Pour commencer

Ce chapitre décrit comment démarrer l'utilisation de votre ASA.

Accéder à la console de l'interface de commande en ligne

Pour la configuration initiale, accédez à l'interface de ligne de commande directement à partir du port de console. Plus tard, vous pourrez configurer l'accès à distance à l'aide de Telnet ou SSH conformément à Accès de gestion. Si votre système est déjà en mode de contexte multiple, l'accès au port de console vous place dans l'espace d'exécution du système.

Si vous obtenez des caractères non lisibles lors de la connexion au port de console, vérifiez les paramètres du port. S'ils sont corrects, essayez le câble avec un autre appareil en utilisant les mêmes paramètres. Si le câble est en bon état, vous devrez peut-être remplacer le matériel du port de console. Envisagez également d'essayer un autre ordinateur de travail pour établir la connexion.

Remarque Pour l'accès à la console ASA virtuel, consultez le guide de démarrage rapide ASA virtuel.

Accéder à la console de l'ISA 3000

Procédez comme suit pour accéder à la console de l'appareil.

Procédure

Étape 1 Connectez un ordinateur au port de la console à l'aide du câble de console fourni, puis connectez-vous à la console à l'aide d'un émulateur de terminal pour 9600 bauds, 8 bits de données, aucune parité, 1 bit d'arrêt, aucun contrôle de flux.

Pour plus de renseignements sur le câble de console, consultez le guide sur le matériel pour votre ASA.

Étape 2 Appuyez sur la touche **Entrée** pour afficher l'invite suivante :

```
ciscoasa>
```

Cette invite indique que vous êtes en mode EXEC utilisateur. Le mode EXEC utilisateur donne uniquement accès aux commandes de base.

Étape 3 Accédez au mode d'exécution privilégié.

enable

Vous êtes invité à en changer le mot de passe la première fois que vous entrez la commande **enable**.

Exemple :

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

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 privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 4 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**.

Accéder à la console du mode plateforme de Firepower 2100

Le port de console Firepower 2100 se connecte à l'interface de ligne de commande de Cisco Secure Firewall eXtensible Operating System (interface de ligne de commande de FXOS). À partir de l'interface de ligne de

commande de FXOS, vous pouvez ensuite vous connecter à la console ASA, puis revenir en arrière. Si vous établissez un lien entre SSH et FXOS, vous pouvez également vous connecter à l'interface de ligne de commande d'ASA; une connexion SSH n'est pas une connexion de console, vous pouvez donc avoir plusieurs connexions ASA à partir d'une connexion SSH FXOS. De même, si vous vous connectez à l'ASA, vous pouvez vous connecter à l'interface de ligne de commande de FXOS.

Avant de commencer

Vous ne pouvez avoir qu'une seule connexion de console à la fois. Lorsque vous vous connectez à la console ASA à partir de la console FXOS, cette connexion est une connexion de console persistante, différente d'une connexion Telnet ou SSH.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. Firepower 2100 est livrée avec un câble série DB-9 à RJ-45, vous aurez donc besoin d'un câble série USB tiers pour établir la connexion. Assurez-vous d'installer les pilotes série USB nécessaires à votre système d'exploitation. 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 FXOS. Entrez les informations d'identification de l'utilisateur; par défaut, vous pouvez vous connecter avec l'utilisateur **admin** et le mot de passe par défaut, **Admin123**.

Étape 2 Connectez-vous à l'ASA :

connect asa

Exemple :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Étape 3 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#
```

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 privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 4 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 5 Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

Étape 6 Si vous vous connectez à l'aide du protocole SSH à l'ASA (après avoir configuré l'accès SSH sur l'ASA), connectez-vous à l'interface de ligne de commande de FXOS.

connect fxos

Vous serez invité à vous authentifier pour accéder à FXOS. Utilisez le nom d'utilisateur : **admin** et le mot de passe : **Admin123** par défaut. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

Exemple :

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Accéder à la console Firepower 1000, 2100 en mode appareil et Secure Firewall 3100

Les ports de console Firepower 1000, 2100 en mode appareil et Secure Firewall 3100 vous relient à l'interface de ligne de commande de l'ASA (contrairement à la console Firepower 2100 en mode plateforme, qui vous relie à l'interface de ligne de commande FXOS). À partir de l'interface de ligne de commande d'ASA, vous pouvez ensuite vous connecter à l'interface de ligne de commande FXOS à l'aide de Telnet à des fins de dépannage.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. Assurez-vous d'installer les pilotes série nécessaires à votre système d'exploitation. 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) dans 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#
```

Accéder à la console ASA sur le Châssis Firepower 4100/9300

Pour la configuration initiale, accédez à l'interface de commande en ligne en vous connectant au superviseur Châssis Firepower 4100/9300 (au port de console ou à distance à l'aide de Telnet ou de SSH), puis en vous connectant au module de sécurité ASA.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande (console ou SSH) du superviseur Châssis Firepower 4100/9300 , puis connectez-vous à l'ASA :

connect module *slot* {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

La première fois que vous accédez au module, vous accédez à l'interface de ligne de commande du module FXOS. Vous devez ensuite vous connecter à l'application ASA.

connect asa

Exemple :

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

Étape 2 Accédez au mode d'exécution privilégié, qui est le niveau de privilège le plus élevé.

enable

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

Exemple :

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

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 privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 3 Entrer en mode de configuration globale.

configure terminal

Exemple :

```
asa# configure terminal
asa(config)#
```

Pour quitter le mode de configuration globale, entrez la commande **disable**, **exit** ou **quit**.

