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, voir Quels sont le et 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.

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 périphérique. 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 la gamme Firepower 1000/2100 de défense contre les menaces Firepower pour obtenir plus de renseignements.

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

À propos de la gestion par CDODéfense contre les menaces

Solution infonuagique Cisco Secure Firewall Management Center

La solution infonuagique centre de gestion offre bon nombre des mêmes fonctions qu'une solution locale centre de gestionet 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.

CDO Méthodes d'intégration

Vous pouvez intégrer un appareil des manières suivantes :

- Provisionnement simplifié à l'aide du numéro de série :
  - Un administrateur du bureau central envoie défense contre les menaces au bureau distant. Aucune préconfiguration n'est requise. En fait, il importe que vous ne configuriez rien sur l'appareil, car l'approvisionnement à faible intervention ne fonctionne pas avec les appareils préconfigurés.

Remarque L'administrateur central peut préenregistrer le défense contre les menaces sur CDO à l'aide du numéro de série défense contre les menaces avant d'envoyer l'appareil à la succursale.

  - L'administrateur du bureau assure le câblage et la mise sous tension de défense contre les menaces .
  - L'administrateur central termine la configuration du défense contre les menaces en utilisant le CDO.

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

- Assistant de préparation à l'aide de l'enregistrement de l'interface de ligne de commande : utilisez cette méthode manuelle si vous devez effectuer une préconfiguration ou si vous utilisez une interface de gestionnaire que le provisionnement rapide ne prend pas en charge.

Défense contre les menaces Interface d'accès du gestionnaire

Vous pouvez utiliser l'interface de gestion ou de l'interface externe pour l'accès du gestionnaire. Cependant, ce guide couvre l'accès à l'interface externe. Le provisionnement à faible intervention humaine ne prend en charge que l'interface extérieure.

L'interface de gestion est une interface particulière configurée séparément des interfaces de données défense contre les menaces , et elle possède ses propres paramètres réseau. Les paramètres réseau de l'interface de gestion sont toujours utilisés même si vous activez l'accès du gestionnaire sur une interface de données. Tout le trafic de gestion continue d'être acheminé depuis ou vers l'interface de gestion. Lorsque vous activez l'accès au gestionnaire sur une interface de données, le défense contre les menaces transfère le trafic de gestion entrant sur le fond de panier vers l'interface de gestion. Pour le trafic de gestion sortant, l'interface de gestion achemine le trafic sur le fond de panier vers l'interface de données.

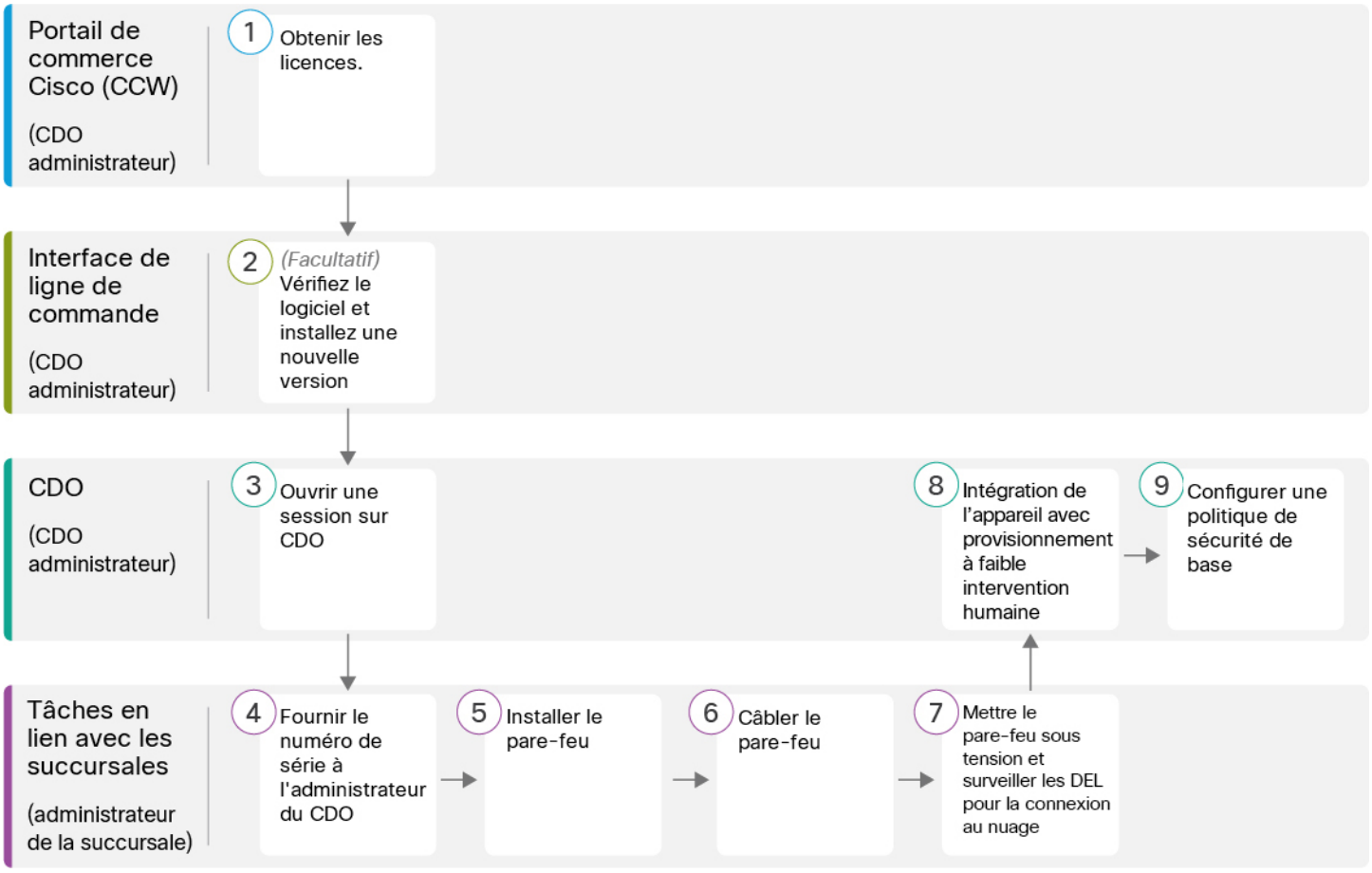
L'accès du gestionnaire à partir d'une interface de données présente les limites suivantes :

- Vous ne pouvez activer l'accès du gestionnaire que sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI exige PPPoE, vous devrez placer un routeur avec support PPPoE entre le défense contre les menaces et le modem WAN.
- L'interface doit être dans le VRF global seulement.
- SSH n'est pas activé par défaut pour les interfaces de données, vous devrez donc activer SSH ultérieurement à l'aide de l'option centre de gestion. Comme la passerelle de l'interface de gestion sera transformée en interfaces de données, vous ne pouvez pas non plus autoriser SSH vers l'interface de gestion à partir d'un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**.

Procédure de bout en bout : Provisionnement à faible intervention

Consultez les tâches suivantes pour déployer défense contre les menaces avec CDO à l'aide d'un provisionnement à faible intervention humaine.

Illustration 1 : Procédure de bout en bout : Provisionnement à faible intervention



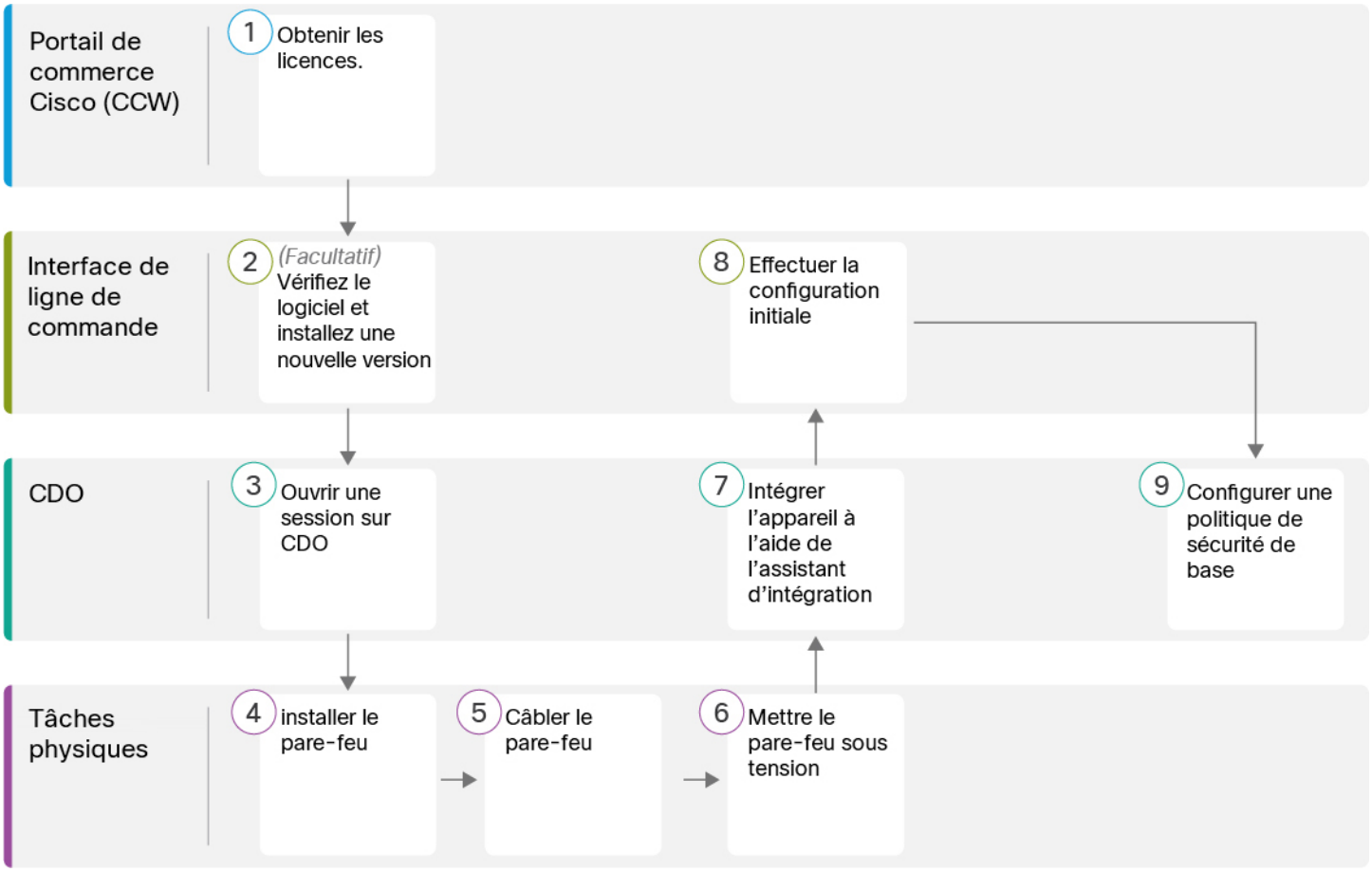
1	Portail de commerce Cisco (CCW) (cDO administrateur)	Obtenir des licences, à la page 7.
2	Interface de ligne de commande (CDO administrateur)	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 8.
3	CDO (CDO administrateur)	Ouvrez une session sur CDO, à la page 10.
4	Tâches en lien avec les succursales (administrateur de la succursale)	Présenter le numéro de série du pare-feu à l'administrateur central, à la page 14.

5	Tâches en lien avec les succursales (administrateur de la succursale)	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.
6	Tâches en lien avec les succursales (administrateur de la succursale)	Câbler le pare-feu, à la page 15.
7	Tâches en lien avec les succursales (administrateur de la succursale)	Mettez le pare-feu sous tension, à la page 16.
8	CDO (CDO administrateur)	Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 17.
9	CDO (CDO administrateur)	Configurer une politique de sécurité de base, à la page 33.

Procédure de bout en bout : Assistant de préparation

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

Illustration 2 : Procédure de bout en bout : Assistant de préparation



1	Portail de commerce Cisco (CCW)	Obtenir des licences, à la page 7.
2	Interface de ligne de commande	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 8.
3	CDO	Ouvrez une session sur CDO, à la page 10.
4	Tâches physiques	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.
5	Tâches physiques	Câbler le pare-feu, à la page 18.
6	Tâches physiques	Mettez le pare-feu sous tension, à la page 20.
7	CDO	Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 20.

