Déploiement d'ASA avec ASDM

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 l'ASA utilisant l'ASDM.

Ce chapitre n'aborde pas les déploiements suivants. Pour en savoir plus à ce sujet, consultez le guide de configuration ASA :

- Basculement
- Configuration de l'interface de ligne de commande

Ce chapitre vous guide dans la configuration d'une politique de sécurité de base; si vous avez des exigences plus avancées, consultez le guide de configuration.

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 l'ASA

L'ASA fournit des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN dans un seul appareil.

Vous pouvez gérer l'ASA en utilisant l'une des solutions de gestion suivantes :

- ASDM (couvert dans ce guide) - Un gestionnaire d'appareil unique inclus sur le périphérique.
- Interface de ligne de commande
- CDOf— Un gestionnaire multi-appareils simplifié, basé sur le nuage.
- Cisco Security Manager : Un gestionnaire pour plusieurs appareils hébergé sur un serveur distinct.

Vous pouvez également accéder à l'interface de ligne de commande de FXOS à des fins de dépannage.

Fonctionnalités non prises en charge

Fonctions générales ASA non prises en charge

Les fonctionnalités ASA suivantes ne sont pas prises en charge sur le Firepower 1010 :

- Mode contexte multiple
- Basculement actif/actif
- Interfaces redondantes
- Mise en grappes
- API REST ASA
- Module ASA FirePOWER
- Filtre de trafic Botnet
- Les inspections suivantes :
  - Cartes d'inspection SCTP (l'inspection avec état SCTP à l'aide d'ACL est prise en charge)
  - Diamètre
  - GTP/GPRS

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique

- Routage multidiffusion
- Routage basé sur une stratégie
- Routage multiples chemins à coûts égaux (ECMP)
- Ensembles en ligne ou interfaces passives
- VXLAN
- EtherChannels
- Basculement et lien d'état
- Zones de circulation
- Balise du groupe de sécurité (SGT)

Migration d'une configuration ASA 5500-X

Vous pouvez copier et coller une configuration ASA 5500-X dans le Firepower 1010. Cependant, vous devrez modifier votre configuration. Notez également certaines différences de comportement entre les plateformes.

1. Pour copier la configuration, entrez la commande**more system:running-config** sur l'ASA 5500-X.
2. Modifiez la configuration si nécessaire (voir ci-dessous).
3. Connectez-vous au port console du Firepower 1010, et entrez en mode de configuration globale :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. Effacez la configuration actuelle à l'aide de la commande **clear configure all**.
5. Collez la configuration modifiée à l'interface dans l'interface de ligne de commande d'ASA.

Ce guide suppose une configuration par défaut, donc si vous collez une configuration existante, certaines procédures de ce guide ne s'appliqueront pas à votre ASA.

