

FDM에서 관리하는 FTD HA 업그레이드

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[배경 정보](#)

[구성](#)

[1단계. 업그레이드 패키지 업로드](#)

[2단계. 준비 상태 확인](#)

[3단계. HA에서 FTD 업그레이드](#)

[4단계. 활성 피어 전환\(선택 사항\)](#)

[5단계. 최종 구축](#)

[유효성 검사](#)

소개

이 문서에서는 Firepower 장치 관리자에서 관리하는 고가용성의 Cisco Secure Firewall Threat Defense의 업그레이드 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- 고가용성(HA) 개념 및 구성
- Cisco Secure FDM(Firepower 장치 관리자) 구성
- Cisco FTD(Secure Firewall Threat Defense) 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 Virtual Cisco FTD, 버전 7.2.8을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

FDM의 작동 방식은 한 번에 한 피어를 업그레이드하는 것입니다. 먼저 Standby를 선택한 다음 Active를 선택하고 Active 업그레이드가 시작되기 전에 장애 조치를 수행합니다.

배경 정보

업그레이드 전에 software.cisco.com에서 업그레이드 패키지를 다운로드해야 합니다.

CLI 클릭에서 활성 FTD에서 `show high-availability configcommand`를 실행하여 HA의 상태를 확인합니다.

```
> show high-availability config
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 3 of 311 maximum
```

```
MAC Address Move Notification Interval not set
```

```
failover replication http
```

```
Version: Ours 9.18(3)53, Mate 9.18(3)53
```

```
Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C
```

```
Last Failover at: 11:57:26 UTC Oct 8 2024
```

```
    This host: Primary - Active
```

```
        Active time: 507441 (sec)
```

```
        slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)
```

```
            Interface diagnostic (0.0.0.0): Normal (Waiting)
```

```
            Interface inside (192.168.45.1): Normal (Waiting)
```

```
            Interface outside (192.168.1.10): Normal (Waiting)
```

```
