

firepower 4100에서 FTD 다중 인스턴스 고가용성 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[설정](#)

[1단계. 인터페이스 사전 구성](#)

[2단계. 컨테이너 인스턴스에 대한 리소스 프로파일 2개를 추가합니다.](#)

[3단계. \(선택 사항\) 컨테이너 인스턴스 인터페이스에 대한 가상 MAC 주소의 MAC 풀 접두사를 추가합니다.](#)

[4단계. 독립형 인스턴스를 추가합니다.](#)

[5단계. 인터페이스 구성](#)

[6단계. 각 인스턴스에 고가용성 쌍을 추가합니다.](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[참조](#)

소개

이 문서에서는 FTD 컨테이너 인스턴스(다중 인스턴스)에서 장애 조치를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Firepower Management Center 및 방화벽 위협 방어에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

Cisco Firepower Management Center Virtual 7.2.5
Cisco Firepower 4145 FTD(NGFW Appliance) 7.2.5
Firepower eXtensible 운영 체제(FXOS) 2.12(0.498)
Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

FTD 다중 인스턴스를 구축하기 전에 시스템 성능에 어떤 영향을 미칠 수 있는지 파악하고 그에 따라 계획을 세워야 합니다. 최적의 구축 및 구성을 위해 항상 Cisco 공식 문서를 참조하거나 Cisco 기술 담당자에게 문의하십시오.

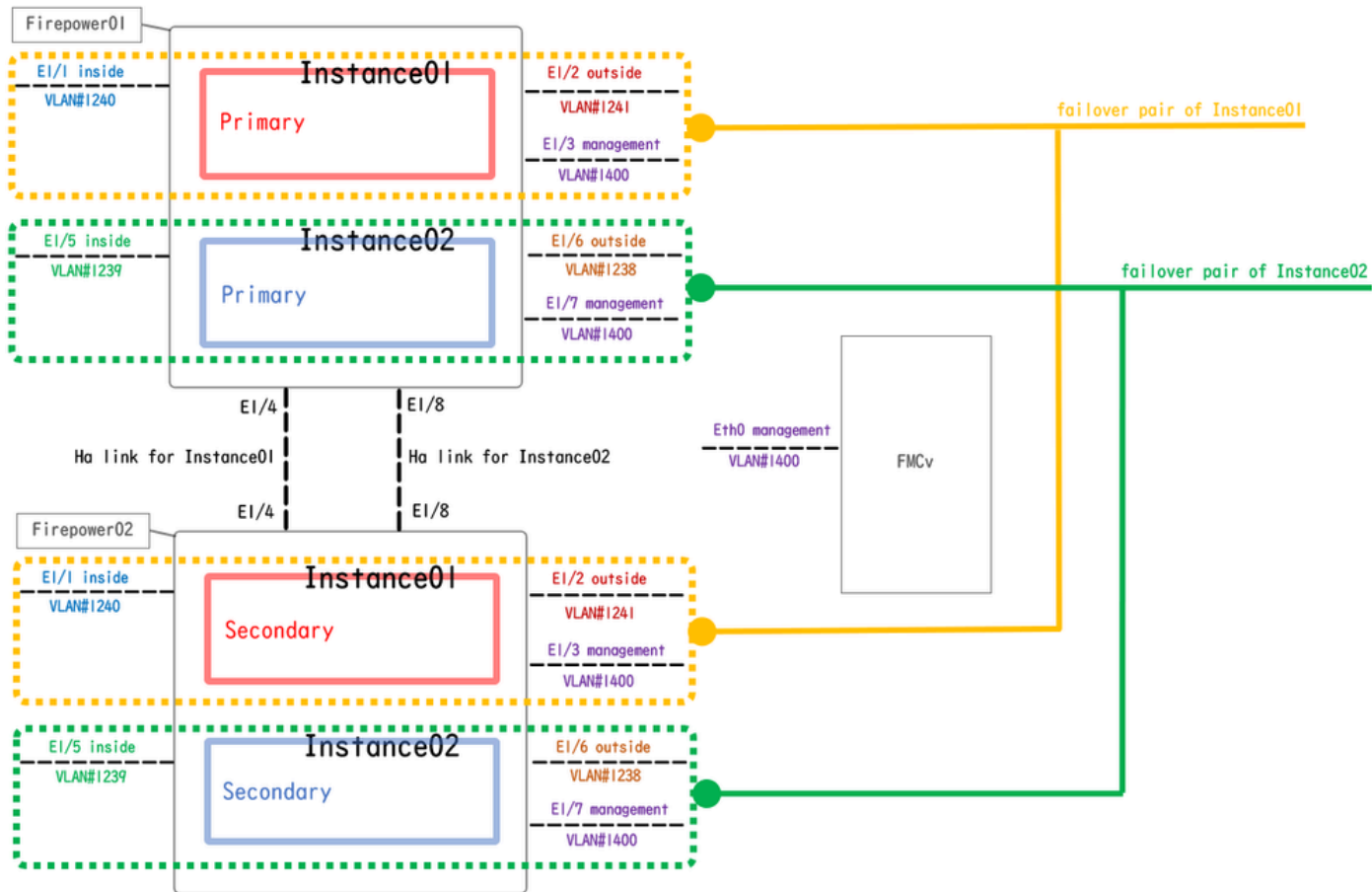
배경 정보

다중 인스턴스는 ASA 다중 컨텍스트 모드와 유사한 FTD(Firepower Threat Defense)의 기능입니다. 단일 하드웨어에서 FTD의 여러 개별 컨테이너 인스턴스를 실행할 수 있습니다. 각 컨테이너 인스턴스는 하드 리소스 분리, 별도의 컨피그레이션 관리, 별도의 리로드, 별도의 소프트웨어 업데이트, 완전한 위협 방어 기능 지원을 허용합니다. 이는 부서나 프로젝트마다 다른 보안 정책이 필요하지만 여러 개의 개별 하드웨어 어플라이언스에 투자하고 싶지 않은 조직에서 특히 유용합니다. 다중 인스턴스 기능은 현재 FTD 6.4 이상을 실행하는 Firepower 4100 및 9300 Series Security Appliance에서 지원됩니다.

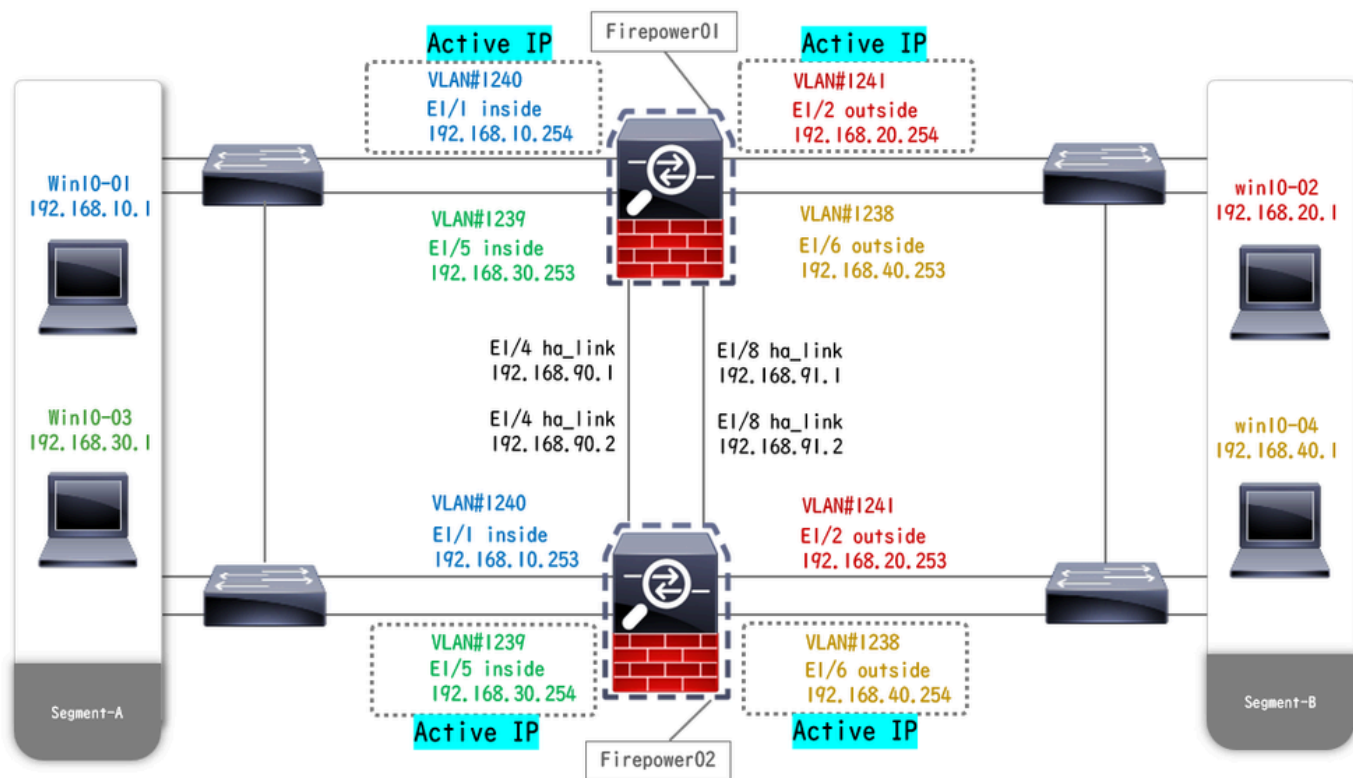
이 문서에서는 최대 14개의 Firepower 인스턴스를 지원하는 Container4145를 사용합니다. Firepower Appliance에서 지원되는 최대 인스턴스는 모델당 [최대 컨테이너 인스턴스 및 리소스를 참조하십시오](#).

