Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド

最終更新：2024 年 10 月 4 日

Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド

このガイドでは、Secure Firewall ASA と Secure Firewall Threat Defense（旧 Firepower Threat Defense）間の再イメージ化の方法、および新しいイメージバージョンを使用した Threat Defense の再イメージ化の方法について説明します。この方法はアップグレードとは異なり、Threat Defense を工場出荷時のデフォルト状態に戻します。ASA の再イメージ化については、ASA の一般的な操作の設定ガイドを参照してください。このガイドでは、ASA の再イメージ化に複数の方法を使用できます。

サポート対象のモデル

ASA ソフトウェアまたは Threat Defense ソフトウェアのいずれかをサポートするモデルは、次のとおりです。ASA および Threat Defense バージョンのサポートについては、『ASA compatibility guide』または『Cisco Secure Firewall Threat Defense 互換性ガイド』を参照してください。

- Firepower 1000
- Firepower 2100
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- ISA 3000
- ASA 5506-X、5506W-X、および 5506H-X（Threat Defense 6.2.3 以前、ASA 9.16 以前）
- ASA 5508-X（Threat Defense 7.0 以前、ASA 9.16 以前）
- ASA 5512-X （Threat Defense 6.2.3 以前、ASA 9.12 以前）
- ASA 5515-X（Threat Defense 6.4 以前、ASA 9.12 以前）
- ASA 5516-X（Threat Defense 7.0 以前、ASA 9.16 以前）
- ASA 5525-X（Threat Defense 6.6 以前、ASA 9.14 以前）
- ASA 5545-X（Threat Defense 6.6 以前、ASA 9.14 以前）
- ASA 5555-X（Threat Defense 6.6 以前、ASA 9.14 以前）

（注） Firepower 4100 および 9300 でも、ASA または Threat Defense のいずれかをサポートしますが、これらは論理デバイスとしてインストールされています。詳細については、FXOS の構成ガイドを参照してください。

（注） ASA 5512-X ～ 5555-X 上の Threat Defense の場合は、シスコのソリッド ステート ドライブ（SSD）を実装する必要があります。詳細については、ASA 5500-X のハードウェア ガイドを参照してください。ASA の場合は、ASA FirePOWER モジュールを使用するためにも SSD が必要です（ASA 5506-X、5508-X、および 5516-X には SSD が標準です）。

Firepower または Cisco Secure Firewall の再イメージ化

Firepower および Cisco Secure Firewall モデルは、脅威に対する防御 または ASA ソフトウェアのいずれかをサポートします。

ソフトウェアのダウンロード

Threat Defense ソフトウェアまたは ASA ソフトウェアを入手します。

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

表 *1 : Threat Defense* のソフトウェア

Threat Defense モデル	ダウンロードの場所	パッケージ
Firepower 1000	参照先：https://www.cisco.com/go/ftd-software	
	Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	パッケージには、cisco-ftd-fp1k.7.4.1-172**SPA** などのファイル名が付けられています。
Firepower 2100	参照先：https://www.cisco.com/go/ftd-software	
	Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	パッケージには、cisco-ftd-fp2k.7.4.1-172**SPA** などのファイル名が付けられています。
Cisco Secure Firewall 3100	参照先：https://www.cisco.com/go/ftd-software	
	Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	• 7.3 以降：パッケージには Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.**tar** のようなファイル名が付いています。 • 7.2：パッケージには、次のようなファイル名が付けられています：cisco-ftd-fp3k.7.2.6-127.**SPA**。
Cisco Secure Firewall 4200	参照先：https://www.cisco.com/go/ftd-software	
	Threat Defense package 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	パッケージには、Cisco_Secure_FW_TD_4200-7.4.1-172.sh.REL.**tar** のようなファイル名がついています。

表 *2 : ASA* ソフトウェア

ASA モデル	ダウンロードの場所	パッケージ
Firepower 1000	参照先： https://www.cisco.com/go/asa-firepower-sw	
	ASA パッケージ 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	パッケージには、次のようなファイル名が付けられています： cisco-asa-fp1k.9.20.2.2.**SPA**。このパッケージには ASA と ASDM が含まれています。
	ASDM ソフトウェア（アップグレード） 現在の ASDM または ASA CLI を使って ASDM の以降のバージョンにアップグレードするには、使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-7202.**bin** のような名前が付いています。
Firepower 2100	参照先： https://www.cisco.com/go/asa-firepower-sw	
	ASA パッケージ 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	パッケージには、次のようなファイル名が付けられています： cisco-asa-fp2k.9.20.2.2.**SPA**。このパッケージには、ASA、ASDM、FXOS、および Secure Firewall Chassis Manager（旧 Firepower Chassis Manager）が含まれています。
	ASDM ソフトウェア（アップグレード） 現在の ASDM または ASA CLI を使って ASDM の以降のバージョンにアップグレードするには、使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-7202.**bin** のような名前が付いています。

ASA モデル	ダウンロードの場所	パッケージ
Cisco Secure Firewall 3100	参照：https://cisco.com/go/asa-secure-firewall-sw [英語]	
	ASA パッケージ 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	パッケージには、次のようなファイル名が付けられています：cisco-asa-fp3k.9.20.2.2.**SPA**。このパッケージには ASA と ASDM が含まれています。
	ASDM ソフトウェア（アップグレード） 現在の ASDM または ASA CLI を使って ASDM の以降のバージョンにアップグレードするには、使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-7202.**bin** のような名前が付いています。
Cisco Secure Firewall 4200 シリーズ	参照：https://cisco.com/go/asa-secure-firewall-sw [英語]	
	ASA パッケージ 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	パッケージには、次のようなファイル名が付けられています：cisco-asa-fp4200.9.20.2.2.**SPA**。このパッケージには ASA と ASDM が含まれています。
	ASDM ソフトウェア（アップグレード） 現在の ASDM または ASA CLI を使って ASDM の以降のバージョンにアップグレードするには、使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-7202.**bin** のような名前が付いています。

ASA→Threat Defense：Firepower または Cisco Secure Firewall

このタスクでは、ASA ソフトウェアから Threat Defense イメージを起動することによって、ASA から Threat Defense に Firepower または Cisco Secure Firewall デバイスを再イメージ化できます。

始める前に

- アップロードするイメージが FTP、HTTP(S)、SCP、SMB、または TFTP サーバーか、EXT2/3/4 または VFAT/FAT32 でフォーマットされた USB ドライブで使用可能であることを確認します。

（注） ASA に強力な暗号化ライセンスがない場合（たとえば、登録していない場合）は、SCP や HTTPS などのセキュアなプロトコルを使用できません。

- ASA インターフェイスを介してサーバーに到達できることを確認してください。デフォルト設定には次の内容が含まれます。
  - Ethernet 1/2：192.168.1.1
  - Management 1/1—Firepower 1010：192.168.45.1；その他のモデル：DHCP およびデフォルトルート
  - Ethernet 1/1：DHCP およびデフォルトルート

  configure factory-default コマンドを使用して、Management 1/1（Firepower 1010）または Ethernet 1/2（その他のモデル）の静的 IP アドレスを設定することもできます。ルートを設定するには、**route** コマンドを参照してください。
- （Firepower 2100）9.12 以前では、プラットフォームモードのみを使用できます。9.13 以降では、アプライアンスモードがデフォルトです。プラットフォームモードのデバイスを 9.13 以降にアップグレードすると、ASA はプラットフォームモードのままになります。モードを確認するには 、ASA CLI で **show fxos mode** コマンドを使用します。他のモデルはアプライアンスモードのみをサポートします。

