

Pour commencer

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

- Accéder à la console de l'interface de commande en ligne, à la page 1
- Activer le mode FIPS, à la page 8
- Configurer l'accès ASDM, à la page 9
- Démarrer ASDM, à la page 12
- Personnaliser le fonctionnement ASDM, à la page 14
- Configurations d'usine par défaut, à la page 16
- Régler le Firepower 2100 en mode appareil ou plateforme, à la page 31
- Commencer avec la configuration, à la page 33
- Utiliser l'outil d'interface de ligne de commande dans ASDM, à la page 34
- Appliquer les modifications de configuration aux connexions, à la page 35

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

Dans certains cas, vous devrez peut-être utiliser l'interface de ligne de commande pour configurer les paramètres de base pour l'accès à ASDM.

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 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#
```

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

Le port de console des Firepower 1000, 2100 en mode appareil et Secure Firewall 3100 vous relie 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 à l'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 de l'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-], .**

Activer le mode FIPS

La norme FIPS, ou Federal Information Processing Standard, est une norme de certification des États-Unis et du Canada. Elle définit les exigences que les modules cryptographiques doivent respecter. Certaines versions d'ASA sont conformes à la norme FIPS 140-3, conformément aux normes du National Institute of Standards (NIST) des États-Unis.

En plus d'activer FIPS sur l'ASA, vous devez également configurer des algorithmes de chiffrement conformes à FIPS.

Vous ne pouvez pas activer FIPS pour la mise en grappe.

Avant de commencer

- Le mode FIPS est uniquement pris en charge sur les versions qui ont fait l'objet de la conformité FIPS. Vous devez désactiver le mode FIPS avant d'effectuer la mise à niveau vers une version de conformité non FIPS.

  Pour savoir quelles versions sont conformes à la norme FIPS et pour afficher leurs certifications, consultez https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html?flt0_general-table0=asa.

- Pour le basculement, les deux unités doivent être en mode FIPS.

Procédure

Étape 1 Activez FIPS sur l'ASA.

fips enable

Exemple :

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot the
 device
```

Lorsque FIPS est activé, FIPS POST s'exécute et imprime le message de console suivant au démarrage :