Configuration ASA 5500-X	Firepower 1010

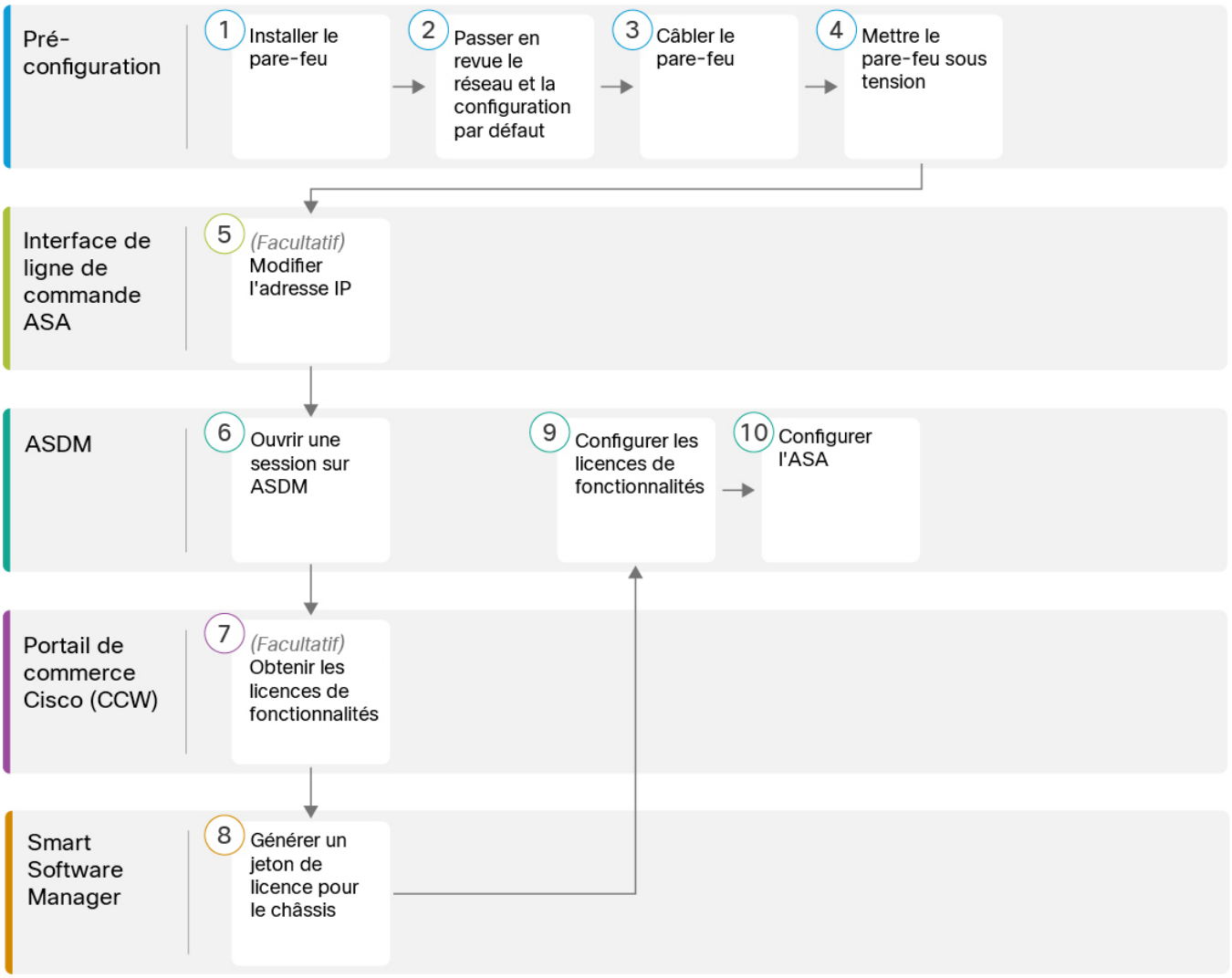
Interfaces de pare-feu Ethernet 1/2 à 1/8	Ports de commutation Ethernet 1/2 à 1/8
	Ces ports Ethernet sont configurés comme ports de commutation par défaut. Pour chaque interface de votre configuration, ajoutez la commande **no switchport** pour en faire des interfaces de pare-feu classiques. Par exemple :
	`interface ethernet 1/2`
	`  no switchport`
	`  ip address 10.8.7.2 255.255.255.0`
	`  nameif inside`

Licence PAK	Licence Smart Les licences PAK ne sont pas appliquées lorsque vous copiez et collez votre configuration. Aucune licence n'est installée par défaut. La licence Smart exige que vous vous connectiez au serveur de licences Smart pour obtenir vos licences. Les licences Smart jouent également sur l'accès ASDM ou SSH (voir ci-dessous).
Accès ASDM initial	Supprimez tout VPN ou toute autre configuration de fonctionnalité de chiffrement renforcé, même si vous avez uniquement configuré le chiffrement faible, si vous ne pouvez pas vous connecter à ASDM ou vous inscrire auprès du serveur de licences Smart. Vous pouvez réactiver ces fonctionnalités après avoir obtenu la licence de chiffrement fort (3DES). Ce problème vient de ce que l'ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement. Si vous activez une fonction de chiffrement fort, le trafic ASDM et HTTPS (comme celui en provenance et à destination du serveur de licences Smart) est bloqué. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté.
ID des interfaces	Assurez-vous de modifier les ID d'interface pour les faire correspondre aux nouveaux ID de matériel. Par exemple, l'ASA 5525-X comprend Management 0/0 et GigabitEthernet 0/0 à 0/5. Firepower 1120 comprend la gestion 1/1 et Ethernet 1/1 à 1/8.

Configuration ASA 5500-X	Firepower 1010
Commandes **boot system** L'ASA 5500-X permet jusqu'à quatre commandes **boot system** pour spécifier l'image de démarrage à utiliser.	Le Firepower 1010 ne permet qu'une seule commande **boot system**, vous devez donc supprimer toutes les commandes sauf une avant de coller. En fait, vous n'avez besoin *d'aucune* commande **boot system** dans votre configuration, car elle n'est pas lue au démarrage pour déterminer l'image de démarrage. La dernière image de démarrage chargée sera toujours exécutée lors du rechargement. La commande **boot system** exécute une action lorsque vous la saisissez : le système valide et décompresse l'image et la copie dans l'emplacement de démarrage (un emplacement interne sur disk0 géré par FXOS). La nouvelle image sera chargée lorsque vous rechargerez l'ASA.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer et configurer l'ASA 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 7.
3	Pré-configuration	Câbler l'appareil, à la page 10.
4	Pré-configuration	Mettez le pare-feu sous tension
5	Interface de ligne de commande ASA	(Facultatif) Changer l'adresse IP, à la page 12.
6	ASDM	Connectez-vous à l'ASDM, à la page 13.

