Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드

최종 변경: 2024년 12월 23일

Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드

이 가이드에서는 Secure Firewall ASA와 Secure Firewall Threat Defense(이전 명칭 Firepower Threat Defense)) 간 새 이미지 버전을 사용하는 방법과 새 이미지 버전으로 Threat Defense의 새 이미지 버전을 수행하는 방법을 설명합니다. 이 방법은 업그레이드와 다르며 Threat Defense를 공장 기본 상태로 설정합니다. ASA 이미지 재설치의 경우 여러 가지의 ASA 이미지 재설치 방법을 사용할 수 있는 ASA 일반 운영 설정 가이드를 참조하십시오.

지원되는 모델

다음 모델은 ASA 소프트웨어 또는 Threat Defense 소프트웨어를 지원합니다. ASA 및 Threat Defense 버전 지원에 대한 자세한 내용은 ASA 호환성 가이드 또는 Cisco Secure Firewall Threat Defense 호환성 가이드를 참조하십시오.

- Firepower 1000
- Secure Firewall 1200
- Firepower 2100(Threat Defense 7.4 이전 버전, ASA 9.20 이전 버전)
- Secure Firewall 3100
- Secure Firewall 4200
- ISA 3000
- ASA 5506-X, 5506W-X 및 5506H-X(Threat Defense 6.2.3 이전 버전, ASA 9.16 이전 버전)
- ASA 5508-X(Threat Defense 7.0 이전 버전, ASA 9.16 이전 버전)
- ASA 5512-X(Threat Defense 6.2.3 이전 버전, ASA 9.12 이전 버전)
- ASA 5515-X(Threat Defense 6.4 이전 버전, ASA 9.12 이전 버전)
- ASA 5516-X(Threat Defense 7.0 이전 버전, ASA 9.16 이전 버전)
- ASA 5525-X(Threat Defense 6.6 이전 버전, ASA 9.14 이전 버전)
- ASA 5545-X(Threat Defense 6.6 이전 버전, ASA 9.14 이전 버전)

- ASA 5555-X(Threat Defense 6.6 이전 버전, ASA 9.14 이전 버전)

참고 Firepower 4100 및 9300 또한 ASA나 Threat Defense를 지원하지만 논리적 디바이스로 설치됩니다. 자세한 내용은 FXOS 컨피그레이션 가이드를 참조하십시오.

참고 ASA 5512-X~5555-X의 Threat Defense의 경우 Cisco SSD(Solid State Drive)를 설치해야 합니다. 자세한 내용은 ASA 5500-X 하드웨어 가이드를 참조하십시오. ASA에서는 ASA FirePOWER 모듈을 사용하려는 경우에도 SSD가 필요합니다. (ASA 5506-X, 5508-X, 5516-X에서는 SSD가 표준입니다.)

Firepower 또는 Secure Firewall 이미지 재설치

Firepower 및 Secure Firewall 모델은 Threat Defense 또는 ASA 소프트웨어를 지원합니다.

소프트웨어 다운로드

Threat Defense 소프트웨어 또는 ASA 소프트웨어를 가져옵니다.

참고 Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

표 *1: Threat Defense* 소프트웨어

Threat Defense 모델	다운로드 위치	패키지
Firepower 1000	참조 페이지: https://www.cisco.com/go/ftd-software	
	Threat Defense package 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-ftd-fp1k.7.4.1-172**SPA**와 같은 형식입니다.
Secure Firewall 1200	참조 페이지: https://www.cisco.com/go/ftd-software	
	Threat Defense package 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 Cisco_Secure_FW_TD_1200-7.6.0-01.sh.REL.**tar**와 같은 형식입니다.
Firepower 2100	참조 페이지: https://www.cisco.com/go/ftd-software	
	Threat Defense package 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-ftd-fp2k.7.4.1-172**SPA**와 같은 형식입니다.
Secure Firewall 3100	참조 페이지: https://www.cisco.com/go/ftd-software	
	Threat Defense package 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	• 7.3 이상 —패키지의 파일 이름은 Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.**tar**와 같은 형식입니다. • 7.2—패키지의 파일 이름은 cisco-ftd-fp3k.7.2.6-127.**SPA**와 같은 형식입니다.
Secure Firewall 4200	참조 페이지: https://www.cisco.com/go/ftd-software	
	Threat Defense package 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 Cisco_Secure_FW_TD_4200-7.4.1-172.sh.REL.**tar**와 같은 형식입니다.

표 *2: ASA* 소프트웨어

ASA 모델	다운로드 위치	패키지
Firepower 1000	참조 페이지: https://www.cisco.com/go/asa-firepower-sw	
	ASA 패키지 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-asa-fp1k.9.20.2.2.**SPA**와 같은 형식입니다. 이 패키지에는 항상 ASA와 ASDM을 포함합니다.
	ASDM 소프트웨어**(**업그레이드**)** 현재 ASDM 또는 ASA CLI를 사용하여 최신 버전의 ASDM으로 업그레이드하려면 사용 중인 *model(*모델*)* > **Adaptive Security Appliance(ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-7202**.bin**과 같은 형식입니다.
Secure Firewall 1200		
Firepower 2100	참조 페이지: https://www.cisco.com/go/asa-firepower-sw	
	ASA 패키지 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-asa-fp2k.9.20.2.2.**SPA**와 같은 형식입니다. 이 패키지에는 ASA, ASDM, FXOS 및 Secure Firewall 섀시 관리자 (이전 명칭은 Firepower Chassis Manager) 가 포함되어 있습니다.
	ASDM 소프트웨어**(**업그레이드**)** 현재 ASDM 또는 ASA CLI를 사용하여 최신 버전의 ASDM으로 업그레이드하려면 사용 중인 *model(*모델*)* > **Adaptive Security Appliance(ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-7202**.bin**과 같은 형식입니다.

ASA 모델	다운로드 위치	패키지
Secure Firewall 3100	참조: https://cisco.com/go/sa-secure-firewall-sw	
	ASA 패키지 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-asa-fp3k.9.20.2.2.**SPA**와 같은 형식입니다. 이 패키지에는 항상 ASA와 ASDM을 포함합니다.
	ASDM 소프트웨어**(**업그레이드**)** 현재 ASDM 또는 ASA CLI를 사용하여 최신 버전의 ASDM으로 업그레이드하려면 사용 중인 *model(*모델*)* > **Adaptive Security Appliance(ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-7202**.bin**과 같은 형식입니다.
Secure Firewall 4200 Series	참조: https://cisco.com/go/sa-secure-firewall-sw	
	ASA 패키지 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-asa-fp4200.9.20.2.2.**SPA**와 같은 형식입니다. 이 패키지에는 항상 ASA와 ASDM을 포함합니다.
	ASDM 소프트웨어**(**업그레이드**)** 현재 ASDM 또는 ASA CLI를 사용하여 최신 버전의 ASDM으로 업그레이드하려면 사용 중인 *model(*모델*)* > **Adaptive Security Appliance(ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-7202**.bin**과 같은 형식입니다.

ASA→Threat Defense: Firepower 또는 Secure Firewall

이 작업은 ASA 소프트웨어에서 Threat Defense 이미지를 부팅하여 Firepower 또는 Secure Firewall 디바이스를 ASA에서 Threat Defense로 이미지 재설치할 수 있습니다.

시작하기 전에

- 업로드할 이미지가 FTP, HTTP(S), SCP, SMB, TFTP 서버 또는 EXT2/3/4 또는 VFAT/FAT32로 포맷된 USB 드라이브에서 사용할 수 있는지 확인합니다.

참고 ASA에 강력한 암호화 라이선스가 없는 경우(예: 등록하지 않은 경우) SCP 또는 HTTPS 같은 보안 프로토콜을 사용할 수 없습니다.

- ASA 인터페이스를 통해 서버에 연결할 수 있는지 확인합니다. 새 기본 구성에는 다음이 포함되어 있습니다.
  - 이더넷 1/2—192.168.1.1
  - 관리 1/1 - Firepower 1010 및 Secure Firewall 1210/1220: 192.168.45.1, 기타 모델: DHCP 및 기본 경로
  - 이더넷 1/1 — DHCP 및 기본 경로

  configure factory-default 명령을 사용하여 관리 1/1(Firepower 1010 및 Secure Firewall 1210/1220) 또는 이더넷 1/2(기타 모델)에 대해 고정 IP 주소를 설정할 수도 있습니다. 경로를 구성하려면 **route** 명령을 참조하십시오.
- (Firepower 2100) 9.12 이전 버전에서는 플랫폼 모드만 사용할 수 있습니다. 9.13 이상에서는 어플라이언스 모드가 기본값입니다. 플랫폼 모드 디바이스를 9.13 이상으로 업그레이드하는 경우 ASA는 플랫폼 모드로 유지됩니다. ASA CLI에서 **show fxos mode** 명령을 사용하여 모드를 확인합니다. 다른 모델은 어플라이언스 모드만 지원합니다.

  플랫폼 모드의 ASA가 있는 경우, FXOS를 사용하여 이미지를 재설치해야 합니다. ASA→Threat Defense: Firepower 2100 플랫폼 모드, 9 페이지을 참조하십시오.
- (Secure Firewall 3100) ASA에서 Secure Firewall 3100에 위협 방어 7.3 이상으로 이미지를 재설치하려면, 먼저 ASA를 9.19 이상으로 업그레이드하여 7.3에 도입된 새로운 이미지 유형을 지원하도록 ROMMON 버전을 업데이트해야 합니다. ASA 업그레이드 가이드를 참조하십시오.