Étape 4 Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **Ctrl-a, d**

Vous souhaiterez peut-être utiliser l'interface de ligne de commande du module FXOS à des fins de résolution de problèmes.

Étape 5 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Configurer l'accès ASDM

Cette section décrit comment accéder à ASDM avec une configuration par défaut et comment configurer l'accès si vous n'avez pas de configuration par défaut.

Utiliser la configuration d'usine par défaut pour l'accès ASDM

Avec une configuration d'usine par défaut, la connectivité ASDM est préconfigurée avec les paramètres réseau par défaut.

Procédure

Connectez-vous à ASDM en utilisant les paramètres d'interface et de réseau suivants :

- L'interface de gestion dépend de votre modèle :
  - Firepower 1010 : Management 1/1 (192.168.45.1), ou Ethernet interne 1/2 à 1/8 (192.168.1.1). 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.
  - Firepower 1100, 2100 en mode appareil, Secure Firewall 3100 : Ethernet interne 1/2 (192.168.1.1) ou Management 1/1 (à partir de DHCP). Les hôtes internes sont limités au réseau 192.168.1.0/24. Les hôtes de gestion sont autorisés dans tous les réseaux.
  - Firepower 2100 en mode plateforme : Management 1/1 (192.168.45.1). Les hôtes de gestion sont limités au réseau 192.168.45.0/24.
  - Firepower 4100/9300 : l'interface de type de gestion et l'adresse IP de votre choix définies lors du déploiement. Les hôtes de gestion sont autorisés dans tous les réseaux.
  - ASA virtuel : Management 0/0 (défini pendant le déploiement). Les hôtes de gestion sont limités au réseau de gestion.
  - ISA 3000 : Management 1/1 (192.168.1.1). Les hôtes de gestion sont limités au réseau 192.168.1.0/24.

Remarque
Si vous passez en mode de contexte multiple, vous pouvez accéder à ASDM à partir du contexte d'administration en utilisant les paramètres réseau ci-dessus.

Sujets connexes

Configurations d'usine par défaut, à la page 12
Activer ou désactiver le mode de contexte multiple
Démarrer ASDM, à la page 11

Personnaliser l'accès ASDM

Utilisation cette procédure si *une ou plusieurs* des conditions suivantes s'appliquent :

- Vous n'avez pas de configuration d'usine par défaut
- Vous souhaitez modifier l'adresse IP de gestion
- Vous souhaitez passer en mode de pare-feu transparent
- Vous souhaitez passer en mode de contexte multiple

Pour le mode routé et unique, pour un accès ASDM rapide et facile, nous vous conseillons d'appliquer la configuration d'usine par défaut avec la possibilité de définir votre propre adresse IP de gestion. Utilisez la procédure de cette section uniquement si vous avez des besoins particuliers, tels que la configuration du mode transparent ou de contexte multiple, ou si vous avez une autre configuration que vous devez conserver.

Remarque Pour l'ASAv, vous pouvez configurer le mode transparent lorsque vous le déployez; cette procédure est donc principalement utile après le déploiement si vous devez effacer votre configuration, par exemple.

Procédure

Étape 1 Accédez à l'interface de ligne de commande au niveau du port de console.

Étape 2 (Facultatif) Activez le mode de pare-feu transparent :

Cette commande efface votre configuration.

firewall transparent

Étape 3 Configurez l'interface de gestion :

```
interface interface_id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

Exemple :

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

Le **niveau de sécurité** est un nombre compris entre 1 et 100, où 100 désigne le niveau le plus sécurisé.

Étape 4 (Pour les hôtes de gestion directement connectés) Définissez le pool DHCP pour le réseau de gestion :

