez utiliser votre appareil mobile pour générer un mot de passe à usage unique. Il est important que l'horloge de votre appareil soit synchronisée avec le temps réel, car l'OTP est basé sur le temps. Faites en sorte que l'horloge de votre appareil soit réglée à l'heure exacte.
- Utilisez une version actuelle de Firefox ou de Chrome.

Procédure

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

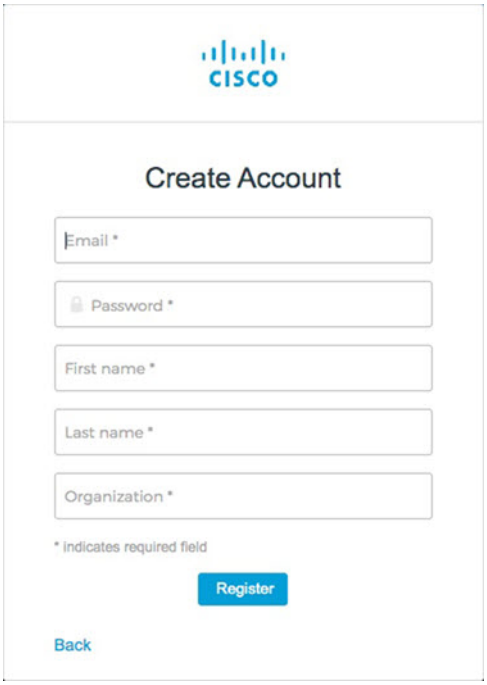
a) Rendez-vous sur https://sign-on.security.cisco.com.
b) Au bas de l'écran de connexion, cliquez sur **Sign up** (s'inscrire).

Illustration 3 : Inscription à Cisco SSO



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

Illustration 4 : Créer un compte



Astuces

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

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

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

a) Dans l'écran **Set up multi-factor authentication** (configurer l'authentification multifacteur), cliquez sur **Configure** (configurer).

b) Cliquez sur **Start setup** (démarrer la configuration) et suivez les invites pour choisir un appareil et vérifier l'appariement de cet appareil avec votre compte.

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

c) À la fin de la configuration avec l'assistant, cliquez sur **Continue to Login** (continuer la connexion).

d) Connectez-vous à Cisco Secure Sign-On avec l'authentification à deux facteurs.

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

a) Choisissez l'appareil mobile que vous jumelez avec Google Authenticator, puis cliquez sur **Next** (suivant).

b) Suivez les invites de l'assistant de configuration pour configurer Google Authenticator.

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

a) Choisissez une question et un mot de passe en cas d'oubli de mot de passe.

b) Choisissez un numéro de téléphone de récupération pour réinitialiser votre compte par SMS.

c) Choisissez une image de sécurité.

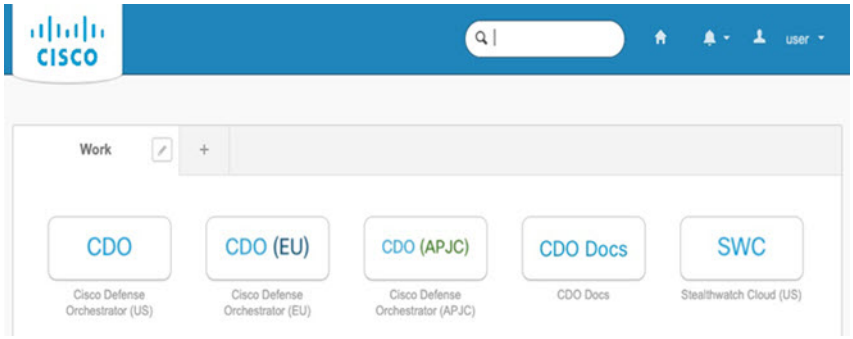
d) Cliquez sur **Create My Account** (créer mon compte).

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

Astuces

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

Illustration 5 : Tableau de bord Cisco SSO



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

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

Avant de commencer

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

- Pour vous connecter à CDO, vous devez d'abord créer votre compte dans Cisco Secure Sign-On et configurer MFA à l'aide de Duo; voir Créer un nouveau compte de connexion Cisco Secure, à la page 5.
- Utilisez une version actuelle de Firefox ou de Chrome.

Procédure

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

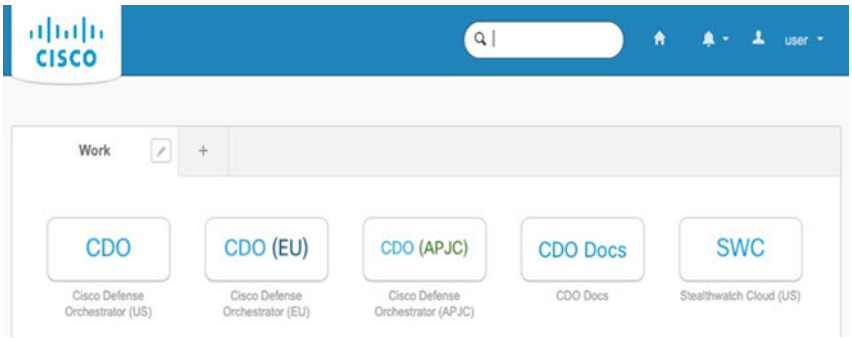
Étape 2 Saisissez votre nom d'utilisateur (**Username**) et votre mot de passe Cisco **Password**.

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

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

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

Illustration 6 : Tableau de bord Cisco SSO



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

- Si vous avez déjà un enregistrement utilisateur sur un locataire existant, vous êtes connecté à ce locataire.
- Si vous avez déjà un enregistrement utilisateur sur plusieurs locataires, vous pourrez choisir le locataire CDO avec lequel la connexion doit s'établir.