프로시저

단계 **1** ASA CLI에 연결합니다.

단계 **2** Smart Software Licensing 서버(ASA CLI/ASDM 또는 Smart Software Licensing 서버)에서 ASA 등록을 취소합니다.

license smart deregister

예제**:**

```
ciscoasa# license smart deregister
```

단계 **3** 플래시 메모리에 Threat Defense 이미지를 다운로드합니다. 다음 단계는 FTP 복사를 보여줍니다.

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

USB 드라이브를 사용하려면 **disk2://**을 사용하는 Firepower 2100을 제외하고 **disk1://**를 지정합니다.

예제:

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
```

예제:

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
```

단계 **4** Threat Defense 이미지(방금 업로드한 이미지)를 부팅합니다.

a) 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

예제:

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

b) 현재 구성된 부트 이미지를 표시합니다(있는 경우).

show running-config boot system

사용자의 구성에는 **boot system** 명령이 없을 수 있습니다. 예를 들어 ROMMON에서 원래 ASA 이미지를 설치했거나, 새 디바이스가 있거나 수동으로 명령을 제거했을 수 있습니다.

예제:

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

c) **boot system** 명령이 구성되어 있는 경우 새 부트 이미지를 입력할 수 있도록 해당 명령을 제거합니다.

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

boot system 명령을 구성하지 않은 경우 이 단계를 건너 뜁니다.

예제:

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

d) Threat Defense 이미지를 부팅합니다.

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

다시 로드하라는 프롬프트가 표시됩니다.

예제:

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.
```

예제:

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.
```

단계 **5** 새시의 재부팅이 완료될 때까지 기다립니다.

FXOS가 먼저 나타나지만 Threat Defense가 나타날 때까지 기다려야 합니다.

애플리케이션을 시작하고 애플리케이션에 연결하면 EULA에 동의하고 CLI에서 초기 설정을 수행하라는 프롬프트가 표시됩니다. Secure Firewall device manager(이전 명칭은 Firepower Device Manager) 또는 Secure Firewall Management Center(이전 명칭은 Firepower Management Center)를 사용하여 디바이스를 관리할 수 있습니다. 사용 중인 모델과 Manager용 빠른 시작 가이드 (http://www.cisco.com/go/ftd-asa-quick)를 참조하여 설치를 계속합니다.

예제:

```
[...]
************ 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 플랫폼 모드

이 작업을 사용하면 Firepower 2100의 플랫폼 모드에서 Threat Defense 로 이미지 재설치를 할 수 있습니다.

참고 이 절차를 수행한 뒤 FXOS 관리자 비밀번호가 **Admin123**으로 재설정됩니다.

시작하기 전에

- 이 절차에서는 FXOS CLI를 사용해야 합니다.
- 9.12 이전 버전에서는 플랫폼 모드만 사용할 수 있습니다. 9.13 이상에서는 어플라이언스 모드가 기본값입니다. 플랫폼 모드 디바이스를 9.13 이상으로 업그레이드하는 경우 ASA는 플랫폼 모드로 유지됩니다. ASA CLI에서 **show fxos mode** 명령을 사용하여 9.13 이상에서 모드를 확인합니다.

  ASA의 어플라이언스 모드에는 이러한 FXOS 명령에 액세스할 수 없습니다. Threat Defense 로의 이미지 재설치는 ASA OS에서 진행됩니다. ASA→Threat Defense: Firepower 또는 Secure Firewall, 5 페이지를 참조하십시오.

프로시저

단계 **1** 업로드하려는 이미지가 FTP, SCP, SFTP, FXOS 관리 1/1 인터페이스에 연결된 TFTP 서버, EXT2/3/4 또는 VFAT/FAT32로 포맷된 USB 드라이브에서 사용할 수 있는지 확인합니다.

FXOS Management 1/1 IP 주소를 확인하거나 변경하려면 Firepower 2100 시작 가이드를 참조하십시오.

단계 **2** Smart Software Licensing 서버(ASA CLI/ASDM 또는 Smart Software Licensing 서버)에서 ASA 등록을 취소합니다.

단계 **3** 콘솔 포트(기본 설정) 또는 관리 1/1 인터페이스에 대한 SSH를 사용해 FXOS CLI에 연결합니다. 콘솔 포트에서 연결하는 경우 FXOS CLI에 즉시 액세스합니다. FXOS 로그인 자격 증명을 입력합니다. 기본 사용자 이름은 **admin**이고 기본 비밀번호는 **Admin123**입니다.

SSH를 사용해 ASA 관리 IP 주소에 연결하는 경우 FXOS에 액세스하기 위해 **connect fxos**를 입력합니다. FXOS 관리 IP 주소로 직접 SSH할 수도 있습니다.

단계 **4** 섀시에 패키지를 다운로드합니다.

a) 펌웨어 모드를 입력합니다.

scope firmware

예제:

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

b) 패키지를 다운로드합니다.

download image *url*

다음 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **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*

예제:

```
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) 다운로드 프로세스를 모니터링합니다.

show download-task

예제:

```
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 #
```

단계 **5** 새 패키지 다운로드가 완료되면(**Downloaded(**다운로드됨**)** 상태) 패키지를 부팅합니다.

a) 새 패키지의 버전 번호를 확인하고 복사합니다.

show package

예제:

```
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) 패키지를 설치합니다.

주의
이 단계에서는 구성을 지웁니다.

scope auto-install

install security-pack version *version*

show package 출력에서 **security-pack version** 번호용으로 **Package-Vers** 값을 복사합니다. 섀시에 이미지가 설치되고 재부팅됩니다. 이 프로세스는 약 5분 정도 걸립니다.

참고
아래와 같은 오류가 표시되면 패키지 버전 대신 패키지 이름을 입력했을 수 있습니다.

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

예제:

```
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 #
```

단계 **6** 섀시의 재부팅이 완료될 때까지 기다립니다.

FXOS가 먼저 표시되지만 Threat Defense 가 시작될 때까지 기다려야 합니다.

애플리케이션을 시작하고 애플리케이션에 연결하면 EULA에 동의하고 CLI에서 초기 설정을 수행하라는 프롬프트가 표시됩니다. device manager 또는 Management Center를 사용하여 디바이스를 관리할 수 있습니다. 사용 중인 모델과 Manager용 빠른 시작 가이드(http://www.cisco.com/go/ftd-asa-quick)를 참조하여 설치를 계속합니다.

예제:

```
[...]
************ 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 또는 Secure Firewall

이 작업은 Firepower 또는 Secure Firewall 디바이스를 Threat Defense에서 ASA로 이미지 재설치할 수 있습니다. Firepower 2100의 경우 기본적으로 ASA는 어플라이언스 모드에 있습니다. 이미지를 재설치한 후에는 ASA를 플랫폼 모드로 변경할 수 있습니다.

참고 이 절차를 수행한 뒤 FXOS 관리자 비밀번호가 **Admin123**으로 재설정됩니다.

프로시저

단계 **1** 업로드하려는 이미지가 관리 1/1 인터페이스 또는 Secure Firewall 4200, 관리 1/1 또는 1/2에 연결된 FTP, HTTP(S), SCP, SFTP 또는 TFTP 서버 또는 EXT2/3/4 또는 VFAT/FAT32로 포맷된 USB 드라이브에서 사용할 수 있는지 확인합니다.

관리 인터페이스 설정에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense 명령 참조에서 Threat Defense **show network** 및 **configure network** 명령을 참조하십시오.

단계 **2** Threat Defense의 라이선스를 해제합니다.

- Management Center에서 Threat Defense를 관리하는 경우 Management Center에서 디바이스를 삭제합니다.
- device manager를 사용해 Threat Defense을 관리하는 경우 Smart Software Licensing 서버(device manager 또는 Smart Software Licensing 서버)에서 디바이스 등록을 취소해야 합니다.

단계 **3** 콘솔 포트(기본 설정) 또는 관리 인터페이스에 대한 SSH를 사용해 FXOS CLI에 연결합니다. 콘솔 포트에서 연결하는 경우 FXOS CLI에 즉시 액세스합니다. FXOS 로그인 자격 증명을 입력합니다. 기본 사용자 이름은 **admin**이고 기본 비밀번호는 **Admin123**입니다.

SSH를 사용해 Threat Defense 관리 IP 주소에 연결하는 경우 FXOS에 액세스하기 위해 **connect fxos**를 입력합니다.

단계 **4** 섀시에 패키지를 다운로드합니다.

a) 펌웨어 모드를 입력합니다.

scope firmware

예제:

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

b) 패키지를 다운로드합니다.

download image *url*

다음 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **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*

예제:

```
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) 다운로드 프로세스를 모니터링합니다.

show download-task

예제:

```
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 #
```

단계 **5** 새 패키지 다운로드가 완료되면(**Downloaded(**다운로드됨**)** 상태) 패키지를 부팅합니다.

a) 새 패키지의 버전 번호를 확인하고 복사합니다.

show package

예제:

```
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) 패키지를 설치합니다.