7	Portail de commerce Cisco (CCW)	Configurer les licences, à la page 14 : Obtenir les licences de fonctionnalités.
8	Smart Software Manager	Configurer les licences, à la page 14 : Générer un jeton de licence pour le châssis.
9	ASDM	Configurer les licences, à la page 14 : Configurer les licences de fonctionnalités.
10	ASDM	Configurer ASA, à la page 18.

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

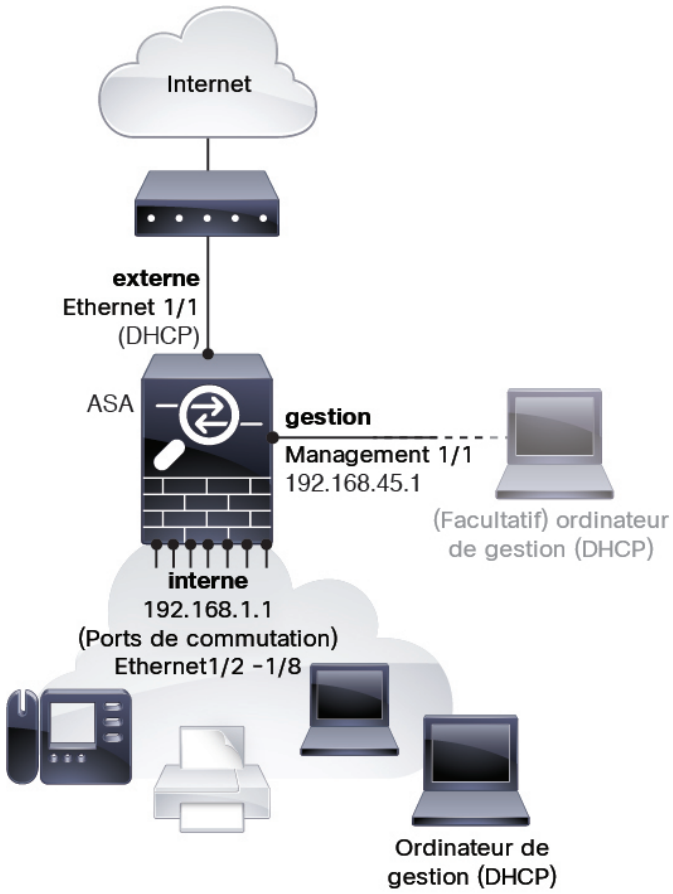
La figure suivante montre le déploiement réseau par défaut pour Firepower 1010, qui fait appel à la configuration par défaut.

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 l'ASA effectue l'ensemble du routage et de la 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 au moyen de l'assistant de démarrage ASDM.

Remarque Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut pour l'accès ASDM, vous pouvez définir l'adresse IP de gestion sur l'interface de ligne de commande ASA. Consultez (Facultatif) Changer l'adresse IP, à la page 12.

Si vous devez modifier l'adresse IP interne, vous pouvez le faire à l'aide de l'assistant de démarrage ASDM. Par exemple, vous devrez peut-être modifier l'adresse IP interne dans les cas suivants :

- Si l'interface externe tente d'obtenir une adresse IP sur le réseau 192.168.1.0, qui est un réseau par défaut commun, le bail DHCP échouera et l'interface externe n'obtiendra pas d'adresse IP. Ce problème se produit parce que l'ASA 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 l'ASA à un réseau interne existant, vous devrez modifier l'adresse IP interne pour qu'elle se trouve sur le réseau existant.



Configuration par défaut de Firepower 1010

La configuration d'usine par défaut du Firepower 1010 concerne les éléments suivants :