  プラットフォームモードの ASA がある場合は、FXOS を使用してイメージを再作成する必要があります。「ASA→Threat Defense ：Firepower 2100 プラットフォームモード （9 ページ）」を参照してください。
- （Cisco Secure Firewall 3100）Cisco Secure Firewall 3100 で ASA から Threat Defense 7.3 以降に再イメージ化を行うには、最初に ASA を 9.19 以降にアップグレードして、7.3 で導入された新しいイメージタイプをサポートするように ROMMON のバージョンを更新する必要があります。『ASA upgrade guide』を参照してください。

手順

ステップ 1 ASA CLI に接続します。

ステップ 2 ASA CLI/ASDM またはスマート ソフトウェア ライセンシング サーバーから、スマート ソフトウェア ライセンシング サーバーの ASA の登録を解除します。

license smart deregister

例：

```
ciscoasa# license smart deregister
```

ステップ 3 Threat Defense イメージをフラッシュ メモリにダウンロードします。この手順ではFTP コピーを示します。

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

USB ドライブを使用するには、**disk1://** を指定します。ただし、**disk2://** を使用する Firepower 2100 は除きます。

例：

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
```

例：

Cisco 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
```

ステップ 4 Threat Defense イメージ（直前にアップロードしたもの）を起動します。

a) グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

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

b) 設定されている現在のブートイメージが存在している場合、これを表示します。

show running-config boot system

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMONから元のASAイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例：

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

c) **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

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

boot system コマンドが設定されていない場合は、この手順をスキップします。

例：

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

d) Threat Defense イメージを起動します。

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

リロードするように求められます。

例：

Cisco 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.
```

例：

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.
```

ステップ 5 シャーシが再起動するまで待ちます。

FXOS が最初に表示されますが、Threat Defense が表示されるまで待つ必要があります。

アプリケーションが起動し、アプリケーションに接続すると、EULA に同意し、CLI で初期設定を実行するように求められます。Secure Firewall Device Manager（旧 Firepower Device Manager）または Secure Firewall Management Center（旧 Firepower Management Center）のいずれかを使用してデバイスを管理できます。セットアップに進むには、http://www.cisco.com/go/ftd-asa-quick でご使用のモデルとマネージャのクイック スタート ガイドを参照してください。

例：

```
[...]
************ 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→Threat Defense ：Firepower 2100 プラットフォームモード

このタスクでは、プラットフォームモードの Firepower 2100 を 脅威に対する防御 に再イメージ化することができます。

（注） この手順を実行すると、FXOS 管理者パスワードは **Admin123** にリセットされます。

始める前に

- この手順では、FXOS CLI を使用する必要があります。
- 9.12 以前では、プラットフォームモードのみを使用できます。9.13 以降では、アプライアンスモードがデフォルトです。プラットフォームモードのデバイスを 9.13 以降にアップグ

レードすると、ASA はプラットフォームモードのままになります。ASA CLI で **show fxos mode** コマンドを使用して、9.13 以降のモードを確認します。

アプライアンス モードの ASA がある場合、これらの FXOS コマンドにアクセスすることはできません。脅威に対する防御への再イメージ化は ASA OS で行われます。ASA→Threat Defense：Firepower または Cisco Secure Firewall （5 ページ）を参照してください。

手順

ステップ 1 アップロードするイメージが FXOS Management 1/1 インターフェイスに接続されている FTP、SCP、SFTP、または TFTP サーバーか、EXT2/3/4 または VFAT/FAT32 でフォーマットされた USB ドライブで使用できることを確認します。

FXOS Management 1/1 の IP アドレスを確認または変更するには、『Cisco Firepower 2100 Getting Started Guide』を参照してください。

ステップ 2 ASA CLI/ASDM またはスマート ソフトウェア ライセンシング サーバーから、スマート ソフトウェア ライセンシング サーバーの ASA の登録を解除します。

ステップ 3 コンソール ポート（推奨）または SSH のいずれかを使用して、FXOS CLI を Management 1/1 インターフェイスに接続します。コンソール ポートで接続する場合は、FXOS CLI にすぐにアクセスします。FXOS ログイン クレデンシャルを入力します。デフォルトのユーザー名は **admin** で、デフォルトのパスワードは **Admin123** です。

SSH を使用して ASA 管理 IP アドレスに接続する場合は、FXOS にアクセスするために **connect fxos** と入力します。また、FXOS 管理 IP アドレスに直接 SSH 接続することもできます。

ステップ 4 シャーシにパッケージをダウンロードします。

a) ファームウェア モードを入力します。

scope firmware

例：

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

b) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **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*

例：

```
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) ダウンロード プロセスをモニターします。

show download-task

例：

```
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 #
```

ステップ 5 新しいパッケージのダウンロードが終了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。

a) 新しいパッケージのバージョン番号を表示し、コピーします。

show package

例：

```
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) パッケージをインストールします。

注意　この手順で設定を消去します。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシはイメージをインストールし、再起動します。このプロセスには約 5 分かかる場合があります。

（注） 次のエラーが表示された場合は、パッケージのバージョンではなく、パッケージの名前が入力されている可能性があります。

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

例：

```
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 #
```

ステップ 6 シャーシが再起動するまで待ちます。

FXOS が最初に起動しますが、 脅威に対する防御 が起動するまで待つ必要があります。

アプリケーションが起動し、アプリケーションに接続すると、EULA に同意し、CLI で初期設定を実行するように求められます。Device Manager または Management Center を使用してデバイスを管理できます。セットアップに進むには、http://www.cisco.com/go/ftd-asa-quick でご使用のモデルとマネージャのクイック スタート ガイドを参照してください。

例：

```
[...]
************ 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 または Cisco Secure Firewall

このタスクでは、Firepower または Cisco Secure Firewall デバイスを Threat Defense から ASA に再イメージ化できます。Firepower 2100 のデフォルトでは、ASA はアプライアンスモードです。再イメージ化した後は、プラットフォームモードに変更できます。

（注） この手順を実行すると、FXOS 管理者パスワードは **Admin123** にリセットされます。

手順

ステップ 1 アップロードするイメージが Management 1/1 インターフェイス、または Cisco Secure Firewall 4200 の場合は Management 1/1 または 1/2 に接続されている FTP、HTTP(S)、SCP、SFTP、または TFTP サーバーか、EXT2/3/4 または VFAT/FAT32 でフォーマットされた USB ドライブで使用できることを確認します。

Management インターフェイス設定の詳細については、「Cisco Secure Firewall Threat Defense コマンドリファレンス」で Threat Defense の **show network** コマンドおよび **configure network** コマンドを参照してください。

ステップ 2 Threat Defense のライセンスを解除します。

- Management Center から Threat Defense を管理している場合は、デバイスを Management Center から削除します。
- Device Manager を使用して Threat Defense を管理している場合は、必ず、Device Manager またはスマート ソフトウェア ライセンシング サーバーのいずれかから、スマート ソフトウェア ライセンシング サーバーのデバイスを登録解除してください。

ステップ 3 コンソール ポート（推奨）または SSH のいずれかを使用して、FXOS CLI を Management インターフェイスに接続します。コンソール ポートで接続する場合は、FXOS CLI にすぐにアクセスします。FXOS ログイン クレデンシャルを入力します。デフォルトのユーザー名は **admin** で、デフォルトのパスワードは **Admin123** です。

SSH を使用して Threat Defense 管理 IP アドレスに接続する場合は、FXOS にアクセスするために **connect fxos** と入力します。

ステップ 4 シャーシにパッケージをダウンロードします。

a) ファームウェア モードを入力します。

scope firmware

例：

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

b) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **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*

例：

```
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) ダウンロード プロセスをモニターします。

show download-task

例：