주의
이 단계에서는 구성을 지웁니다.

scope auto-install

install security-pack version *version*

show package 출력에서 **security-pack version** 번호용으로 **Package-Vers** 값을 복사합니다. 섀시가 이미지를 설치하고 재부팅합니다. 이 프로세스는 재로딩을 포함해 약 30분 정도 소요됩니다.

참고
아래와 같은 오류가 표시되면 패키지 버전 대신 패키지 이름을 입력했을 수 있습니다.

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

예제:

```
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 #
```

단계 **6** 섀시의 재부팅이 완료될 때까지 기다립니다.

ASA 9.13 이상**(**어플라이언스 모드에 기본값**)**

ASA가 시작되고 CLI에서 사용자 EXEC 모드에 액세스합니다.

예제:

```
[...]
```

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

ASA 9.12 이전**(**플랫폼 모드에 기본값**)**

FXOS가 먼저 표시되지만 ASA가 시작될 때까지 기다려야 합니다.

애플리케이션이 시작되고 애플리케이션에 연결하면 CLI에서 사용자 EXEC 모드에 액세스합니다.

예제**:**

```
 [...]
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 또는 Secure Firewall

Secure Firewall 3100에만 해당하는 경우, 이미지 재설치 방법은 최신 버전에 따라 달라집니다.

Threat Defense→Threat Defense: Firepower 또는 Secure Firewall(3100 제외)

이러한 모델은 구성만 삭제하는 것부터 이미지를 교체하여 공장 기본 상태로 디바이스를 복원하는 등 여러 수준의 이미지 재설치를 제공합니다.

프로시저

단계 **1** 이미지 재설치 절차에 대한 자세한 내용은 문제 해결 가이드를 참조하십시오.

단계 **2** 새 버전을 로드하려면 "새 소프트웨어 버전으로 시스템 이미지 재설치" 절차를 사용합니다.

부트 불가 또는 비밀번호 재설정과 같은 문제 해결을 위해 다른 이미지 재설치 방법을 사용합니다.

Threat Defense→Threat Defense: Secure Firewall 3100

Secure Firewall 3100은 구성만 삭제하는 것부터 이미지를 교체하여 공장 기본 상태로 디바이스를 복원하는 등 여러 수준의 이미지 재설치를 제공합니다. 시작 및 종료 버전에 따라 이미지 재설치에 대한 다음 옵션을 참조하십시오.

프로시저

단계 **1** **7.2**로 이미지 재설치 또는 **7.3** 이상에서 **7.3** 이상으로 이미지 재설치**:** 이미지 재설치 절차에 대한 자세한 내용은 문제 해결 가이드를 참조하십시오.

새 버전을 로드하려면 "새 소프트웨어 버전으로 시스템 이미지 재설치" 절차를 사용합니다.

부트 불가 또는 비밀번호 재설정과 같은 문제 해결을 위해 다른 이미지 재설치 방법을 사용합니다.

단계 **2** **7.1/7.2**에서 **7.3** 이상으로 이미지 재설치**:** 7.1/7.2에서 7.3 이상으로 이미지 재설치하려는 경우, 먼저 ASA 9.19 이상으로 이미지 재설치한 다음 7.3 이상으로 이미지 재설치해야 합니다.

7.3 이상에서는 새로운 유형의 이미지 파일을 사용합니다. 이 이미지 파일을 사용하려면 먼저 ROMMON을 업데이트해야 하므로 7.3 이상으로 이미지 재설치하기 전에 ASA 9.19 이상(이전 ROMMON에서도 지원되지만 새 ROMMON으로 업그레이드)로 이미지 재설치해야 합니다. 별도의 ROMMON 업데이터는 없습니다.

참고
7.1/7.2에서 7.3 이상으로 업그레이드하려는 경우 평소와 같이 업그레이드할 수 있습니다. ROMMON은 업그레이드 프로세스의 일부로 업데이트됩니다.

a) 위협 방어를 ASA 9.19 이상으로 이미지 재설치합니다. Threat Defense→ASA: Firepower 또는 Secure Firewall, 13 페이지을 참조하십시오.
b) ASA를 위협 방어 7.3 이상으로 이미지 재설치합니다. ASA→Threat Defense: Firepower 또는 Secure Firewall, 5 페이지의 내용을 참조하십시오.

ASA→ASA: Firepower 및 Secure Firewall

부팅 문제를 해결하고 비밀번호 복구를 수행하려면 ASA 이미지 재설치가 필요할 수 있습니다. 일반 업그레이드 시에는 이미지 재설치를 수행할 필요가 없습니다.

프로시저

단계 **1** 이미지 재설치 절차에 대한 자세한 내용은 문제 해결 가이드를 참조하십시오.

단계 **2** 새 소프트웨어 이미지를 로드하려면 이미지를 재설치하는 대신 ASA 업그레이드 가이드를 참조하십시오.

ASA 5500-X 또는 ISA 3000 이미지 재설치

대다수의 ASA 5500-X 또는 ISA 3000 Series 모델은 Threat Defense 또는 ASA 소프트웨어를 지원합니다.

콘솔 포트 액세스 필요

이미지 재설치를 수행하려면 컴퓨터를 콘솔 포트에 연결해야 합니다.

ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X의 경우 연결을 설정하려면 서드파티 직렬 대 USB 케이블을 사용해야 할 수도 있습니다. 기타 모델은 소형 USB 유형 B 콘솔 포트를 포함하므로 모든 소형 USB 케이블을 사용할 수 있습니다. Windows의 경우, software.cisco.com에서 USB 직렬 드라이버를 설치해야 할 수도 있습니다. 콘솔 포트 옵션과 드라이버 요건에 대한 자세한 내용은 하드웨어 가이드(http://www.cisco.com/go/asa5500x-install)를 참조하십시오.

9600 보드, 8 데이터 비트, 패리티 없음, 1 정지 비트, 흐름 제어 없음에 터미널 에뮬레이터 설정을 사용합니다.

소프트웨어 다운로드

Threat Defense 소프트웨어 또는 ASA, ASDM 및 ASA FirePOWER 모듈 소프트웨어를 가져옵니다. 이 문서의 절차상 초기 다운로드를 위해 TFTP 서버에 소프트웨어를 둬야 합니다. 다른 이미지는 기타 서버 유형(예: HTTP 또는 FTP)에서 다운로드할 수 있습니다. 정확한 소프트웨어 패키지 및 서버 유형의 경우, 절차를 참조하십시오.

참고 Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

주의 Threat Defense 부팅 이미지와 시스템 패키지는 버전별 및 모델별로 적용됩니다. 플랫폼에 따라 올바른 부팅 이미지 및 시스템 패키지가 있는지 확인합니다. 부팅 이미지와 시스템 패키지가 일치하지 않으면 부팅 실패가 발생할 수 있습니다. 새 시스템 패키지와 오래된 부팅 이미지를 사용하면 불일치가 발생합니다.

표 *3: Threat Defense* 소프트웨어

Threat Defense 모델	다운로드 위치	패키지
ASA 5506-X, ASA 5508-X 및 ASA 5516-X	참조 페이지: http://www.cisco.com/go/asa-firepower-sw	참고 또한 **.sh**로 끝나는 패치 파일을 확인할 수 있습니다. 패치 업그레이드 프로세스에 대해서는 이 문서에서 다루지 않습니다.
	부트 이미지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	부트 이미지의 파일 이름은 ftd-boot-9.6.2.0.**lfbff**와 같은 형식입니다.
	시스템 소프트웨어 설치 패키지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	시스템 소프트웨어 설치 패키지의 파일 이름은 ftd-6.1.0-330.**pkg**와 같은 형식입니다.
ASA 5512-X ~ ASA 5555-X	참조 페이지: http://www.cisco.com/go/asa-firepower-sw	참고 또한 **.sh**로 끝나는 패치 파일을 확인할 수 있습니다. 패치 업그레이드 프로세스에 대해서는 이 문서에서 다루지 않습니다.
	부트 이미지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	부트 이미지의 파일 이름은 ftd-boot-9.6.2.0.**cdisk**와 같은 형식입니다.
	시스템 소프트웨어 설치 패키지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	시스템 소프트웨어 설치 패키지의 파일 이름은 ftd-6.1.0-330.**pkg**와 같은 형식입니다.

Threat Defense 모델	다운로드 위치	패키지
ISA 3000	참조: http://www.cisco.com/go/isa3000-software	참고 또한 **.sh**로 끝나는 패치 파일을 확인할 수 있습니다. 패치 업그레이드 프로세스에 대해서는 이 문서에서 다루지 않습니다.
	부트 이미지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	부트 이미지의 파일 이름은 ftd-boot-9.9.2.0**.lfbff**와 같은 형식입니다.
	시스템 소프트웨어 설치 패키지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	시스템 소프트웨어 설치 패키지의 파일 이름은 ftd-6.2.3-330**.pkg**와 같은 형식입니다.

표 *4: ASA* 소프트웨어

ASA 모델	다운로드 위치	패키지
ASA 5506-X, ASA 5508-X 및 ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA 소프트웨어 사용 중인 *model(모델)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(버전)*을 선택합니다.	ASA 소프트웨어 파일 이름은 asa962-**lfbff-k8.SPA**와 같은 형식입니다.
	ASDM 소프트웨어 사용 중인 *model(모델)* > **Adaptive Security Appliance (ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(버전)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-762**.bin**과 같은 형식입니다.
	REST API 소프트웨어 사용 중인 *model(모델)* > **Adaptive Security Appliance REST API Plugin(Adaptive Security Appliance REST API** 플러그인**)** > *version(버전)*을 선택합니다.	API 소프트웨어 파일 이름은 asa-restapi-132-**lfbff-k8.SPA**와 같은 형식입니다. REST API를 설치하려면 API 빠른 시작 가이드를 참조하십시오.
	ROMMON 소프트웨어 사용 중인 *model(모델)* > **ASA Rommon Software(ASA Rommon** 소프트웨어**)** > *version(버전)*을 선택합니다.	ROMMON 소프트웨어 파일 이름은 asa5500-firmware-1108**.SPA**와 같은 형식입니다.

ASA 모델	다운로드 위치	패키지
ASA 5512-X ~ ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA 소프트웨어 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **Adaptive Security Appliance(ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	ASA 소프트웨어 파일 이름은 asa962-**smp-k8.bin**과 같은 형식입니다.
	ASDM 소프트웨어 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **Adaptive Security Appliance(ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-762**.bin**과 같은 형식입니다.
	REST API 소프트웨어 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **Adaptive Security Appliance REST API Plugin(Adaptive Security Appliance REST API** 플러그인**)** > *version(*버전*)*을 선택합니다.	API 소프트웨어 파일 이름은 asa-restapi-132-**lfbff-k8.SPA**와 같은 형식입니다. REST API를 설치하려면 API 빠른 시작 가이드를 참조하십시오.
	Cisco APIC(Application Policy Infrastructure Controller)용 **ASA** 디바이스 패키지 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **ASA for Application Centric Infrastructure (ACI) Device Packages(ACI(Application Centric Infrastructure)**용 **ASA** 디바이스 패키지**)** > *version(*버전*)*을 선택합니다.	APIC 1.2(7) 이상의 경우 Policy Orchestration with Fabric Insertion 또는 Fabric Insertion 전용 패키지를 선택합니다. 디바이스 패키지 소프트웨어 파일 이름은 asa-device-pkg-1.2.7.10**.zip**과 같은 형식입니다. ASA 디바이스 패키지를 설치하려면 Cisco APIC 레이어 4~레이어 7 서비스 구축 가이드의 "디바이스 패키지 가져오기" 장을 참조하십시오.

ASA 모델	다운로드 위치	패키지
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA 소프트웨어 사용 중인 *model(모델)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(버전)*을 선택합니다.	ASA 소프트웨어 파일 이름은 asa962-**lfbff-k8.SPA**와 같은 형식입니다.
	ASDM 소프트웨어 사용 중인 *model(모델)* > **Adaptive Security Appliance (ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(버전)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-762**.bin**과 같은 형식입니다.
	REST API 소프트웨어 사용 중인 *model(모델)* > **Adaptive Security Appliance REST API Plugin(Adaptive Security Appliance REST API** 플러그인**)** > *version(버전)*을 선택합니다.	API 소프트웨어 파일 이름은 asa-restapi-132-**lfbff-k8.SPA**와 같은 형식입니다. REST API를 설치하려면 API 빠른 시작 가이드를 참조하십시오.

ROMMON 이미지 업그레이드(ASA 5506-X, 5508-X 및 5516-X, ISA 3000)

다음 단계에 따라 ASA 5506-X 시리즈, ASA 5508-X, ASA 5516-X 및 ISA 3000용 ROMMON 이미지를 업그레이드합니다. ASA 모델의 경우 시스템에서 ROMMON 버전은 1.1.8 이상이어야 합니다. 최신 버전으로 업그레이드하는 것이 좋습니다.

새 버전으로 업그레이드만 가능하며 다운그레이드할 수 없습니다.

주의 1.1.15용 ASA 5506-X, 5508-X 및 5516-X ROMMON 업그레이드 및 1.0.5용 ISA 3000 ROMMON 업그레이드에는 이전 ROMMON 버전보다 약 2배 더 긴 시간(약 15분)이 소요됩니다. 업그레이드 중에는 디바이스의 전원을 껐다가 켜지 마십시오. 30분 이내에 업그레이드가 완료되지 않거나 실패하면 Cisco 기술 지원에 문의하십시오. 디바이스의 전원을 껐다가 켜거나 재설정하지 마십시오.

시작하기 전에

Cisco.com에서 새 ROMMON 이미지를 가져와 ASA에 복사할 서버에 둡니다. ASA는 FTP, TFTP, SCP, HTTP(S) 및 SMB 서버를 지원합니다. 다음 위치에서 이미지를 다운로드합니다.

- 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

프로시저

단계 **1** Threat Defense 소프트웨어의 경우 진단 CLI를 시작한 다음 활성화 모드를 시작합니다.

system support diagnostic-cli

enable

비밀번호를 입력하라는 메시지가 표시되면 비밀번호를 입력하지 않고 Enter 키를 누릅니다.

예제:

```
> 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#
```

단계 **2** ASA 플래시 메모리에 ROMMON 이미지를 복사합니다. 이 절차에서는 FTP 복사를 보여줍니다. 다른 서버 유형의 경우 **copy ?** 구문을 입력합니다.

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

Threat Defense 소프트웨어의 경우 데이터 인터페이스가 구성되어 있는지 확인합니다. 진단 CLI에서는 전용 관리 인터페이스에 액세스할 수 없습니다. 또한 CSCvn57678로 인해 **copy** 명령이 Threat Defense 버전의 경우 일반 Threat Defense CLI에서 작동하지 않을 수 있으므로 해당 방법으로 전용 관리 인터페이스에 액세스할 수 없습니다.

단계 **3** 현재 버전을 보려면 **show module** 명령을 입력하고 MAC 주소 범위 테이블의 Mod 1에 대한 출력에서 Fw 버전을 확인하십시오.

```
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
```

단계 **4** ROMMON 이미지를 업그레이드합니다.

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

예제:

```
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]
```

단계 **5** 프롬프트가 표시되면 ASA 다시 로드를 확인합니다.

ASA는 ROMMON 이미지를 업그레이드한 다음 운영 체제를 다시 로드합니다.

ASA →Threat Defense: ASA 5500-X 또는 ISA 3000

ASA를 Threat Defense 소프트웨어 이미지로 재설치하려면 ROMMON 프롬프트에 액세스해야 합니다. ROMMON에서는 Threat Defense 부팅 이미지를 다운로드하려면 관리 인터페이스에서 TFTP를 사용해야 합니다. TFTP만 지원됩니다. 그런 다음 부팅 이미지에서 HTTP나 FTP를 사용해 Threat Defense 시스템 소프트웨어 설치 패키지를 다운로드할 수 있습니다. TFTP 다운로드에 시간이 오래 걸릴 수 있습니다. 패킷 손실을 방지하기 위해 ASA와 TFTP 서버 간에 연결이 안정적인지 확인합니다.

시작하기 전에

ASA를 이미지로 다시 설치 프로세스를 쉽게 수행하려면 다음과 같이 하십시오.

1. **backup** 명령을 사용하여 전체 시스템 백업을 수행합니다.

   자세한 내용과 기타 백업 기술은 컨피그레이션 가이드를 참조하십시오.

2. **show activation-key** 명령을 사용하여 라이선스를 재설치할 수 있도록 현재 액티베이션 키를 복사하고 저장합니다.

3. ISA 3000의 경우 Management Center를 사용할 때 하드웨어 바이패스를 비활성화합니다. 이 기능은 버전 6.3 이상의 device manager에서만 사용이 가능합니다.

프로시저

단계 **1** 관리 인터페이스에 있는 ASA에서 액세스 가능한 TFTP 서버에 Threat Defense 부팅 이미지(소프트웨어 다운로드, 18 페이지 참조)를 다운로드합니다.

ASA 5506-X, 5508-X, 5516-X, ISA 3000의 경우 관리 1/1 포트를 사용하여 이미지를 다운로드해야 합니다. 다른 모델의 경우, 모든 인터페이스를 사용할 수 있습니다.

단계 **2** 관리 인터페이스에 있는 ASA에서 액세스 가능한 HTTP 또는 FTP 서버에 Threat Defense 시스템 소프트웨어 설치 패키지(소프트웨어 다운로드, 18 페이지 참조)를 다운로드합니다.

단계 **3** 콘솔 포트에서 ASA를 다시 로드합니다.

reload

예제:

```
ciscoasa# reload
```

단계 **4** 부팅 중에 ROMMON 프롬프트와 연결하라는 메시지가 나타나면 **Esc** 키를 누릅니다.

모니터를 자세히 살펴봅니다.

예제:

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

이 시점에서 **Esc** 키를 누릅니다.

다음 메시지가 나타나고 너무 오래 기다린 경우 부팅을 완료한 후 ASA를 다시 로드해야 합니다.

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

단계 **5** 네트워크 설정을 설정하고 다음 ROMMON 명령을 사용하여 부트 이미지를 로드합니다.

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 부팅 이미지가 다운로드되고 부팅 CLI에 부팅됩니다.

다음 정보를 참조하십시오.

- **interface**- (ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 전용) 관리 인터페이스 ID를 지정합니다. 기타 모델은 항상 관리 1/1 인터페이스를 사용합니다.
- **set**- 네트워크 설정을 표시합니다. 또한 서버에 대한 연결성을 확인하기 위해 **ping** 명령을 사용할 수 있습니다.
- **sync**- 네트워크 설정을 저장합니다.
- **tftpdnld**- 부트 이미지를 로드합니다.

예제:

ASA 5555-X의 예:

```
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-X의 예:

```
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
```

서버 연결 문제를 해결하려면 **Ping**을 실행합니다.

```
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 >
```

단계 **6** **setup**을 입력하고 관리 인터페이스에서 시스템 소프트웨어 패키지를 다운로드 및 설치하기 위한 HTTP 또는 FTP 서버와의 임시 연결을 설정하도록 네트워크 설정을 구성합니다.