네트워크 다이어그램

이 문서에서는 이 다이어그램에서 다중 인스턴스의 HA에 대한 컨피그레이션 및 확인을 소개합니다



논리적 컨피그레이션 다이어그램

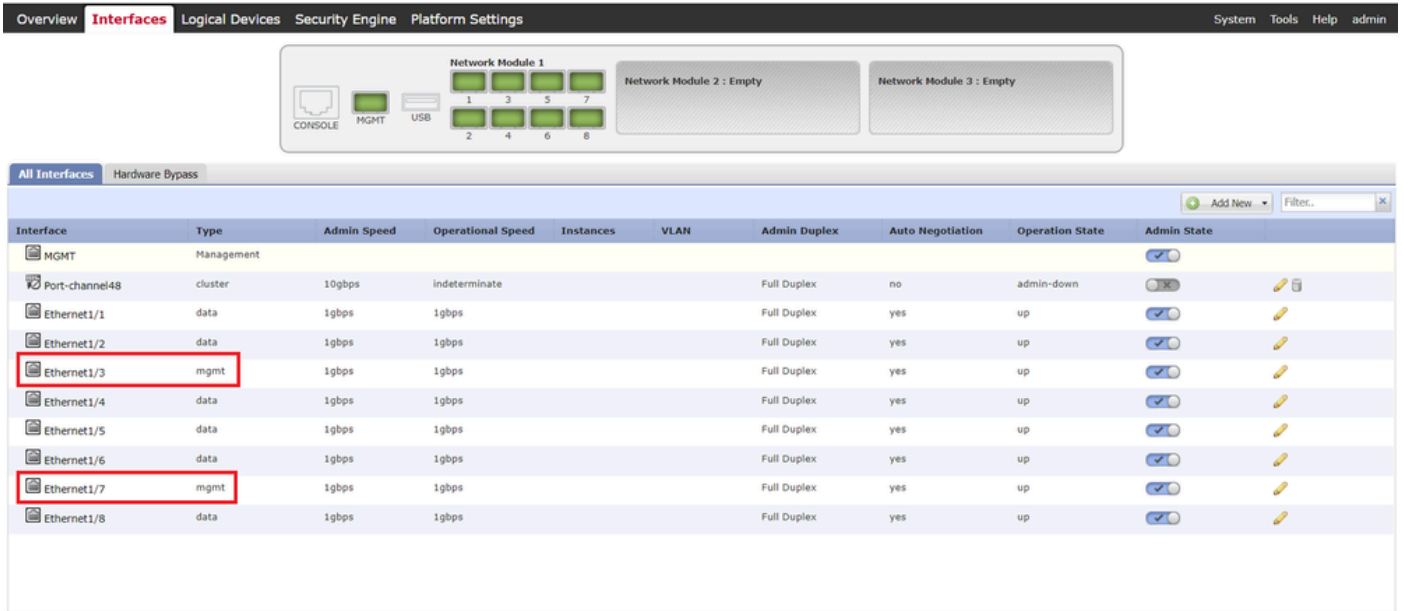


물리적 컨피그레이션 다이어그램

설정

1단계. 인터페이스 사전 구성

a. FCM의 인터페이스로 이동합니다. 2개의 관리 인터페이스를 설정합니다. 이 예에서는 Ethernet1/3 및 Ethernet1/7입니다.



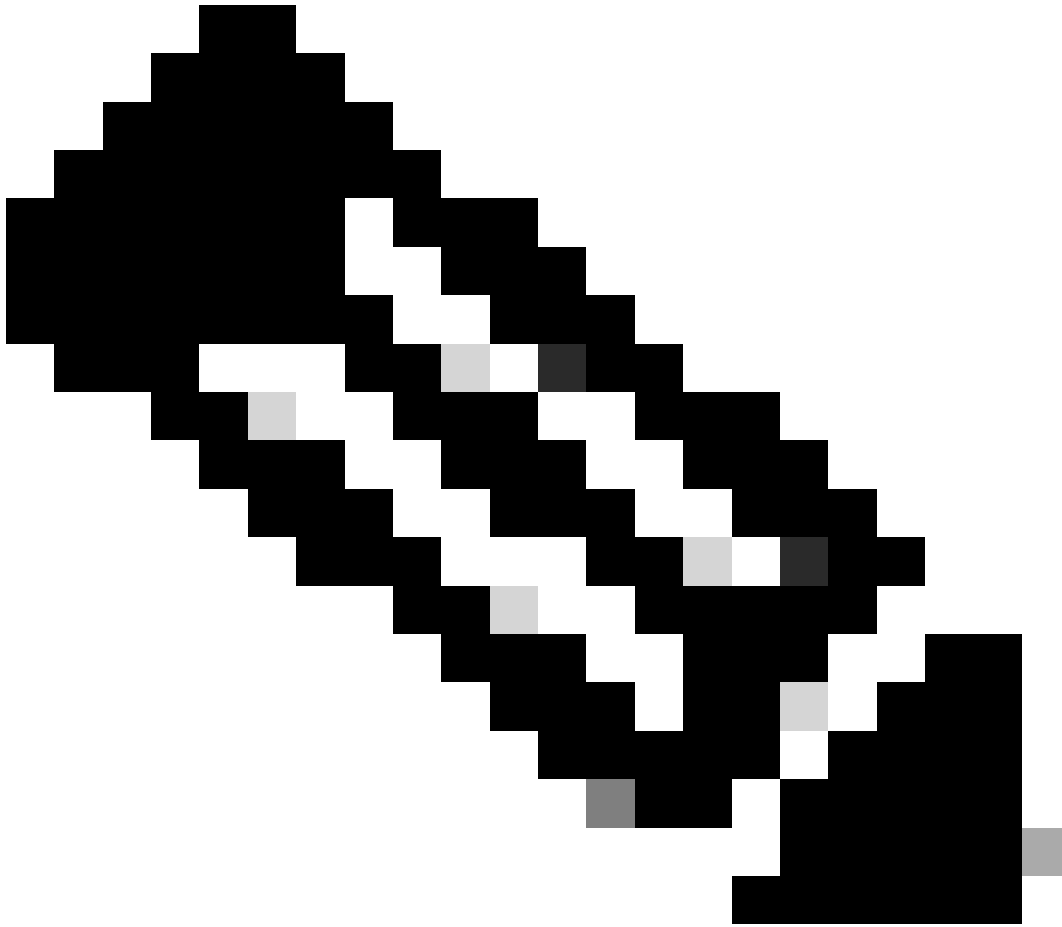
인터페이스 사전 구성

2단계. 컨테이너 인스턴스에 대한 리소스 프로파일 2개를 추가합니다.

a. Platform Settings(플랫폼 설정) > Resource Profiles(리소스 프로파일) > Add on FCM(FCM에 추가)으로 이동합니다. 첫 번째 리소스 프로파일을 설정합니다.

이 예에서는 다음을 수행합니다.

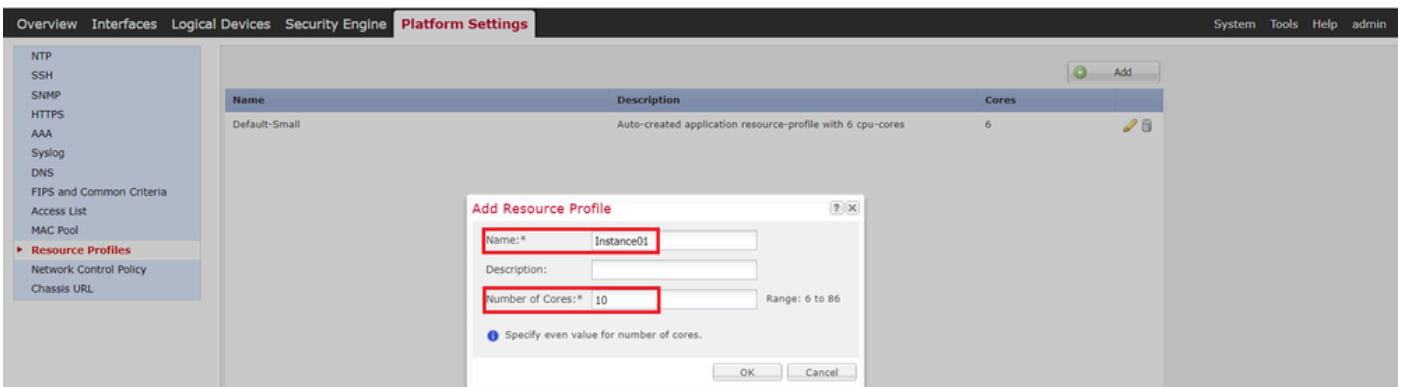
- 이름: Instance01
- 코어 수: 10



참고: 컨테이너 인스턴스 쌍의 HA에서는 동일한 리소스 프로파일 특성을 사용해야 합니다.

프로파일 이름을 1~64자로 설정합니다. 이 프로파일을 추가한 후에는 이름을 변경할 수 없습니다.

프로파일의 코어 수를 6에서 최대 사이로 설정합니다.

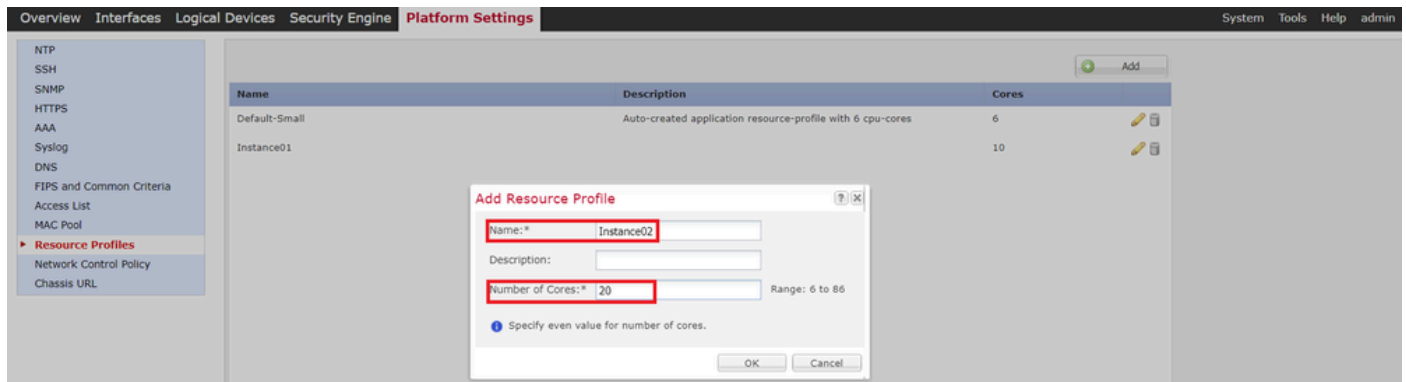


첫 번째 리소스 프로파일 추가

b. 2단계에서 a.를 반복하여 두 번째 리소스 프로필을 구성합니다.