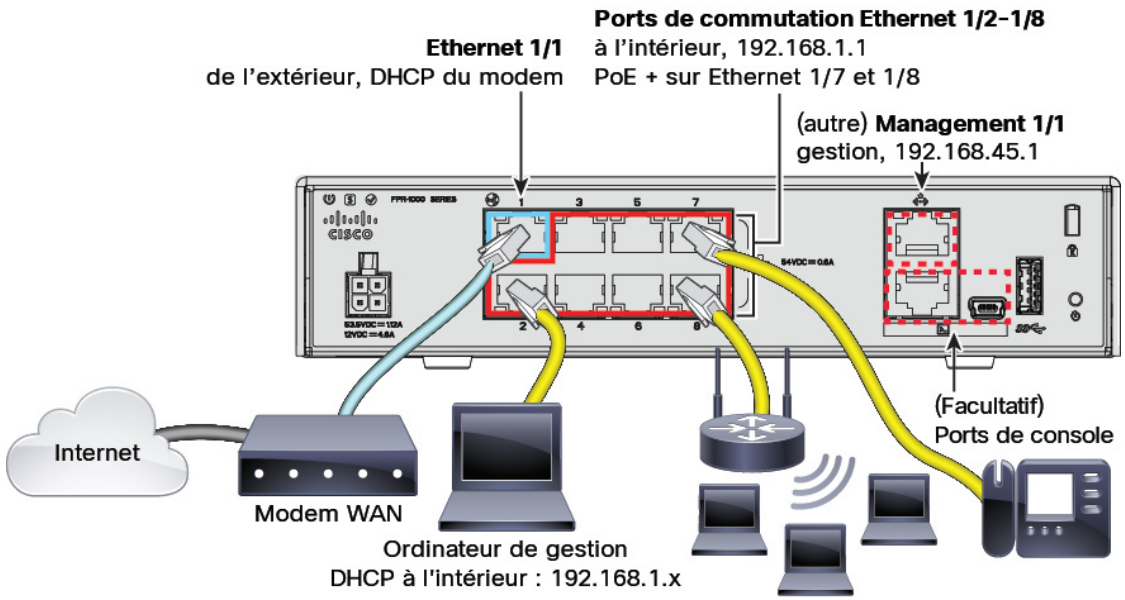
- **Commutateur matériel** : Ethernet 1/2 à 1/8 appartient à VLAN 1
- **inside→outside (flux de trafic)** : Ethernet 1/1 (externe), VLAN1 (interne)
- **management** (gestion) : Management 1/1 (gestion), adresse IP 192.168.45.1
- **adresse IP externe** de DHCP, adresse IP interne — 192.168.1.1
- **serveur DHCP** sur interface interne, interface de gestion
- **Voie de routage par défaut** depuis l'extérieur de DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes de gestion sont limités au réseau 192.168.45.0/24 et les hôtes internes sont limités au réseau 192.168.4.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : Les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
```

```
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Câbler l'appareil



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 (ports de commutation internes). 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'interface interne possède une adresse IP par défaut (192.168.1.1) et 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 internes du réseau (voir Configuration par défaut de Firepower 1010, à la page 8).

- Management 1/1 : Connectez votre ordinateur de gestion directement à l'interface de gestion Management 1/1. Vous pouvez aussi connecter l'interface de la gestion Management 1/1 à votre réseau de gestion; assurez-vous que votre ordinateur de gestion se trouve sur le réseau de gestion, car seuls les clients de ce réseau peuvent accéder à l'ASA. L'interface Management 1/1 a une adresse IP par défaut (192.168.45.1) et exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris l'ordinateur de gestion). Assurez-vous donc que ces paramètres ne sont pas en conflit avec les paramètres du réseau de gestion existants (voir Configuration par défaut de Firepower 1010, à la page 8).

  Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Changer l'adresse IP, à la page 12.

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

Pour l'octroi de licences Smart Software, un accès Internet est nécessaire à l'ASA pour pouvoir accéder à l'autorité de licence.

Étape 4 Connectez les périphériques internes aux autres ports de commutation internes, 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

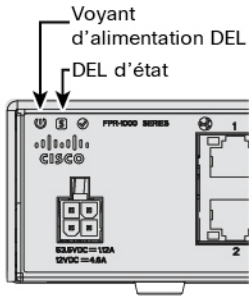
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne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

Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut pour l'accès ASDM, vous pouvez définir l'adresse IP de gestion sur l'interface de gestion au niveau de l'interface de ligne de commande ASA.

Remarque Cette procédure restaure la configuration par défaut et définit également l'adresse IP que vous avez choisie. Par conséquent, si vous apportez des modifications à la configuration ASA que vous souhaitez conserver, n'utilisez pas cette procédure.

Procédure

Étape 1 Connectez-vous au port de console ASA et passez en mode de configuration globale. Consultez Accédez à ASA et Interface de ligne de commande FXOS, à la page 20 pour de plus amples renseignements.

Étape 2 Restaurez la configuration par défaut avec l'adresse IP de votre choix.

configure factory-default [*ip_address* [*mask*]]

Exemple :

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
```

```
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Étape 3 Enregistrez la configuration par défaut dans la mémoire flash.

write memory

Connectez-vous à l'ASDM

Lancez l'ASDM pour pouvoir configurer l'ASA.

Le ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement, de sorte que vous pouvez vous connecter au gestionnaire de logiciels intelligents et utiliser ASDM immédiatement. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur ASA. D'autres fonctions qui nécessitent un cryptage renforcé (comme le VPN) doivent avoir le cryptage renforcé activé, ce qui exige que vous vous inscriviez d'abord au Smart Software Manager.

Remarque Si vous tentez de configurer des fonctions pouvant utiliser un cryptage renforcé avant de vous inscrire - même si vous ne configurez qu'un cryptage faible - votre connexion HTTPS sera interrompue sur cette interface, et vous ne pourrez pas vous reconnecter. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer le ASA, vous connecter à une interface de gestion uniquement, ou vous connecter à une interface non configurée pour une fonction de cryptage renforcé.