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9
```

```
INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
ciscoasa>
```

Étape 2 Enregistrez la configuration et rechargez.

write memory

reload

Étape 3 (Facultatif) Exécutez les autotests de mise sous tension.

fips self-test poweron

Les tests comprennent le test d'algorithme cryptographique, le test d'intégrité logicielle et le test des fonctions critiques.

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 16
Activer ou désactiver le mode de contexte multiple
Démarrer ASDM, à la page 12

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 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 17
Définir le mode du pare-feu (mode unique)
Accéder à la console de l'ISA 3000, à la page 1
Démarrer ASDM, à la page 12

Démarrer ASDM

Lancez ASDM à l'aide du lanceur ASDM. 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 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**.

Personnaliser le fonctionnement ASDM

Vous pouvez installer un certificat d'identité pour lancer ASDM avec succès et augmenter la mémoire du paquet ASDM afin qu'il puisse gérer des configurations plus importantes.

Installer un certificat d'identité pour ASDM

Lorsque vous utilisez la mise à jour 51 de Java 7 et les versions ultérieures, le lanceur ASDM nécessite un certificat de confiance. Une méthode simple pour répondre aux exigences en matière de certificats consiste à installer un certificat d'identité autosigné.

Consultez le document suivant pour installer un certificat d'identité autosigné sur l'ASA afin de l'utiliser avec ASDM, et pour enregistrer le certificat avec Java.

http://www.cisco.com/go/asdm-certificate

Augmenter la mémoire de configuration de l'ASDM

ASDM prend en charge une taille de configuration maximale de 512 Ko. Si vous dépassez cette quantité, vous risquez de rencontrer des problèmes de performance. Par exemple, lorsque vous chargez la configuration, la boîte de dialogue d'état indique le pourcentage de la configuration qui est terminée, mais avec des configurations importantes, elle cesse de s'augmenter et semble suspendre l'opération, même si ASDM est toujours en train de traiter la configuration. Si cette situation se produit, nous vous recommandons d'augmenter la mémoire vive du système ASDM. Pour confirmer que vous subissez un épuisement de la mémoire, supervisez la console Java pour détecter le message « java.lang.OutOfMemoryError ».

En outre, nous vous conseillons de réduire la taille de votre configuration si possible, par exemple en supprimant les objets inutilisés.

Augmenter la mémoire de configuration de l'ASDM sous Windows

Pour augmenter la taille de la mémoire du tas ASDM, modifiez le fichier **run.bat** en suivant la procédure suivante.

Procédure

Étape 1 Aller dans le répertoire d'installation d'ASDM, par exemple C :\NProgram Files (x86)\NCisco Systems\NASDM.

Étape 2 Modifiez le fichier **run.bat** à l'aide d'un éditeur de texte.

Étape 3 Dans la ligne qui commence par « start javaw.exe », modifiez l'argument préfixé par « -Xmx » pour préciser la taille du tas souhaitée. Par exemple, remplacez-la par -Xmx768M pour 768 Mo ou -Xmx1G pour 1 Go.

Pour les configurations très volumineuses, vous devrez peut-être spécifier une taille de pile allant jusqu'à 2 Go.

Étape 4 Enregistrez le fichier **run.bat** .

Augmenter la mémoire de configuration de l'ASDM sous Mac OS

Pour augmenter la taille de la mémoire du tas ASDM, modifiez le fichier **Info.plist** en suivant la procédure suivante.

Procédure

Étape 1 Cliquez avec le bouton droit de la souris sur l'icône **Cisco ASDM-IDM** et choisissez **Show Package Contents** (afficher le contenu du paquet).

Étape 2 Dans le dossier **Contents** (contenus), double-cliquez sur le fichier **Info.plist**. Si les outils de développeur sont installés, ils s'ouvrent dans le **Property List Editor** (Éditeur de liste de propriétés). Sinon, ils s'ouvrent dans **TextEdit**.

Étape 3 Sous **Java** > **VMOptions**, modifiez la chaîne préfixée par « -Xmx » pour préciser la taille du tas souhaitée. Par exemple, remplacez-la par -Xmx768M pour 768 Mo ou -Xmx1G pour 1 Go.

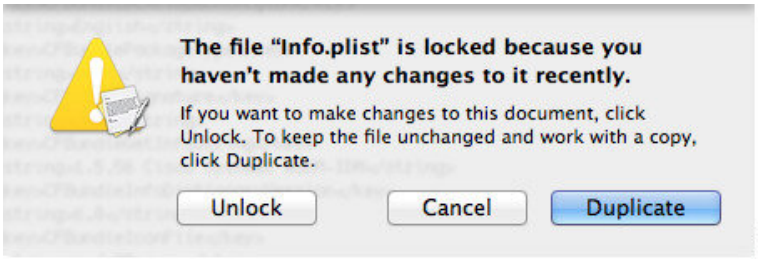
```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>


