Guide de recréation d'image de Cisco Secure Firewall ASA et Secure Firewall Threat Defense

Dernière modification : 2025-04-30

Guide de recréation d'image de Cisco Secure Firewall ASA et de Secure Firewall Threat Defense

Ce guide explique comment recréer une image entre Cisco Secure Firewall ASA et Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense), et comment procéder à une recréation d'image Thread Defense à l'aide d'une nouvelle version de l'image. À la différence d'une mise à niveau, cette méthode rétablit les paramètres d'usine de Thread Defense. Pour la recréation d'image ASA, consultez le guide de configuration de l'utilisation générale d'ASA qui propose différentes méthodes pour ce faire.

Modèles compatibles

Les modèles suivants prennent en charge le logiciel pour ASA ou le logiciel Thread Defense. Pour la prise en charge des versions ASA et Thread Defense, consultez le Guide de compatibilité ASA ou Guide de compatibilité de Cisco Secure Firewall Threat Defense.

- Firepower 1000
- Secure Firewall 1200
- Firepower 2100 (Thread Defense version 7.4 ou antérieure; ASA version 9.20 ou antérieure)
- Secure Firewall 3100
- Secure Firewall 4200
- ISA 3000
- ASA 5506-X, 5506W-X et 5506H-X (Défense contre les menaces version 6.2.3 ou antérieure; ASA version 9.16 ou antérieure)
- ASA 5508-X (Thread Defense version 7.0 ou antérieure; ASA version 9.16 ou antérieure)
- ASA 5512-X (Thread Defense version 6.2.3 ou antérieure; ASA version 9.12 ou antérieure)
- ASA 5515-X (Thread Defense version 6.4 ou antérieure; ASA version 9.12 ou antérieure)
- ASA 5516-X (Thread Defense version 7.0 ou antérieure; ASA version 9.16 ou antérieure)
- ASA 5525-X (Thread Defense version 6.6 ou antérieure; ASA version 9.14 ou antérieure)
- ASA 5545-X (Thread Defense version 6.6 ou antérieure; ASA version 9.14 ou antérieure)
- ASA 5555-X (Thread Defense version 6.6 ou antérieure; ASA version 9.14 ou antérieure)

Remarque Les modèles Firepower 4100 et 9300 prennent également en charge ASA ou Thread Defense, mais ils sont installés en tant que périphériques logiques. Pour plus de renseignements, consultez les guides de configuration de FXOS.

Remarque Pour Thread Defense sur les modèles ASA 5512-X à 5555-X, vous devez installer un disque SSD Cisco. Pour plus de renseignements, consultez le Guide sur le matériel pour l'ASA 5500-X. Concernant ASA, le disque SSD est également nécessaire pour utiliser le module ASA FirePOWER. (Le disque SSD est inclus dans la configuration standard des modèles ASA 5506-X, 5508-X et 5516-X.)

Recréer l'image d'un appareil Firepower ou Secure Firewall

Les modèles Firepower et Secure Firewall prennent en charge le logiciel pour Défense contre les menaces ou pour l'ASA.

Télécharger le logiciel

Procurez-vous le logiciel Thread Defense ou le logiciel pour ASA.

Remarque Un identifiant Cisco.com et un contrat de service Cisco sont nécessaires.

Tableau 1 : Logiciel Défense contre les menaces

Modèle Défense contre les menaces	Emplacement de téléchargement	Progiciels
Firepower 1000	Voir : www.cisco.com/go/ftd-software.	
	Package Défense contre les menaces Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour le package : cisco-ftd-fp1k.7.4.1-172**SPA**.

Modèle Défense contre les menaces	Emplacement de téléchargement	Progiciels
Secure Firewall 1200	Voir : www.cisco.com/go/ftd-software.	
	Package Défense contre les menaces Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour le package : Cisco_Secure_FW_TD_1200-7.6.0-01.sh.REL.**tar**
Firepower 2100	Voir : www.cisco.com/go/ftd-software.	
	Package Défense contre les menaces Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour le package : cisco-ftd-fp2k.7.4.1-172**SPA**.
Secure Firewall 3100	Voir : www.cisco.com/go/ftd-software.	
	Package Défense contre les menaces Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	• Version 7.3 ou ultérieure – Exemple de nom de fichier utilisé pour le package : Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.**tar** • Version 7.2 – Exemple de nom de fichier utilisé pour le package : cisco-ftd-FP3k.7.2.6-127.**SPA**.
Secure Firewall 4200	Voir : www.cisco.com/go/ftd-software.	
	Package Défense contre les menaces Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour le package : Cisco_Secure_FW_TD_4200-7.4.1-172.sh.REL.**tar**

Tableau 2 : Logiciel pour ASA

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower 1000	Voir : https://www.cisco.com/go/asa-firepower-sw	
	Package ASA Choisissez votre *modèle* > **Logiciel pour ASA (Appareil de sécurité adaptable)** > *version*.	Exemple de nom de fichier utilisé pour le package : cisco-asa-fp1k.9.20.2.2.**SPA**. Ce package comprend ASA et ASDM.
	Logiciel ASDM (mise à niveau) Pour procéder à une mise à niveau vers une version ultérieure d'ASDM en utilisant votre instance actuelle d'ASDM ou l'interface de ligne de commande ASA, choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7202.**bin**.
Secure Firewall 1200		

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower de la série 2100	Voir : https://www.cisco.com/go/asa-firepower-sw	
	Package ASA Choisissez votre *modèle* > **Logiciel pour ASA (Appareil de sécurité adaptable)** > *version*.	Exemple de nom de fichier utilisé pour le package : cisco-asa-fp2k.9.20.2.2.**SPA**. Ce package comprend ASA, ASDM, FXOS et Cisco Secure Firewall chassis manager (anciennement Firepower Chassis Manager).
	Logiciel ASDM (mise à niveau) Pour procéder à une mise à niveau vers une version ultérieure d'ASDM en utilisant votre instance actuelle d'ASDM ou l'interface de ligne de commande ASA, choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7202.**bin**.
Secure Firewall 3100	Voir : https://cisco.com/go/asa-secure-firewall-sw	
	Package ASA Choisissez votre *modèle* > **Logiciel pour ASA (Appareil de sécurité adaptable)** > *version*.	Exemple de nom de fichier utilisé pour le package : cisco-asa-fp3k.9.20.2.2.**SPA**. Ce package comprend ASA et ASDM.
	Logiciel ASDM (mise à niveau) Pour procéder à une mise à niveau vers une version ultérieure d'ASDM en utilisant votre instance actuelle d'ASDM ou l'interface de ligne de commande ASA, choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7202.**bin**.
Cisco Secure Firewall 4200 series	Voir : https://cisco.com/go/asa-secure-firewall-sw	
	Package ASA Choisissez votre *modèle* > **Logiciel pour ASA (Appareil de sécurité adaptable)** > *version*.	Exemple de nom de fichier utilisé pour le package : cisco-asa-fp4200.9.20.2.2.**SPA**. Ce package comprend ASA et ASDM.
	Logiciel ASDM (mise à niveau) Pour procéder à une mise à niveau vers une version ultérieure d'ASDM en utilisant votre instance actuelle d'ASDM ou l'interface de ligne de commande ASA, choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7202.**bin**.

ASA→Threat Defense : Firepower ou Secure Firewall

Cette tâche vous permet de recréer l'image d'un appareil Firepower ou Secure Firewall d'ASA vers Thread Defense en démarrant l'image Thread Defense à partir du logiciel pour ASA.

Avant de commencer

- Assurez-vous que l'image que vous souhaitez charger est disponible sur un serveur FTP, HTTP(S), SCP, SMB ou TFTP, ou sur un lecteur USB formaté en EXT2/3/4 ou en VFAT/FAT32.
- Assurez-vous que le l'interface ASA permet d'accéder au serveur. La configuration par défaut est la suivante :
  - Ethernet 1/2 (interne) – 192.168.1.1
  - Management 1/1 (gestion) – 1010/1210/1220 : 192.168.45.1. Autres modèles : DHCP et route par défaut
  - Ethernet 1/1 (externe) – DHCP et route par défaut

  Si DHCP ne vous fournit pas de route par défaut et que vous devez procéder à un téléchargement à partir d'un serveur distant, configurez la route à l'aide de la commande **route**.

  Vous pouvez également utiliser la commande **configure factory-default** pour définir une adresse IP statique pour Management 1/1 (1010/1210/1220) ou Ethernet 1/2 (autres modèles).
- Pour utiliser la commande « copy » avec un serveur SCP, vous devez :
  - activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**,
  - générer une paire de clés à l'aide de la commande **crypto key generate**.
- (Firepower 2100) Dans les versions 9.12 et antérieures, seul le mode plateforme est disponible. Dans les versions 9.13 et ultérieures, le mode appareil est le mode par défaut. Si vous mettez à niveau un appareil en mode plateforme vers la version 9.13 (ou ultérieure), l'ASA reste en mode plateforme. Pour identifier le mode actuel, utilisez la commande **show fxos mode** dans l'interface de ligne de commande ASA. Les autres modèles ne prennent en charge que le mode appareil.

  Si vous disposez d'un ASA en mode plateforme, vous devez utiliser FXOS pour recréer l'image. Consultez ASA→Défense contre les menaces : Firepower 2100 – Mode plateforme, à la page 8.
- (Secure Firewall 3100) Pour une recréation d'image d'ASA vers Threat Defense 7.3+ sur un appareil Secure Firewall 3100, vous devez d'abord mettre à niveau ASA vers la version 9.19+ pour ensuite effectuer la mise à jour de la version de ROMMON et pouvoir prendre en charge le nouveau type d'image introduit dans la version 7.3. Consultez le Guide de mise à niveau de l'ASA.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de l'appareil de sécurité adaptable Cisco.

Étape 2 Annulez l'enregistrement de l'ASA sur le serveur Smart Software Licensing, à partir de l'interface de ligne de commande ASA/ASDM ou du serveur Smart Software Licensing.

license smart deregister

Exemple :

```
ciscoasa# license smart deregister
```

Étape 3 Téléchargez l'image Thread Defense dans la mémoire flash. Cette étape illustre une commande « copy FTP ».

copy ftp://[[*user@*]*server_ip*[*/path*]*/ftd_image_name* **disk***n***:/**[*path/*]*ftd_image_name*

Pour utiliser le lecteur USB, entrez **disk1://**, sauf pour le Firepower 2100, qui utilise **disk2://**.

Remarque
L'ASA ne peut pas résoudre les noms de domaine complets en utilisant le DNS avec la commande **copy**. Vous devez utiliser une adresse IP pour désigner le serveur.

Exemple :

Firepower 2100

```
ciscoasa# copy ftp://dwinchester@10.1.1.1/cisco-ftd-fp2k.7.4.1-172.SPA
disk0:/cisco-ftd-fp2k.7.4.1-172.SPA
```

Exemple :

Secure Firewall 3100

```
ciscoasa# copy ftp://dwinchester@10.1.1.1/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar
disk0:/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar
```

Étape 4 Démarrez l'image Thread Defense (celle que vous venez de charger).

a) Accédez au mode de configuration globale.

configure terminal

Exemple :

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

b) Affichez l'image de démarrage actuellement configurée, le cas échéant.

show running-config boot system

Notez que la commande **boot system** peut ne pas figurer dans votre configuration, notamment si vous avez installé l'image ASA d'origine à partir de ROMMON, si vous disposez d'un nouvel appareil ou si vous avez supprimé la commande manuellement.

