Reimage a Secure FTD for 1000, 2100, and 3100 Series

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Before You Begin

Configure

Validation

Related Information

Introduction

This document describes an example of a reimage procedure for the Secure Firewall Threat Defense (FTD).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Threat Defense 2110 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Specific requirements for this document include:

- A console cable connected on the FTD.
- A TFTP Server with the installation package (.SPA) already uploaded.

This reimage procedure is supported on appliances:

- Cisco Secure Firewall Threat Defense 1000 Series
- Cisco Secure Firewall Threat Defense 2100 Series
- Cisco Secure Firewall Threat Defense 3100 Series

Before You Begin

1. A reimage procedure erases all previous configurations. To restore any configurations, generate a backup before you start this procedure.
2. This procedure only applies for Firewalls running FTD software.
3. Verify the model is compatible with this procedure.

Configure

Step 1. Format the appliance:

I. Connect to the console port of your appliance and create a console connection.

II. Log into the FXOS chassis CLI.

III. Type **connect local-mgmt** to move to the management console.

III. Use the command **format everything** to delete all configurations and boot images on the appliance.

III. Type **yes** to confirm the procedure.

```
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
```

Step 2. Interrupt the boot process by pressing **ESC** key to enter ROMMON mode:

```
********************************************************************************
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 >
```

Step 3. Fill the network and remote storage parameters with your configurations to prepare for the TFTP download.