```
dhcpd address ip_address-ip_address interface_name
```

dhcpd enable *interface_name*

Exemple :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

Assurez-vous de ne pas inclure l'adresse de l'interface dans la plage.

Étape 5 (Pour les hôtes de gestion à distance) Configurez une route vers les hôtes de gestion :

route *management_ifc management_host_ip mask gateway_ip* **1**

Exemple :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

Étape 6 Activez le serveur HTTP pour ASDM :

http server enable

Étape 7 Autoriser le ou les hôte(s) de gestion à accéder à ASDM :

http *ip_address mask interface_name*

Exemple :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

Étape 8 Enregistrez la configuration :

write memory

Étape 9 (Facultatif) Définissez le mode sur plusieurs modes :

mode multiple

Lorsque vous y êtes invité, confirmez que vous souhaitez convertir la configuration existante pour en faire le contexte d'administration. Vous êtes alors invité à recharger l'ASA.

Exemples

La configuration suivante convertit le mode de pare-feu en mode transparent, configure l'interface de gestion Management 0/0 et active ASDM pour un hôte de gestion :

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
```

```
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

Sujets connexes

Rétablir les valeurs par défaut de la configuration, à la page 13
Définir le mode du pare-feu
Accéder à la console de l'ISA 3000, à la page 1
Démarrer ASDM, à la page 11

Démarrer ASDM

Lancez ASDM à l'aide du lancement ASDM-IDM. Le lanceur est une application téléchargée à partir de l'ASA à l'aide d'un navigateur que vous pouvez utiliser pour vous connecter à n'importe quelle adresse IP ASA. Vous n'avez pas besoin de télécharger à nouveau le lanceur si vous souhaitez vous connecter à d'autres ASA.

Dans ASDM, vous pouvez choisir une autre adresse IP ASA à gérer.

Cette section décrit comment se connecter à ASDM pour la première fois, puis lancer ASDM à l'aide du lanceur.

ASDM stocke les fichiers dans le répertoire \Users\<user_id>\.asdm, y compris le cache, le journal et les préférences, ainsi que dans le répertoire Temp, y compris les profils Secure Client (services client sécurisés).

Procédure

Étape 1 Sur le PC que vous avez spécifié comme client ASDM, saisissez l'URL suivante :

https://*asa_ip_address***/admin**

Remarque
Assurez-vous de préciser **https://** et **http://** ou simplement l'adresse IP (par défaut HTTP); l'ASA ne transfère pas automatiquement une requête HTTP vers HTTPS.

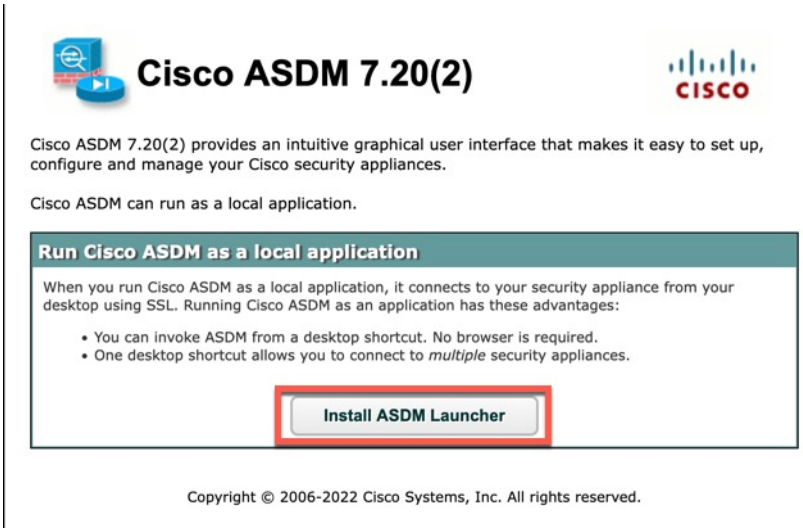
La page de lancement ASDM apparaît avec les boutons suivants :

Installer le lanceur ASDM

Étape 2 Pour télécharger le lanceur et démarrer ASDM :

a) Cliquez sur **Install ASDM Launcher**.

Illustration 1 : Installer le lanceur ASDM



b) Laissez les champs du nom d'utilisateur et du mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**.

   En l'absence d'authentification HTTPS, vous pouvez accéder à ASDM sans nom d'utilisateur et mot de passe **d'activation**, qui est vide par défaut. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité à modifier le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide; voir Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet. **Remarque** : Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé. Même sans authentification, si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.

c) Enregistrez le programme d'installation sur votre ordinateur, puis démarrez le programme d'installation. Le lanceur ASDM-IDM s'ouvre automatiquement une fois l'installation terminée.

d) Saisissez la gestion des adresses IP, le même nom d'utilisateur et mot de passe (vide pour une nouvelle installation), puis cliquez sur **OK**.

Configurations d'usine par défaut

La configuration d'usine par défaut est la configuration appliquée par Cisco aux nouveaux ASA.

- Firepower 1010 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou des ports de commutation internes.
- Firepower 1100 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou de l'interface interne.

- Firepower 2100 —Mode plateforme (par défaut) : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide de Cisco Secure Firewall chassis manager (anciennement Firepower Chassis Manager) et d'ASDM à partir de l'interface de gestion.

  Mode appareil : si vous passez en mode appareil, la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou de l'interface interne.

- Secure Firewall 3100 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion Management 1/1 ou de l'interface interne.

- Châssis Firepower 4100/9300 : lorsque vous déployez l'unité autonome ou une grappe d'ASA, la configuration d'usine par défaut configure une interface pour la gestion afin que vous puissiez vous y connecter à l'aide d'ASDM, avec lequel vous pouvez ensuite terminer votre configuration.

- ASA virtuel : en fonction de votre hyperviseur, dans le cadre du déploiement, la configuration de déploiement (les paramètres de déploiement virtuel initiaux) configure une interface pour la gestion afin que vous puissiez vous y connecter à l'aide d'ASDM, avec lequel vous pouvez ensuite terminer votre configuration. Vous pouvez également configurer des adresses IP de basculement. Vous pouvez également appliquer une configuration « d'usine par défaut » si vous le souhaitez.

- ISA 3000 : la configuration par défaut est une configuration en mode de pare-feu transparent presque complète avec toutes les interfaces internes et externes sur le même réseau; vous pouvez vous connecter à l'interface de gestion avec ASDM pour définir l'adresse IP de votre réseau. Le contournement matériel est activé pour deux paires d'interfaces .

Pour les appareils, la configuration d'usine par défaut est disponible uniquement pour le mode de pare-feu routé et le mode de contexte unique, sauf pour l'ISA 3000, où la configuration d'usine par défaut n'est disponible qu'en mode transparent. Pour l'ASA virtuel et l'Châssis Firepower 4100/9300 , vous pouvez choisir le mode transparent ou routé lors du déploiement.