        slot 1: snort rev (1.0) status (up)
```

```
        slot 2: diskstatus rev (1.0) status (up)
```

```
    Other host: Secondary - Standby Ready
```

```
        Active time: 8 (sec)
```

```
Interface diagnostic (0.0.0.0): Normal (Waiting)
Interface inside (0.0.0.0): Normal (Waiting)
Interface outside (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

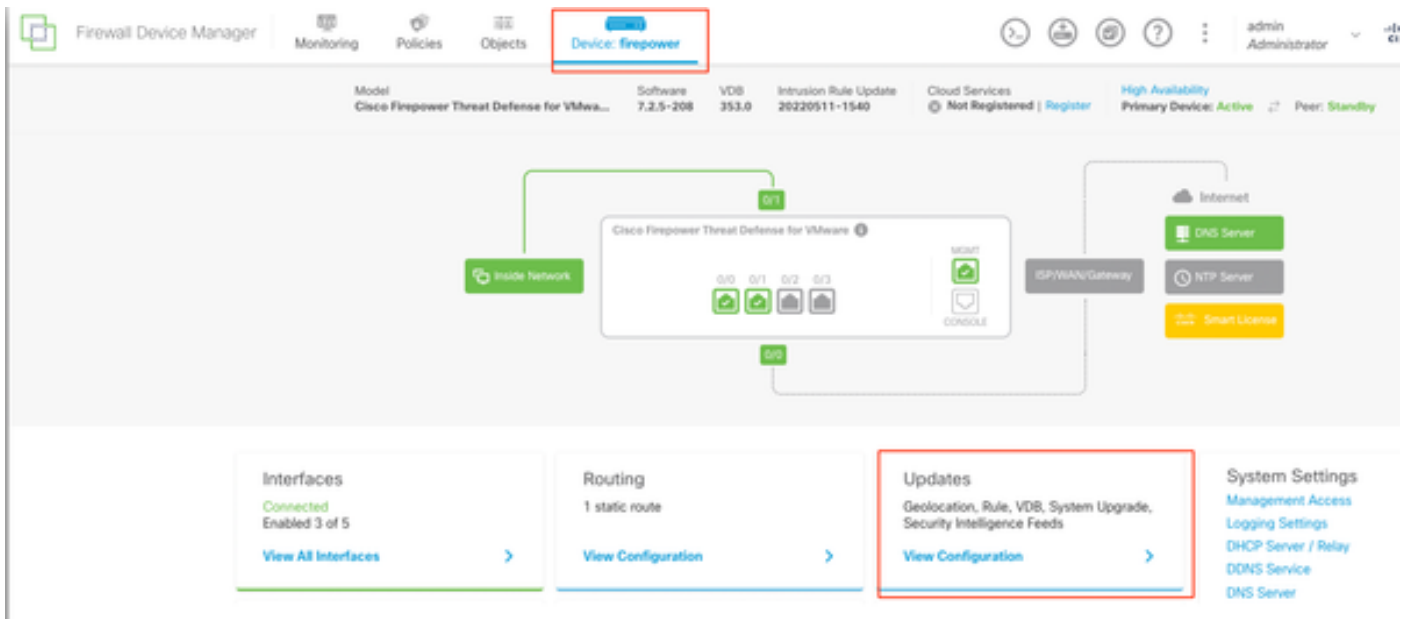
오류가 표시되지 않으면 업그레이드를 계속 진행합니다.

구성

1단계. 업그레이드 패키지 업로드

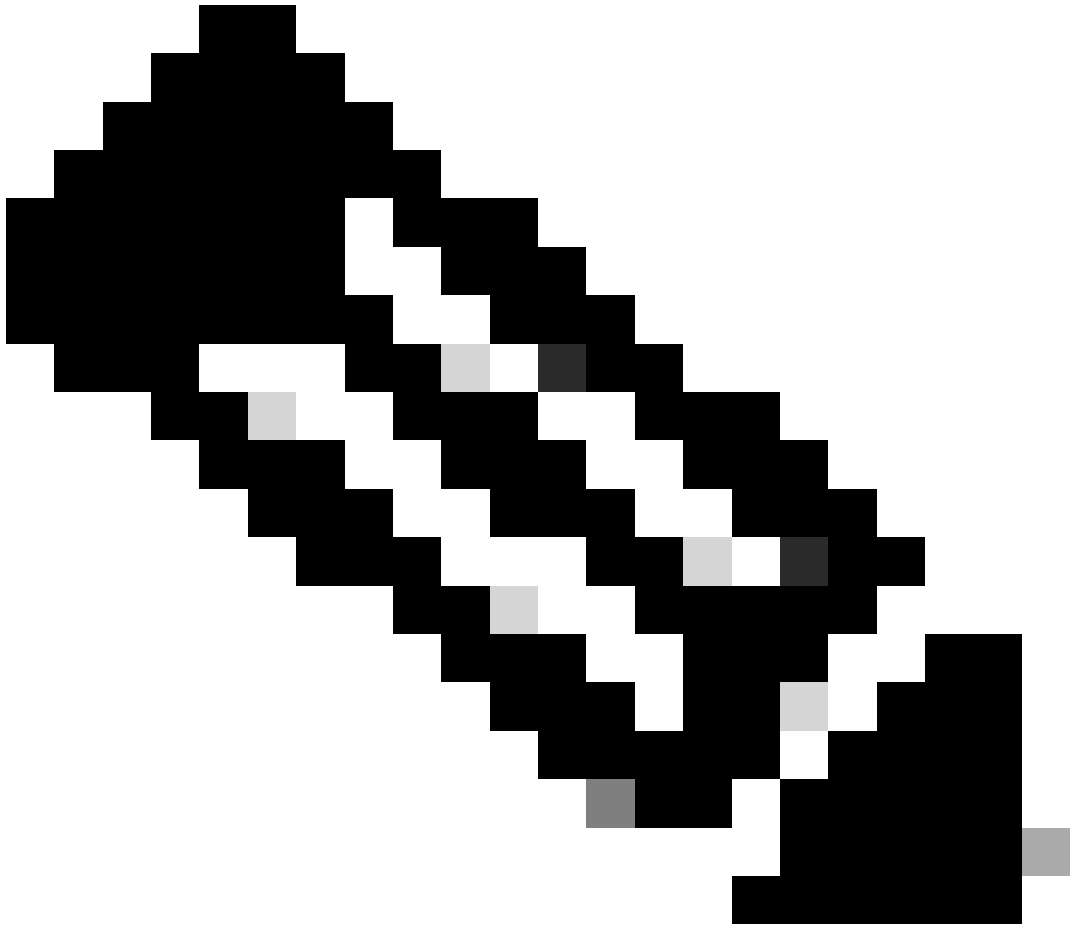
- GUI를 사용하여 FDM에 FTD 업그레이드 패키지를 업로드합니다.

이는 FTD 모델 및 원하는 버전에 따라 Cisco 소프트웨어 사이트에서 이전에 다운로드해야 합니다. Device(디바이스) > Updates(업데이트) > System Upgrade(시스템 업그레이드)로 이동합니다.



업데이트

- 이전에 다운로드한 이미지를 찾은 다음 업로드를 선택합니다.



참고: 활성 및 대기 노드에 이미지를 업로드합니다.

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

There are no software upgrades available on the system.

Upload an upgrade file to install.

BROWSE

준비 검사 실행

2단계. 준비 상태 확인

준비 상태 검사에서는 어플라이언스가 업그레이드를 진행할 준비가 되었는지 확인합니다.


- Run Upgrade Readiness Check를 선택합니다.

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **Not Performed Yet** | [Run Upgrade Readiness Check](#)

UPGRADE NOW


i Reboot required

준비 검사 실행

System Upgrade

Current version 7.2.5-208

i Important
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)


File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL....  Replace file 14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25


Readiness Check	Not Performed Yet	Run Upgrade Readiness Check
-----------------	-------------------	---

UPGRADE NOW **i Reboot required**

준비 상태 검사 실행

i Important