Avant de commencer

- Consultez les notes de version d'ASDM sur Cisco.com pour connaître les exigences d'exécution d'ASDM.

Procédure

Étape 1 Entrez l'URL suivante dans votre navigateur.

- **https://192.168.1.1** : Adresse IP d'interface interne .Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutation interne (Ethernet 1/2 à 1/8).
- **https://192.168.45.1** : Adresse IP de l'interface de gestion.

Remarque Assurez-vous de spécifier **https://**, et non **http://** ou simplement l'adresse IP (qui est par défaut HTTP); le ASA ne transmet pas automatiquement une requête HTTP à HTTPS.

La page Web **Cisco ASDM** s'affiche. Il est possible que des avertissements de sécurité s'affichent dans votre navigateur parce que le certificat n'est pas installé sur ASA; vous pouvez ignorer ces avertissements et visiter la page Web en toute sécurité.

Étape 2 Cliquez sur l'une des options suivantes : **Installer le lanceur ASDM** ou **Exécuter ASDM**.

Étape 3 Suivez les instructions à l'écran pour lancer ASDM selon l'option que vous avez choisie.

Le lanceur **Cisco ASDM-IDM** apparaît.

Étape 4 Laissez les champs du nom d'utilisateur et du mot de passe vides , et cliquez **OK**.

La principale fenêtre ASDM s'ouvre.

Configurer les licences

Le ASA utilise les licences intelligentes. Vous pouvez utiliser le système habituel de licences intelligentes, qui nécessite un accès à Internet ; ou pour une gestion hors ligne, vous pouvez configurer la réservation permanente de licences ou Smart Software Manager sur site (anciennement connu sous le nom de serveur satellite). Pour plus d'informations sur ces méthodes d'octroi de licences hors ligne, consultez Cisco ASA Series Feature Licenses; ce guide s'applique aux licences Smart habituelles.

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

Lorsque vous enregistrez le châssis, Smart Software Manager émet un certificat d'ID pour la communication entre le pare-feu et Smart Software Manager. Il assigne également le pare-feu au compte virtuel approprié. jusqu'à ce que vous vous inscriviez à Smart Software Manager, vous ne pourrez pas modifier la configurationaux fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'en sera pas affecté autrement. Voici les fonctionnalités de licences :

- Standard
- Security Plus permet le basculement entre le mode actif/en veille.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.
- AnyConnect : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only.

Le ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement, de sorte que vous pouvez vous connecter au gestionnaire de logiciels intelligents et utiliser ASDM immédiatement. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur ASA. D'autres fonctions qui nécessitent un cryptage renforcé (comme le VPN) doivent avoir le cryptage renforcé activé, ce qui exige que vous vous inscriviez d'abord au Smart Software Manager.

Remarque Si vous tentez de configurer des fonctions pouvant utiliser un cryptage renforcé avant de vous inscrire - même si vous ne configurez qu'un cryptage faible - votre connexion HTTPS sera interrompue sur cette interface, et vous ne pourrez pas vous reconnecter. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer le ASA, vous connecter à une interface de gestion uniquement, ou vous connecter à une interface non configurée pour une fonction de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour le ASA à partir de Smart Software Manager, cochez la case **Allow export-controlled functionality on the products registered with this token (autoriser la fonctionnalité d'exportation contrôlée sur les produits enregistrés avec ce jeton)** afin que la licence complète de cryptage renforcé soit appliquée (votre compte doit être qualifié pour son utilisation). La licence de chiffrement renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement sur le châssis. Dans ce cas-là, aucune action supplémentaire n'est requise. Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

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.

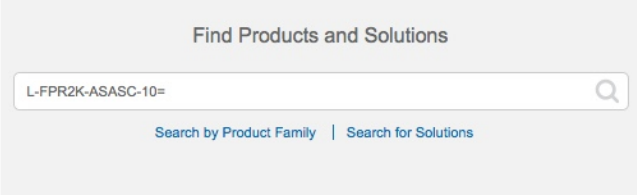
- Votre compte Smart Software Manager doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

Étape 1 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin, y compris au minimum la licence standard.

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

Illustration 1 : Recherche de licences



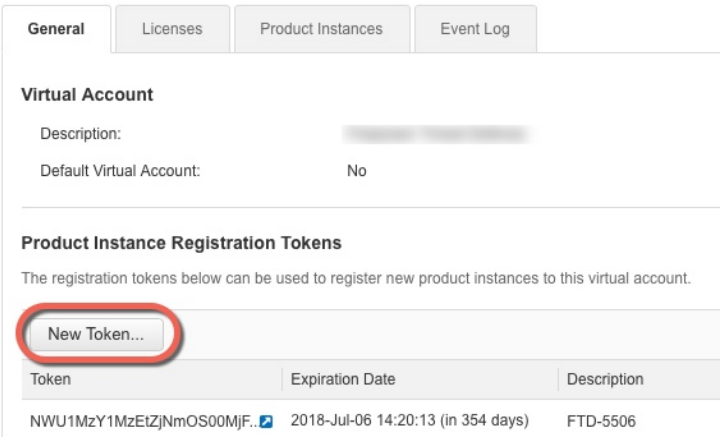
- Licence standard — L-FPR1000-ASA=. La licence standard est gratuite, mais vous devez toujours l'ajouter à votre compte de licences Smart.
- Licence Security Plus — L-FPR1010-SEC-PL=. La licence Security Plus permet le basculement.