8	Interface de ligne de commande ou Gestionnaire d'appareil	• Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 22. • Effectuer la configuration initiale à l'aide du Gestionnaire d'appareil, à la page 27.
9	CDO	Configurer une politique de sécurité de base, à la page 33.

Préconfiguration de l'administrateur central

Cette section décrit comment obtenir des licences de fonctionnalités pour votre pare-feu; comment installer une nouvelle version du logiciel avant le déploiement; et comment se connecter à CDO.

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 de sécurité et IPS de nouvelle génération
- **Programme malveillant** : défense contre les programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only

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.

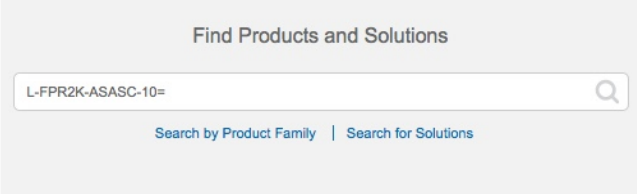
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines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



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

- Combinaison de licences englobant les menaces, les logiciels malveillants et les adresses URL :
  - L-FPR1010T-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-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- RA VPN : Voir le Guide de commande Cisco AnyConnect.

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.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une version différente, procédez comme suit. Nous vous recommandons d'installer votre version cible avant de configurer le pare-feu. Vous pouvez également effectuer une mise à niveau une fois que vous êtes opérationnel, mais la mise à niveau, qui préserve votre configuration, peut prendre plus de temps que cette procédure.

Quelle version dois-je exécuter?

Cisco recommande d'exécuter une version Gold Star indiquée par une étoile dorée à côté du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de version décrite dans https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; par exemple, ce bulletin décrit la numérotation des versions à court terme (avec les dernières fonctionnalités), la numérotation des versions à long terme (versions de maintenance et correctifs pour une période plus longue) ou la numérotation des versions à très long terme (versions de maintenance et correctifs pour le période la plus longue, pour la certification gouvernementale).

Avant de commencer

Pour le provisionnement à faible intervention humaine, si vous vous connectez et que vous modifiez le mot de passe, vous désactivez le processus de provisionnement à faible intervention humaine. Vous ne devez vous

connecter et effectuer une nouvelle image que si vous savez déjà que vous devez modifier la version du logiciel. Si vous vous êtes connecté et que vous souhaitez restaurer la capacité de provisionnement à faible intervention humaine sans installer de logiciel, vous pouvez effectuer une réinitialisation d'usine. Consultez le Guide de dépannage FXOS.

Procédure

Étape 1 Mettez le pare-feu sous tension et connectez-vous au port de console. Reportez-vous à Mettez le pare-feu sous tension, à la page 20 et à Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 44 pour en savoir davantage.

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

Vous vous connectez à Interface de ligne de commande FXOS. Lors de votre première connexion, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez effectuer une réinitialisation d'usine pour rétablir le mot de passe par défaut. Consultez le guide de dépannage FXOS pour la procédure de réinitialisation d'usine.

Exemple :

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

[...]

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

[...]