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL....  Replace file 14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25

Readiness Check	 Please Wait...
-----------------	--

UPGRADE NOW **i Reboot required**

준비 검사 실행


System(시스템) > Upgrade(업그레이드)로 이동하여 진행 상황을 확인할 수 있습니다.

System Upgrade


Current version 7.2.5-208

Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check  **Precheck Success** | [Run Upgrade Readiness Check](#)
14 Oct 2024 05:51 PM

UPGRADE NOW

 Reboot required

준비 검사 실행

업그레이드는 FTD에서 모두 준비도 검사가 완료되고 결과가 Success(성공)인 경우에 수행할 수 있습니다.

3단계. HA에서 FTD 업그레이드

- Standby FDM을 선택하고 Upgrade Now를 클릭합니다.

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **✔ Precheck Success** | [Run Upgrade Readiness Check](#)
14 Oct 2024 05:51 PM

UPGRADE NOW

i Reboot required

지금 업그레이드

업그레이드를 시작하기 전에

1. 시스템 업그레이드와 동시에 시스템 복원을 시작하지 마십시오.
2. 업그레이드 중에는 시스템을 재부팅하지 마십시오. 재부팅이 필요한 경우 업그레이드 중 적절한 시간에 시스템이 자동으로 재부팅됩니다.
3. 업그레이드 중에 디바이스의 전원을 끄지 마십시오. 업그레이드를 중단하면 시스템을 사용할 수 없게 됩니다.

업그레이드가 시작되면 시스템에서 로그아웃됩니다.

설치가 완료되면 디바이스가 재부팅됩니다.

Confirm System Upgrade



Before starting the upgrade:

1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. **Do not power off the device** during the upgrade. Interrupting the upgrade can leave the system in an unusable state.

You will be logged out of the system when the upgrade begins.
After the installation completes, the device will be rebooted.

UPGRADE OPTIONS

- Automatically cancel on upgrade failure and roll back to the previous version

CANCEL

CONTINUE

계속

참고: 업그레이드는 FTD당 약 20분이 소요됩니다.

CLI에서는 업그레이드 폴더 /ngfw/var/log/sf에서 진행 상황을 확인할 수 있습니다. expert 모드로 이동하고 루트 액세스를 입력합니다.

