FTD HA(장애 조치)를 다른 FMC로 마이그레이션

목차

소개

- 약어
- 사전 요구 사항
- 사용되는 구성 요소
- 토폴로지

구성

- 1단계. 기본 방화벽에서 디바이스 컨피그레이션 내보내기
- 2단계. 보조 FTD를 활성 상태로 만듭니다.
- 3단계. FTD HA 중단
- 4단계. FTD1(이전의 기본) 데이터 인터페이스 격리
- 5단계. FTD 공유 정책 내보내기
- 6단계. 기존/소스 FMC에서 FTD1(Ex-Primary)을 삭제/등록 취소합니다
- 7단계. FTD 정책 구성 객체를 FMC2(대상 FMC)로 가져옵니다.
- 8단계. FTD1(ex-Primary)을 FMC2에 등록
- 9단계. FTD 디바이스 컨피그레이션 객체를 FMC2(대상 FMC)로 가져옵니다
- 10단계. FTD 컨피그레이션을 완료합니다.
- 11단계. 배포된 FTD 구성 확인
- 12단계. 컷오버 실행
- 13단계. 두 번째 FTD를 FMC2(대상 FMC)로 마이그레이션
- 14단계. FTD HA 다시 구성

참조

소개

이 문서에서는 기존 FMC에서 다른 FMC로 FTD HA를 마이그레이션하는 절차에 대해 설명합니다.

독립형 방화벽을 새 FMC로 마이그레이션하려면 https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/222480-migrate-an-ftd-from-one-fmc-to-another-f.html을 참조하십시오

약어

ACP = 액세스 제어 정책

ARP = ARP(Address Resolution Protocol)

CLI = 명령줄 인터페이스

FMC = 보안 방화벽 관리 센터

FTD = 보안 방화벽 위협 방어

GARP = 무상 ARP

HA = 고가용성

MW = 유지 보수 기간

UI = 사용자 인터페이스

사전 요구 사항

마이그레이션 프로세스를 시작하기 전에 다음 전제 조건을 갖추었는지 확인하십시오.

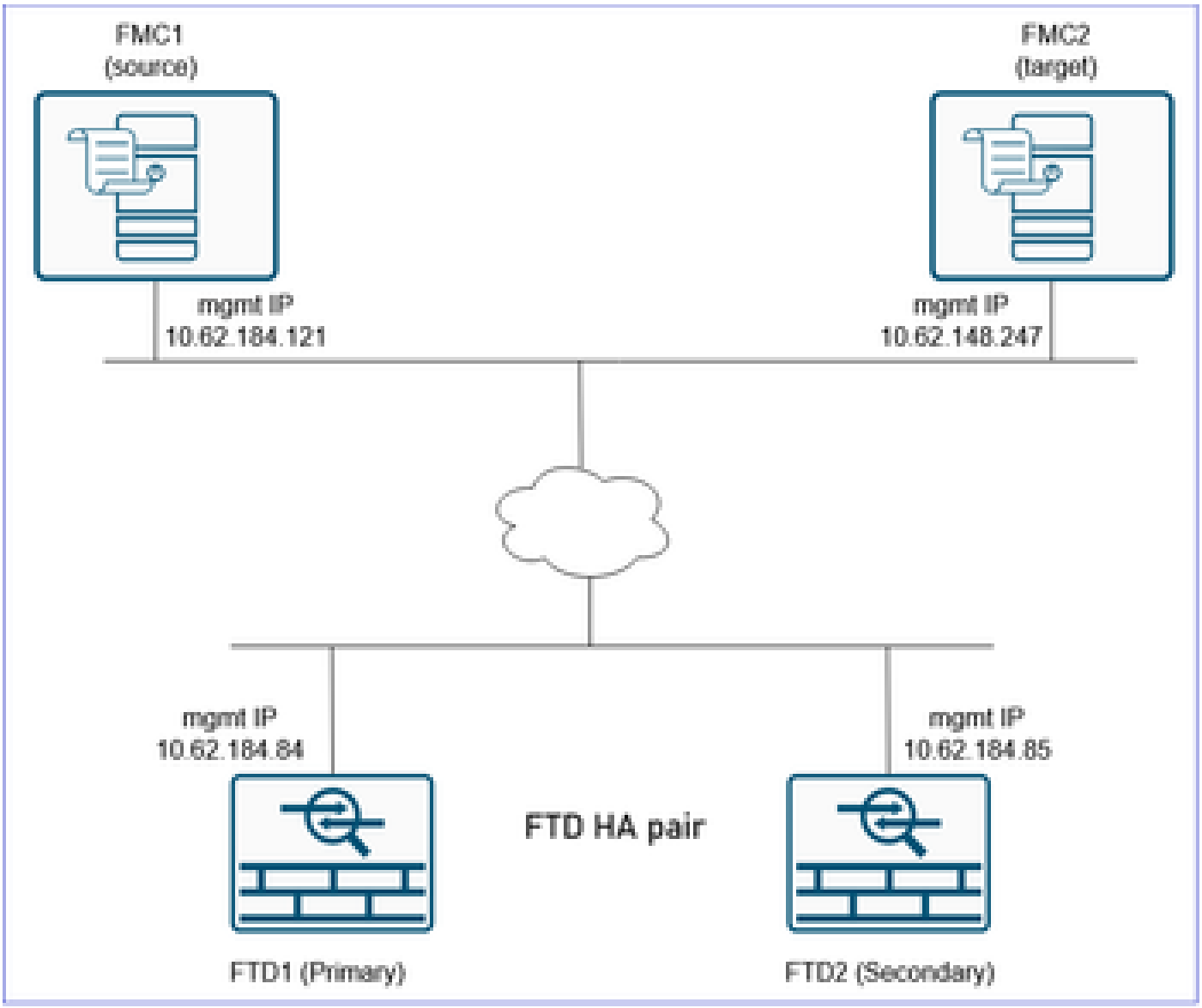
- 소스 및 대상 FMC 모두에 대한 UI 및 CLI 액세스
- FMC 및 방화벽 모두에 대한 관리 자격 증명
- 두 방화벽에 대한 콘솔 액세스
- L3 업스트림 및 다운스트림 디바이스에 액세스합니다(ARP 캐시를 지워야 하는 경우).
- 대상/대상 FMC의 버전이 소스/이전 FMC와 동일한지 확인합니다.
- 대상/대상 FMC에 소스/이전 FMC와 동일한 라이센스가 있는지 확인합니다.
- MW가 전송 트래픽에 영향을 미치므로 마이그레이션을 수행하도록 준비해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Firewall 31xx, FTD 버전 7.4.2.2.
- Secure Firewall Management Center 버전 7.4.2.2.
- 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.

토폴로지



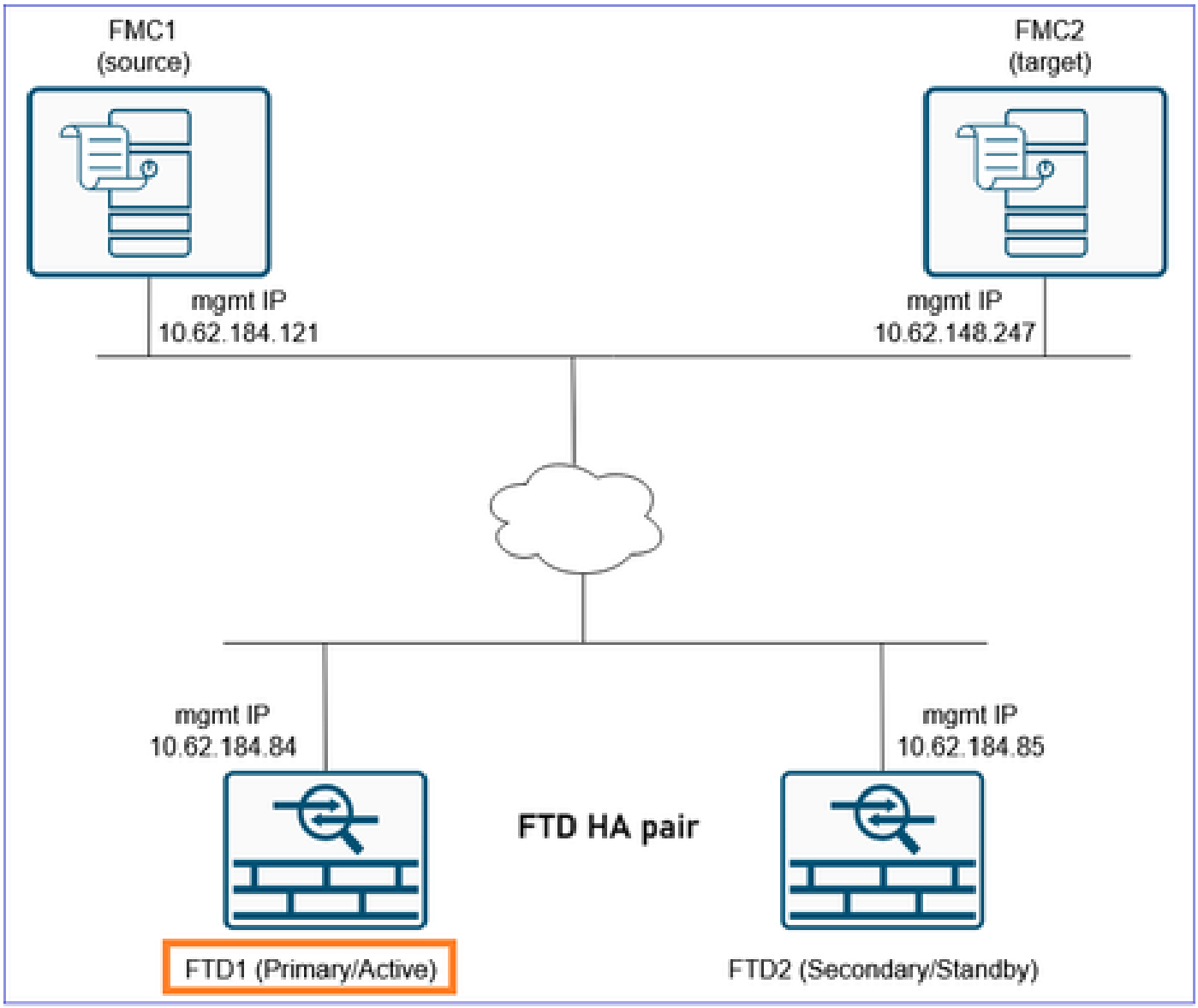
구성

마이그레이션 단계

이 시나리오에서는 다음 상태를 고려합니다.

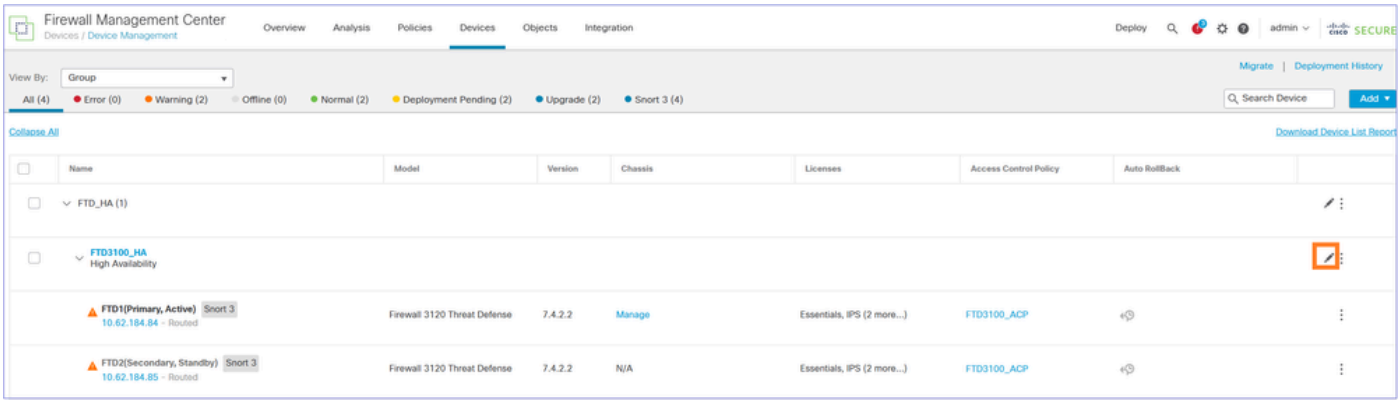
FTD1: 기본/활성

FTD2: 보조/대기

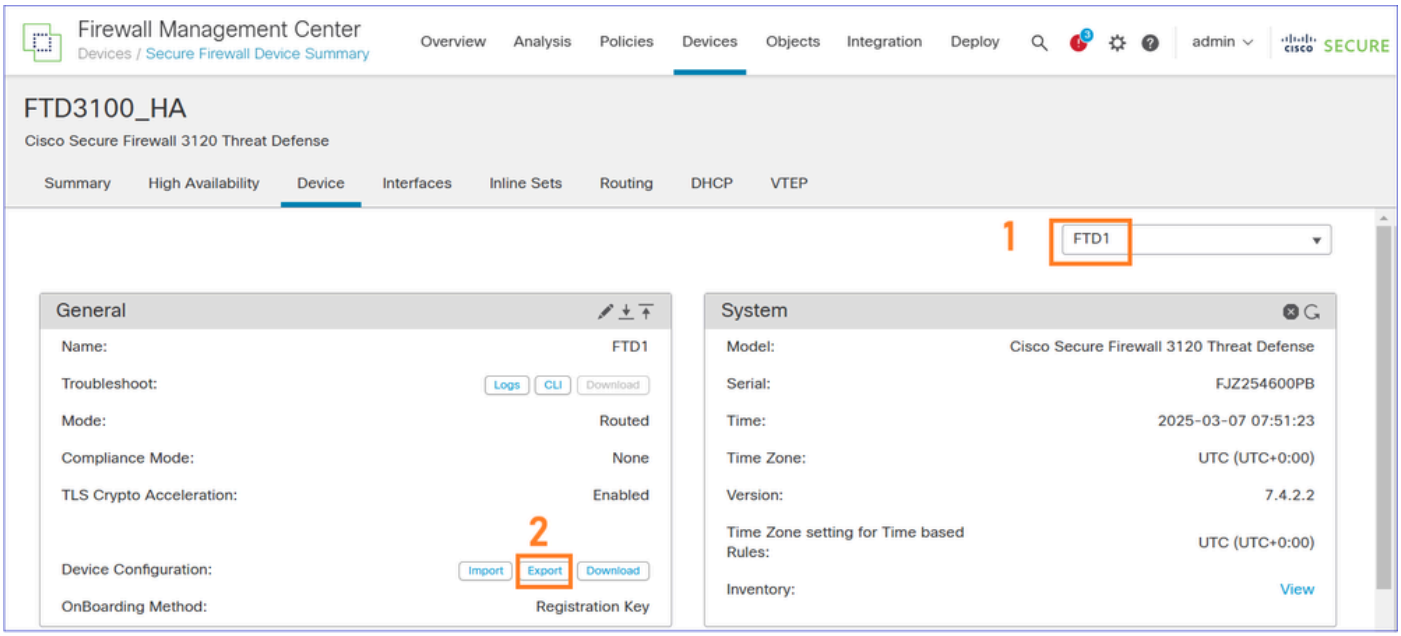


1단계. 기본 방화벽에서 디바이스 컨피그레이션 내보내기

FMC1(소스 FMC)에서 Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다. FTD HA 쌍을 선택하고 Edit를 선택합니다.

