Défense contre les menaces Déploiement avec le Gestionnaire d'appareil

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

Pour voir tous les systèmes d'exploitation et gestionnaires disponibles, consultez Quels sont le et le gestionnaire d'applications pour vous?. Ce chapitre s'applique à défense contre les menaces avec le gestionnaire d'appareil.

Ce chapitre explique comment effectuer l'installation et la configuration initiales de défense contre les menaces à l'aide de l'assistant d'installation de l'appareil basé sur le Web.

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

À propos du pare-feu

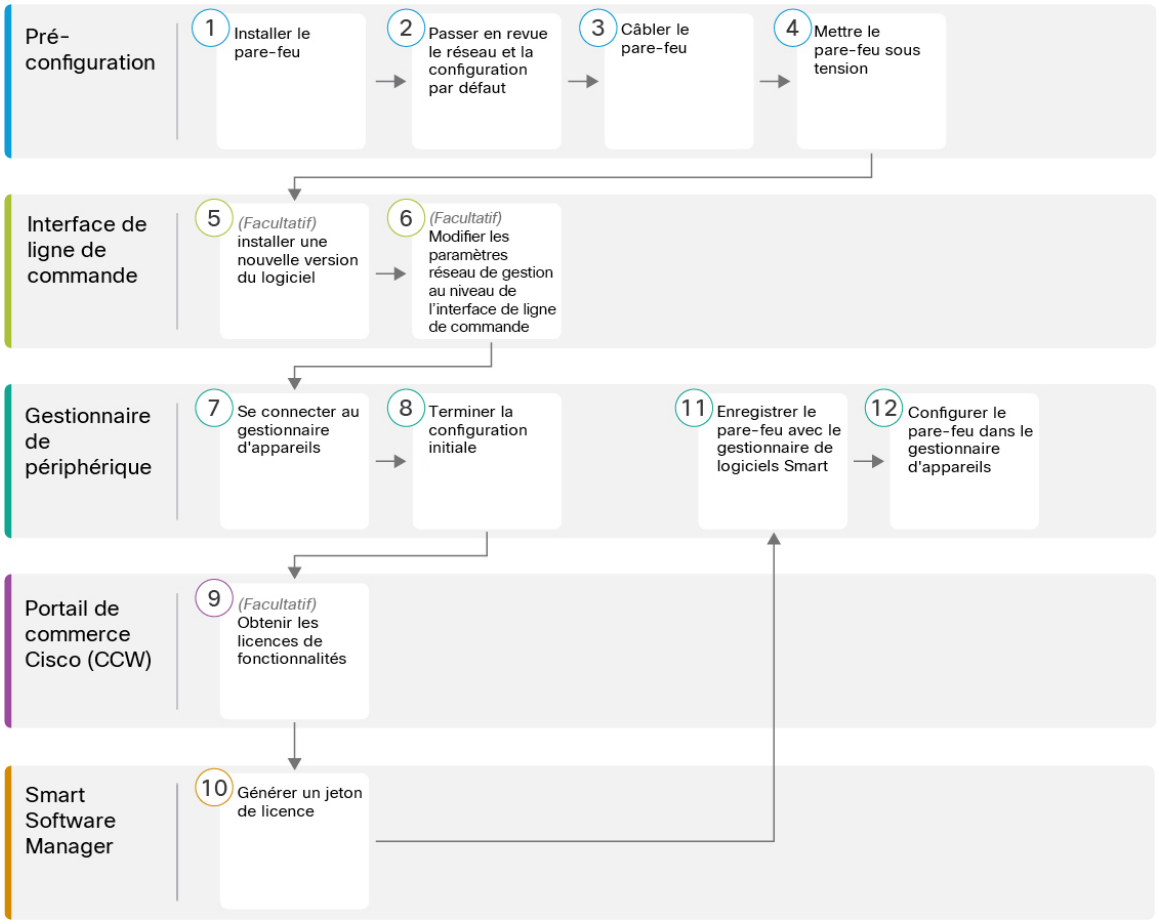
Le matériel peut exécuter un logiciel défense contre les menaces ou un logiciel ASA. La commutation entre défense contre les menaces et ASA nécessite de recréer l'image du périphérique. Vous devez également recréer l'image si vous avez besoin d'une version logicielle différente de celle actuellement 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.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer défense contre les menaces avec gestionnaire d'appareil sur votre châssis.



1	Pré-configuration	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.

2	Pré-configuration	Passer en revue le déploiement du réseau et la configuration par défaut, à la page 3.
3	Pré-configuration	Câbler l'appareil, à la page 7.
4	Pré-configuration	Mettez le pare-feu sous tension.
5	Interface de ligne de commande	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 9
6	Interface de ligne de commande	(Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 10.
7	Gestionnaire d'appareil	Se connecter à Gestionnaire d'appareil, à la page 13.
8	Gestionnaire d'appareil	Terminer la configuration initiale, à la page 13.
9	Portail de commerce Cisco (CCW)	(Facultatif) Configurer les licences, à la page 15 : Licences de fonctionnalité optionnelles
10	Smart Software Manager	Configurer les licences, à la page 15 : Générer un jeton de licence.
11	Gestionnaire d'appareil	Configurer les licences, à la page 15 : Enregistrer le périphérique auprès du serveur de licences Smart.
12	Gestionnaire d'appareil	Configurer le pare-feu dans le Gestionnaire d'appareil, à la page 21.

Passer en revue le déploiement du réseau et la configuration par défaut

Vous pouvez gérer le défense contre les menaces à partir de gestionnaire d'appareil l'interface Management 1/1 ou de l'interface interne. L'interface de gestion dédiée est une interface spéciale qui a ses propres paramètres réseau.

La figure suivante montre le déploiement réseau recommandé. Si vous connectez l'interface externe directement à un modem câble ou DSL, nous vous recommandons de mettre le modem en mode pont pour que défense contre les menaces effectue tout le routage et le NAT pour vos réseaux internes.Si vous devez configurer PPPoE pour que l'interface externe se connecte à votre fournisseur de services Internet, vous pouvez le faire après avoir terminé la configuration initiale dans gestionnaire d'appareil.