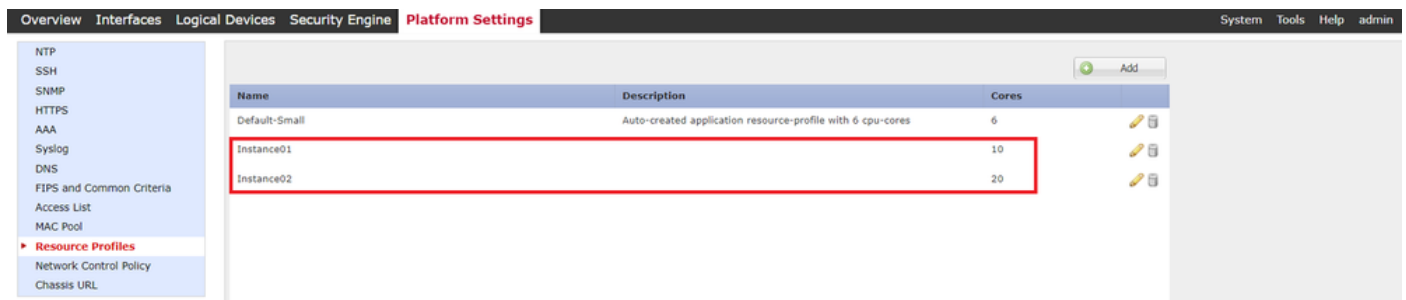
이 예에서는 다음을 수행합니다.

- 이름: Instance02
- 코어 수: 20



두 번째 리소스 프로필 추가

c. 2개의 리소스 프로필이 추가되었는지 확인합니다.



리소스 프로필 확인

3단계. (선택 사항) 컨테이너 인스턴스 인터페이스에 대한 가상 MAC 주소의 MAC 풀 접두사를 추가합니다.

액티브/스탠바이 인터페이스에 대한 가상 MAC 주소를 수동으로 설정할 수 있습니다. 다중 인스턴스 기능의 경우 가상 MAC 주소가 설정되지 않은 경우 새시는 인스턴스 인터페이스에 대한 MAC 주소를 자동으로 생성하고 각 인스턴스의 공유 인터페이스에서 고유한 MAC 주소를 사용하도록 보장합니다.

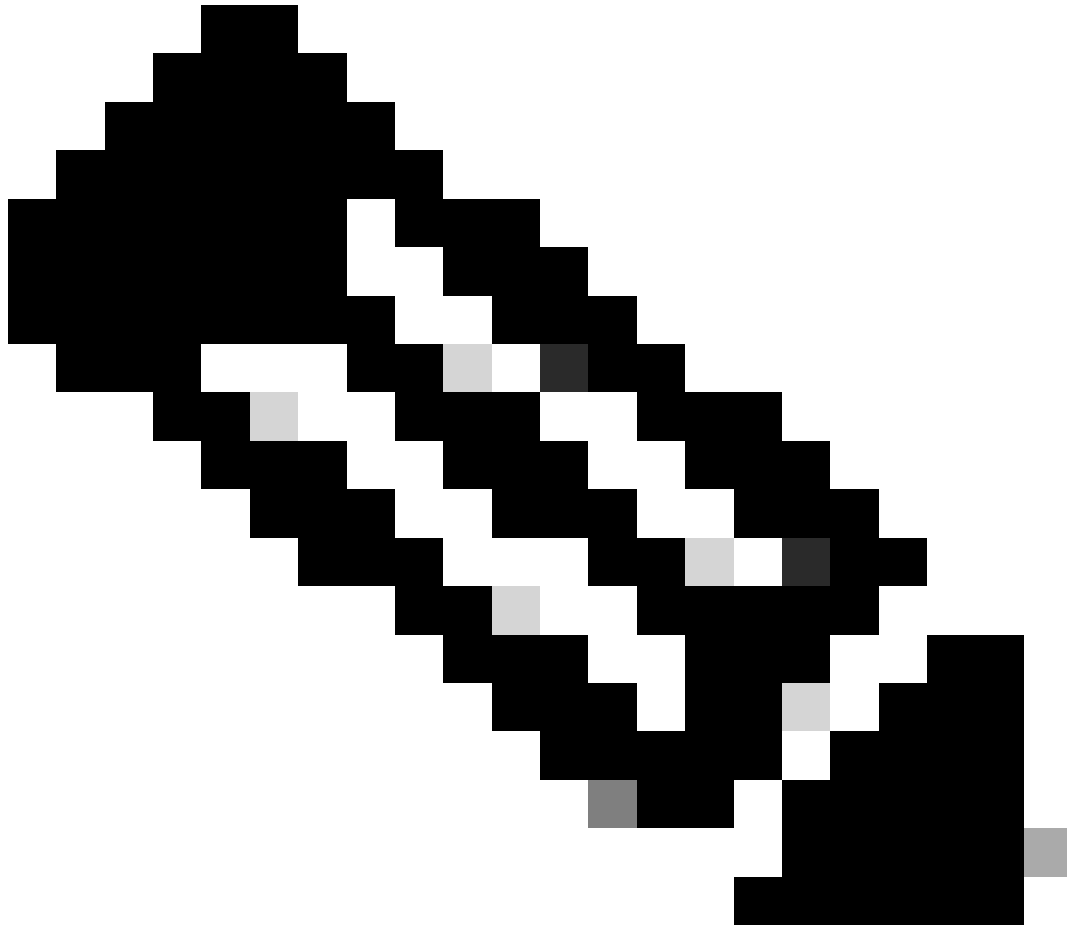
MAC 주소에 대한 자세한 내용은 [내용은 Add a MAC Pool Prefix and View MAC Addresses for Container Instance Interfaces\(MAC 풀 접두사 추가 및 컨테이너 인스턴스 인터페이스의 MAC 주소 보기\)](#)를 참조하십시오.

4단계. 독립형 인스턴스를 추가합니다.

a. Logical Devices(논리적 디바이스) > Add Standalone(독립형 추가)으로 이동합니다. 첫 번째 인스턴스를 설정합니다.

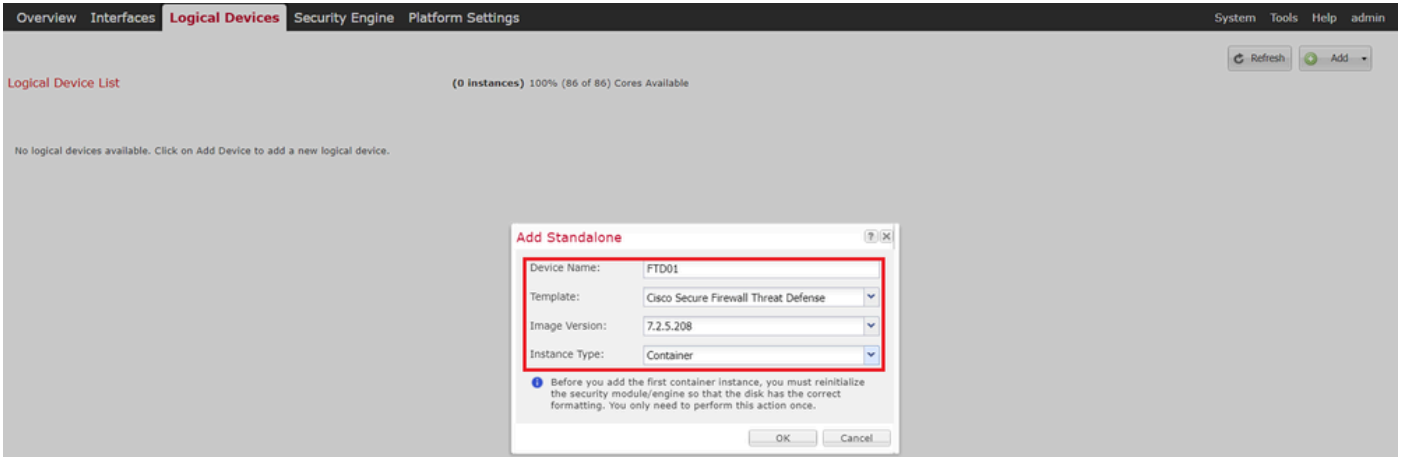
이 예에서는 다음을 수행합니다.

- 장치 이름 : FTD01



참고: 컨테이너 애플리케이션을 구축하는 유일한 방법은 Instance Type(인스턴스 유형)이 Container(컨테이너)로 설정된 App-Instance(애플리케이션 인스턴스)를 사전 구축하는 것입니다. 컨테이너를 선택합니다.

논리적 디바이스를 추가한 후에는 이 이름을 변경할 수 없습니다.