firepower#
```

Étape 2 Sur l'interface de ligne de commande de FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

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

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

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

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, consultez Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 22. Par défaut, l'interface de gestion utilise DHCP.

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

b) Effectuez la reimage procedure (procédure permettant de refaire l'image) dans le guide de dépannage FXOS.

Étape 4 Pour le provisionnement à faible intervention humaine, *ne vous connectez pas au pare-feu* après la création d'une nouvelle image; la connexion démarre la configuration initiale. Le provisionnement à faible intervention humaine ne fonctionne que sur les pare-feu avec de nouvelles installations qui n'ont pas été configurées.

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 13.
- Si vous n'avez pas un compte Cisco Secure Sign-On, passez à Créer un nouveau compte de connexion Cisco Secure, à la page 10.

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.

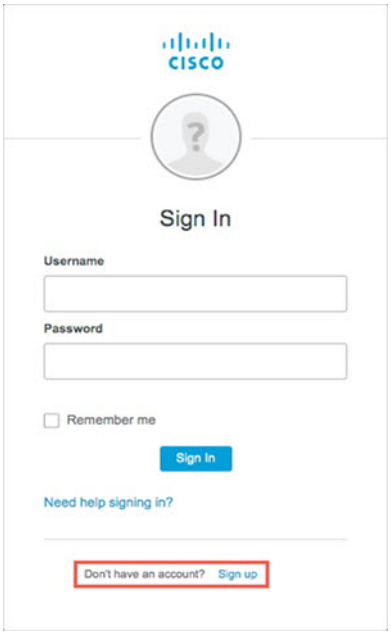
Procédure

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

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

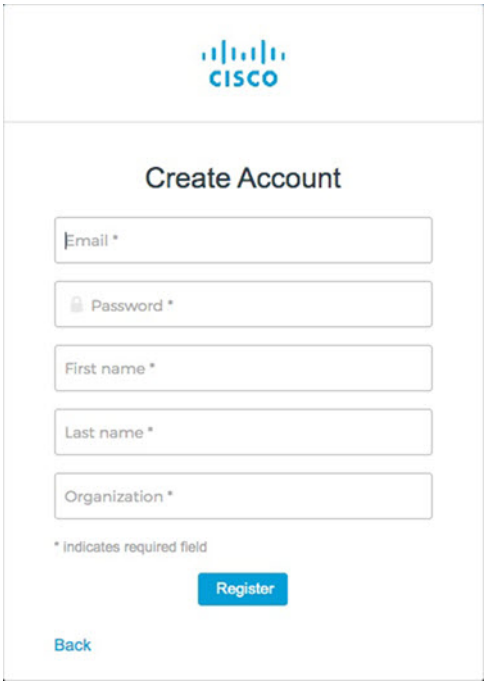
b) Au bas de l'écran de connexion, cliquez sur **Sign up** (s'inscrire).

Illustration 4 : Inscription à Cisco SSO



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

Illustration 5 : 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.

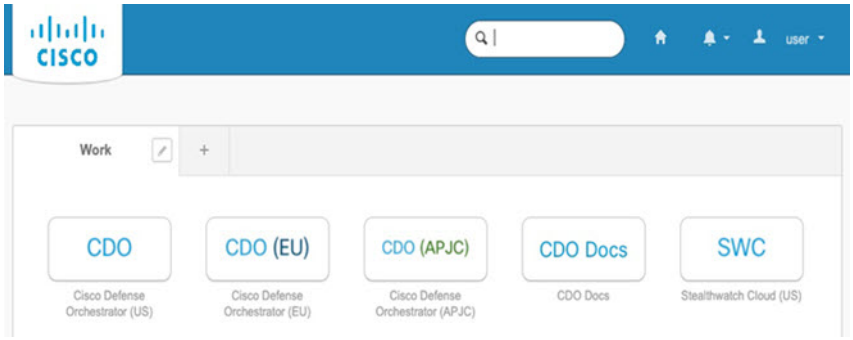
c) Choisissez une image de sécurité.

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 6 : 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 10.
- Utilisez une version actuelle de Firefox ou de Chrome.

Procédure

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

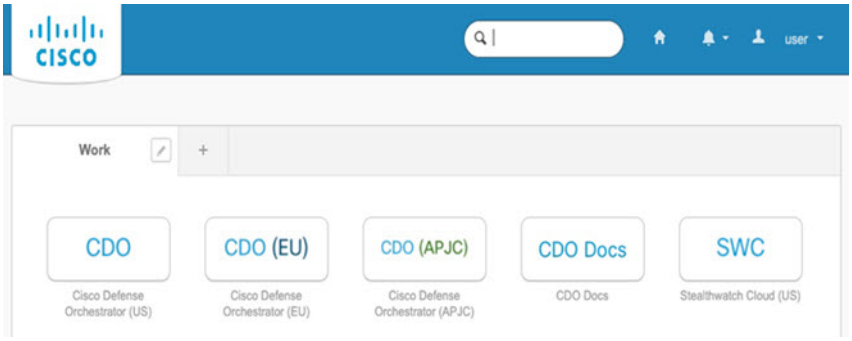
Étape 2 Saisissez votre nom d'utilisateur (**Username**) et votre mot de passe Cisco **Password**.

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 7 : 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.

Déployer le pare-feu pour un provisionnement à faible intervention humaine

Après avoir reçu défense contre les menaces du siège central, il ne vous reste plus qu'à câbler et à mettre le pare-feu sous tension pour qu'il ait accès à Internet depuis l'interface extérieure. L'administrateur central peut alors terminer la configuration.

Présenter le numéro de série du pare-feu à l'administrateur central

Avant de mettre le pare-feu en rack ou de jeter la boîte d'expédition, notez le numéro de série afin de pouvoir vous coordonner avec l'administrateur central.

Procédure

Étape 1 Déballez le châssis et les composants du châssis.

Faites l'inventaire de votre pare-feu et de ce qui est emballé avant de connecter des câbles ou de mettre le pare-feu sous tension. Vous devez également vous familiariser avec la disposition du châssis, les composants et les DEL.

Étape 2 Enregistrez le numéro de série du pare-feu.

Le numéro de série du pare-feu se trouve sur la boîte d'expédition. Il peut également se trouver sur une étiquette en bas du châssis du pare-feu.

Étape 3 Envoyez le numéro de série du pare-feu à l'administrateur réseau de CDO de votre service informatique ou bureau central.

Votre administrateur réseau a besoin de votre numéro de série de pare-feu pour faciliter le provisionnement à faible intervention, se connecter au pare-feu et le configurer à distance.

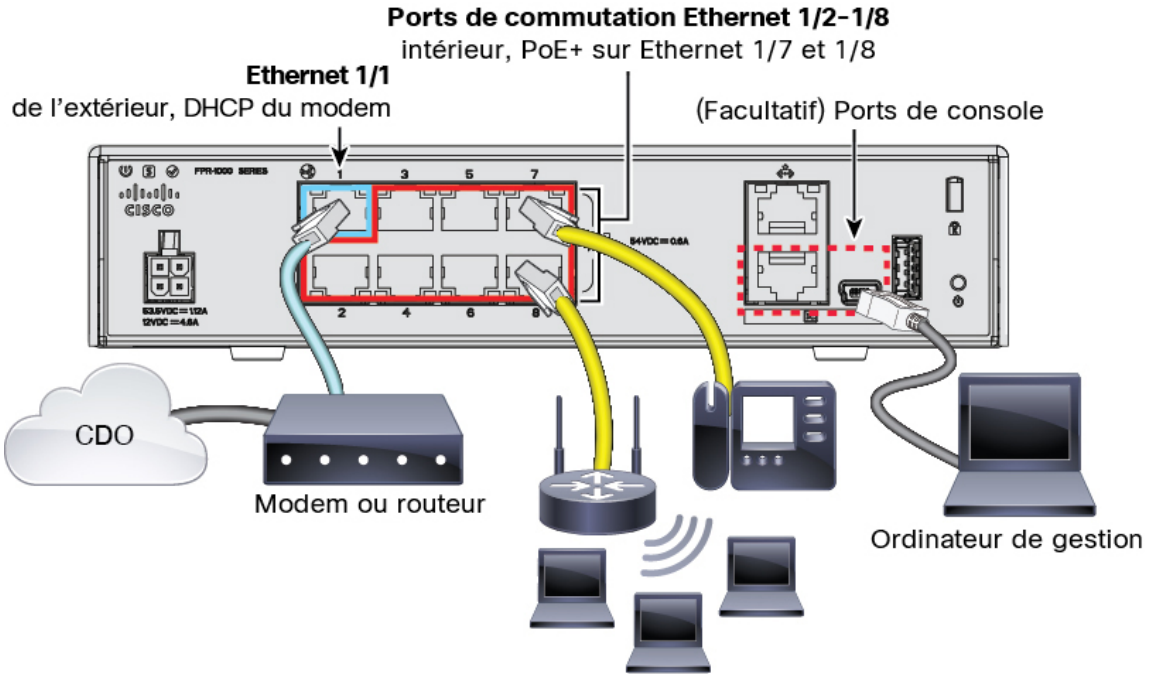
Communiquez avec l'administrateur de CDO pour élaborer un calendrier d'intégration.

Câbler le pare-feu

Cette rubrique décrit comment connecter le Firepower 1010 à votre réseau de manière à ce qu'il puisse être géré par CDO.

Si vous avez reçu un pare-feu dans votre succursale et que votre travail consiste à le brancher sur votre réseau, regardez cette vidéo. La vidéo décrit votre pare-feu et les séquences de DEL sur le pare-feu qui indiquent l'état du pare-feu. En cas de besoin, vous pourrez confirmer l'état du pare-feu auprès de votre service informatique en regardant simplement les DEL.

Illustration 8 : Câblage du Firepower 1010



Le provisionnement à faible intervention prend en charge la connexion à CDO sur Ethernet 1/1 (externe).

Remarque Les ports Ethernet 1/2 à 1/8 sont configurés comme ports de commutation matérielle; PoE+ est également disponible sur Ethernet 1/7 et 1/8.

Procédure

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

Étape 2 Connectez le câble réseau de l'interface Ethernet 1/1 à votre modem de réseau étendu (WAN). Votre modem WAN est la connexion de votre succursale à Internet et sera également la route de votre pare-feu vers Internet.

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

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

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

À la succursale, la connexion à la console n'est pas requise pour une utilisation quotidienne; cependant, elle peut être nécessaire dans le contexte du dépannage.

Mettez le pare-feu sous tension

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

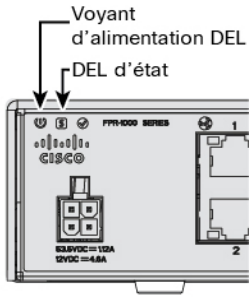
Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

Étape 4 Observez la DEL d'état en arrière ou sur le dessus de l'appareil; lorsque le périphérique démarre correctement, la DEL d'état est verte et clignote rapidement.

En cas de problème, la DEL d'état est orange et clignote rapidement. Si cela se produit, appelez votre service informatique.

Étape 5 Observez la DEL d'état en arrière ou sur le dessus de l'appareil; lorsque le périphérique se connecte au nuage Cisco, la DEL d'état est verte et clignote rapidement.

En cas de problème, la DEL d'état clignote en orange et en vert et le périphérique n'atteint pas le nuage Cisco. Si cela se produit, assurez-vous que votre câble réseau est connecté à l'interface Ethernet 1/1 et à votre modem WAN. Si, après avoir ajusté le câble réseau, l'appareil n'atteint pas le nuage Cisco après environ 10 minutes supplémentaires, appelez votre service informatique.

Prochaine étape

- Communiquez avec votre service informatique pour confirmer votre calendrier et vos activités d'intégration. Vous devriez avoir un plan de communication en place avec l'administrateur de CDO à votre siège central.
- Après avoir effectué cette tâche, votre administrateur CDO sera en mesure de configurer et de gérer l'appareil à distance. Vous avez terminé.

Préparation d'un appareil avec un provisionnement à faible intervention humaine

Préparation de défense contre les menaces en utilisant le provisionnement à faible intervention humaine et le numéro de série de l'appareil.

Procédure

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

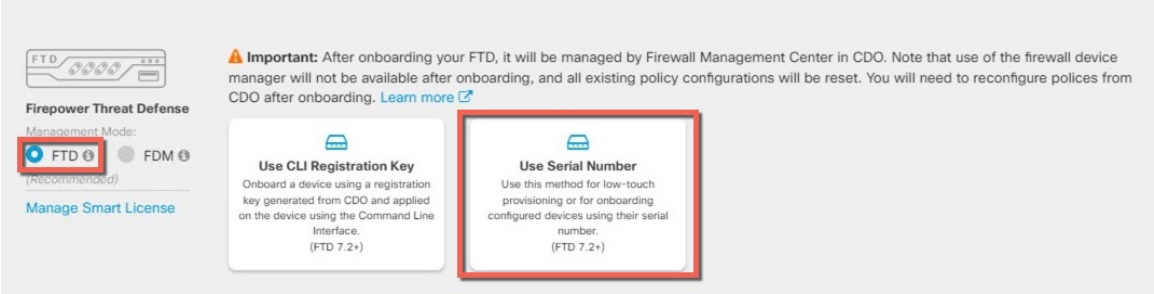
Étape 2 Sélectionnez la vignette **FTD**.

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

À tout moment, après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Manage Smart License (gérer la licence Smart)** pour inscrire ou modifier les licences Smart existantes disponibles pour votre appareil. Consultez pour savoir quelles licences sont disponibles.Obtenir des licences, à la page 7

Étape 4 Sélectionnez Use Serial Number (Utiliser le numéro de série) comme méthode de préparation.

Illustration 9 : Utiliser le numéro de série



Étape 5 Dans la zone **Connection (connexion)**, saisissez le **numéro de série du périphérique** et le **nom du périphérique**, puis cliquez sur **Next (suivant)**.

Étape 6 Dans la zone **Password Reset (réinitialisation du mot de passe)**, cliquez sur le bouton radio **Yes, this new device hasevered in or selected for a manager (oui, ce nouveau périphérique n'a jamais été connecté ou configuré pour un gestionnaire)**, puis cliquez sur **Next (suivant)**.

Étape 7 Pour **l'affectation de politique**, utilisez le menu déroulant pour choisir une politique de contrôle d'accès pour le périphérique. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 8 Pour la **licence par abonnement**, cochez chacune des licences de fonctionnalité que vous souhaitez activer. Cliquez sur **Next** (suivant).

Étape 9 (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 périphérique après son intégration à CDO.

Prochaine étape

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

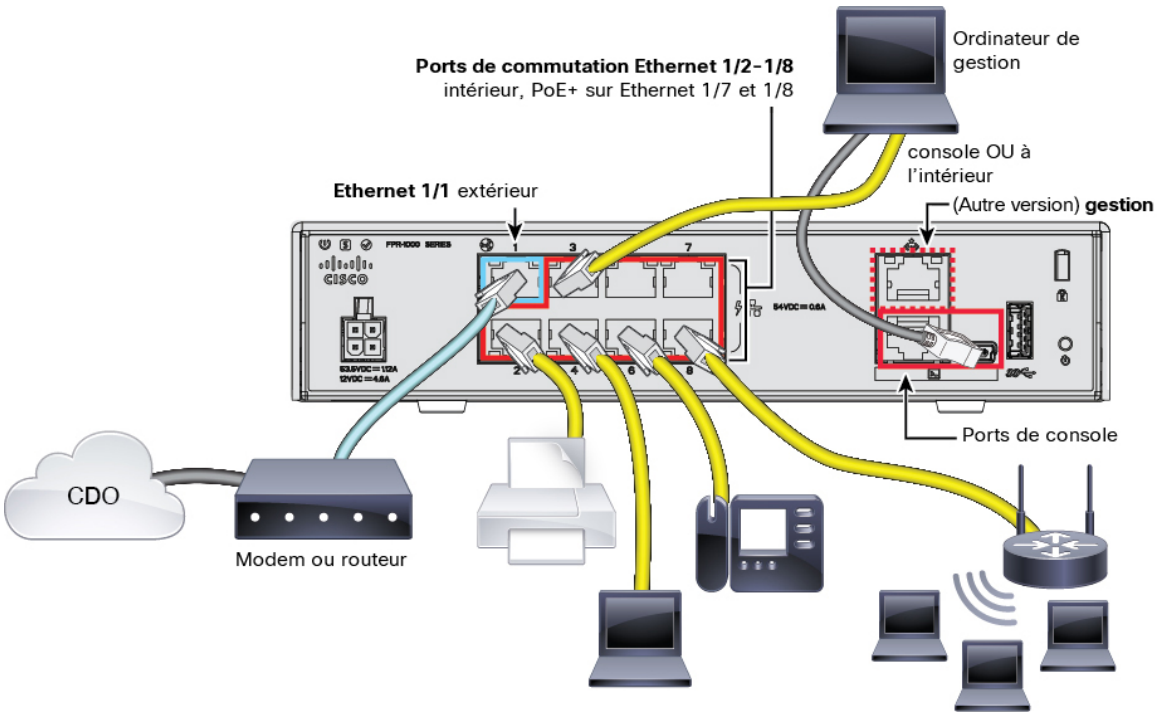
Déployer le pare-feu avec l'assistant de préparation

Cette section décrit comment configurer le pare-feu pour la préparation à l'aide de l'assistant de préparation CDO.

Câbler le pare-feu

Cette rubrique décrit comment connecter le Firepower 1010 à votre réseau de manière à ce qu'il puisse être géré par CDO.

Illustration 10 : Câblage du Firepower 1010



Vous pouvez vous connecter à CDO sur l'interface externe ou l'interface de gestion, selon l'interface que vous avez définie pour l'accès du gestionnaire lors de la configuration initiale. Ce guide présente l'interface externe.

Remarque Les ports Ethernet 1/2 à 1/8 sont configurés comme ports de commutation matérielle; PoE+ est également disponible sur Ethernet 1/7 et 1/8.

Procédure

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

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

Vous pouvez également utiliser l'interface de gestion pour l'accès du gestionnaire. Cependant, ce guide aborde principalement l'accès à l'interface externe, car c'est le scénario le plus probable pour les succursales à distance.

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

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

Étape 4 Connectez l'ordinateur de gestion au port de console ou à une interface interne.

Si vous effectuez la configuration initiale à l'aide de l'interface de ligne de commande, vous devrez vous connecter au port de console. Le port de console peut également être requis à des fins de dépannage. Si vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil, connectez-vous à une interface interne.

Mettez le pare-feu sous tension

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

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Avant de commencer

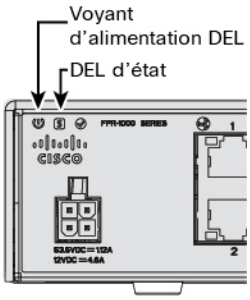
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne permet pas un arrêt progressif de votre système.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

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 la CDO, cliquez sur **Inventory inventory)** , puis sur le bouton bleu plus ( ) pour la **Préparation** d'un appareil.

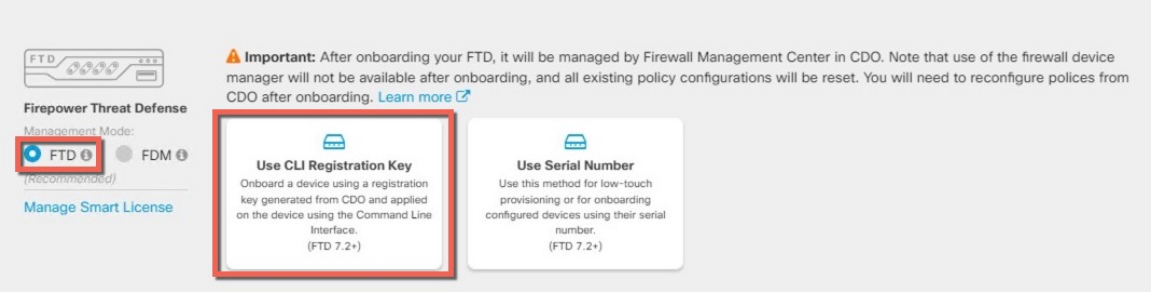
Étape 2 Sélectionnez la vignette **FTD**.

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

À tout moment, après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Manage Smart License (gérer la licence Smart)** pour inscrire ou modifier les licences Smart existantes disponibles pour votre appareil. Consultez pour savoir quelles licences sont disponibles.Obtenir des licences, à la page 7

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

Illustration 11 : Utiliser la clé d'enregistrement de l'interface de ligne de commande



Étape 5 Saisissez le **nom du périphérique**, 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 périphérique. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

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

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

configure manager add *cdo_hostname registration_key nat_id display_name*

Terminez la configuration initiale au niveau de l'interface de ligne de commande ou à l'aide de la fonction gestionnaire d'appareil:

- Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 22— Copiez cette commande dans l'interface de ligne de commande FTD après que vous ayez terminé le script de démarrage.
- Effectuer la configuration initiale à l'aide du Gestionnaire d'appareil, à la page 27— Copiez les parties de la commande *cdo_hostname*, *registration_key*, et *nat_id* dans les champs **Centre de gestion/Nom d'hôte du CDO/adresse IP**, **Centre de gestion/Clé d'enregistrement du CDO**, et **NAT ID**.

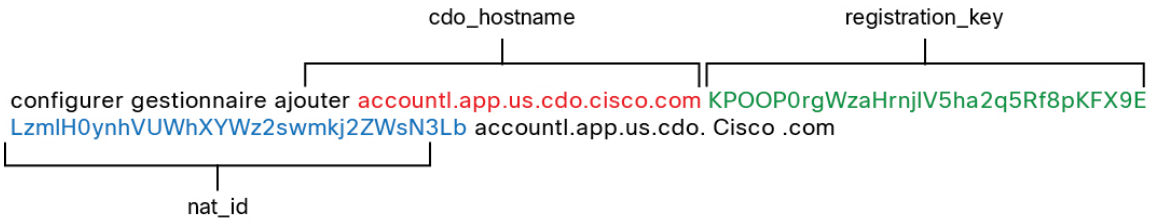
Exemple :

Exemple de commande pour la configuration de l'interface de ligne de commande :

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

Exemples de composants de commande pour la configuration de l'interface graphique :

Illustration 12 : configurer le gestionnaire ajoute des composants de commande



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 périphérique après son intégration à CDO.

Prochaine étape

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

Effectuer la configuration initiale

Effectuez la configuration initiale de défense contre les menaces à l'aide de l'interface de ligne de commande ou à l'aide de gestionnaire d'appareil.

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

Connectez-vous à l'interface de ligne de commande défense contre les menaces pour effectuer la configuration initiale. Lorsque vous utilisez l'interface de ligne de commande pour la configuration initiale, seuls les paramètres de l'interface de gestion et de l'interface d'accès du gestionnaire sont conservés. Lorsque vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil, *toute* la configuration de l'interface effectuée dans gestionnaire d'appareil est conservée lorsque vous passez à CDO pour la gestion, en plus des paramètres de l'interface de gestion et de l'interface d'accès du gestionnaire. Vous observerez que les autres paramètres de configuration par défaut, comme la politique de contrôle d'accès, ne sont pas conservés.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande défense contre les menaces sur le port de console.

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

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

La première fois que vous vous connectez à FXOS, vous êtes invité à changer le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devrez recréer l'image du périphérique pour réinitialiser le mot de passe selon sa valeur par défaut. Consultez le FXOS guide de dépannage pour la procédure pour réimager.

Exemple :

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

[...]

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

[...]

firepower#
```