Remarque En plus des fichiers image et de la configuration (masquée) par défaut, les dossiers et fichiers suivants sont standard dans la mémoire flash : log/, crypto_archive/ et coredumpinfo/coredump.cfg. La date de ces fichiers peut ne pas correspondre à celle des fichiers image dans la mémoire flash. Ces fichiers facilitent le dépannage potentiel; ils n'indiquent pas qu'une défaillance s'est produite.

Rétablir les valeurs par défaut de la configuration

Cette section décrit comment restaurer les valeurs par défaut de la configuration. Pour l'ASA virtuel, cette procédure efface la configuration de déploiement et applique la configuration suivante :

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
```

```
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

Remarque Sur le Firepower 4100/9300, la restauration de la configuration d'usine par défaut efface simplement la configuration; pour restaurer la configuration par défaut, vous devez redéployer l'ASA à partir du superviseur.

Avant de commencer

Cette fonctionnalité est disponible uniquement en mode de pare-feu routé, sauf pour l'ISA 3000, où cette commande est prise en charge uniquement en mode transparent. En outre, cette fonctionnalité est disponible uniquement en mode de contexte unique; un ASA avec une configuration effacée n'a pas de contextes définis à configurer automatiquement à l'aide de cette fonctionnalité.

Procédure

Étape 1 Restaurez les valeurs par défaut de la configuration :

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

Exemple :

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

Remarque
Cette commande ne supprime pas le mode (appareil ou plateforme) actuellement défini pour Firepower 2100.

Si vous spécifiez l'*ip_address*, vous définissez l'adresse IP interne ou de l'interface de gestion, selon votre modèle, au lieu d'utiliser l'adresse IP par défaut. Consultez les directives de modèle suivantes pour savoir quelle interface est définie par l'option *ip_address* :

- Firepower 1010 : définit l'adresse IP de l'interface de **gestion**.
- Firepower 1100 : définit l'adresse IP de l'interface **interne**.
- Firepower 2100 en mode appareil : définit l'adresse IP de l'interface **interne**.
- Firepower 2100 en mode plateforme : définit l'adresse IP de l'interface de **gestion**.
- Secure Firewall 3100 : définit l'adresse IP de l'interface **interne**.
- Firepower 4100/9300 : aucun effet.
- ASA virtuel : définit l'adresse IP de l'interface de **gestion**.
- ISA 3000 : définit l'adresse IP de l'interface de **gestion**.

La commande **http** utilise le sous-réseau que vous spécifiez. De même, la plage de commandes **dhcpd address** se compose de toutes les adresses disponibles supérieures à l'adresse IP que vous spécifiez. Par exemple, si

vous spécifiez 10.5.6.78 avec un filtre d'adresse locale 255.255.255.0, la plage d'adresses DHCP sera 10.5.6.79-10.5.6.254.

Pour Firepower 1000 et Firepower 2100 en mode appareil, et Secure Firewall 3100 : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. Cette modification de configuration n'affecte pas l'image au démarrage : l'image actuellement chargée continue d'être utilisée.

Pour Firepower 2100 en mode plateforme : ce modèle n'utilise pas la commande **boot system**; les paquets sont gérés par FXOS.

Pour tous les autres modèles : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. La commande **boot system** vous permet de démarrer à partir d'une image en particulier. La prochaine fois que vous rechargez l'ASA après avoir restauré la configuration d'usine, il démarre à partir de la première image de la mémoire flash interne; si vous n'avez pas d'image dans la mémoire flash interne, l'ASA ne démarre pas.

Exemple :

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
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
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Étape 2 Enregistrez la configuration par défaut dans la mémoire flash :

write memory

Cette commande enregistre la configuration d'exécution à l'emplacement par défaut pour la configuration de démarrage, même si vous avez précédemment configuré la commande **boot** pour définir un emplacement différent; lorsque la configuration a été effacée, ce chemin a également été effacé.

Restaurer la configuration du déploiement de l'ASA virtuel

Cette section décrit comment restaurer la configuration du déploiement de l'ASA virtuel (Day0).

Procédure

Étape 1 Pour le basculement, mettez hors tension l'unité en veille.

Pour empêcher l'unité en veille de devenir active, vous devez l'éteindre. Si vous la laissez activée, lorsque vous effacez la configuration de l'unité active, l'unité en veille devient active. Lorsque l'ancienne unité active se recharge et se reconnecte via la liaison de basculement, l'ancienne configuration sera synchronisée à partir de la nouvelle unité active, effaçant ainsi la configuration de déploiement souhaitée.

Étape 2 Restaurez la configuration de déploiement après le rechargement. Pour le basculement, saisissez cette commande sur l'unité active :

write erase

Remarque
L'ASA virtuel démarre l'image en cours d'exécution, de sorte que vous n'êtes pas revenu à l'image de démarrage d'origine. Pour utiliser l'image de démarrage d'origine, consultez la commande **boot image**.

N'enregistrez pas la configuration.

Étape 3 Rechargez l'ASA virtuel et chargez la configuration de déploiement :

reload

Étape 4 Pour le basculement, mettez sous tension l'unité en veille.

Après le rechargement de l'unité active, mettez sous tension l'unité en veille. La configuration de déploiement se synchronisera avec l'unité en veille.

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
!
```