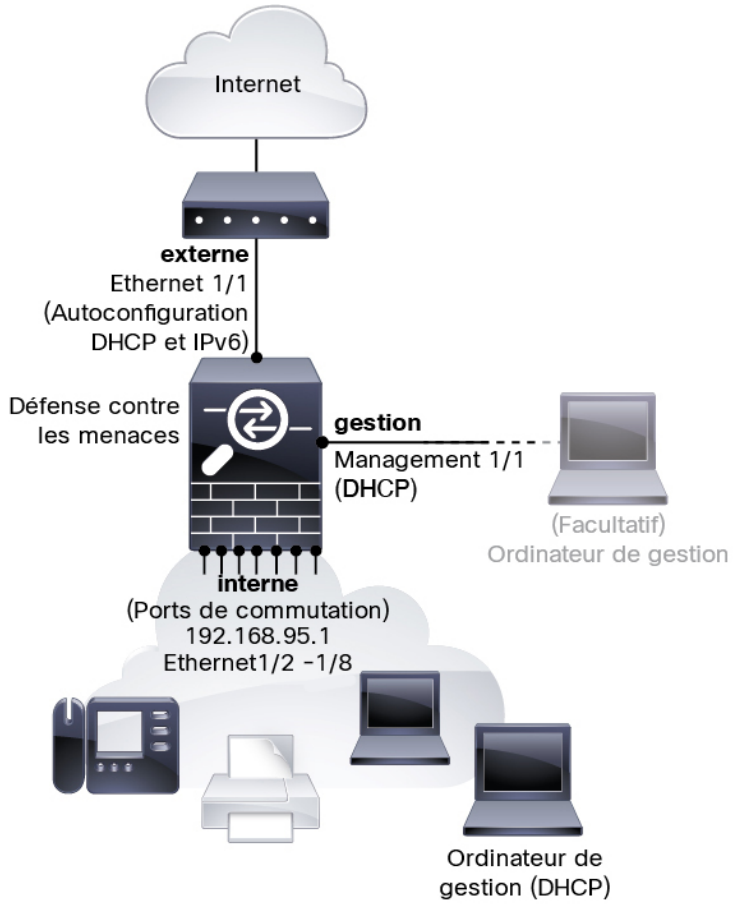
Remarque Si vous ne pouvez pas utiliser l’adresse IP de gestion par défaut (par exemple, votre réseau de gestion n’inclut pas de serveur DHCP), vous pouvez vous connecter au port de console et effectuer la configuration initiale au niveau de l’interface de ligne de commande, y compris la définition de l’adresse IP de gestion, de la passerelle et d’autres paramètres réseau de base.

Si vous devez changer l'adresse IP interne, vous pouvez le faire après avoir terminé la configuration initiale dans le gestionnaire d'appareil. Par exemple, vous devrez peut-être modifier l'adresse IP interne dans les cas suivants :

- (version 7.0 ou ultérieure) L’adresse IP interne est 192.168.95.1.(versions 6.7 et antérieures) L’adresse IP interne est 192.168.1.1. Si l’interface externe tente d’obtenir une adresse IP sur le réseau 192.168.1.0, qui est un réseau commun par défaut, le bail DHCP échouera et l’interface externe n’obtiendra pas d’adresse IP. Ce problème se produit parce que défense contre les menaces ne peut pas avoir deux interfaces sur le même réseau. Dans ce cas, vous devez modifier l’adresse IP interne pour être sur un nouveau réseau.
- Si vous ajoutez défense contre les menaces à un réseau interne existant, vous devrez modifier l’adresse IP interne pour qu’elle se trouve sur le réseau existant.

La figure suivante montre le déploiement du réseau par défaut pourdéfense contre les menaces pour l'utilisation du gestionnaire d'appareil avec la configuration par défaut.

Illustration 1 : Suggestion de déploiement réseau



Remarque Pour les versions 6.7 et antérieures, l'adresse IP interne est 192.168.1.1.

Pour les versions 6.5 et antérieures, l'adresse IP de gestion Management 1/1 est 192.168.45.45.

Configuration par défaut

La configuration du pare-feu après la configuration initiale comprend les éléments suivants :

- **interne** : adresse IP (version 7.0 ou ultérieure) 192.168.95.1; (version antérieure à 7.0) 192.168.1.1.
  - (version 6.5 ou ultérieure) **Commutateur matériel** : Ethernet 1/2 à 1/8 appartient à VLAN 1
  - (6.4) **Commutateur logiciel** (commutation et transition intégrées) : Ethernet 1/2 à 1/8 appartient à l'interface de groupe de pont (BVI) 1
- **externe** : Ethernet 1/1, adresse IP à partir de DHCP IPv4 et de l'autoconfiguration IPv6
- flux de trafic **interne** → **externe**
- **management** (gestion) : Management 1/1 (gestion)

- (versions 6.6 et ultérieures) Adresse IP du protocole DHCP
- (version 6.5 et versions antérieures) Adresse IP 192.168.45.45

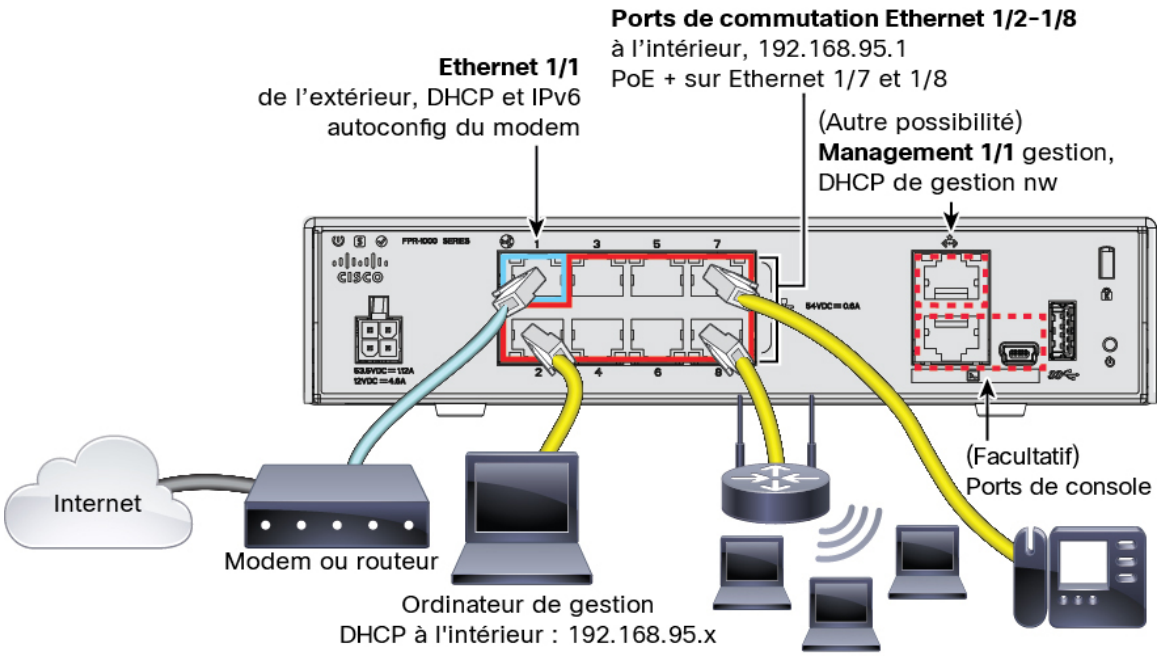
Remarque L'interface Management 1/1 est une interface spéciale distincte des interfaces de données utilisées pour la gestion, l'octroi de licences Smart et les mises à jour de bases de données. L'interface physique est partagée avec une deuxième interface logique, l'interface de diagnostic. Le diagnostic est une interface de données, mais se limite à d'autres types de trafic de gestion (vers l'appareil et à partir de l'appareil), comme syslog ou SNMP. L'interface de diagnostic n'est généralement pas utilisée. Consultez la section Guide Cisco Secure Firewall Device Manager Configuration pour obtenir plus de renseignements.