```
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 #
```

ステップ 5 新しいパッケージのダウンロードが終了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。

a) 新しいパッケージのバージョン番号を表示し、コピーします。

show package

例：

```
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) パッケージをインストールします。

注意 この手順で設定を消去します。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシがイメージをインストールして再起動します。このプロセス（リロードを含む）には約 30 分かかる場合があります。

（注） 次のエラーが表示された場合は、パッケージのバージョンではなく、パッケージの名前が入力されている可能性があります。

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

例：

```
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 #
```

ステップ 6 シャーシが再起動するまで待ちます。

ASA 9.13 以降（デフォルトではアプライアンス モード）

ASA が起動したら、CLI でユーザー EXEC モードにアクセスします。

例：

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

ASA 9.12 以前（デフォルトではプラットフォームモード）

FXOS が最初に起動しますが、 ASA が起動するまで待つ必要があります。

アプリケーションが起動し、アプリケーションに接続したら、CLI でユーザー EXEC モードにアクセスします。

例：

```
 [...]
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 または Cisco Secure Firewall

Cisco Secure Firewall 3100 の場合のみ、再イメージ化方法は現在のバージョンによって異なります。

Threat Defense→Threat Defense：Firepower または Cisco Secure Firewall（3100 を除く）

これらのモデルは、デバイスを工場出荷時のデフォルトの状態に復元するための設定のみの消去からイメージの置換に至るまで複数レベルの再イメージ化を提供します。

手順

ステップ 1 再イメージ化の手順については、『Troubleshooting Guide』を参照してください。

ステップ 2 新しいバージョンをロードする場合は、「Reimage the System with a New Software Version」の手順を使用します。

起動できない、パスワードをリセットするなどのトラブルシューティングには、他の再イメージ化方法を使用します。

Threat Defense→Threat Defense：Cisco Secure Firewall 3100

Cisco Secure Firewall 3100 は、設定のみの消去からイメージの置換、デバイスの工場出荷時のデフォルト状態への復元に至るまで、さまざまなレベルで再イメージ化を提供します。再イメージ化については、開始バージョンと終了バージョンに応じて次のオプションを参照してください。

手順

ステップ 1 **7.2 への再イメージ化、または 7.3 以降から 7.3 以降への再イメージ化**：再イメージ化の手順については、『Troubleshooting Guides』を参照してください。

新しいバージョンをロードする場合は、「Reimage the System with a New Software Version」の手順を使用します。

起動できない、パスワードをリセットするなどのトラブルシューティングには、他の再イメージ化方法を使用します。

ステップ 2 **7.1/7.2 から 7.3 以降への再イメージ化**：7.1/7.2 から 7.3 以降への再イメージ化を行う場合は、最初に ASA 9.19 以降に再イメージ化を実行してから 7.3 以降に再イメージ化を行う必要があります。

7.3 以降では新しいタイプのイメージファイルを使用しますが、このイメージファイルを使用するには、事前に ROMMON を更新しておく必要があります。そのため、7.3 以降への再イメージ化を行う前に ASA 9.19 以降（古い ROMMON でサポートされていますが、一緒に新しい ROMMON へアップグレードされます）に再イメージ化を実行しておく必要があります。個別の ROMMON アップデータはありません。

（注） 7.1/7.2 から 7.3 以降へは、通常の方法でアップグレードできます。ROMMON は、このアップグレードプロセスの一環として更新されます。

a) Threat Defense から ASA 9.19 以降へ再イメージ化を行います。Threat Defense→ASA：Firepower または Cisco Secure Firewall （13 ページ） を参照してください。
b) ASA から Threat Defense 7.3 以降へ再イメージ化を行います。ASA→Threat Defense：Firepower または Cisco Secure Firewall （5 ページ） を参照してください。

ASA→ASA：Firepower および Cisco Secure Firewall

ブートアップの問題をトラブルシューティングし、パスワードの回復を実行するには、ASA の再イメージ化が必要になる場合があります。通常のアップグレードでは、再イメージ化を実行する必要はありません。

手順

ステップ 1 再イメージ化の手順については、『Troubleshooting Guide』を参照してください。
ステップ 2 新しいソフトウェアイメージをロードするには、再イメージ化ではなく『ASA Upgrade Guide』を参照してください。

ASA 5500-x または ISA 3000 の再イメージ化

ASA 5500-X シリーズまたは ISA 3000 シリーズのモデルの多くは、Threat Defense ソフトウェアと ASA ソフトウェアのいずれかをサポートします。

必要なコンソール ポート アクセス

再イメージ化を実行するには、コンピュータをコンソール ポートに接続する必要があります。

ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X では、サードパーティ製のシリアル USB 変換ケーブルを使用して接続する必要がある場合があります。他のモデルには、ミニ USB タイプ B コンソール ポートが搭載されているため、ミニ USB ケーブルを使用できます。Windows では、software.cisco.com から USB シリアル ドライバのインストールが必要な場合があります。コンソール ポート オプションおよびドライバ要件の詳細については、http://www.cisco.com/go/asa5500x-install でハードウェア ガイドを参照してください。

9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを使用します。

ソフトウェアのダウンロード

Threat Defense ソフトウェアまたは ASA、ASDM、および ASA FirePOWER モジュールソフトウェアを入手します。このドキュメントの手順を実行するには、初期ダウンロード用の TFTP サーバーにソフトウェアを配置する必要があります。他のイメージは、他のタイプ（HTTP、FTP など）のサーバからダウンロードできます。正確なソフトウェア パッケージとサーバ タイプについては、手順を参照してください。

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

注目 Threat Defense のブートイメージとシステムパッケージは、バージョンおよびモデルに固有です。プラットフォームに適切なブート イメージとシステム パッケージがあることを確認します。ブート イメージとシステム パッケージの間に不一致があると、ブート障害が発生する可能性があります。一致しない場合は、新しいシステム パッケージで古いブートイ メージが使用されます。

表 *3 : Threat Defense* のソフトウェア

Threat Defense モデル	ダウンロードの場所	パッケージ
ASA 5506-X、ASA 5508-X、および ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw を参照してください。	（注） ファイル名の最後が **.sh** のパッチファイルも表示されます。パッチアップグレード プロセスについては、このドキュメントでは説明しません。
	ブート イメージ 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	ブート イメージのファイルには ftd-boot-9.6.2.0.**lfbff** のような名前が付いています。
	システム ソフトウェア インストール パッケージ 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	システム ソフトウェア インストール パッケージのファイルには ftd-6.1.0-330.**pkg** のような名前が付いています。
ASA 5512-X ～ ASA 5555-X	http://www.cisco.com/go/asa-firepower-sw を参照してください。	（注） ファイル名の最後が **.sh** のパッチファイルも表示されます。パッチアップグレード プロセスについては、このドキュメントでは説明しません。
	ブート イメージ 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	ブート イメージのファイルには ftd-boot-9.6.2.0.**cdisk** のような名前が付いています。
	システム ソフトウェア インストール パッケージ 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	システム ソフトウェア インストール パッケージのファイルには ftd-6.1.0-330.**pkg** のような名前が付いています。

Threat Defense モデル	ダウンロードの場所	パッケージ
ISA 3000	http://www.cisco.com/go/isa3000-softwareを参照してください。	（注） ファイル名の最後が **.sh** のパッチファイルも表示されます。パッチアップグレード プロセスについては、このドキュメントでは説明しません。
	ブート イメージ 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	ブート イメージのファイルには ftd-boot-9.9.2.0.**lfbff** のような名前が付いています。
	システム ソフトウェア インストール パッケージ 使用しているモデル > [Firepower Threat Defense Software] > バージョンの順に選択します。	システム ソフトウェア インストール パッケージのファイルには ftd-6.2.3-330.**pkg** のような名前が付いています。

表 *4 : ASA* ソフトウェア

ASA モデル	ダウンロードの場所	パッケージ
ASA 5506-X、ASA 5508-X、および ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA ソフトウェアのファイルには asa962-**lfbff-k8.SPA** のような名前が付いています。
	ASDM ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762.**bin** のような名前が付いています。
	REST API ソフトウェア 使用しているモデル > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイック スタート ガイド』 を参照してください。
	ROMmon ソフトウェア ご使用のモデル > [ASA Rommon Software] > バージョンの順に選択します。	ROMMON ソフトウェアのファイルには asa5500-firmware-1108.**SPA** のような名前が付いています。

ASA モデル	ダウンロードの場所	パッケージ
ASA 5512-X ～ ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA ソフトウェアのファイルには asa962-**smp-k8.bin** のような名前が付いています。
	ASDM ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。
	REST API ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイック スタート ガイド』 を参照してください。
	Cisco Application Policy Infrastructure Controller（APIC）の ASA デバイス パッケージ 使用しているモデル > [Software on Chassis] > [ASA for Application Centric Infrastructure (ACI) Device Packages] > バージョンの順に選択します。	APIC 1.2(7) 以降では、ファブリック挿入によるポリシー オーケストレーションまたはファブリック挿入のみのパッケージを選択します。デバイス ソフトウェアのファイルには asa-device-pkg-1.2.7.10**.zip** のような名前が付いています。ASA デバイス パッケージをインストールするには、『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Importing a Device Package」の章を参照してください。

ASA モデル	ダウンロードの場所	パッケージ
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA ソフトウェアのファイルには asa962-**lfbff-k8.SPA** のような名前が付いています。
	ASDM ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762.**bin** のような名前が付いています。
	REST API ソフトウェア 使用しているモデル > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイックスタート ガイド』を参照してください。

ROMMONイメージのアップグレード（ASA5506-X、5508-X、5516-X、およびISA3000）

ASA 5506-X シリーズ、ASA 5508-X、ASA 5516-X、および ISA 3000 の ROMMON イメージをアップグレードするには、次の手順に従います。 ASA モデルの場合、システムの ROMMON バージョンは 1.1.8 以上である必要があります。最新バージョンへのアップグレードを推奨します。

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。

注意 ASA 5506-X、5508-X、5516-X の ROMMON 1.1.15 へのアップグレード、および ISA 3000 の ROMMON 1.0.5 へのアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカル サポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

始める前に

Cisco.com から新しい ROMMON イメージを取得して、サーバー上に置いて ASA にコピーします。ASA は、FTP サーバー、TFTP サーバー、SCP サーバー、HTTP（S）サーバー、および SMB サーバーをサポートしています。次の URL からイメージをダウンロードします。

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

手順

ステップ 1 Threat Defense ソフトウェアの場合は、診断 CLI を入力してから、有効モードを開始します。

system support diagnostic-cli

enable

パスワードの入力を求められたら、パスワードを入力せずに Enter キーを押します。

例：