Étape 3 Connectez-vous à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 4 La première fois que vous vous connectez à défense contre les menaces , vous êtes invité à accepter le contrat de licence de l'utilisateur final (cLUF). Ensuite, le script de configuration de l'interface de ligne de commande apparaît pour les paramètres de l'interface de gestion.

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

Remarque Vous ne pouvez pas relancer l'assistant de configuration de l'interface de ligne de commande à moins d'effacer la configuration; par exemple, en recréant l'image. Cependant, tous ces paramètres peuvent être modifiés ultérieurement au niveau de l'interface de ligne de commande à l'aide des commandes **configure network**. Consultez Références de commandes pour Cisco Secure Firewall Threat Defense.

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

Consultez les consignes suivantes :

- **Configurer IPv4 au moyen de DHCP ou manuellement ?**— Sélectionnez **manual (manuellement)**. Bien que vous ne prévoyiez pas utiliser l'interface de gestion, vous devez définir une adresse IP, par exemple une adresse privée. Vous ne pouvez pas configurer une interface de données pour la gestion si l'interface de gestion est définie sur DHCP, car la voie de routage par défaut, qui doit se fonder sur des **interfaces de données** (voir la puce suivante), pourrait être remplacée par une autre reçue du serveur DHCP.

- **Enter the IPv4 default gateway for the management interface** (saisissez la passerelle IPv4 par défaut pour l'interface de gestion) : Définissez la passerelle comme interface de données (**data-interfaces**). Ce paramètre fait passer le trafic de gestion sur le fond de panier afin qu'il puisse être distribué au moyen de l'interface de données d'accès du gestionnaire.
- **Gérer l'appareil localement ?**— Saisissez**no (non)** pour utiliser CDO. Une réponse **yes (oui)** signifie que vous utiliserez plutôt gestionnaire d'appareil.
- **Configurer le mode pare-feu?** : Entrez **Routed** (routage). L'accès du gestionnaire externe n'est pris en charge qu'en mode pare-feu routé.

Exemple :

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

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

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

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

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

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

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

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

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

Étape 5 Configurez l'interface extérieure pour l'accès du gestionnaire.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base pour l'interface externe. Consultez les détails suivants pour utiliser cette commande :

- L'interface de gestion ne peut pas utiliser DHCP si vous souhaitez utiliser une interface de données pour la gestion. Si vous n'avez pas défini l'adresse IP manuellement lors de la configuration initiale, vous pouvez la définir maintenant à l'aide de la commande **configure network** {**ipv4** | **ipv6**} **manual**. Si vous n'avez pas encore défini la passerelle d'interface de gestion sur **data-interfaces** (interfaces de données), cette commande la configurera maintenant.
- Lorsque vous ajoutez le défense contre les menaces à CDO, CDO découvre et maintient la configuration de l'interface, y compris les paramètres suivants : nom et adresse IP de l'interface, route statique vers la passerelle, serveurs DNS et serveur DDNS. Pour plus d'informations sur la configuration du serveur DNS, voir ci-dessous. Dans CDO, vous pouvez ultérieurement apporter des modifications à la configuration de l'interface d'accès du gestionnaire, mais veillez à ne pas effectuer de changements susceptibles d'empêcher le défense contre les menaces ou CDO de rétablir la connexion de gestion. Si la connexion du gestionnaire est interrompue, le défense contre les menaces inclut la commande **configure policy rollback** pour restaurer le déploiement précédent.
- Si vous configurez une URL de mise à niveau du serveur DDNS, le défense contre les menaces ajoute automatiquement les certificats de toutes les principales autorités de certification du groupe Cisco Trusted Root CA afin que le défense contre les menaces puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le défense contre les menaces prend en charge tout serveur DDNS qui utilise la spécification DynDNS Remote API (https://help.dyn.com/remote-access-api/).
- Cette commande définit le serveur DNS de l'interface de *données*. Le serveur DNS de gestion que vous définissez avec le script d'installation (ou à l'aide de la commande **configure network dns servers**) est utilisé pour le trafic de gestion. Le serveur de données DNS est utilisé pour DDNS (si configuré) ou pour les politiques de sécurité s'appliquant à cette interface.

  Sur CDO, les serveurs DNS de l'interface de données sont configurés dans la politique Paramètres de la plateforme que vous affectez à défense contre les menaces . Lorsque vous ajoutez le défense contre les menaces à CDO, le paramètre local est maintenu, et les serveurs DNS ne sont *pas* ajoutés à une politique de paramètres de plateforme. Toutefois, si vous attribuez ultérieurement une politique de paramètres de plateforme au défense contre les menaces qui inclut une configuration DNS, cette configuration remplacera le paramètre local. Nous vous suggérons de configurer activement les paramètres de la plateforme DNS pour qu'ils correspondent à ce paramètre afin de synchroniser le CDO et le défense contre les menaces .

  De plus, les serveurs DNS locaux ne sont retenus CDO que si les serveurs DNS ont été découverts lors de l'enregistrement initial. Par exemple, si vous avez enregistré l'appareil à l'aide de l'interface de gestion, mais que vous configurez plus tard une interface de données à l'aide de la commande **configure network management-data-interface**, vous devez alors configurer manuellement tous ces paramètres dans CDO, y compris les serveurs DNS, pour qu'ils correspondent à la configuration défense contre les menaces .
- Vous pouvez changer l'interface de gestion après avoir enregistré le défense contre les menaces à CDO, soit à l'interface de gestion ou à une autre interface de données.

- Le nom de domaine complet que vous définissez dans l'assistant de configuration sera utilisé pour cette interface.
- Vous pouvez effacer toute la configuration de l'appareil dans le cadre de la commande; vous pouvez utiliser cette option dans un scénario de découverte, mais nous ne vous suggérons pas de l'utiliser pour la configuration initiale ou le fonctionnement normal.
- Pour désactiver la gestion des données, entrez la commande **configure network management-data-interface disable**.

Exemple :

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Exemple :

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 6 Identifiez le CDO qui gérera cela à l'aide de la commande défense contre les menaces **configure manager add** générée par le CDO. Reportez-vous à Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 20 pour générer la commande.

Exemple :

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

```
Manager successfully configured.
```

Effectuer la configuration initiale à l'aide du Gestionnaire d'appareil

Connectez-vous au gestionnaire d'appareil pour effectuer la configuration initiale du défense contre les menaces . Lorsque vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil, *toute* la configuration de l'interface effectuée dans le gestionnaire d'appareil est conservée lorsque vous passez à CDO pour la gestion, en plus de l'interface de gestion et des paramètres d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande, seuls les paramètres d'interface de gestion et d'accès au gestionnaire sont conservés (par exemple, la configuration par défaut de l'interface interne n'est pas conservée).

Procédure

Étape 1 Connectez votre ordinateur de gestion à à l'une des interfaces suivantes : Ethernet1/2 à 1/8.

Étape 2 Connectez-vous au gestionnaire d'appareil.

a) Saisissez l'URL suivante dans votre navigateur: **https://192.168.95.1**

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

c) Vous devrez lire et accepter le contrat de licence utilisateur final et modifier le mot de passe administrateur.

Étape 3 Utilisez l'assistant de configuration lorsque vous vous connectez pour la première fois au gestionnaire d'appareil pour terminer la configuration initiale. Vous pouvez également ignorer l'assistant de configuration en cliquant sur **Ignorer la configuration du périphérique en bas de la page.**

Après avoir terminé l'assistant de configuration, en plus de la configuration par défaut pour l'interface intérieure (Ethernet1/2 à 1/8, qui sont des ports de commutateur sur VLAN1), vous aurez la configuration pour une interface extérieure (Ethernet1/1) qui sera maintenue lorsque vous passerez à la gestion CDO.

a) Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

1. **Adresse de l'interface extérieure** : Cette interface est généralement la passerelle Internet et peut être utilisée comme interface d'accès au gestionnaire. Vous ne pouvez pas sélectionner une autre interface externe lors de la configuration initiale du périphérique. La première interface de données est l'interface externe par défaut.

   Si vous souhaitez utiliser une interface différente de l'extérieur (ou de l'intérieur) pour l'accès du gestionnaire, vous devrez la configurer manuellement après avoir terminé l'assistant d'installation.

   Configure IPv4 (configuration de l'adresse IPv4) : l'adresse IPv4 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE une fois que l'installation de l'assistant est terminée.

Configure IPv6 (configuration de l'adresse IPv6) : l'adresse IPv6 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv6.

2. **Interface de gestion**

   Vous ne verrez pas les paramètres de l'interface de gestion si vous avez effectué la configuration initiale sur l'interface de ligne de commande.

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

   DNS Servers (serveurs DNS) : le serveur DNS pour l'adresse de gestion du système. Entrez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. Par défaut, les serveurs DNS publics OpenDNS sont sélectionnés. Si vous modifiez les champs et souhaitez revenir à la valeur par défaut, cliquez sur **Use OpenDNS** (utiliser OpenDNS) pour recharger les adresses IP appropriées dans les champs.

   Firewall Hostname (nom d'hôte du pare-feu) : le nom d'hôte de l'adresse de gestion du système.

b) Configurez la **Time Setting (configuration de l'heure) (NTP)** et cliquez sur **Next (Suivant)**.

   1. **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
   2. **NTP Time Server** (serveur horaire NTP) : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou pour saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

c) Sélectionnez **Start 90 day evaluation period without registration** (commencer la période d'évaluation de 90 jours sans inscription).

   N'enregistrez pas le défense contre les menaces avec Smart Software Manager; toutes les licences sont effectuées dans CDO.

d) Cliquez sur **Finish** (terminer).

e) Vous êtes invité à choisir **Cloud Management** (gestion en nuage) ou **Standalone** (autonome). Pour le CDO fourni dans Cisco Cloud centre de gestion, sélectionnez **Standalone (autonome)**, puis **Got It (j'ai compris)**.

   L'option de **gestion du cloud** est destinée aux fonctionnalités CDO/FDM existantes.

Étape 4 (Peut être requis) Configurez l'interface de gestion. Consultez l'interface de gestion sur **Device (appareil)** > **Interfaces**.