```
> expert
```

```
admin@firepower:~$ sudo su
```

```
Password:
```

```
root@firepower:/home/admin# cd /ngfw/var/log/sf
```

```
root@firepower:/ngfw/var/log/sf# ls
```

```
Cisco_FTD_Upgrade-7.2.8.
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf
```

```
ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst
```

```
ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
```

```
ui: Upgrade complete
```

```
ui: The system will now reboot.
```

```
ui: System will now reboot.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):
```

```
System will reboot in 5 seconds due to system upgrade.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):
```

```
System will reboot now due to system upgrade.
```

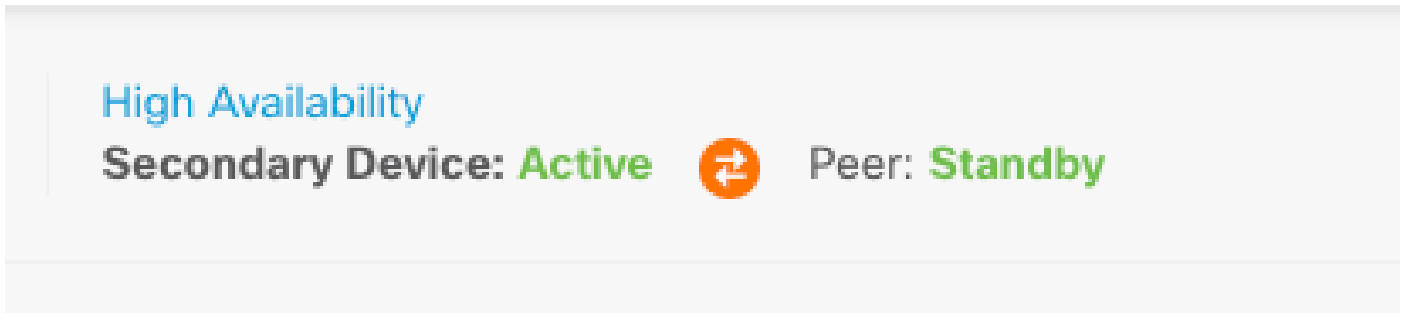
```
Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):
```

```
The system is going down for reboot NOW!
```

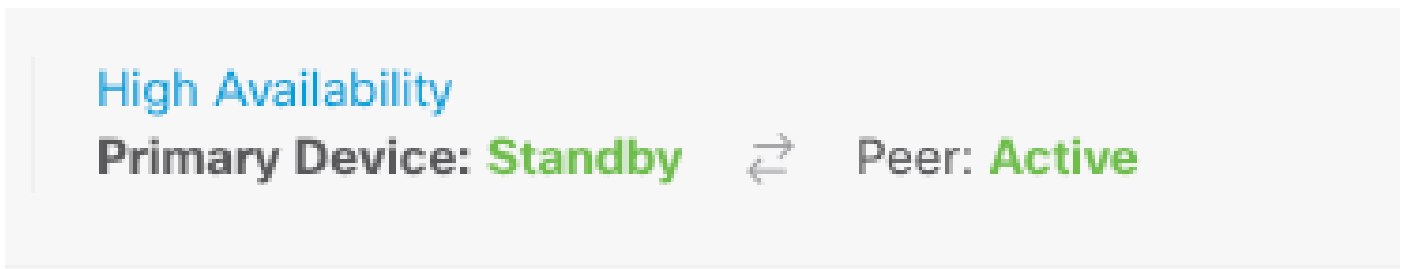
두 번째 유닛을 업그레이드합니다.

이 장치를 활성화하려면 역할을 전환하십시오. Device(디바이스) > High Availability(고가용성)를 선택한 다음 기어 메뉴에서 Switch Mode(스위치 모드)를 선택합니다. 디바이스의 상태가 active로 변경될 때까지 기다린 후 트래픽이 정상적으로 흐르고 있는지 확인합니다. 그런 다음 로그아웃합니다

업그레이드: 새 스탠바이에 로그인하고, 패키지를 업로드하고, 디바이스를 업그레이드하고, 진행 상황을 모니터링하고, 성공을 확인하려면 이전 단계를 반복합니다.



고가용성



고가용성

CLI에서 LINA(system support diagnostic-cli)로 이동하고 commandshow failover state를 사용하여 스탠바이 FTD에서 장애 조치 상태를 확인합니다.

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
primary_ha> enable
```

```
Password:
```

```
primary_ha# show failover state
```