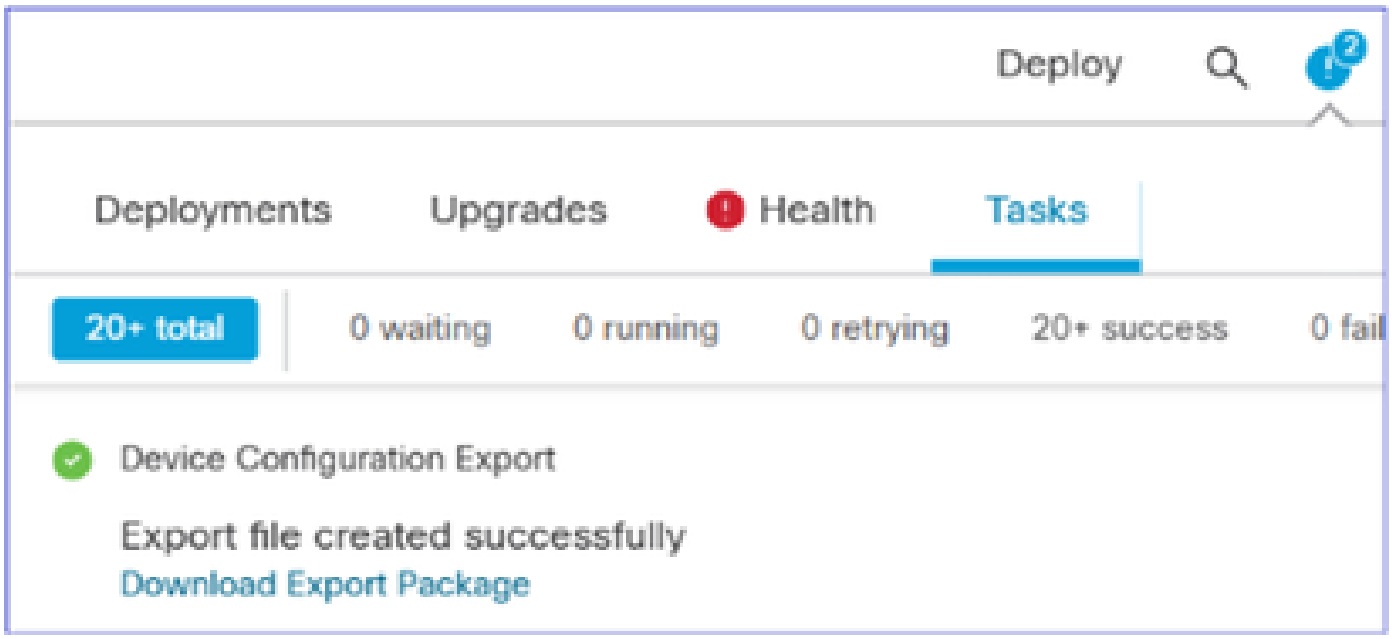


Device(디바이스) 탭으로 이동합니다. Primary/Active FTD(이 경우 FTD1)가 선택되었는지 확인하고 Export(내보내기)를 선택하여 디바이스 컨피그레이션을 내보냅니다.



참고: 내보내기 옵션은 7.1 소프트웨어 릴리스 이상에서 사용할 수 있습니다.

Notifications(알림) > Tasks(작업) 페이지로 이동하여 내보내기가 완료되었는지 확인할 수 있습니다. 그런 다음 Download Export Package(내보내기 패키지 다운로드)를 선택합니다.



또는 General(일반) 영역에서 Download(다운로드) 버튼을 클릭할 수 있습니다. sfo 파일을 가져옵니다(예: DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo).

파일에는 다음과 같은 장치 관련 컨피그레이션이 포함되어 있습니다.

- 라우티드 인터페이스
- 인라인 집합
- 라우팅
- DHCP
- VTEP

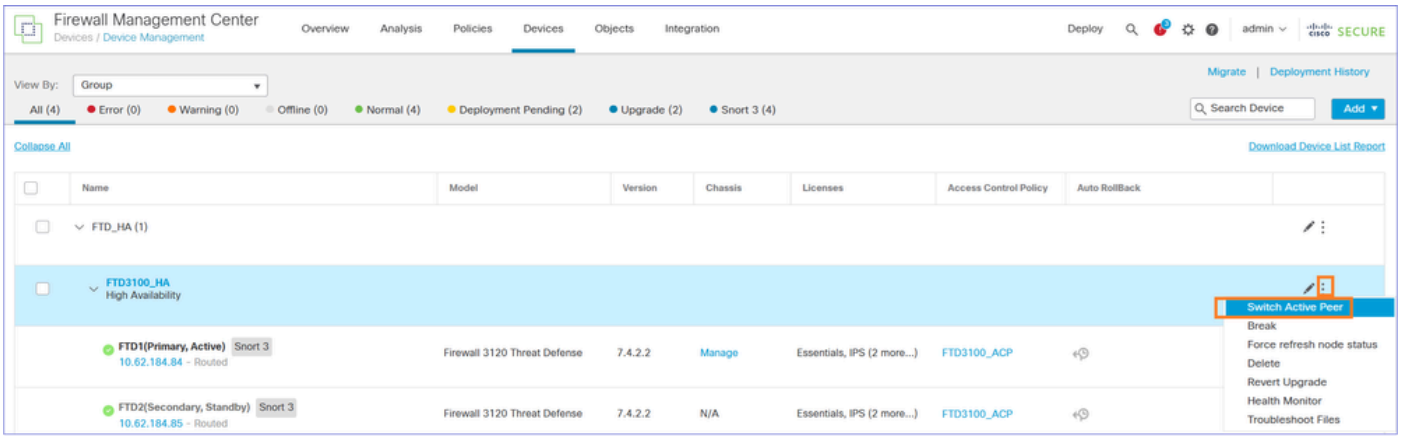
- 연결된 개체

참고: 내보낸 컨피그레이션 파일은 동일한 FTD로만 다시 가져올 수 있습니다. FTD의 UUID는 가져온 sfo 파일의 내용과 일치해야 합니다. 동일한 FTD를 다른 FMC에 등록하고 sfo 파일을 가져올 수 있습니다.

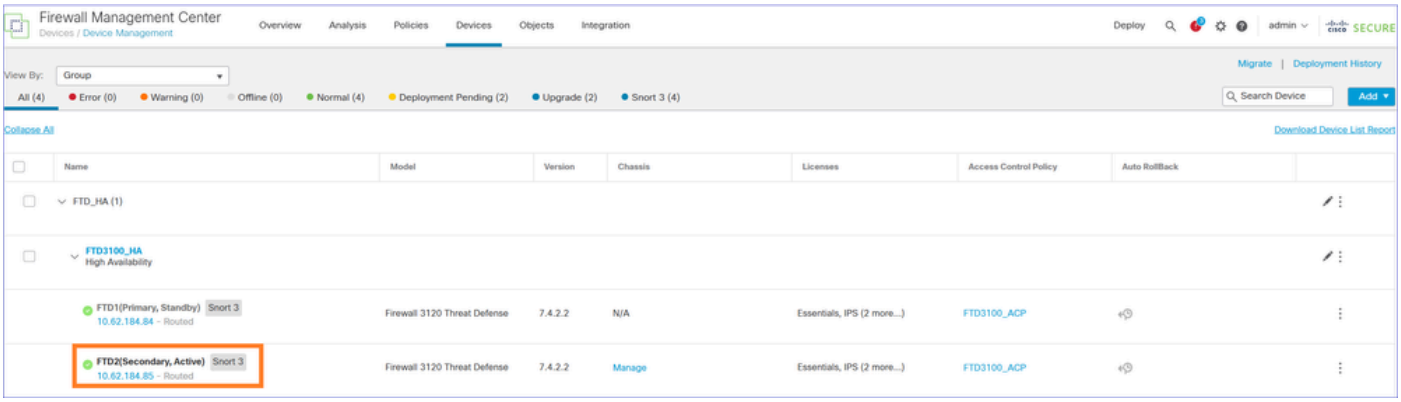
참조: '디바이스 컨피그레이션 내보내기 및 가져오기'
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

2단계. 보조 FTD를 활성 상태로 만듭니다.

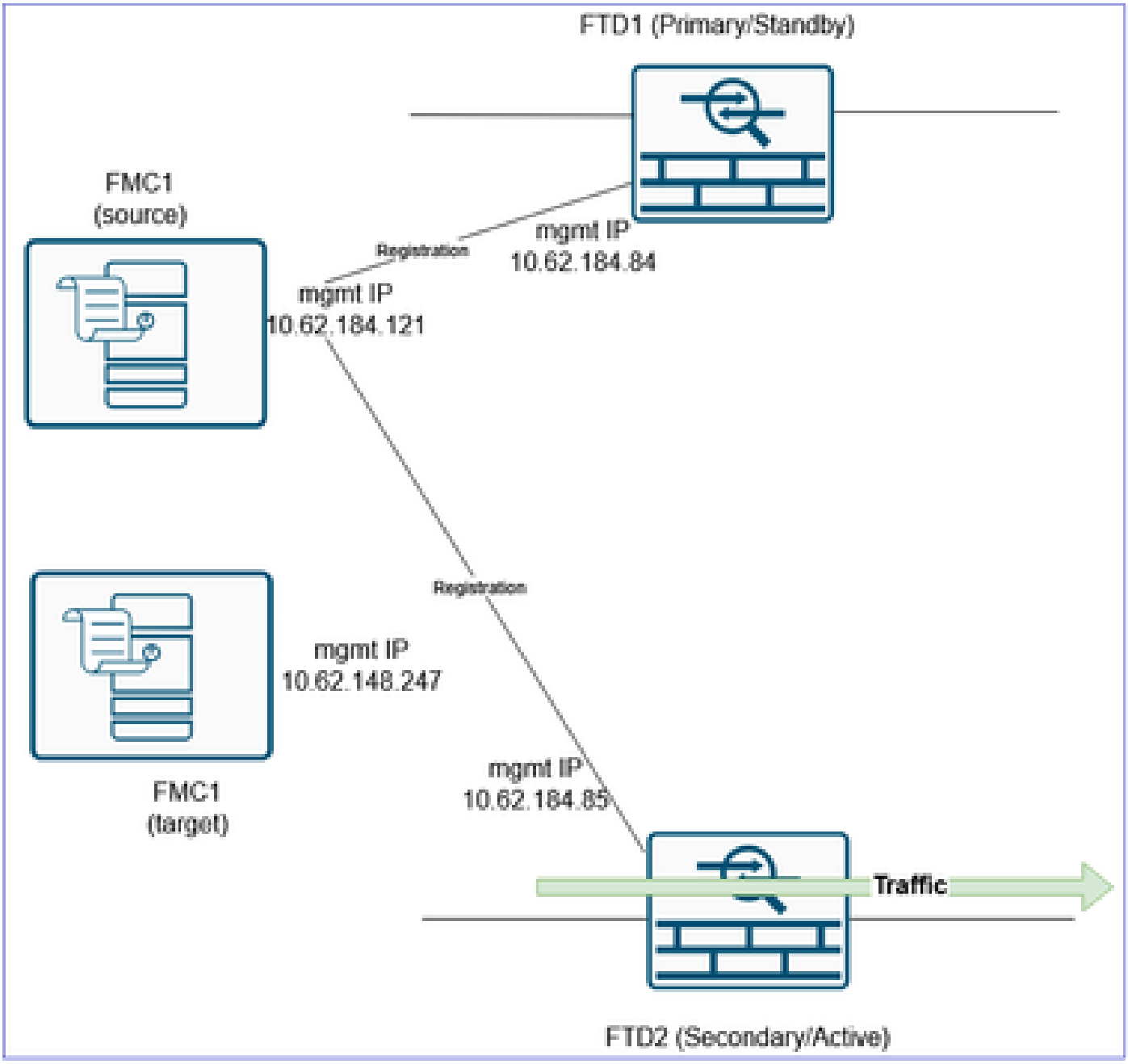
Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 FTD HA 쌍을 선택하고 Switch Active Pair(활성 쌍 전환)를 선택합니다.



결과는 FTD1(Primary/Standby) 및 FTD(Secondary/Active)입니다.

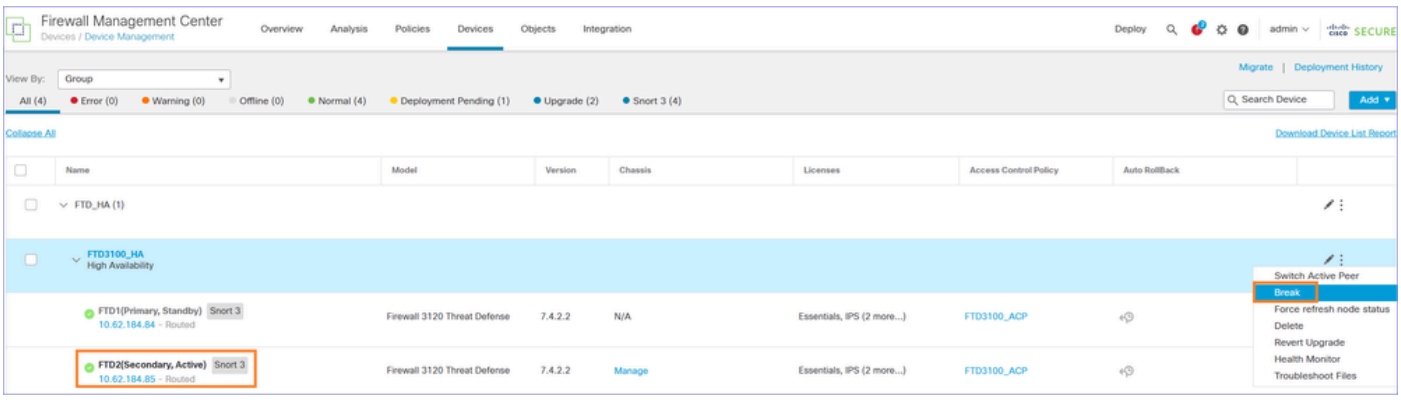


이제 트래픽은 보조/활성 FTD에 의해 처리됩니다.

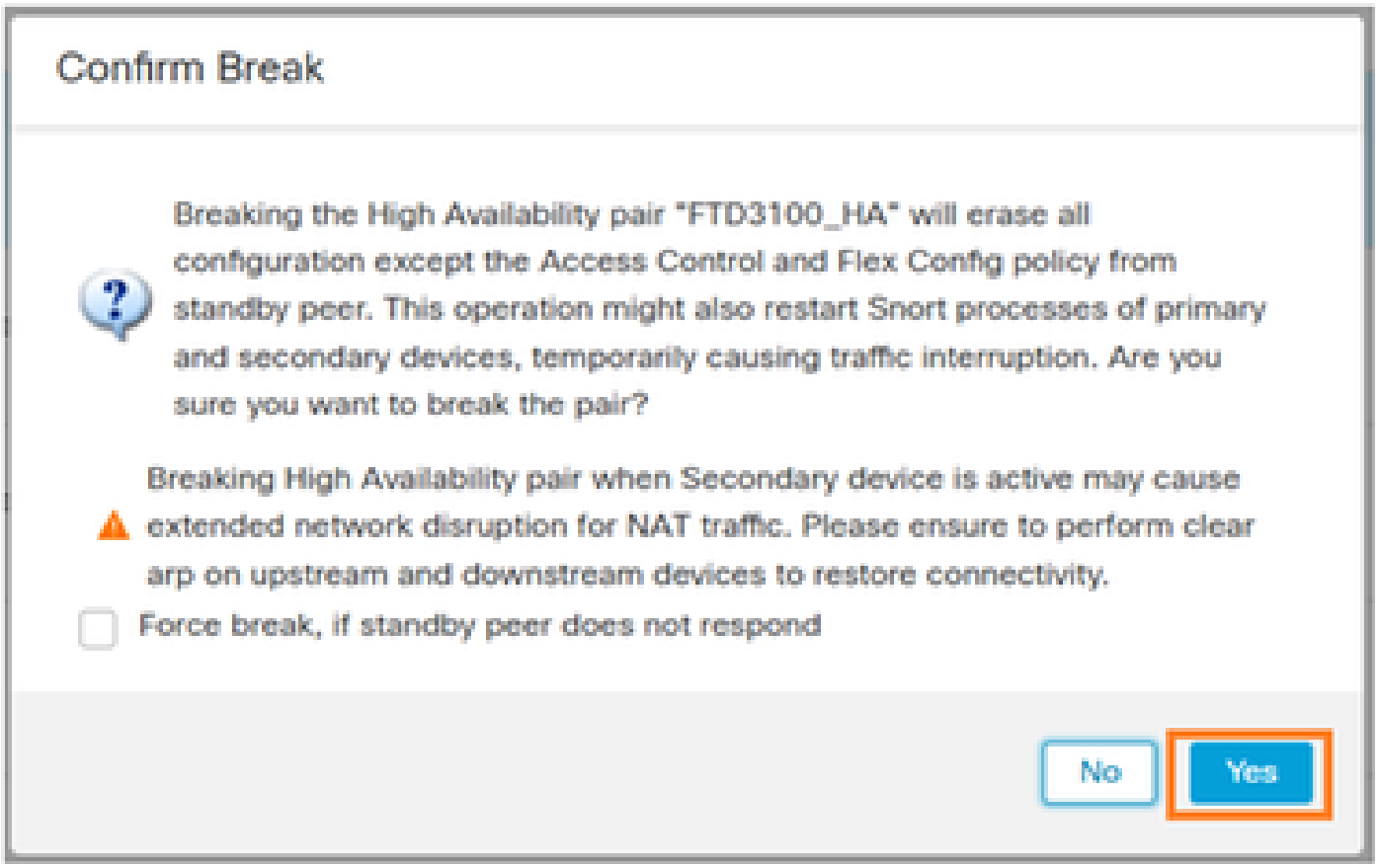


3단계. FTD HA 중단

Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 FTD HA를 중단합니다.