- **serveur DNS pour la gestion** : OpenDNS : (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35 ou les serveurs que vous définissez pendant la configuration. Les serveurs DNS obtenus à partir du protocole DHCP ne sont jamais utilisés.
- **NTP** : Serveurs NTP de Cisco : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org ou les serveurs que vous définissez pendant la configuration.
- **Routage par défaut**
  - **Interfaces de données** : Obtenues de l'extérieur du DHCP ou d'une adresse IP de passerelle que vous définissez pendant la configuration.
  - **Interface de gestion** : (version 6.6 ou ultérieure) Obtenue du DHCP de gestion. Si vous ne recevez pas de passerelle, la voie de routage par défaut passe par le fond de panier et par les interfaces de données. (version 6.5 et antérieure) Par l'intermédiaire du fond de panier et des interfaces de données

    Il convient de signaler que l'interface de gestion nécessite un accès Internet pour l'octroi de licences et les mises à jour, que ce soit par l'entremise du fond de panier ou à l'aide d'une passerelle Internet distincte. Il convient de signaler que seul le trafic provenant de l'interface de gestion peut passer par le fond de panier; autrement, la gestion n'autorise pas le trafic traversant pour le trafic entrant depuis le réseau.
- **Serveur DHCP** : Activé sur l'interface interne et sur l'interface de gestion (des versions 6.5 ou antérieures uniquement)
- **Gestionnaire d'appareil access (accès)**— Tous les hôtes autorisés sur le gestionnaire et l'interface interne.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur

Câbler l'appareil

Illustration 2 : Câblage du Firepower 1010



Remarque Pour les versions 6.7 ou antérieures, l'adresse IP interne est 192.168.1.1.

Pour les versions 6.5 et antérieures, l'adresse IP par défaut de gestion Management 1/1 est 192.168.45.45.

Remarque Dans les versions 6.5 ou ultérieures, 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. Dans la version 6.4, les ports Ethernet 1/2 à 1/8 sont configurés comme des membres de groupes de ponts (ports de commutation logicielle); PoE+ n'est pas disponible. Le câblage initial est le même pour les deux versions.

Assurez la gestion de Firepower 1010 au moyen de l'interface de gestion Management 1/1 ou de l'Ethernet 1/2 à 1/8. Selon la configuration par défaut, Ethernet 1/1 est également défini comme externe.

Procédure

Étape 1 Installez et familiarisez-vous avec votre matériel à l'aide du guide d'installation du matériel.

Étape 2 Connectez votre ordinateur de gestion à l'une des interfaces suivantes :

- Ethernet 1/2 à 1/8 : Connectez votre ordinateur de gestion directement à l'un des ports de commutation internes (Ethernet 1/2 à 1/8). L'adresse IP par défaut de l'interface interne est (192.168.95.1). Cette interface exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris

l'ordinateur de gestion). Assurez-vous donc que ces paramètres n'entrent pas en conflit avec les paramètres du réseau interne (voir Configuration par défaut, à la page 5).

- Management 1/1 (interface désignée MGMT) : Connectez l'interface de gestion Management 1/1 à votre réseau de gestion et assurez-vous que votre ordinateur de gestion est relié au réseau de gestion ou y a accès. La gestion 1/1 obtient une adresse IP à partir d'un serveur DHCP sur votre réseau de gestion ; si vous utilisez cette interface, vous devez déterminer l'adresse IP attribuée à défense contre les menaces afin de pouvoir vous connecter à l'adresse IP à partir de votre ordinateur de gestion.

  Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut pour configurer une adresse IP statique, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 10.

Étape 3 Connectez le réseau externe à l'interface Ethernet 1/1.

Par défaut, l'adresse IP est obtenue à l'aide du protocole DHCP IPv4 et de la configuration automatique IPv6, mais vous pouvez définir une adresse statique lors de la configuration initiale.

Étape 4 Connectez les appareils internes aux ports de commutation restants, Ethernet 1/2 à 1/8.

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

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

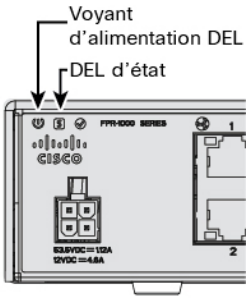
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne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

(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).

Procédure

Étape 1 Connexion à l'interface de ligne de commande. Consultez Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 25 pour de plus amples renseignements. Cette procédure illustre l'utilisation du port de console, mais vous pouvez utiliser SSH à la place.

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 (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 10. 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.

(Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande

Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut, vous pouvez vous connecter au port de console et effectuer la configuration initiale au niveau de l'interface de ligne de commande, y compris la définition de l'adresse IP de gestion, de la passerelle et d'autres paramètres réseau de base. Vous ne pouvez configurer que les paramètres de l'interface de gestion; vous ne pouvez pas configurer d'interfaces internes ou externes, que vous pouvez configurer ultérieurement dans l'interface graphique.

Remarque Vous ne pouvez pas relancer le script 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.

Procédure

Étape 1 Connexion au port de la console défense contre les menaces . Consultez Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 25 pour de plus amples renseignements.

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

Vous vous connectez à l'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 devrez recréer l'image du périphérique pour réinitialiser le mot de passe selon sa valeur par défaut. Consultez le guide de dépannage FXOS pour consulter la procédure de recréation d'image.

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

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 3 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). Vous verrez ensuite le script de configuration de l'interface de ligne de commande.