- Chiffrement renforcé (3DES/AES) — L-FPR1K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.
- Anyconnect — Voir le Guide de commande Cisco AnyConnect. Vous n'activez pas cette licence directement dans le ASA.

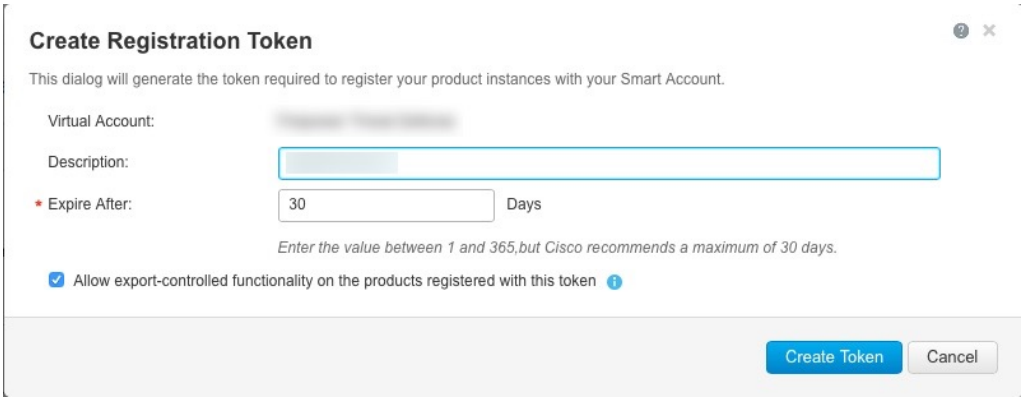
Étape 2 Dans Cisco Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

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.

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 ASA.

Illustration 2 : Afficher le jeton

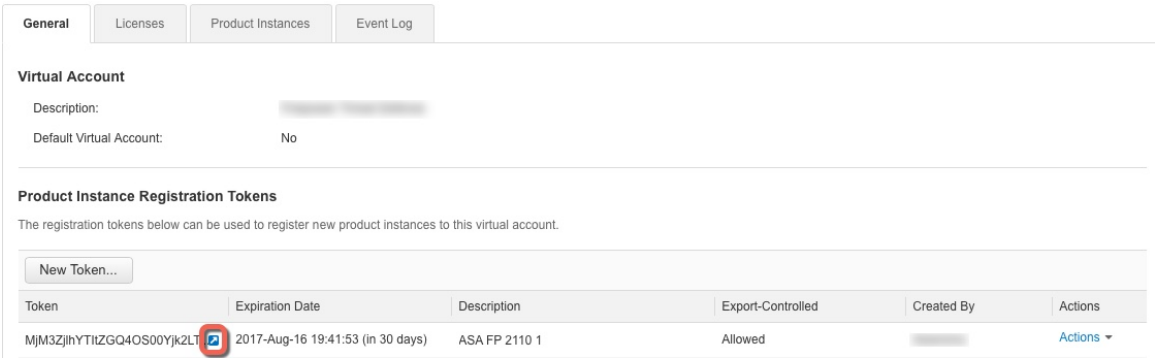
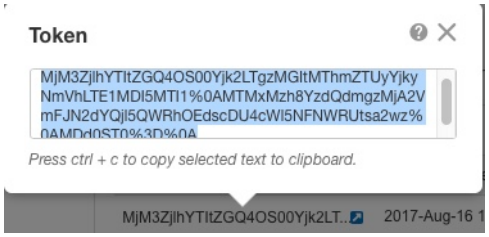


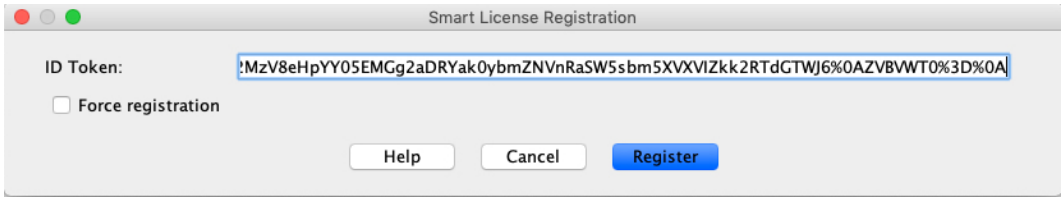
Illustration 3 : Copier le jeton



Étape 3 Dans ASDM, choisissez **Configuration** > **Device Management (gestion d'appareils)** > **Licensing (licences)** > **Smart Licensing (licences Smart)**.