참고
DHCP 서버가 있는 경우 Threat Defense는 자동으로 네트워크 구성을 설정합니다. DHCP를 사용할 때는 다음 샘플 시작 메시지를 참조하십시오.

```
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
```

예제:

```
                  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>
```

단계 **7** Threat Defense 시스템 소프트웨어 설치 패키지를 다운로드합니다. 다음 단계는 HTTP 설치를 보여줍니다.

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

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다.

예제**:**

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

내부 플래시 드라이브를 지울 것인지 묻는 프롬프트가 표시됩니다. **Y**를 입력합니다.

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

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

설치 프로세스에서 플래시 드라이브를 지우고 시스템 이미지를 다운로드합니다. 설치를 계속할지 묻는 프롬프트가 표시됩니다. **Y**를 입력합니다.

```
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
```

설치가 완료되면 **Enter** 키를 눌러 디바이스를 재부팅합니다.

```
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.
```

재부팅에는 30분 이상 소요되며 훨씬 더 오래 걸릴 수도 있습니다. 재부팅 시 사용자는 Threat Defense CLI에 있게 됩니다.

단계 **8** 네트워크 연결 문제를 해결하려면 다음 예를 참조하십시오.

예제:

네트워크 인터페이스 컨피그레이션 보기:

```
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)
...
```

서버 **Ping:**

```
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>
```

네트워크 연결 테스트를 위한 트레이스라우트:

```
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>
```

단계 **9** 설치 실패 문제를 해결하려면 다음 예를 참조하십시오.

예제:

"Timed Out(시간 초과**)"** 오류

다운로드 단계에서 파일 서버에 연결할 수 없는 경우 시간 초과 오류가 발생합니다.

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

timed out
Upgrade aborted
firepower-boot>
```

이 경우 ASA에서 파일 서버에 연결할 수 있는지 확인합니다. 파일 서버를 ping하여 확인할 수 있습니다.

"Package Not Found(패키지를 찾을 수 없음**)"** 오류

파일 서버에 연결할 수 있지만 파일 경로 또는 이름이 잘못된 경우 "패키지를 찾을 수 없음" 오류가 발생합니다.

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

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

이 경우 Threat Defense 패키지 파일 경로 및 이름이 올바른지 확인하십시오.

알 수 없는 오류로 설치 실패

일반적으로 시스템 소프트웨어를 다운로드한 후에 설치를 진행하면 일반적으로 "알 수 없는 오류로 설치 실패"가 표시됩니다. 이 오류가 발생하면 설치 로그를 확인하여 장애를 해결할 수 있습니다.

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

또한 부팅 CLI 관련 문제에 대해 동일한 명령을 사용해 /var/log/cisco에서 upgrade.log, pyos.log, commandd.log를 확인할 수 있습니다.

단계 **10** device manager 또는 Management Center를 사용하여 디바이스를 관리할 수 있습니다. 사용 중인 모델과 Manager용 빠른 시작 가이드(http://www.cisco.com/go/ftd-asa-quick)를 참조하여 설치를 계속합니다.

Threat Defense→ASA: ASA 5500-X 또는 ISA 3000

Threat Defense 를 ASA 소프트웨어 이미지로 재설치하려면 ROMMON 프롬프트에 액세스해야 합니다. ROMMON에서 디스크를 지운 다음 ASA 이미지를 다운로드하기 위해 관리 인터페이스에서 TFTP를 사용합니다. 이때 TFTP만 지원됩니다. ASA를 다시 로드한 후, 기본 설정을 구성한 다음 FirePOWER 모듈 소프트웨어를 로드할 수 있습니다.

시작하기 전에

- 패킷 손실을 방지하기 위해 ASA와 TFTP 서버 간에 연결이 안정적인지 확인합니다.

프로시저

단계 **1** Management Center에서 Threat Defense 를 관리하는 경우 Management Center에서 디바이스를 삭제합니다.

단계 **2** device manager를 사용해 Threat Defense 을 관리하는 경우 Smart Software Licensing 서버(device manager 또는 Smart Software Licensing 서버)에서 디바이스 등록을 취소해야 합니다.

단계 **3** 관리 인터페이스에 있는 Threat Defense 에서 액세스 가능한 TFTP 서버에 ASA 이미지(소프트웨어 다운로드, 18 페이지 참조)를 다운로드합니다.

ASA 5506-X, 5508-X, 5516-X, ISA 3000의 경우 관리 1/1 포트를 사용하여 이미지를 다운로드해야 합니다. 다른 모델의 경우, 모든 인터페이스를 사용할 수 있습니다.

단계 **4** 콘솔 포트에서 Threat Defense 디바이스를 재부팅합니다.

reboot

재부팅하려면 **yes**를 입력합니다.

예제:

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

단계 **5** 부팅 중에 ROMMON 프롬프트와 연결하라는 메시지가 나타나면 **Esc** 키를 누릅니다.

모니터를 자세히 살펴봅니다.

예제:

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

이 시점에서 **Esc** 키를 누릅니다.

다음 메시지가 나타나고 너무 오래 기다린 경우 부팅을 완료한 후 Threat Defense 를 다시 부팅해야 합니다.

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

단계 **6** Threat Defense 에서 모든 디스크를 지웁니다. 내부 플래시를 disk0이라고 합니다. 외부 USB 드라이브가 있는 경우, disk1입니다.

예제:

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

이 단계에서는 ASA가 여러 가지 오류를 유발하는 잘못된 컨피그레이션 파일을 로드하려고 시도하지 않도록 Threat Defense 파일을 지웁니다.

단계 **7** 네트워크 설정을 지정하고 다음 ROMMON 명령을 사용하여 ASA 이미지를 로드합니다.

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 이미지가 다운로드되고 CLI에 부팅됩니다.

다음 정보를 참조하십시오.

- **interface-** (ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 전용) 관리 인터페이스 ID를 지정합니다. 기타 모델은 항상 관리 1/1 인터페이스를 사용합니다.
- **set-** 네트워크 설정을 표시합니다. 또한 서버에 대한 연결성을 확인하기 위해 **ping** 명령을 사용할 수 있습니다.
- **sync-** 네트워크 설정을 저장합니다.
- **tftpdnld-** 부트 이미지를 로드합니다.

예제**:**

ASA 5555-X의 예**:**

```
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-X의 예**:**

```
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
```

예제**:**

서버 연결 문제를 해결하려면 **Ping**을 실행합니다**.**

```
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 >
```

단계 **8** 네트워크 설정을 구성하고 디스크를 준비합니다.

ASA가 처음으로 부팅될 때는 컨피그레이션이 없습니다. ASDM 액세스를 위해 관리 인터페이스를 구성하려면 인터랙티브 프롬프트를 따르거나 저장된 컨피그레이션을 붙여 넣을 수 있습니다. 또는 저장된 컨피그레이션이 없는 경우, 권장되는 컨피그레이션(아래)을 붙여 넣을 수 있습니다.

저장된 컨피그레이션이 없는 경우, ASA FirePOWER 모듈을 사용할 계획이라면 권장되는 컨피그레이션을 붙여넣는 것이 좋습니다. ASA FirePOWER 모듈은 관리 인터페이스에서 관리되며 업데이트를 위해 인터넷에 연결해야 합니다. 간단한 권장되는 네트워크 구축은 관리에 연결해주는 내부 스위치(FirePOWER 관리 전용), 내부 인터페이스(ASA 관리 및 내부 트래픽용) 및 동일한 내부 네트워크에 대한 관리 PC를 포함합니다. 네트워크 구축에 대한 자세한 내용은 빠른 시작 가이드를 참조하십시오.

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

a) ASA 콘솔 프롬프트에서 관리 인터페이스에 대한 몇 가지 컨피그레이션을 입력할지 묻는 프롬프트가 표시됩니다.

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

컨피그레이션을 붙여 넣거나 동일한 네트워크 구축을 위해 권장되는 컨피그레이션을 생성하려면 **no**를 입력하고 절차를 계속 진행합니다.

관리 인터페이스를 구성하려는 경우, ASDM에 연결할 수 있으며 **yes**를 입력하고 프롬프트에 따라 작업을 수행합니다.

b) 콘솔 프롬프트에서 권한 있는 EXEC 모드에 액세스합니다.

enable

다음 프롬프트가 나타납니다.

```
Password:
```

c) **Enter**를 누릅니다. 기본적으로 비밀번호는 비어 있습니다.

d) 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

e) 인터랙티브 프롬프트를 사용하지 않은 경우, 프롬프트에서 컨피그레이션을 복사하여 붙여 넣습니다.