L'interface de gestion doit avoir la passerelle définie sur les interfaces de données. Par défaut, l'interface de gestion reçoit une adresse IP et une passerelle de DHCP. Si vous ne recevez pas de passerelle de DHCP (par exemple, vous n'avez pas connecté cette interface à un réseau), la passerelle utilisera par défaut les interfaces de données et vous n'aurez rien à configurer. Si vous avez reçu une passerelle de DHCP, vous devez plutôt configurer cette interface avec une adresse IP statique et définir la passerelle sur les interfaces de données.

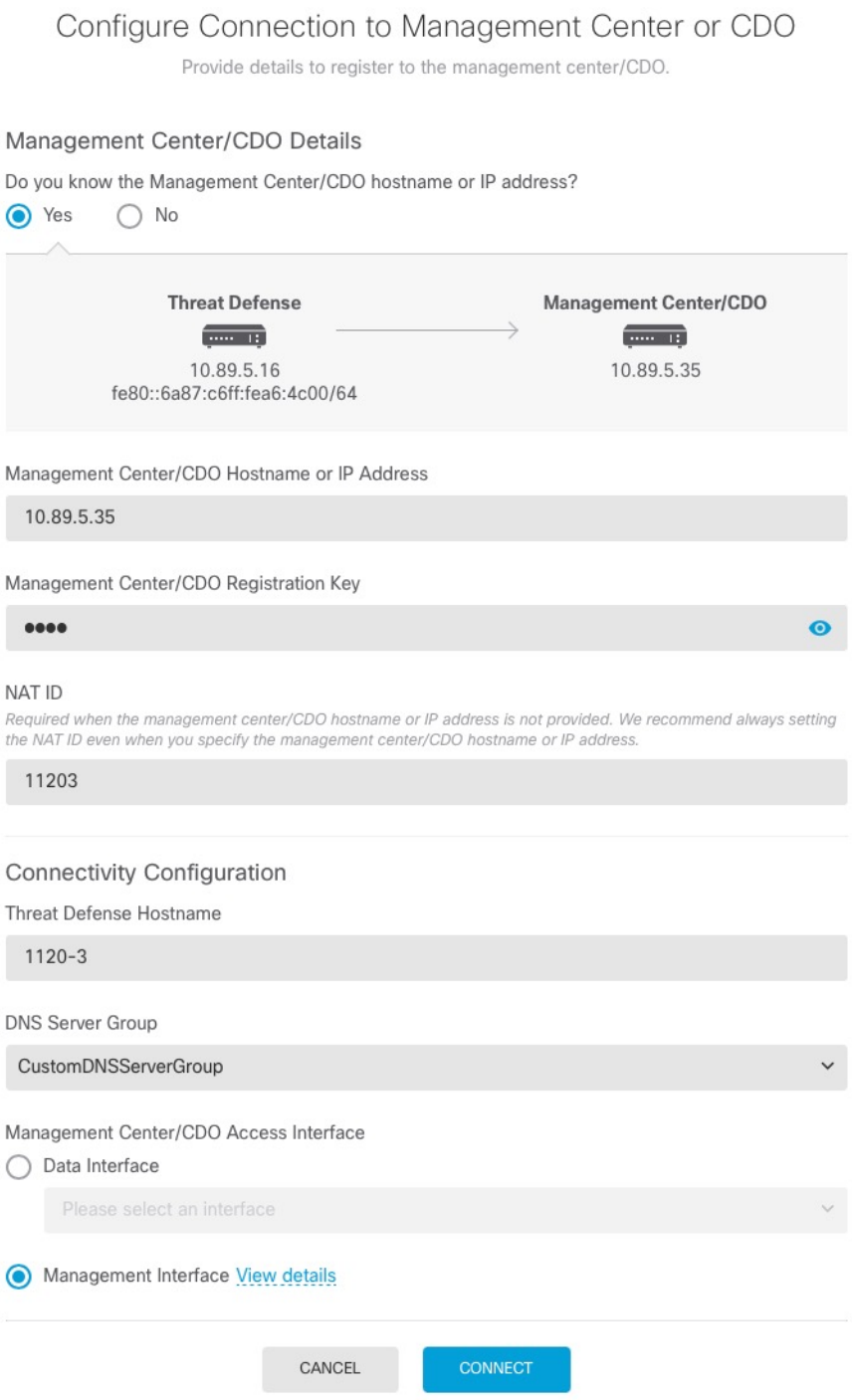
Étape 5 Si vous voulez configurer des interfaces supplémentaires, y compris une interface autre que l'extérieur ou l'intérieur que vous voulez utiliser pour l'accès du gestionnaire, sélectionnez **Périphérique**, puis cliquez sur le lien dans le résumé des **interfaces**.

Pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareil, voirConfigurer le pare-feu dans le Gestionnaire d'appareil. Les autres gestionnaire d'appareil configurations ne seront pas conservées lorsque vous enregistrerez l'appareil dans CDO.

Étape 6 Sélectionnez **Device (appareil)** > **System Settings (paramètres système)** > **Central Management (gestion centrale)**, et cliquz sur **Proceed (exécuter)** pour mettre en place la gestion du centre de gestion.

Étape 7 Configurez les détails du **centre de gestion/CDO.**

Illustration 13 : Détails du Centre de gestion/CDO



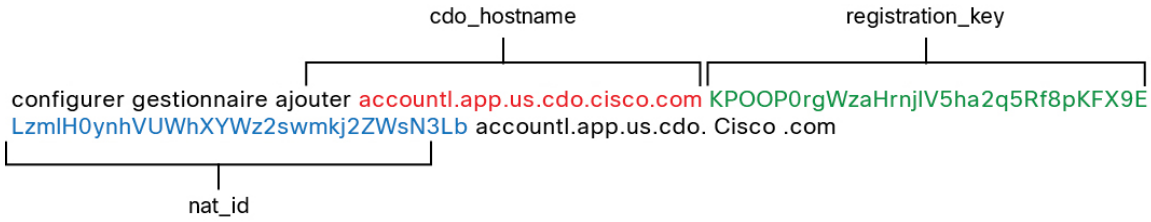
a) Pour **, connaissez-vous le nom d'hôte ou l'adresse IP** du centre de gestion/CDO, cliquez sur **Yes (oui)**.

CDO génère la commande **configure manager add**. Reportez-vous à Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 20 pour générer la commande.

configure manager add *cdo_hostname registration_key nat_id display_name*

Exemple :

Illustration 14 : configurer le gestionnaire ajoute des composants de commande



b) Copiez les parties *cdo_hostname*, *registration_key*, et *nat_id* de la commande dans les champs **Management Center (centre de gestion)/CDO Hostname (nom d'hôte CDO)/IP Address (adresse IP)**, **Management Center (centre de gestion)/CDO Registration Key (clé d'enregistrement CDO)**, et les champs **NAT ID**.

Étape 8 Configurez la **configuration de la connectivité.**

a) Précisez le **nom d'hôte FTD**.

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

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

Choisissez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNServerGroup**, qui comprend les serveurs OpenDNS.

Ce paramètre définit le serveur DNS de l'interface de *données*. Le serveur DNS de gestion que vous avez défini avec l'assistant de configuration est utilisé pour le trafic de gestion. Le serveur de données DNS est utilisé pour DDNS (si configuré) ou pour les politiques de sécurité s'appliquant à cette interface. Vous êtes susceptible de choisir le même groupe de serveurs DNS que celui que vous avez utilisé pour la gestion, car le trafic de gestion et de données atteint le serveur DNS par l'interface externe.

Sur CDO, les serveurs DNS de l'interface de données sont configurés dans la politique Paramètres de la plateforme que vous affectez à défense contre les menaces . Lorsque vous ajoutez le défense contre les menaces à CDO, le paramètre local est maintenu, et les serveurs DNS ne sont *pas* ajoutés à une politique de paramètres de plateforme. Toutefois, si vous attribuez ultérieurement une politique de paramètres de plateforme audéfense contre les menaces qui inclut une configuration DNS, cette configuration remplacera le paramètre local. Nous vous suggérons de configurer activement les paramètres de la plateforme DNS pour qu'ils correspondent à ce paramètre afin de synchroniser le CDO et le défense contre les menaces .

De plus, les serveurs DNS locaux ne sont retenus CDO que si les serveurs DNS ont été découverts lors de l'enregistrement initial.

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

Vous pouvez choisir n'importe quelle interface configurée, mais ce guide suppose que vous l'utilisez à l'extérieur.

Étape 9 Si vous avez choisi une interface de données différente de l'extérieur, ajoutez une route par défaut.

Vous verrez un message vous demandant de vérifier que vous avez une route par défaut dans l'interface. Si vous avez choisi l'extérieur, vous avez déjà configuré cette route dans le cadre de l'assistant de configuration. Si vous avez choisi une autre interface, vous devez configurer manuellement une route par défaut avant de

vous connecter à CDO. Reportez-vous à Configurer le pare-feu dans le Gestionnaire d'appareilpour plus d'informations sur la configuration des routes statiques dans le gestionnaire d'appareil.

Étape 10 Cliquez sur **Add a Dynamic DNS (DDNS) method (ajouter une méthode DNS dynamique (DDNS))**.

Le DDNS garantit que CDO peut atteindre le défense contre les menaces à son nom de domaine complet (FQDN) si l'adresse IP de défense contre les menaces change. Consultez **Device (appareil)** > **System Settings (paramètres système)** > **DDNS Service (service DDNS)** pour configurer le service DDNS.

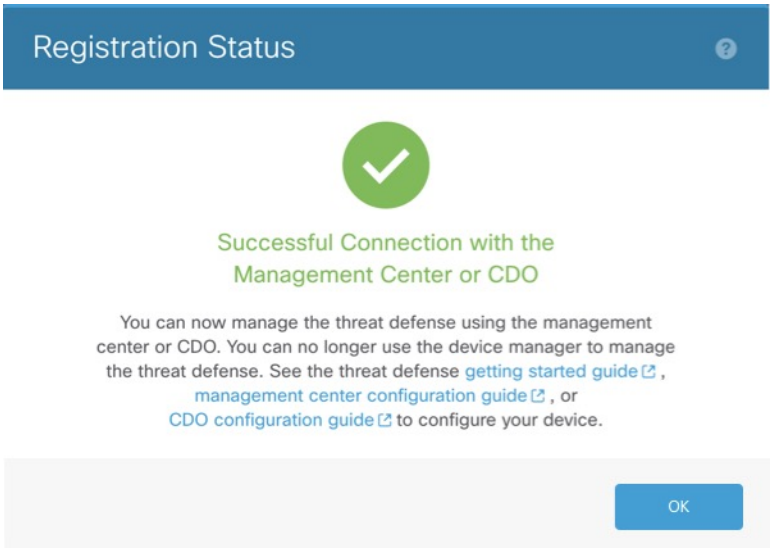
Si vous configurez le DDNS avant d'ajouter le défense contre les menaces à CDO, le défense contre les menaces ajoute automatiquement les certificats de toutes les principales autorités de certification du groupe Cisco Trusted Root CA afin que le défense contre les menaces puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le défense contre les menaces prend en charge tout serveur DDNS qui utilise la spécification DynDNS Remote API (https://help.dyn.com/remote-access-api/).

Étape 11 Cliquez sur **Connect (connexion)**. La boîte de dialogue **Registration Status (état de l'enregistrement)** affiche l'état actuel du commutateur vers CDO. Après l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**, accédez à CDO et ajoutez le pare-feu.

Si vous souhaitez annuler le basculement vers CDO, cliquez sur **Cancel Registration (annuler l'enregistrement)**. Sinon, ne fermez pas la fenêtre du gestionnaire d'appareilnavigateur avant l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**. Si vous le faites, le processus sera suspendu et ne reprendra que lorsque vous vous reconnecterez au.gestionnaire d'appareil

Si vous restez connecté au gestionnaire d'appareilaprès l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**, vous finirez par voir la boîte de dialogue **Connexion réussie avec le centre de gestion ou le CDO**, après quoi vous serez déconnecté du gestionnaire d'appareil.

Illustration 15 : Connexion réussie



Configurer une politique de sécurité de base

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

- Interfaces intérieure et extérieure - Attribuez une adresse IP statique à l'interface intérieure. Vous avez configuré les paramètres de base de l'interface externe dans le cadre de la configuration de l'accès du gestionnaire, mais vous devez toujours l'affecter à une zone de sécurité.
- DHCP server (serveur DHCP) : Utilisez un serveur DHCP sur l'interface interne pour les clients.
- NAT : Utilisez l'interface PAT sur l'interface externe.
- Access control (contrôle d'accès) : Autorisez le trafic de l'intérieur vers l'extérieur.
- SSH - Activez SSH sur l'interface d'accès du gestionnaire.