Étape 4 Cliquez sur **Register** (Inscrire).

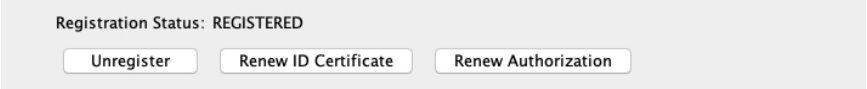
Étape 5 Saisissez le jeton d'enregistrement dans le champ **ID Token** (jeton d'ID).



Vous pouvez éventuellement cocher la case **Force registration (Forcer l'enregistrement)** pour enregistrer le ASA qui est déjà enregistré, mais qui pourrait ne pas être synchronisé avec Cisco Smart Software Manager. Par exemple, utilisez **Force registration (forcer l'enregistrement)** si le ASA a été accidentellement retiré de Cisco Smart Software Manager.

Étape 6 Cliquez sur **Register** (Inscrire).

Le ASA Le s'enregistre auprès de Cisco Smart Software Manager à l'aide de l'interface extérieure préconfigurée, et demande l'autorisation pour les droits de licence configurés. Le Cisco Smart Software Manager applique également la licence de cryptage renforcé (3DES/AES) si votre compte le permet. ASDM actualise la page lorsque l'état de la licence est mis à jour. Vous pouvez également choisir **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Smart License (Licence intelligente)** pour vérifier l'état de la licence, en particulier si l'enregistrement échoue.



Étape 7 Définissez les paramètres suivants :

a) Cochez la case **Enable Smart license configuration** (activer la configuration de licence Smart).

b) Dans la liste déroulante **Feature Tier** (niveaux de fonctionnalités), choisissez **Standard**.

Seul le niveau standard est disponible.

c) (Facultatif) Cochez la case **Enable Security Plus** (activer Security Plus).

Le niveau Security Plus permet le basculement entre le mode actif/en veille.

Étape 8 Cliquez sur **Apply** (appliquer).

Étape 9 Cliquez sur l'icône **Save** (enregistrer) dans la barre d'outils.

Étape 10 Quittez ASDM, puis relancez-le.

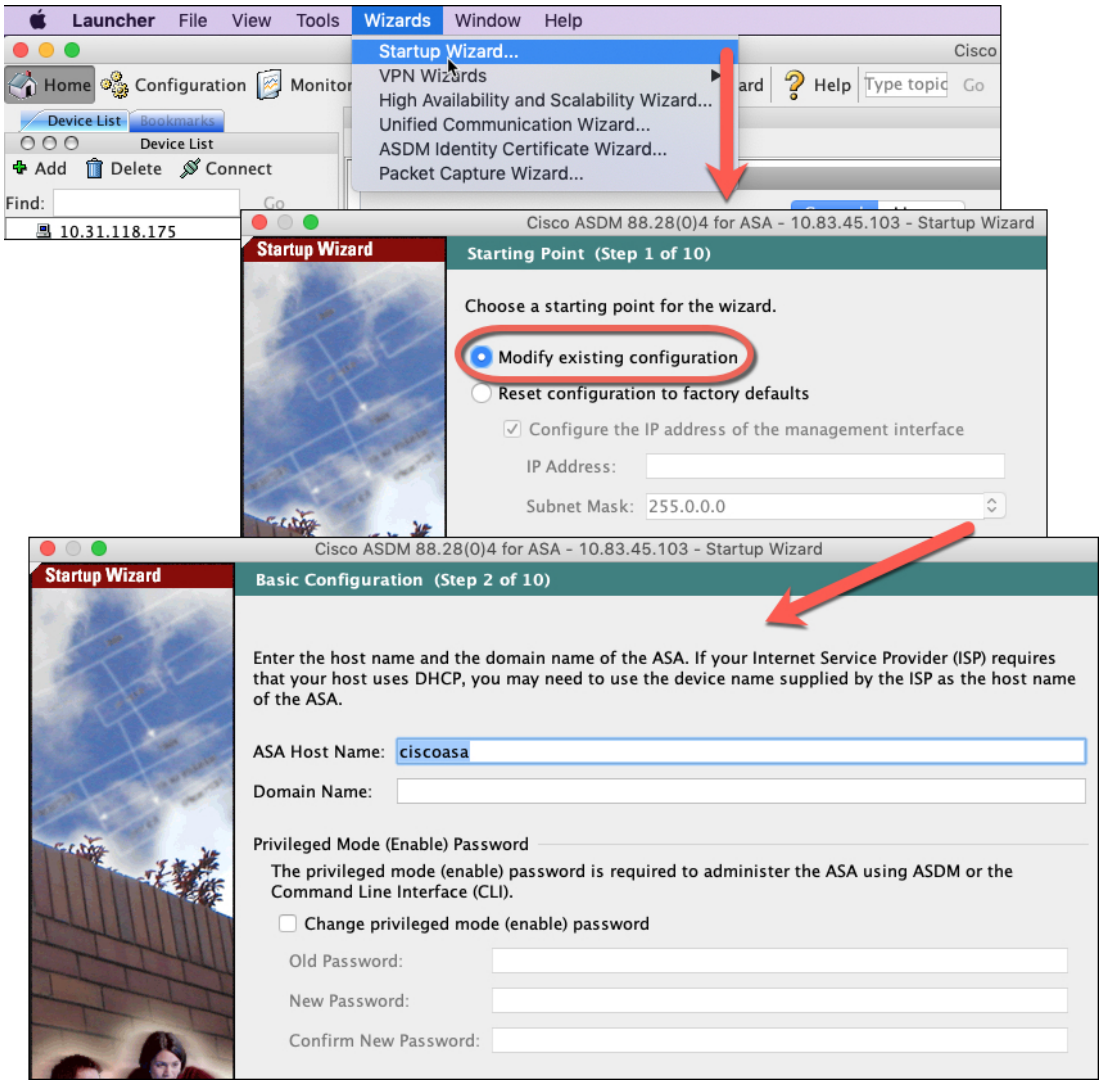
Lorsque vous modifiez les licences, vous devez relancer ASDM pour afficher les écrans mis à jour.