- Si vous n'avez pas encore d'enregistrement utilisateur sur un locataire existant, vous pourrez en savoir plus sur CDO ou demander un compte d'essai.

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

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

Procédure

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

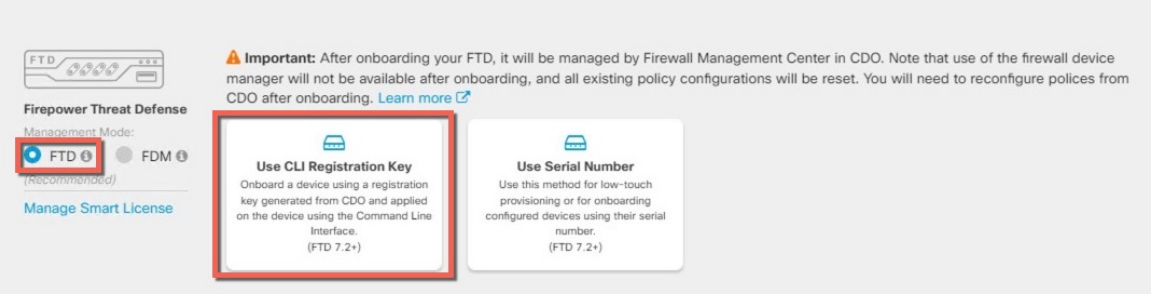
Étape 2 Sélectionnez la vignette **FTD**.

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

À tout moment, après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Manage Smart License (gérer la licence Smart)** pour inscrire ou modifier les licences Smart existantes disponibles pour votre appareil. Consultez pour savoir quelles licences sont disponibles.Obtenir des licences, à la page 3

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

Illustration 7 : Utiliser la clé d'enregistrement de l'interface de ligne de commande



Étape 5 Saisissez le **Device Name** (Nom du dispositif), puis cliquez sur **Next** (Suivant).

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

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

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

configure manager add *nom_de_domaine_cdo clé_d_enregistrement identifiant_nat nom_d_affichage*

Dans le gestionnaire de châssis lorsque vous déployez le dispositif logique (consultez Gestionnaire de châssis : ajouter le dispositif logique Défense contre les menaces, à la page 10), copiez ceci

Exemple :

Exemple de commande :

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

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

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

Prochaine étape

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

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

Vous pouvez déployer défense contre les menaces à partir du Firepower 4100 en tant qu'instance native autonome. CDO ne prend pas en charge les instances ou les grappes de contenant.

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

Avant de commencer

- Configurer l'interface de gestion à utiliser avec défense contre les menaces; voir Interfaces de configuration. L'interface de gestion est requise. Vous pouvez activer ultérieurement la gestion à partir d'une interface de données; mais vous devez affecter une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données. Il convient de souligner que cette interface de gestion est différente du port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**).
- Vous devez également configurer au moins une interface de données.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce dispositif
  - l'adresse IP et le masque de réseau de l'interface de gestion

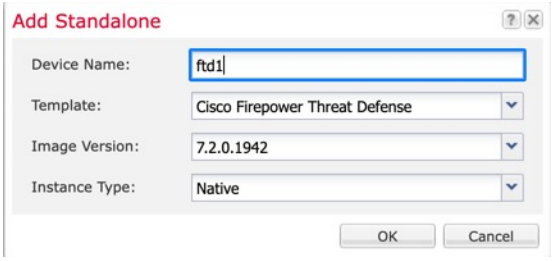
- Adresse IP de la passerelle
- Nom d'hôte de CDO, clé d'enregistrement et ID de NAT généré par CDO. Consultez Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 9.
- Adresse IP du serveur DNS

Procédure

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

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

Illustration 8 : Ajouter un dispositif autonome



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

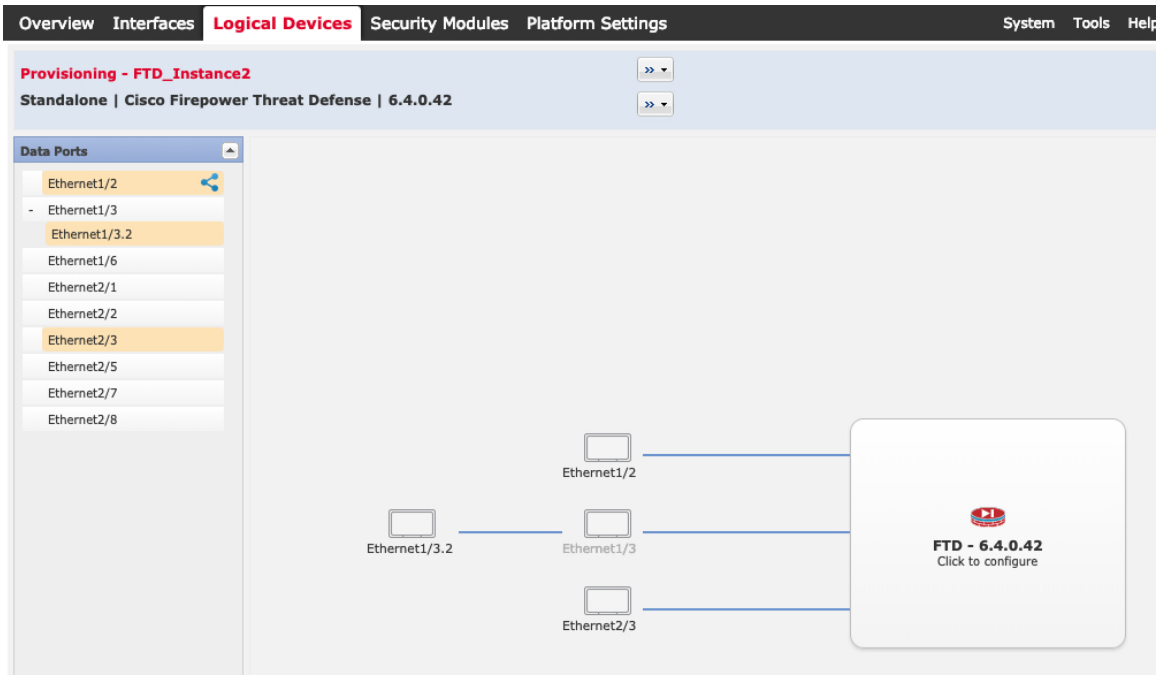
Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de dispositif utilisé dans la configuration de l'application.