이 창이 나타납니다. 예 선택



참고: 이 시점에서는 HA 중단 시 Snort 엔진이 다시 시작된 이후 몇 초 동안 일부 트래픽 중단이 발생할 수 있습니다. 또한 메시지에서 언급한 것처럼, NAT를 사용하고 트래픽 중단이 장기화되는 경우 업스트림 및 다운스트림 디바이스에서 ARP 캐시를 지우는 것이 좋습니다.

FTD HA를 분리한 후에는 FMC에 두 개의 독립형 FTD가 있습니다.

컨피그레이션 관점에서 FTD2(ex-Active)는 장애 조치 관련 컨피그레이션을 제외하고 여전히 컨피그레이션을 유지하며 트래픽을 처리합니다.

```
<#root>

FTD3100-4#

show failover


Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
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 1 of 1288 maximum
MAC Address Move Notification Interval not set
```

<#root>

FTD3100-4#

show interface ip brief

```
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/1           unassigned      YES           unset  up          up
Port-channel1              unassigned      YES           unset  up          up
Port-channel1.200          10.0.200.70     YES           manual up          up
Port-channel1.201          10.0.201.70     YES           manual up          up
```

FTD1(ex-Standby)에서 모든 컨피그레이션이 제거되었습니다.

<#root>

FTD3100-3#

show failover

```
Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
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 1 of 1288 maximum
MAC Address Move Notification Interval not set
```

<#root>

FTD3100-3#

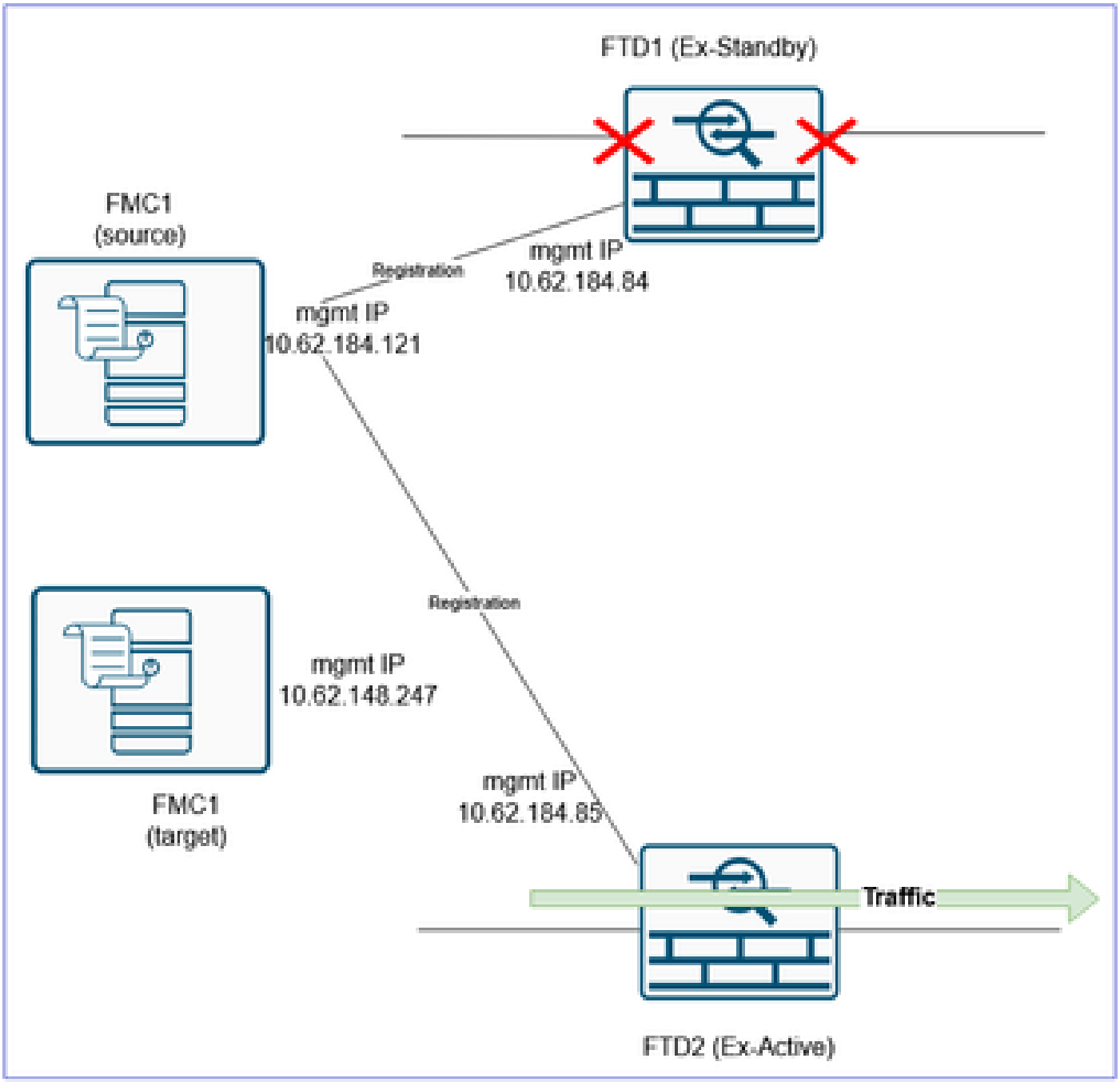
show interface ip brief

```
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/1           unassigned      YES           unset  up          up
Ethernet1/1                unassigned      YES           unset  admin down  down
Ethernet1/2                unassigned      YES           unset  admin down  down
Ethernet1/3                unassigned      YES           unset  admin down  down
Ethernet1/4                unassigned      YES           unset  admin down  down
Ethernet1/5                unassigned      YES           unset  admin down  down
Ethernet1/6                unassigned      YES           unset  admin down  down
Ethernet1/7                unassigned      YES           unset  admin down  down
Ethernet1/8                unassigned      YES           unset  admin down  down
Ethernet1/9                unassigned      YES           unset  admin down  down
Ethernet1/10               unassigned      YES           unset  admin down  down
Ethernet1/11               unassigned      YES           unset  admin down  down
Ethernet1/12               unassigned      YES           unset  admin down  down
Ethernet1/13               unassigned      YES           unset  admin down  down
Ethernet1/14               unassigned      YES           unset  admin down  down
```

```
Ethernet1/15               unassigned      YES           unset  admin down  down
Ethernet1/16               unassigned      YES           unset  admin down  down
```

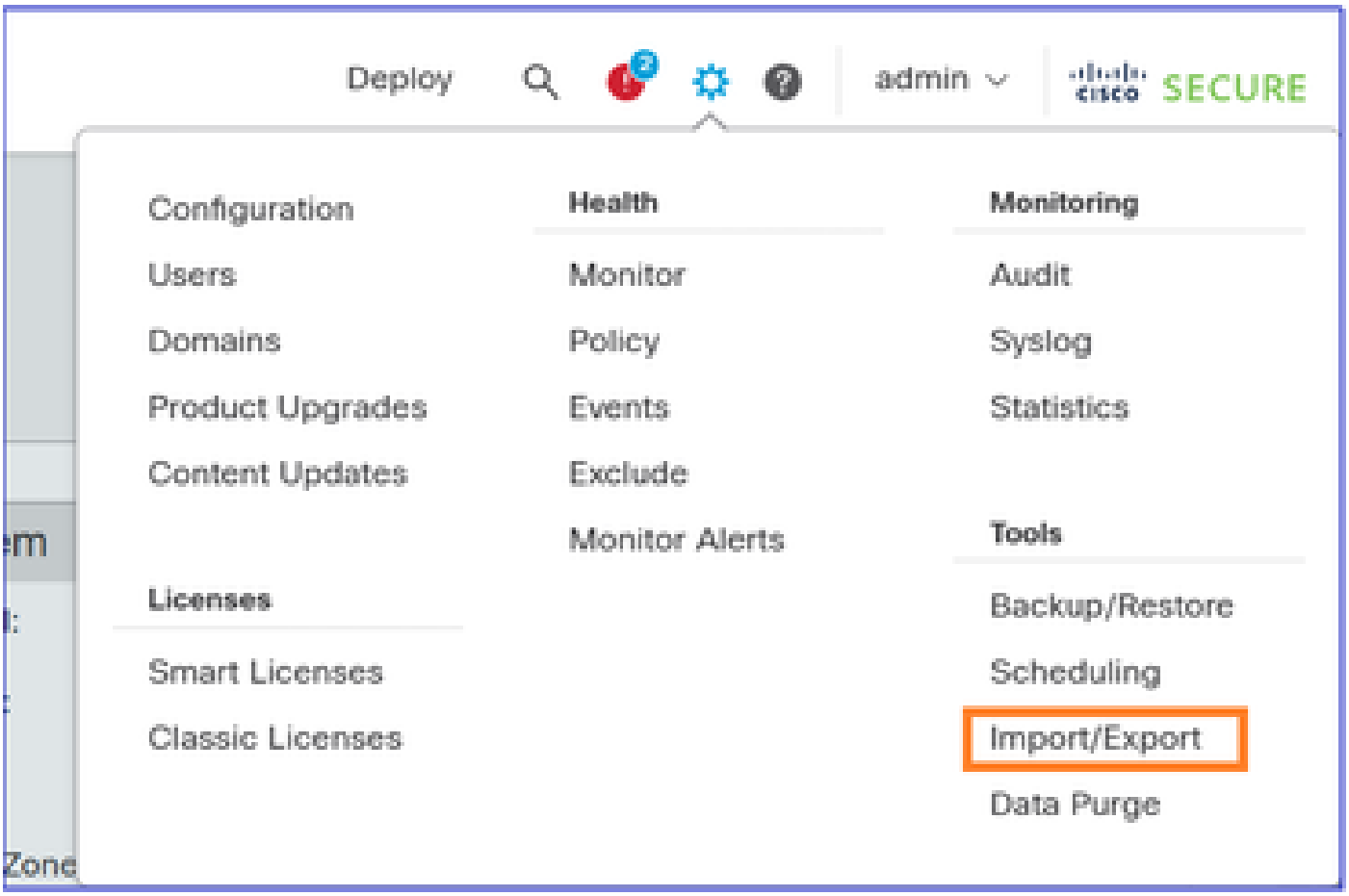
4단계. FTD1(이전의 기본) 데이터 인터페이스 격리

FTD1(ex-Primary)에서 데이터 케이블을 분리합니다. FTD 관리 포트만 연결된 상태로 둡니다.



5단계. FTD 공유 정책 내보내기

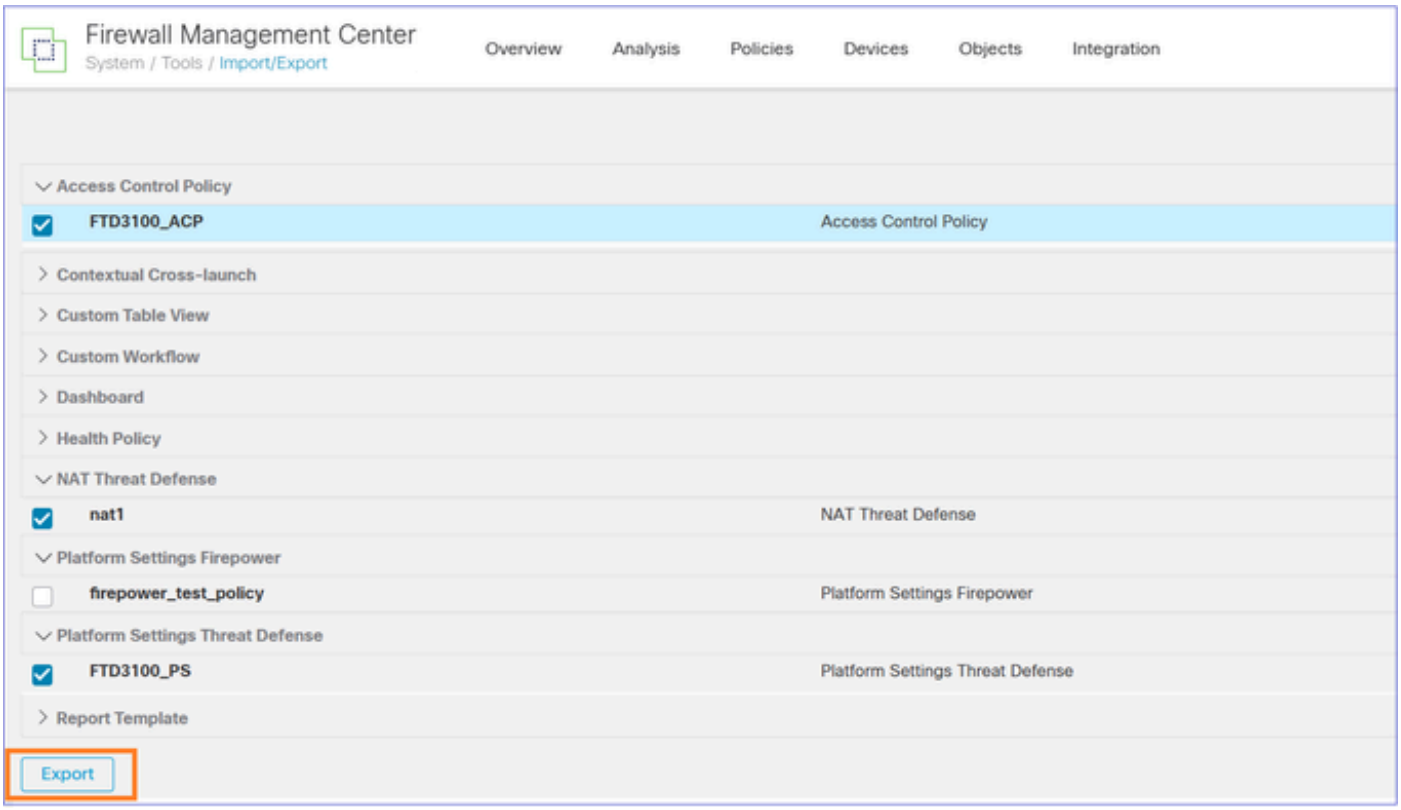
System > Tools로 이동하고 Import/Export를 선택합니다.



디바이스에 연결된 다양한 정책을 내보냅니다. 다음과 같이 FTD에 연결된 모든 정책을 익스포트해야 합니다.

- ACP(액세스 제어 정책)
- NAT(Network Address Translation) 정책
- 상태 정책(사용자 지정 시)
- FTD 플랫폼 설정

등등.



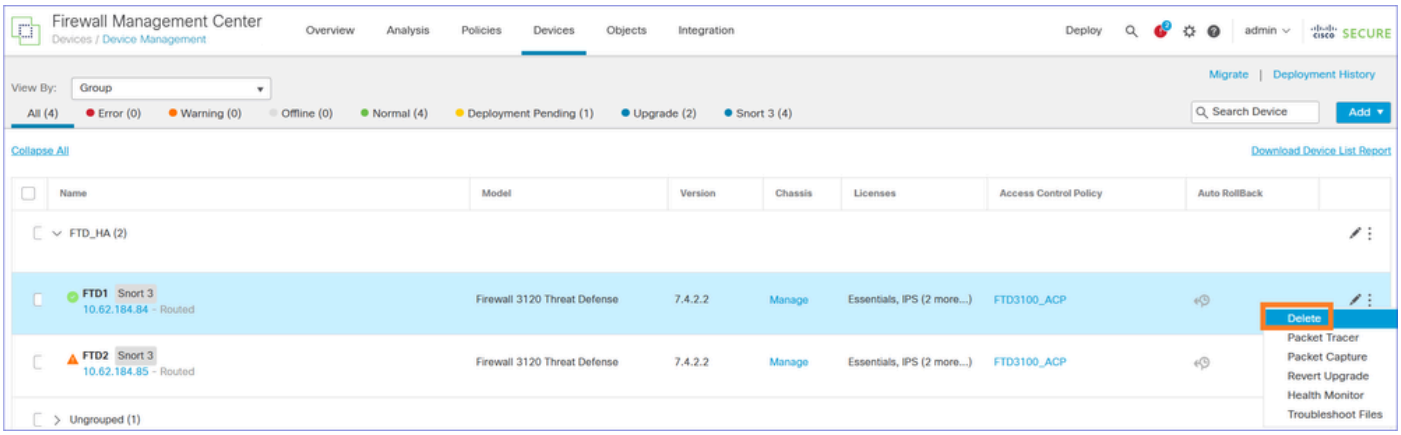
참고: 이 작성 시에는 VPN 관련 컨피그레이션 내보내기가 지원되지 않습니다. 디바이스 등록 후 FMC2(대상 FMC)에서 VPN을 수동으로 재구성해야 합니다.