저장된 컨피그레이션이 없으나 빠른 시작 가이드에 설명된 대로 간단한 컨피그레이션을 사용하려는 경우, 프롬프트에서 다음 컨피그레이션을 복사하여 IP 주소 및 인터페이스 ID를 알맞게 변경하십시오. 프롬프트를 사용했지만 이 컨피그레이션을 대신 사용하려는 경우 **clear configure all** 명령을 사용하여 컨피그레이션을 먼저 지웁니다.

```
interface gigabitethernetn/n
   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-X의 경우, wifi 인터페이스에 대해 다음을 추가합니다.

```
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) 디스크를 다시 포맷합니다.

format disk0:

format disk1:

내부 플래시를 disk0이라고 합니다. 외부 USB 드라이브가 있는 경우, disk1입니다. 디스크를 다시 포맷하지 않는 경우, ASA 이미지를 복사하려고 시도할 때 다음 오류가 표시됩니다.

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

g) 새 컨피그레이션을 저장합니다.

write memory

단계 **9** ASA 및 ASDM 이미지를 설치합니다.

ROMMON 모드에서 ASA를 부팅해도 다시 로드를 통해 시스템 이미지가 보존되지 않습니다. 플래시 메모리에 이미지를 계속해서 다운로드해야 합니다. 또한 플래시 메모리에 ASDM을 다운로드해야 합니다.

a) ASA 및 ASDM 이미지(소프트웨어 다운로드, 18 페이지 참조)를 ASA에서 액세스 가능한 서버에 다운로드합니다. ASA는 여러 서버 유형을 지원합니다. 자세한 내용은 **copy** 명령을 참조하십시오.
http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2171368.

b) ASA 플래시 메모리에 ASA 이미지를 복사합니다. 다음 단계는 FTP 복사를 보여줍니다.

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

예제:

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

c) ASA 플래시 메모리에 ASDM 이미지를 복사합니다. 다음 단계는 FTP 복사를 보여줍니다.

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

예제:

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

d) ASA를 다시 로드합니다.

reload

disk0의 이미지를 사용하여 ASA를 다시 로드합니다.

단계 **10** (선택 사항) ASA FirePOWER 모듈 소프트웨어를 설치합니다.

이 절차에 따라 ASA FirePOWER 부트 이미지를 설치하고 SSD를 분할하며 시스템 소프트웨어를 설치해야 합니다.

a) 부트 이미지를 ASA에 복사합니다. 시스템 소프트웨어를 전송하지 마십시오. 나중에 SSD로 다운로드됩니다. 다음 단계는 FTP 복사를 보여줍니다.

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

예제:

```
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) Cisco.com의 ASA FirePOWER Services 시스템 소프트웨어 설치 패키지를 관리 인터페이스에서 액세스할 수 있는 HTTP, HTTPS 또는 FTP 서버에 다운로드합니다. ASA의 disk0에 다운로드하지 마십시오.

c) ASA disk0에서 ASA FirePOWER 모듈 부트 이미지 위치를 설정합니다.

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

예제:

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

d) ASA FirePOWER 부트 이미지를 로드합니다.

sw-module module sfr recover boot

예제:

```
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 모듈이 부팅할 때까지 몇 분 정도 기다린 후 현재 실행 중인 ASA FirePOWER 부트 이미지에 대한 콘솔 세션을 엽니다. 로그인 프롬프트로 이동하려면 세션을 연 후 **Enter** 키를 눌러야 할 수 있습니다. 기본 사용자 이름은 **admin**이고 기본 비밀번호는 **Admin123**입니다.

예제:

```
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
```

모듈 부트가 완료되지 않을 경우 session 명령이 실패하고 ttyS1을 통해 연결할 수 없다는 메시지가 표시됩니다. 기다렸다가 다시 시도하십시오.

a) 시스템 소프트웨어 설치 패키지를 설치할 수 있도록 시스템을 구성합니다.

setup

다음에 대한 프롬프트가 표시됩니다. 관리 주소, 게이트웨이 및 DNS 정보는 구성을 위한 핵심 설정입니다.

- 호스트 이름 - 공백 없이 영숫자 최대 65자를 사용합니다. 하이픈은 허용됩니다.
- 네트워크 주소 - 고정 IPv4 또는 IPv6 주소를 사용하거나, DHCP(IPv4용) 또는 IPv6 상태 비저장 자동 컨피그레이션을 설정할 수 있습니다.
- DNS 정보 - 하나 이상의 DNS 서버를 지정해야 합니다. 도메인 이름 및 검색 도메인도 설정할 수 있습니다.
- NTP 정보 - NTP를 활성화하고, 시스템 시간 설정을 위해 NTP 서버를 구성할 수 있습니다.

예제:

```
asasfr-boot> setup

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

a) 다음을 입력하여 시스템 소프트웨어 설치 패키지를 설치합니다.

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

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다. HTTP, HTTPS 또는 FTP URL을 사용합니다. 사용자 이름과 비밀번호가 필요한 경우 입력하라는 메시지가 표시됩니다. 파일이 큰 경우 네트워크 상태에 따라 다운로드하는 데 시간이 오래 걸릴 수 있습니다.

설치가 완료되면 시스템이 다시 부팅됩니다. 애플리케이션 구성 요소 설치 및 ASA FirePOWER Services 시작에 필요한 시간은 매우 다릅니다. 최첨단 플랫폼은 10분 이상의 시간이 걸리지만 사양이 낮은 플랫폼은 60-80분 이상이 소요될 수 있습니다. (**show module sfr** 출력에 모든 프로세스가 UP으로 표시되어야 합니다.)

예제:

```
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) 패치 릴리스를 설치해야 하는 경우, 관리자(ASDM 또는 Management Center)에서 나중에 수행할 수 있습니다.

단계 **11** 액티베이션 키를 저장하지 않은 기존 ASA로 Strong Encryption 라이선스 및 기타 라이선스를 받습니다. 자세한 내용은 http://www.cisco.com/go/license를 참조하십시오. **Manage(**관리**)** > **Licenses(**라이선스**)** 섹션에서 라이선스를 다시 다운로드할 수 있습니다.

ASDM(및 기타 다른 기능)을 사용하려면 강력한 암호화(3DES/AES) 라이선스를 설치해야 합니다. 이전에 Threat Defense 디바이스를 이미지로 재설치하기 전에 이 ASA의 라이선스 액티베이션 키를 저장한 경우, 액티베이션 키를 재설치할 수 있습니다. 액티베이션 키를 저장하지 않았지만 이 ASA에 대해 라이선스를 소유한 경우, 이 라이선스를 다시 다운로드할 수 있습니다. 새로운 ASA의 경우, 새로운 ASA 라이선스를 요청해야 합니다.

단계 **12** 새 ASA용 라이선스를 받습니다.

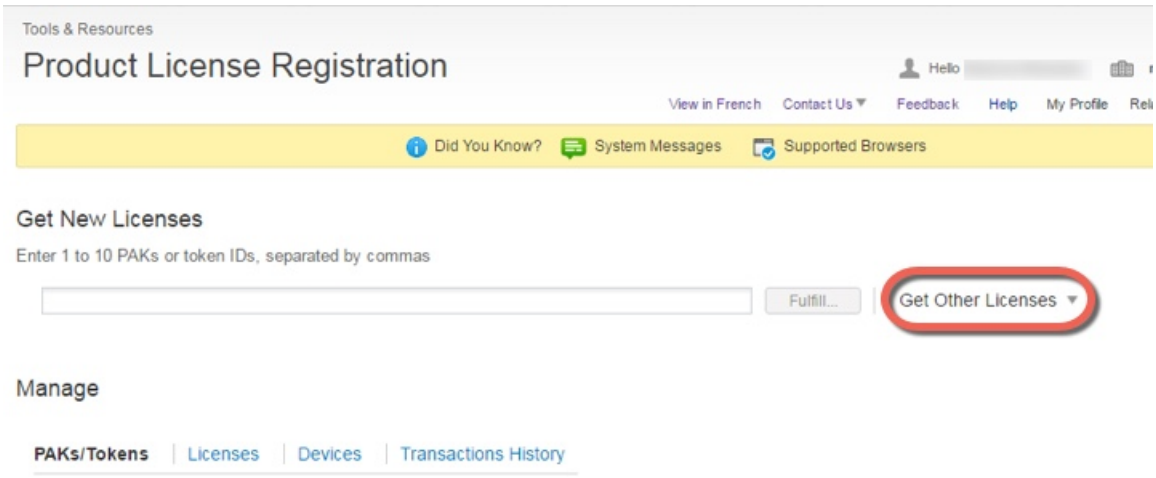
a) 다음 명령을 입력하여 ASA의 시리얼 번호를 가져옵니다.

show version | grep Serial

이 시리얼 번호는 하드웨어 외부에 인쇄된 섀시 시리얼 번호와는 다릅니다. 섀시 시리얼 번호는 기술 지원에 사용되지만 라이선싱에 대해서는 사용되지 않습니다.

b) http://www.cisco.com/go/license를 확인한 후 **Get Other Licenses(**다른 라이선스 가져오기**)**를 클릭합니다.