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

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

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

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



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

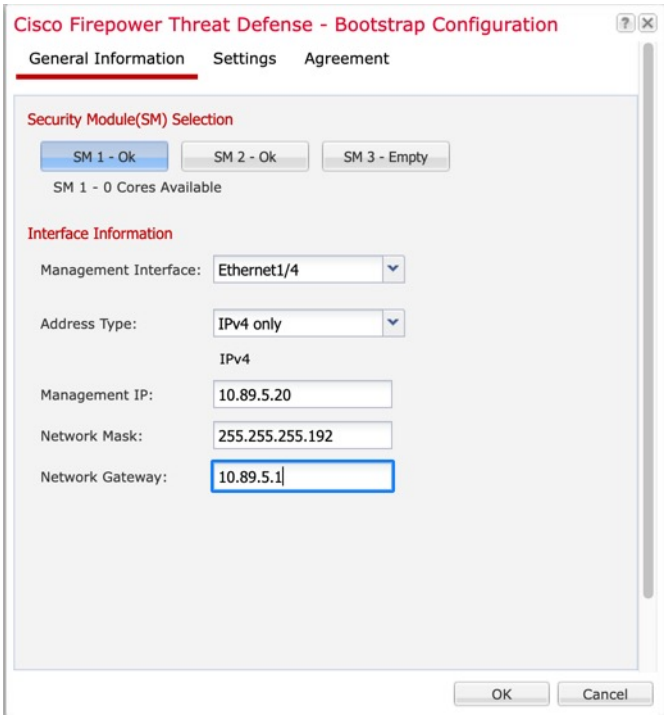
Hardware Bypass : Les ports compatibles sont représentés par l'icône suivante : . Pour certains modules d'interface, vous pouvez activer la fonction de contournement matériel pour les interfaces d'ensemble en ligne uniquement. Le contournement matériel garantit que le trafic continue de circuler entre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

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

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

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

Illustration 9 : Renseignements généraux



a) 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.

b) 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).

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

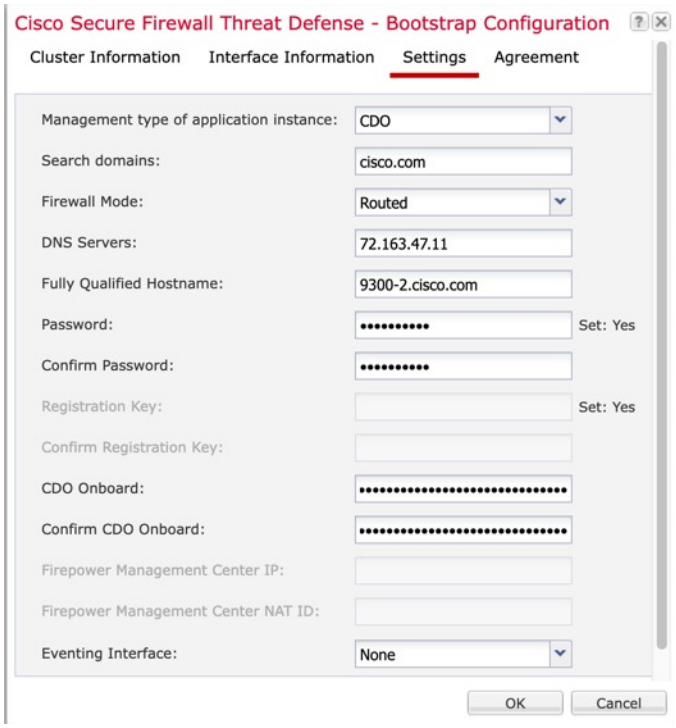
   Définissez une adresse IP unique pour cette interface.

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

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

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

Illustration 10 : Paramètres



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

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

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

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

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

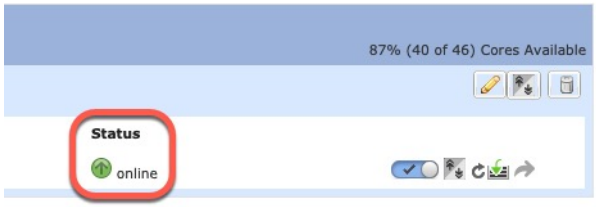
e) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour défense contre les menaces.
f) Saisissez un mot de passe (**Password**) pour l'utilisateur admin défense contre les menaces pour l'accès à l'interface de ligne de commande.
g) Copiez la commande générée par CDO dans les champs **CDO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

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

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

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

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



Configurer une politique de sécurité de base

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

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

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

1	Configurer les interfaces.
2	Configurer le serveur DHCP.
3	Ajouter la voie de routage par défaut.

4	Configurer NAT.
5	Permettre le trafic de l'intérieur vers l'extérieur.
6	Déployer la configuration.

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.