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 :

- **Enter the IPv4 default gateway for the management interface** (saisissez la passerelle IPv4 par défaut pour l'interface de gestion). Si vous définissez une adresse IP manuelle, saisissez les interfaces de données (**data-interfaces**) ou l'adresse IP du routeur de passerelle. Le paramètre **data-interfaces** envoie le trafic de gestion sortant sur le fond de panier pour quitter une interface de données. Ce paramètre est utile si vous ne disposez pas d'un réseau de gestion distinct pouvant accéder à Internet. Le trafic provenant de l'interface de gestion comprend l'enregistrement des licences et les mises à jour de base de données qui nécessitent un accès Internet. Si vous utilisez des **data-interfaces (interfaces de données)**, vous pouvez toujours utiliser le gestionnaire d'appareil (ou SSH) sur l'interface de gestion si vous êtes directement connecté au réseau de gestion, mais pour la gestion à distance de réseaux ou d'hôtes particuliers, vous devez ajouter une route statique à l'aide de la commande **configure network static-routes**. Notez que la gestion de gestionnaire d'appareil sur les interfaces de données n'est pas touchée par ce paramètre. Si vous utilisez DHCP, le système utilise la passerelle fournie par DHCP et utilise les interfaces de données (**data-interfaces**) comme méthode de secours si DHCP ne fournit pas de passerelle.
- **If your networking information has changed, you will need to reconnect** (si vos informations réseau ont changé, vous devrez vous reconnecter) : Si vous êtes connecté avec SSH à l'adresse IP par défaut, mais que vous avez changé l'adresse IP au moment de la configuration initiale, vous serez déconnecté. Reconnectez-vous avec la nouvelle adresse IP et le nouveau mot de passe. Les connexions à la console ne sont pas touchées.
- **Gérer l'appareil localement ?**— Saisissez **yes (oui)** pour utiliser le gestionnaire d'appareil ou le CDO/gestionnaire d'appareil. Une réponse **no (non)** signifie que vous avez l'intention d'utiliser le centre de gestion pour gérer l'appareil.

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 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]: 10.10.10.1
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]: yes