Configuration par défaut de Firepower 1100

La configuration d'usine par défaut du Firepower 1100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **gestion**—Management 1/1 (gestion), adresse IP de DHCP
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
```

```
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Configuration par défaut du mode plateforme de Firepower 2100

Vous pouvez configurer Firepower 2100 pour un fonctionnement en mode plateforme; le mode appareil est le mode par défaut.

Remarque Pour les versions antérieures à la version 9.13 (1), le mode plateforme était la seule option par défaut. Si vous effectuez une mise à niveau à partir du mode plateforme, ce mode est maintenu.

Configuration ASA

La configuration d'usine par défaut d'ASA sur Firepower 2100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, adresse IP interne — 192.168.1.1
- **serveur DHCP** sur interface interne
- **Voie de routage par défaut** depuis l'extérieur de DHCP
- **management** (gestion) : Management 1/1 (gestion), adresse IP 192.168.45.1
- Accès **ASDM** : hôtes de gestion.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Initialisation du trafic de **gestion FXOS** : le châssis FXOS peut initier le trafic de gestion sur l'interface externe ASA.
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
```

```
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

Configuration FXOS

La configuration d'usine par défaut de FXOS sur Firepower 2100 concerne les éléments suivants :

- **Interface Management 1/1** : adresse IP 192.168.45.45
- **Passerelle par défaut** : interfaces de données ASA
- **Firewall Chassis Manager et l'accès SSH** : depuis le réseau du gestionnaire uniquement.
- **Nom d'utilisateur par défaut** : le nom d'utilisateur **admin** et le mot de passe par défaut **Admin123**.
- **Serveur DHCP** : plage d'adresses IP de clients 192.168.45.10-192.168.45.12
- **NTP** : Serveurs NTP de Cisco : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
- Serveurs **DNS** , OpenDNS : 208.67.222.222, 208.67.220.220
- **Ethernet 1/1 et Ethernet 1/2** : activés

Configuration par défaut du mode appareil de Firepower 2100

Le Firepower 2100 fonctionne en mode Appliance (appareil) par défaut.

Remarque Pour les versions antérieures à la version 9.13 (1), le mode plateforme était la seule option par défaut. Si vous effectuez une mise à niveau à partir du mode plateforme, le mode plateforme est maintenu.

La configuration d'usine par défaut pour le Firepower 2100 en mode appareil concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **adresse IP de gestion** : depuis DHCP—Management 1/1 (gestion)
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

```
!
```

Configuration par défaut de Secure Firewall 3100

La configuration d'usine par défaut pour Secure Firewall 3100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **gestion**—Management 1/1 (gestion), adresse IP de DHCP
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

```
!
```

Configuration par défaut de Châssis Firepower 4100/9300

Lorsque vous déployez l'ASA sur le Châssis Firepower 4100/9300 , vous pouvez prédéfinir de nombreux paramètres qui vous permettent de vous connecter à l'interface de gestion à l'aide d'ASDM. Une configuration typique comprend les paramètres suivants :

- Interface de gestion :
  - Interface de type de gestion de votre choix définie sur le superviseur Châssis Firepower 4100/9300
  - Nommée « gestion »
  - Adresse IP de votre choix
  - Niveau de sécurité 0
  - Gestion uniquement
- Route par défaut via l'interface de gestion
- Accès ASDM : tous les hôtes autorisés.

La configuration d'une unité autonome comprend les commandes suivantes. Pour une configuration supplémentaire des unités en grappe, consultez Créer une grappe ASA.

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

Configuration par défaut d'ISA 3000

La configuration d'usine par défaut pour ISA 3000 concerne les éléments suivants :

- **Transparent firewall mode** (Mode de pare-feu transparent) : un pare-feu transparent est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.
- **1 Bridge Virtual Interface** (1 interface virtuelle de pont) : toutes les interfaces membres se trouvent dans le même réseau (**adresse IP *non* préconfigurée; vous devez le définir pour qu'il corresponde à votre réseau**) : GigabitEthernet 1/1 (outside1), GigabitEthernet 1/2 (inside1), GigabitEthernet 1/3 (inside2), GigabitEthernet 1/4 (inside2)

- Toutes les interfaces **internes et externes** peuvent communiquer entre elles.
- Interface **Management 1/1** : 192.168.1.1/24 pour l'accès à ASDM.
- **DHCP** pour les clients sur la gestion.
- Accès **ASDM** : hôtes de gestion.
- L'option **Hardware bypass** (Contournement matériel) est activée pour les paires d'interfaces suivantes : GigabitEthernet 1/1 et 1/2; GigabitEthernet 1/3 et 1/4

Remarque Lorsque l'ISA 3000 perd de l'alimentation et passe en mode de contournement matériel, seules les paires d'interfaces ci-dessus peuvent communiquer; inside1 et inside2, et outside1 et outside2 ne peuvent plus communiquer. Toutes les connexions existantes entre ces interfaces seront perdues. Lorsque l'alimentation revient, il y a une brève interruption de la connexion lorsque l'ASA prend en charge les flux.

La configuration comprend les commandes suivantes :