```
> 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#
```

ステップ 2 ROMMON イメージを ASA フラッシュ メモリにコピーします。この手順では、FTP コピーを表示します。他のサーバータイプのシンタックスの場合は **copy ?** と入力します。

copy ftp://[*username***:***password***@**]*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

Threat Defense ソフトウェアの場合は、データインターフェイスが設定されていることを確認します。診断CLIは、専用の管理インターフェイスにアクセスできません。また、CSCvn57678により、**copy** コマンドは Threat Defense バージョンの通常の Threat Defense CLI では機能しない場合があるため、その方法で専用の管理インターフェイスにはアクセスできません。

ステップ 3 現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
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
```

ステップ 4 ROMMON イメージをアップグレードします。

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

例：

```
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]
```

ステップ 5 プロンプトが表示されたら、確認して ASA をリロードします。

ASA が ROMMON イメージをアップグレードして、その後オペレーティングシステムをリロードします。

ASA→Threat Defense ：ASA 5500-X または ISA 3000

ASA を 脅威に対する防御 ソフトウェアに再イメージ化するには、ROMMON プロンプトにアクセスする必要があります。ROMMON では、管理インターフェイスで TFTP を使用して 脅威に対する防御 ブート イメージをダウンロードする必要があります。サポートされているのは TFTP のみです。その後、ブート イメージは、HTTP または FTP を使用して、脅威に対する防御 システム ソフトウェアのインストール パッケージをダウンロードできます。TFTP のダウンロードには時間がかかることがあります。パケットの損失を防ぐために、ASA と TFTP サーバーの間の接続が安定していることを確認してください。

始める前に

再イメージ化して ASA に戻すプロセスを容易にするために、次の手順を実行します。

1. **backup** コマンドを使用して完全なシステム バックアップを実行します。

   詳細および他のバックアップ方法については、構成ガイドを参照してください。

2. 現在のアクティベーション キーをコピーして保存します。これにより、**show activation-key** コマンドを使用してライセンスを再インストールできるようになります。

3. ISA 3000 で Management Center を使用している場合は、ハードウェアバイパスを無効にします。この機能は、バージョン 6.3 以降で Device Manager を使用している場合にのみ実行できます。

手順

ステップ 1 管理インターフェイスの ASA からアクセス可能な TFTP サーバーに 脅威に対する防御 ブート イメージ（ソフトウェアのダウンロード （19 ページ）を参照）をダウンロードします。

ASA 5506-X、5508-X、5516-X、ISA 3000：管理 1/1 ポートを使用してイメージをダウンロードする必要があります。他のモデルでは、任意のインターフェイスを使用できます。

ステップ 2 管理インターフェイスの ASA からアクセス可能な HTTP または FTP サーバーに 脅威に対する防御 システム ソフトウェアのインストール パッケージをダウンロードします（ソフトウェアのダウンロード （19 ページ）を参照）。

ステップ 3 コンソール ポートから、ASA をリロードします。

reload

例：

```
ciscoasa# reload
```

ステップ 4 ブートアップ中に ROMMON プロンプトを表示するよう要求されたら、Esc を押します。

モニタを注視します。

例：

```
[...]
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.
```

この時点で、Esc を押します。

次のメッセージが表示された場合は、時間がかかりすぎです。起動の終了後、再度 ASA をリロードする必要があります。

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

ステップ 5 次の ROMMON コマンドを使用してネットワーク設定を指定し、ブート イメージをロードします。

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftpdnld

脅威に対する防御ブートイメージがダウンロードされ、ブートCLIにブートアップされます。

次の情報を参照してください。

- **interface**：（ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X のみ）インターフェイス ID を指定します。他のモデルは常に管理 1/1 インターフェイスを使用します。
- **set**：ネットワーク設定を表示します。**ping** コマンドを使用してサーバへの接続を確認することもできます。
- **sync**：ネットワーク設定を保存します。
- **tftpdnld**：ブート イメージをロードします。

例：

ASA 5555-X の例：

```
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
```

ASA 5506-X の例：

```
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
```

サーバーへの接続をトラブルシューティングするには、Ping を実行します。

```
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 >
```

ステップ 6 **setup** と入力して、管理インターフェイスのネットワーク設定を行い、システム ソフトウェア パッケージをダウンロードしてインストールできるようにHTTPまたはFTPサーバーへの一時的な接続を確立します。

（注） DHCPサーバーがある場合、Threat Defense は自動的にネットワーク設定を実行します。DHCP を使用する場合は、次のサンプルの起動メッセージを参照してください。

```
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
```

例：

```
                    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>
```