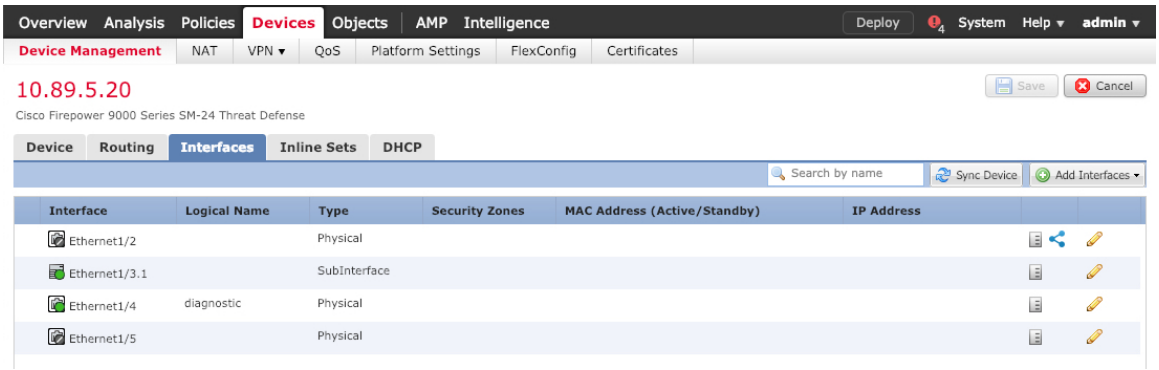
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

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

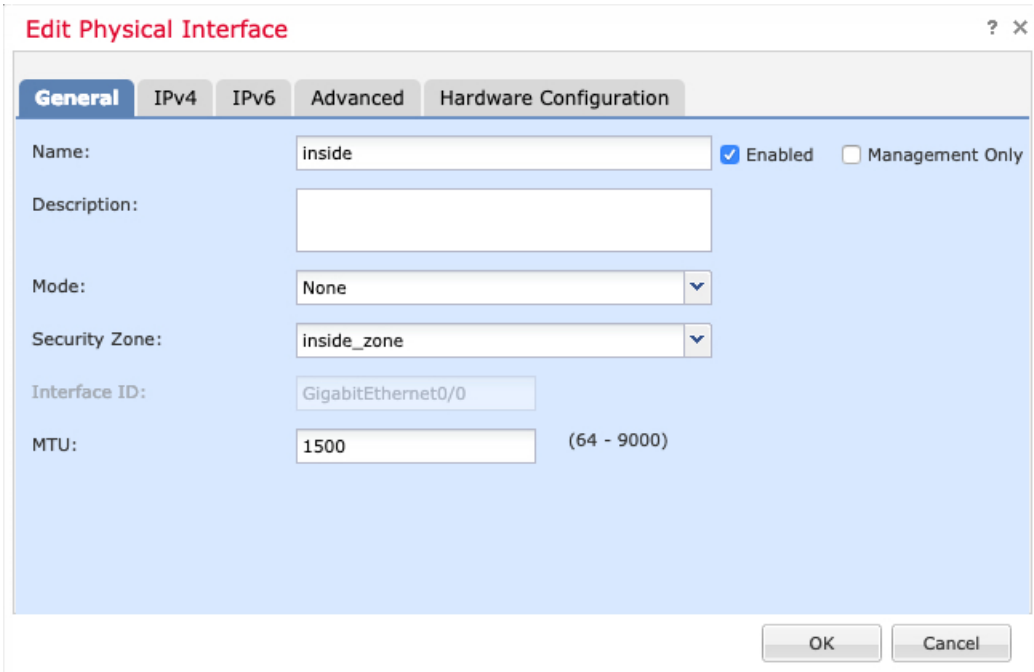
Étape 1 Choisissez **Devices (Dispositifs)** > **Device Management (Gestion du dispositif)**, et cliquez sur **Modifier** (✎) pour le pare-feu.

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).

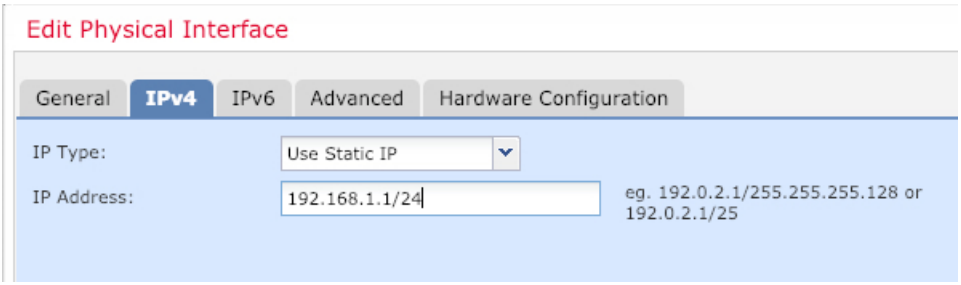
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

   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**.