그림 *1:* 다른 라이선스 가져오기

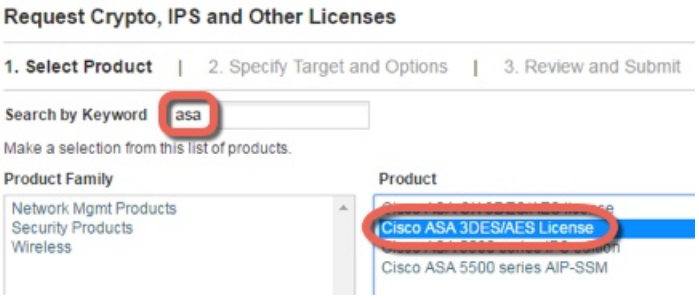


c) **IPS, Crypto, Other(IPS,** 암호화**,** 기타**)**를 선택합니다.

그림 ***2: IPS,*** 암호화, 기타

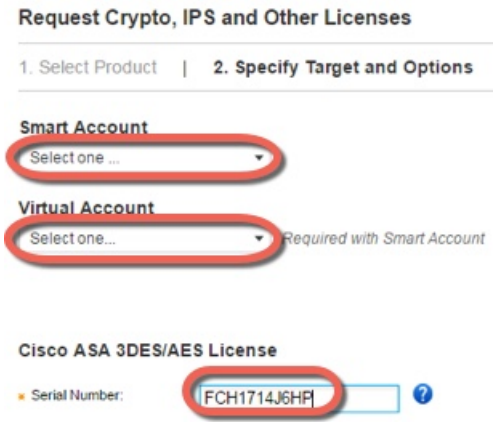
d) **Search by Keyword(**키워드별 검색**)** 필드에서 **asa**를 입력하고 **Cisco ASA 3DES/AES License(Cisco ASA 3DES/AES** 라이선스**)**를 선택합니다.

그림 ***3: Cisco ASA 3DES/AES*** 라이선스



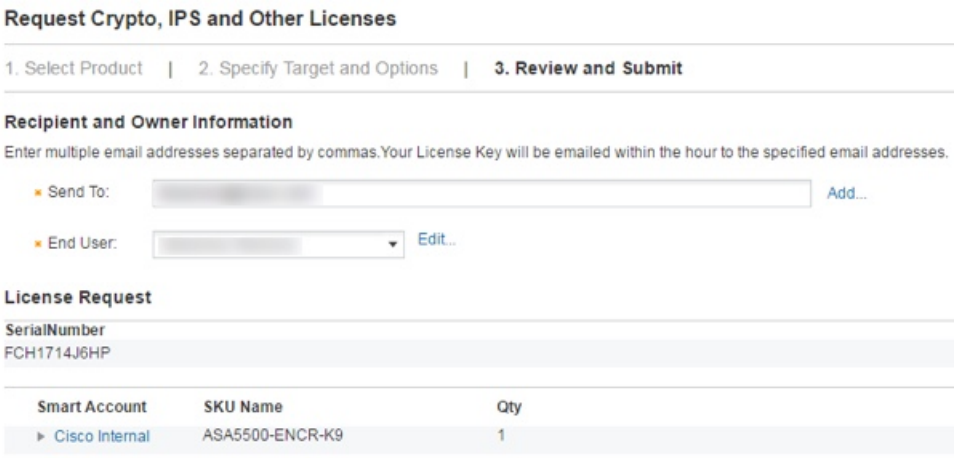
e) **Smart Account(**스마트 어카운트**)**, **Virtual Account(**가상 어카운트**)**를 선택하고 ASA **Serial Number(**시리얼 번호**)**를 입력한 후에 **Next(**다음**)**를 클릭합니다.

그림 ***4:*** 스마트 어카운트, 가상 어카운트, 및 시리얼 번호



f) 이메일 전송 주소 및 최종 사용자 이름이 자동으로 채워집니다. 필요 시 추가 이메일 주소를 입력합니다. **I Agree(**동의합니다**.)** 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다.

그림 *5:* 제출



g) 그러면 액티베이션 키가 포함된 이메일이 수신됩니다. 하지만 **Manage(**관리**)** > **Licenses(**라이선스**)** 영역에서 키를 즉시 다운로드할 수도 있습니다.

h) 기본 라이선스에서 Security Plus 라이선스로 업그레이드하거나 AnyConnect 라이선스를 구매하려는 경우 http://www.cisco.com/go/ccw를 참조하십시오. 라이선스를 구매하면 http://www.cisco.com/go/license에서 입력할 수 있는 PAK(제품 인증 키)가 포함된 이메일을 받게 됩니다. AnyConnect 라이선스의 경우, 사용자 세션의 동일한 풀을 사용하는 여러 ASA에 적용할 수 있는 다용도의 PAK를 받습니다. 결과 액티베이션 키는 영구 라이선스(3DES/AES 포함)에 현재까지 등록한 모든 기능을 포함합니다. 기간별 라이센스의 경우, 각 라이센스에는 별도의 액티베이션 키가 있습니다.

단계 **13** 액티베이션 키를 적용합니다.

activation-key *key*

예제**:**

```
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.
```

이 ASA에서 아직 액티베이션 키를 설치하지 않았으므로 “Failed to retrieve permanent activation key.(영구 액티베이션 키를 검색하는 데 실패했습니다.)” 메시지가 표시됩니다. 이 메시지는 무시하셔도 됩니다.

하나의 영구 키만 설치하고, 여러 개의 기간별 키를 설치할 수 있습니다. 새 영구 키를 입력하면 이전에 설치한 키를 덮어씁니다. 3DES/AES 라이선스를 설치한 후에 추가 라이선스를 주문한 경우, 통합된 액티베이션 키는 3DES/AES 라이선스 외에 모든 라이선스를 포함하므로 3DES/AES 전용 키를 덮어쓸 수 있습니다.

단계 **14** ASA FirePOWER 모듈은 ASA에서 제공되는 별도의 라이선싱 메커니즘을 사용합니다. 라이선스를 미리 설치하지 않았지만 주문에 따라 이 상자는 다음 라이선스에 대한 라이선스 액티베이션 키를 다운로드할 수 있도록 인쇄물에 PAK를 포함할 수 있습니다.

- **Control and Protection(**제어 및 보호**)**. 제어는 "AVC(Application Visibility and Control)" 또는 "앱"이라고도 합니다. 보호는 "IPS"라고도 합니다. 이 라이선스에 대한 액티베이션 키 외에 이러한 기능에 대한 자동화된 업데이트를 위해 "사용 권한" 서브스크립션이 필요합니다.

  Control(제어**)**(AVC) 업데이트는 Cisco 지원 계약에 포함됩니다.

  Protection(보호**)**(IPS) 업데이트의 경우 http://www.cisco.com/go/ccw에서 IPS 서브스크립션을 구매해야 합니다. 이 서브스크립션은 규칙, 엔진, 취약점, 지리적 위치 업데이트에 대한 자격을 포함합니다. 참고**:** 사용 권한 서브스크립션은 ASA FirePOWER 모듈용 PAK/라이선스 액티베이션 키를 생성하거나 요구하지 않으며 업데이트 사용 권한만 제공합니다.

ASA FirePOWER Services를 포함하는 ASA 5500-X를 구매하지 않은 경우, 필요한 라이선스를 다운로드하기 위해 업그레이드 번들을 구매할 수 있습니다. 자세한 내용은 Cisco ASA with FirePOWER Services 주문 가이드를 참조하십시오.

구매할 수 있는 기타 라이선스는 다음과 같습니다.

- **Secure Firewall Threat Defense Malware Defense** 라이선스
- **Secure Firewall Threat Defense URL** 필터링 라이선스

이 라이선스는 ASA FirePOWER 모듈용 PAK/라이선스 액티베이션 키를 생성합니다. 주문 정보는 Cisco ASA with FirePOWER Services 주문 가이드를 참조하십시오. Cisco Secure Firewall Management Center 기능 라이선스의 내용도 참조하십시오.

제어 및 보호 라이선스 및 기타 선택적인 라이선스를 설치하려면, 사용 중인 모델별 ASA 빠른 시작 가이드를 참조하십시오.

Threat Defense→Threat Defense: ASA 5500-X 또는 ISA 3000

이 절차에서는 ROMMON을 사용하여 기존 Threat Defense 을 새 버전의 Threat Defense 소프트웨어로 이미지 재설치하는 방법을 설명합니다. 이 절차는 디바이스를 공장 기본 조건으로 복원합니다. 일반 업그레이드를 수행하려는 경우 업그레이드 가이드를 참조하십시오.

ROMMON에서는 새 Threat Defense 부팅 이미지를 다운로드하려면 관리 인터페이스에서 TFTP를 사용해야 합니다. TFTP만 지원됩니다. 그런 다음 부팅 이미지에서 HTTP나 FTP를 사용해 Threat Defense 시스템 소프트웨어 설치 패키지를 다운로드할 수 있습니다. TFTP 다운로드에 시간이 오래 걸릴 수 있습니다. 패킷 손실을 방지하기 위해 Threat Defense 와 TFTP 서버 간에 연결이 안정적인지 확인합니다.

프로시저

단계 **1** Management Center를 사용해 Threat Defense 을 관리하는 경우 Management Center에서 디바이스를 삭제합니다.