ステップ 7 脅威に対する防御 システム ソフトウェアのインストール パッケージをダウンロードします。この手順では、HTTP のインストールを示します。

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

確認メッセージに応答しない場合は、**noconfirm** オプションを指定します。

例：

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

内部フラッシュ ドライブを消去するように求められます。**y** と入力します。

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

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

インストール プロセスによってフラッシュ ドライブが消去され、システム イメージがダウンロードされます。インストールを続行するように求められます。**y** と入力します。

```
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
```

インストールが完了したら、**Enter** キーを押してデバイスをリブートします。

```
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.
```

リブートには約30分かかりますが、より長時間かかる可能性があります。再起動時に、Threat Defense CLI が表示されます。

ステップ 8 ネットワーク接続をトラブルシューティングするには、次の例を参照してください。

例：

ネットワーク インターフェイスの設定の表示

```
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)
...
```

サーバーに対して ping を実行します。

```
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>
```

traceroute を使用して、ネットワーク接続をテストします。

```
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>
```

ステップ 9 インストールの失敗をトラブルシューティングするには、次の例を参照してください。

例：

「Timed out」エラー

ダウンロード段階で、ファイル サーバーに到達できない場合は、タイムアウトが原因で失敗します。

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

timed out
Upgrade aborted
firepower-boot>
```

この場合は、ASA からファイル サーバーに到達可能であることを確認します。ファイル サーバに ping を実行することで確認できます。

「Package not found」エラー

ファイル サーバーに到達可能であっても、ファイル パスまたは名前が間違っている場合は、「Package not found」というエラーでインストールが失敗します。

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

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

この場合は、Threat Defense パッケージのファイルパスと名前が正しいことを確認します。

インストールが不明なエラーで失敗した

システム ソフトウェアのダウンロード後にインストールが行われると、原因は通常、「Installation failed with unknown error」と表示されます。このエラーが発生した場合は、インストール ログを表示して失敗をトラブルシューティングできます。

```
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 ...
...
```

また、ブート CLI 関連の問題に対して同じコマンドを使用して、/var/log/cisco の下にある upgrade.log、pyos.log、commandd.log を表示することもできます。

ステップ 10 Device Manager または Management Center を使用してデバイスを管理できます。セットアップに進むには、http://www.cisco.com/go/ftd-asa-quick でご使用のモデルとマネージャのクイック スタート ガイドを参照してください。

Threat Defense →ASA：ASA 5500-X または ISA 3000

脅威に対する防御 を ASA ソフトウェアに再イメージ化するには、ROMMON プロンプトにアクセスする必要があります。ROMMON では、ディスクを消去し、管理インターフェイスで TFTP を使用して ASA イメージをダウンロードする必要があります。サポートされるのは、TFTP のみです。ASA をリロードしたら、基本設定を指定し、FirePOWER モジュール ソフトウェアをロードできます。

始める前に

- パケットの損失を防ぐために、ASA と TFTP サーバーの間の接続が安定していることを確認してください。

手順

ステップ 1 Management Center から 脅威に対する防御 を管理している場合は、デバイスを Management Center から削除します。

ステップ 2 Device Manager を使用して 脅威に対する防御 を管理している場合は、必ず、Device Manager またはスマート ソフトウェア ライセンシング サーバーのいずれかから、スマート ソフトウェア ライセンシング サーバーのデバイスを登録解除してください。

ステップ 3 管理インターフェイスの 脅威に対する防御 でアクセス可能な TFTP サーバーに ASA イメージ（ソフトウェアのダウンロード （19 ページ）を参照）をダウンロードします。

ASA 5506-X、5508-X、5516-X、ISA 3000：管理 1/1 ポートを使用してイメージをダウンロードする必要があります。他のモデルでは、任意のインターフェイスを使用できます。

ステップ 4 コンソールポートで、脅威に対する防御 デバイスを再起動します。

reboot

yes と入力して再起動します。

例：

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

ステップ 5 ブートアップ中に ROMMON プロンプトを表示するよう要求されたら、Esc を押します。

モニタを注視します。

例：

```
[...]
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.
```

この時点で、Esc を押します。

次のメッセージが表示された場合は時間がかかりすぎるため、ブート終了後に再度 脅威に対する防御 をリロードする必要があります。

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

ステップ 6 脅威に対する防御 のすべてのディスクを消去します。内部フラッシュは disk0 と呼ばれます。外部 USB ドライブがある場合、そのドライブは disk1 です。

例：

```
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:
.......................
[...]
```

この手順では、ASA が誤った設定ファイルのロードを試みることで多数のエラーが発生しないように、脅威に対する防御 ファイルを消去します。

ステップ 7 次の ROMMON コマンドを使用してネットワーク設定を指定し、ASA イメージをロードします。

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftpdnld

ASA イメージがダウンロードされ、CLI にブートアップされます。

次の情報を参照してください。

- **interface**：（ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X のみ）インターフェイス ID を指定します。他のモデルは常に管理 1/1 インターフェイスを使用します。
- **set**：ネットワーク設定を表示します。**ping** コマンドを使用してサーバへの接続を確認することもできます。
- **sync**：ネットワーク設定を保存します。
- **tftpdnld**：ブート イメージをロードします。

例：

ASA 5555-X の例：

```
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
```

ASA 5506-X の例：

```
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
```

例：

サーバーへの接続をトラブルシューティングするには、**Ping** を実行します。

```
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 >
```

ステップ 8 ネットワークの設定を構成し、ディスクを準備します。

ASA の初期ブートアップ時は、ASA が設定されていません。インタラクティブ プロンプトに従って ASDM アクセス用に管理インターフェイスを設定するか、保存された設定を貼り付けるか、保存された設定がない場合は推奨設定（この後を参照）を貼り付けることができます。

保存された設定がない場合、ASA FirePOWER モジュールの使用を予定しているときは、推奨設定を貼り付けることをお勧めします。ASA FirePOWER モジュールは、管理インターフェイスで管理され、更新のためにインターネットにアクセスできる必要があります。シンプルな推奨ネットワーク配置には、Management（FirePOWER の管理専用）、内部インターフェイス（ASA の管理および内部トラフィック用）、および管理 PC を同じ内部ネットワークに接続するための内部スイッチが含まれます。ネットワーク配置の詳細については、次のクイック スタート ガイドを参照してください。

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

a) ASA コンソール プロンプトで、管理インターフェイスの設定の入力を求められます。

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

設定を貼り付けるか、シンプルなネットワーク配置の推奨設定を作成する場合は、**no** と入力して、手順を続行します。

ASDM サーバに接続できるように管理インターフェイスを設定する場合は、**yes** と入力し、プロンプトに従います。

b) コンソール プロンプトで、特権 EXEC モードにアクセスします。

enable

次のプロンプトが表示されます。

```
Password:
```

c) Enter キーを押します。 デフォルトでは、パスワードは空白です。

d) グローバル コンフィギュレーション モードにアクセスします。

configure terminal

e) インタラクティブ プロンプトを使用していない場合は、プロンプトで設定をコピーして貼り付けます。

設定が保存されておらず、クイック スタート ガイドに記載された簡易設定を使用する場合は、プロンプトで次の設定をコピーして、必要に応じて IP アドレスとインタ フェース ID を変更します。プロンプトを使用した後、この設定を代わりに使用するには、まず **clear configure all** コマンドを使用して設定をクリアする必要があります。

```
interface gigabitethernet0/0
```

```
   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
```

ASA 5506W-X の場合は、Wi-Fi インターフェイス用に以下を追加します。

```
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) ディスクを再フォーマットします。

format disk0:

format disk1:

内部フラッシュは disk0 と呼ばれます。外部 USB ドライブがある場合、そのドライブは disk1 です。ディスクを再フォーマットしない場合は、ASA イメージをコピーしようとすると、次のエラーが表示されます。