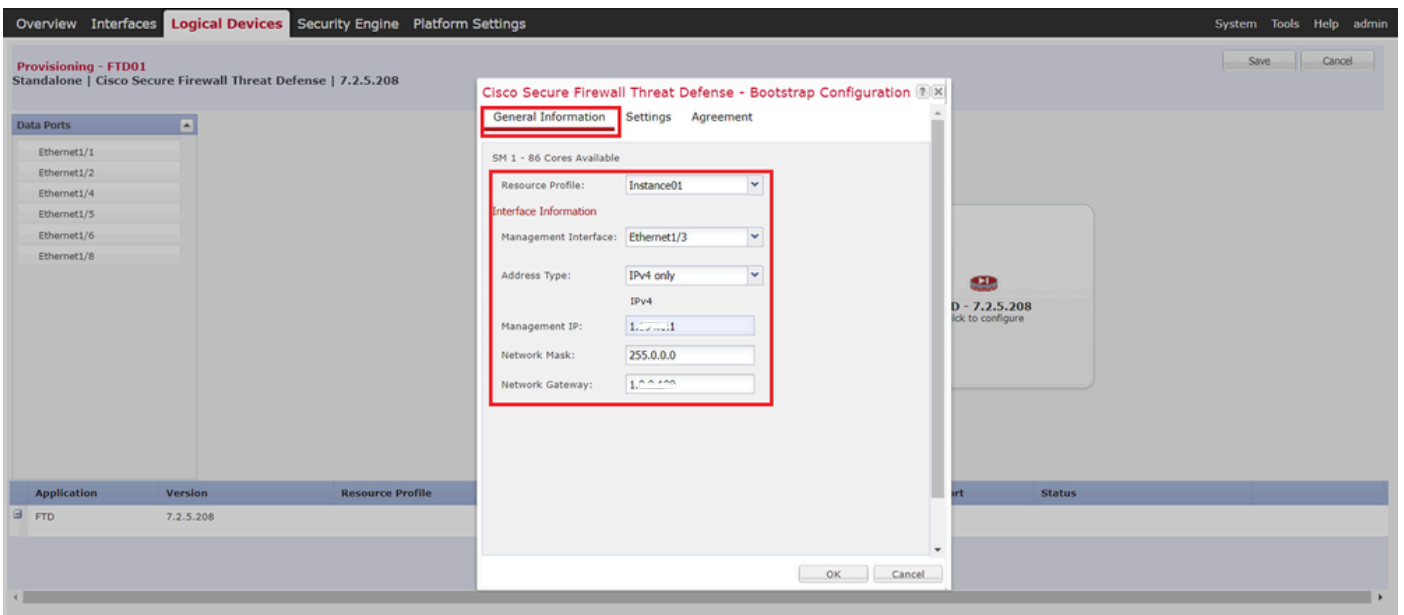
인스턴스 추가

5단계. 인터페이스 구성

a. Instance01에 대한 자원 프로파일, 관리 인터페이스, 관리 IP를 설정합니다.

이 예에서는 다음을 수행합니다.

- 리소스 프로파일: Instance01
- 관리 인터페이스 : Ethernet1/3
- 관리IP: x.x.1.1

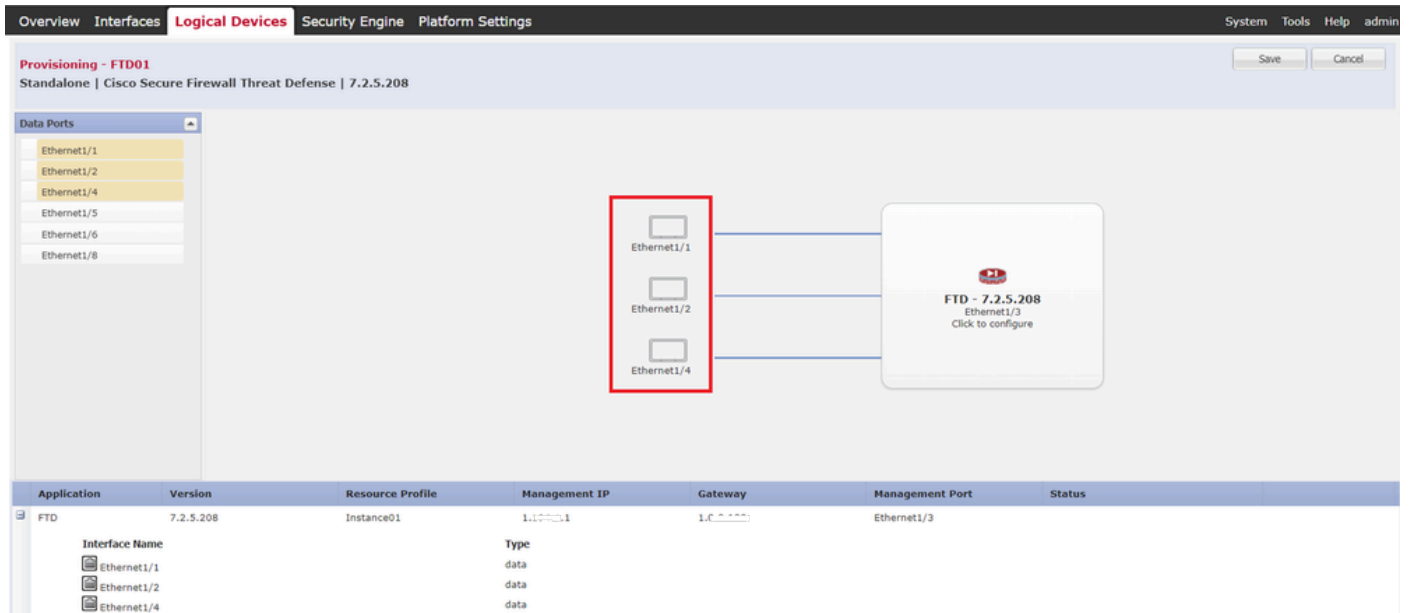


프로파일/관리 인터페이스/관리 IP 구성

b. 데이터 인터페이스를 설정합니다.

이 예에서는 다음을 수행합니다.

- 이더넷1/1(내부용)
- 이더넷1/2(외부용)
- Ethernet1/4(HA 링크에 사용)



데이터 인터페이스 설정

c. Logical Devices(논리적 디바이스)로 이동합니다. 인스턴스 부팅을 기다리는 중입니다.



Instance01의 상태 확인

d. 4.a단계 및 5.a~c단계에서 a.를 반복하여 두 번째 인스턴스를 추가하고 해당 인스턴스에 대한 세부 정보를 설정합니다.

이 예에서는 다음을 수행합니다.

- 장치 이름 : FTD11
- 인스턴스 유형 : 컨테이너
- 리소스 프로필 : Instance02
- 관리 인터페이스 : Ethernet1/7
- ManagementIP: x.x.10.1
- 이더넷1/5 = 내부
- 이더넷1/6 = 외부
- 이더넷1/8 = HA 링크

e. FCM에서 2개의 인스턴스가 온라인 상태인지 확인합니다.

Logical Device List							(2 Container Instances) 66% (56 of 86) Cores Available	
FTD11							Standalone Status:ok	
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance02	10.1	1.0.0.0	Ethernet1/7	Online		
FTD01							Standalone Status:ok	
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance01	10.1	1.0.0.0	Ethernet1/3	Online		

기본 디바이스의 인스턴스 상태 확인

f. (선택 사항) scope ssa 실행 **scope slot 1** 및 **show app-Instance** 명령을 사용하여 Firepower CLI에서 2 인스턴스가 온라인 상태를 확인합니다.

```
<#root>
```

```
FPR4145-ASA-K9#
```

```
scope ssa
```

```
FPR4145-ASA-K9 /ssa #
```

```
scope slot 1
```

```
FPR4145-ASA-K9 /ssa/slot #
```

```
show app-Instance
```

```
Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deploy
```

```
Online
```

```
7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11
```

```
Online
```

```
7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online
```

g. 보조 디바이스에서도 동일하게 수행합니다. 2개의 인스턴스가 온라인 상태인지 확인합니다.

Logical Device List							(2 Container Instances) 66% (56 of 86) Cores Available	
FTD12							Standalone Status:ok	
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance02	10.2	1.0.0.0	Ethernet1/7	Online		
FTD02							Standalone Status:ok	
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance01	10.2	1.0.0.0	Ethernet1/3	Online		

보조 디바이스의 인스턴스 상태 확인

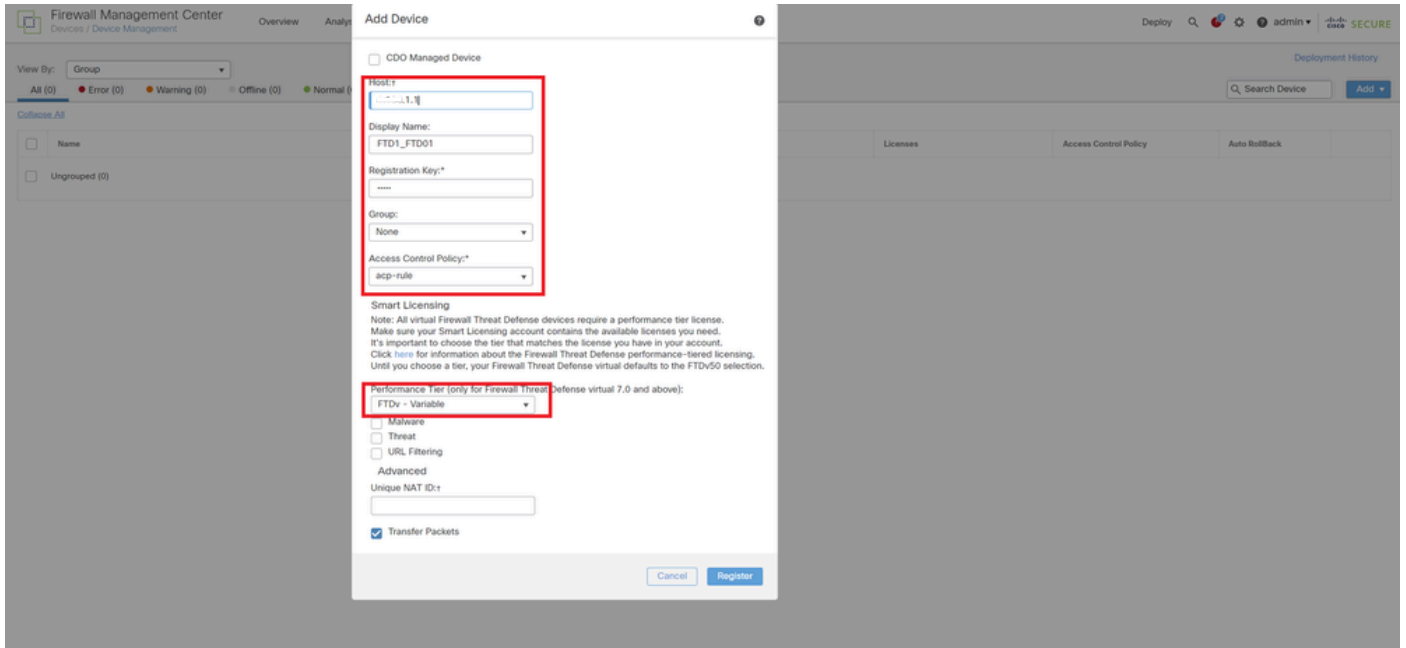
6단계. 각 인스턴스에 고가용성 쌍을 추가합니다.

a. Devices(디바이스) > Add Device on FMC(FMC에 디바이스 추가)로 이동합니다. 모든 인스턴스를 FMC에 추가합니다.