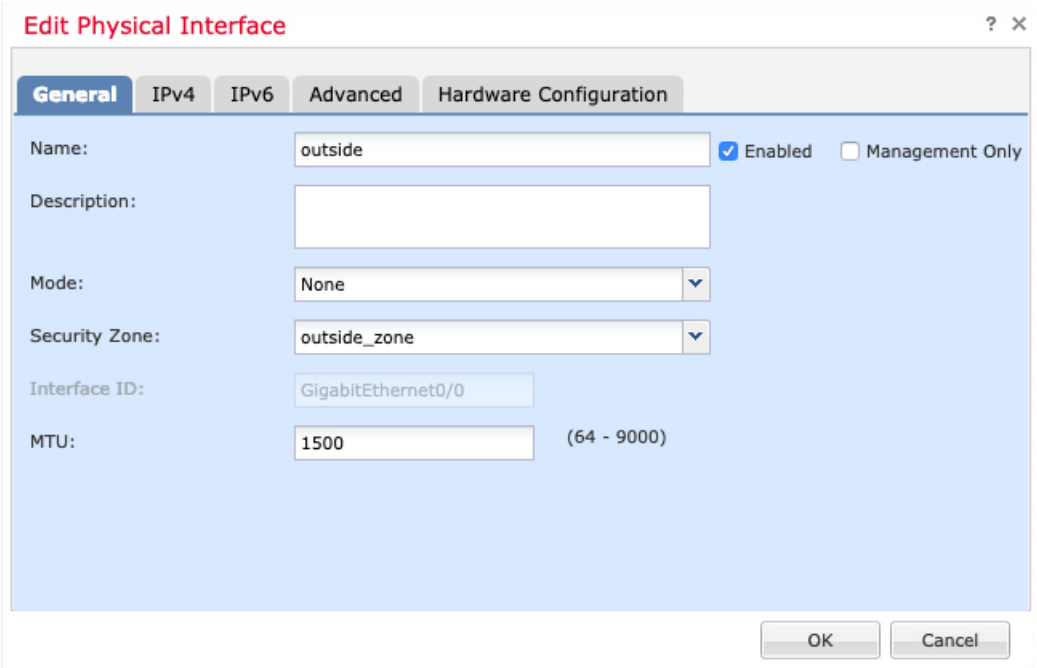


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

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.

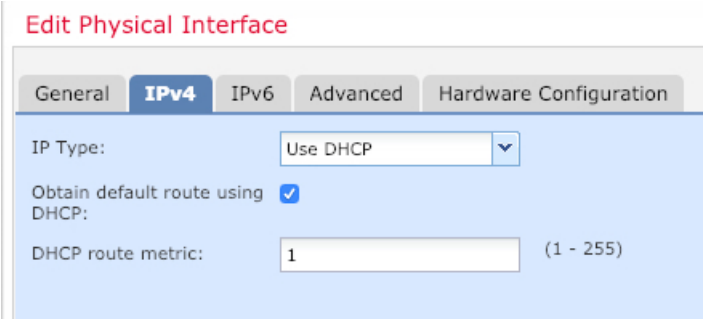
Par exemple, nommez l'interface **externe**.

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

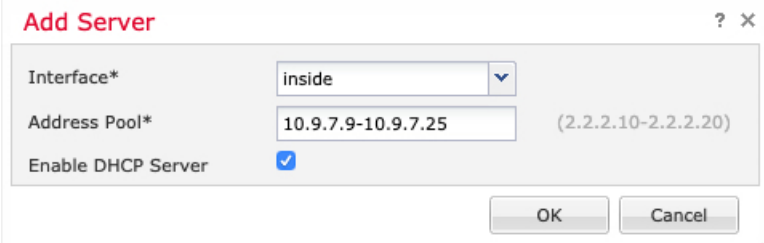
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de Défense contre les menaces.

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).

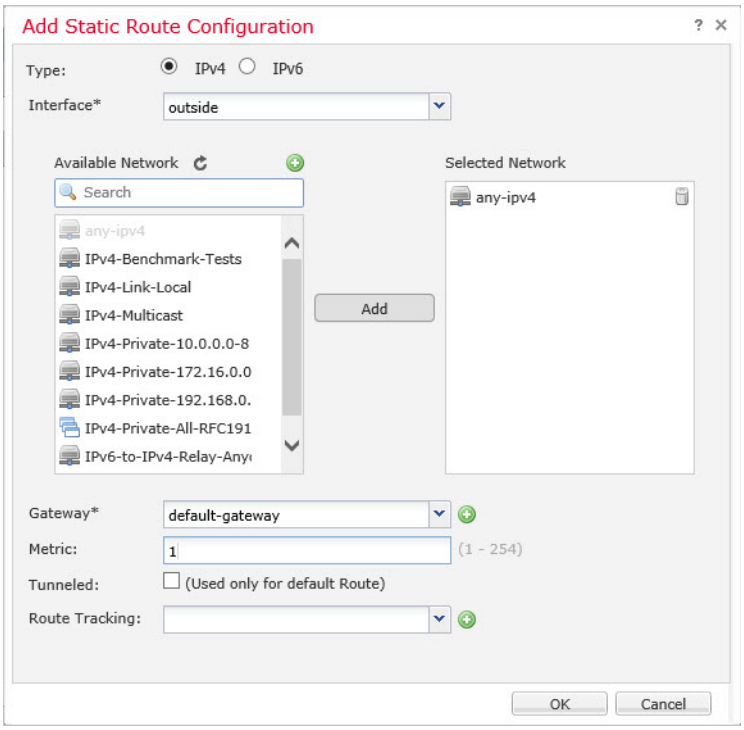
Ajouter la voie de routage par défaut

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.