관련 개선 사항 Cisco 버그 ID CSCwf05294

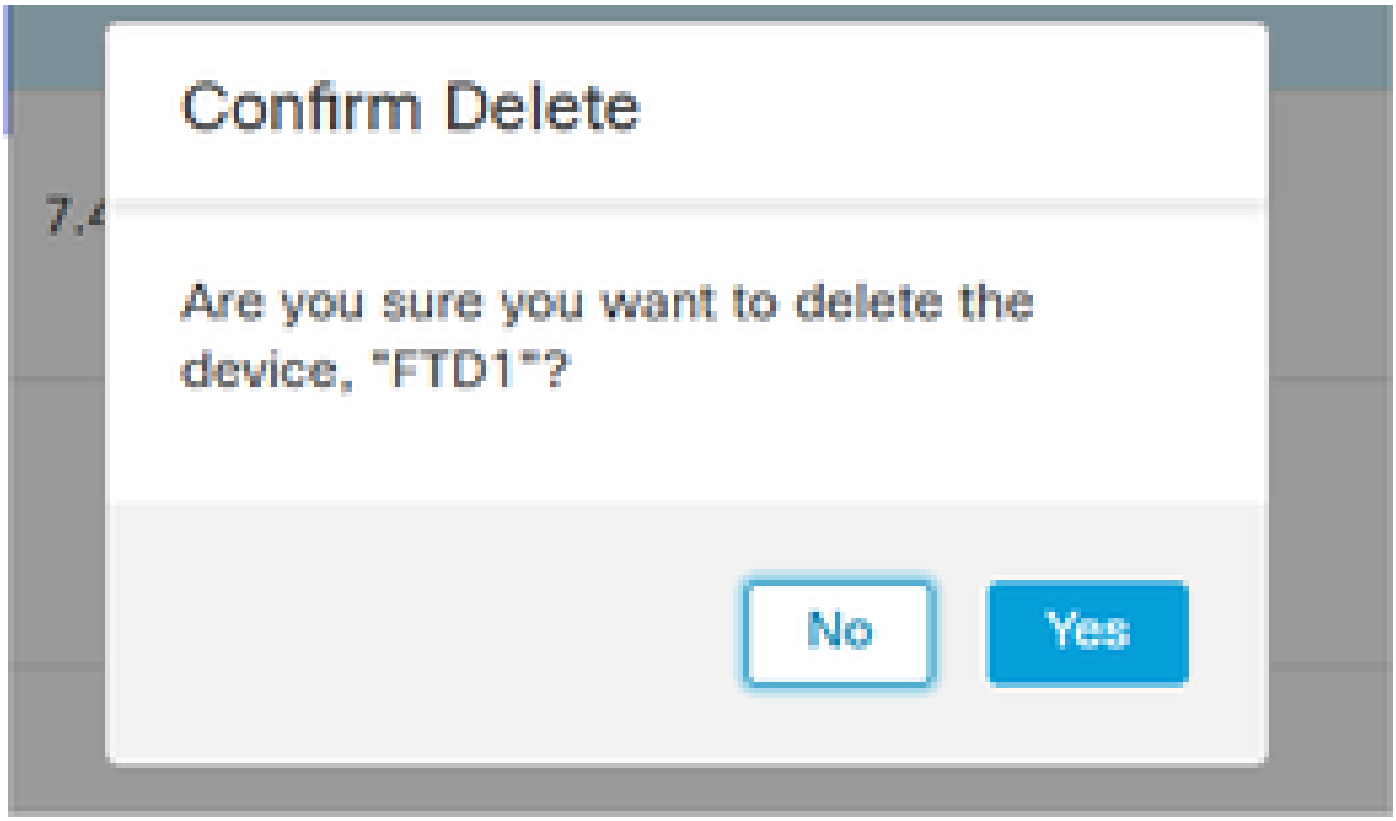
.

결과는 .sfo 파일입니다(예: ObjectExport_20250306082738.sfo)

6단계. 기존/소스 FMC에서 FTD1(Ex-Primary)을 삭제/등록 취소합니다



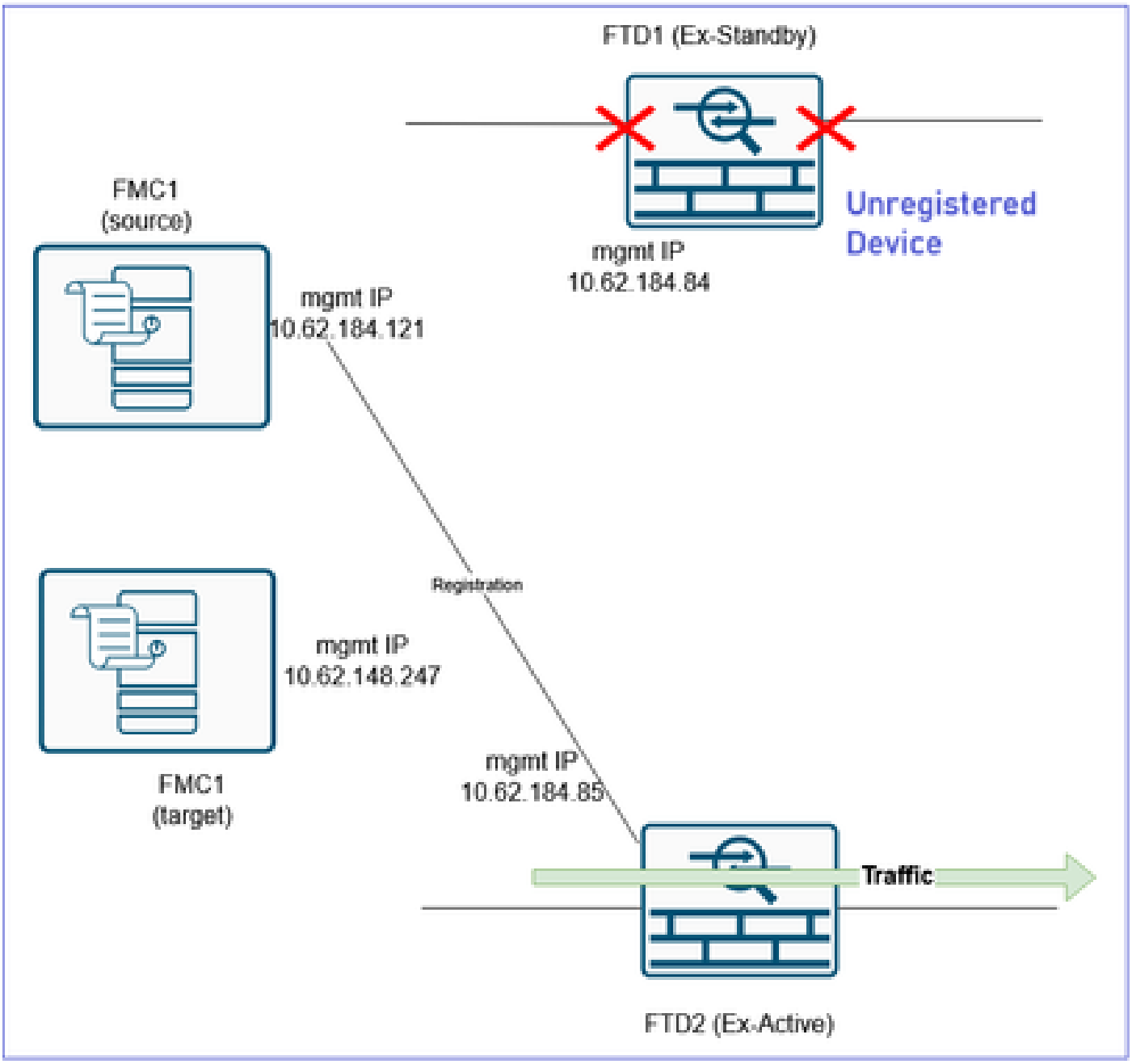
디바이스 삭제 확인:



FTD1 CLI 확인:

```
<#root>

>

show managers

No managers configured.

>
```

FTD1 디바이스 삭제 후의 현재 상태:

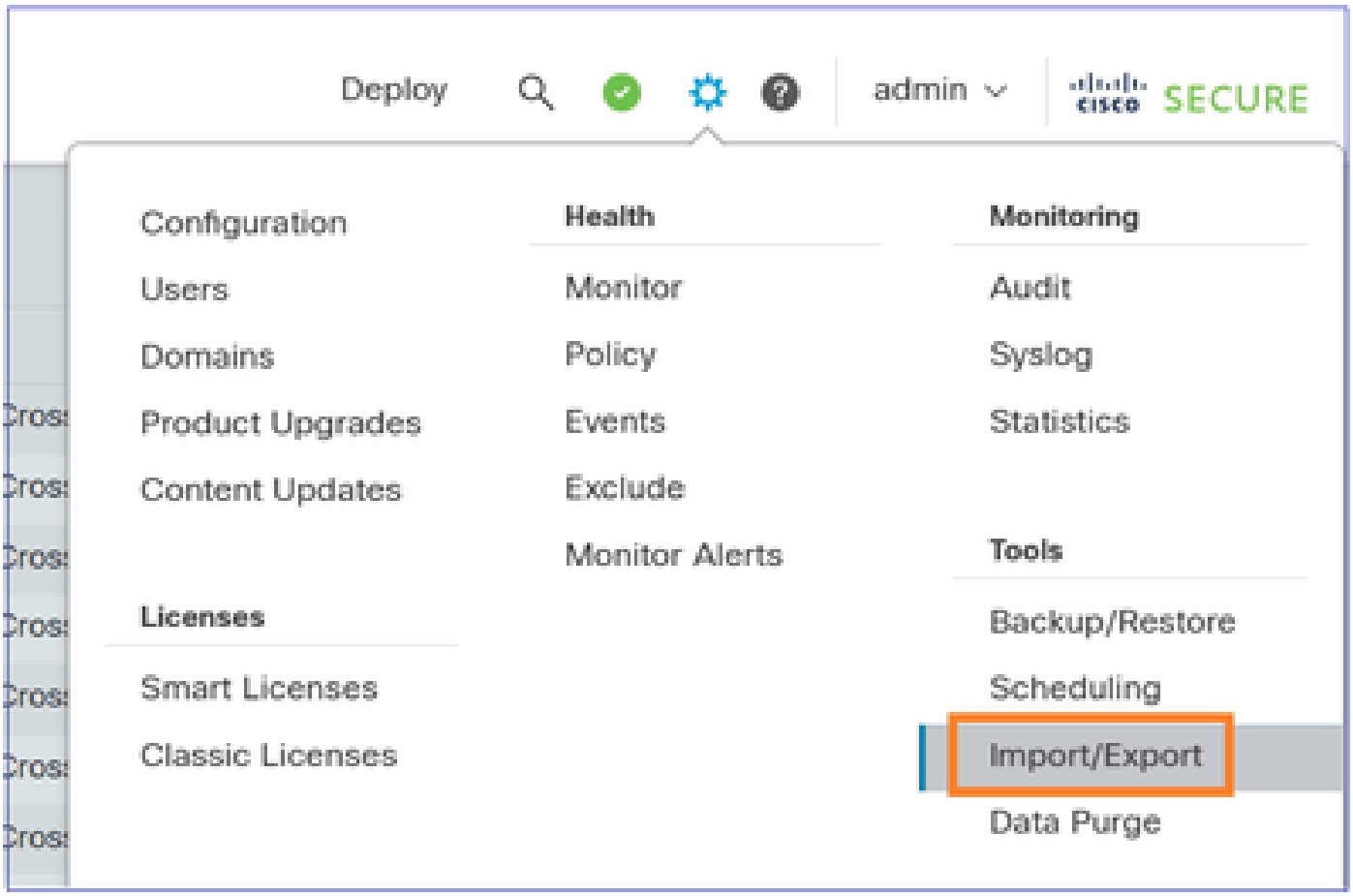


7단계. FTD 정책 구성 객체를 FMC2(대상 FMC)로 가져옵니다.

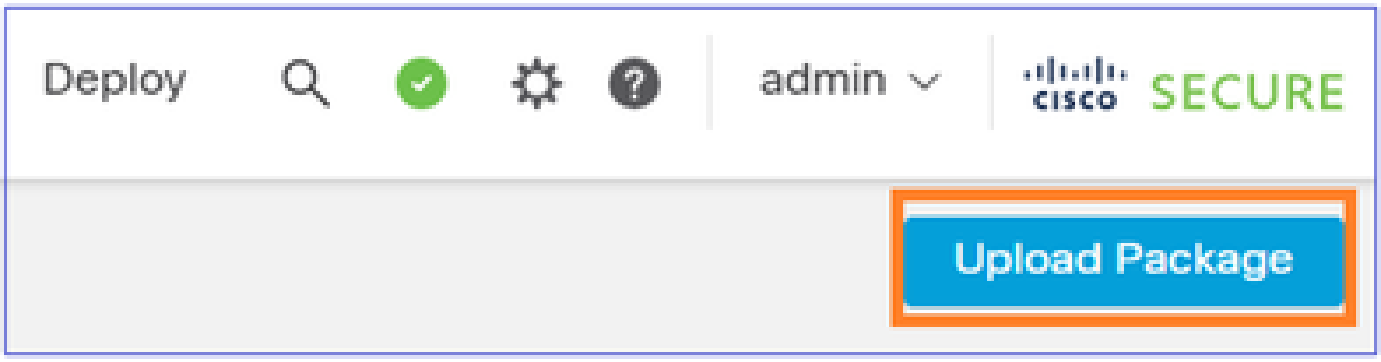
참고: 이 문서에서는 단일 FTD HA 쌍을 새 FMC로 마이그레이션하는 방법을 중점적으로 다룹니다. 반면, 동일한 정책(예: ACP, NAT)을 공유하는 여러 방화벽과 객체를 마이그레이션하려는 경우 단계적으로 이러한 사항을 고려해야 합니다.
- 대상 FMC에 동일한 이름의 기존 정책이 있는 경우 다음과 같은 질문을 받습니다.
  a. 정책을 교체하거나
  b. 다른 이름으로 새 이름을 만듭니다. 이렇게 하면 이름이 다른 중복 개체(접미사 _1)가 생성됩니다.

- 옵션 'b'로 이동한 경우 9단계에서 새로 생성된 객체를 마이그레이션된 정책(ACP 보안 영역, NAT 보안 영역, 라우팅, 플랫폼 설정 등)에 재할당합니다.

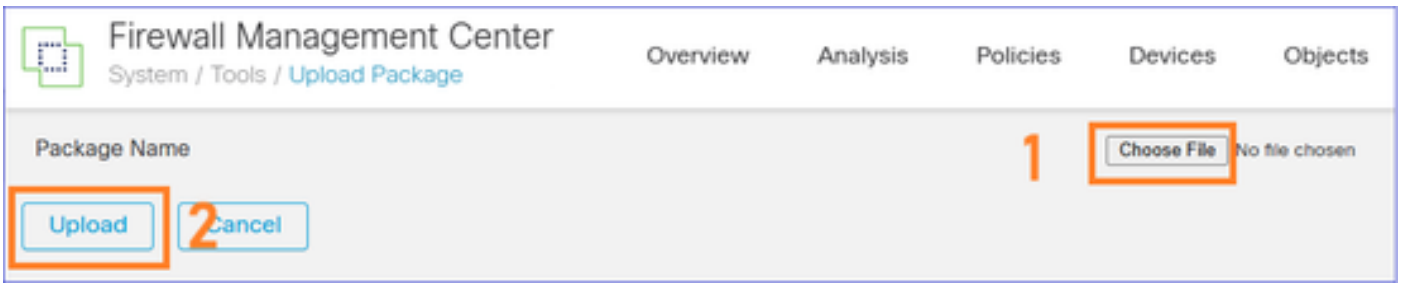
FMC2(대상 FMC)에 로그인하고 5단계에서 내보낸 FTD Policies sfo 객체를 가져옵니다.