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

g) 新しい設定を保存します。

write memory

ステップ 9 ASA イメージと ASDM イメージをインストールします。

ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。また、ASDM をフラッシュ メモリにダウンロードする必要もあります。

a) ASA からアクセス可能なサーバに ASA イメージと ASDM イメージ（ソフトウェアのダウンロード （19 ページ）を参照）をダウンロードします。ASA は多数のタイプのサーバー

をサポートします。詳細については **copy** コマンド（http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2171368）を参照してください。

b) ASA イメージを ASA フラッシュ メモリにコピーします。この手順では FTP コピーを示します。

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

例：

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

c) ASDM イメージを ASA フラッシュ メモリにコピーします。この手順では FTP コピーを示します。

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

例：

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

d) ASA をリロードします。

reload

ASA が disk0 にあるイメージを使用してリロードされます。

ステップ 10 （任意） ASA FirePOWER モジュール ソフトウェアをインストールします。

ASA FirePOWER ブート イメージをインストールし、SSD を区分化して、この手順に従ってシステム ソフトウェアをインストールする必要があります。

a) ブート イメージを ASA にコピーします。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。この手順では FTP コピーを示します。

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

例：

```
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) 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバーに、Cisco.com から ASA FirePOWER サービスのシステム ソフトウェア インストール パッケージをダウンロードします。そのソフトウェアを ASA 上の disk0 にダウンロードしないでください。

c) ASA disk0 で ASA FirePOWER モジュール ブート イメージの場所を設定します。

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

例：

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

d) ASA FirePOWER ブート イメージをロードします。

sw-module module sfr recover boot

例：

```
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) ASA FirePOWER モジュールが起動するまで数分待ってから、現在実行中の ASA FirePOWER ブート イメージへのコンソール セッションを開きます。セッションを開いてログイン プロンプトを表示した後で、**Enter** キーを押さなければならない場合があります。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

例：

```
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
```

モジュールのブートが完了しない場合は、ttyS1 を介して接続できないというメッセージが表示されて session コマンドが失敗します。しばらく待ってから再試行してください。

a) システム ソフトウェア インストール パッケージをインストールできるようにシステムを設定します。

setup

次のプロンプトが表示されます。管理アドレスとゲートウェイ、および DNS 情報が重要な設定であることに注意してください。

- Host name：最大 65 文字の英数字で、スペースは使用できません。ハイフンは使用できます。
- Network address：スタティック IPv4 または IPv6 アドレスを設定するか、DHCP（IPv4 の場合）、または IPv6 ステートレス自動設定を使用します。
- DNS information：少なくとも 1 つの DNS サーバを特定する必要があります。ドメイン名を設定してドメインを検索することもできます。
- NTP information：システム時刻を設定するために、NTP を有効にして NTP サーバを設定できます。

例：

```
asasfr-boot> setup

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

a) システム ソフトウェア イメージ パッケージをインストールします。

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

確認メッセージに応答しない場合は、**noconfirm** オプションを指定します。HTTP、HTTPS、または FTP URL を使用します。ユーザー名とパスワードが必要な場合は、それらを入力するよう示されます。このファイルはサイズが大きいため、ネットワークによっては、ダウンロードに時間がかかる場合があります。

インストールが完了すると、システムが再起動します。アプリケーション コンポーネントのインストールと ASA FirePOWER サービスが開始するまでに必要な時間は大幅に異なります。ハイエンド プラットフォームでは 10 分以上かかる場合がありますが、ローエンド プラットフォームでは 60 ～ 80 分以上かかることがあります（**show module sfr** の出力で、すべてのプロセスがアクティブであると表示される必要があります。）

例：

```
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) パッチリリースをインストールする必要がある場合は、後でマネージャ（ASDM または Management Center）から実行できます。

ステップ 11 アクティベーション キーを保存しなかった既存の ASA の強力な暗号化ライセンスとその他のライセンスを取得します。http://www.cisco.com/go/license を参照してください。**[管理**

（**Manage**）] > **[ライセンス（Licenses）]** セクションで、ライセンスを再ダウンロードできます。

ASDM（および他の多数の機能）を使用するには、高度暗号化（3DES/AES）ライセンスをインストールする必要があります。以前の手順で Threat Defense デバイスに再イメージ化する前に、この ASA からライセンス アクティベーション キーを保存した場合は、そのアクティベーションキーを再インストールできます。アクティベーションキーを保存していなくても、この ASA のライセンスを所有している場合は、ライセンスを再ダウンロードできます。新しい ASA の場合は、新しい ASA ライセンスを要求する必要があります。

ステップ 12 新しい ASA のライセンスを取得します。

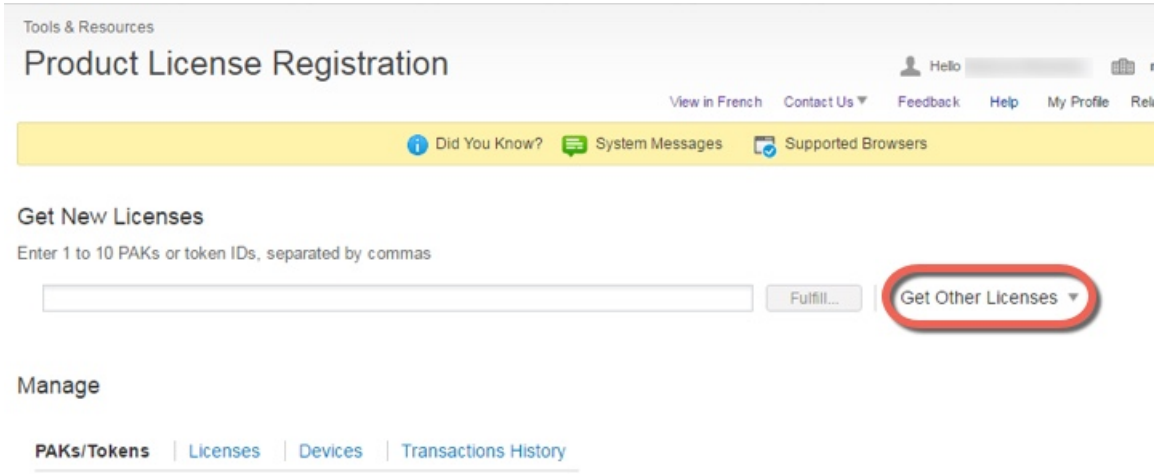
a) 次のコマンドを入力して、ASA のシリアル番号を取得します。

show version | grep Serial

このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。

b) Http://www.cisco.com/go/license を参照し、[他のライセンスを取得（Get Other Licenses）] をクリックします。

図 *1*：他のライセンスの取得

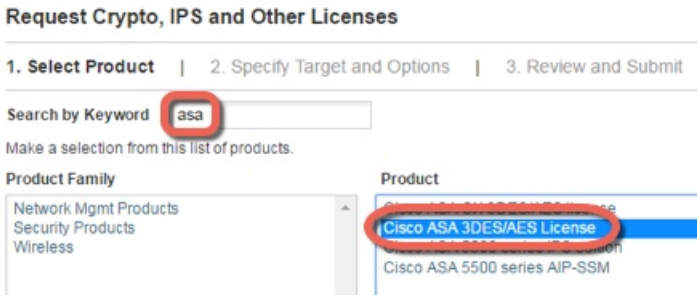


c) [IPS、Crypto、その他（IPS, Crypto, Other）] を選択します。

図 *2 : IPS*、*Crypto*、その他

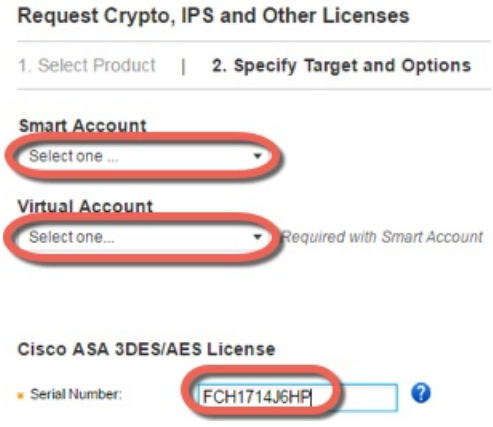
d) [キーワード検索（Search by Keyword）] フィールドに **asa** と入力し、[Cisco ASA 3DES/AES License] を選択します。