I. The parameters needed to be filled are:

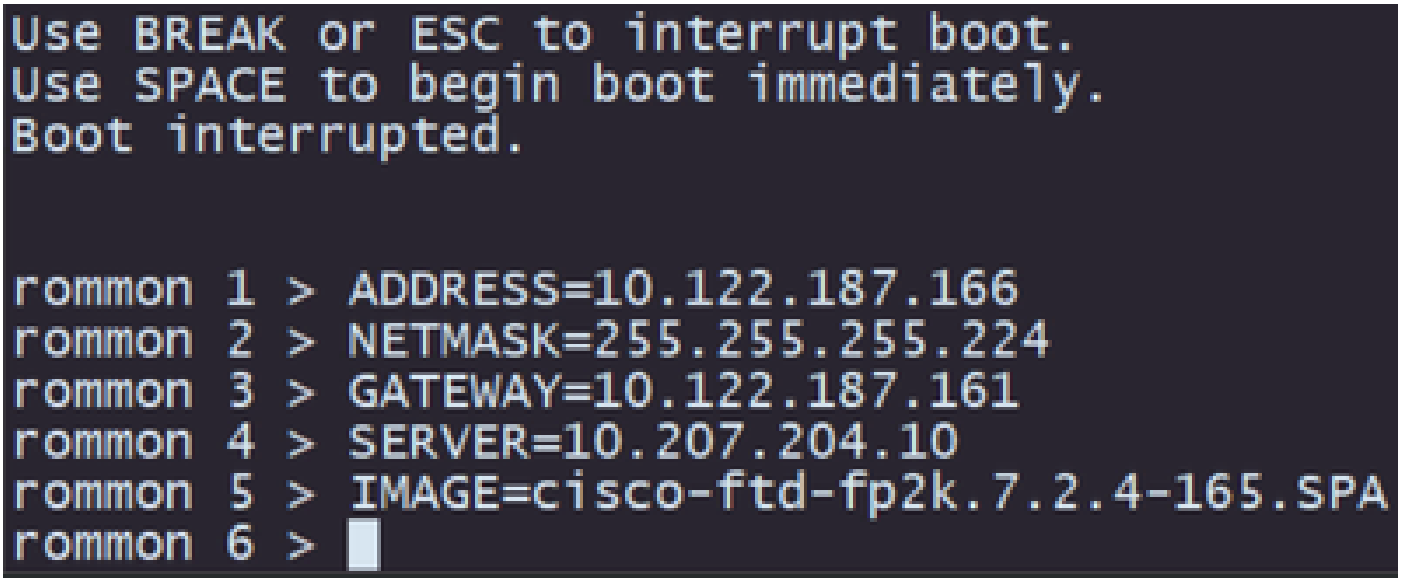
A. ADDRESS = ip_address

B. NETMASK = netmask

C. GATEWAY = gateway_ip

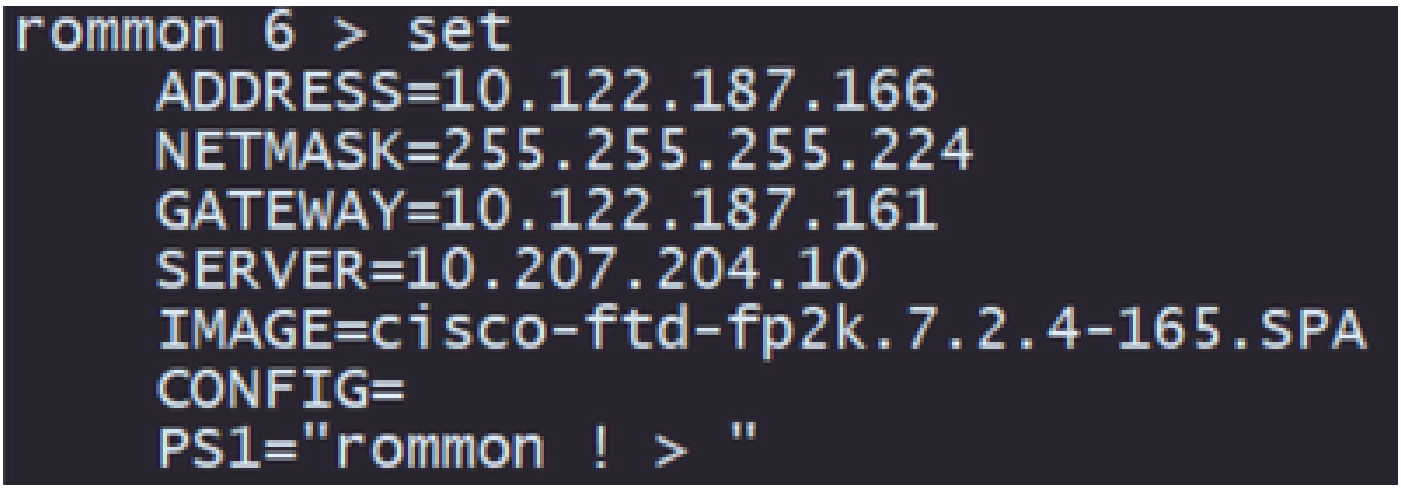
D. SERVER = remote_storage_server

E. IMAGE = path_to_the_file



Caution: ROMMON Mode supports TFTP protocol and USB. FTP, SCP, and SFTP are not supported on the initial boot up process.

Step 4. Type **set** to confirm the provided configurations:



Note: Validate that the provided information is correct, and if you notice an error, adjust the parameter and type set again.

Step 5. Type **sync** to apply the network and remote storage configurations:



Step 6. Initiate the boot process with the command **tftp -b**:

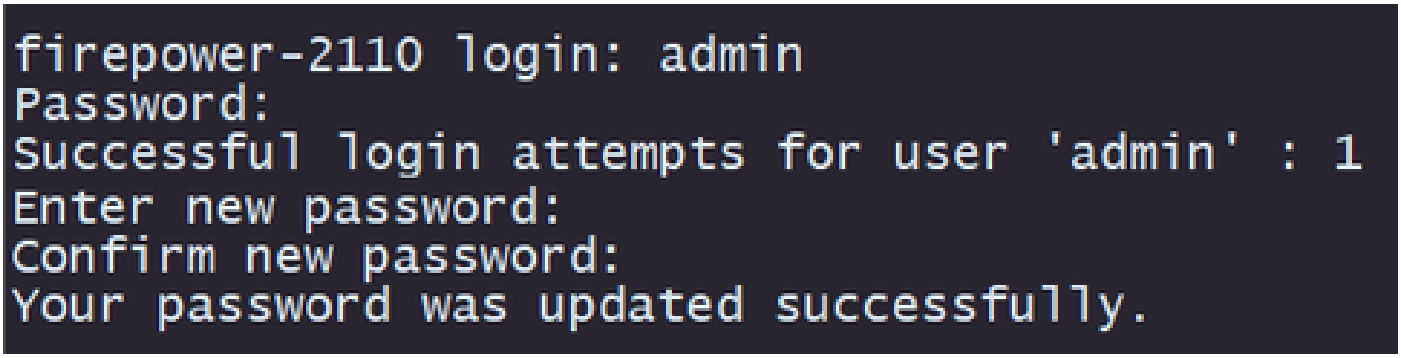
```
rommon 8 > tftp -b
Enable boot bundle: tftp_reqsize = 268435456

            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!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Note: If the download for the boot image is successful, you are going to see several exclamation marks (!) confirming the download, otherwise review that your configurations are appropriate, or validate if your device can reach the remote storage server.

Step 7. Once the system comes up, log into the device using default credentials (admin/Admin123) and change the appliance password:



Note: This error can get displayed while the initial setup is occurring, however, it is going to be cleared after you install the threat defense software as described in later steps.

```
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
```

Step 8. Configure the IP of the management interface:

I. Move to the fabric scope with the command **scope fabric-interconnect a**.

II. Set the management IP configuration with the command **set out-of-band static ip** ip **netmask**netmask gwgateway.

```
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
```

Step 9. Download the Threat Defense installation package:

I. Move to firmware scope with the command **scope firmware**.

II. Download the installation package:

A. If you are using a USB, you can use the command **download image** usbA:package_name.

B. If you are using a supported remote storage server, you can use the command **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 #
```

Note: When using remote storage servers, it is required to use absolute paths on the syntax of the command as displayed on the example.

Step 10. Validate the download progress with the command **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
```

Note: Once the download state transitions to Downloaded, you can proceed to the next step.

Step 11. Review that the package is already on the firmware list with command **show package**:

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

Note: Copy the package version as it is going to be used on the installation of the Threat Defense software.

Step 12. Install the Threat Defense software to finalize the reimage:

I. Move to the install scope with command **scope auto-install**.

II. Proceed with the install of the threat defense software with command **install security-pack version**

version **force**.

III. Two confirmation prompts are going to appear on the console. Please confirm both of them by typing **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.
```

⚠ **Caution**: The reimage process takes up to 45 minutes. Be aware that the firewall is going to reboot while installing.

Validation

Validate the upgrade process with the command **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 #
```

Related Information

- Cisco Secure Firewall ASA Upgrade Guide
- Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 1200/3100/4200 with Threat Defense