Interfaces de configuration

Ajoutez l'interface VLAN1 pour les ports de commutation ou convertissez les ports de commutation en interfaces de pare-feu, attribuez des interfaces aux zones de sécurité et définissez les adresses IP. En règle générale, vous devez configurer au moins deux interfaces pour 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. Par défaut, Ethernet 1/1 est une interface de pare-feu standard que vous pouvez utiliser à l'extérieur, et les autres interfaces sont des ports de commutation sur VLAN 1; après avoir ajouté l'interface VLAN1, vous pouvez en faire votre interface interne. Vous pouvez également affecter des ports de commutation à d'autres réseaux VLAN, ou convertir des ports de commutation en interfaces de pare-feu.

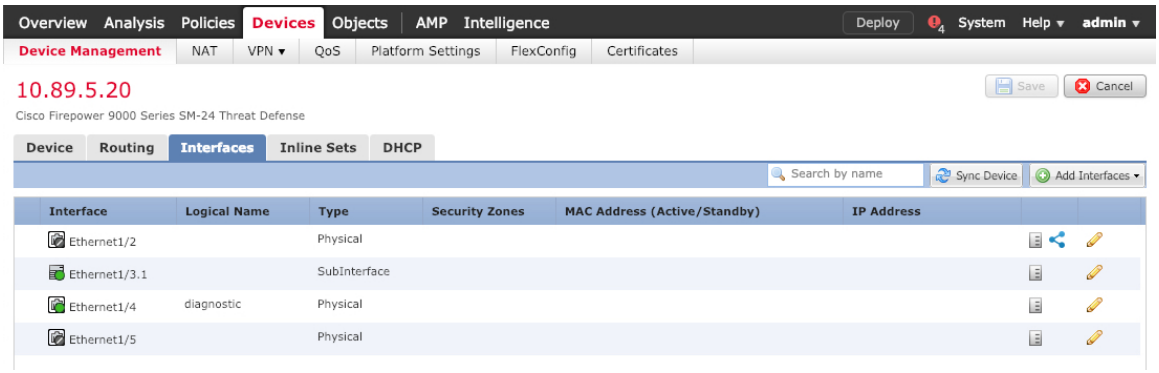
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

Dans l'exemple suivant, une interface interne (VLAN1) est configurée en mode routage avec une adresse statique et une interface externe est configurée en mode routage à l'aide de DHCP (Ethernet 1/1).

Procédure

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

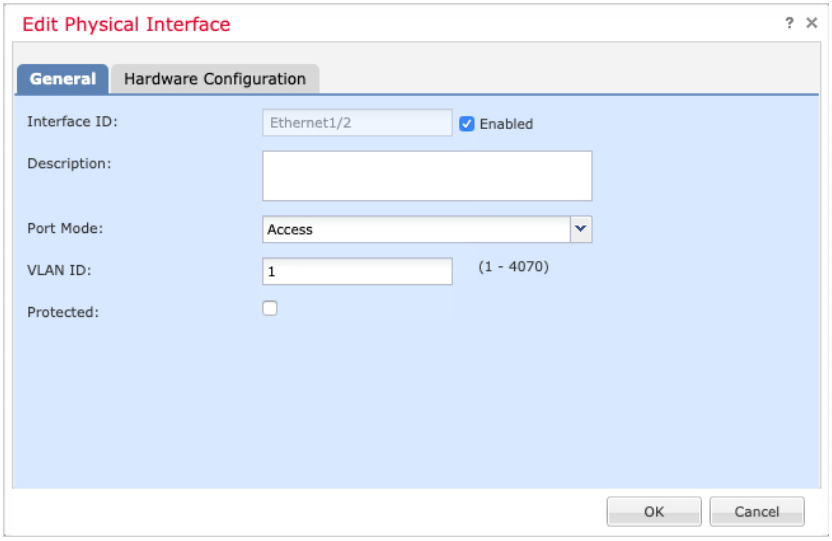
Étape 2 Cliquez sur **Interfaces**.



Étape 3 (Facultatif) Désactivez le mode de port de commutation pour n'importe lequel des ports de commutation (Ethernet1/2 à 1/8) en cliquant sur le curseur dans la colonne **SwitchPort** qu'il s'affiche comme désactivé ().

Étape 4 Activez les ports de commutateur.

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



b) Activez l'interface en cochant la case **Enabled** (activé).

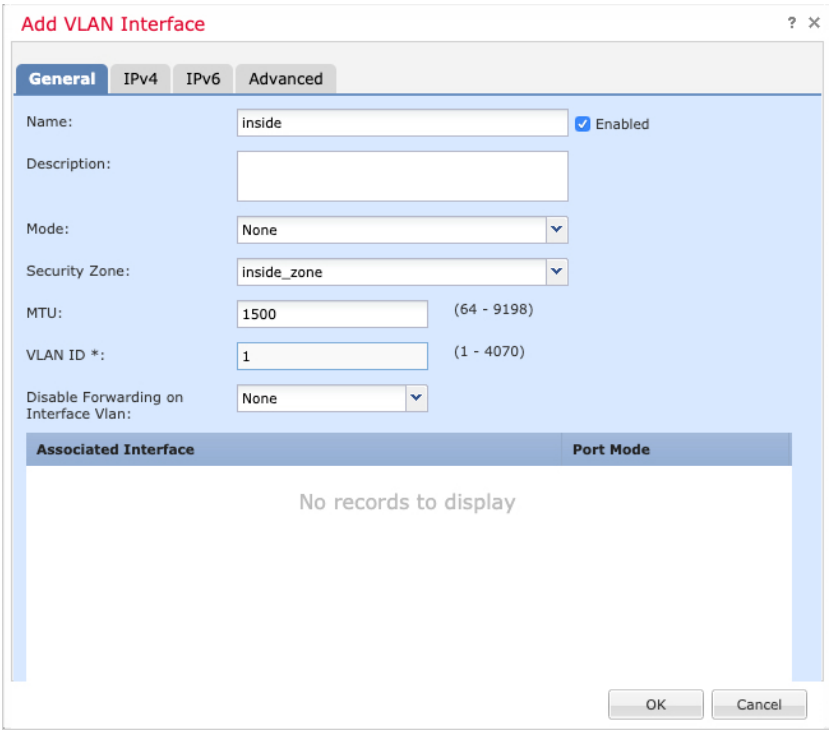
c) (Facultatif) Modifiez l'ID du VLAN; la valeur par défaut est 1. Vous allez ensuite ajouter une interface VLAN correspondant à cet ID.

d) Cliquez sur **OK**.

Étape 5 Ajouter une interface VLAN *interne*.

a) Cliquez **Add Interfaces (ajoutez des interfaces)** > **VLAN Interface (interfaces VLAN)**.

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



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

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

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

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

e) 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.

f) Définissez le numéro VLAN (**VLAN ID**) sur **1**.

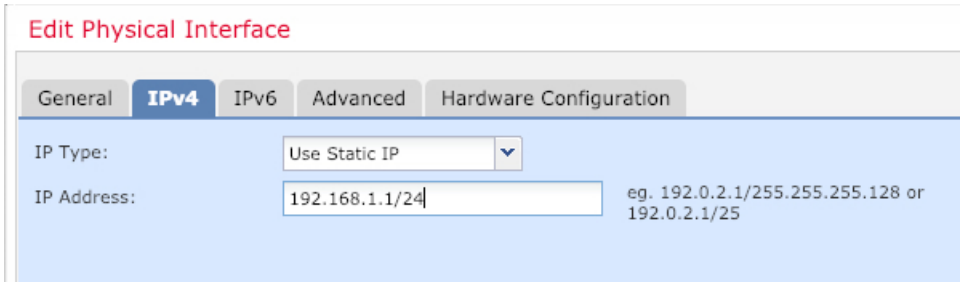
Par défaut, tous les ports de commutation sont définis sur VLAN 1; si vous choisissez un numéro VLAN différent dans ce cas-ci, vous devez également modifier chaque port de commutation pour qu'il soit sur le nouveau numéro VLAN.

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

g) 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**.

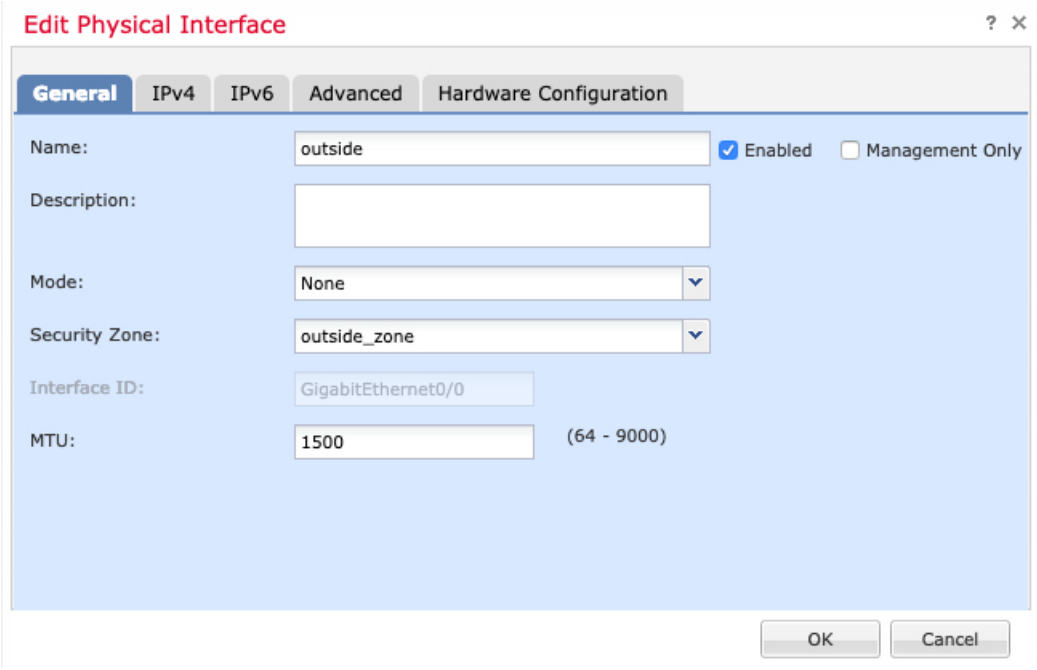


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

h) Cliquez sur **OK**.

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

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



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

a) 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**.

b) Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Configurer le serveur DHCP

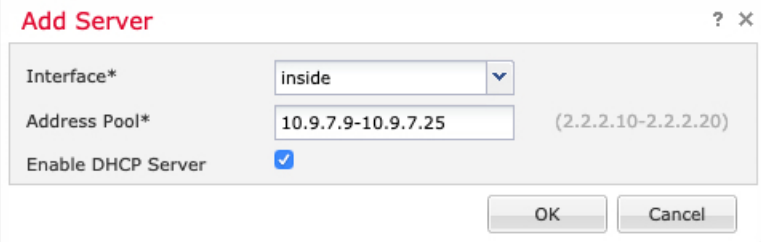
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de défense contre les menaces .

Procédure

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

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

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



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

Étape 4 Cliquez sur **OK**.

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

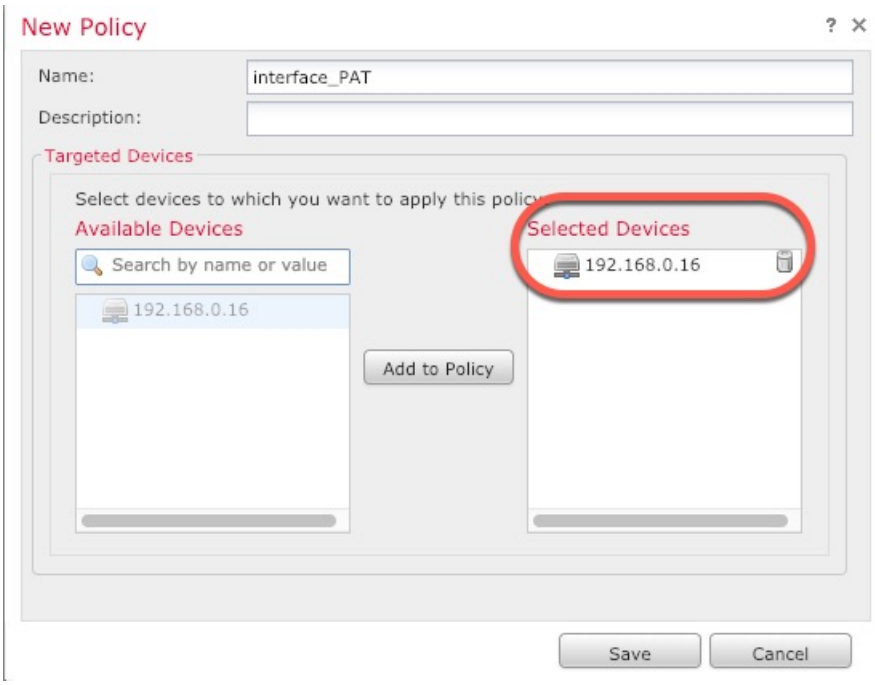
Configurer NAT

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 menances)**.

