

# Recreación de imágenes de una defensa segura frente a amenazas de firewall para las series 1000, 2100 y 3100

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Antes de comenzar](#)

[Configurar](#)

[Validación](#)

## Introducción

Este documento describe un ejemplo de un procedimiento de recreación de imágenes para Secure Firewall Threat Defence (anteriormente Firepower Threat Defense).

## Prerequisites

## Requirements

Cisco recomienda conocer estos temas:

- No hay requisitos específicos para esta guía

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Firewall Threat Defence 2110 (FTD) versión 7.2.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Los requisitos específicos para este documento incluyen:

- Un cable de consola conectado al FTD
- Un servidor TFTP con el paquete de instalación (.SPA) ya cargado

Este procedimiento de recreación de imágenes es compatible con los dispositivos:

- Cisco Secure Firewall Threat Defence serie 1000
- Cisco Secure Firewall Threat Defence serie 2100
- Cisco Secure Firewall Threat Defence serie 3100

## Antes de comenzar

1. Un procedimiento de recreación de imágenes borra todas las configuraciones anteriores. Para restaurar cualquier configuración, genere una copia de seguridad antes de iniciar este procedimiento.
2. Este procedimiento sólo se aplica a los firewalls que ejecutan el software FTD.
3. Compruebe que el modelo es compatible con este procedimiento.

## Configurar

### Paso 1. Formatear el dispositivo:

- I. Conéctese al puerto de consola de su dispositivo y cree una conexión de consola.
- II. Inicie sesión en la CLI del chasis FXOS.
- III. Escriba **connect local-mgmt** para pasar a la consola de administración.
- III. Utilice el comando **format everything** para eliminar todas las configuraciones e imágenes de arranque en el dispositivo.
- III. Escriba **sí** para confirmar el procedimiento

```
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
```

### Paso 2. Interrumpa el proceso de arranque presionando la tecla ESC para ingresar al modo 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 >
```

### Paso 3. Llene los parámetros de red y almacenamiento remoto con sus configuraciones para prepararse para la descarga de TFTP:

- I. Los parámetros que deben rellenarse son:
  - A. ADDRESS=*ip\_address*
  - B. NETMASK=*máscara de red*
  - C. GATEWAY=*gateway\_ip*

D. SERVER=*remote\_storage\_server*

E. IMAGE=*ruta\_al\_archivo*

```
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 > █
```

---

**Precaución:** El modo ROMMON sólo admite el protocolo TFTP, FTP, SCP y SFTP y USB no se admiten en el proceso de arranque inicial.

---

**Paso 4.** Escriba **set** para confirmar las configuraciones proporcionadas:

```
rommon 6 > set
ADDRESS=10.122.187.166
NETMASK=255.255.255.224
GATEWAY=10.122.187.161
SERVER=10.207.204.10
IMAGE=cisco-ftd-fp2k.7.2.4-165.SPA
CONFIG=
PS1="rommon ! > "
```

---

**Nota:** Valide que la información proporcionada es correcta y, si observa un error, ajuste el parámetro y el tipo **establecido de nuevo**.

---

**Paso 5.** Escriba **sync** para aplicar las configuraciones de red y almacenamiento remoto:

```
rommon 7 > sync
rommon 8 >
```

**Paso 6.** Inicie el proceso de arranque con el comando **tftp -b:**

```
rommon 8 > tftp -b
Enable boot bundle: tftp_reqsize = 268435456

ADDRESS: 10.122.187.166
NETMASK: 255.255.255.224
GATEWAY: 10.122.187.161
SERVER: 10.207.204.10
IMAGE: cisco-ftd-fp2k.7.2.4-165.SPA
MACADDR: 18:59:f5:d9:6a:00
VERBOSITY: Progress
RETRY: 40
PKTTIMEOUT: 7200
BLKSIZE: 1460
CHECKSUM: Yes
PORT: GbE/1
PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.7.2.4-165.SPA from 10.207.204.10!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! █
```

---

**Nota:** Si la descarga de la imagen de inicio se realiza correctamente, verá varios signos de

---

---

exclamación (!) que confirman la descarga; de lo contrario, revise que las configuraciones sean adecuadas o valide si el dispositivo puede alcanzar el servidor de almacenamiento remoto.

---

**Paso 7.** Una vez que el sistema se active, inicie sesión en el dispositivo con las credenciales predeterminadas (admin/Admin123) y cambie la contraseña del dispositivo:

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

---

**Nota:** Este error puede mostrarse mientras se realiza la configuración inicial; sin embargo, se borrará después de instalar el software de Threat Defence como se describe en los pasos posteriores.

---

```
Jun 14 21:37:17 firepower-2110 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
nfra-version-missing][org-root/fw-infra-pack-default] Bundle version in firmware
re-install
```

**Paso 8.** Configure la IP de la interfaz de administración:

- I. Pase al ámbito del fabric con el comando **scope fabric-interconnect a**
- II. Establezca la configuración IP de administración con el comando **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 255.255.255.0 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
```

**Paso 9.** Descargue el paquete de instalación de Threat Defence:

- I. Pase al ámbito del firmware con el comando **scope firmware**
- II. Descargue el paquete de instalación:
  - A. Si está utilizando un USB, puede utilizar el comando **download image usbA:package\_name**
  - B. Si está utilizando un servidor de almacenamiento remoto compatible, puede utilizar el comando **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.SF
firepower-2110 /firmware # █
```

---

**Nota:** Al utilizar servidores de almacenamiento remoto, es necesario utilizar rutas de acceso absolutas en la sintaxis del comando, como se muestra en el ejemplo.

---

**Paso 10.** Valide el progreso de la descarga con el comando **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
```

**Nota:** Una vez que el estado de descarga pasa a *Descargado*, puede continuar con el siguiente paso.

**Paso 11.** Revise que el paquete ya está en la lista de firmware con el comando `show package`:

```
firepower-2110 /firmware # show package
Name Package-Vers
-----
cisco-ftd-fp2k.7.2.4-165.SPA 7.2.4-165
```

**Nota:** copie la *versión* del *paquete* tal y como se va a utilizar en la instalación del software Threat Defence.

**Paso 12.** Instale el software Threat Defence para finalizar la recreación de imágenes:

- I. Pase al ámbito de instalación con el comando **scope auto-install**.
- II. Continúe con la instalación del software Threat Defence con el comando **install security-pack version version force**
- III. Dos mensajes de confirmación van a aparecer en la consola, confirme ambos escribiendo **sí**.

```
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.
```

**Precaución:** el proceso de recreación de imágenes tarda hasta 45 minutos. Tenga en cuenta que el firewall se reiniciará durante la instalación.



# Validación

Valide el proceso de actualización con el comando **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:FirmwareSyst
emDeploy:ValidateApplicationPack)
firepower-2110 /firmware/auto-install # █
```

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).