Exemple :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.20.2.2.SPA
```

c) Si une commande **boot system** est configurée, supprimez-la afin de pouvoir préciser la nouvelle image de démarrage.

no boot system disk*n***:/**[*path/*]*asa_image_name*

Si aucune commande **boot system** n'est configurée, ignorez cette étape.

Exemple :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.20.2.2.SPA
```

d) Démarrez avec l'image Thread Defense.

boot system disk*n***:/**[*path*/]*ftd_image_name*

Vous êtes invité à procéder au rechargement.

Exemple :

Secure Firewall 3100

```
ciscoasa(config)# boot system disk0:/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar

fxos_set_boot_system_image(filename: Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar)
fxos_get_current_bundle_version(instance 41)
The system is currently installed with security software package 9.20.2.2, which has:
   - The platform version:  2.14.1.131
   - The CSP (asa) version: 9.20.2.2
Preparing new image for install...
!!!!!!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Attention:
   If you proceed the system will be re-imaged and reboot automatically.
   All existing configuration will be lost and the default configuration applied.
Do you want to proceed? [confirm]
Finalizing image install process...

Installation succeeded.
```

Exemple :

Firepower 2100

```
ciscoasa(config)# boot system disk0:/cisco-ftd-fp2k.7.4.1-172.SPA

fxos_set_boot_system_image(filename: cisco-ftd-fp2k.7.4.1-172.SPA)
fxos_get_current_bundle_version(instance 41)
The system is currently installed with security software package 9.20.2.2, which has:
   - The platform version:  2.14.1.131
   - The CSP (asa) version: 9.20.2.2
Preparing new image for install...
!!!!!!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Attention:
   If you proceed the system will be re-imaged and reboot automatically.
   All existing configuration will be lost and the default configuration applied.
Do you want to proceed? [confirm]
Finalizing image install process...

Installation succeeded.
```

Étape 5 Attendez que le redémarrage du châssis soit terminé.

FXOS démarre en premier, mais vous devez encore attendre le démarrage de Thread Defense.

Une fois que l'application est lancée et que vous y êtes connecté, vous êtes invité à accepter le CLUF et à procéder à la configuration initiale par l'entremise de l'interface de ligne de commande. Pour gérer votre appareil, vous pouvez utiliser le Cisco Secure Firewall device manager (anciennement Firepower Device Manager) ou le Cisco Secure Firewall Management Center (anciennement Firepower Management Center). Consultez le guide de démarrage rapide de votre modèle et de votre gestionnaire pour poursuivre la configuration : http://www.cisco.com/go/ftd-asa-quick

Exemple :

```
[...]
************ Attention *********

   Initializing the configuration database.  Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.

************ Attention *********
Executing S09database-init                                              [  OK  ]
Executing S11database-populate

Cisco FPR Series Security Appliance
firepower login: admin
Password:
Successful login attempts for user 'admin' : 1

Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
[...]

User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower>
firepower# connect ftd
You must accept the EULA to continue.
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
[...]
```

ASA→Défense contre les menaces : Firepower 2100 – Mode plateforme

Cette tâche vous permet de recréer l'image du Firepower 2100 en mode plateforme dans Défense contre les menaces.

Remarque À l'issue de cette procédure, le mot de passe administrateur de FXOS est réinitialisé sur **Admin123**.

Avant de commencer

- Pour cette procédure, vous devez utiliser l'interface de ligne de commande FXOS.
- Dans la version 9.12 ou antérieure, seul le mode plateforme est disponible. Dans les versions 9.13 et ultérieures, le mode appareil est le mode par défaut. Si vous mettez à niveau un appareil en mode plateforme vers la version 9.13 (ou ultérieure), l'ASA reste en mode plateforme. Vérifiez le mode de la

version 9.13 ou ultérieure en utilisant la commande **show fxos mode** dans l'interface de ligne de commande ASA.

Si vous disposez d'un ASA en mode appareil, vous n'avez pas accès à ces commandes FXOS. La recréation de l'image sur Défense contre les menaces s'effectue dans le système d'exploitation de l'ASA. Consultez ASA→Threat Defense : Firepower ou Secure Firewall, à la page 5.

Procédure

Étape 1 Assurez-vous que l'image que vous souhaitez charger est disponible sur un serveur FTP, SCP, SFTP ou TFTP connecté à l'interface de gestion Management 1/1 de FXOS, ou sur un lecteur USB formaté en EXT2/3/4 ou en VFAT/FAT32.

Pour vérifier ou modifier l'adresse IP de l'interface de gestion Management 1/1 de FXOS, consultez le Guide de démarrage de Firepower 2100.

Étape 2 Annulez l'enregistrement de l'ASA sur le serveur Smart Software Licensing, à partir de l'interface de ligne de commande ASA/ASDM ou du serveur Smart Software Licensing.

Étape 3 Connectez-vous à l'interface de ligne de commande FXOS, soit à partir du port de la console (de préférence), soit en utilisant SSH pour accéder à l'interface de gestion Management 1/1. Si vous vous connectez à partir du port de la console, vous accédez immédiatement à l'interface de ligne de commande FXOS. Entrez les coordonnées de connexion FXOS. Le nom d'utilisateur par défaut est **admin** et le mot de passe par défaut **Admin123**.

Si vous vous connectez à l'adresse IP de l'interface de gestion ASA à l'aide du protocole SSH, entrez **connect fxos** pour accéder à FXOS. Vous pouvez également utiliser le protocole SSH pour vous connecter directement à l'adresse IP de l'interface de gestion FXOS.

Étape 4 Téléchargez le package sur le châssis.

a) Entrez en mode micrologiciel.

scope firmware

Exemple :

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Téléchargez le package.

download image *url*

Précisez l'URL du fichier en cours d'importation en utilisant l'un des modèles suivants :

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path/filename*

Exemple :

```
firepower-2110 /firmware # download image
scp://admin@10.88.29.181/cisco-ftd-fp2k.7.4.1-172.SPA
Password:
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Surveillez le processus de téléchargement.

show download-task

Exemple :

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-ftd-fp2k.7.4.1-172.SPA
              Scp      10.122.84.45             0 admin           Downloading
firepower-2110 /firmware #
```

Étape 5 Une fois le nouveau package téléchargé (état **Downloaded** [Téléchargé]), démarrez-le.

a) Affichez et copiez le numéro de version du nouveau package.

show package

Exemple :

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.20.2.2.SPA                9.20.2.2
cisco-ftd-fp2k.7.4.1-172.SPA               7.4.1-172
firepower-2110 /firmware #
```

b) Installez le package.

Mise en garde
Cette étape efface votre configuration.

scope auto-install

install security-pack version *version*

Dans la sortie**show package** , copiez la valeur **Package-Vers** (version du package) pour le numéro **security-pack version**. Le châssis installe l'image et redémarre. Ce processus peut prendre environ 5 minutes.

Remarque
Si vous rencontrez l'erreur ci-dessous, il se peut que vous ayez saisi le *nom* du package, et non sa *version* :

```
Invalid software pack
Please contact technical support for help
```

Exemple :

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 7.4.1-172

The system is currently installed with security software package 9.20.2.2, which has:
   - The platform version: 2.14.1.131
   - The CSP (asa) version: 9.20.2.2
If you proceed with the upgrade 7.4.1-172, it will do the following:
   - upgrade to the new platform version 2.14.1.131
   - reimage the system from CSP asa version 9.20.2.2 to the CSP ftd version 7.4.1-172

Do you want to proceed ? (yes/no): yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no): yes

Triggered the install of software package version 7.4.1-172
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

Étape 6 Attendez que le redémarrage du châssis soit terminé.

FXOS démarre en premier, mais vous devez encore attendre le démarrage de Défense contre les menaces.

Une fois que l'application est lancée et que vous y êtes connecté, vous êtes invité à accepter le CLUF et à procéder à la configuration initiale par l'entremise de l'interface de ligne de commande. Vous pouvez utiliser le gestionnaire d'appareil ou le centre de gestion pour gérer votre appareil. Consultez le guide de démarrage rapide de votre modèle et de votre gestionnaire pour poursuivre la configuration : http://www.cisco.com/go/ftd-asa-quick

Exemple :

```
[...]
************ Attention *********

   Initializing the configuration database.  Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.

************ Attention *********
Executing S09database-init                                              [  OK  ]
Executing S11database-populate

Cisco FPR Series Security Appliance
firepower login: admin
Password:
Successful login attempts for user 'admin' : 1

Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
[...]
```

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower>
firepower# connect ftd
You must accept the EULA to continue.
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
[...]
```

Threat Defense→ASA : Firepower ou Secure Firewall

Cette tâche vous permet de recréer l'image Thread Defense d'un appareil Firepower ou Secure Firewall dans ASA. Sur le Firepower 2100, l'ASA fonctionne par défaut en mode appareil. Après la recréation d'image, vous pouvez passer en mode plateforme.

Remarque À l'issue de cette procédure, le mot de passe administrateur de FXOS est réinitialisé sur **Admin123**.

Procédure

Étape 1 Assurez-vous que l'image que vous souhaitez charger est disponible sur un serveur FTP, HTTP(S), SCP, SFTP ou TFTP connecté à l'interface de gestion Management 1/1 (ou pour le Secure Firewall 4200, à l'interface de gestion Management 1/1 ou 2/2), ou sur un lecteur USB formaté en EXT2/3/4 ou en VFAT/FAT32.

Pour plus de renseignements sur les paramètres de l'interface de gestion, consultez les commandes Thread Defense **show network** et **configure network** dans Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Étape 2 Annulez la licence Thread Defense.

- Si vous gérez Thread Defense à partir du centre de gestion, supprimez l'appareil à partir du centre de gestion.
- Si vous gérez Thread Defense à l'aide du gestionnaire d'appareil, annulez l'enregistrement de l'appareil sur le serveur Smart Software Licensing , à partir du gestionnaire d'appareil ou du serveur Smart Software Licensing.

Étape 3 Connectez-vous à l'interface de ligne de commande FXOS, soit à partir du port de la console (de préférence), soit en utilisant SSH pour accéder à l'interface de gestion. Si vous vous connectez à partir du port de la console, vous accédez immédiatement à l'interface de ligne de commande FXOS. Entrez les coordonnées de connexion FXOS. Le nom d'utilisateur par défaut est **admin** et le mot de passe par défaut **Admin123**.

Si vous vous connectez à l'adresse IP de l'interface de gestion Thread Defense à l'aide du protocole SSH, entrez **connect fxos** pour accéder à FXOS.

Étape 4 Téléchargez le package sur le châssis.

a) Entrez en mode micrologiciel.

scope firmware

Exemple :

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Téléchargez le package.

download image *url*

Précisez l'URL du fichier en cours d'importation en utilisant l'un des modèles suivants :

- **ftp:**//*username@server*/[*path*/]*image_name*
- **http:**//*username@server*/[*path*/]*image_name*
- **https:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path*/*filename*

Exemple :

```
firepower-2110 /firmware # download image
scp://admin@10.88.29.181/cisco-asa-fp2k.9.20.2.2.SPA
Password:
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Surveillez le processus de téléchargement :

show download-task

Exemple :

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.20.2.2.SPA
              Scp      10.122.84.45             0 admin           Downloading
firepower-2110 /firmware #
```

Étape 5 Une fois le nouveau package téléchargé (état **Downloaded** [Téléchargé]), démarrez-le.

a) Affichez et copiez le numéro de version du nouveau package.

show package

Exemple :

```
firepower-2110 /firmware # show package
```

```
Name                                         Package-Vers
-------------------------------------------- ------------
cisco-asa-fp2k.9.20.2.2.SPA                  9.20.2.2
cisco-ftd-fp2k.7.4.1-172.SPA                 7.4.1-172
firepower-2110 /firmware #
```

b) Installez le package.