>
```

Étape 4 Connectez-vous à gestionnaire d'appareil sur la nouvelle adresse IP de gestion.

Se connecter à Gestionnaire d'appareil

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

Avant de commencer

- Utilisez une version actuelle de Firefox, Chrome, Safari, Edge ou Internet Explorer.

Procédure

Étape 1 Entrez l'URL suivante dans votre navigateur.

- (version 7.0 ou ultérieure) Interne Inside (Ethernet1/2 through 1/8)—**https://192.168.95.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutation interne (Ethernet 1/2 à 1/8).
- (version 6.7 ou antérieure) Interne(Ethernet 1/2 à 1/8) : **https://192.168.1.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutation interne (Ethernet 1/2 à 1/8).
- (version 6.6. ou ultérieure) Management (gestion) : **https://***management_ip*. Étant donné que l'interface de gestion est un client DHCP, l'adresse IP dépend de votre serveur DHCP. Si vous avez modifié l'adresse IP de gestion lors de la configuration de l'interface de ligne de commande, saisissez cette adresse.
- (version 6.5 ou antérieure) Management (: gestion) **https://192.168.45.45**. Si vous avez modifié l'adresse IP de gestion lors de la configuration de l'interface de ligne de commande, saisissez cette adresse.

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

Prochaine étape

- Exécutez l'assistant de configuration gestionnaire d'appareil; voir Terminer la configuration initiale, à la page 13.

Terminer la configuration initiale

Utilisez l'assistant de configuration lorsque vous vous connectez pour la première fois au gestionnaire d'appareil pour terminer la configuration initiale. Après avoir terminé la configuration avec l'assistant, vous devriez avoir un périphérique qui fonctionne avec quelques règles de base en place :

- Une interface externe (Ethernet1/1) et une interface interne. Les interfaces Ethernet 1/2 à 1/8 sont des ports de commutation sur l'interface interne VLAN1 (version 6.5 ou ultérieure) ou des membres du groupe de ponts interne sur BVI1 (6.4).
- Zones de sécurité pour les interfaces interne et externe.
- Une règle d'accès qui fait confiance au trafic interne et externe.
- Une règle d'interface NAT qui traduit tout le trafic interne vers externe vers des ports uniques sur l'adresse IP de l'interface externe.

- Un serveur DHCP fonctionnant sur l'interface interne.

Remarque Si vous avez effectué la procédure (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 10, certaines de ces tâches, notamment la modification du mot de passe d'administrateur et la configuration des interfaces externe et de gestion, devraient déjà avoir été effectuées.

Procédure

Étape 1 Vous devrez lire et accepter le contrat de licence utilisateur final et modifier le mot de passe administrateur.

Vous devez suivre ces étapes pour continuer.

Étape 2 Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

Remarque Vos paramètres sont déployés sur l'appareil lorsque vous cliquez sur **Next** (suivant). L'interface sera désignée comme « externe » et sera ajoutée à la zone de sécurité « outside_zone ». Vérifiez que vos paramètres sont corrects.

a) **Interface externe** : Il s'agit du port de données que vous avez connecté à votre routeur de passerelle. 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.

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.

b) **Interface de gestion**

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.

Étape 3 Configurez les paramètres d'heure du système et cliquez sur **Next** (suivant).

a) **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
b) **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.

Étape 4 (Facultatif) Configurez les licences Smart pour le système.

Votre achat de l'appareil défense contre les menaces inclut automatiquement une licence de base. Toutes les licences supplémentaires sont facultatives.

Vous devez avoir un compte de licence Smart pour obtenir et appliquer les licences requises par le système. Au départ, vous pouvez utiliser la licence d'évaluation de 90 jours, puis configurer les licences Smart ultérieurement.

Pour enregistrer le périphérique maintenant, cliquez sur le lien pour vous connecter à votre compte Smart Software Manager et ; voir Configurer les licences, à la page 15.

Pour utiliser la licence d'évaluation, sélectionnez **Start 90 day evaluation period without registration** (commencer la période d'évaluation de 90 jours sans inscription).

Étape 5 Cliquez sur **Finish** (terminer).

Prochaine étape

- Bien que vous puissiez continuer à utiliser la licence d'évaluation, nous vous recommandons d'enregistrer et d'autoriser votre appareil; voir Configurer les licences, à la page 15.
- Vous pouvez également choisir de configurer l'appareil à l'aide de gestionnaire d'appareil; voir Configurer le pare-feu dans le Gestionnaire d'appareil, à la page 21.

Configurer les licences

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

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

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

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

- **Threat (menace)** : Renseignements 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

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.

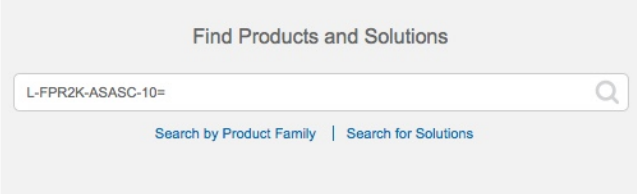
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

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.

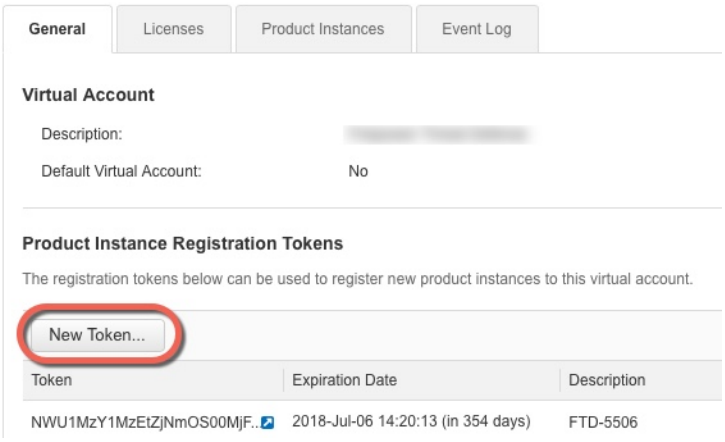
- Combinaison de licences englobant les menaces, les logiciels malveillants et les adresses URL :
  - L-FPR1010T-TMC=

  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.

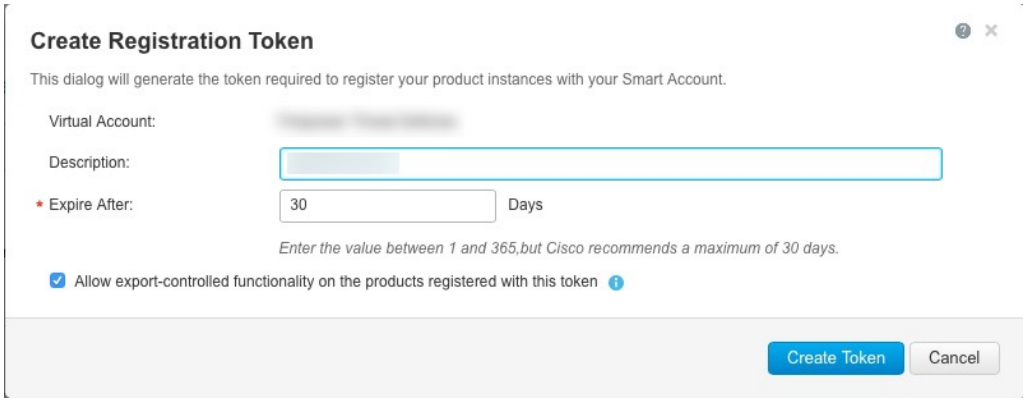
Étape 2 Dans le Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous voulez ajouter ce périphérique.

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

