

Réinstallez un pare-feu sécurisé de défense contre les menaces pour les gammes 1000, 2100 et 3100

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Avant de commencer](#)

[Configurer](#)

[Validation](#)

Introduction

Ce document décrit un exemple de procédure de réinstallation pour Secure Firewall Threat Defense (anciennement Firepower Threat Defense).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Il n'existe aucune exigence spécifique pour ce guide

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Threat Defense 2110 (FTD) version 7.2.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les exigences spécifiques de ce document sont les suivantes :

- Un câble de console connecté au FTD
- Un serveur TFTP avec le package d'installation (.SPA) déjà chargé

Cette procédure de réinstallation est prise en charge sur les appliances :

- Cisco Secure Firewall Threat Defense 1000
- Cisco Secure Firewall Threat Defense, série 2100
- Cisco Secure Firewall Threat Defense, série 3100

Avant de commencer

- Une procédure de réinstallation efface toutes les configurations précédentes. Pour restaurer des configurations, générez une sauvegarde avant de commencer cette procédure.
- Cette procédure s'applique uniquement aux pare-feu exécutant le logiciel FTD.
- Vérifiez que le modèle est compatible avec cette procédure.

Configurer

Étape 1. Formatez l'appliance :

- I. Connectez-vous au port de console de votre appliance et créez une connexion console.
- II. Connectez-vous à l'ILC du châssis FXOS.
- III. Tapez **connect local-mgmt** pour accéder à la console de gestion.
- III. Utilisez la commande **format everything** pour supprimer toutes les configurations et les images de démarrage sur l'appliance.
- III. Tapez **yes** pour confirmer la procédure

```
firepower-2110# connect local-mgmt admin
firepower-2110(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

Étape 2. Interrompez le processus de démarrage en appuyant sur la touche ESC pour passer en mode ROMMON :

```
*****
Cisco System ROMMON, Version 1.0.12, RELEASE SOFTWARE
Copyright (c) 1994-2019 by Cisco Systems, Inc.
Compiled Mon 06/17/2019 16:23:23.36 by builder
*****

Current image running: Boot ROM0
Last reset cause: ResetRequest (0x00001000)
DIMM_1/1 : Present
DIMM_2/1 : Absent

Platform FPR-2110 with 16384 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 18:59:f5:d9:6a:00

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 >
```

Étape 3. Remplissez les paramètres de réseau et de stockage distant avec vos configurations pour préparer le téléchargement TFTP :

I. Les paramètres à remplir sont les suivants :

- A. ADDRESS=*adresse_ip*
- B. NETMASK=*masque_reseau*
- C. GATEWAY=*ip_passerelle*
- D. SERVER=*serveur_stockage_distant*
- E. IMAGE=*chemin_vers_le_fichier*

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 > ADDRESS=10.122.187.166
rommon 2 > NETMASK=255.255.255.224
rommon 3 > GATEWAY=10.122.187.161
rommon 4 > SERVER=10.207.204.10
rommon 5 > IMAGE=cisco-ftd-fp2k.7.2.4-165.SPA
rommon 6 > █
```

 **Attention** : le mode ROMMON prend en charge le protocole TFTP et les protocoles USB, FTP, SCP et SFTP ne sont pas pris en charge lors du processus de démarrage initial.

Étape 7. Une fois que le système est activé, connectez-vous au périphérique à l'aide des informations d'identification par défaut (admin/Admin123) et modifiez le mot de passe de l'appliance :

```
firepower-2110 login: admin
Password:
Successful login attempts for user 'admin' : 1
Enter new password:
Confirm new password:
Your password was updated successfully.
```

 **Remarque** : cette erreur peut s'afficher pendant la configuration initiale. Cependant, elle sera effacée après l'installation du logiciel de défense contre les menaces, comme décrit dans les étapes suivantes.

```
Jun 14 21:37:17 firepower-2110 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>> [F1309][critical][default-i
nfra-version-missing][org-root/fw-infra-pack-default] Bundle version in firmware package is empty, need to
re-install
```