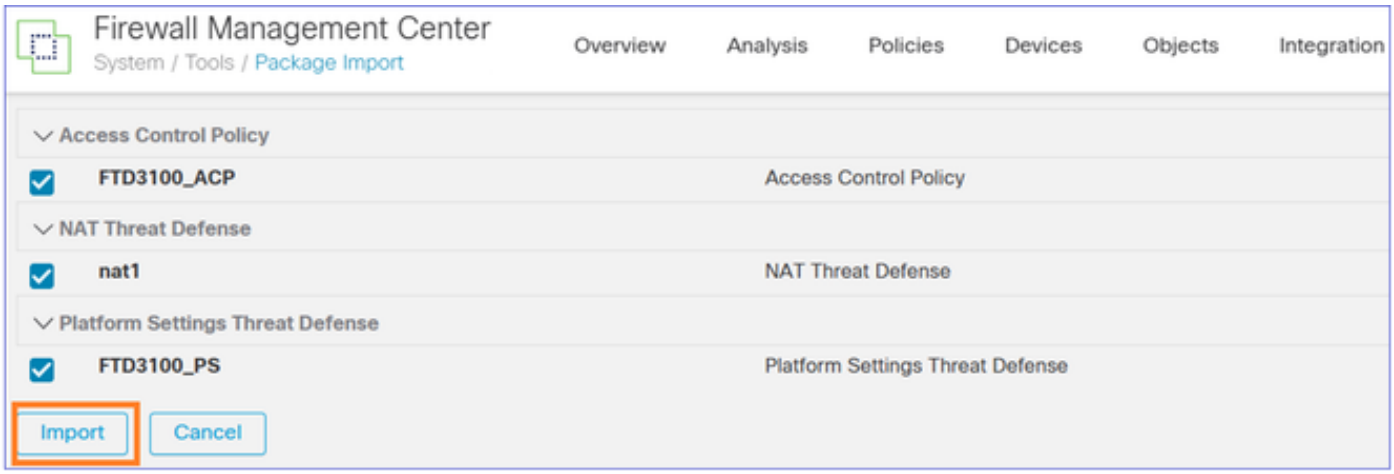
패킷 업로드 선택:



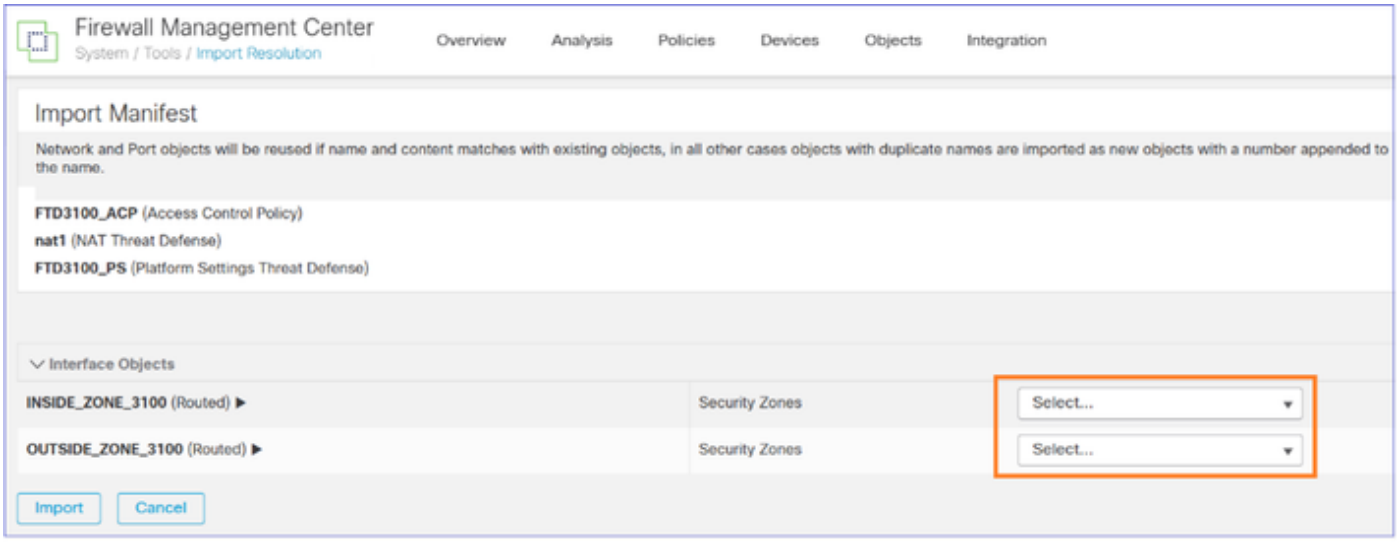
파일을 업로드합니다.



정책을 가져옵니다.



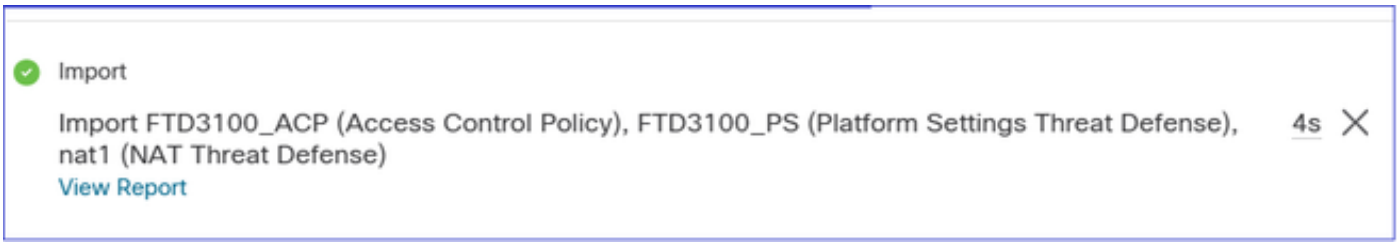
FMC2(대상 FMC)에서 인터페이스 개체/보안 영역을 생성합니다.



FMC1(소스 FMC)에서 보유했던 것과 동일한 이름을 지정할 수 있습니다.

Import(가져오기)를 선택하면 Task(작업)에서 관련 정책을 FMC2(대상 FMC)로 가져오기 시작합니다.

작업이 완료되었습니다.

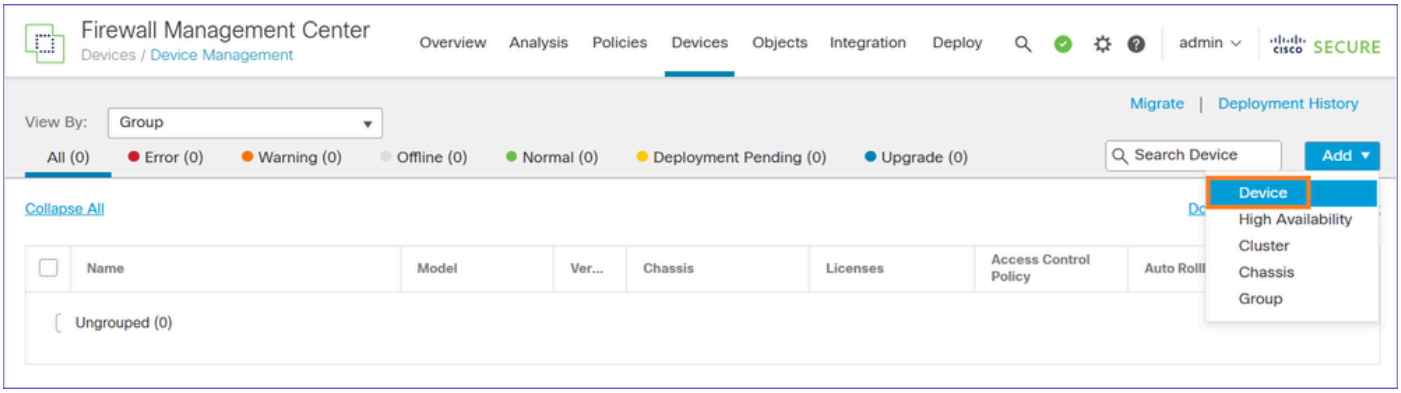


8단계. FTD1(ex-Primary)을 FMC2에 등록

FTD1(ex-Primary) CLI로 이동하여 새 관리자를 구성합니다.