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
```

```
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
```

Configuration du déploiement ASA virtuel

Lorsque vous déployez l'ASA virtuel, vous pouvez prédéfinir de nombreux paramètres qui vous permettent de vous connecter à l'interface de gestion Management 0/0 à l'aide d'ASDM. Une configuration typique comprend les paramètres suivants :

- Mode de pare-feu routé ou transparent
- Interface de gestion Management 0/0 :
  - Nommée « gestion »
  - Adresse IP ou DHCP
  - Niveau de sécurité 0
- Route statique pour l'adresse IP de l'hôte de gestion (s'il ne se trouve pas sur le sous-réseau de gestion)
- Serveur HTTP activé ou désactivé
- Accès HTTP pour l'adresse IP de l'hôte de gestion
- (Facultatif) Adresses IP de liaison de basculement pour GigabitEthernet 0/8 et adresse IP de secours Management 0/0
- Serveur DNS
- Jeton d'ID de licence Smart
- Niveau de débit de la licence Smart et niveau de fonctionnalité Essentials
- (Facultatif) URL et port du mandataire HTTP Smart Call Home
- (Facultatif) Paramètres de gestion SSH :
  - Adresses IP du client
  - Nom d'utilisateur et mot de passe locaux
  - Authentification requise pour SSH à l'aide de la base de données LOCALE
- (Facultatif) API REST activée ou désactivée

Remarque Pour enregistrer avec succès l'ASA virtuel auprès de l'autorité de licence de Cisco, l'ASA virtuel nécessite un accès Internet. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Consultez l'exemple de configuration suivant pour une unité autonome :

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

Remarque La licence Essentials était appelée licence « Standard ».

Consultez l'exemple de configuration suivant pour une unité principale dans une paire de basculement :

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
```

```
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

Régler le Firepower 2100 en mode appareil ou plateforme

Le Firepower 2100 exécute un système d'exploitation sous-jacent appelé le FXOS. Vous pouvez exécuter Firepower 2100 dans les modes suivants :

- Mode appareil (par défaut) : le mode appareil vous permet de configurer tous les paramètres de l'ASA. Seules les commandes de dépannage avancées sont disponibles à partir de l'interface de ligne de commande de FXOS.
- Mode plateforme : lorsque vous êtes en mode plateforme (Platform), vous devez configurer les paramètres de fonctionnement de base et les paramètres de l'interface matérielle dans FXOS. Ces paramètres comprennent l'activation des interfaces, l'établissement de canaux EtherChannels, du protocole NTP, de la gestion des images, etc. Vous pouvez utiliser l'interface web Firewall Chassis Manager ou l'interface de ligne de commande FXOS. Vous pouvez ensuite configurer votre politique de sécurité dans le système d'exploitation ASA en utilisant ASDM ou l'interface de ligne de commande de l'ASA.

Cette procédure vous explique comment changer de mode.

Mise en garde Lorsque vous modifiez le mode, vous devez recharger le système, et la configuration est effacée. La configuration par défaut est appliquée au rechargement. Assurez-vous de conserver une copie de la configuration d'origine pour référence.

Vous observez que les commandes **clear configure all** et **configure factory-default** ne suppriment pas le mode actuel.

Avant de commencer

Vous ne pouvez changer de mode qu'au niveau de l'interface de ligne de commande.

Procédure

Étape 1 (Facultatif) Sauvegardez votre configuration actuelle. Consultez Sauvegarde et restauration de configurations ou d'autres fichiers

Bien qu'il existe de légères différences entre une configuration en mode appareil et une configuration en mode plateforme, une copie de l'ancienne configuration peut constituer un bon point de départ. Par exemple, en mode plateforme, la configuration du protocole NTP, du système DNS et du canal EtherChannel ne fait pas partie de la configuration de l'ASA; elle ne sera donc pas incluse dans votre sauvegarde, mais la plupart des autres paramètres de l'ASA sont valides pour les deux modes.

Étape 2 Affichez le mode actuel.

show fxos mode

Exemple :

```
ciscoasa(config)# show fxos mode
Mode is currently set to appliance
```

Étape 3 Définissez le mode selon le mode plateforme.

no fxos mode appliance

write memory

reload

Après avoir défini le mode, vous devez enregistrer la configuration et recharger le périphérique. Avant le rechargement, vous pouvez rétablir la valeur d'origine du mode sans interruption.

Mise en garde
Lorsque vous rechargez, la configuration est effacée. La configuration par défaut est appliquée au rechargement.

Exemple :

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Étape 4 Définissez le mode selon le mode appareil.

fxos mode appliance

write memory

reload

Après avoir défini le mode, vous devez enregistrer la configuration et recharger le périphérique. Avant le rechargement, vous pouvez rétablir la valeur d'origine du mode sans interruption.

Mise en garde
Lorsque vous rechargez, la configuration est effacée. La configuration par défaut est appliquée au rechargement.

Exemple :

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684
```

```
23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Travailler avec la configuration

Cette section décrit comment utiliser la configuration. Les renseignements de cette section s'appliquent aux contextes de sécurité uniques et multiples, sauf lorsque cela est indiqué.

À propos de la configuration de démarrage et de la configuration en cours d'exécution

Startup Configuration (configuration de démarrage)

Lorsque l'ASA démarre, il charge la configuration à partir d'un fichier texte appelé configuration de démarrage. Ce fichier réside par défaut en tant que fichier masqué dans la mémoire flash interne. Vous pouvez toutefois spécifier un fichier différent pour la configuration de démarrage qui réside dans le système de fichiers visible. Utilisez la commande suivante pour spécifier une nouvelle configuration de démarrage :

boot config {**disk0:/** | **disk1:/**} [*path/*]*filename*

Enregistrez le nouvel emplacement :

write memory

Par exemple :

```
ciscoasa (config)# boot config disk0:/startup.cfg
ciscoasa (config)# write memory
```

Utilisation de configurations volumineuses

L'espace disponible dans le répertoire de démarrage masqué est limité. Si votre configuration est très volumineuse (par exemple, plus de 16 Mo), vous ne pourrez pas enregistrer la configuration de démarrage. Dans ce cas, vous devez utiliser la commande **boot config** pour enregistrer la configuration de démarrage dans le système de fichiers visible. Par exemple, si vous chargez une configuration volumineuse dans la mémoire en cours d'exécution et que vous essayez de l'enregistrer, le message d'erreur suivant peut s'afficher si vous saisissez **write memory** et que la configuration est trop volumineuse :