State	Last Failure Reason	Date/Time
-------	---------------------	-----------

This host - Primary
Standby Ready None
Other host - Secondary
Active None

====Configuration State====

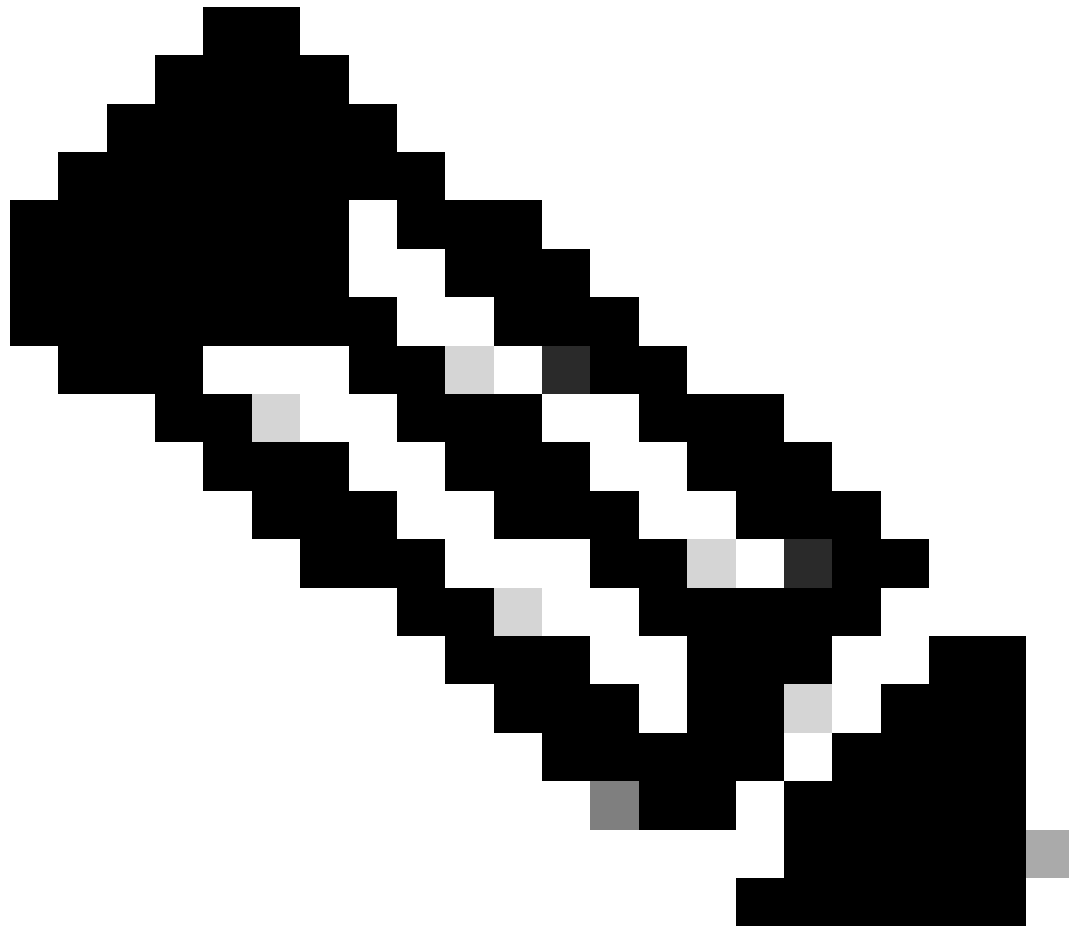
Sync Skipped - STANDBY

====Communication State====

Mac set

primary_ha#

4단계. 활성 피어 전환(선택 사항)