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



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



- **Description**
- **Expire After** (expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token**(autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton : Active l'indicateur de conformité à l'exportation si vous êtes dans un pays qui autorise un cryptage renforcé. Vous devez sélectionner cette option maintenant si vous prévoyez d'utiliser cette fonctionnalité. Si vous activez cette fonctionnalité ultérieurement, vous devrez réenregistrer votre appareil avec une nouvelle clé de produit et recharger l'appareil. Si vous ne voyez pas cette option, votre compte ne prend pas en charge la fonctionnalité d'exportation contrôlée.

Le jeton est ajouté à votre inventaire.

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

Illustration 4 : Afficher le jeton

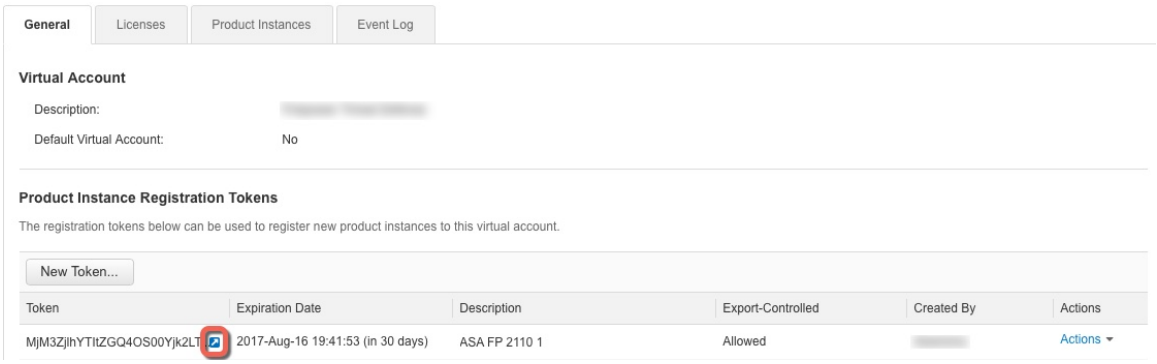
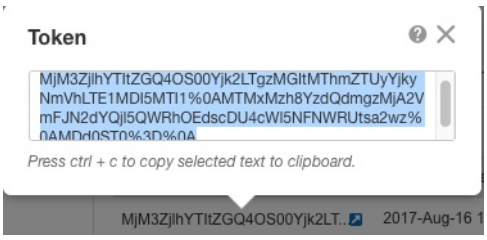


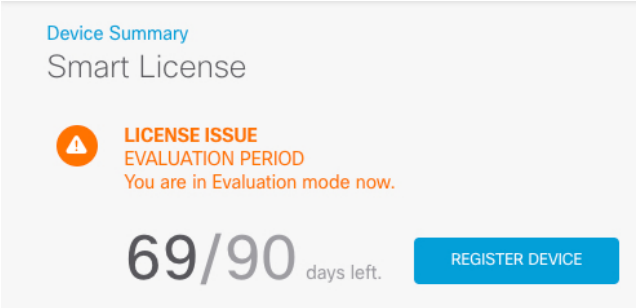
Illustration 5 : Copier le jeton



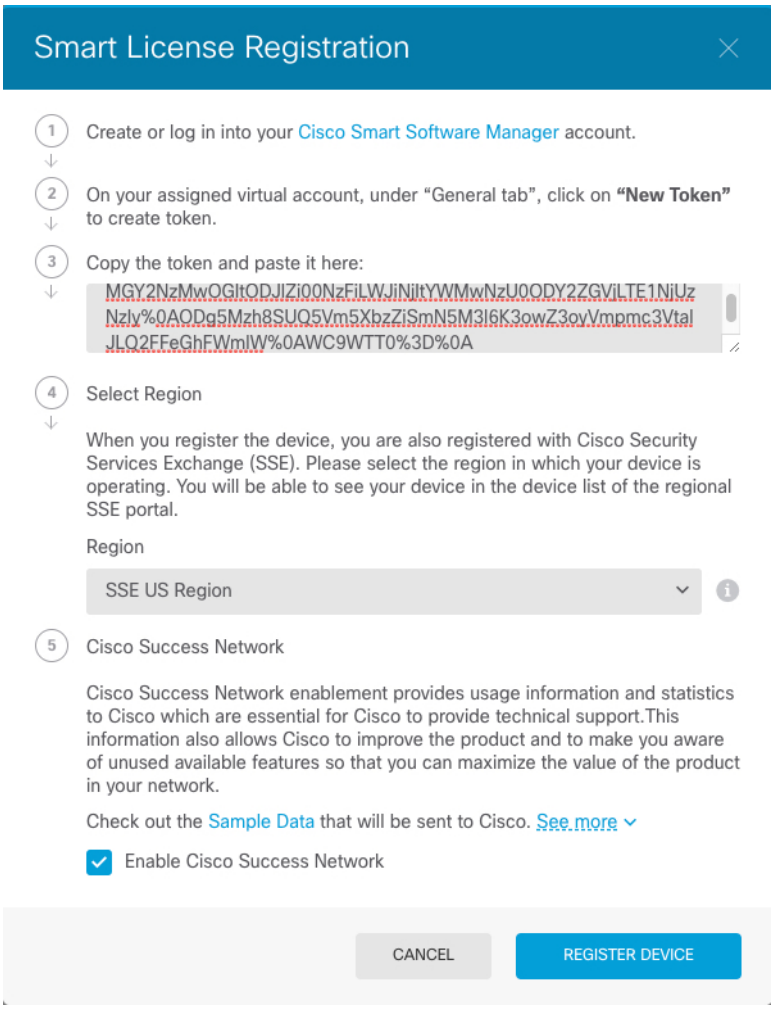
Étape 3 Dans le gestionnaire d'appareil, cliquez sur **Device (appareil)**, et puis dans le sommaire **Smart License** cliquez sur **View Configuration (voir configuration)**.

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

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



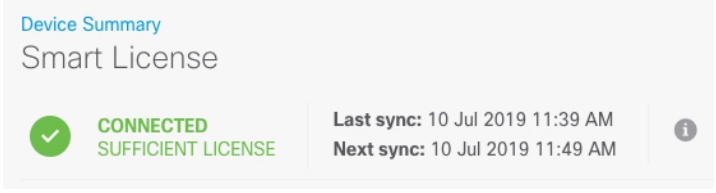
Suivez ensuite les instructions de la boîte de dialogue **Smart License Registration** pour coller votre jeton :



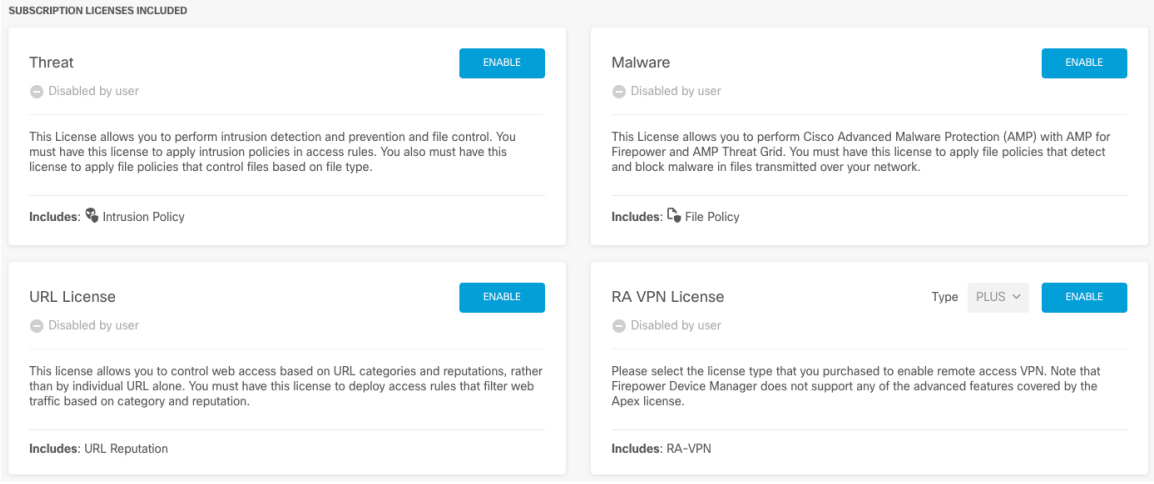
Étape 5 Cliquez sur **Register Device** (enregistrer l'appareil).

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

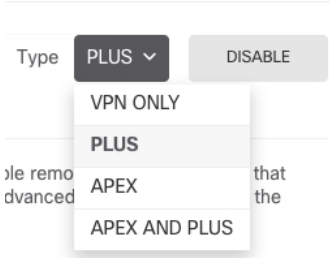
Une fois que l'appareil a été enregistré et que vous avez actualisé la page, les éléments suivants apparaissent :



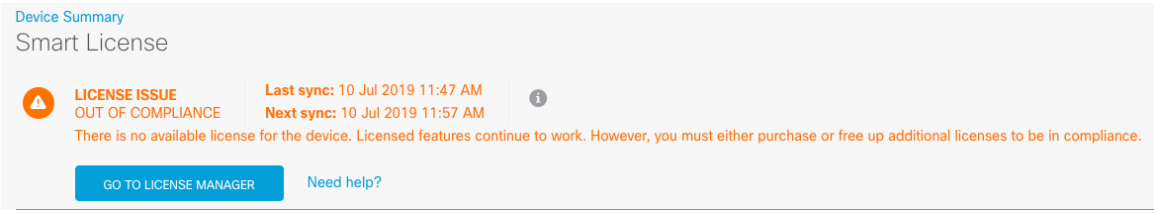
Étape 6 Cliquez sur **Enable/Disable** (activer/désactiver) pour chaque licence facultative, au besoin.



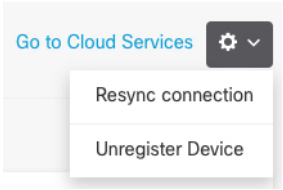
- **Enable** (activer) : Enregistre la licence avec votre compte Cisco Smart Software Manager et active les fonctionnalités contrôlées. Vous pouvez maintenant configurer et déployer les politiques contrôlées par la licence.
- **Disable** (désactiver) : Désinscrit la licence de votre compte Cisco Smart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



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



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



Configurer le pare-feu dans le Gestionnaire d'appareil

Les étapes suivantes donnent un aperçu des fonctionnalités supplémentaires que vous pourriez souhaiter configurer. Veuillez cliquer sur le bouton d'aide (**?**) dans une page pour obtenir des renseignements détaillés sur chaque étape.

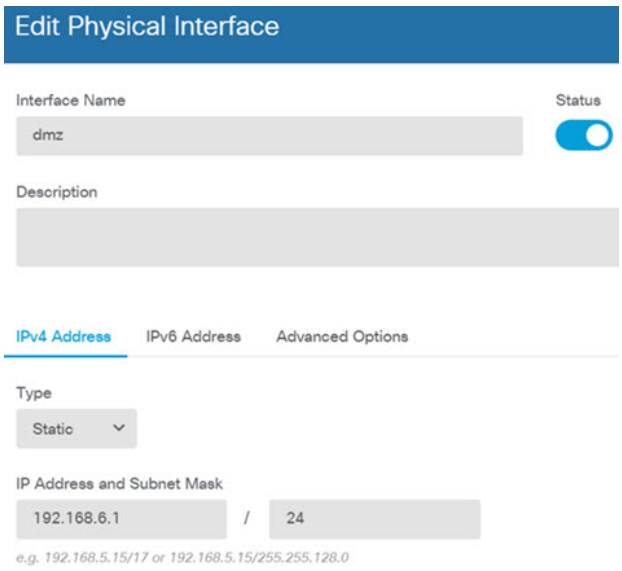
Procédure

Étape 1 Si vous avez souhaitez convertir une interface de groupe de pont (6.4) ou souhaitez convertir un port de commutation en une interface de pare-feu (6.5 et versions ultérieures), choisissez **Device** (périphérique), puis cliquez sur le lien dans le résumé des **Interfaces**.

Cliquez sur l'icône de modification ( ) pour chaque interface afin de définir le mode, l'adresse IP et d'autres paramètres.

Dans l'exemple suivant, une interface est configurée pour être utilisée comme « zone démilitarisée » (DMZ), où vous placez des ressources accessibles au public, comme votre serveur Web. Lorsque vous avez terminé, cliquez sur **Save** (enregistrer).

Illustration 6 : Modifier l'interface



Étape 2 Si vous avez configuré de nouvelles interfaces, sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

Modifiez ou créez de nouvelles zones, selon le cas. Chaque interface doit appartenir à une zone, car vous configurez les politiques en fonction des zones de sécurité et non des interfaces. Vous ne pouvez pas placer les interfaces dans des zones lors de leur configuration. Par conséquent, vous devez toujours modifier les objets des zones après avoir créé de nouvelles interfaces ou modifié le but des interfaces existantes.

L'exemple suivant montre comment créer une nouvelle zone dmz pour l'interface dmz.

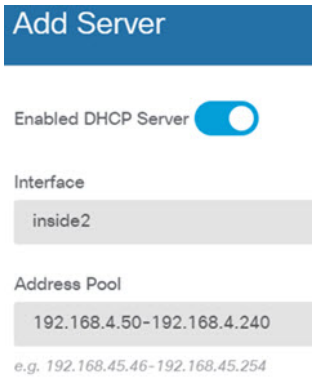
Illustration 7 : Objet de zone de sécurité

Étape 3 Si vous souhaitez que les clients internes utilisent le protocole DHCP pour obtenir une adresse IP du périphérique, sélectionnez **Device (appareil)** > **System Settings (paramètres système)** > **DHCP Server (serveur DHCP)**, puis sélectionnez l'onglet des serveurs DHCP (**DHCP Servers**).

Un serveur DHCP est déjà configuré pour l'interface interne, mais vous pouvez modifier l'ensemble des adresses ou même le supprimer. Si vous avez configuré d'autres interfaces internes, il est très courant de configurer un serveur DHCP pour ces interfaces. Cliquez sur le signe plus (+) pour configurer le serveur et l'ensemble d'adresses pour chaque interface interne.

Vous pouvez également affiner la liste WINS et DNS fournie aux clients dans l'onglet **Configuration**. L'exemple suivant montre comment configurer un serveur DHCP sur l'interface interne 2 avec l'ensemble d'adresses 192.168.4.50-192.168.4.240.

Illustration 8 : Serveur DHCP



Étape 4 Sous **Device** (périphérique), cliquez sur **View Configuration** (afficher la configuration) (ou **Create First Static Route** pour créer la première voie de routage statique) dans le groupe **Routing** (routage) et configurez le routage par défaut.

La voie de routage par défaut s'oriente normalement vers le routeur ISP (ou en amont) qui se trouve à côté de l'interface externe. Une voie de routage IPv4 par défaut est configuré sur any-ipv4 (0.0.0.0/0), alors qu'un routage IPv6 par défaut est configuré sur any-ipv6 (:: 0/0). Créez le routage pour chaque version IP que vous utilisez. Si vous utilisez le protocole DHCP pour obtenir une adresse pour l'interface externe, vous avez peut-être déjà accès au routage par défaut dont vous avez besoin.