Mise en garde
Cette étape efface votre configuration.

scope auto-install

install security-pack version *version*

Dans la sortie **show package** , copiez la valeur **Package-Vers** (Version du package) pour le numéro **security-pack version**. Le châssis installe l'image et redémarre. Ce processus, rechargement compris, peut prendre environ 30 minutes.

Remarque
Si vous rencontrez l'erreur ci-dessous, il se peut que vous ayez saisi le *nom* du package, et non sa *version* :

```
Invalid software pack
Please contact technical support for help
```

Exemple :

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.20.2.2

The system is currently installed with security software package 7.4.1-172, which has:
   - The platform version: 2.14.1.131
   - The CSP (ftd) version: 7.4.1-172
If you proceed with the upgrade 9.20.2.2, it will do the following:
   - upgrade to the new platform version 2.14.1.131
   - reimage the system from CSP ftd version 7.4.1-172 to the CSP asa version 9.20.2.2

Do you want to proceed ? (yes/no): yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no): yes

Triggered the install of software package version 9.20.2.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

Étape 6 Attendez que le redémarrage du châssis soit terminé.

ASA version 9.13 ou ultérieure (par défaut en mode appareil)

L'ASA démarre et vous accédez au mode EXEC utilisateur dans l'interface de ligne de commande.

Exemple :

```
 [...]
Attaching to ASA CLI ...
Type help or '?' for a list of available commands.
ciscoasa>
```

ASA version 9.12 ou antérieure (par défaut en mode plateforme)

FXOS démarre en premier, mais vous devez encore attendre le démarrage de l'ASA.

Une fois que l'application est lancée et que vous y êtes connecté, vous accédez au mode EXEC utilisateur dans l'interface de ligne de commande.

Exemple :

```
 [...]
Cisco FPR Series Security Appliance
firepower-2110 login: admin
Password:

Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2024, Cisco Systems, Inc. All rights reserved.
[...]

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
[press Enter to see the prompt below:]

firepower-2110# connect asa
Attaching to ASA CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa>
```

Threat Defense→Threat Defense : Firepower ou Secure Firewall

Pour le Secure Firewall 3100 uniquement, la méthode de recréation d'image dépend de la version que vous utilisez.

Threat Defense→Threat Defense : Firepower ou Secure Firewall (sauf 3100)

Ces modèles offrent plusieurs niveaux de recréation d'image, du simple effacement de la configuration au remplacement de l'image, en passant par la restauration des paramètres d'usine de l'appareil.

Procédure

Étape 1 Pour plus de renseignements sur les procédures de recréation d'image, consultez le Guide de résolution de problèmes.

Étape 2 Si vous souhaitez charger une nouvelle version, utilisez la procédure « Recréer l'image du système avec une nouvelle version du logiciel ».

Utilisez les autres méthodes de recréation d'image à des fins de dépannage, par exemple si vous ne parvenez pas à démarrer l'ordinateur ou à réinitialiser le mot de passe.

Threat Defense→Threat Defense : Secure Firewall 3100

Le modèle Cisco Secure Firewall 3100 offre plusieurs niveaux de recréation d'image, du simple effacement de la configuration au remplacement de l'image, en passant par la restauration des paramètres d'usine de l'appareil. Consultez les options de recréation d'image suivantes, qui varient en fonction de vos versions de départ et d'arrivée.

Procédure

Étape 1 **Recréation d'image vers la version 7.2, ou de la version 7.3 ou ultérieure vers la version 7.3 ou ultérieure :** pour connaître les procédures de recréation d'image, consultez le guide de dépannage.

Si vous souhaitez charger une nouvelle version, utilisez la procédure « Recréer l'image du système avec une nouvelle version du logiciel ».

Utilisez les autres méthodes de recréation d'image à des fins de dépannage, par exemple si vous ne parvenez pas à démarrer l'ordinateur ou à réinitialiser le mot de passe.

Étape 2 **Recréation d'image de la version 7.1/7.2 vers la version 7.3 ou ultérieure :** si vous souhaitez procéder à une recréation d'image de la version 7.1/7.2 vers la version 7.3 ou ultérieure, vous devez d'abord recréer l'image dans ASA 9.19 ou dans une version ultérieure, puis dans la version 7.3 ou ultérieure.

Les versions 7.3 et ultérieures utilisent un nouveau type de fichier image. Avant de pouvoir l'utiliser, vous devez mettre à jour ROMMON, ce qui explique pourquoi vous devez procéder à la recréation d'image dans ASA 9.19 ou dans une version ultérieure (ces versions étant prises en charge par l'ancienne version de ROMMON, tout en permettant la mise à niveau vers la nouvelle version) avant de pouvoir récréer l'image dans la version 7.3 ou ultérieure. Il n'y a pas de programme de mise à jour de ROMMON distinct.

Remarque
Si vous souhaitez procéder à une *mise à niveau* de la version 7.1/7.2 vers la version 7.3 ou ultérieure, vous pouvez appliquer la procédure de mise à niveau standard. ROMMON sera mis à jour dans le cadre du processus de mise à niveau.

a) Procédez à une recréation d'image de Threat Defense vers ASA 9.19 ou toute version ultérieure. Consultez Threat Defense→ASA : Firepower ou Secure Firewall, à la page 12.

b) Procédez à une recréation d'image d'ASA vers Threat Defense 7.3 ou version ultérieure. Consultez ASA→Threat Defense : Firepower ou Secure Firewall, à la page 5.

ASA→ASA : Firepower et Secure Firewall

Il peut être nécessaire de recréer l'image d'un appareil de sécurité adaptable (ASA) pour effectuer le dépannage des problèmes de démarrage et récupérer le mot de passe. Dans le cadre d'une mise à niveau normale, aucune recréation d'image n'est requise.

Procédure

Étape 1 Pour plus de renseignements sur les procédures de recréation d'image, consultez le Guide de résolution de problèmes.

Étape 2 Pour charger une nouvelle image logicielle, consultez le Guide de mise à niveau de l'ASA plutôt que de recréer l'image.

Recréer l'image de l'ASA 5500-X ou de l'ISA 3000

De nombreux modèles des séries ASA 5500-X ou ISA 3000 prennent en charge les logiciels Thread Defense ou ASA.

Accès au port de la console requis

Pour procéder à la recréation d'image, vous devez connecter votre ordinateur au port de la console.

Pour les modèles ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X, vous devrez peut-être utiliser un câble série-USB tiers afin d'établir la connexion. D'autres modèles sont équipés d'un port de console Mini USB Type B, ce qui vous permet d'utiliser n'importe quel câble mini USB. Sous Windows, il peut être nécessaire d'installer un pilote USB à partir de software.cisco.com. Pour plus de renseignements sur les options de port de la console et sur les pilotes requis, consultez le guide sur le matériel : http://www.cisco.com/go/asa5500x-install

Utilisez un émulateur de terminal pour 9600 bauds, 8 bits de données, aucune parité, 1 bit d'arrêt, aucun contrôle de flux.

Télécharger le logiciel

Procurez-vous le Thread Defense ou les logiciels pour les modules ASA, ASDM et ASA FirePOWER. Les procédures décrites dans ce document exigent que vous installiez le logiciel sur un serveur TFTP pour le téléchargement initial. D'autres images peuvent être téléchargées à partir d'autres types de serveurs (HTTP ou FTP, par exemple). Pour obtenir les caractéristiques exactes du progiciel et du type de serveur, consultez les procédures.

Remarque Un identifiant Cisco.com et un contrat de service Cisco sont nécessaires.

Attention L'image de démarrage Thread Defense et le progiciel sont spécifiques à la version et au modèle. Assurez-vous d'avoir l'image de démarrage et le progiciel correspondant à votre plateforme. Une incompatibilité entre l'image de démarrage et le progiciel peut entraîner un échec de démarrage. Ce type d'incompatibilité peut se produire si vous utilisez une image de démarrage plus ancienne avec un progiciel plus récent.

Tableau 3 : Logiciel Défense contre les menaces

Modèle Défense contre les menaces	Emplacement de téléchargement	Progiciels
ASA 5506-X, ASA 5508-X et ASA 5516-X	Voir : http://www.cisco.com/go/asa-firepower-sw.	**Remarque** Vous verrez également des fichiers de correctif se terminant par **.sh**. Le processus de mise à niveau des correctifs n'est pas décrit dans le présent document.
	Image de démarrage Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier de l'image de démarrage : ftd-boot-9.6.2.0**.lfbff**.
	Package d'installation du logiciel système Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour le package d'installation du logiciel système : ftd-6.1.0-330**.pkg**.

Modèle Défense contre les menaces	Emplacement de téléchargement	Progiciels
ASA 5512-X à ASA 5555-X	Voir : http://www.cisco.com/go/asa-firepower-sw.	**Remarque** Vous verrez également des fichiers de correctif se terminant par **.sh**. Le processus de mise à niveau des correctifs n'est pas décrit dans le présent document.
	Image de démarrage Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour l'image de démarrage : ftd-boot-9.6.2.0**.cdisk**.
	Package d'installation du logiciel système Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour le package d'installation du logiciel système : ftd-6.1.0-330**.pkg**.
ISA 3000	Voir : http://www.cisco.com/go/isa3000-software	**Remarque** Vous verrez également des fichiers de correctif se terminant par **.sh**. Le processus de mise à niveau des correctifs n'est pas décrit dans le présent document.
	Image de démarrage Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour l'image de démarrage : ftd-boot-9.9.2.0**.lfbff**.
	Package d'installation du logiciel système Choisissez votre *modèle* > **Logiciel Firepower Threat Defense** > *Version*.	Exemple de nom de fichier utilisé pour le package d'installation du logiciel système : ftd-6.2.3-330**.pkg**.

Tableau 4 : Logiciel pour ASA

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA 5506-X, ASA 5508-X et ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	Logiciel pour ASA Choisissez votre *modèle* > **Logiciel pour ASA (Appareil de sécurité adaptable)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel pour ASA : **asa962-lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire des appareils de sécurité adaptables (ASA)** > *Version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel pour API REST Choisissez votre *modèle* > **API REST pour le module d'extension ASA (Adaptive Security Appliance)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel pour API : **asa-servapi-132-lfbff-k8.SPA**. Pour installer l'API REST, consultez le Guide de démarrage rapide de l'API.
	Logiciel ROMMON Choisissez votre *modèle* > **Logiciel Rommon pour ASA** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ROMMON : asa5500-firmware-1108**.SPA**.
ASA 5512-X à ASA 5555-X	http://www.cisco.com/go/asa-software	
	Logiciel pour ASA Choisissez votre *modèle* > **Logiciels sur châssis** > **Logiciel pour ASA (Adaptative Security Appliance)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel pour ASA : asa962-**smp-k8.bin**.
	Logiciel ASDM Choisissez votre *modèle* > **Logiciels sur châssis** > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel pour API REST Choisissez votre *modèle* > **Logiciels sur châssis** > **REST API pour module d'extension pour ASA (Adaptive Security Appliance)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel pour API : **asa-servapi-132-lfbff-k8.SPA**. Pour installer l'API REST, consultez le Guide de démarrage rapide de l'API.
	Package pour ASA pour APIC (Cisco Application Policy Infrastructure Controller) Choisissez votre *modèle* > **Logiciels sur châssis** > **Packages pour ASA pour ACI (Infrastructure axée sur les applications)** > *version*.	Pour APIC 1.2(7) et les versions ultérieures, choisissez le package Policy Orchestration avec Fabric Insertion ou le package Fabric Insertion seulement. Exemple de nom de fichier utilisé pour le package pour appareil : asa-device-pkg-1.2.7.10**.zip**. Pour installer le package pour ASA, consultez le chapitre « Importation d'un package pour appareil » du Guide de déploiement des services APIC de Cisco pour les couches 4 à 7.