図 *3 : Cisco ASA 3DES/AES* ライセンス



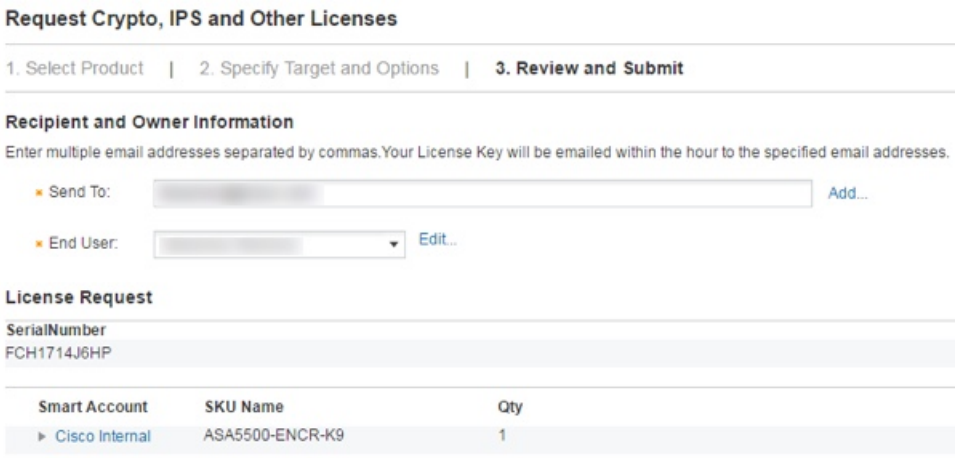
e) [スマートアカウント（Smart Account）]、[バーチャルアカウント（Virtual Account）] を選択し、ASA の [シリアルナンバー（Serial Number）] を入力して、[次へ（Next）] をクリックします。

図 *4 :* スマート アカウント、バーチャル アカウント、シリアル番号



f) 送信先の電子メールアドレスとエンドユーザー名は自動的に入力されます。必要に応じて追加の電子メールアドレスを入力します。[同意する（I Agree）] チェックボックスをオンにして、[送信（Submit）] をクリックします。

図 *5*：送信



g) その後、アクティベーション キーの記載された電子メールが届きますが、**[管理（Manage）]>[ライセンス（Licenses）]**エリアからキーをすぐにダウンロードすることもできます。

h) 基本ライセンスから Security Plus ライセンスへのアップグレード、または AnyConnect ライセンスの購入を希望する場合は、http://www.cisco.com/go/ccw を参照してください。ライセンスの購入後に、http://www.cisco.com/go/license で入力可能な製品認証キー（PAK）が記載された電子メールが送られてきます。AnyConnect ライセンスの場合、ユーザ セッションの同じプールを使用する複数の ASA に適用できるマルチユース PAK を受け取ります。取得したアクティベーション キーには、永続ライセンス（3DES/AES ライセンスを含む）用にそれまでに登録した機能がすべて含まれています。時間ベース ライセンスの場合は、ライセンスごとに個別のアクティベーション キーがあります。

ステップ 13 アクティベーション キーを適用します。

activation-key *key*

例：

```
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.
```

この ASA にはまだアクティベーション キーがインストールされていないため、「Failed to retrieve permanent activation key.」というメッセージが表示されます。このメッセージは無視できます。

永続キーを 1 つだけと、複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。3DES/AES ライセンスをインストールした後に追加のライセンスを注文した場合は、組み合わせたアクティベーション キーにすべてのライセンスと 3DES/AES ライセンスが含まれるため、3DES/AES 専用キーを上書きできます。

ステップ 14 ASA FirePOWER モジュールは、ASA とは別のライセンス メカニズムを使用します。ライセンスはプリインストールされていませんが、注文に応じて、次のライセンスのライセンス アクティベーション キーを取得できる PAK が記載されたプリントアウトがボックスに同梱されている場合があります。

- **Control および Protection**：Control は、「Application Visibility and Control（AVC）」または「アプリケーション」とも呼ばれます。Protection は、「IPS」とも呼ばれます。これらの機能を自動的に更新するには、ライセンス用のアクティベーション キーに加え、「使用権」サブスクリプションも必要になります。

  Control（AVC）の更新には、シスコ サポート契約が含まれます。

  Protection（IPS）の更新には、http://www.cisco.com/go/ccw から IPS サブスクリプションを購入する必要があります。このサブスクリプションには、ルール、エンジン、脆弱性、および位置情報を更新する権利が含まれます。**注**：この使用権サブスクリプションは、ASA FirePOWER モジュールの PAK/ライセンス アクティベーション キーを生成も要求もしません。これは、更新を使用する権利を提供するだけです。

ASA FirePOWER サービスを含む ASA 5500-X を購入していない場合は、アップグレード バンドルを購入して必要なライセンスを取得することができます。詳細については、『Cisco ASA with FirePOWER Services Ordering Guide』を参照してください。

購入できるその他のライセンスには、次のものがあります。

- **Cisco Secure Firewall Threat Defense のマルウェア防御ライセンス**
- **Cisco Secure Firewall Threat Defense の URL フィルタリングライセンス**

これらのライセンスは、ASA FirePOWER モジュールの PAK/ライセンス アクティベーション キーを生成します。発注情報については、『Cisco ASA with FirePOWER Services Ordering Guide』を参照してください。Cisco Secure Firewall Management Center 機能ライセンスも参照してください。

Control と Protection のライセンス、およびその他のオプションのライセンスをインストールする方法については、使用しているモデル用の ASA クイックスタート ガイドを参照してください。

Threat Defense →Threat Defense ：ASA 5500-X または ISA 3000

この手順では、ROMMON を使用して既存の 脅威に対する防御 を新しいバージョンの 脅威に対する防御 ソフトウェアに再イメージ化する方法について説明します。この手順では、デバイスを工場出荷時のデフォルト状態に復元します。通常のアップグレードを実行する場合は、代わりにアップグレード ガイドを参照してください。

ROMMON では、管理インターフェイスで TFTP を使用して新しい 脅威に対する防御 ブートイメージをダウンロードする必要があります。サポートされているのは TFTP のみです。その後、ブートイメージは、HTTP または FTP を使用して、脅威に対する防御 システム ソフトウェアのインストール パッケージをダウンロードできます。TFTP のダウンロードには時間がかか

る場合があります。パケットの損失を防ぐために、脅威に対する防御 と TFTP サーバーの間の接続が安定していることを確認してください。

手順

ステップ 1 Management Center を使用して 脅威に対する防御 を管理している場合は、デバイスを Management Center から削除します。

ステップ 2 Device Manager を使用して 脅威に対する防御 を管理している場合は、必ず Device Manager またはスマート ソフトウェア ライセンシング サーバーからスマート ソフトウェア ライセンシング サーバーのデバイスを登録解除してください。

ステップ 3 管理インターフェイスの 脅威に対する防御 からアクセス可能な TFTP サーバーに 脅威に対する防御 ブート イメージ（ソフトウェアのダウンロード （19 ページ）を参照）をダウンロードします。

