

1000、2100、および3100シリーズ向けのセキュアファイアウォール脅威対策の再イメージ化

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[はじめに](#)

[設定](#)

[検証](#)

概要

このドキュメントでは、Secure Firewall Threat Defense (旧称Firewall Threat Defense) の再イメージ化の手順の例をFirepowerします。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- このガイドに関する特別な要件はありません

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Threat Defense 2110(FTD)バージョン7.2.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントに関する特定の要件は次のとおりです。

- FTDに接続されたコンソールケーブル
- インストールパッケージ(.SPA)はすでにアップロードされています

この再イメージ化の手順は、アプライアンスでサポートされています。

- Cisco Secure Firewall Threat Defense 1000シリーズ
- Cisco Secure Firewall Threat Defense 2100シリーズ
- Cisco Secure Firewall Threat Defense 3100シリーズ

はじめに

1. 再イメージ化の手順により、以前の設定がすべて消去されます。設定を復元するには、この手順を開始する前にバックアップを生成します。
2. この手順は、FTDソフトウェアを実行しているファイアウォールにのみ適用されます。
3. モデルがこの手順と互換性があることを確認します。

設定

ステップ 1 : アプライアンスをフォーマットします。

- I. アプライアンスのコンソールポートに接続し、コンソール接続を作成します。
- II. FXOSシャーシのCLIにログインします。
- III. `connect local-mgmt`と入力して、管理コンソールに移動します。
- III. `format everything` コマンドを使用して、アプライアンス上のすべての設定とブートイメージを削除します。
- III. `yes`と入力して手順を確認します

```
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
```

ステップ 2 : Escキーを押してブートプロセスを中断し、ROMMONモードに入ります。

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

ステップ 3 : TFTPダウンロードの準備として、ネットワークとリモートストレージのパラメータに設定を入力します。

1.入力する必要があるパラメータは次のとおりです。

- A. ADDRESS=ip_address
- B. NETMASK=ネットマスク
- C. ゲートウェイ=gateway_ip
- D. SERVER=remote_storage_server
- E. IMAGE=path_to_the_file

```
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 > █
```

注意:ROMMONモードではTFTPプロトコルのみがサポートされ、初期ブートアッププロセスではFTP、SCP、SFTP、およびUSBはサポートされません。

ステップ 4 : setと入力して、提供された設定を確認します。

```
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 ! > "
```

注 : 提供された情報が正しいことを確認し、エラーが発生した場合は、パラメータを調整してsetと再度入力します。

ステップ 5 : syncと入力して、ネットワークとリモートストレージの設定を適用します。

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

手順 6 : tftp -bコマンドを使用して、ブートプロセスを開始します。

```
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
PKTIMEOUT: 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!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

注 : ブートイメージのダウンロードが正常に完了すると、ダウンロードを確認する感嘆符(!)がいくつか表示されます。それ以外の場合は、構成が適切であることを確認するか、デバイスがリモート記憶域サーバーに到達できるかどうかを検証します。

手順 7 : システムが起動したら、デフォルトのクレデンシャル(admin/Admin123)を使用してデバイスにログインし、アプライアンスのパスワードを変更します。

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

注 : このエラーは、初期セットアップの実行中に表示される場合がありますが、後の手順で説明するように、脅威対策ソフトウェアをインストールした後でクリアされます。

```
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
```

ステップ 8 : 管理インターフェイスのIPを設定します。

- I. scope fabric-interconnect a コマンドを使用して、ファブリックスコープに移動します。
- II. コマンド set out-of-band static ip ip netmask netmask gw gateway を使用して、管理IP設定を設定します

```
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
```

ステップ 9 : Threat Defense インストールパッケージをダウンロードします。

- I. scope firmware コマンドを使用して、ファームウェアスコープに移動します。
- II. インストールパッケージをダウンロードします。
 - A. USB を使用している場合は、download image usbA:package_name コマンドを使用できます。
 - B. サポートされているリモートストレージサーバを使用している場合は、download image tftp/ftp/scp/sftp://path_to_your_package コマンドを使用できます。

```
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 # █
```

注 : リモートストレージサーバを使用する場合は、例に示すように、コマンドの構文に絶対パスを使用する必要があります。

ステップ 10: show download-taskコマンドを使用して、ダウンロードの進捗状況を確認します。

```
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
```

注: ダウンロードの状態がDownloadedに移行したら、次の手順に進むことができます。

ステップ 11 show packageコマンドを使用して、パッケージがすでにファームウェアリストにあることを確認します。

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

注: Threat Defenseソフトウェアのインストール時に使用するパッケージバージョンをコピーします。

ステップ 12 脅威対策ソフトウェアをインストールして、再イメージ化を完了します。

- I. scope auto-installコマンドを使用して、インストールスコープに移動します。
- II. install security-pack version version forceコマンドを使用して、脅威対策ソフトウェアのインストールを続行します。
- III. コンソールに2つの確認プロンプトが表示されるので、yesと入力して両方を確認します。

```
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.
```

注意：再イメージ化プロセスには最大で45分かかります。インストール中にファイアウォールがリブートされるので注意してください。

検証

show detailコマンドを使用して、アップグレードプロセスを検証します。

```
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 # █
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。