Modèle ASA	Emplacement de téléchargement	Progiciels
ISA 3000	http://www.cisco.com/go/isa3000-software	
	Logiciel pour ASA Choisissez votre *modèle* > **Logiciel pour ASA (Appareil de sécurité adaptable)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel pour ASA : **asa962-lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire des appareils de sécurité adaptables (ASA)** > *Version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel pour API REST Choisissez votre *modèle* > **API REST pour le module d'extension ASA (Adaptive Security Appliance)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel pour API : **asa-servapi-132-lfbff-k8.SPA**. Pour installer l'API REST, consultez le Guide de démarrage rapide de l'API.

Mise à niveau de l'image ROMMON (ASA 5506-X, 5508-X et 5516-X, ISA 3000)

Pour les modèles ASA 5506-X, ASA 5508-X, ASA 5516-X, ISA 3000, procédez comme suit afin de mettre à niveau l'image ROMMON. Pour les modèles ASA, vous devez avoir installé la version 1.1.8 ou toute version ultérieure de ROMMON sur votre système. Nous vous recommandons d'effectuer la mise à niveau vers la dernière version.

Seule une mise à niveau vers une nouvelle version est possible; la rétrogradation n'est pas prise en charge.

⚠

Mise en garde La mise à niveau de ROMMON vers la version 1.1.15 sur les modèles ASA 5506-X, 5508-X et 5516-X, tout comme la mise à niveau vers la version 1.1.15 sur les modèles ISA 3000 prend deux fois plus de temps que pour les versions précédentes (environ 15 minutes). **N'éteignez pas** l'appareil pendant la mise à niveau. Si la mise à niveau prend plus de 30 minutes ou si elle échoue, contactez l'assistance technique de Cisco. **N'éteignez pas** l'appareil et ne le réinitialisez pas.

Avant de commencer

Procurez-vous la nouvelle image ROMMON sur Cisco.com et enregistrez-la sur un serveur pour ensuite la copier sur l'ASA. L'ASA prend en charge les serveurs FTP, TFTP, SCP, HTTP(S) et SMB. Téléchargez l'image de :

- ASA 5506-X, 5508-X et 5516-X : https://software.cisco.com/download/home/286283326/type
- ISA 3000 : https://software.cisco.com/download/home/286288493/type

Procédure

Étape 1 Pour le logiciel Thread Defense, accédez à l'interface de ligne de commande de dépistage et passez en mode d'activation.

system support diagnostic-cli

activer

Lorsque vous y êtes invité, appuyez sur Entrée sans saisir de mot de passe.

Exemple :

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa> enable
Password:
ciscoasa#
```

Étape 2 Copiez l'image ROMMON sur la mémoire flash de l'ASA. Cette procédure illustre la commande « copy FTP ». Entrez **copy ?** pour la syntaxe appropriée pour les autres types de serveurs.

copy ftp://[*noms d'utilisateur***:***mot de passe***@**]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

En ce qui concerne le logiciel Thread Defense, assurez-vous qu'une interface de données est configurée puisque l'interface de ligne de commande de dépistage n'a pas accès à l'interface de gestion dédiée. En outre, CSCvn57678 peut empêcher la commande **copy** de fonctionner dans l'interface de ligne de commande Thread Defense standard avec votre version de Thread Defense. Dans un tel cas, cette méthode ne vous permettra pas d'accéder à l'interface de gestion dédiée.

Étape 3 Pour connaître la version installée, entrez la commande **show module** et consultez la version du pare-feu (FW) dans la sortie du module 1 du tableau des plages d'adresses MAC :

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

Étape 4 Procédez à la mise à niveau de l'image ROMMON :

upgrade rommon disk0:asa5500-firmware-*XXXX***.SPA**

Exemple :

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
```

```
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

Étape 5 Lorsque vous y êtes invité, appuyez sur Confirmer pour recharger l'ASA.

L'ASA met à niveau l'image ROMMON, puis recharge le système d'exploitation.

ASA→Défense contre les menaces : ASA 5500-X ou ISA 3000

Pour recréer l'image de l'ASA dans le logiciel Défense contre les menaces, vous devez accéder à l'invite ROMMON. Dans ROMMON, vous devez utiliser TFTP dans l'interface de gestion pour télécharger l'image de démarrage Défense contre les menaces. Seul le protocole TFTP est pris en charge. L'image de démarrage peut ensuite télécharger le package d'installation du logiciel système Défense contre les menaces à l'aide de HTTP ou de FTP. Le téléchargement par TFTP peut prendre beaucoup de temps. Assurez-vous d'avoir une connexion stable entre l'ASA et le serveur TFTP pour éviter toute perte de paquets.

Avant de commencer

Pour faciliter le processus de recréation d'image dans un ASA, procédez comme suit :

1. Effectuez une sauvegarde complète du système à l'aide de la commande **backup**.

   Pour plus de renseignements et pour explorer d'autres techniques de sauvegarde, consultez le guide de configuration.

2. Copiez et enregistrez les clés d'activation actuelles pour ensuite pouvoir réinstaller vos licences à l'aide de la commande **show activation-key**.

3. Pour l'ISA 3000, désactivez le contournement matériel lorsque vous utilisez le centre de gestion. Cette fonctionnalité est uniquement accessible par l'entremise du gestionnaire d'appareil dans la version 6.3 (ou ultérieure).

Procédure

Étape 1 Téléchargez l'image de démarrage Défense contre les menaces (voir Télécharger le logiciel, à la page 18) sur un serveur TFTP auquel l'ASA a accès dans l'interface de gestion.

Pour les modèles ASA 5506-X, 5508-X, 5516-X, ISA 3000 : vous devez utiliser le port de gestion Management 1/1 afin de télécharger l'image. Pour les autres modèles, vous pouvez utiliser n'importe quelle interface.

Étape 2 Téléchargez le package d'installation du logiciel système Défense contre les menaces (voir Télécharger le logiciel, à la page 18) sur un serveur HTTP ou FTP auquel l'ASA a accès dans l'interface de gestion.

Étape 3 À partir du port de la console, rechargez l'ASA :

reload

Exemple :

```
ciscoasa# reload
```

Étape 4 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à accéder à l'invite pour ROMMON.

Observez attentivement le moniteur.

Exemple :

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

Appuyez sur la touche **Échap**.

Si le message suivant s'affiche, cela signifie que vous avez attendu trop longtemps. Vous devez alors recharger l'ASA, une fois le démarrage terminé :

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

Étape 5 Configurez les paramètres réseau et chargez l'image de démarrage à l'aide des commandes ROMMON suivantes :

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftpdnld

L'image de démarrage Défense contre les menaces est téléchargée et l'interface de ligne de commande démarre.

Consultez les renseignements suivants :

- **interface** (ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X uniquement) : précise l'ID de l'interface. Les autres modèles utilisent toujours l'interface de gestion Management 1/1.
- **set** : affiche les paramètres réseau. Vous pouvez également utiliser la commande **ping** pour vérifier la connectivité avec le serveur.
- **sync** : enregistre les paramètres réseau.
- **tftpdnld** : charge l'image de démarrage.

Exemple :

Exemple pour l'ASA 5555-X :

```
rommon 0 > interface gigabitethernet0/0
rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.255.0
rommon 3 > server 10.86.118.21
rommon 4 > gateway 10.86.118.1
rommon 5 > file ftd-boot-latest.cdisk
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=ftd-boot-latest.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 7 > sync

Updating NVRAM Parameters...

rommon 8 > tftpdnld
```

Exemple pour l'ASA 5506-X :

```
rommon 0 > address 10.86.118.4
rommon 1 > netmask 255.255.255.0
rommon 2 > server 10.86.118.21
rommon 3 > gateway 10.86.118.21
rommon 4 > file ftd-boot-latest.lfbff
rommon 5 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=ftd-boot-latest.lfbff
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 6 > sync
```

```
Updating NVRAM Parameters...

rommon 7 > tftpdnld
```

Envoyer un message Ping pour résoudre un problème de connectivité avec le serveur :

```
rommon 1 > ping 10.123.123.2
Sending 10, 32-byte ICMP Echoes to 10.123.123.2 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

Étape 6 Entrez **setup** et configurez les paramètres réseau de l'interface de gestion pour établir une connectivité temporaire avec le serveur HTTP ou FTP, ce qui vous permettra de télécharger et d'installer le package système.

Remarque
Si vous disposez d'un serveur DHCP, Thread Defense définit automatiquement la configuration réseau. Consultez les exemples de messages de démarrage suivants si vous utilisez DHCP :

```
Configuring network interface using DHCP
Bringing up network interface.
Depending on your network, this might take a couple of minutes when using DHCP...
ifup: interface lo already configured
Using IPv4 address: 10.123.123.123
Using IPv6 address: fe80::2a0:c9ff:fe00:0
Using DNS server: 64.102.6.247
Using DNS server: 173.36.131.10
Using default gateway: 10.123.123.1
```

Exemple :

```
                   Cisco FTD Boot 6.3.0
                Type ? for list of commands
firepower-boot>
firepower-boot>setup


 Welcome to Cisco FTD Setup
 [hit Ctrl-C to abort]
 Default values are inside []

Enter a hostname [firepower]: example.cisco.com
Do you want to configure IPv4 address on management interface?(y/n) [Y]: y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]:
n
Enter an IPv4 address: 10.123.123.123
Enter the netmask: 255.255.255.0
Enter the gateway: 10.123.123.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: n
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address [64.102.6.247]: 10.123.123.2
Do you want to configure Secondary DNS Server? (y/n) [y]: n
Any previously configured secondary DNS servers will be removed.
Do you want to configure Local Domain Name? (y/n) [n]: n
Do you want to configure Search domains? (y/n) [y]: n
Any previously configured search domains will be removed.
```

```
Do you want to enable the NTP service? [N]: n
Please review the final configuration:
Hostname: example.cisco.com
Management Interface Configuration

IPv4 Configuration: static
 IP Address: 10.123.123.123
 Netmask: 255.255.255.0
 Gateway: 10.123.123.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
 DNS Server:
 10.123.123.2

NTP configuration: Disabled

CAUTION:
You have selected IPv6 stateless autoconfiguration, which assigns a global address
based on network prefix and a device identifier. Although this address is unlikely
to change, if it does change, the system will stop functioning correctly.
We suggest you use static addressing instead.

Apply the changes?(y,n) [Y]: y
Configuration saved successfully!
Applying...
Restarting network services...
Done.
Press ENTER to continue...
firepower-boot>
```

Étape 7 Téléchargez le package d'installation du logiciel système Défense contre les menaces. Cette étape illustre une installation avec HTTP.

system install [**noconfirm**] *url*

Incluez l'option **noconfirm** si vous ne souhaitez pas répondre aux messages de confirmation.