Remarque Les voies de routage que vous définissez sur cette page concernent uniquement les interfaces de données. Elles n'ont aucun impact sur l'interface de gestion. Définissez la passerelle de gestion sous **Device (appareil)** > **System Settings (paramètres système)** > **Management Interface (interface de gestion)**.

L'exemple suivant montre une voie de routage par défaut pour IPv4. Dans cet exemple, la passerelle isp-gateway est un objet réseau qui identifie l'adresse IP de la passerelle du fournisseur de services Internet (vous devez obtenir l'adresse de votre fournisseur de services Internet). Vous pouvez créer cet objet en cliquant sur **Create New Network** (créer un nouveau réseau) au bas du menu déroulant **Gateway** (passerelle).

Illustration 9 : Routage par défaut

Étape 5 Sélectionnez les politiques sous **Policies** et configurez les politiques de sécurité pour le réseau.

L'assistant de configuration de périphérique active le flux du trafic entre la zone interne et la zone externe ainsi que la NAT d'interface pour toutes les interfaces vers l'interface externe. Même si vous configurez de nouvelles interfaces, si vous les ajoutez à l'objet dans la zone interne, la règle de contrôle d'accès s'applique automatiquement à celles-ci.

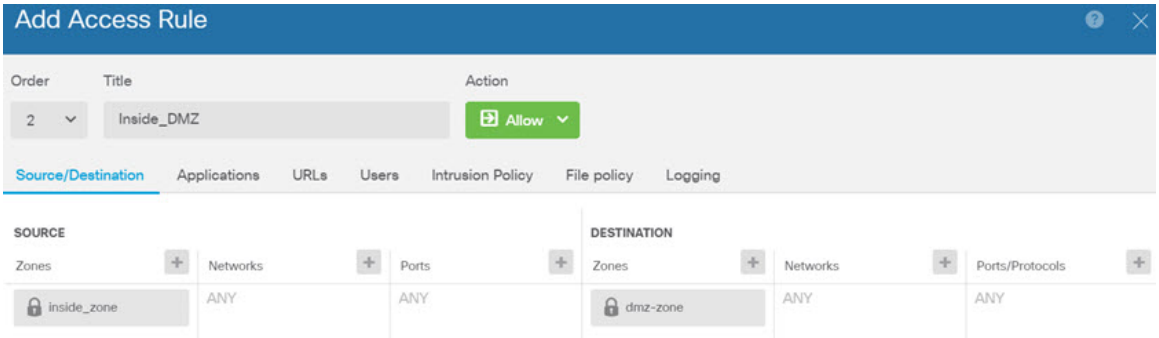
Cependant, si vous avez plusieurs interfaces internes, vous avez besoin d'une règle de contrôle d'accès pour permettre la circulation du trafic d'une zone interne à une autre. Si vous ajoutez d'autres zones de sécurité, vous avez besoin de règles pour autoriser le trafic en provenance et à destination de ces zones. Il s'agit de vos modifications minimales.

En outre, vous pouvez configurer d'autres politiques pour fournir des services supplémentaires et affiner la NAT et les règles d'accès afin d'obtenir les résultats requis par votre organisation. Vous pouvez configurer les politiques suivantes :

- **Déchiffrement SSL** : Si vous souhaitez inspecter les connexions chiffrées (comme HTTPS) pour détecter les intrusions, les logiciels malveillants, etc., vous devez déchiffrer les connexions. Utilisez la politique de déchiffrement SSL pour déterminer les connexions qui doivent être déchiffrées. Le système rechiffre la connexion après l'avoir inspectée.
- **Identité** : Si vous souhaitez corréler l'activité du réseau à des utilisateurs individuels ou contrôler l'accès au réseau en fonction de l'utilisateur ou de l'appartenance à un groupe d'utilisateurs, utilisez la politique d'identité pour déterminer l'utilisateur associé à une adresse IP source donnée.
- **Renseignements de sécurité** : Utilisez la politique sur les renseignements de sécurité pour supprimer rapidement les connexions en provenance des adresses IP ou des URL de la liste noire ou vers celles-ci. En inscrivant sur la liste noire les mauvais sites connus, vous n'avez pas besoin de les prendre en compte dans votre politique de contrôle d'accès. Cisco fournit des flux régulièrement mis à jour d'adresses et d'adresses URL incorrectes afin que la liste noire issue des renseignements de sécurité se mette à jour de façon dynamique. En utilisant les flux, vous n'avez pas besoin de modifier la politique pour ajouter ou supprimer des éléments dans la liste noire.
- **NAT (traduction d'adresses réseau)** : Utilisez le protocole NAT pour convertir les adresses IP internes en adresses de routage externe.
- **Contrôle d'accès** : Utilisez la politique de contrôle d'accès pour déterminer les connexions autorisées sur le réseau. Vous pouvez procéder au filtrage selon la zone de sécurité, l'adresse IP, le protocole, le port, l'application, l'adresse URL, l'utilisateur ou le groupe d'utilisateurs. Vous pouvez aussi appliquer également des politiques en lien avec la prévention des intrusions et avec la présence de fichiers (logiciels malveillants) en utilisant des règles de contrôle d'accès. Utilisez cette politique pour mettre en œuvre le filtrage d'URL.
- **Intrusion** : Utilisez les politiques de prévention des intrusions pour rechercher les menaces connues. Bien que vous appliquiez des politiques de prévention des intrusions à l'aide de règles de contrôle d'accès, vous pouvez modifier lesdites politiques pour activer ou désactiver sélectivement des règles de prévention précises en lien avec les intrusions.

L'exemple suivant montre comment autoriser le trafic entre la zone interne et la zone dmz dans la politique de contrôle d'accès. Dans cet exemple, aucune option n'est définie sous les autres onglets, à l'exception de la journalisation (**Logging**), pour laquelle l'option **At End of Connection** (à la fin de la connexion) est sélectionnée.

Illustration 10 : Politique de contrôle d'accès



Étape 6 Choisissez **Device** (appareil), puis cliquez sur **View Configuration** (afficher la configuration) sous **Updates** (mises à jour) et configurez les calendriers de mise à jour pour les bases de données système.

Si vous utilisez des politiques de prévention des intrusions, configurez des mises à jour régulières pour les règles et pour les bases de données de vulnérabilités (VDB). Si vous utilisez des flux de renseignements de sécurité, définissez un calendrier de mise à jour pour ceux-ci. Si vous utilisez la géolocalisation comme critères de correspondance dans toute politique de sécurité, définissez un calendrier de mise à jour pour cette base de données.

Étape 7 Cliquez sur le bouton **Deploy** (déployer) dans le menu, puis cliquez sur le bouton Deploy Now ( ) pour déployer immédiatement vos modifications sur le périphérique.

Les modifications ne sont actives sur le périphérique que lorsque vous les déployez.

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#
```