```
%Erreur d'écriture. nvRAM:/startup-config (pas d'espace gauche sur le périphérique :)
```

Dans ce cas, assurez-vous de réenregistrer la configuration en cours d'exécution dans un nouvel emplacement de fichier avant de recharger l'ASA. Sinon, l'ASA risque de ne pas charger la configuration complète.

Running Configuration (configuration en cours d'exécution)

Lorsque vous saisissez une commande, la modification n'est appliquée qu'à la configuration en cours d'exécution dans la mémoire. Vous devez enregistrer manuellement la configuration en cours d'exécution dans la configuration de démarrage pour que vos modifications soient conservées après un rechargement.

Enregistrer les modifications de configuration

Cette section décrit comment enregistrer votre configuration.

Enregistrer les modifications de configuration en mode de contexte unique

Pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage, procédez comme suit.

Procédure

Enregistrez la configuration en cours d'exécution dans la configuration de démarrage :

write memory

Remarque
La commande **copy running-config startup-config** est équivalente à la commande **write memory**.

Enregistrer les modifications de configuration en mode de contexte multiple

Vous pouvez enregistrer chaque configuration de contexte (et de système) séparément, ou vous pouvez enregistrer toutes les configurations de contexte en même temps.

Enregistrer chaque contexte et système séparément

Utilisez la procédure suivante pour enregistrer la configuration système ou du contexte.

Procédure

À partir du contexte ou du système, enregistrez la configuration en cours d'exécution dans la configuration de démarrage :

write memory

Pour le mode de contexte multiple, les configurations de démarrage de contexte peuvent résider sur des serveurs externes. Dans ce cas, l'ASA enregistre la configuration sur le serveur que vous avez identifié dans l'URL de contexte, sauf pour une URL HTTP ou HTTPS, qui ne vous permet pas d'enregistrer la configuration sur le serveur.

Remarque
La commande **copy running-config startup-config** est équivalente à la commande **write memory**.

Enregistrer toutes les configurations de contexte en même temps

Utilisez la procédure suivante pour enregistrer simultanément toutes les configurations de contexte ainsi que la configuration système.

Procédure

À partir de l'espace d'exécution du système, enregistrez la configuration en cours d'exécution dans la configuration de démarrage pour tous les contextes et la configuration système :

write memory all [**/noconfirm**]

Si vous ne saisissez pas le mot clé **/noconfirm**, l'invite suivante s'affiche :

```
Are you sure [Y/N]:
```

Après avoir saisi **Y**, l'ASA enregistre la configuration système et chaque contexte. Les configurations de démarrage de contexte peuvent résider sur des serveurs externes. Dans ce cas, l'ASA enregistre la configuration sur le serveur que vous avez identifié dans l'URL de contexte, sauf pour une URL HTTP ou HTTPS, qui ne vous permet pas d'enregistrer la configuration sur le serveur.

Après que l'ASA a enregistré chaque contexte, le message suivant s'affiche :

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Parfois, un contexte n'est pas enregistré en raison d'une erreur. Consultez les renseignements suivants pour les erreurs :

- Pour les contextes qui ne sont pas enregistrés en raison d'une mémoire faible, le message suivant s'affiche :

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- Pour les contextes qui ne sont pas enregistrés, car la destination à distance est inaccessible, le message suivant s'affiche :

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- Pour les contextes qui ne sont pas enregistrés, car le contexte est verrouillé, le message suivant s'affiche :

  ```
  Unable to save the configuration for the following contexts as these contexts are locked.
  context 'a' , context 'x' , context 'z' .
  ```

  Un contexte n'est verrouillé que si un autre utilisateur enregistre déjà la configuration ou est en train de supprimer le contexte.

- Pour les contextes qui ne sont pas enregistrés, car la configuration de démarrage est en lecture seule (par exemple, sur un serveur HTTP), le rapport de messages suivant est imprimé à la fin de tous les autres messages :

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context 'a' , context 'b' , context 'c' .
  ```

- Pour les contextes qui ne sont pas enregistrés en raison de mauvais secteurs dans la mémoire flash, le message suivant s'affiche :

```
The context 'context a' could not be saved due to Unknown errors
```

Copier la configuration de démarrage dans la configuration en cours d'exécution

Utilisez l'une des commandes suivantes pour copier une nouvelle configuration de démarrage dans la configuration en cours d'exécution :

- **copy startup-config running-config**

  Fusionne la configuration de démarrage avec la configuration en cours d'exécution. Une fusion ajoute toutes les nouvelles commandes de la nouvelle configuration à la configuration en cours d'exécution. Si les configurations sont identiques, aucune modification ne se produit. Si des commandes sont en conflit ou si des commandes influent sur le fonctionnement du contexte, l'effet de la fusion dépend de la commande. Vous pourriez obtenir des erreurs ou des résultats inattendus.

- **reload**

  Recharge l'ASA, qui charge la configuration de démarrage et supprime la configuration en cours d'exécution.

- **clear configure all** and then **copy startup-config running-config**

  Charge la configuration de démarrage et supprime la configuration en cours d'exécution sans nécessiter un rechargement.

Afficher la configuration

Les commandes suivantes vous permettent d'afficher les configurations en cours d'exécution et de démarrage :

- **show running-config**

  Affiche la configuration en cours d'exécution.

- **show running-config** *command*

  Affiche la configuration en cours d'exécution d'une commande spécifique.

- **show startup-config**

  Affiche la configuration de démarrage.