Exemple :

```
> system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg
```

Vous êtes invité à effacer le lecteur flash interne. Entrez **y**.

```
######################## WARNING #############################
# The content of disk0: will be erased during installation! #
############################################################

Do you want to continue? [y/N] y
```

Le processus d'installation efface le lecteur flash et télécharge l'image du système. Vous êtes invité à poursuivre l'installation. Entrez **y**.

```
Erasing disk0 ...
Verifying
Downloading
Extracting
Package Detail
```

```
 Description: Cisco ASA-NGFW 6.3.0 System Install
 Requires reboot: Yes

Do you want to continue with upgrade? [y]: y
```

Une fois l'installation terminée, appuyez sur **Entrée** pour redémarrer l'appareil.

```
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

Le redémarrage prendra au moins 30 minutes et même beaucoup plus. Au redémarrage, vous accéderez à l'interface de ligne de commande Thread Defense.

Étape 8 Pour résoudre les problèmes de connectivité du réseau, consultez les exemples suivants.

Exemple :

Visualiser la configuration de l'interface réseau :

```
firepower-boot>show interface
eth0 Link encap:Ethernet HWaddr 00:a0:c9:00:00:00
 inet addr:10.123.123.123 Bcast:10.123.123.255 Mask:255.255.255.0
 inet6 addr: fe80::2a0:c9ff:fe00:0/64 Scope:Link
 inet6 addr: 2001:420:270d:1310:2a0:c9ff:fe00:0/64 Scope:Global
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:522369 errors:0 dropped:0 overruns:0 frame:0
 TX packets:2473 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:42120849 (40.1 MiB) TX bytes:170295 (166.3 KiB)
...
```

Envoyer un message Ping à un serveur :

```
firepower-boot>ping www.example.com
PING www.example.com (10.125.29.106) 56(84) bytes of data.
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=1 ttl=42 time=28.8 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=2 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=3 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=4 ttl=42 time=29.0 ms
^C
--- www.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 28.159/28.549/29.022/0.437 ms

firepower-boot>
```

Activer Traceroute pour tester la connectivité du réseau :

```
firepower-boot>traceroute -n 10.100.100.1
traceroute to 10.100.100.1 (10.100.100.1), 30 hops max, 60 byte packets
 1 10.123.123.1 0.937 ms 1.078 ms 1.154 ms^C
firepower-boot>
```

Étape 9 Pour résoudre les problèmes d'installation, consultez les exemples suivants.

Exemple :

Erreur **« Timed out »** d'expiration du délai

Au moment du téléchargement, si le serveur de fichiers n'est pas accessible, le processus échoue pour cause d'expiration du délai.

```
   ...
Erasing disk0 ...
Verifying

timed out
Upgrade aborted
firepower-boot>
```

Dans ce cas, assurez-vous que le serveur de fichiers est accessible à partir de l'ASA. Vous pouvez le vérifier en envoyant un message Ping au serveur de fichiers.

Erreur **« Package not found »** indiquant un package introuvable

Si le serveur de fichiers est accessible, mais que le chemin ou le nom du fichier est incorrect, l'installation échoue en affichant l'erreur « Package not found » :

```
  ...
Erasing disk0 ...
Verifying

Package not found. Please correct the URL, which should include the full path including
package name.
Upgrade aborted.
firepower-boot>
```

Dans ce cas, assurez-vous que le chemin et le nom de fichier du package Thread Defense sont corrects.

Erreur **Installation failed with unknown error** indiquant qu'une erreur inconnue a provoqué l'échec de l'installation

Si l'installation échoue après le téléchargement du logiciel système, la cause affichée indique souvent « Installation failed with unknown error ». Lorsque cette erreur se produit, vous pouvez résoudre le problème en consultant le journal d'installation :

```
firepower-boot>support view logs

===View Logs===

============================
Directory: /var/log
----------sub-dirs----------
cisco
sa
-----------files------------
2015-09-24 19:56:33.150011 | 102668 | install.log
2015-09-24 19:46:28.400002 | 292292 | lastlog
2015-09-24 19:45:15.510001 | 250 | ntp.log
2015-09-24 19:46:28.400002 | 5760 | wtmp

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s
```

```
Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> install.log
Thu Sep 24 19:53:44 UTC 2015: Begin installation ...
Found hard drive(s): /dev/sda
Erasing files from flash ...
...
```

Vous pouvez également utiliser la même commande afin de consulter les journaux upgrade.log, pyos.log et commandd.log sous /var/log/cisco pour les problèmes liés à l'interface de ligne de commande de démarrage.

Étape 10 Vous pouvez utiliser le gestionnaire d'appareil ou le centre de gestion pour gérer votre appareil. Consultez le guide de démarrage rapide de votre modèle et de votre gestionnaire pour poursuivre la configuration : http://www.cisco.com/go/ftd-asa-quick

Défense contre les menaces→ASA : ASA 5500-X ou ISA 3000

Pour recréer l'image Défense contre les menaces dans le logiciel pour ASA, vous devez accéder à l'invite pour ROMMON. Dans ROMMON, vous devez effacer les disques, puis utiliser TFTP dans l'interface de gestion pour télécharger l'image ASA. Seul le protocole TFTP est pris en charge. Une fois l'ASA rechargé, vous pouvez configurer les paramètres de base, puis charger le logiciel pour le module FirePOWER.

Avant de commencer

- Assurez-vous que la connexion est stable entre l'ASA et le serveur TFTP pour éviter toute perte de paquets.

Procédure

Étape 1 Si vous gérez Défense contre les menaces à partir du centre de gestion, supprimez l'appareil à partir du centre de gestion.

Étape 2 Si vous gérez Défense contre les menaces à l'aide du gestionnaire d'appareil, annulez l'enregistrement de l'appareil sur le serveur Smart Software Licensing , à partir du gestionnaire d'appareil ou du serveur Smart Software Licensing.

Étape 3 Téléchargez l'image ASA (voir Télécharger le logiciel, à la page 18) sur un serveur TFTP auquel Défense contre les menaces a accès dans l'interface de gestion.

Pour les modèles ASA 5506-X, 5508-X, 5516-X, ISA 3000 : vous devez utiliser le port de gestion Management 1/1 afin de télécharger l'image. Pour les autres modèles, vous pouvez utiliser n'importe quelle interface.

Étape 4 Sur le port de la console, redémarrez l'appareil Défense contre les menaces.

reboot

Entrez **yes** (oui) pour le redémarrer.

Exemple :

```
> reboot
This command will reboot the system.  Continue?
```

```
Please enter 'YES' or 'NO': yes
```

Étape 5 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à accéder à l'invite pour ROMMON.

Observez attentivement le moniteur.

Exemple :

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

Appuyez sur la touche **Échap**.

Si le message suivant s'affiche, cela signifie que vous avez attendu trop longtemps. Vous devez alors redémarrer Défense contre les menaces une fois le redémarrage terminé :

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

Étape 6 Effacez tous les disques présents sur Défense contre les menaces. La mémoire flash interne s'appelle « disk0 ». Si vous disposez d'un lecteur USB externe, il portera le nom « disk1 ».

Exemple :

```
Example:
rommon #0> erase disk0:

About to erase the selected device, this will erase
all files including configuration, and images.
Continue with erase? y/n [n]: y

Erasing Disk0:
.......................
[...]
```

Cette étape efface les fichiers Défense contre les menaces pour que l'ASA ne tente pas de charger un fichier de configuration incorrect, ce qui provoquerait de nombreuses erreurs.

Étape 7 Configurez les paramètres réseau et chargez l'image ASA à l'aide des commandes ROMMON suivantes :

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftpdnld

L'image ASA sera téléchargée et l'interface de ligne de commande démarrera.

Consultez les renseignements suivants :

- **interface** (ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X uniquement) : précise l'ID de l'interface. Les autres modèles utilisent toujours l'interface de gestion Management 1/1.
- **set** : affiche les paramètres réseau. Vous pouvez également utiliser la commande **ping** pour vérifier la connectivité avec le serveur.
- **sync** : enregistre les paramètres réseau.
- **tftpdnld** : charge l'image de démarrage.

Exemple :

Exemple pour l'ASA 5555-X :

```
rommon 2 > interface gigabitethernet0/0
rommon 3 > address 10.86.118.4
rommon 4 > netmask 255.255.255.0
rommon 5 > server 10.86.118.21
rommon 6 > gateway 10.86.118.1
rommon 7 > file asalatest-smp-k8.bin
rommon 8 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asalatest-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 9 > sync

Updating NVRAM Parameters...

rommon 10 > tftpdnld
```

Exemple pour l'ASA 5506-X :

```
rommon 2 > address 10.86.118.4
rommon 3 > netmask 255.255.255.0
rommon 4 > server 10.86.118.21
rommon 5 > gateway 10.86.118.21
rommon 6 > file asalatest-lfbff-k8.SPA
```

```
rommon 7 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=asalatest-lfbff-k8.SPA
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 8 > sync

Updating NVRAM Parameters...

rommon 9 > tftpdnld
```

Exemple :

Envoyer un message Ping pour résoudre un problème de connectivité avec le serveur :

```
rommon 1 > ping 10.123.123.2
Sending 10, 32-byte ICMP Echoes to 10.123.123.2 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

Étape 8 Configurez les paramètres réseau et préparez les disques.

Lors du premier démarrage de l'ASA, rien n'est configuré. Vous pouvez alors configurer l'interface de gestion pour permettre l'accès à ASDM en suivant les invites interactives, coller une configuration précédemment enregistrée, ou si vous n'en avez pas, utiliser la configuration recommandée (ci-dessous).

Si vous n'avez aucune configuration enregistrée, nous vous suggérons de coller la configuration recommandée, en particulier si vous prévoyez utiliser le module ASA FirePOWER. Le module ASA FirePOWER, dont la gestion s'effectue dans l'interface de gestion, requiert un accès Internet pour les mises à jour. Le déploiement recommandé du réseau, qui est aussi très simple à effectuer, prévoit l'utilisation d'un commutateur interne pour connecter l'interface de gestion (réservée à la gestion de FirePOWER), l'interface interne (pour la gestion de l'ASA et le trafic interne) et votre PC de gestion au sein du même réseau interne. Pour plus de renseignements sur le déploiement du réseau, consultez le guide de démarrage rapide :

- http://www.cisco.com/go/asa5506x-quick
- http://www.cisco.com/go/asa5508x-quick
- http://www.cisco.com/go/asa5500x-quick

a) À l'invite de la console ASA, vous devrez configurer l'interface de gestion.

```
Pre-configure Firewall now through interactive prompts [yes]?
```

Si vous souhaitez coller une configuration ou créer la configuration recommandée pour un déploiement de réseau simplifié, entrez **no** et poursuivez la procédure.

Si vous souhaitez configurer l'interface de gestion de manière à pouvoir vous connecter à ASDM, entrez **yes** et suivez les invites.

b) À l'invite de la console, accédez au mode d'exécution privilégié.

enable

Le message suivant s'affiche :

```
Password:
```

c) Appuyez sur **Entrée**. Par défaut, le mot de passe est une valeur vide.
d) Accédez au mode de configuration globale.

configure terminal

e) Si vous n'avez pas encore utilisé les invites interactives, copiez et collez votre configuration dans l'invite.