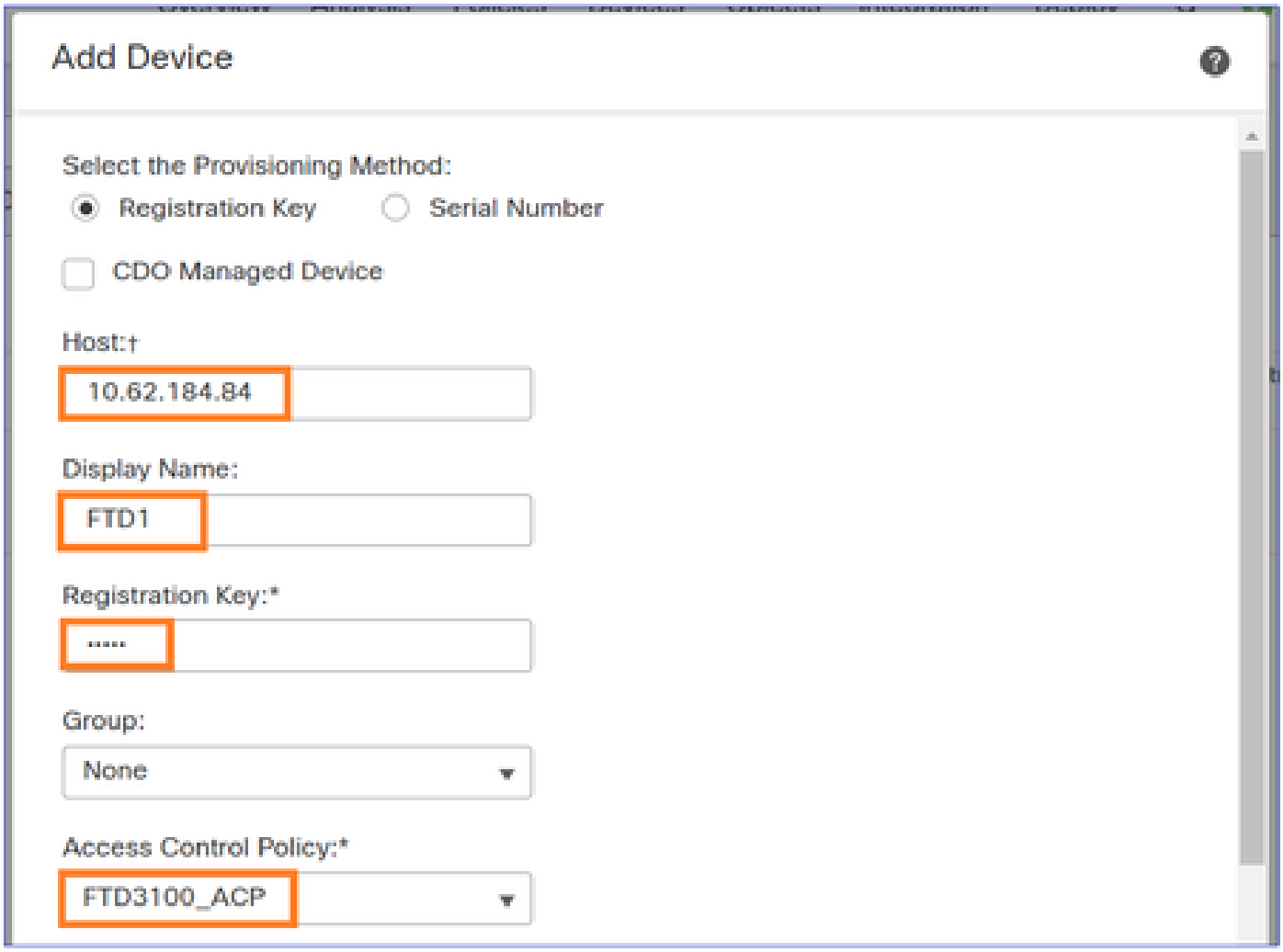
```
<#root>

>

configure manager add 10.62.148.247 cisco


Manager 10.62.148.247 successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

FMC2(대상 FMC) UI Devices(FMC UI 디바이스) > Device Management(디바이스 관리)로 이동하고 FTD 디바이스를 추가합니다.

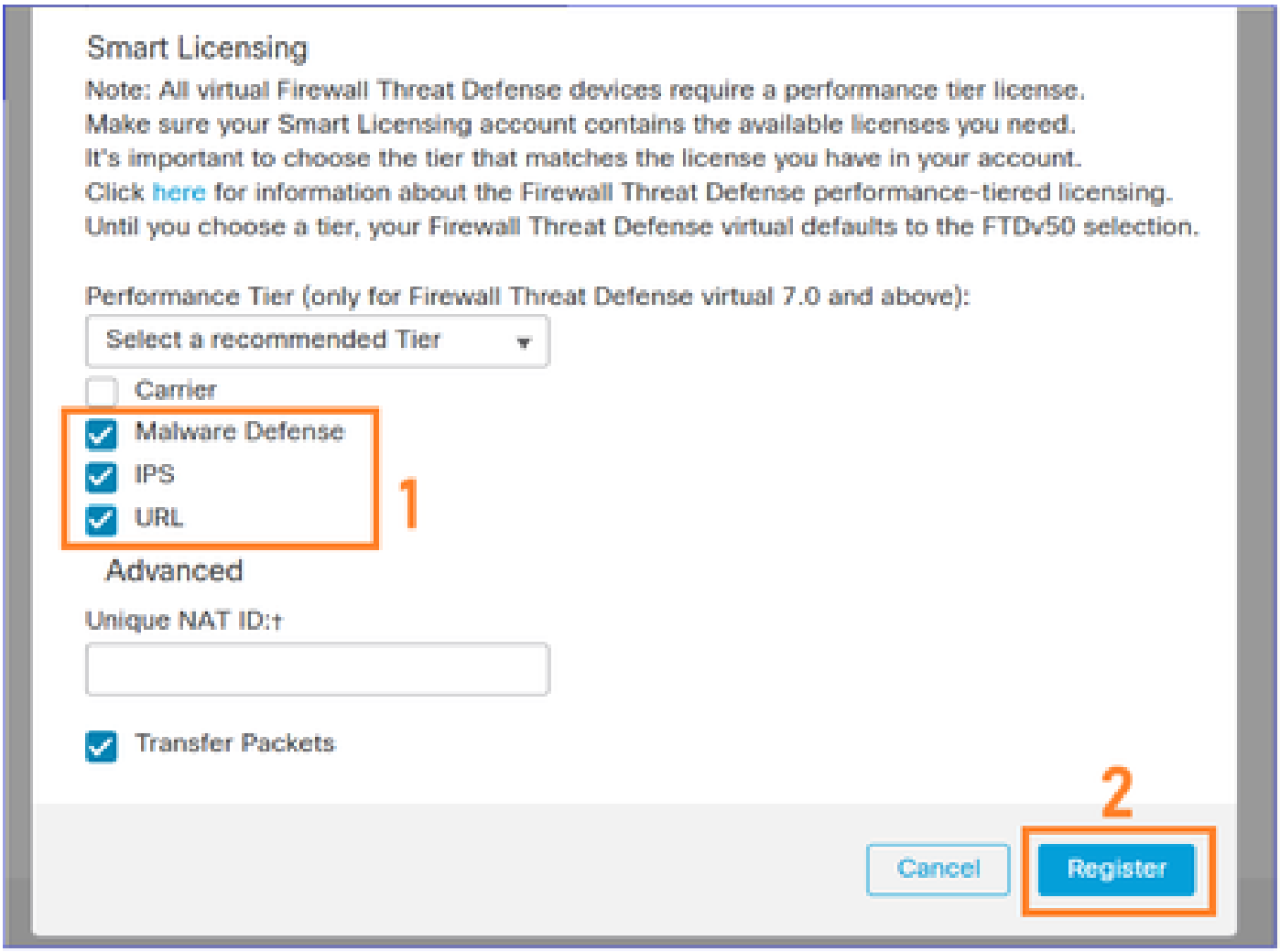


디바이스 등록이 실패할 경우 이 문서를 참조하여 문제를 해결하십시오.
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

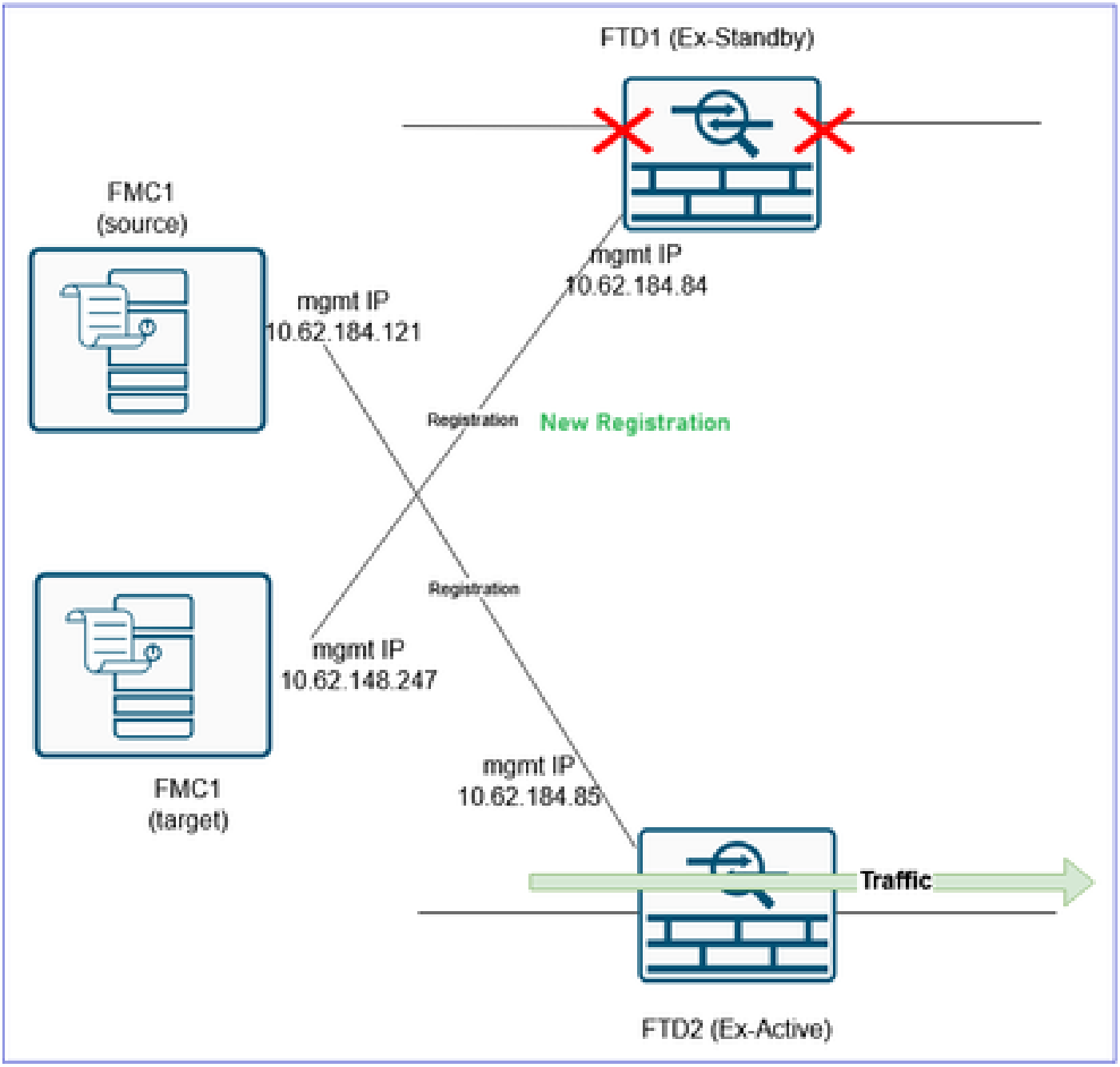
이전 단계에서 가져온 액세스 제어 정책을 할당합니다.



필요한 라이센스를 적용하고 디바이스를 등록합니다.


Smart Licensing
Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.
Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):
Select a recommended Tier
Carrier
Malware Defense
IPS
URL
1
Advanced
Unique NAT ID:†
Transfer Packets
2
Cancel
Register

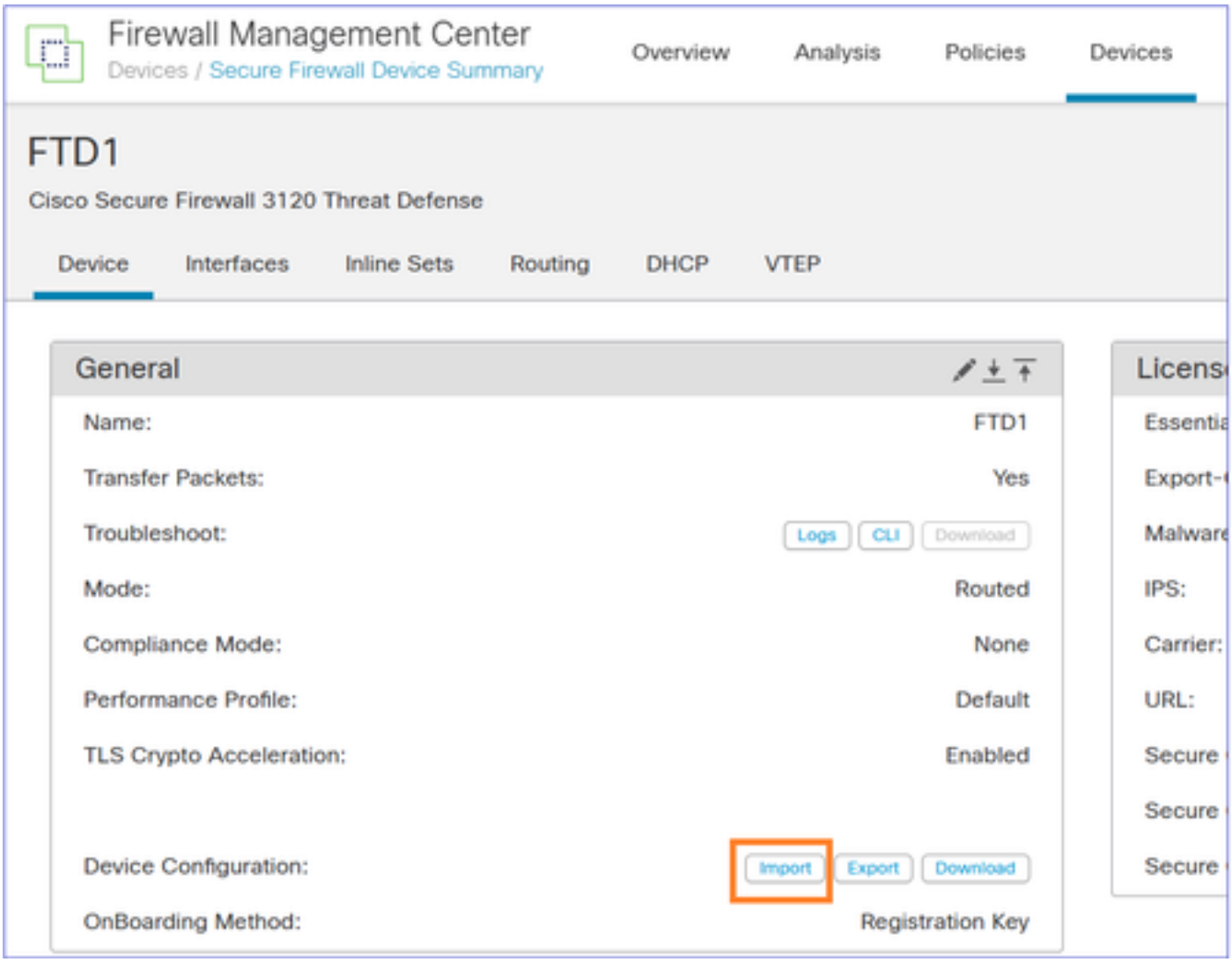
결과:



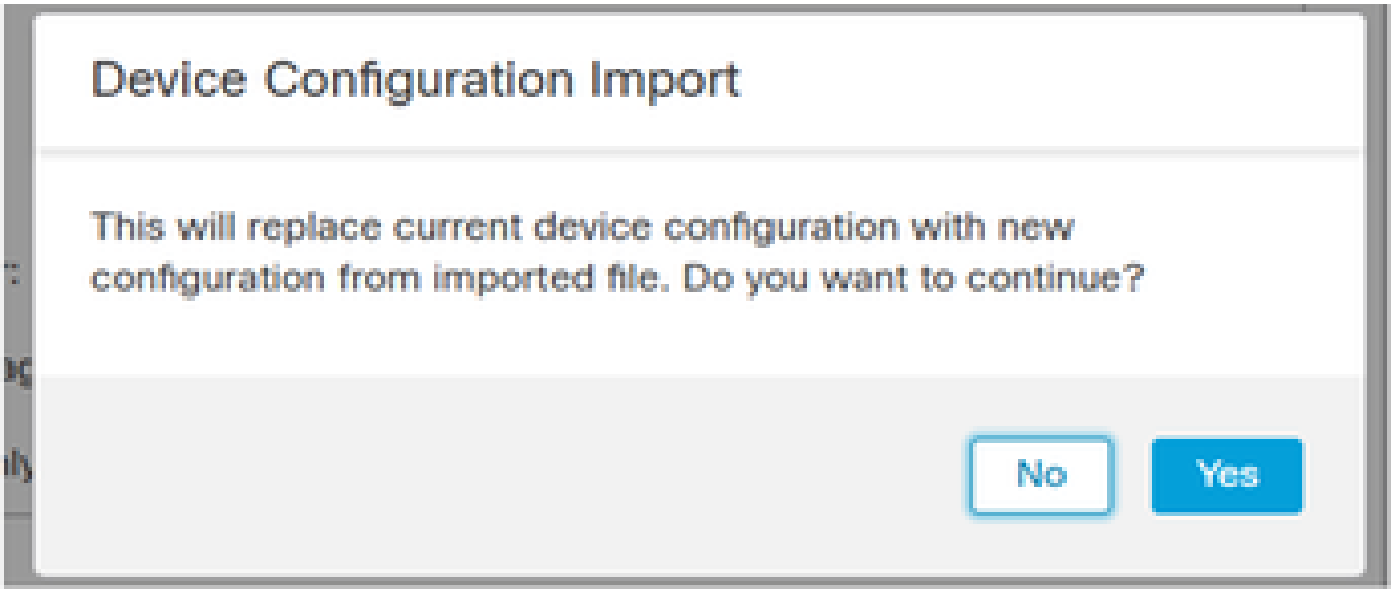
9단계. FTD 디바이스 컨피그레이션 객체를 FMC2(대상 FMC)로 가져옵니다

FMC2(대상 FMC)에 로그인하고 Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 이전 단계에서 등록한 FTD 디바이스를 수정합니다.

Device(디바이스) 탭으로 이동하고 2단계에서 내보낸 FTD Policies(FTD 정책) sfo 객체를 가져옵니다.

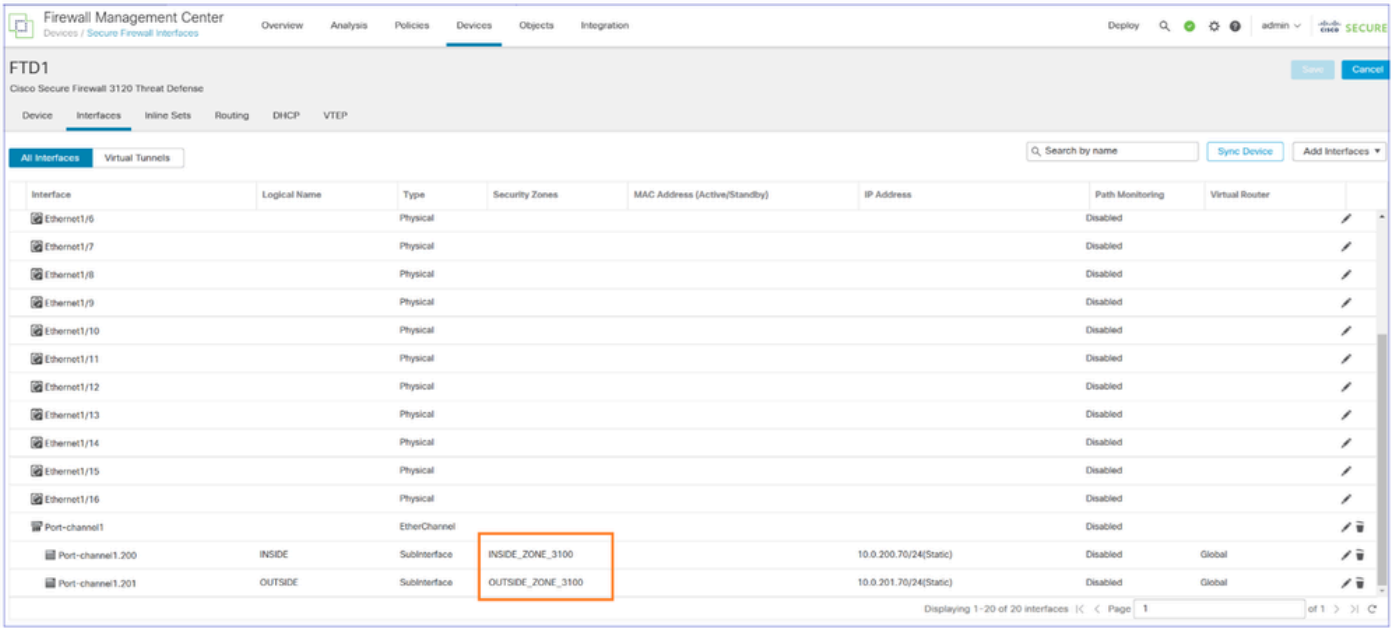


참고: 7단계에서 옵션 'b'(새 정책 생성)로 이동한 경우 새로 생성된 객체를 마이그레이션된 정책(ACP 보안 영역, NAT 보안 영역, 라우팅, 플랫폼 설정 등)에 재할당해야 합니다.



FMC 작업이 시작됩니다.