  <key>CFBundleDocumentTypes</key>
    <array>
```

Pour les configurations très volumineuses, vous devrez peut-être spécifier une taille de pile allant jusqu'à 2 Go.

Étape 4 Si ce fichier est verrouillé, une erreur telle que la suivante s'affiche :



Étape 5 Cliquez sur **Unlock** (déverrouiller) et enregistrez le fichier.

Si vous ne voyez pas la boîte de dialogue **Unlock** (déverrouiller), quittez l'éditeur, cliquez avec le bouton droit de la souris sur l'icône **Cisco ASDM-IDM**, choisissez **Copy Cisco ASDM-IDM** (copier Cisco ASDM-IDM), et collez-le à un endroit où vous avez des droits d'écriture, comme le bureau. Modifiez ensuite la taille du tas à partir de cette copie.

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 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 leChâssis 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. Les procédures de l'interface de ligne de commande et ASDM sont fournies. 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, 6100 : cette commande efface la **boot system**commande, 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.

Étape 3 (Procédure ASDM.) Dans la fenêtre d'application principale d'ASDM, procédez comme suit :

a) Choisissez **File (Fichier)** > **Reset Device to the Factory Default Configuration (Réinitialiser le périphérique à la configuration d'usine par défaut)**.

La boîte de dialogue **Reset Device to the Default Configuration (Réinitialiser le périphérique à la configuration par défaut)** apparaît.

b) (Facultatif) Renseignez le champ **Management IP address** (Adresse IP de gestion) de l'interface de gestion ou interne, au lieu d'utiliser l'adresse par défaut.

Consultez l'étape précédente relative à l'interface de ligne de commande pour en savoir plus sur l'adresse IP d'interface définie par modèle.

c) (Facultatif) Choisissez le **Management Subnet Mask** (Filtre d'adresse locale de gestion) dans la liste déroulante.

d) Cliquez sur **OK**.

Une boîte de dialogue de confirmation s'affiche.

Remarque Pour Firepower 1000 et Firepower 2100 en mode appareil, et Secure Firewall 3100 : cette commande efface l'emplacement de l'image de démarrage, 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 l'emplacement de l'image de démarrage; les paquets sont gérés par FXOS.

Pour tous les autres modèles : cette action efface également l'emplacement de l'image de démarrage, si elle est présente, ainsi que le reste de la configuration. Le volet **Configuration > Device Management (Gestion des périphériques) > System Image/Configuration (Configuration système/image) > Boot Image/Configuration (Image de démarrage/Configuration)** vous permet de démarrer à partir d'une image en particulier, y compris une image sur la mémoire externe. 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.

e) Cliquez sur **Oui**.

f) Après avoir restauré la configuration par défaut, enregistrez cette configuration dans la mémoire flash interne. Choisissez **File (Fichier)** > **Save Running Configuration to Flash (Enregistrer la configuration en cours d'exécution dans la mémoire flash)**.

Le choix de cette option enregistre la configuration d'exécution à l'emplacement par défaut pour la configuration de démarrage, même si vous avez déjà configuré 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]
```

Commencer avec la configuration

Pour configurer et superviser l'ASA, procédez comme suit.

Remarque ASDM prend en charge une configuration maximale de 512 Ko. Si vous dépassez cette limite, vous risquez de rencontrer des problèmes de performances. Consultez Augmenter la mémoire de configuration de l'ASDM, à la page 14.

Procédure

Étape 1 Pour la configuration initiale à l'aide de l'assistant de démarrage, choisissez **Wizards (Assistants)** > **Startup Wizard (Assistant de démarrage)**.

Étape 2 Pour utiliser l'assistant VPN IPsec pour configurer les connexions VPN IPsec, sélectionnez **Wizards (Assistants)** > **IPsec VPN Wizard (Assistant VPN IPsec)** et complétez chaque écran qui s'affiche.

Étape 3 Si vous souhaitez utiliser l'assistant SSL VPN pour configurer les connexions SSL VPN, sélectionnez **Wizards (Assistants)** > **SSL VPN Wizard (Assistant SSL VPN)** et complétez chaque écran qui s'affiche.

Étape 4 Pour configurer les paramètres de haute disponibilité et d'évolutivité, choisissez **Wizards (Assistants)** > **High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité)**.

Étape 5 Si vous souhaitez utiliser l'assistant de capture de paquets pour configurer la capture de paquets, sélectionnez **Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)**.

Étape 6 Pour afficher les différentes couleurs et les différents styles disponibles dans l'interface graphique utilisateur d'ASDM, choisissez **View (Afficher)** > **Office Look and Feel (Aspect et convivialité du bureau)**.

Étape 7 Pour configurer les fonctionnalités, cliquez sur le bouton **Configuration** dans la barre d'outils, puis cliquez sur l'un des boutons de fonctionnalité pour afficher le volet de configuration associé.

Remarque Si le champ Configuration est vide, cliquez sur **Refresh** (Actualiser) dans la barre d'outils pour afficher le contenu de l'écran.