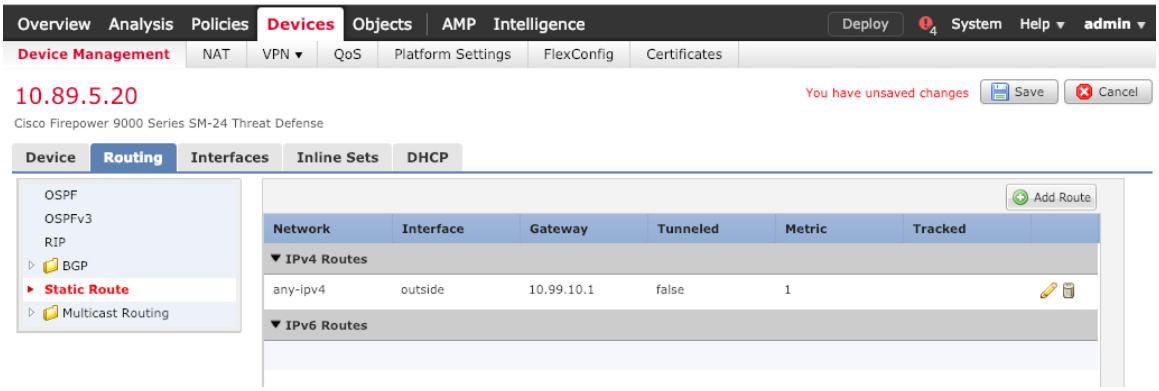
Étape 2 Sélectionnez **Routing (routage)** > **Static Route (route statique)**, cliquez sur **Add Route (ajouter route)**, et définissez ce qui suit :



- **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).

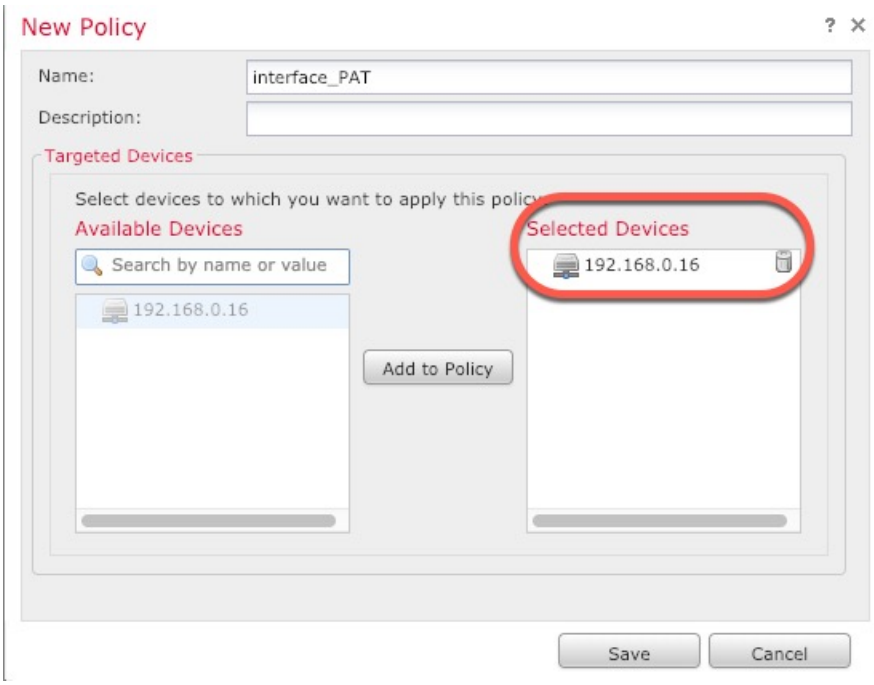
Configurer NAT

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.

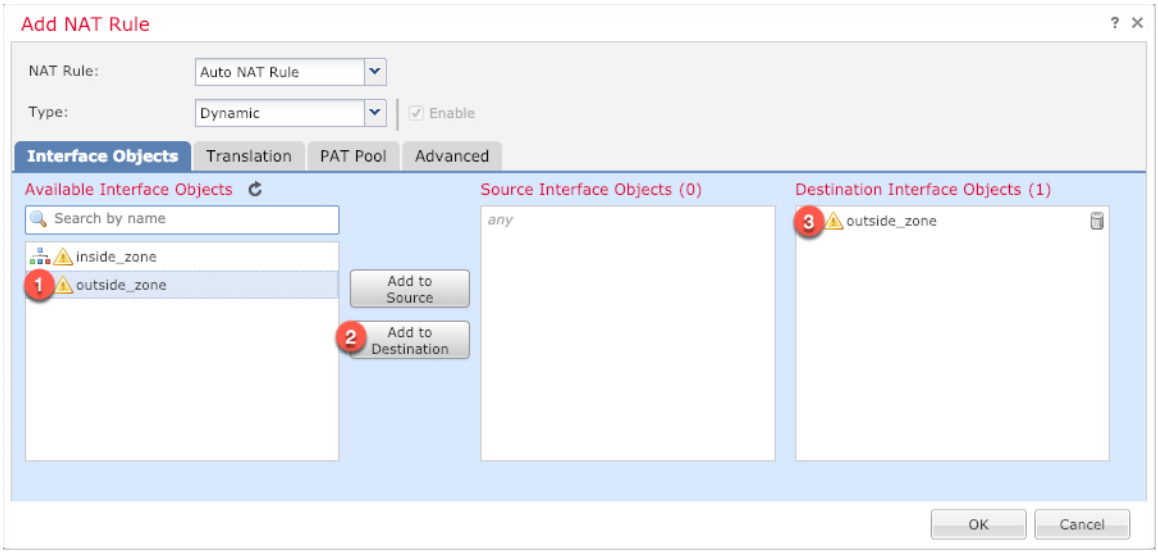
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