디바이스 컨피그레이션은 FTD1에 적용됩니다(예: 보안 영역, ACP, NAT 등).



⚠ 주의: 여러 액세스 제어 요소로 확장되는 ACP가 있는 경우 ACP 컴파일 프로세스(tmatch 컴파일)를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 이 명령을 사용하여 ACP 컴파일 상태를 확인할 수 있습니다.

<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed

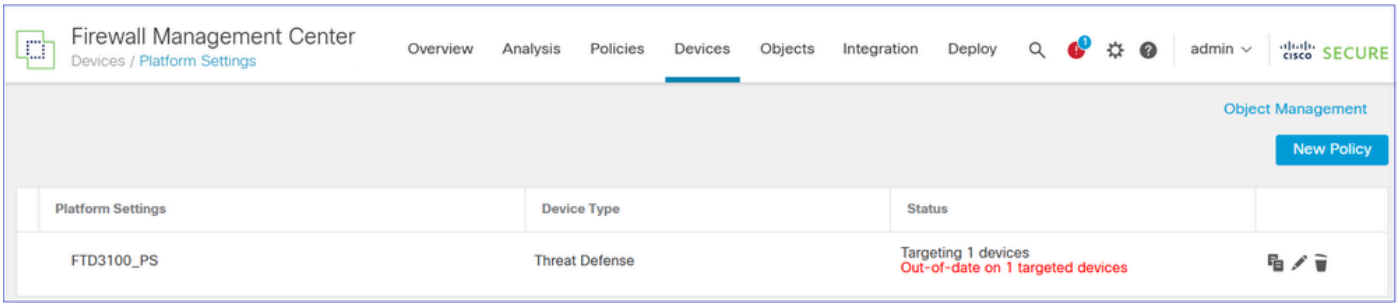
10단계. FTD 컨피그레이션을 완료합니다.

이 시점에서 FMC2(대상 FMC)에 등록하고 디바이스 정책을 가져온 후에도 FTD1에서 계속 누락될 수 있는 모든 기능을 구성하는 것이 목표입니다.

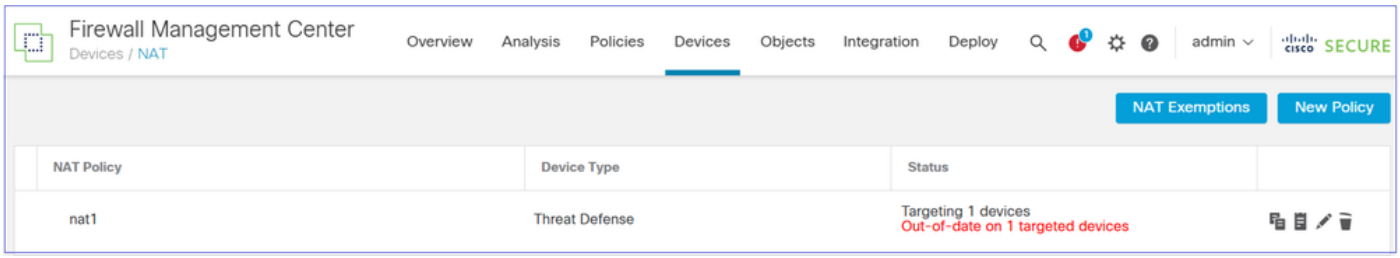
NAT, 플랫폼 설정, QoS 등의 정책이 적용되는지 확인합니다. FTD에 할당됩니다. 정책이 할당되었

지만 구축이 보류 중임을 알 수 있습니다.

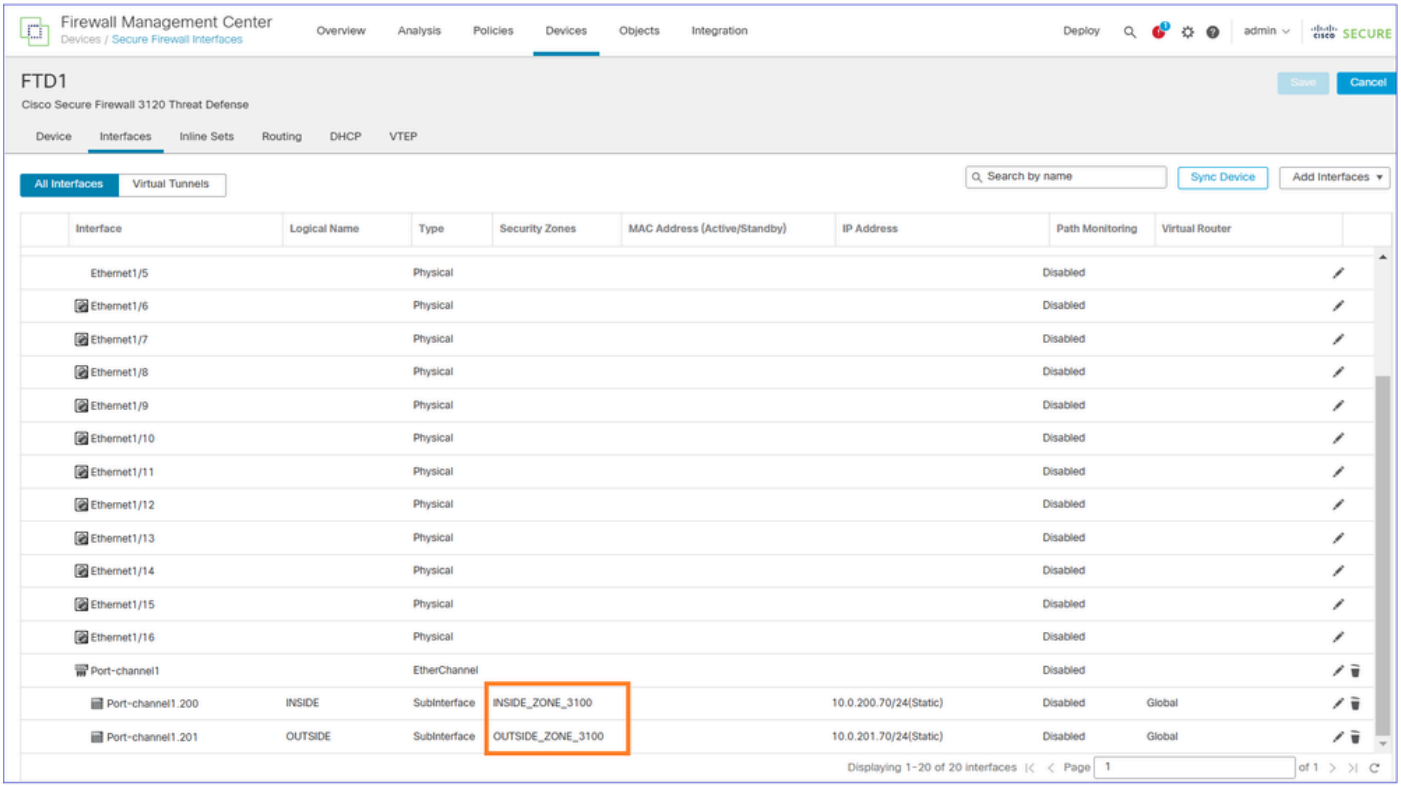
예를 들어, 플랫폼 설정을 가져와 디바이스에 할당하지만 구축을 보류 중입니다.



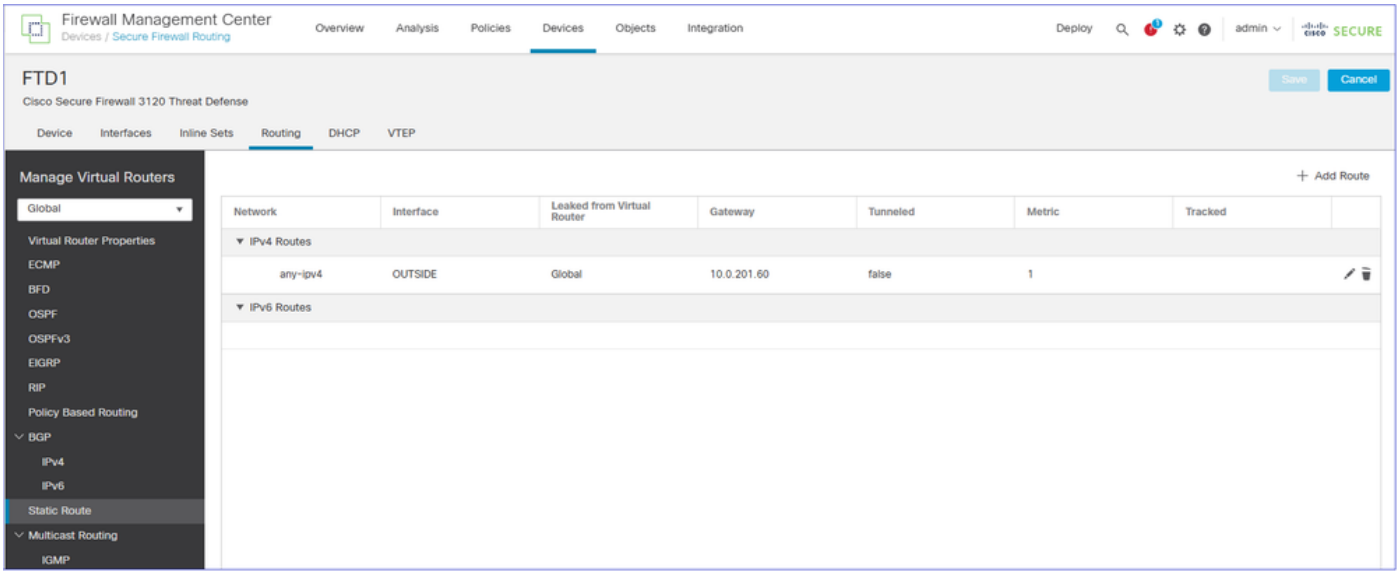
NAT가 구성된 경우 NAT 정책을 가져와 디바이스에 할당하지만, 구축을 보류 중입니다.



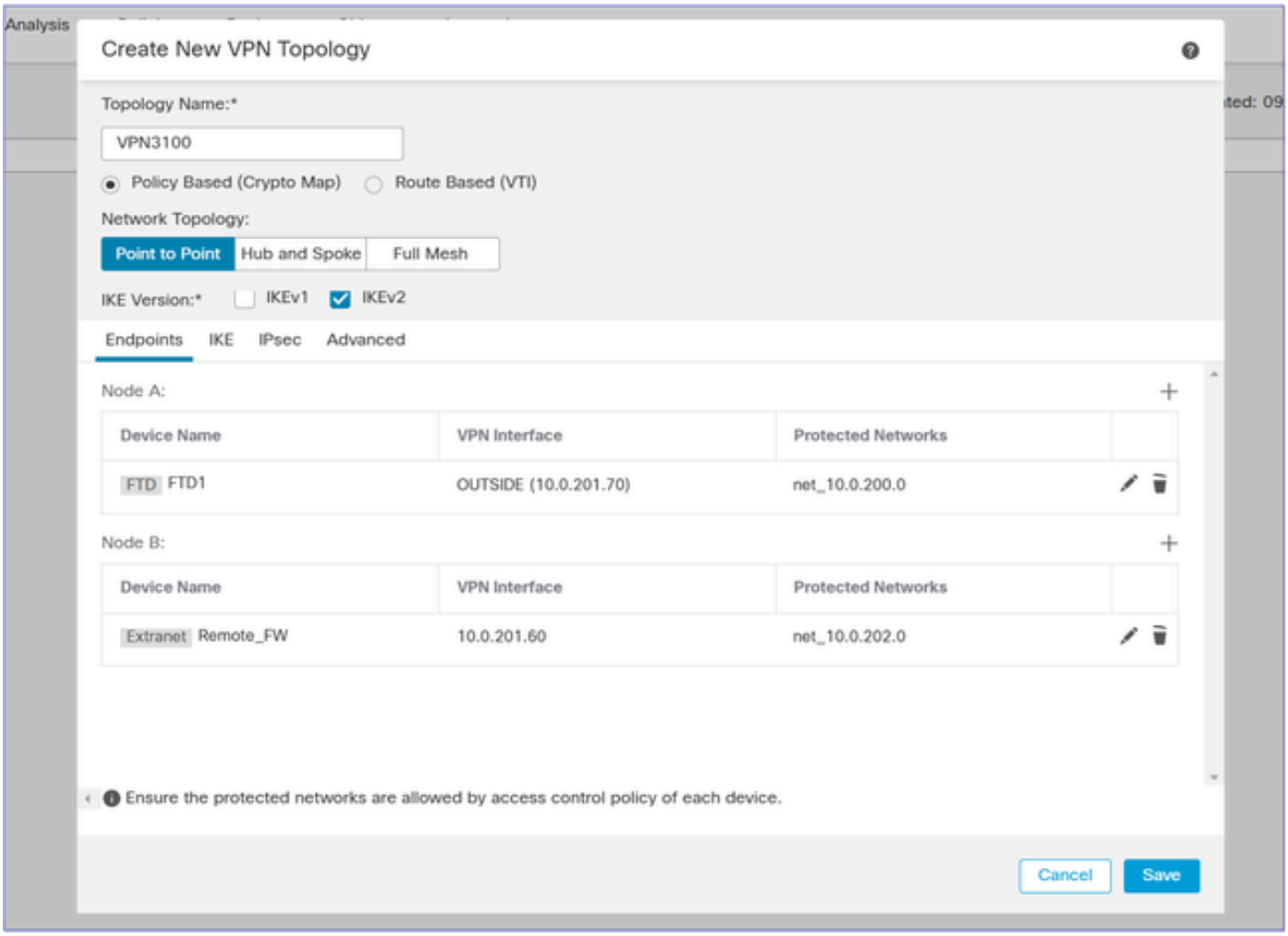
보안 영역은 인터페이스에 적용됩니다.



라우팅 컨피그레이션은 FTD 디바이스에 적용됩니다.

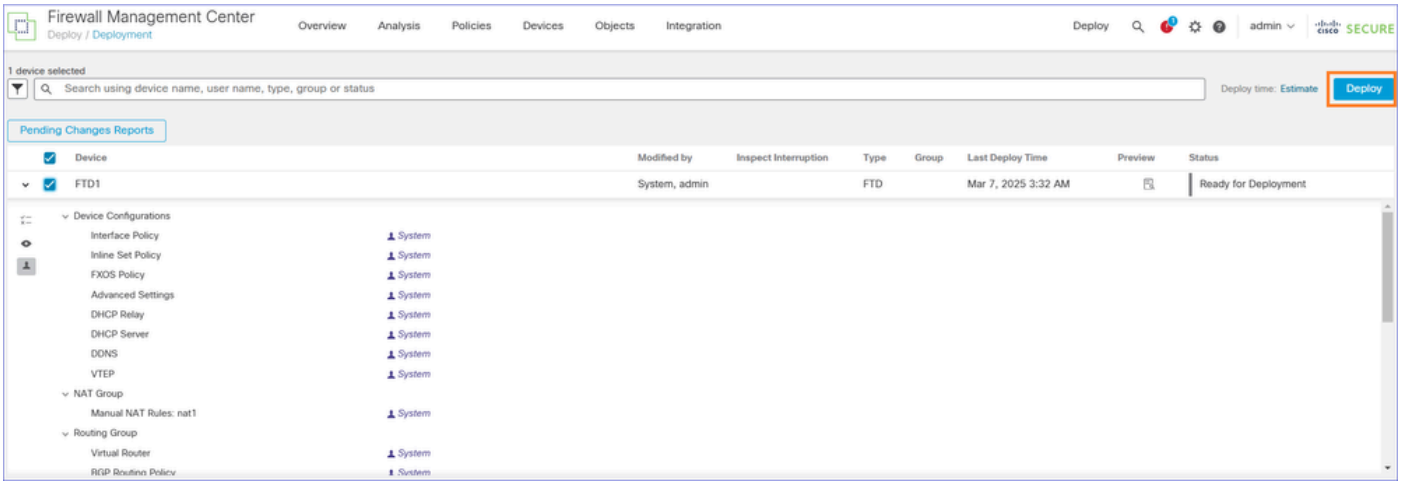


참고: 이제 자동으로 마이그레이션할 수 없는 정책(예: VPN)을 구성할 때입니다.



참고: 마이그레이션된 FTD에 대상 FMC로도 마이그레이션된 S2S VPN 피어가 있는 경우 모든 FTD를 대상 FMC로 이동한 후 VPN을 구성해야 합니다.

보류 중인 변경 내용을 배포합니다.



11단계. 배포된 FTD 구성 확인

이 단계에서 목표는 FTD CLI에서 모든 컨피그레이션이 제대로 되어 있는지 확인하는 것입니다.

두 FTD의 'show running-config' 출력을 비교하는 것이 좋습니다. WinMerge 또는 diff와 같은 도구를 사용하여 비교할 수 있습니다.

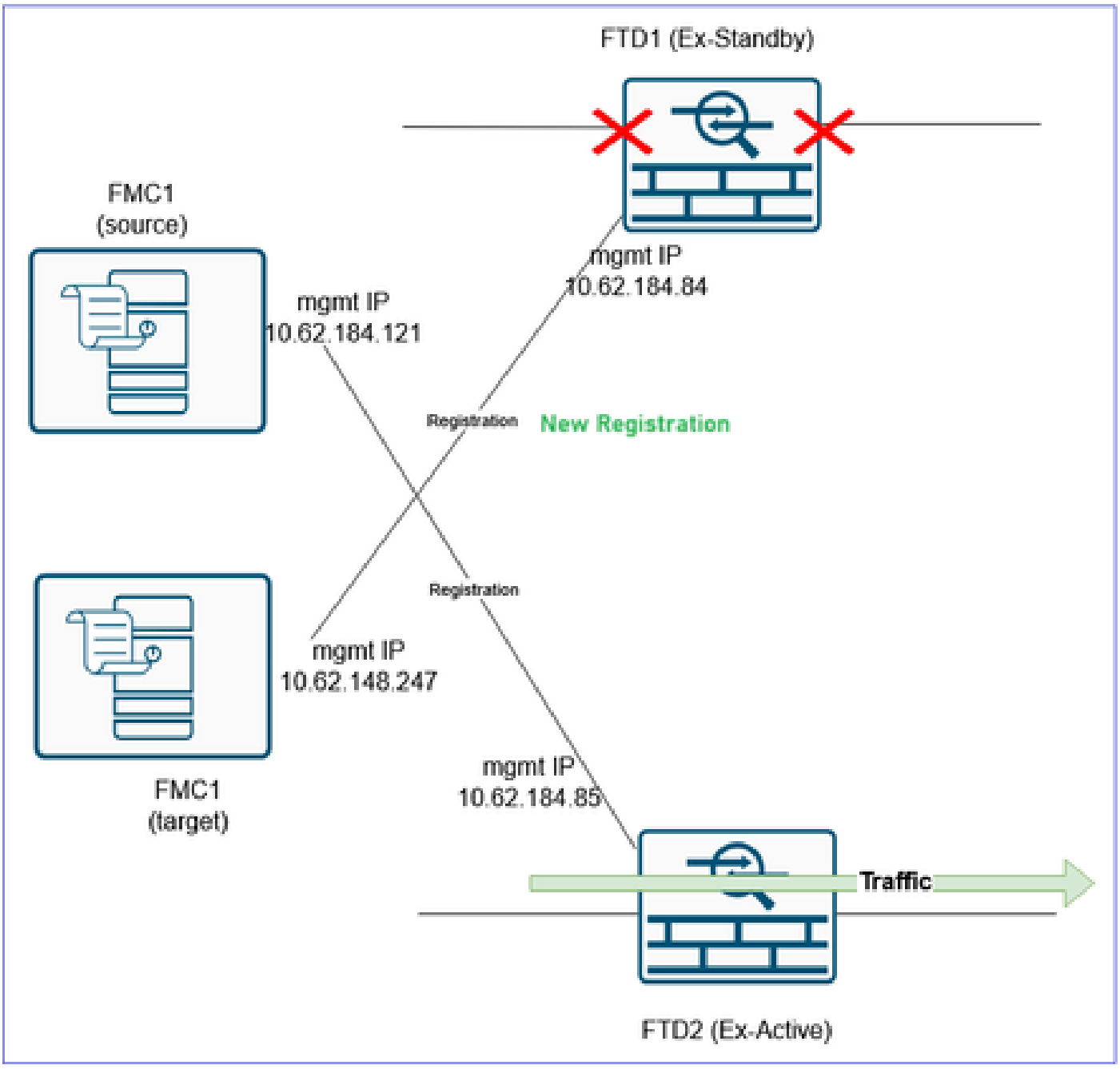