Effacer et supprimer les paramètres de configuration

Pour effacer les paramètres, entrez l'une des commandes suivantes :

- **clear configure** *configurationcommand* [*level2configurationcommand*]

Efface toute la configuration pour une commande spécifiée. Si vous ne souhaitez effacer la configuration que pour une version spécifique de la commande, vous pouvez saisir une valeur pour *level2configurationcommand*.

Par exemple, pour effacer la configuration de toutes les commandes **aaa**, saisissez la commande suivante :

```
ciscoasa(config)# clear configure aaa
```

Pour effacer la configuration uniquement des commandes **aaa authentication**, saisissez la commande suivante :

```
ciscoasa(config)# clear configure aaa authentication
```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

  Désactive les paramètres ou les options spécifiques d'une commande. Dans ce cas, vous utilisez la commande **no** pour supprimer la configuration spécifique identifiée par *qualifier*.

  Par exemple, pour supprimer une commande **access-list** spécifique, saisissez suffisamment de commandes pour l'identifier de façon unique; vous devrez peut-être saisir la commande complète :

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group obj_icmp_1
```

- **write erase**

  Efface la configuration de démarrage.

Remarque Pour l'ASA virtuel, cette commande restaure la configuration de déploiement après un rechargement. Pour effacer complètement la configuration, utilisez la commande **clear configure all**.

- **clear configure all**

  Efface la configuration d'exécution.

Remarque En mode de contexte multiple, si vous entrez **clear configure all**, vous supprimez également tous les contextes et empêchez leur exécution. Les fichiers de configuration de contexte ne sont pas effacés et restent dans leur emplacement d'origine.

Remarque Pour Firepower 1000 et Firepower 2100 en mode appareil, et Secure Firewall 3100 : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. Cette modification de configuration n'affecte pas l'image au démarrage : l'image actuellement chargée continue d'être utilisée.

Pour Firepower 2100 en mode plateforme : ce modèle n'utilise pas la commande **boot system**; les paquets sont gérés par FXOS.

Pour tous les autres modèles : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. La commande **boot system** vous permet de démarrer à partir d'une image spécifique, y compris une image sur la carte de mémoire flash externe. La prochaine fois que vous rechargez l'ASA, il démarre à partir de la première image de la mémoire flash interne; si vous n'avez pas d'image dans la mémoire flash interne, l'ASA ne démarre pas.

Remarque Cette commande ne supprime pas le mode (appareil ou plateforme) actuellement défini pour Firepower 2100.

Créer des fichiers de configuration texte hors ligne

Ce guide décrit comment utiliser l'interface de ligne de commande pour configurer l'ASA; lorsque vous enregistrez des commandes, les modifications sont écrites dans un fichier texte. Au lieu d'utiliser l'interface de ligne de commande, vous pouvez modifier un fichier texte directement sur votre ordinateur et coller une configuration à l'invite de ligne de commande du mode de configuration dans son intégralité ou ligne par ligne. Vous pouvez également télécharger un fichier texte dans la mémoire flash interne de l'ASA. Consultez Logiciels et configurations pour en savoir plus sur le téléchargement du fichier de configuration sur l'ASA.

Dans la plupart des cas, les commandes décrites dans ce guide sont précédées d'une invite d'interface de ligne de commande. L'invite dans l'exemple suivant est « ciscoasa(config)# » :

```
ciscoasa(config)# context a
```

Dans le fichier de configuration texte, vous n'êtes pas invité à saisir des commandes, l'invite est donc omise comme suit :

```
context a
```

Pour en savoir plus sur le formatage du fichier, consultez Utilisation de l'interface de commande en ligne.

Appliquer les modifications de configuration aux connexions

Lorsque vous apportez des modifications à la configuration de la politique de sécurité, toutes les *nouvelles* connexions utilisent la nouvelle politique de sécurité. Les connexions existantes continuent d'utiliser la

politique qui était configurée au moment de l'établissement de la connexion. La sortie de la commande **show** pour les anciennes connexions reflète l'ancienne configuration et, dans certains cas, n'inclura pas de données sur les anciennes connexions.

Par exemple, si vous supprimez une **politique de service** QoS d'une interface, puis ajoutez une version modifiée, la commande **show service-policy** affiche uniquement les compteurs QoS associés aux nouvelles connexions qui correspondent à la nouvelle politique de service; les connexions existantes sur l'ancienne politique ne s'affichent plus dans la sortie de la commande.

Pour vous assurer que toutes les connexions utilisent la nouvelle politique, vous devez déconnecter les connexions actuelles afin qu'elles puissent se reconnecter à l'aide de la nouvelle politique.

Pour déconnecter les connexions, saisissez la commande suivante :

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*]] [**port** *src_port* [*-src_port*]] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [*-dest_port*]]

  Cette commande met fin aux connexions, quel que soit leur état. Reportez-vous à la commande **show conn** pour afficher toutes les connexions actuelles.

  Sans arguments, cette commande efface toutes les connexions de transit. Pour effacer également les connexions vers la boîte (y compris votre session de gestion actuelle), utilisez le mot clé **all**. Pour effacer des connexions spécifiques en fonction de l'adresse IP source, de l'adresse IP de destination, du port et/ou du protocole, vous pouvez spécifier les options souhaitées.

Recharger l'ASA

Pour recharger l'ASA, suivez la procédure ci-dessous.

La commande **reload** n'est pas répliquée sur les nœuds de données pour la mise en grappe ou sur l'unité de secours/secondaire pour le basculement.

En mode de contexte multiple, vous pouvez seulement recharger à partir de l'espace d'exécution du système.

Procédure

Rechargez l'ASA.

reload

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.