Étape 2 Nommez la politique, sélectionnez le ou les périphériques 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.

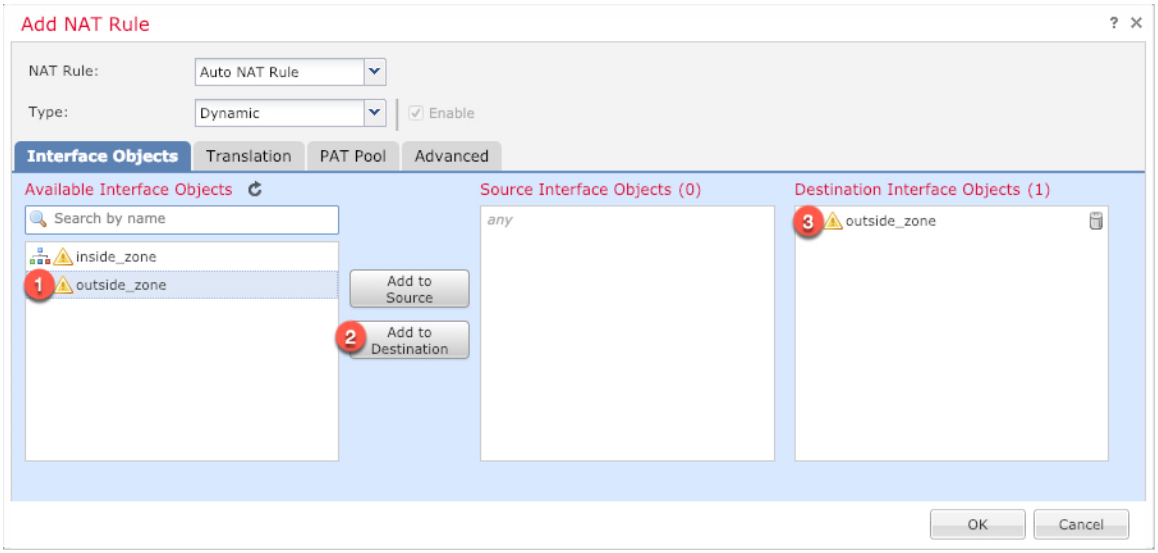
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

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

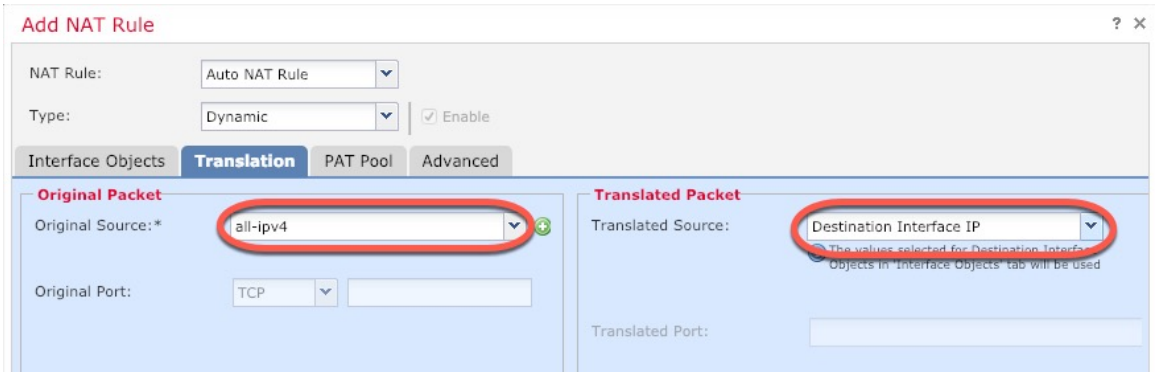
Étape 4 Configurez les options des règles de base :

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

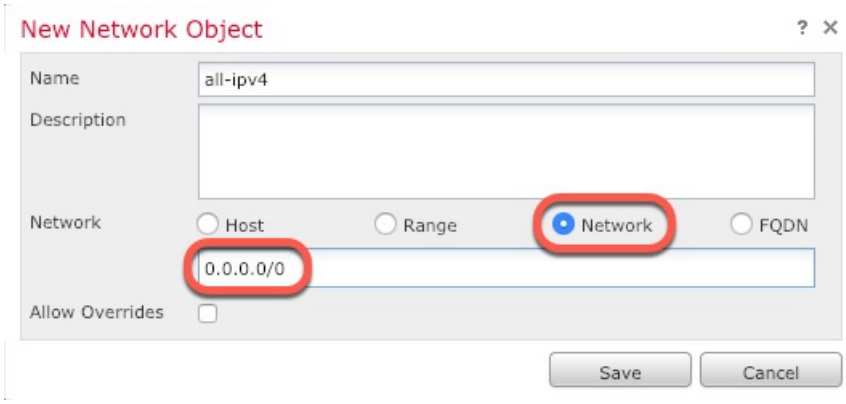
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



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).

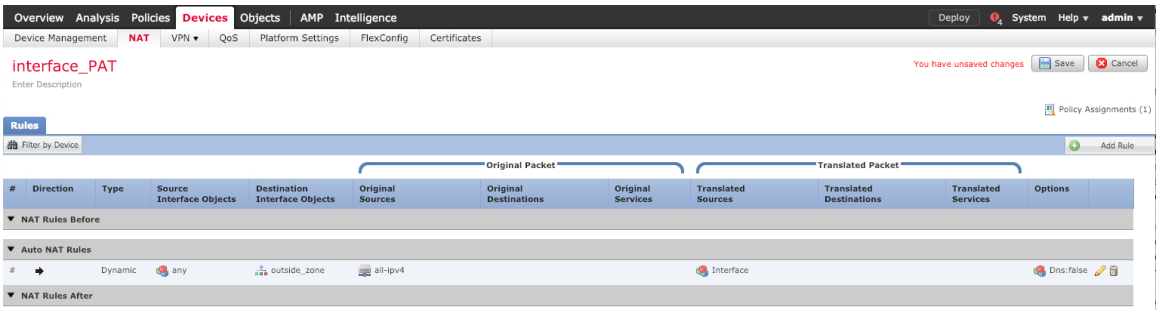


Remarque Vous ne pouvez pas utiliser l'objet**any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **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**.

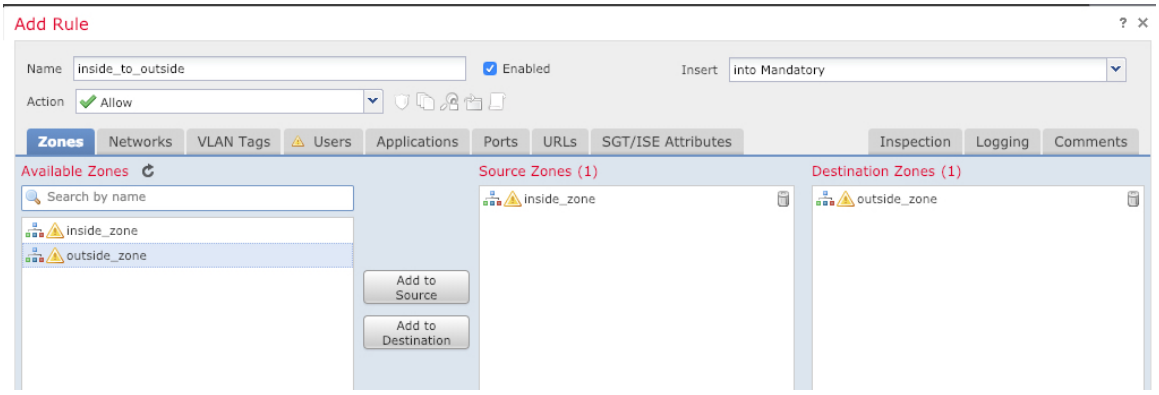
Permettre le trafic de l'intérieur vers l'extérieur

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 périphérique. 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 :



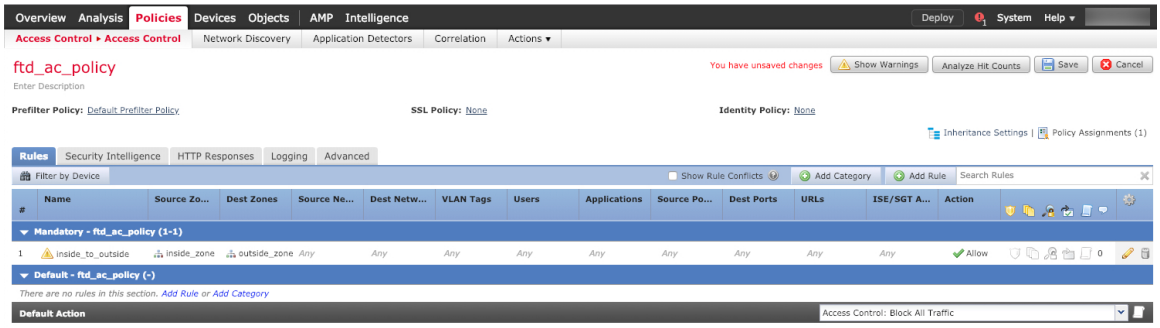
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

- **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).

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

Si vous avez activé centre de gestionl'accès sur une interface de données, telle que externe, vous devez activer SSH sur cette interface en suivant la procédure suivante. Cette section décrit comment activer les connexions SSH à une ou plusieurs interfaces de *données* sur le défense contre les menaces . SSH n'est pas pris en charge par l'interface de diagnostic logique.

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

L'interface de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. SSH pour les interfaces de données partage la liste d'utilisateurs interne et externe avec SSH pour l'interface de gestion. Les autres paramètres sont configurés séparément : pour les interfaces de données, activez SSH et accédez aux listes à l'aide de cet écran; le trafic SSH pour les interfaces de données utilise la configuration de routage normale, et non les voies de routage statiques configurées lors de l'installation ou au niveau de la CLI.

Pour l'interface de gestion, afin de configurer une liste d'accès SSH, consultez la commande **configure ssh-access-list** dans la Références de commandes pour Cisco Secure Firewall Threat Defense. Pour configurer une voie de routage statique, voir la commande **configure network static-routes**. Par défaut, vous configurez la voie de routage par défaut via l'interface de gestion, lors de la configuration initiale.

Pour utiliser le protocole SSH, vous n'avez pas non plus besoin d'une règle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.

Vous ne pouvez utiliser SSH que vers une interface accessible; si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe.

Le périphérique autorise un maximum de cinq (5) connexions SSH simultanées.

Remarque Après qu'un utilisateur ait échoué à trois reprises à se connecter à l'interface de commande au moyen de SSH, l'appareil met fin à la connexion SSH.

Avant de commencer

- Vous pouvez configurer les utilisateurs SSH internes au niveau de l'interface de ligne de commande (CLI) à l'aide de la commande **configure user add**. Par défaut, il existe un utilisateur administrateur (**admin**) pour lequel vous avez configuré le mot de passe lors de la configuration initiale. Vous pouvez également configurer des utilisateurs externes sur LDAP ou RADIUS en configurant l'authentification externe (**External Authentication**) dans les paramètres de la plateforme.
- Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions SSH avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser tout (**any**) groupe d'objets réseau fourni par le système. Au lieu de cela, utilisez **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Platform Settings (paramètres de la plateforme)** et créez ou modifiez la politique défense contre les menaces .

Étape 2 Sélectionnez **Secure Shell**.