Si vous n'avez pas de configuration enregistrée et que vous souhaitez utiliser la configuration simplifiée décrite dans le guide de démarrage rapide, copiez la configuration suivante à l'invite, en modifiant les adresses IP et les ID d'interface. Si vous avez déjà utilisé les invites, mais que vous préférez utiliser cette configuration, effacez d'abord la configuration existante à l'aide de la commande **clear configure all**.

```
interface gigabitethernetn/n
   nameif outside
   ip address dhcp setroute
   no shutdown
interface gigabitethernetn/n
   nameif inside
   ip address ip_address netmask
   security-level 100
   no shutdown
interface managementn/n
   no shutdown
object network obj_any
   subnet 0 0
   nat (any,outside) dynamic interface
http server enable
http inside_network netmask inside
dhcpd address inside_ip_address_start-inside_ip_address_end inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

Pour l'ASA 5506W-X, ajoutez les éléments suivants pour l'interface Wi-Fi :

```
same-security-traffic permit inter-interface
interface GigabitEthernet 1/9
security-level 100
nameif wifi
ip address ip_address netmask
no shutdown
http wifi_network netmask wifi
dhcpd address wifi_ip_address_start-wifi_ip_address_end wifi
dhcpd enable wifi
```

f) Reformatez les disques :

format disk0:

format disk1:

La mémoire flash interne s'appelle « disk0 ». Si vous disposez d'un lecteur USB externe, il portera le nom « disk1 ». Si vous ne reformatez pas les disques, l'erreur suivante s'affiche au moment où vous essayez de copier l'image ASA :

```
%Error copying ftp://10.86.89.125/asa971-smp-k8.bin (Not enough space on device)
```

g) Enregistrez la nouvelle configuration :

write memory

Étape 9 Installez les images pour ASA et pour ASDM.

Le démarrage de l'ASA en mode ROMMON ne permet pas de conserver l'image du système après un rechargement. Vous devez donc télécharger l'image dans la mémoire flash. Vous devez également télécharger ASDM dans la mémoire flash.

a) Téléchargez les images ASA et ASDM (voir Télécharger le logiciel, à la page 18) sur un serveur auquel l'ASA a accès. L'ASA prend en charge de nombreux types de serveurs. Pour plus de renseignements, consultez la rubrique consacrée à la commande **copy** : http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2171368.

b) Copiez l'image ASA dans la mémoire flash de l'ASA. Cette étape illustre une commande « copy FTP ».

copy ftp://*utilisateur***:***mot de passe***@***server_ip***/***asa_file* **disk0:***asa_file*

Exemple :

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asa961-smp-k8.bin disk0:asa961-smp-k8.bin
```

c) Copiez l'image ASDM dans la mémoire flash de l'ASA. Cette étape illustre une commande « copy FTP ».

copy ftp://*user***:***password***@***server_ip***/***asdm_file* **disk0:***asdm_file*

Exemple :

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asdm-761.bin disk0:asdm-761.bin
```

d) Rechargez l'ASA :

reload

L'ASA se recharge en utilisant l'image copiée dans disk0.

Étape 10 (Facultatif) Installez le logiciel pour le module ASA FirePOWER.

Vous devez installer l'image de démarrage ASA FirePOWER, partitionner le disque SSD et installer le logiciel système en suivant cette procédure.

a) Copiez l'image de démarrage sur l'ASA. Ne transférez pas le logiciel système. Il sera téléchargé ultérieurement sur le disque SSD. Cette étape illustre une commande « copy FTP ».

copy ftp://*utilisateur***:***mot de passe***@***server_ip***/***firepower_boot_file* **disk0:***firepower_boot_file*

Exemple :

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asasfr-5500x-boot-6.0.1.img
disk0:/asasfr-5500x-boot-6.0.1.img
```

b) Téléchargez le package d'installation du logiciel système des services ASA FirePOWER à partir de Cisco.com et transférez-le sur un serveur HTTP, HTTPS ou FTP accessible à partir de l'interface de gestion. Ne le téléchargez pas vers disk0 sur l'ASA.

c) Définissez l'emplacement de l'image de démarrage du module ASA FirePOWER dans ASA disk0 :

sw-module module sfr recover configure image disk0:*file_path*

Exemple :

```
ciscoasa# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-6.0.1.img
```

d) Chargez l'image de démarrage ASA FirePOWER :

sw-module module sfr recover boot

Exemple :

```
ciscoasa# sw-module module sfr recover boot

Module sfr will be recovered. This may erase all configuration and all data
on that device and attempt to download/install a new image for it. This may take
several minutes.

Recover module sfr? [confirm] y
Recover issued for module sfr.
```

e) Patientez quelques minutes, le temps que le module ASA FirePOWER démarre, puis ouvrez une session sur la console pour accéder à l'image de démarrage ASA FirePOWER désormais en cours d'exécution. Vous devrez peut-être appuyer sur **Entrée** après avoir ouvert la session pour accéder à l'invite de connexion. Le nom d'utilisateur par défaut est **admin** et le mot de passe par défaut **Admin123**.

Exemple :

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

asasfr login: admin
Password: Admin123
```

Si le démarrage du module n'est pas terminé, la commande « session » échoue et un message vous informe qu'il est impossible de se connecter par l'entremise de ttyS1. Attendez et réessayez.

a) Configurez le système pour ainsi pouvoir installer le package d'installation du logiciel système.

setup

Vous êtes invité à fournir les informations suivantes. Notez que l'adresse de gestion et la passerelle, ainsi que les informations DNS, sont les principaux paramètres à configurer.

- Nom de domaine : un maximum de 65 caractères alphanumériques, sans espace. Les traits d'union sont autorisés.
- Adresse réseau : vous pouvez définir une adresse IPv4 ou IPv6 statique, ou utiliser la configuration automatique sans état DHCP (pour IPv4) ou IPv6.

- Informations DNS : vous devez indiquer au moins un serveur DNS, et vous pouvez également définir le nom de domaine et le domaine de recherche.
- Informations NTP : vous pouvez activer le protocole NTP et configurer les serveurs NTP pour régler l'horloge du système.

Exemple :

```
asasfr-boot> setup

                Welcome to Cisco FirePOWER Services Setup
                          [hit Ctrl-C to abort]
                        Default values are inside []
```

a) Installez le package d'installation du logiciel système :

system install [**noconfirm**] *url*

Incluez l'option **noconfirm** si vous ne souhaitez pas répondre aux messages de confirmation. Utilisez une URL HTTP, HTTPS ou FTP. Si un nom d'utilisateur et un mot de passe sont exigés, vous serez invité à les fournir. Ce fichier est volumineux et son téléchargement peut prendre un certain temps, selon le réseau.

Une fois l'installation terminée, le système redémarre. Le temps nécessaire à l'installation des composants applicatifs et au démarrage des services ASA FirePOWER est très variable : 10 minutes ou plus pour les plateformes haut de gamme, et de 60 à 80 minutes ou plus pour les plateformes bas de gamme. (La sortie **show module sfr** doit indiquer que tous les processus sont en cours.)

Exemple :

```
asasfr-boot> system install
http://admin:pa$$wd@upgrades.example.com/packages/asasfr-sys-6.0.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 6.0.1-58 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system. [type
Enter]
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2016):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

a) Si nécessaire, vous pourrez installer une version corrigée ultérieurement à partir de votre gestionnaire : ASDM ou centre de gestion.

Étape 11 Procurez-vous une licence de cryptage renforcé et d'autres licences pour un ASA existant dont vous n'avez pas enregistré la clé d'activation : voir http://www.cisco.com/go/license. Accédez à la section **Gérer** > **les licences** pour télécharger à nouveau vos licences.

Pour utiliser ASDM (et de nombreuses autres fonctionnalités), vous devez installer la licence de cryptage renforcé (3DES/AES). Si vous avez enregistré la clé d'activation de la licence relative à cet ASA avant de procéder à la recréation d'image sur l'appareil Thread Defense, vous pouvez réinstaller cette clé. Si vous n'avez pas enregistré la clé d'activation, mais que vous possédez des licences pour cet ASA, vous pouvez à nouveau les télécharger. Pour un nouvel ASA, vous devrez demander de nouvelles licences ASA.

Étape 12 Procurez-vous des licences pour un nouvel ASA.

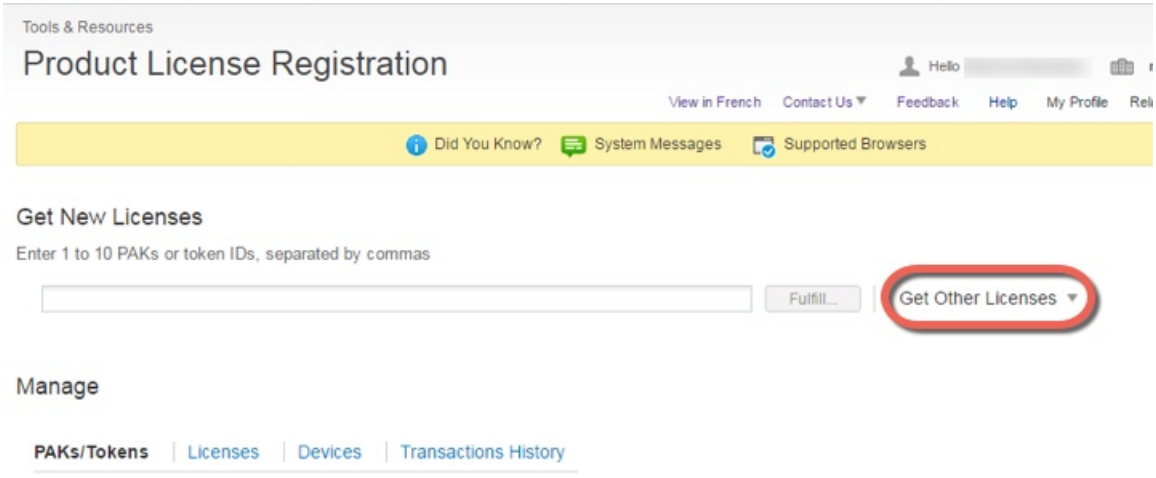
a) Utilisez la commande suivante pour obtenir le numéro de série de votre ASA :

show version | grep Serial

Ce numéro de série est différent de celui du châssis indiqué à l'extérieur du matériel. Le numéro de série du châssis est utilisé pour l'assistance technique, mais pas pour les licences.

b) Accédez à la page http://www.cisco.com/go/license et cliquez sur **Get Other Licenses** (obtenir d'autres licences).

Illustration 1 : Get Other Licenses (obtenir d'autres licences)

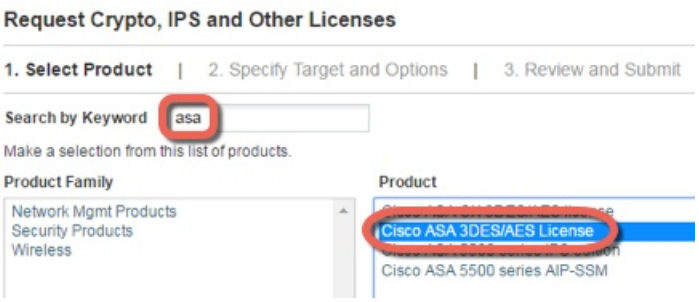


c) Choisissez **IPS, Crypto, Other**.

Illustration 2 : IPS, Crypto, Othe (IPS, cryptage, autre)

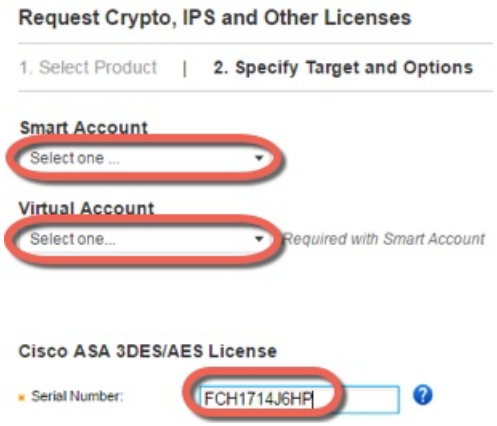
d) Dans le champ de recherche par mot-clé **Search by Keyword** (rechercher par mot clé), entrez **asa** et sélectionnez la licence **Cisco ASA 3DES/AES License**.