이 예에서는 다음을 수행합니다.

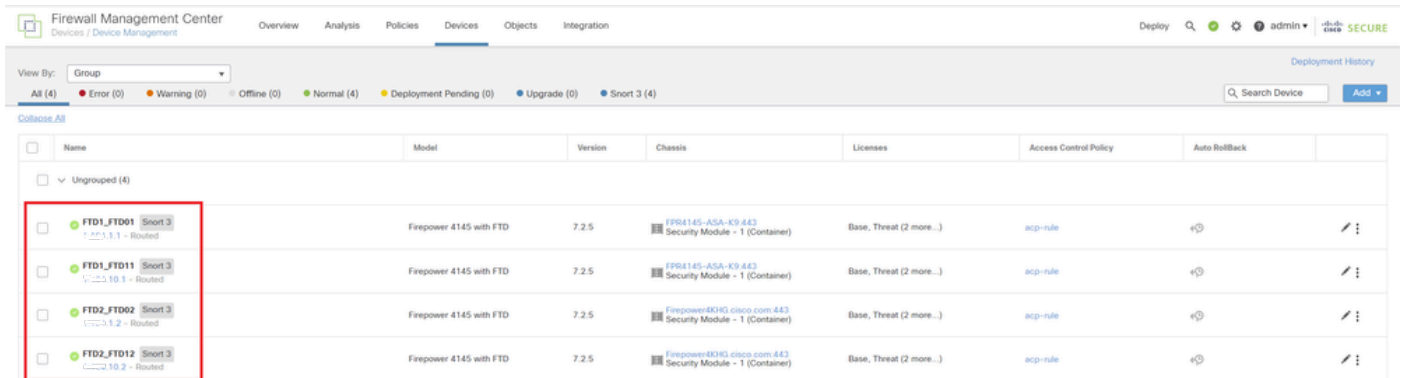
- FTD1의 Instance01에 대한 표시 이름: FTD1_FTD01
- FTD1의 Instance02에 대한 표시 이름: FTD1_FTD11
- FTD2의 Instance01에 대한 표시 이름: FTD2_FTD02
- FTD2의 Instance02에 대한 표시 이름: FTD2_FTD12

이 그림에서는 FTD1_FTD01에 대한 설정을 보여 줍니다.



FTD 인스턴스를 FMC에 추가

b. 모든 인스턴스가 정상인지 확인합니다.



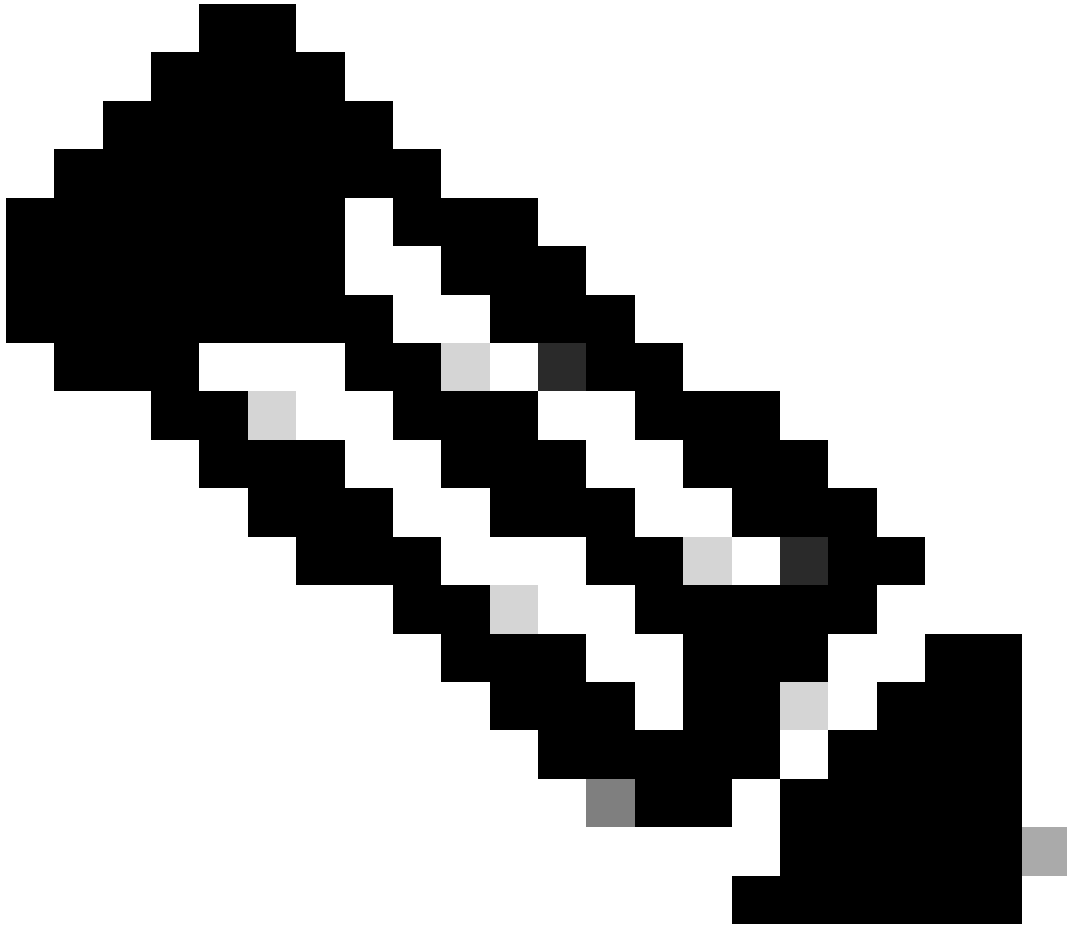
FMC에서 인스턴스 상태 확인

c. Devices(디바이스) > Add High Availability(고가용성 추가)로 이동합니다. 첫 번째 장애 조치 쌍을 설정합니다.

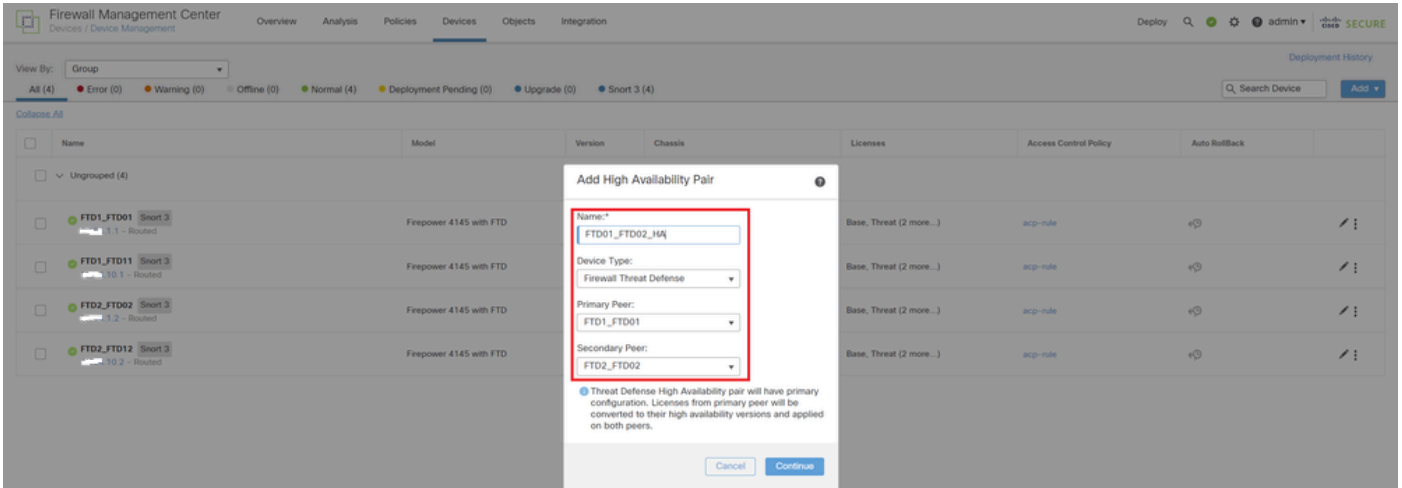
이 예에서는 다음을 수행합니다.

·이름: FTD01_FTD02_HA

· 주 피어 : FTD1_FTD01



참고: 올바른 유닛을 기본 유닛으로 선택해야 합니다.



첫 번째 장애 조치 쌍 추가

d. 첫 번째 장애 조치 쌍에서 장애 조치 링크에 대한 IP를 설정합니다.