참고: 보조 디바이스가 Active(활성)이면 운영에 아무런 영향을 미치지 않습니다.

기본 디바이스를 액티브 상태로, 보조 디바이스를 스탠바이 상태로 유지하는 것은 발생할 수 있는 모든 장애 조치를 추적하는 데 도움이 되는 모범 사례입니다.

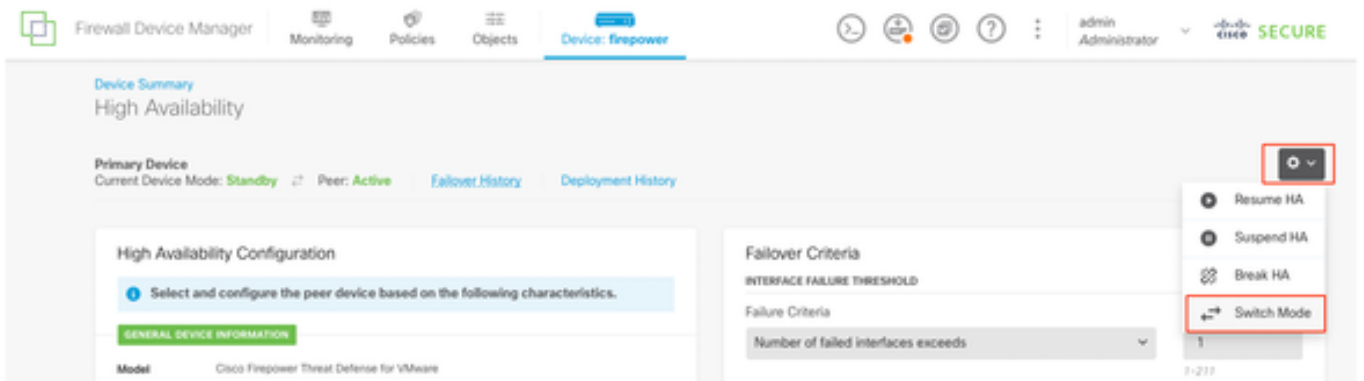
이 경우 FTD Active가 이제 Standby가 됩니다. 수동 장애 조치를 사용하여 다시 Active로 설정할 수 있습니다.

- Devices(디바이스) > High Availability(고가용성)로 이동합니다.