Illustration 3 : Licence Cisco ASA 3DES/AES



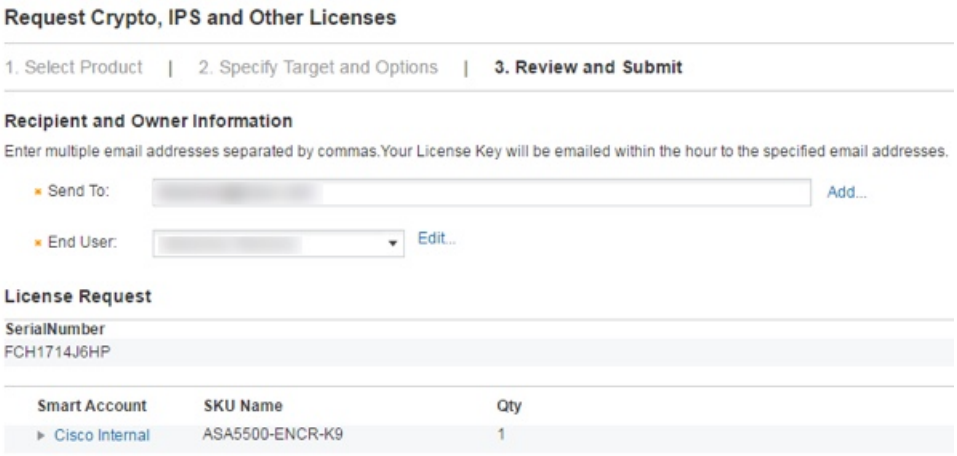
e) Sélectionnez votre compte Smart (**Smart Account**) et votre compte virtuel (**Virtual Account**), entrez le numéro de série (**Serial Number**) de l'ASA, puis cliquez sur **Next** (suivant) pour passer à l'étape suivante.

Illustration 4 : Smart Account (compte Smart), Virtual Account (compte virtuel) et Serial Number (numéro de série)



f) L'adresse courriel du destinataire et le nom de l'utilisateur final sont automatiquement remplis. Si nécessaire, entrez les autres adresses courriel requises. Cochez la case **I Agree** (j'accepte) pour indiquer votre accord, puis cliquez sur **Submit** (envoyer) pour envoyer le tout.

Illustration 5 : Submit (envoyer)



g) Vous recevrez alors un courriel contenant la clé d'activation, mais vous pouvez aussi la télécharger immédiatement depuis la zone de gestion des licences **Manage (gérer)** > **Licenses (licences)**.

h) Si vous souhaitez procéder à une mise à niveau de la licence de base vers la licence Security Plus, ou acheter une licence AnyConnect, consultez la page http://www.cisco.com/go/ccw. Après avoir acheté une licence, vous recevrez un courriel contenant une clé d'autorisation de produit (PAK) que vous pourrez entrer sur la page www.cisco.com/go/license. Pour les licences AnyConnect, vous recevez une clé PAK multiutilisation que vous pourrez appliquer à plusieurs ASA partageant le même ensemble de séances de l'utilisateur. La clé d'activation obtenue comprend toutes les fonctionnalités que vous avez enregistrées jusqu'à présent pour les licences permanentes, y compris la licence 3DES/AES. En ce qui concerne les licences à durée déterminée, chacune possède une clé d'activation distincte.

Étape 13 Indiquez la clé d'activation.

activation-key *key*

Exemple :

```
ciscoasa(config)# activation-key 7c1aff4f e4d7db95 d5e191a4 d5b43c08 0d29c996
Validating activation key. This may take a few minutes...
Failed to retrieve permanent activation key.
Both Running and Flash permanent activation key was updated with the requested key.
```

Étant donné qu'aucune clé d'activation n'était encore installée pour cet ASA, le message « Failed to retrieve permanent activation key » indiquant l'échec de la récupération de la clé d'activation permanente s'affiche. Vous pouvez ignorer ce message.

Vous ne pouvez installer qu'une seule clé permanente. En revanche, vous pouvez installer plusieurs clés à durée déterminée. Si vous entrez une nouvelle clé permanente, celle-ci remplacera la clé déjà installée. Si vous avez commandé d'autres licences après avoir installé la licence 3DES/AES, la clé d'activation combinée englobe toutes ces licences ainsi que la licence 3DES/AES, ce qui vous permet de remplacer la clé dédiée pour la licence 3DES/AES.

Étape 14 Le module ASA FirePOWER utilise un mécanisme de gestion des licences distinct de celui de l'ASA. Aucune licence n'est préinstallée, mais selon votre commande, la boîte peut contenir une clé PAK vous permettant d'obtenir une clé d'activation pour les licences suivantes :

- **Contrôle et protection**. Le contrôle est également connu sous le nom d'« AVC » (Application Visibility and Control, ou Visibilité et contrôle d'application) ou « Applications ». Quant à la protection, elle porte également le nom « IPS » (ou Système de prévention des intrusions). En plus de la clé d'activation de ces licences, vous avez également besoin d'abonnements de type « droit d'utilisation » pour la mise à jour automatisée de ces fonctionnalités.

  Les mises à jour du **Contrôle** (AVC) sont incluses dans un contrat de service d'assistance Cisco.

  Les mises à jour de la **Protection** (IPS) nécessitent un abonnement IPS que vous pouvez obtenir sur la page http://www.cisco.com/go/ccw. Cet abonnement donne droit aux mises à jour pour les règles, les moteurs, les vulnérabilités et la géolocalisation. **Remarque** : un abonnement de type « droit d'utilisation » ne génère ni ne requiert aucune clé PAK/clé d'activation de licence pour le module ASA FirePOWER. Il donne simplement le droit d'utiliser les mises à jour.

Si vous n'avez pas acheté l'ASA 5500-X avec les services ASA FirePOWER, vous pouvez acheter une offre groupée de mise à niveau pour obtenir les licences nécessaires. Pour plus de renseignements, consultez le Guide de commande des pare-feu Cisco ASA avec services FirePOWER.

Vous pouvez également acheter les licences suivantes :

- **Licence Cisco Secure Firewall Threat Defense Malware Defense**
- **Licence Cisco Secure Firewall Threat Defense URL Filtering**

Ces licences génèrent une clé PAK/clé d'activation de licence pour le module ASA FirePOWER. Pour plus de renseignements sur le processus de commande, consultez le Guide de commande des pare-feu Cisco ASA avec services FirePOWER. Consultez également la section Licences de fonctionnalités de Cisco Secure Firewall Management Center.

Pour installer les licences de contrôle et de protection, ainsi que d'autres licences facultatives, consultez le guide de démarrage rapide ASA correspondant à votre modèle.

Défense contre les menaces→Défense contre les menaces : ASA 5500-X ou ISA 3000

Cette procédure explique comment utiliser ROMMON pour recréer l'image d'une instance existante de Défense contre les menaces dans une nouvelle version du logiciel Défense contre les menaces. Cette procédure restaure les paramètres d'usine de l'appareil. Si vous préférez effectuer une mise à niveau classique, consultez plutôt le guide de mise à niveau.

Dans ROMMON, vous devez utiliser TFTP dans l'interface de gestion pour télécharger la nouvelle image de démarrage Défense contre les menaces. Seul le protocole TFTP est pris en charge. L'image de démarrage peut ensuite télécharger le package d'installation du logiciel système Défense contre les menaces à l'aide de HTTP ou de FTP. Le téléchargement par TFTP peut prendre beaucoup de temps. Assurez-vous d'avoir une connexion stable entre le Défense contre les menaces et le serveur TFTP pour éviter toute perte de paquets.

Procédure

Étape 1 Si vous gérez Défense contre les menaces à l'aide du centre de gestion, supprimez l'appareil à partir du centre de gestion.

Étape 2 Si vous gérez Défense contre les menaces à l'aide du gestionnaire d'appareil, annulez l'enregistrement de l'appareil sur le serveur Smart Software Licensing , à partir du gestionnaire d'appareil ou du serveur Smart Software Licensing.

Étape 3 Téléchargez l'image de démarrage Défense contre les menaces (voir Télécharger le logiciel, à la page 18) sur un serveur TFTP auquel Défense contre les menaces a accès dans l'interface de gestion.

Pour les modèles ASA 5506-X, 5508-X, 5516-X, ISA 3000 : vous devez utiliser le port de gestion Management 1/1 afin de télécharger l'image. Pour les autres modèles, vous pouvez utiliser n'importe quelle interface.

Étape 4 Téléchargez le package d'installation du logiciel système Défense contre les menaces (voir Télécharger le logiciel, à la page 18) sur un serveur HTTP ou FTP auquel Défense contre les menaces a accès dans l'interface de gestion.

Étape 5 Sur le port de la console, redémarrez l'appareil Thread Defense.

reboot

Exemple :

Entrez **yes** (oui) pour le redémarrer.

Exemple :

```
> reboot
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO': yes
```

Étape 6 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à accéder à l'invite pour ROMMON.

Observez attentivement le moniteur.

Exemple :

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

Appuyez sur la touche **Échap**.

Si le message suivant s'affiche, cela signifie que vous avez attendu trop longtemps. Vous devez alors recharger Défense contre les menaces, une fois le démarrage terminé :

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

Étape 7 Effacez tous les disques sur Défense contre les menaces. La mémoire flash interne s'appelle « disk0 ». Si vous disposez d'un lecteur USB externe, il portera le nom « disk1 ».

Exemple :

```
Example:
rommon 1 > erase disk0:
erase: Erasing 7583 MBytes ...................................

rommon 2 >
```

Cette étape efface les anciennes images de démarrage et images du système Défense contre les menaces. Si vous n'effacez pas l'image du système, n'oubliez pas de quitter le processus de démarrage après avoir chargé celle-ci à l'étape suivante, sinon Défense contre les menaces chargera l'ancienne image du système Défense contre les menaces, ce qui peut être long et vous obligera à tout recommencer.

Étape 8 Configurez les paramètres réseau et chargez la nouvelle image de démarrage à l'aide des commandes ROMMON suivantes :

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file *path/filename*

set

sync

tftpdnld

L'image de démarrage Thread Defense est téléchargée et l'interface de ligne de commande démarre.

Remarque
Si vous n'avez pas effacé le disque à l'étape précédente, vous devez appuyer sur la touche **Échap** pour accéder à l'interface de ligne de commande de démarrage :

```
============================================
Use ESC to interrupt boot and launch boot CLI.
Use SPACE to launch Cisco FTD immediately.
Cisco FTD launch in 24 seconds ...
Launching boot CLI ...
...
```

Consultez les renseignements suivants :

- **interface** (ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X uniquement) : précise l'ID de l'interface. Les autres modèles utilisent toujours l'interface de gestion Management 1/1.
- **set** : affiche les paramètres réseau. Vous pouvez également utiliser la commande **ping** pour vérifier la connectivité avec le serveur.
- **sync** : enregistre les paramètres réseau.
- **tftpdnld** : charge l'image de démarrage.