Étape 3 Déterminez les interfaces et les adresses IP qui permettent les connexions SSH.

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

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.
b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet (ou groupe) de réseau qui établit les hôtes ou les réseaux que vous autorisez à établir des connexions SSH. Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) : Ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste de la zone de sécurité sélectionnée et l'ajouter en

cliquant sur **Add**. Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

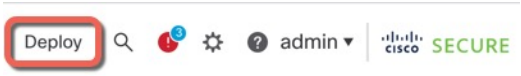
Déployer la configuration

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 16 : Déployer



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

Illustration 17 : Déployer tout

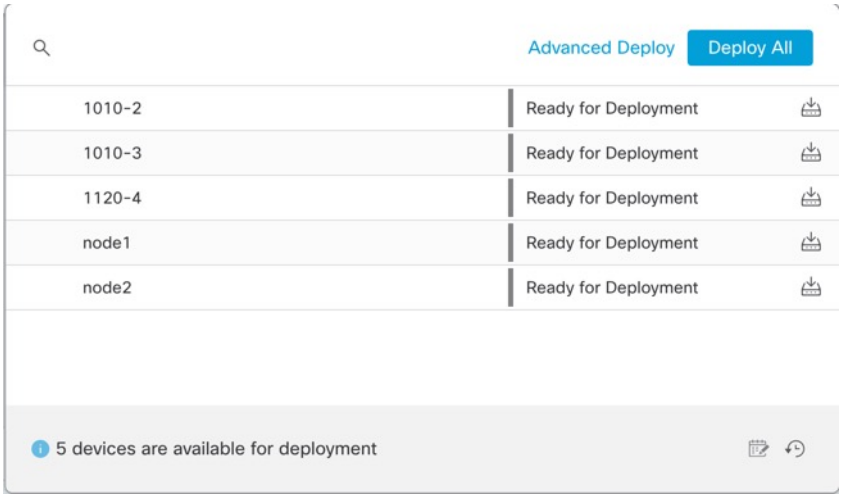
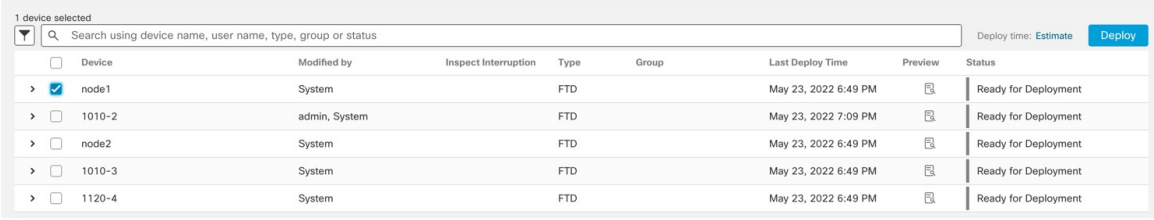
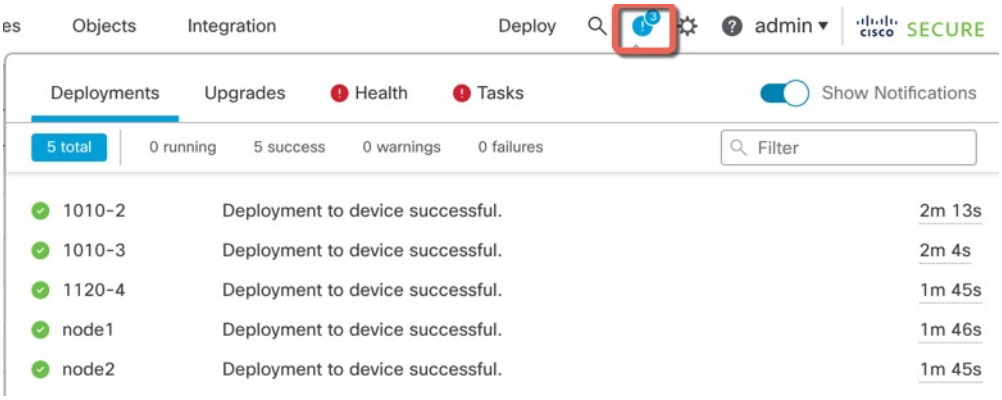


Illustration 18 : Déploiement avancé



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 19 : État du déploiement



Dépannage et maintenance

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

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

Vous pouvez également accéder à Interface de ligne de commande FXOSà des fins de dépannage.

Remarque Vous pouvez également vous connecter en SSH à l'interface de gestion du périphérique défense contre les menaces . Contrairement à une session de console, la session SSH passe par défaut à l'interface de ligne de commande défense contre les menaces , à partir de laquelle vous pouvez vous connecter à Interface de ligne de commande FXOS à l'aide de la commande **connect fxos**. Vous pouvez ensuite vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Cette procédure décrit l'accès au port de la console, qui est par défaut le Interface de ligne de commande FXOS.

Procédure

Étape 1 Pour accéder à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. Firepower 1000 est livrée avec un câble série USB A-vers-B. Veillez à installer tous les pilotes série USB nécessaires pour votre système d'exploitation (voir le guide matériel du Firepower 1010 et le). Le port de console est par défaut le Interface de ligne de commande FXOS. Utilisez les paramètres de série suivants :

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

Vous vous connectez à Interface de ligne de commande FXOS. Connectez-vous à l'interface de ligne de commande en utilisant le nom d'utilisateur **admin** et le mot de passe que vous avez défini lors de la configuration initiale (la valeur par défaut est **Admin123**).

Exemple :

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Étape 2 Accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après la connexion, pour des informations sur les commandes disponibles dans l'interface de ligne de commande, entrez **help** ou **?**. Pour des remseignements sur l'usage, consultez Références de commandes pour Cisco Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande défense contre les menaces , saisissez la commande **exit** ou la commande **logout**.

Cette commande vous ramène à l'invite Interface de ligne de commande FXOS. Pour plus d'informations sur les commandes disponibles dans Interface de ligne de commande FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Résoudre les problèmes de connectivité de gestion sur l'interface de données

Lorsque vous utilisez une interface de données pour l'accès du gestionnaire au lieu d'utiliser l'interface de gestion dédiée, vous devez faire attention à la modification des paramètres d'interface et de réseau de défense contre les menaces dans le CDO afin de ne pas interrompre la connexion. Si vous changez le type d'interface de gestion des changements après avoir ajouté le défense contre les menaces à CDO (de données à Gestion, ou de Gestion à données), si les interfaces et les paramètres réseau ne sont pas configurés correctement, vous pouvez perdre la connexion de gestion.

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

Afficher l'état de la connexion de gestion

Dans CDO, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (accès au gestionnaire - Détails de la configuration)** > **Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion. Vous pouvez également utiliser la commande **sftunnel-status** pour afficher des informations plus complètes.

Consultez l'exemple de sortie suivant au sujet d'une connexion interrompue; il n'y a pas d'information de connexion à un canal homologue, ni aucune information de pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Voir les informations sur le réseau défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , affichez les paramètres de réseau de l'interface de données de gestion et d'accès du gestionnaire :

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
```

```
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

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

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

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

Vérifiez que défense contre les menaces est enregistré auprès du CDO

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que l'enregistrement du CDO a été effectué. Remarque : Cette commande n'affichera pas l'état *actuel* de la connexion de gestion.

show managers

```
> show managers
Type                      : Manager
Host                      : account1.app.us.cdo.cisco.com
Display name              : account1.app.us.cdo.cisco.com
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

Envoyez un message Ping au CDO

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer un message Ping au CDO à partir des interfaces de données :

ping *cdo_hostname*

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer un message Ping au CDO à partir de l'interface de gestion, qui devrait être acheminé par le fond de panier vers les interfaces de données :

ping system *cdo_hostname*

Saisissez les paquets sur l'interface interne défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , saisissez les paquets sur l'interface interne du fond de panier (nlp_int_tap) pour voir si des paquets de gestion sont envoyés :

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

Vérifier l'état de l'interface interne, les statistiques et le nombre de paquets

Dans l'interface de ligne de commande défense contre les menaces , consultez les informations sur l'interface interne du fond de panier, , nlp_int_tap :

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Vérifiez le routage et la NAT

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que la route par défaut (S*) a été ajoutée et que des règles NAT internes existent pour l'interface de gestion (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Vérifier les autres paramètres

Consultez les commandes suivantes pour vérifier que tous les autres paramètres sont présents. Vous pouvez également voir un grand nombre de ces commandes sur la page de CDO **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (accès au gestionnaire - Détails de la configuration)** > **CLI Output (extrant de l'interface de ligne de commande)**.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Faire une recherche de mise à jour DDNS réussie

Dans l'interface de ligne de commande défense contre les menaces , vérifiez si la mise à niveau DDNS a réussi :

debug ddns

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

Si la mise à jour échoue, utilisez les commandes **debug http** et **debug ssl**. Pour les échecs de validation de certificat, vérifiez que les certificats racine sont installés sur le périphérique comme suit :

show crypto ca certificates *trustpoint_name*

Pour vérifier le fonctionnement du DDNS :

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Vérifiez les fichiers de journaux de CDO

See https://cisco.com/go/fmc-reg-error.

Restaurer la configuration en cas de perte de connexion de CDO

Si vous utilisez une interface de données sur le défense contre les menaces pour l'accès du gestionnaire, et que vous déployez un changement de configuration à partir de CDO qui a des répercussions sur la connectivité du réseau, vous pouvez restaurer la configuration sur le défense contre les menaces à la dernière configuration

déployée afin de pouvoir restaurer la connexion de gestion. Vous pouvez alors ajuster les paramètres de configuration dans CDO afin que la connexion au réseau soit maintenue, et redéployer. Vous pouvez utiliser la fonction de restauration même si vous ne perdez pas la connectivité. Cela ne se limite pas à ce dépannage.

Consultez les consignes suivantes :

- Seul le déploiement précédent est disponible localement sur défense contre les menaces ; vous ne pouvez pas restaurer les déploiements précédents.
- Le restaurer ne touche que les configurations que vous pouvez définir dans CDO. Par exemple, la restauration ne touche aucune configuration locale liée à l'interface de commande dédiée, que vous ne pouvez configurer qu'au niveau de l'interface de ligne de commande défense contre les menaces . Notez que si vous avez modifié les paramètres de l'interface de données après le dernier déploiement du CDO à l'aide de la commande **configure network management-data-interface** et que vous utilisez ensuite la commande de restauration, ces paramètres ne seront pas conservés ; ils seront restaurés aux paramètres du dernier CDO déployé.
- Les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions seront interrompues, car la configuration actuelle sera effacée.

Procédure

Étape 1 À l'interface de ligne de commande défense contre les menaces , restaurez la configuration précédente.

configure policy rollback

Après la restauration, le défense contre les menaces notifie le CDO que la restauration a été effectuée avec succès. Dans le CDO, l'écran de déploiement affiche une enseigne indiquant que la configuration a été restaurée.

Remarque Si la restauration échoue et que la gestion de la CDO est rétablie, reportez-vous à https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html pour connaître les problèmes de déploiement courants. Dans certains cas, la restauration peut échouer après le rétablissement de l'accès au gestionnaire du CDO; dans ce cas, vous pouvez résoudre les enjeux de la configuration du CDO, et redéployer à partir du CDO.

Exemple :

Pour le défense contre les menaces qui utilise une interface de données pour l'accès du gestionnaire :

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Étape 2 Vérifiez que la connexion de gestion a été rétablie.

Dans CDO, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (Accès au gestionnaire - Détails de la configuration)** > **Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 46.

Mettez le pare-feu hors tension à l'aide du CDO

Il est important que vous éteigniez votre système correctement. Débrancher l'alimentation ou appuyer sur le commutateur d'alimentation peut gravement endommager le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en permanence en arrière-plan, et que le fait de débrancher ou de couper l'alimentation ne permet pas l'arrêt en douceur de votre pare-feu.

Vous pouvez arrêter votre système correctement à l'aide de CDO.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion d'appareil)**.

Étape 2 À côté du périphérique que vous souhaitez redémarrer, cliquez sur l'icône de modification ( ).

Étape 3 Cliquez sur l'onglet **Device** (appareil).

Étape 4 Cliquez sur l'icône d'arrêt du périphérique ( ) dans la section **System** (système).

Étape 5 Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.

Étape 6 Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

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

Si vous n'avez pas de connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Étape 7 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Prochaines étapes

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