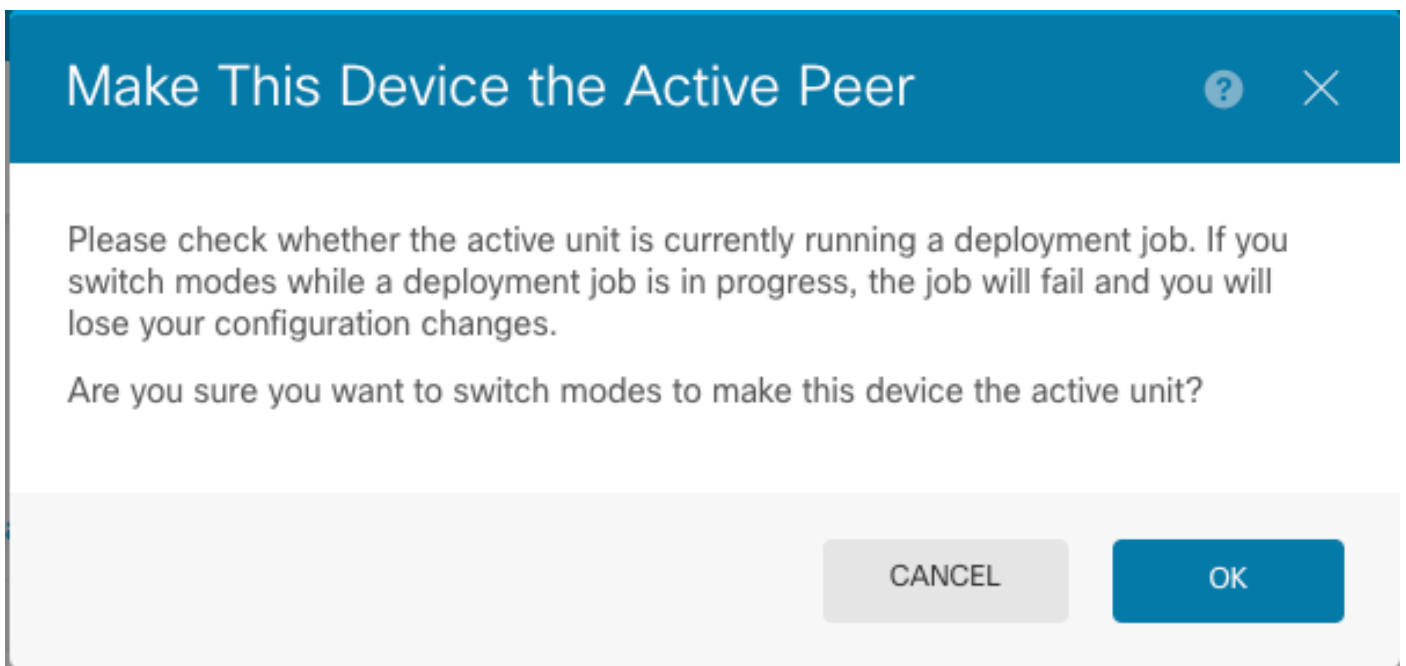
고가용성

- 스위치 모드를 선택합니다.



스위치 모드

- 장애 조치를 확인하려면 OK를 선택합니다.



활성 피어

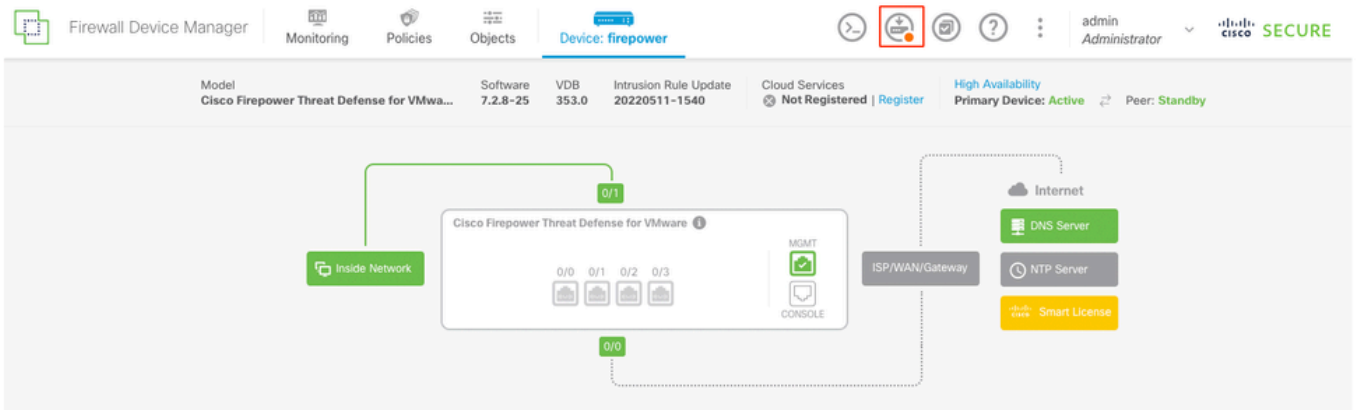
업그레이드 및 장애 조치 완료 시 HA 상태 검증



디바이스

5단계. 최종 구축

- Deployment(구축) 탭 아래에서 DEPLOY NOW(지금 구축)를 클릭하여 디바이스에 정책을 구축합니다.