Étape 8 Pour superviser l'ASA, cliquez sur le bouton **Monitoring** (Supervision) dans la barre d'outils, puis cliquez sur un bouton de fonctionnalité pour afficher le volet de supervision associé.

Utiliser l'outil d'interface de ligne de commande dans ASDM

Cette section explique comment saisir des commandes à l'aide d'ASDM et comment utiliser l'interface de ligne de commande.

Utiliser l'outil d'interface de ligne de commande

Cette fonctionnalité fournit un outil texte pour envoyer des commandes à l'ASA et afficher les résultats.

Les commandes que vous pouvez saisir avec l'outil d'interface de ligne de commande dépendent de vos privilèges d'utilisateur. Passez en revue votre niveau de privilège dans la barre d'état au bas de la fenêtre d'application principale d'ASDM pour vous assurer que vous disposez des privilèges requis pour exécuter les commandes d'interface de ligne de commande de niveau privilégié.

Avant de commencer

- Les commandes saisies dans l'outil d'interface de ligne de commande d'ASDM peuvent fonctionner différemment de celles saisies par le biais d'une connexion de terminal à l'ASA.
- Erreurs de commande : si une erreur se produit parce que vous avez saisi une commande incorrecte, la commande incorrecte est ignorée et les commandes restantes sont traitées. Un message s'affiche dans la zone Response (Réponse) pour vous informer si une erreur s'est produite ou non, ainsi que d'autres renseignements connexes.
- Commandes interactives : les commandes interactives ne sont pas prises en charge dans l'outil d'interface de ligne de commande. Pour utiliser ces commandes dans ASDM, utilisez le mot clé **noconfirm** s'il est disponible, comme indiqué dans la commande suivante :

  ```
  crypto key generate rsa modulus 1024 noconfirm
  ```

- Évitez les conflits avec d'autres administrateurs : plusieurs utilisateurs administratifs peuvent mettre à jour la configuration en cours d'exécution de l'ASA. Avant d'utiliser l'outil d'interface de ligne de commande d'ASDM pour apporter des modifications à la configuration, vérifiez qu'il y a d'autres sessions administratives actives. Si plusieurs utilisateurs configurent l'ASA en même temps, les modifications les plus récentes prennent effet.

  Pour afficher d'autres sessions administratives qui sont actuellement actives sur le même ASA, choisissez **Monitoring (Supervision) > Propriétés (Propriétés) > Device Access (Accès au périphérique)**.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue **Command Line Interface** (Interface de ligne de commande) apparaît.

Étape 2 Choisissez le type de commande (ligne unique ou plusieurs lignes) que vous souhaitez, puis choisissez la commande dans la liste déroulante ou saisissez-la dans le champ fourni.

Étape 3 Cliquez sur **Send** (Envoyer) pour exécuter la commande.

Étape 4 Pour saisir une nouvelle commande, cliquez sur **Clear Response** (Effacer la réponse), puis choisissez (ou saisissez) une autre commande à exécuter.

Étape 5 Cochez la case **Enable context-sensitive help (?)** (Activer l'aide contextuelle (?)) pour fournir une aide contextuelle pour cette fonctionnalité. Décochez cette case pour désactiver l'aide contextuelle.

Étape 6 Après avoir fermé la boîte de dialogue **Command Line Interface** (Interface de ligne de commande), si vous avez modifié la configuration, cliquez sur **Refresh** (Actualiser) pour afficher les modifications dans ASDM.

Afficher les commandes ignorées par ASDM sur l'appareil

Cette fonctionnalité vous permet d'afficher la liste des commandes non prises en charge par ASDM. En règle générale, ASDM les ignore. ASDM ne modifie ni ne supprime ces commandes de votre configuration en cours d'exécution. Consultez Commandes non prises en charge pour de plus amples renseignements.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **Show Commands Ignored by ASDM on Device (Afficher les commandes ignorées par ASDM sur le périphérique)**.

Étape 2 Cliquez sur **OK** lorsque vous avez terminé.

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.

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.

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.