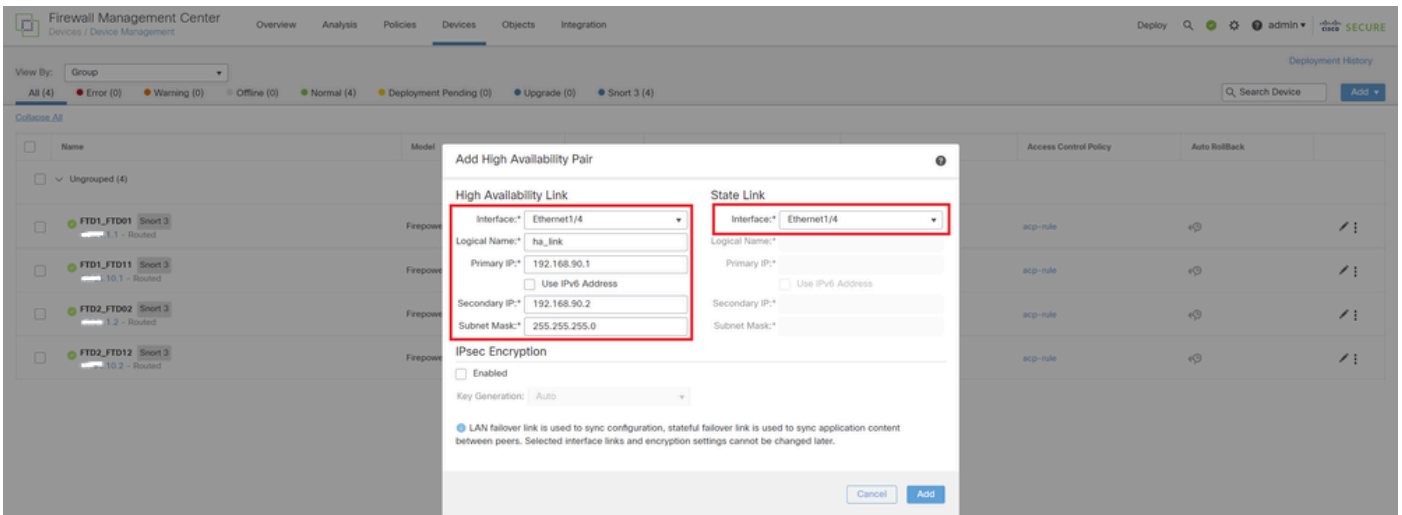
이 예에서는 다음을 수행합니다.

·고가용성 링크 : Ethernet1/4

·상태 링크 : Ethernet1/4

· 기본 IP: 192.168.90.1/24

·보조 IP: 192.168.90.2/24



첫 번째 장애 조치 쌍에 대한 HA 인터페이스 및 IP 설정

e. 장애 조치 상태 확인

·FTD1_FTD01 : Primary, 활성

·FTD2_FTD02 : 보조, 대기

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
FTD01_FTD02_HA (High Availability)						
FTD1_FTD01 (Primary, Active)	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+
FTD2_FTD02 (Secondary, Standby)	Firepower 4145 with FTD	7.2.5	Firepower40303.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+
FTD1_FTD11	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+
FTD2_FTD12	Firepower 4145 with FTD	7.2.5	Firepower40303.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+

첫 번째 장애 조치 쌍의 상태 확인

f. Devices(디바이스) > FTD01_FTD02_HA(이 예에서는) > Interfaces(인터페이스)를 클릭합니다. 데이터 인터페이스에 대한 활성 IP를 설정합니다.

이 예에서는 다음을 수행합니다.

- 이더넷1/1(내부) : 192.168.10.254/24
- 이더넷1/2(외부): 192.168.20.254/24
- 이더넷1/3(진단): 192.168.80.1/24

이 그림에서는 Ethernet1/1의 Active IP에 대한 설정을 보여 줍니다.

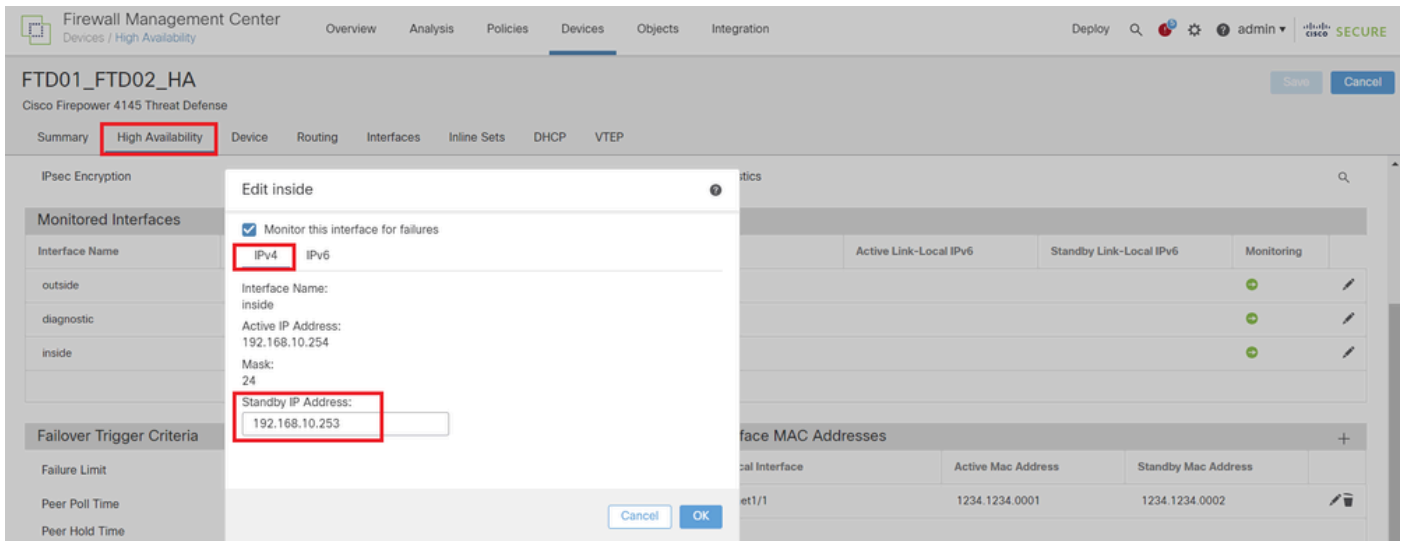
데이터 인터페이스에 대한 활성 IP 설정

g. Devices(디바이스) > FTD01_FTD02_HA(이 예에서) > High Availability(고가용성)를 클릭합니다. 데이터 인터페이스의 스탠바이 IP를 설정합니다.

이 예에서는 다음을 수행합니다.

- 이더넷1/1(내부) : 192.168.10.253/24
- 이더넷1/2(외부): 192.168.20.253/24
- 이더넷1/3(진단): 192.168.80.2/24

이 그림에서는 Ethernet1/1의 Standby IP에 대한 설정을 보여 줍니다.



데이터 인터페이스에 대한 대기 IP 설정

h. 6.c~g 단계를 반복하여 두 번째 장애 조치 쌍을 추가합니다.

이 예에서는 다음을 수행합니다.

·이름: FTD11_FTD12_HA

·주 피어: FTD1_FTD11

·세컨더리 피어 : FTD2_FTD12

· High Availability Link : 이더넷1/8

·주 링크 : 이더넷1/8

·이더넷1/8(ha_link Active): 192.168.91.1/24

·이더넷1/5(내부 액티브): 192.168.30.254/24

·이더넷1/6(외부 액티브): 192.168.40.254/24

·이더넷1/7(진단 활성): 192.168.81.1/24

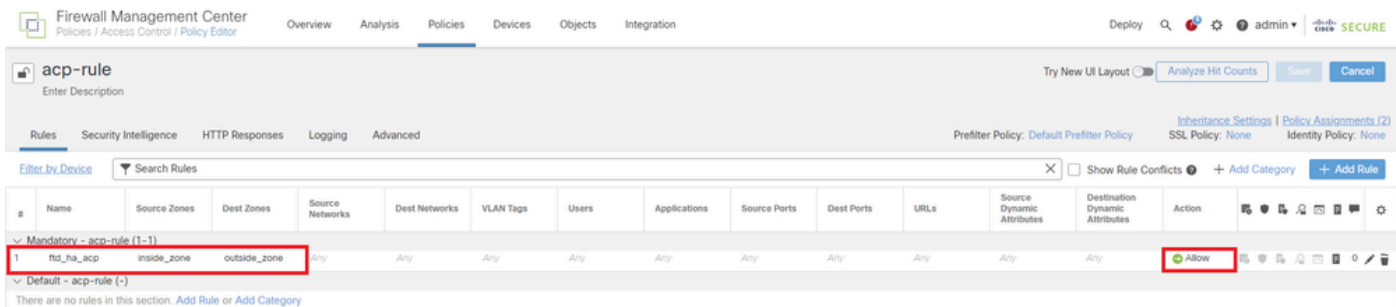
·이더넷1/8(ha_link Standby): 192.168.91.2/24

·이더넷1/5(Inside Standby): 192.168.30.253/24

·이더넷1/6(Outside Standby): 192.168.40.253/24

·이더넷1/7(진단 대기): 192.168.81.2/24

i. Logical Devices(논리적 디바이스) > Add Standalone(독립형 추가)으로 이동합니다. 내부에서 외부로의 트래픽을 허용하도록 ACP 규칙을 설정합니다.



ACP 규칙 설정

j. FTD에 설정을 구축합니다.

k. CLI에서 HA 상태 확인

각 인스턴스의 HA 상태는 ASA와 동일한 Firepower CLI에서도 확인됩니다.