Pending Changes



✓ **Last Deployment Completed Successfully**
14 Oct 2024 06:26 PM. [See Deployment History](#)

Deployed Version (14 Oct 2024 06:26 PM)	Pending Version	LEGEND
Rule Update Version Edited: 20220511-1540		
lastSuccessSRUDate: 2024-10-08 06:15:04Z	2024-10-14 12:53:26Z	
-	lspVersions[1]: 20220511-1540	
VDB Version Edited: 353		
+ Snort Version Added: 3.1.21.800-2		
-	snortVersion: 3.1.21.800-2	
-	snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor...	
-	name: 3.1.21.800-2	
Data SSL Cipher Setting Edited: DefaultDataSSLCipherSetting		
SSL Cipher Edited: DefaultSSLCipher		
-	protocolVersions[0]: TLSV1	
-	protocolVersions[1]: DTLSV1	
-	protocolVersions[2]: TLSV1_1	
Intrusion Policy Edited: Security Over Connectivity - Cisco Talos		
Intrusion Policy Edited: Maximum Detection - Cisco Talos		
MORE ACTIONS ▾	CANCEL	DEPLOY NOW ▾

정책 구축

유효성 검사

HA 상태 및 업그레이드가 완료되었는지 확인하려면 상태를 확인해야 합니다.

1차 대상: 활성

보조: 스탠바이 준비

둘 다 최근에 변경된 버전(이 예에서는 7.2.8)에 속합니다.



장애 조치

- 자세한 내용은 CLI 클릭을 통해 명령 `show failover state` and `show failover`를 사용하여 장애 조치 상태를 확인합니다.

firepower Cisco FX-OS(Extensible Operating System) v2.12.1(빌드 73)
 Cisco Firepower Threat Defense for VMware v7.2.8(빌드 25)

> show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	None	

====Configuration State====

Sync Skipped

====Communication State====

Mac set

> show failover

Failover On

Failover unit Primary

Failover LAN Interface: failover-link GigabitEthernet0/2 (up)

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(4)210, Mate 9.18(4)210

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 14:13:56 UTC Oct 15 2024

This host: Primary - Active

Active time: 580 (sec)

slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (192.168.45.1): Normal (Waiting)

Interface outside (192.168.1.10): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - Standby Ready

Active time: 91512 (sec)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (0.0.0.0): Normal (Waiting)

Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics

Link : failover-link GigabitEthernet0/2 (up)

Stateful Obj	xmit	xerr	rcv	rerr
General	11797	0	76877	0

sys cmd	11574	0	11484	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	176	0	60506	0
ARP tbl	45	0	4561	0
Xlate_Timeout	0	0	0	0
IPv6 ND tbl	0	0	0	0
VPN IKEv1 SA	0	0	0	0
VPN IKEv1 P2	0	0	0	0
VPN IKEv2 SA	0	0	0	0
VPN IKEv2 P2	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0
SIP Tx	0	0	0	0
SIP Pinhole	0	0	0	0
Route Session	1	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	30	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Umbrella Device-ID	0	0	0	0
Rule DB B-Sync	0	0	30	0
Rule DB P-Sync	1	0	266	0
Rule DB Delete	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	31	123591
Xmit Q:	0	1	12100

두 FTD가 동일한 버전에 있고 HA 상태가 정상이면 업그레이드가 완료된 것입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.