단계 **2** device manager를 사용해 Threat Defense 을 관리하는 경우 Smart Software Licensing 서버(device manager 또는 Smart Software Licensing 서버)에서 디바이스 등록을 취소해야 합니다.

단계 **3** 관리 인터페이스에 있는 Threat Defense 에서 액세스 가능한 TFTP 서버에 Threat Defense 부팅 이미지(소프트웨어 다운로드, 18 페이지 참조)를 다운로드합니다.

ASA 5506-X, 5508-X, 5516-X, ISA 3000의 경우 관리 1/1 포트를 사용하여 이미지를 다운로드해야 합니다. 다른 모델의 경우, 모든 인터페이스를 사용할 수 있습니다.

단계 **4** 관리 인터페이스에 있는 Threat Defense 에서 액세스 가능한 HTTP 또는 FTP 서버에 Threat Defense 시스템 소프트웨어 설치 패키지(소프트웨어 다운로드, 18 페이지 참조)를 다운로드합니다.

단계 **5** 콘솔 포트에서 Threat Defense 디바이스를 재부팅합니다.

reboot

예제:

재부팅하려면 **yes**를 입력합니다.

예제:

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

단계 **6** 부팅 중에 ROMMON 프롬프트와 연결하라는 메시지가 나타나면 **Esc** 키를 누릅니다.

모니터를 자세히 살펴봅니다.

예제:

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

이 시점에서 **Esc** 키를 누릅니다.

다음 메시지가 나타나고 너무 오래 기다린 경우 부팅을 완료한 후 Threat Defense 를 다시 로드해야 합니다.

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

단계 **7** Threat Defense 에서 모든 디스크를 지웁니다. 내부 플래시를 disk0이라고 합니다. 외부 USB 드라이브가 있는 경우, disk1입니다.

예제:

```
Example:
rommon 1 > erase disk0:
```

```
erase: Erasing 7583 MBytes ......................................

rommon 2 >
```

이 단계에서는 이전의 Threat Defense 부팅 및 시스템 이미지를 지웁니다. 시스템 이미지를 삭제하지 않는 경우, 다음 단계에서 부팅 이미지를 로드한 후에 부팅 프로세스를 종료해야 합니다. 만약 종료 창에서 종료하지 않는 경우 Threat Defense 은 계속해서 이전의 Threat Defense 시스템 이미지를 로드하므로 시간이 오래 걸릴 수 있으며 이 절차를 다시 시작해야 합니다.

단계 **8** 네트워크 설정을 설정하고 다음 ROMMON 명령을 사용하여 새 부트 이미지를 로드합니다.

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 부팅 이미지가 다운로드되고 부팅 CLI에 부팅됩니다.

참고
이전 단계에서 디스크를 지우지 않은 경우에는 **ESC** 키를 눌러 부팅 CLI를 시작해야 합니다.

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

다음 정보를 참조하십시오.

- **interface**- (ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 전용) 관리 인터페이스 ID를 지정합니다. 기타 모델은 항상 관리 1/1 인터페이스를 사용합니다.
- **set**- 네트워크 설정을 표시합니다. 또한 서버에 대한 연결성을 확인하기 위해 **ping** 명령을 사용할 수 있습니다.
- **sync**- 네트워크 설정을 저장합니다.
- **tftpdnld**- 부트 이미지를 로드합니다.

예제**:**

ASA 5508-X의 예**:**

```
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-X의 예:

```
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
```

서버 연결 문제를 해결하려면 **Ping**을 실행합니다.

```
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 >
```

단계 **9** **setup**을 입력하고 관리 인터페이스에서 시스템 소프트웨어 패키지를 다운로드 및 설치하기 위한 HTTP 또는 FTP 서버와의 임시 연결을 설정하도록 네트워크 설정을 구성합니다.

참고
DHCP 서버가 있는 경우 Threat Defense는 자동으로 네트워크 구성을 설정합니다. DHCP를 사용할 때는 다음 샘플 시작 메시지를 참조하십시오.

```
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
```

예제:

```
                  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>
```

단계 **10** Threat Defense 시스템 소프트웨어 설치 패키지를 다운로드합니다. 다음 단계는 HTTP 설치를 보여줍니다.

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

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다.

예제**:**

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

내부 플래시 드라이브를 지울 것인지 묻는 프롬프트가 표시됩니다. **Y**를 입력합니다.

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

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

설치 프로세스에서 플래시 드라이브를 지우고 시스템 이미지를 다운로드합니다. 설치를 계속할지 묻는 프롬프트가 표시됩니다. **Y**를 입력합니다.

```
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
```

설치가 완료되면 **Enter** 키를 눌러 디바이스를 재부팅합니다.

```
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.
```

재부팅에는 30분 이상 소요되며 훨씬 더 오래 걸릴 수도 있습니다. 재부팅 시 사용자는 Threat Defense CLI에 있게 됩니다.

단계 **11** 네트워크 연결 문제를 해결하려면 다음 예를 참조하십시오.

예제:

네트워크 인터페이스 컨피그레이션 보기:

```
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)
...
```

서버 **Ping:**

```
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>
```

네트워크 연결 테스트를 위한 트레이스라우트:

```
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>
```

단계 **12** 설치 실패 문제를 해결하려면 다음 예를 참조하십시오.

예제**:**

"Timed Out(시간 초과**)"** 오류

다운로드 단계에서 파일 서버에 연결할 수 없는 경우 시간 초과 오류가 발생합니다.

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

timed out
Upgrade aborted
firepower-boot>
```

이 경우 ASA에서 파일 서버에 연결할 수 있는지 확인합니다. 파일 서버를 ping하여 확인할 수 있습니다.

"Package Not Found(패키지를 찾을 수 없음**)"** 오류

파일 서버에 연결할 수 있지만 파일 경로 또는 이름이 잘못된 경우 "패키지를 찾을 수 없음" 오류가 발생합니다.

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

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

이 경우 Threat Defense 패키지 파일 경로 및 이름이 올바른지 확인하십시오.

알 수 없는 오류로 설치 실패

일반적으로 시스템 소프트웨어를 다운로드한 후에 설치를 진행하면 일반적으로 "알 수 없는 오류로 설치 실패"가 표시됩니다. 이 오류가 발생하면 설치 로그를 확인하여 장애를 해결할 수 있습니다.

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

또한 부팅 CLI 관련 문제에 대해 동일한 명령을 사용해 /var/log/cisco에서 upgrade.log, pyos.log, commandd.log를 확인할 수 있습니다.

단계 **13** device manager 또는 Management Center를 사용하여 디바이스를 관리할 수 있습니다. 사용 중인 모델과 Manager용 빠른 시작 가이드(http://www.cisco.com/go/ftd-asa-quick)를 참조하여 설치를 계속합니다.

ASA→ASA: ASA 5500-X 또는 ISA 3000

부트할 수 없는 경우 ROMMON을 사용하여 이미지를 부트할 수 있습니다. 그러면 ASA OS에서 플래시 메모리로 새 이미지 파일을 다운로드할 수 있습니다.

프로시저

단계 **1** ASA의 전원을 끈 후 전원을 켭니다.

단계 **2** 시작 과정에서 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

단계 **3** ROMMOM 모드에서 다음과 같이 ASA에 대한 인터페이스 설정을 정의합니다. 여기에는 IP 주소, TFTP 서버 주소, 게이트웨이 주소, 소프트웨어 이미지 파일, 포트 등이 포함됩니다.

```
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
```

참고
네트워크에 연결된 상태여야 합니다.

interface 명령은 ASA 5506-X, ASA 5508-X 및 ASA 5516-X, ISA 3000 플랫폼에서 무시되므로 관리 1/1 인터페이스의 해당 플랫폼에서 TFTP 복구를 수행해야 합니다.

단계 **4** 설정을 검증합니다.

```
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
```

단계 **5** TFTP 서버를 ping합니다.

```
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)
```

단계 **6** 나중에 사용하기 위해 네트워크 설정을 저장합니다.

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

단계 **7** 소프트웨어 이미지를 로드합니다.

```
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...
```

소프트웨어 이미지가 성공적으로 로드되면 ASA는 자동으로 ROMMON 모드를 종료합니다.

단계 **8** ROMMON 모드에서 ASA를 부팅해도 다시 로드를 통해 시스템 이미지가 보존되지 않습니다. 플래시 메모리에 이미지를 계속해서 다운로드해야 합니다. 전체 업그레이드 절차에 대한 내용은 Cisco ASA 업그레이드 가이드를 참고하십시오.

다음 단계는 무엇인가요?

사용 중인 모델 및 관리 애플리케이션별 빠른 시작 가이드를 참조하십시오.

- ASA 5506-X

    - Firepower Device Manager용 ASA 5506-X
    - Firepower Management Center용 ASA 5506-X
    - ASA용 ASA 5506-X
- ASA 5508-X/5516-X
- ASA 5512-X ~ ASA 5555-X
    - Firepower Device Manager용 ASA 5512-X~ASA 5555-X
    - Firepower Management Center용 ASA 5512-X~ASA 5555-X
    - ASA용 ASA 5512-X~ASA 5555-X
- Firepower 1010
- Firepower 1100
- Firepower 2100
- Secure Firewall 3100
- Secure Firewall 4200
- ISA 3000