FTD1_FTD01(Primary Instance01)의 HA 상태를 확인하려면 **show running-config failover** 실행 및 **show failover** 명령

```
<#root>
```

```
// confirm HA status of FTD1_FTD01 (Instance01 of Primary Device) >
```

```
show running-config failover
```

```
failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication http
```

```
show failover
```

```
Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host: P
..... Other host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic
```

실행 **show running-config failover** 및 **show failover** 명령을 사용하여 FTD1_FTD11(Primary Instance02)의 HA 상태를 확인합니다.

```
<#root>
```

```
// confirm HA status of FTD1_FTD11 (Instance02 of Primary Device) >
```

```
show running-config failover
```

```
failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication http
```

```
show failover
```

```
Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host: P
Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16
```

FTD2_FTD02(Secondary Instance01)의 HA 상태를 확인하려면 **show running-config failover** 실행 및 **show failover** 명령을 수행합니
다.

```
<#root>
```


// confirm HA status of FTD2_FTD02 (Instance01 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha_link Ethernet1/4 failover replication h

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) This host:
Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-

FTD2_FTD12(보조 인스턴스02)의 HA 상태를 확인하려면 실행 **show running-config failover** 및 **show failover** 명령을 수행합니다.

<#root>

// confirm HA status of FTD2_FTD12 (Instance02 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha_link Ethernet1/8 failover replication h
Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

1. 라이선스 사용 확인

모든 라이선스는 컨테이너 인스턴스가 아니라 보안 엔진/새시별로 소비됩니다.

. 보안 엔진/새시당 1개의 베이스라인이 자동으로 할당됩니다.

. 기능 라이선스는 각 인스턴스에 수동으로 할당되지만, 기능 /보안 엔진/새시당 하나의 라이선스만 소비합니다. 특정 기능 라이선스
의 경우 사용 중인 인스턴스 수와 상관없이 총 1개의 라이선스만 있으면 됩니다.

이 표에서는 이 문서에서 라이선스가 소비되는 방식을 보여줍니다.

FPR01	인스턴스01	기본, URL 필터링, 악성코드, 위협
	인스턴스02	기본, URL 필터링, 악성코드, 위협
FPR02	인스턴스01	기본, URL 필터링, 악성코드, 위협
	인스턴스02	기본, URL 필터링, 악성코드, 위협

총 라이선스 수

기본	URL 필터링	악성코드	위협
2	2	2	2

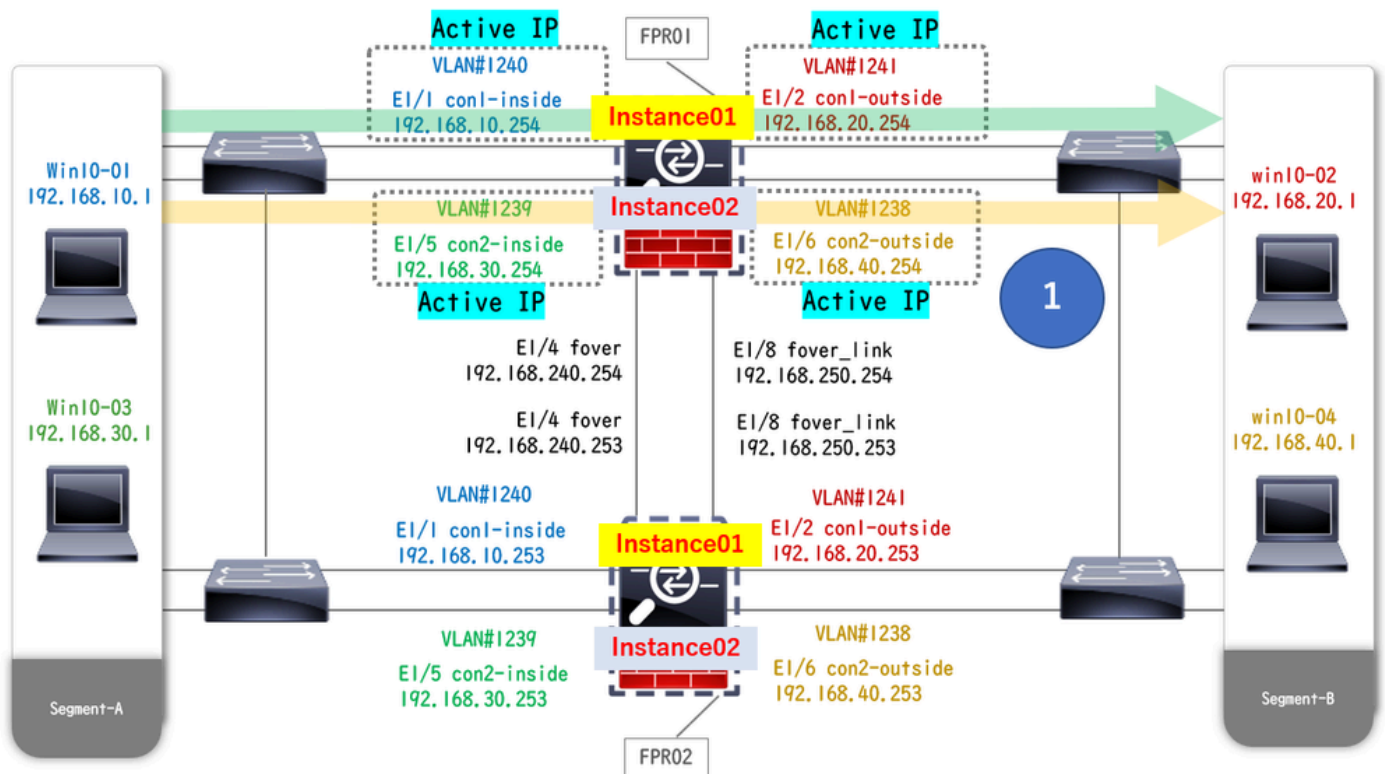
FMC GUI에서 사용된 라이선스 수를 확인합니다.

License Type/Device Name	License Status	Device Type	Domain	Group
Base (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
Malware (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
Threat (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
URL Filtering (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A

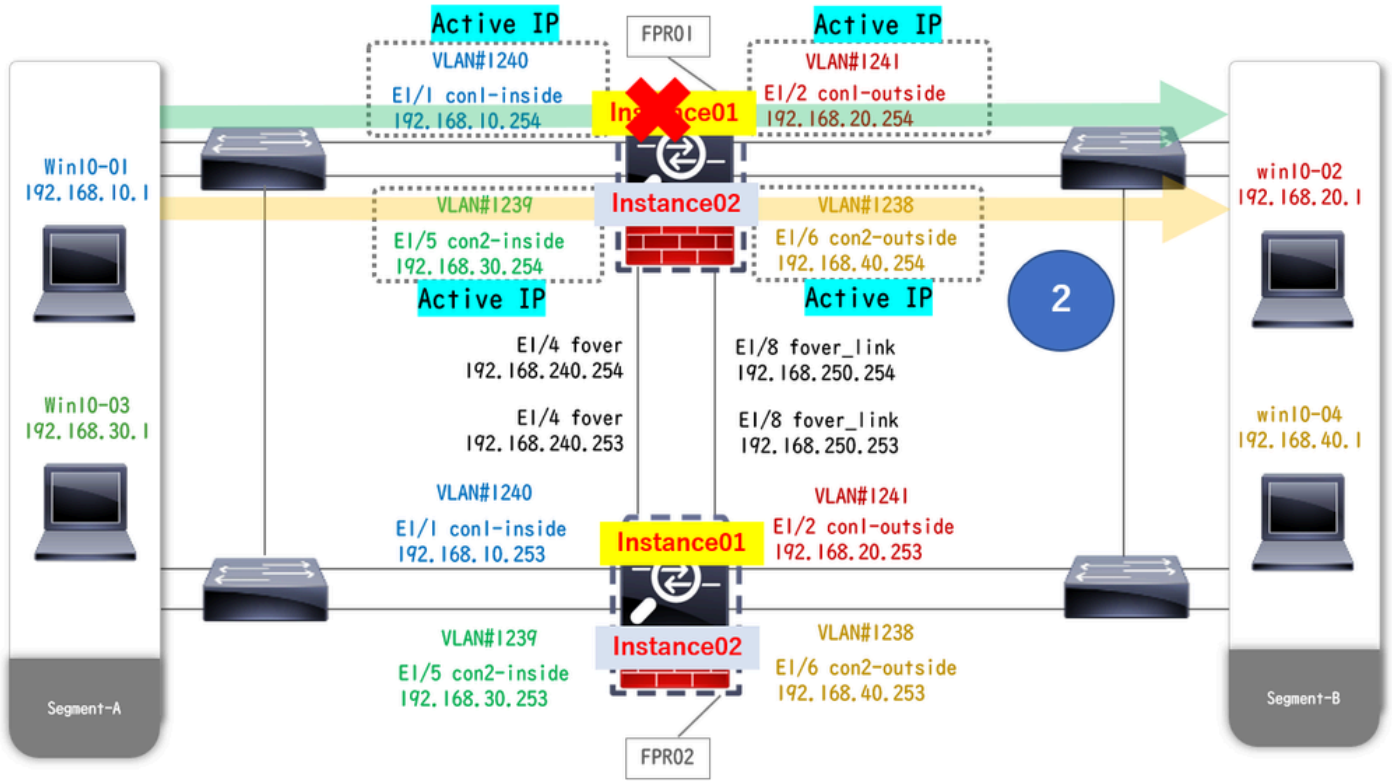
사용된 라이선스 확인

다음을 확인합니다.