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

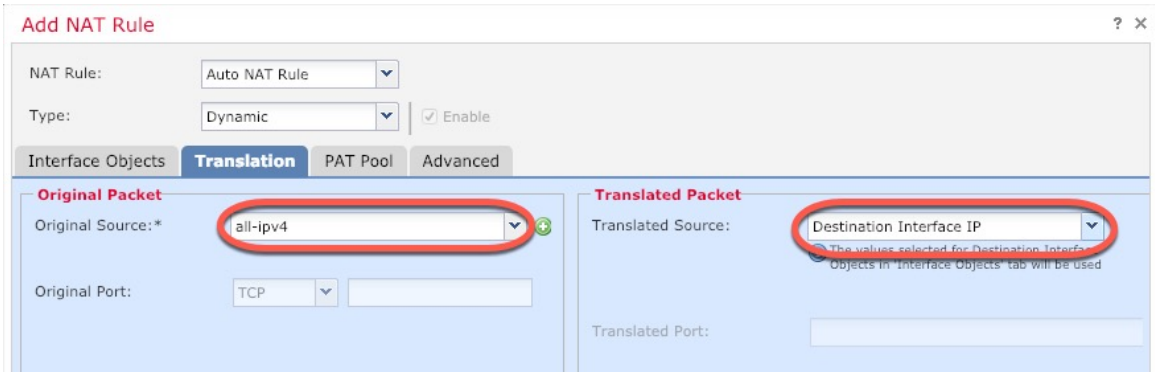
Étape 4 Configurez les options des règles de base :

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

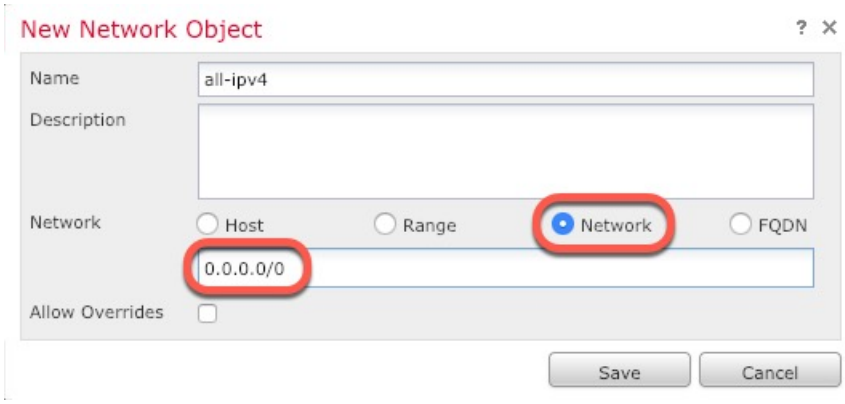
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



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).

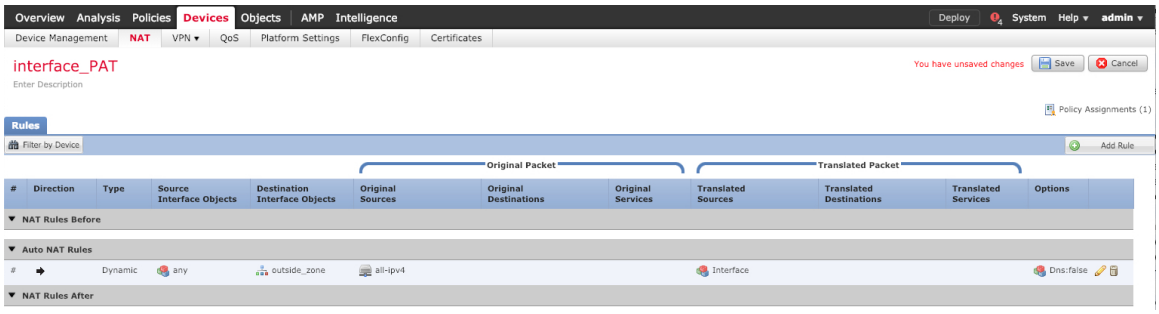


Remarque
Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **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**.

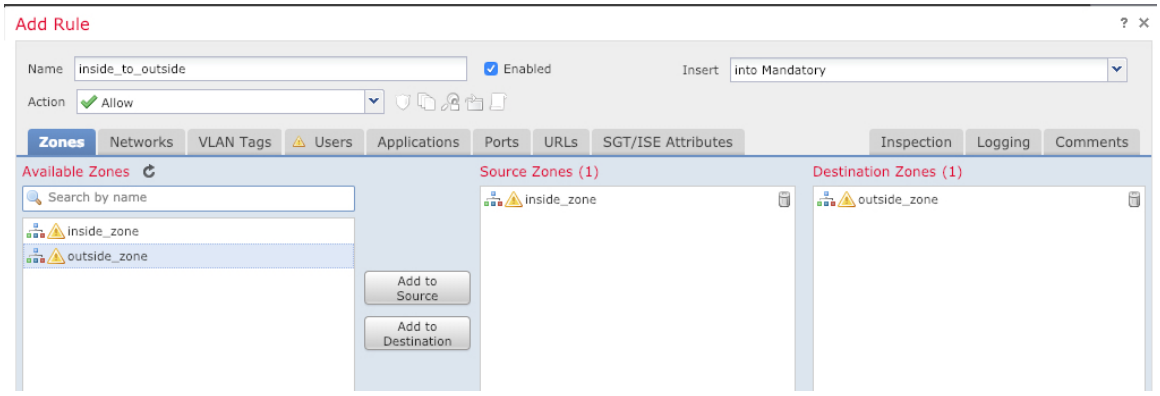
Permettre le trafic de l'intérieur vers l'extérieur