Consulter l'information sur le matériel

Utilisez l'interface de ligne de commande (CLI) pour afficher des informations au sujet de votre matériel, y compris le modèle de périphérique, la version du matériel, le numéro de série et les composants du châssis, y compris les blocs d'alimentation et les modules de réseau. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console; voir Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 25.

Procédure

Étape 1 Pour afficher le modèle matériel du périphérique, utilisez la commande **show model**.

>**show model**

Exemple :

```
> show model
Cisco Firepower 1010 Threat Defense
```

Étape 2 Pour afficher le numéro de série du châssis, utilisez la commande **show serial-number**.

>**show serial-number**

Exemple :

```
> show serial-number
JMX1943408S
```

Ces informations sont également affichées dans **show version system**, **show running-config** et **show inventory**.

Étape 3 Pour afficher des informations sur tous les produits Cisco installés dans le périphérique réseau auxquels sont attribués un identifiant de produit (PID), un identifiant de version (VID) et un numéro de série (SN), utilisez la commande **show inventory**.

>**show inventory**

a) À partir de l'interface de ligne de commande défense contre les menaces :

Exemple :

```
> show inventory
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010          , VID: V00     , SN: JMX1943408S
```

b) À partir de l'interface de ligne de commande de FXOS :

Exemple :

```
firepower /chassis # show inventory
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-1010        Cisco Systems, In JMX1943408S 0.3
```

Arrêter le pare-feu

Il est important que vous éteigniez votre système correctement. Débrancher l'alimentation d'alimentation peut endommager gravement 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 système de pare-feu.

Le châssis Firepower 1010 n'a pas de commutateur d'alimentation externe.Vous pouvez désactiver le pare-feu à l'aide de gestionnaire d'appareil ou utiliser l'interface de ligne de commande de FXOS.

Mettez le pare-feu hors tension à l'aide de Gestionnaire d'appareil

Vous pouvez arrêter votre système correctement en utilisant le gestionnaire d'appareil.

Procédure

Étape 1 Utilisez le gestionnaire d'appareil pour mettre le pare-feu hors tension.

Remarque Pour les versions 6.4 et antérieures, saisissez la commande **shutdown** dans l'interface de ligne de commande gestionnaire d'appareil.

a) Cliquez sur **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Reboot/Shutdown (redémarrage/arrêt)**.
b) Cliquez sur **Shut Down** (arrêter).

Étape 2 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 3 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Mettre le périphérique hors tension au niveau de l'interface de ligne de commande (CLI)

Vous pouvez utiliser l'interface de ligne de commande (CLI) FXOS pour arrêter le système en toute sécurité et éteindre le périphérique. Pour accéder à l'interface de ligne de commande, connectez-vous au port de console; voir Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 25.

Procédure

Étape 1 Dans le Interface de ligne de commande FXOS, connectez-vous à local-mgmt :

firepower # **connect local-mgmt**

Étape 2 Envoyez la commande **shutdown** :

firepower(local-mgmt) # **shutdown**

Exemple :

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Étape 3 Surveillez les messages-guides du système lorsque le pare-feu se ferme. La notification suivante s'affichera :

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

Étape 4 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Quelle est l'étape suivante?

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

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

Quelle est l'étape suivante?