Étape 8. Configurez l'adresse IP de l'interface de gestion :

- I. Accédez à l'étendue du fabric à l'aide de la commande **scope fabric-interconnect a**
- II. Définissez la configuration IP de gestion avec la commande **set out-of-band static ip ip netmask netmask gw gateway**

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # set out-of-band static ip 10.122.187.168 netmask 255.255.255.224 gw
10.122.187.161
Warning: when committed, this change may disconnect the current CLI session.
Use commit-buffer command to commit the changes.
firepower-2110 /fabric-interconnect* # commit-buffer
```

Étape 9. Téléchargez le package d'installation Threat Defense :

- I. Passez à la portée du micrologiciel avec la commande **scope firmware**
- II. Téléchargez le package d'installation :
 - R. Si vous utilisez une clé USB, vous pouvez utiliser la commande **download image usbA : package_name**
 - B. Si vous utilisez un serveur de stockage distant pris en charge, vous pouvez utiliser la commande **download image tftp/ftp/scp/sftp://path_to_your_package**

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.207.204.10/cisco-ftd-fp2k.7.2.4-165.SPA
firepower-2110 /firmware # █
```

 **Remarque** : lorsque vous utilisez des serveurs de stockage distants, vous devez utiliser des chemins absolus sur la syntaxe de la commande, comme indiqué dans l'exemple.

Étape 10. Validez la progression du téléchargement à l'aide de la commande **show download-task** :

```
firepower-2110 /firmware # show download-task
```

Download task:						
File Name	Protocol	Server	Port	Userid	State	
cisco-ftd-fp2k.7.2.4-165.SPA	Tftp	10.207.204.10		0	Downloaded	

 **Remarque** : une fois que l'état de téléchargement passe à *Téléchargé*, vous pouvez passer à l'étape suivante.

Étape 11. Vérifiez que le package figure déjà dans la liste des microprogrammes avec la commande `show package` :

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

Name	Package-Vers
cisco-ftd-fp2k.7.2.4-165.SPA	7.2.4-165

 **Remarque** : copiez la *version* du *package* telle qu'elle sera utilisée lors de l'installation du logiciel Threat Defense.

Étape 12. Installez le logiciel Threat Defense pour finaliser la réinstallation :

- I. Passez à l'étendue d'installation avec la commande **scope auto-install**.
- II. Procédez à l'installation du logiciel de défense contre les menaces avec la commande **install security-pack version *version* force**
- III. Deux invites de confirmation vont apparaître sur la console. Confirmez-les en tapant **yes**.

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 7.2.4 force
```

Invalid software pack
Please contact technical support for help 5

The system is currently installed with security software package not set, which has:
- The platform version: not set
If you proceed with the upgrade 7.2.4-165, it will do the following:
- upgrade to the new platform version 2.12.0.499
- install with CSP ftd version 7.2.4.165
During the upgrade, the system will be reboot

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

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

Triggered the install of software package version 7.2.4-165
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.

 **Attention** : le processus de réinstallation peut prendre jusqu'à 45 minutes. Sachez que le pare-feu va redémarrer pendant l'installation.

Validez le processus de mise à niveau avec la commande **show detail** :

```
firepower-2110 /firmware/auto-install # show detail
Firmware Auto-Install:
  Package-Vers: 7.2.4-165
  Oper State: Scheduled
  Installation Time: 2023-06-14T22:07:28.777
  Upgrade State: Validating Images
  Upgrade Status: validating the software package
  Validation Software Pack Status:
  Firmware Upgrade Status: Ok
  Firmware Upgrade Message:
  Current Task: Validating the application pack(FSM-STAGE:sam:dme:FirmwareSystemDeploy:ValidateApplicationPack)
firepower-2110 /firmware/auto-install # █
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.