Configurer ASA

Grâce à ASDM, vous pouvez utiliser des assistants pour configurer les fonctionnalités de base et les fonctionnalités avancées. Vous pouvez également configurer manuellement les fonctionnalités non visées par les assistants de configuration.

Procédure

Étape 1 Sélectionnez **Wizards (assistants) > Startup Wizard (assistants de démarrage)**, puis cliquez sur la touche radio **Modify existing configuration** (modifier la configuration existante).



Étape 2 L'assistant de démarrage (**Startup Wizard**) vous guide tout au long de la configuration :

- des interfaces pour activer
- Interfaces, y compris la définition des adresses IP d'interface intérieure et extérieure et l'activation des interfaces.
- du routage statique;
- Le serveur DHCP
- et plus encore...

Étape 3 (Facultatif) Dans le menu **Wizards** (assistants), exécutez d'autres assistants.

Étape 4 Pour continuer à configurer votre ASA, consultez les documents disponibles pour votre version de logiciel à la page d'orientation dans la documentation de la gamme Cisco ASA.

Accédez à ASA et Interface de ligne de commande FXOS

Vous pouvez utiliser le ASA et l'interface de ligne de commande pour résoudre les problèmes ou configurer le ASA au lieu d'utiliser ASDM. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console. Vous pouvez ultérieurement configurer l'accès SSH au ASA sur n'importe quelle interface ; l'accès SSH est désactivé par défaut. Consultez ASA le guide de configuration des opérations générales pour obtenir plus de renseignements.

Vous pouvez également accéder à Interface de ligne de commande FXOSdepuis le ASA et l'interface de ligne de commande à des fins de résolution des problèmes.

Procédure

Étape 1 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 à votre système d'exploitation. (voir le Firepower 1010 guide matériel). Utilisez les paramètres de série suivants :

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

Vous vous connectez à l'interface de ligne de commande d'ASA. Aucun identifiant d'utilisateur n'est requis pour l'accès à la console par défaut.

Étape 2 Accédez au mode d'exécution privilégié.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Le mot de passe d'activation que vous définissez sur l'ASA est également le mot de passe de l'utilisateur **administrateur** FXOS si l'ASA ne parvient pas à démarrer et que vous passez en mode Failsafe (sécurité intégrée)FXOS.

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode d'exécution privilégié, entrez la commande **disable**, **exit**ou **quit**.

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Étape 4 (Facultatif) Connectez-vous au Interface de ligne de commande FXOS.

connect fxos [**admin**]

- **admin** : Fournit un accès au niveau administrateur. Sans cette option, les utilisateurs ont un accès en lecture seule. Notez qu'aucune commande de configuration n'est disponible même en mode admin.

Vous n'êtes pas invité à saisir les informations d'authentification de l'utilisateur. Le nom d'utilisateur actuel de l'ASA est transmis au moyen de FXOS, et aucune connexion supplémentaire n'est requise. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

À l'intérieur de FXOS, vous pouvez visualiser l'activité des utilisateurs en utilisant la commande **scope security/show audit-logs**.

Exemple :

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Quelle est l'étape suivante?

- Pour continuer de configurer votre ASA, reportez-vous aux documents disponibles pour votre version du logiciel dans la navigation de la documentation Cisco de la série ASA.
- Pour le dépannage, consultez le guide de dépannage de FXOS.

Quelle est l'étape suivante?