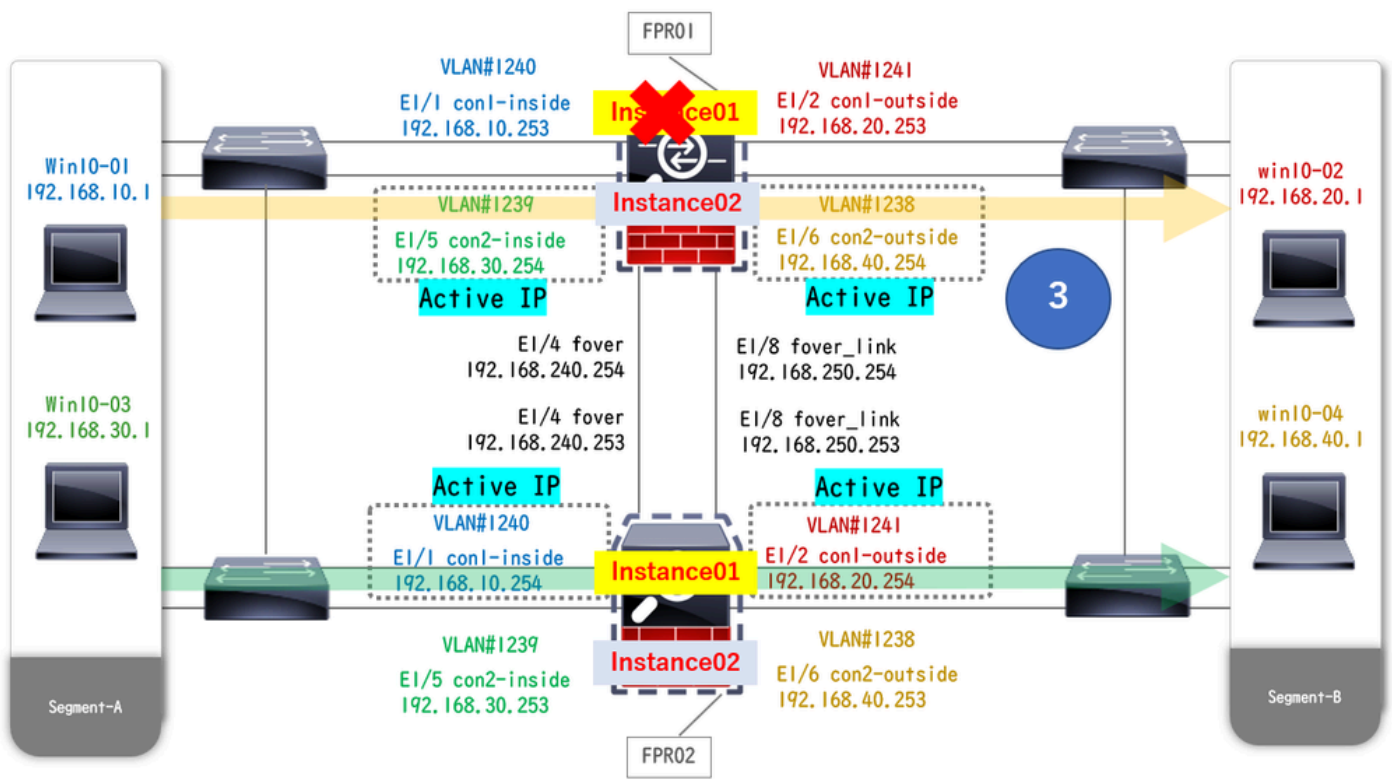
FTD1_FTD01(기본 인스턴스 01)에서 충돌이 발생하면 인스턴스 01의 장애 조치가 트리거되고 스탠바이 측의 데이터 인터페이스가 원래 액티브 인터페이스의 IP/MAC 주소를 인수하여 트래픽(이 문서의 FTP 연결)이 Firepower에 의해 지속적으로 전달되도록 합니다.



충돌 전



충돌 중



장애 조치가 트리거됨

1단계. Win10-01에서 Win10-02로의 FTP 연결을 시작합니다.

2단계. 명령 show conn 을 실행하여 FTP 연결이 두 Instance01에 모두 설정되어 있는지 확인합니다.

<#root>

// Confirm the connection in Instance01 of FPR01 >

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1

3단계. Win10-03에서 Win10-04로의 FTP 연결을 시작합니다.

4단계. FTP **show conn** 연결이 두 Instance02에 모두 설정되어 있는지 확인하려면 명령을 실행합니다.

<#root>

// Confirm the connection in Instance02 of FPR01 >

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1

5단계. 실행 **connect ftd FTD01** 및 **system support diagnostic-cli** 명령을 사용하여 ASA CLI에 입력합니다. 실행 **enable** 및 **crashinfo force watchdog** 명령을 사용하여 기본/액티브 유닛에서 Instance01을 강제로 충돌 시킵니다.

<#root>

Firepower-module1>

connect ftd FTD01

>

system support diagnostic-cli

FTD01>

enable

Password: FTD01# FTD01#

crashinfo force watchdog

reboot. Do you wish to proceed? [confirm]:

6단계. 장애 조치는 Instance01에서 발생하며 FTP 연결이 중단되지 않습니다. FPR02 show failover에서 Instance01의 상태를 확인하려면 명령 show conn을 실행하고 실행하십시오.

<#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) This host: Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside (

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

7단계. Instance01에서 발생한 충돌은 Instance02에 영향을 미치지 않았습니다. 실행 show failover 및 show conn 명령을 사용하여 Instance02의 상태를 확인합니다.

<#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

8단계. FMC에서 Devices > All로 이동합니다. HA 상태를 확인합니다.

·FTD1_FTD01 : Primay, Standby

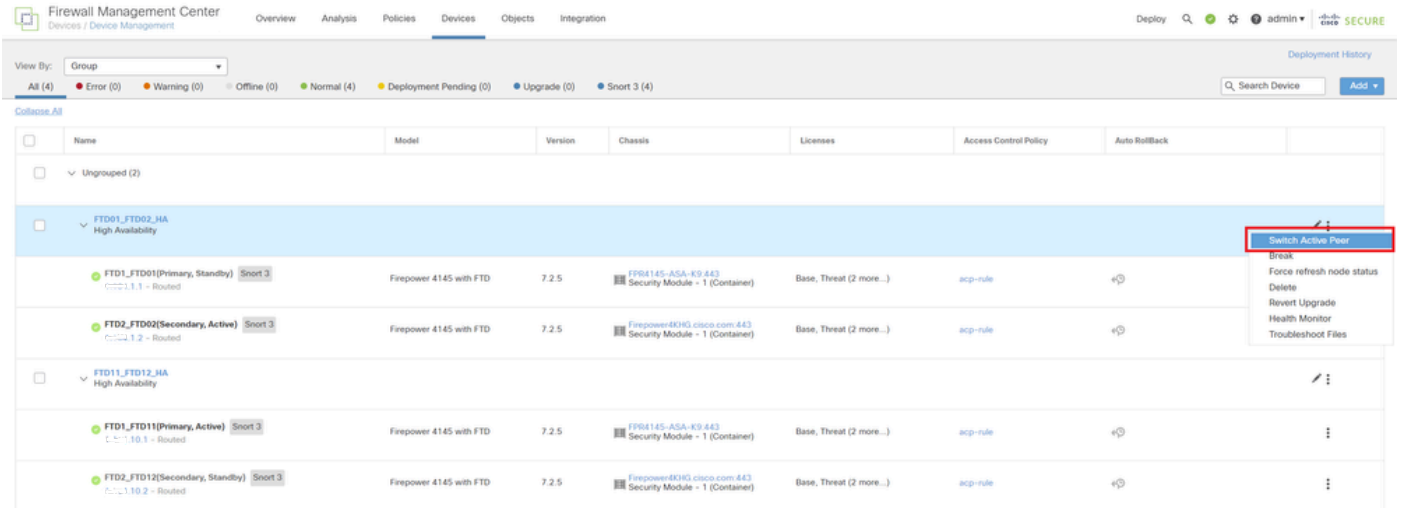
·FTD2_FTD02 : 보조, 활성

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
FTD01_FTD02_HA High Availability						
FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	
FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	
FTD11_FTD12_HA High Availability						
FTD1_FTD11(Primary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	
FTD2_FTD12(Secondary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	

HA 상태 확인

9단계. (선택 사항)FPR01의 Instance01이 정상으로 돌아간 후 HA의 상태를 수동으로 전환할 수 있습니다. 이는 FMC GUI 또는 FRP CLI에서 수행할 수 있습니다.

FMC에서 Devices(디바이스) > All(모두)로 이동합니다. FTD01_FTD02_HA에 대한 HA 상태를 전환하려면 Switch Active Peer(활성 피어 전환)를 클릭합니다.



The screenshot shows the FMC interface with the 'Devices' tab selected. A table lists HA configurations. The configuration 'FTD01_FTD02_HA' is highlighted in blue. A context menu is open over this configuration, with the 'Switch Active Peer' option highlighted in red. Other options in the menu include Break, Force refresh node status, Delete, Revert Upgrade, Health Monitor, and Troubleshoot Files.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
Ungrouped (2)						
FTD01_FTD02_HA High Availability						
FTD1_FTD01(Primary, Standby) Snort 3 1.1.1 - Routed	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	
FTD2_FTD02(Secondary, Active) Snort 3 1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4145.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	
FTD11_FTD12_HA High Availability						
FTD11_FTD11(Primary, Active) Snort 3 1.1.1 - Routed	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	
FTD21_FTD12(Secondary, Standby) Snort 3 1.1.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4145.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	

스위치 HA 상태

Firepower CLI에서 ASA CLI connect ftd FTD01를 system support diagnostic-cli 시작하려면 실행 및 명령을 입력합니다. 실행 enable 및 failover active 명령을 사용하여 FTD01_FTD02_HA에 대해 HA를 전환합니다.

```
<#root>
```

```
Firepower-module1>
```

```
connect ftd FTD01
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available
```

```
enable
```

```
firepower#
```

```
failover active
```

문제 해결

장애 조치 상태의 유효성을 검사하려면 명령 show failover 을 show failover history 실행합니다.

```
<#root>
```

>

show failover

```
Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (I
```

>

show failover history

```
===== From State To State Reason =
```

< debug fover option> 명령을 실행하여 장애 조치의 디버그 로그를 활성화합니다.

<#root>

>

debug fover

```
auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution c
```

참조

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-fire.html>

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance_solution.html

<https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497>

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.