Exemple :

Exemple pour l'ASA 5508-X :

```
rommon 0 > address 10.86.118.4
rommon 1 > netmask 255.255.255.0
rommon 2 > server 10.86.118.1
rommon 3 > gateway 10.86.118.21
rommon 4 > file ftd-boot-latest.lfbff
rommon 5 > set
    ADDRESS=10.86.118.4
    NETMASK=255.255.255.0
    GATEWAY=10.86.118.1
    SERVER=10.86.118.21
    IMAGE=ftd-boot-latest.lfbff
    CONFIG=
    PS1="rommon ! > "


rommon 6 > sync
rommon 7 > tftpdnld
             ADDRESS: 10.86.118.4
             NETMASK: 255.255.255.0
             GATEWAY: 10.86.118.1
              SERVER: 10.86.118.21
               IMAGE: ftd-boot-latest.lfbff
             MACADDR: 84:b2:61:b1:92:e6
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: GbE/1
             PHYMODE: Auto Detect

IP: Detected unsupported IP packet fragmentation.  Try reducing TFTP_BLKSIZE.
IP: Retrying with a TFTP block size of 512..
Receiving ftd-boot-99.15.1.178.lfbff from 10.19.41.228!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Exemple pour l'ASA 5555-X :

```
rommon 0 > interface gigabitethernet0/0
rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.255.0
rommon 3 > server 10.86.118.21
rommon 4 > gateway 10.86.118.1
rommon 5 > file ftd-boot-latest.cdisk
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  NETMASK=255.255.255.0
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=ftd-boot-latest.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon 7 > sync
```

```
Updating NVRAM Parameters...

rommon 8 > tftpdnld
```

Envoyer un message Ping pour résoudre un problème de connectivité avec le serveur :

```
rommon 1 > ping 10.123.123.2
Sending 10, 32-byte ICMP Echoes to 10.123.123.2 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

Étape 9 Entrez **setup** et configurez les paramètres réseau de l'interface de gestion pour établir une connectivité temporaire avec le serveur HTTP ou FTP, ce qui vous permettra de télécharger et d'installer le package système.

Remarque
Si vous disposez d'un serveur DHCP, Thread Defense définit automatiquement la configuration réseau. Consultez les exemples de messages de démarrage suivants si vous utilisez DHCP :

```
Configuring network interface using DHCP
Bringing up network interface.
Depending on your network, this might take a couple of minutes when using DHCP...
ifup: interface lo already configured
Using IPv4 address: 10.123.123.123
Using IPv6 address: fe80::2a0:c9ff:fe00:0
Using DNS server: 64.102.6.247
Using DNS server: 173.36.131.10
Using default gateway: 10.123.123.1
```

Exemple :

```
                    Cisco FTD Boot 6.3.0
                 Type ? for list of commands
firepower-boot>
firepower-boot>setup


 Welcome to Cisco FTD Setup
 [hit Ctrl-C to abort]
 Default values are inside []

Enter a hostname [firepower]: example.cisco.com
Do you want to configure IPv4 address on management interface?(y/n) [Y]: y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]:
n
Enter an IPv4 address: 10.123.123.123
Enter the netmask: 255.255.255.0
Enter the gateway: 10.123.123.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: n
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address [64.102.6.247]: 10.123.123.2
Do you want to configure Secondary DNS Server? (y/n) [y]: n
Any previously configured secondary DNS servers will be removed.
Do you want to configure Local Domain Name? (y/n) [n]: n
Do you want to configure Search domains? (y/n) [y]: n
Any previously configured search domains will be removed.
```

```
Do you want to enable the NTP service? [N]: n
Please review the final configuration:
Hostname: example.cisco.com
Management Interface Configuration

IPv4 Configuration: static
 IP Address: 10.123.123.123
 Netmask: 255.255.255.0
 Gateway: 10.123.123.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
 DNS Server:
 10.123.123.2

NTP configuration: Disabled

CAUTION:
You have selected IPv6 stateless autoconfiguration, which assigns a global address
based on network prefix and a device identifier. Although this address is unlikely
to change, if it does change, the system will stop functioning correctly.
We suggest you use static addressing instead.

Apply the changes?(y,n) [Y]: y
Configuration saved successfully!
Applying...
Restarting network services...
Done.
Press ENTER to continue...
firepower-boot>
```

Étape 10 Téléchargez le package d'installation du logiciel système Thread Defense. Cette étape illustre une installation avec HTTP.

system install [**noconfirm**] *url*

Incluez l'option **noconfirm** si vous ne souhaitez pas répondre aux messages de confirmation.

Exemple :

```
> system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg
```

Vous êtes invité à effacer le lecteur flash interne. Entrez **y**.

```
######################## WARNING #############################
# The content of disk0: will be erased during installation! #
############################################################

Do you want to continue? [y/N] y
```

Le processus d'installation efface le lecteur flash et télécharge l'image du système. Vous êtes invité à poursuivre l'installation. Entrez **y**.

```
Erasing disk0 ...
Verifying
Downloading
Extracting
Package Detail
```

```
 Description: Cisco ASA-NGFW 6.3.0 System Install
 Requires reboot: Yes

Do you want to continue with upgrade? [y]: y
```

Une fois l'installation terminée, appuyez sur **Entrée** pour redémarrer l'appareil.

```
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

Le redémarrage prendra au moins 30 minutes et même beaucoup plus. Au redémarrage, vous accéderez à l'interface de ligne de commande Thread Defense.

Étape 11 Pour résoudre les problèmes de connectivité du réseau, consultez les exemples suivants.

Exemple :

Visualiser la configuration de l'interface réseau :

```
firepower-boot>show interface
eth0 Link encap:Ethernet HWaddr 00:a0:c9:00:00:00
 inet addr:10.123.123.123 Bcast:10.123.123.255 Mask:255.255.255.0
 inet6 addr: fe80::2a0:c9ff:fe00:0/64 Scope:Link
 inet6 addr: 2001:420:270d:1310:2a0:c9ff:fe00:0/64 Scope:Global
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:522369 errors:0 dropped:0 overruns:0 frame:0
 TX packets:2473 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:42120849 (40.1 MiB) TX bytes:170295 (166.3 KiB)
...
```

Envoyer un message Ping à un serveur :

```
firepower-boot>ping www.example.com
PING www.example.com (10.125.29.106) 56(84) bytes of data.
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=1 ttl=42 time=28.8 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=2 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=3 ttl=42 time=28.1 ms
64 bytes from qg-in-f106.1e100.net (74.125.29.106): icmp_seq=4 ttl=42 time=29.0 ms
^C
--- www.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 28.159/28.549/29.022/0.437 ms

firepower-boot>
```

Activer Traceroute pour tester la connectivité du réseau :

```
firepower-boot>traceroute -n 10.100.100.1
traceroute to 10.100.100.1 (10.100.100.1), 30 hops max, 60 byte packets
 1 10.123.123.1 0.937 ms 1.078 ms 1.154 ms^C
firepower-boot>
```

Étape 12 Pour résoudre les problèmes d'installation, consultez les exemples suivants.

Exemple :

Erreur **« Timed out »** d'expiration du délai

Au moment du téléchargement, si le serveur de fichiers n'est pas accessible, le processus échoue pour cause d'expiration du délai.

```
   ...
Erasing disk0 ...
Verifying

timed out
Upgrade aborted
firepower-boot>
```

Dans ce cas, assurez-vous que le serveur de fichiers est accessible à partir de l'ASA. Vous pouvez le vérifier en envoyant un message Ping au serveur de fichiers.

Erreur **« Package not found »** indiquant un package introuvable

Si le serveur de fichiers est accessible, mais que le chemin ou le nom du fichier est incorrect, l'installation échoue en affichant l'erreur « Package not found » :

```
  ...
Erasing disk0 ...
Verifying

Package not found. Please correct the URL, which should include the full path including
package name.
Upgrade aborted.
firepower-boot>
```

Dans ce cas, assurez-vous que le chemin et le nom de fichier du package Thread Defense sont corrects.

Erreur **Installation failed with unknown error** indiquant qu'une erreur inconnue a provoqué l'échec de l'installation

Si l'installation échoue après le téléchargement du logiciel système, la cause affichée indique souvent « Installation failed with unknown error ». Lorsque cette erreur se produit, vous pouvez résoudre le problème en consultant le journal d'installation :

```
firepower-boot>support view logs

===View Logs===

============================
Directory: /var/log
----------sub-dirs----------
cisco
sa
-----------files------------
2015-09-24 19:56:33.150011 | 102668 | install.log
2015-09-24 19:46:28.400002 | 292292 | lastlog
2015-09-24 19:45:15.510001 | 250 | ntp.log
2015-09-24 19:46:28.400002 | 5760 | wtmp

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s
```

```
Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> install.log
Thu Sep 24 19:53:44 UTC 2015: Begin installation ...
Found hard drive(s): /dev/sda
Erasing files from flash ...
...
```

Vous pouvez également utiliser la même commande afin de consulter les journaux upgrade.log, pyos.log et commandd.log sous /var/log/cisco pour les problèmes liés à l'interface de ligne de commande de démarrage.

Étape 13 Vous pouvez utiliser le gestionnaire d'appareil ou le centre de gestion pour gérer votre appareil. Consultez le guide de démarrage rapide de votre modèle et de votre gestionnaire pour poursuivre la configuration : http://www.cisco.com/go/ftd-asa-quick

ASA→ASA : ASA 5500-X ou ISA 3000

Si l'appareil ne parvient pas à démarrer, vous pouvez démarrer avec l'image ROMMON. Vous pouvez ensuite télécharger un nouveau fichier image dans la mémoire flash à partir du système d'exploitation de l'ASA.

Procédure

Étape 1 Mettez l'ASA hors tension, puis rallumez-le.

Étape 2 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 3 En mode ROMMON, définissez les paramètres d'interface avec l'ASA, notamment l'adresse IP, l'adresse du serveur TFTP, l'adresse de la passerelle, le fichier d'image logicielle et le port, comme suit :

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

Remarque
Assurez-vous que la connexion au réseau est déjà établie.

Sur les plateformes ASA 5506-X, ASA 5508-X, ASA 5516-X et ISA 3000, la commande **interface** ne fonctionne pas, ce qui oblige à utiliser l'interface Management 1/1 pour la récupération TFTP.

Étape 4 Validez les paramètres :

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
```

```
  RETRY=20
```

Étape 5 Envoyez un message Ping au serveur TFTP :

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

Étape 6 Enregistrez les paramètres réseau pour une utilisation ultérieure :

```
rommon #8> sync
Updating NVRAM Parameters...
```

Étape 7 Chargez l'image logicielle :

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

Une fois l'image logicielle chargée, l'ASA quitte automatiquement le mode ROMMON.

Étape 8 Le démarrage de l'ASA en mode ROMMON ne permet pas de conserver l'image du système après un rechargement. Vous devez donc télécharger l'image dans la mémoire flash. Consultez le Guide de mise à niveau de Cisco ASA pour accéder aux procédures de mise à niveau complètes.

Prochaines étapes?

Consultez le guide de démarrage rapide correspondant à votre modèle et à votre application de gestion :

- ASA 5506-X
  - ASA 5506-X pour Firepower Device Manager
  - ASA 5506-X pour Firepower Management Center

    - ASA 5506-X pour ASA
- ASA 5508-X/5516-X
- ASA 5512-X à ASA 5555-X
    - ASA 5512-X à ASA 5555-X pour Firepower Device Manager
    - ASA 5512-X à ASA 5555-X pour Firepower Management Center
    - ASA 5512-X à ASA 5555-X pour ASA
- Firepower 1010
- Firepower 1100
- Firepower 2100
- Secure Firewall 3100
- Secure Firewall 4200
- ISA 3000

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.