ASA 5506-X、5508-X、5516-X、ISA 3000：管理 1/1 ポートを使用してイメージをダウンロードする必要があります。他のモデルでは、任意のインターフェイスを使用できます。

ステップ 4 管理インターフェイスの 脅威に対する防御 からアクセス可能な HTTP または FTP サーバーに 脅威に対する防御 システムソフトウェアのインストールパッケージをダウンロードします（ソフトウェアのダウンロード （19 ページ）を参照）。

ステップ 5 コンソールポートで、Threat Defense デバイスを再起動します。

reboot

例：

yes と入力して再起動します。

例：

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

ステップ 6 ブートアップ中に ROMMON プロンプトを表示するよう要求されたら、Esc を押します。

モニタを注視します。

例：

```
[...]
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.
```

この時点で、Esc を押します。

次のメッセージが表示された場合は、時間がかかりすぎています。起動の終了後、再度 脅威に対する防御 をリロードする必要があります。

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

ステップ 7 脅威に対する防御 上のすべてのディスクを消去します。内部フラッシュは disk0 と呼ばれます。外部 USB ドライブがある場合、そのドライブは disk1 です。

例：

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

rommon 2 >
```

この手順では、古い 脅威に対する防御 ブート イメージとシステム イメージを消去します。システム イメージを消去しない場合は、次の手順でブート イメージをロードした後に、ブート プロセスをエスケープする必要があります。エスケープ ウィンドウが表示されない場合、脅威に対する防御 は古い 脅威に対する防御 システム イメージのロードを続行します。これには時間がかかることがあり、その場合は、この手順を再度開始する必要があります。

ステップ 8 次の ROMMON コマンドを使用して、ネットワーク設定を指定し、新しいブート イメージをロードします。

interface *interface_id*

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file *path/filename*

set

sync

tftpdnld

Threat Defense ブート イメージがダウンロードされ、ブート CLI にブートアップされます。

（注） 前の手順でディスクを消去しなかった場合は、Esc を押してブート CLI に入る必要があります。

```
==============================================
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 ...
...
```

次の情報を参照してください。

- **interface**：（ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X のみ）インターフェイス ID を指定します。他のモデルは常に管理 1/1 インターフェイスを使用します。
- **set**：ネットワーク設定を表示します。**ping** コマンドを使用してサーバへの接続を確認することもできます。
- **sync**：ネットワーク設定を保存します。
- **tftpdnld**：ブート イメージをロードします。

例：

ASA 5508-X の例：

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

ASA 5555-X の例：

```
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
```

サーバーへの接続をトラブルシューティングするには、Ping を実行します。

```
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 >
```

ステップ 9 **setup** と入力して、管理インターフェイスのネットワーク設定を行い、システム ソフトウェア パッケージをダウンロードしてインストールできるようにHTTPまたはFTPサーバーへの一時的な接続を確立します。

（注） DHCPサーバーがある場合、Threat Defense は自動的にネットワーク設定を実行します。DHCP を使用する場合は、次のサンプルの起動メッセージを参照してください。

```
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
```

例：

```
                  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>
```

ステップ 10 Threat Defense システム ソフトウェアのインストール パッケージをダウンロードします。この手順では、HTTP のインストールを示します。

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

確認メッセージに応答しない場合は、**noconfirm** オプションを指定します。

例：

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

内部フラッシュ ドライブを消去するように求められます。**y** と入力します。

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

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

インストール プロセスによってフラッシュ ドライブが消去され、システム イメージがダウンロードされます。インストールを続行するように求められます。**y** と入力します。

```
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
```

インストールが完了したら、 **Enter** キーを押してデバイスをリブートします。

```
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.
```

リブートには約30分かかりますが、より長時間かかる可能性があります。再起動時に、Threat Defense CLI が表示されます。

ステップ 11 ネットワーク接続をトラブルシューティングするには、次の例を参照してください。

例：

ネットワーク インターフェイスの設定の表示

```
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)
...
```

サーバーに対して ping を実行します。

```
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>
```

traceroute を使用して、ネットワーク接続をテストします。

```
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>
```

ステップ 12 インストールの失敗をトラブルシューティングするには、次の例を参照してください。

例：

「Timed out」エラー

ダウンロード段階で、ファイルサーバーに到達できない場合は、タイムアウトが原因で失敗します。

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

timed out
Upgrade aborted
firepower-boot>
```

この場合は、ASA からファイル サーバーに到達可能であることを確認します。ファイル サーバに ping を実行することで確認できます。

「Package not found」エラー

ファイル サーバーに到達可能であっても、ファイル パスまたは名前が間違っている場合は、「Package not found」というエラーでインストールが失敗します。

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

Package not found. Please correct the URL, which should include the full path including
 package name.
```

```
Upgrade aborted.
firepower-boot>
```

この場合は、Threat Defense パッケージのファイルパスと名前が正しいことを確認します。

インストールが不明なエラーで失敗した

システム ソフトウェアのダウンロード後にインストールが行われると、原因は通常、「Installation failed with unknown error」と表示されます。このエラーが発生した場合は、インストール ログを表示して失敗をトラブルシューティングできます。

```
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 ...
...
```

また、ブート CLI 関連の問題に対して同じコマンドを使用して、/var/log/cisco の下にある upgrade.log、pyos.log、commandd.log を表示することもできます。

ステップ 13 Device Manager または Management Center を使用してデバイスを管理できます。セットアップに進むには、http://www.cisco.com/go/ftd-asa-quick でご使用のモデルとマネージャのクイック スタート ガイドを参照してください。

ASA→ASA：ASA 5500-X または ISA 3000

起動できない場合は、ROMMON を使用してイメージを起動できます。その後、ASA OS からフラッシュメモリに新しいイメージファイルをダウンロードできます。

手順

ステップ 1 ASA の電源を切ってから、再び電源をオンにします。

ステップ 2 スタートアップの間に、ROMMONモードに入るようにプロンプト表示されたら、**Escape**キーを押します。

ステップ 3 ROMMONモードで、IPアドレス、TFTPサーバアドレス、ゲートウェイアドレス、ソフトウェアイメージファイル、およびポートを含む、ASAに対するインターフェイス設定を次のように定義します。

```
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
```

（注） ネットワークへの接続がすでに存在することを確認してください。

インターフェイスコマンドはASA 5506-X、ASA 5508-X、ASA 5516-X、およびISA 3000プラットフォームで無視されるため、これらのプラットフォームでManagement 1/1インターフェイスからTFTPリカバリを実行する必要があります。

ステップ 4 設定を検証します。

```
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
```

ステップ 5 TFTPサーバーにpingを送信します。

```
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)
```

ステップ 6 ネットワーク設定を、後で使用できるように保管しておきます。

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

ステップ 7 システムソフトウェアイメージをロードします。

```
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...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 8 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

次のステップ

ご使用のモデルと管理アプリケーションのクイック スタート ガイドを参照してください。

- ASA 5506-X
  - ASA 5506-X シリーズ用 Firepower Device Manager
  - ASA 5506-X シリーズ用 Firepower Management Center
  - ASA 5506-X シリーズ用 ASA
- ASA 5508-X/5516-X
- ASA 5512-X ～ ASA 5555-X
  - ASA 5512-X ～ ASA 5555-X シリーズ用 Firepower Device Manager
  - ASA 5512-X ～ ASA 5555-X シリーズ用 Firepower Management Center
  - ASA 5512-X ～ ASA 5555-X シリーズ用 ASA
- Firepower 1010
- Firepower 1100
- Firepower 2100
- Cisco Secure Firewall 3100

- Cisco Secure Firewall 4200
- ISA 3000

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。