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 :



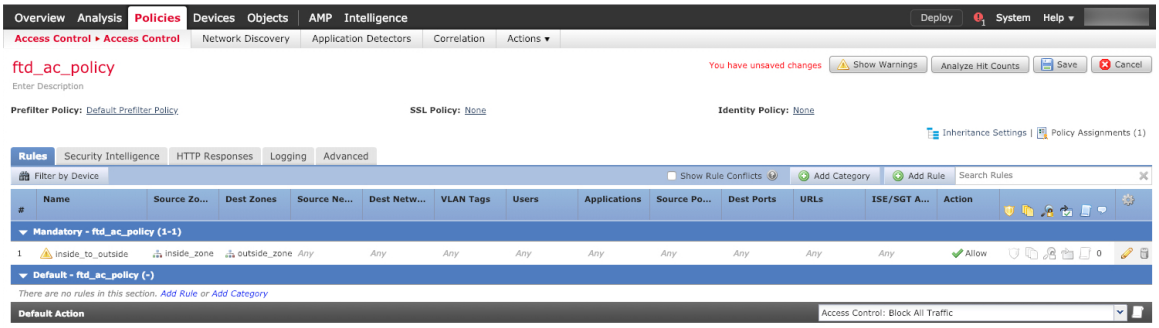
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

- **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).

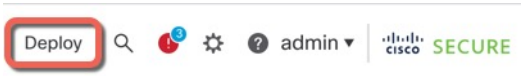
Déployer la configuration

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 11 : 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 12 : Déployer tout

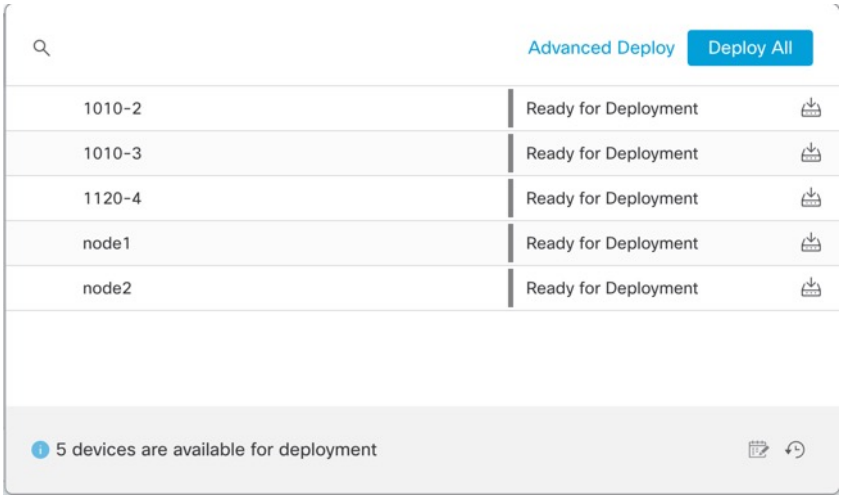
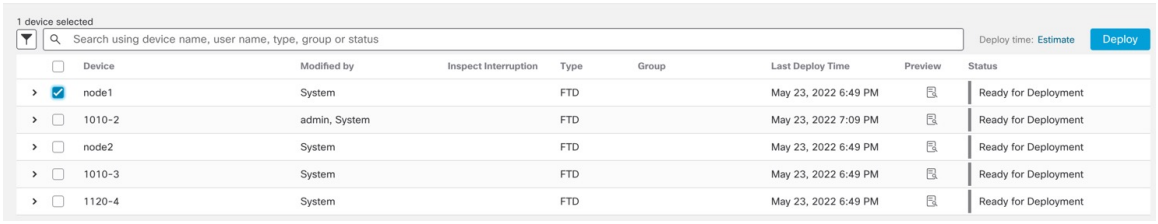
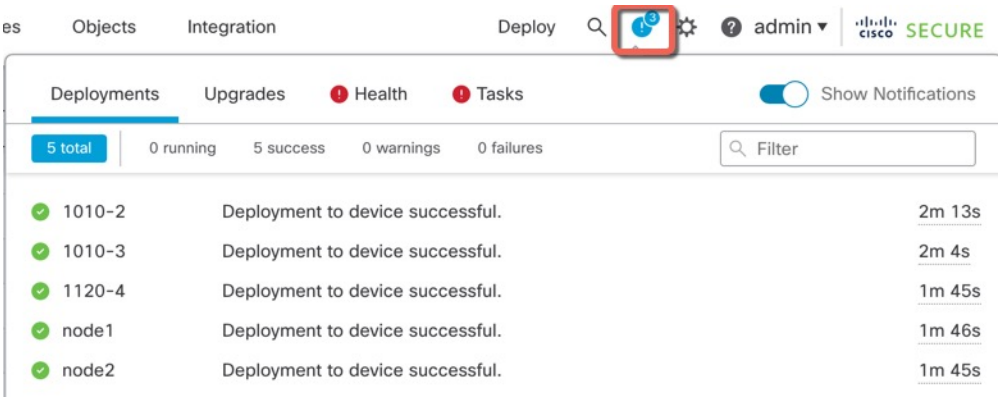


Illustration 13 : Déploiement avancé



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 14 : État du déploiement



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

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

Procédure

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

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

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

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

a) Connectez-vous au security 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#
```

Prochaines étapes

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

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.