일반적으로 볼 수 있는 차이점은 다음과 같습니다.

- 장치 일련 번호
- 인터페이스 설명
- ACL 규칙 ID
- 컨피그레이션 크립토체크섬

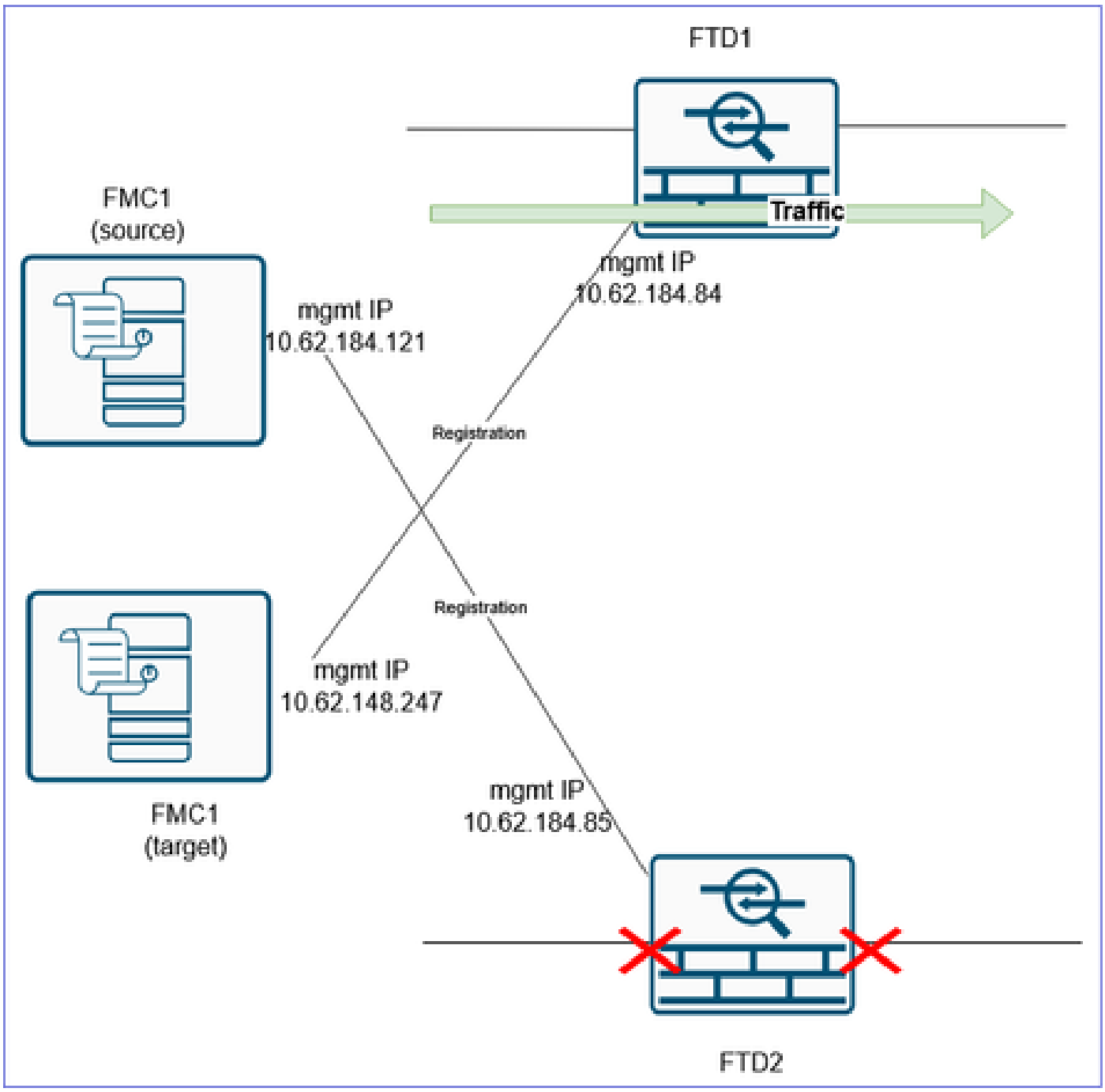
12단계. 컷오버 실행

이 단계에서 목표는 현재 트래픽을 처리하고 있지만 여전히 기존/소스 FMC에 등록된 FTD2에서 대상 FMC에 등록된 FTD1로 트래픽을 전환하는 것입니다.

공격 전:


FTD1 (Ex-Standby)
FMC1
(source)
mgmt IP
10.62.184.84
mgmt IP
10.62.184.121
Registration
New Registration
Registration
mgmt IP
10.62.148.247
FMC1
(target)
mgmt IP
10.62.184.85
Traffic
FTD2 (Ex-Active)

이후:



⚠ 주의: 컷오버를 할 수 있도록 MW를 준비합니다. 컷오버 과정에서 모든 트래픽이 FTD1로 전환되고 VPN이 다시 설정되는 등 여러 가지 상황이 발생할 수 있습니다.

⚠ 주의: ACP 컴파일이 완료될 때까지 컷오버를 시작하지 마십시오(위의 10단계 참조).

⚠ 경고: FTD2에서 데이터 케이블을 분리하거나 관련 스위치포트를 종료해야 합니다. 그렇지 않으면 두 디바이스 모두 트래픽을 처리할 수 있습니다!

⚠ 주의: 두 디바이스 모두 동일한 IP 컨피그레이션을 사용하므로 인접한 L3 디바이스의 ARP 캐시를 업데이트해야 합니다. 트래픽 컷오버를 신속하게 수행하려면 인접한 디바이스의 ARP 캐시를 수동으로 지우는 것이 좋습니다.

팁: GARP 패킷을 전송하고 FTD CLI 명령을 사용하여 인접 디바이스의 ARP 캐시를 업데이트할 수도 있습니다.

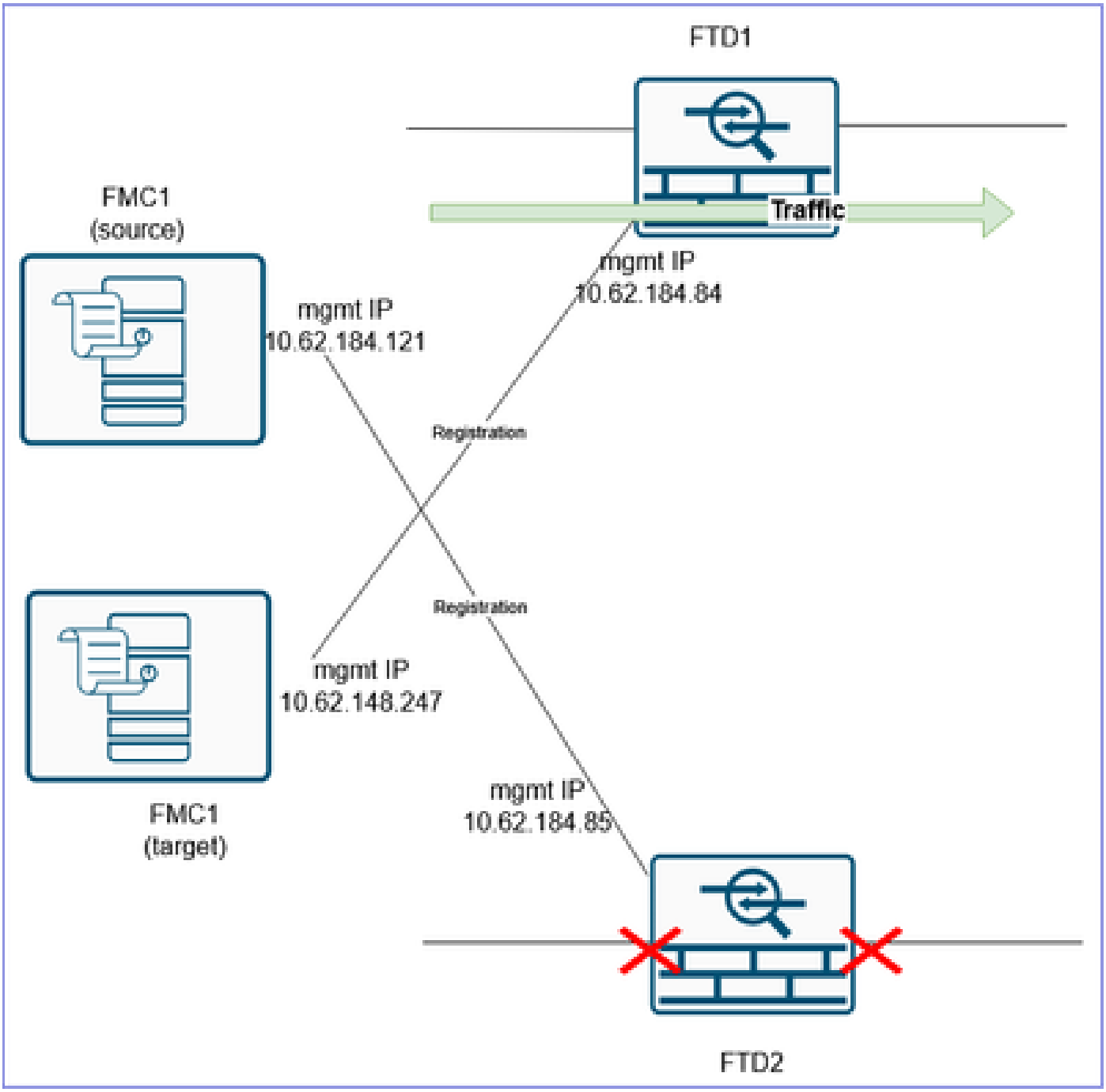
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

FW가 소유하는 모든 IP에 대해 이 명령을 반복해야 합니다. 따라서 방화벽이 보유한 모든 IP에 대해 GARP 패킷을 전송하는 것보다 인접 디바이스의 ARP 캐시만 지우는 것이 더 빠를 수 있습니다.

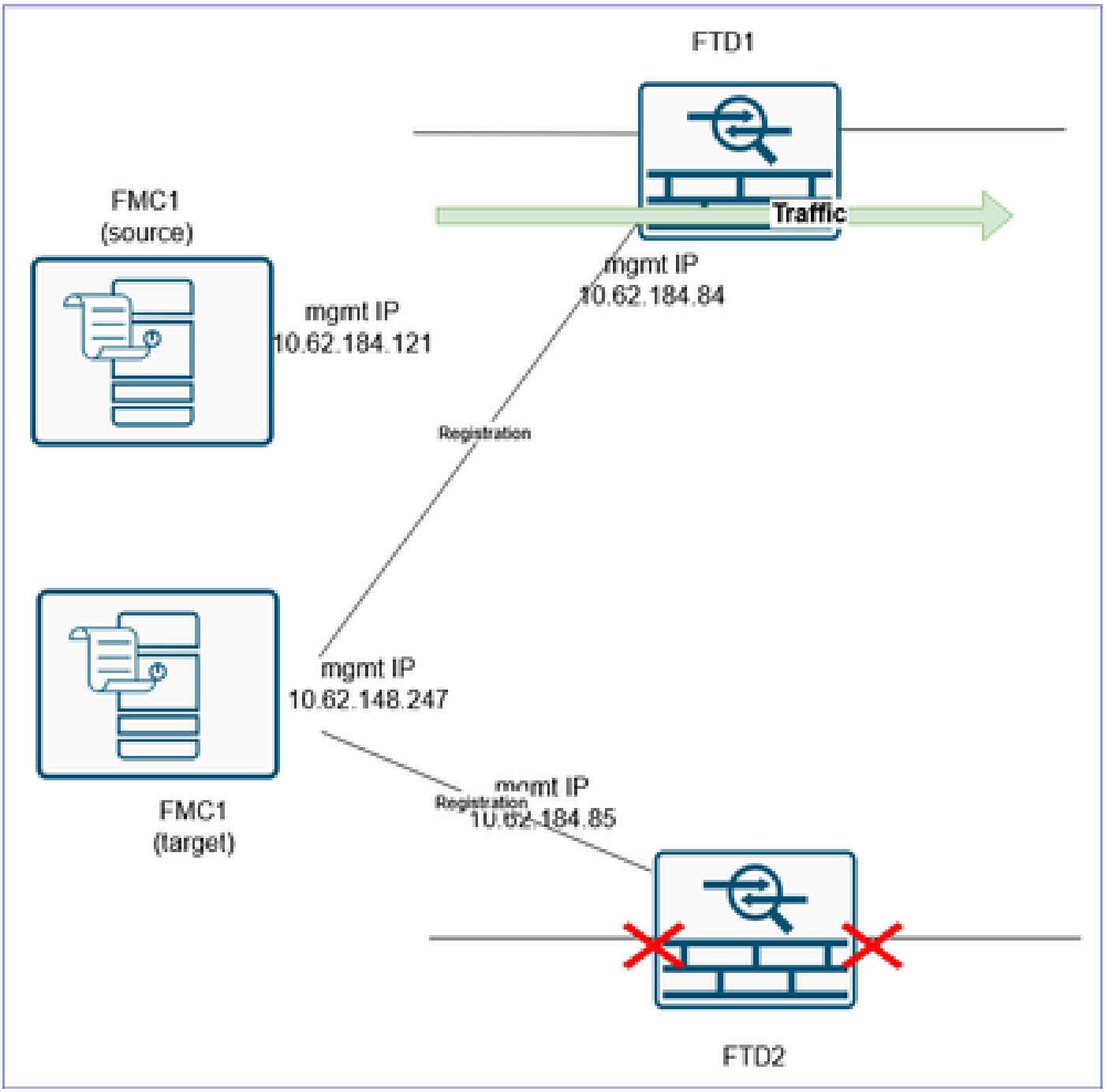
13단계. 두 번째 FTD를 FMC2(대상 FMC)로 마이그레이션

마지막 항목은 HA 쌍을 수정하는 것입니다. 이렇게 하려면 먼저 FMC1(소스 FMC)에서 FTD2를 삭제하고 이를 FMC2(대상 FMC)에 등록해야 합니다.

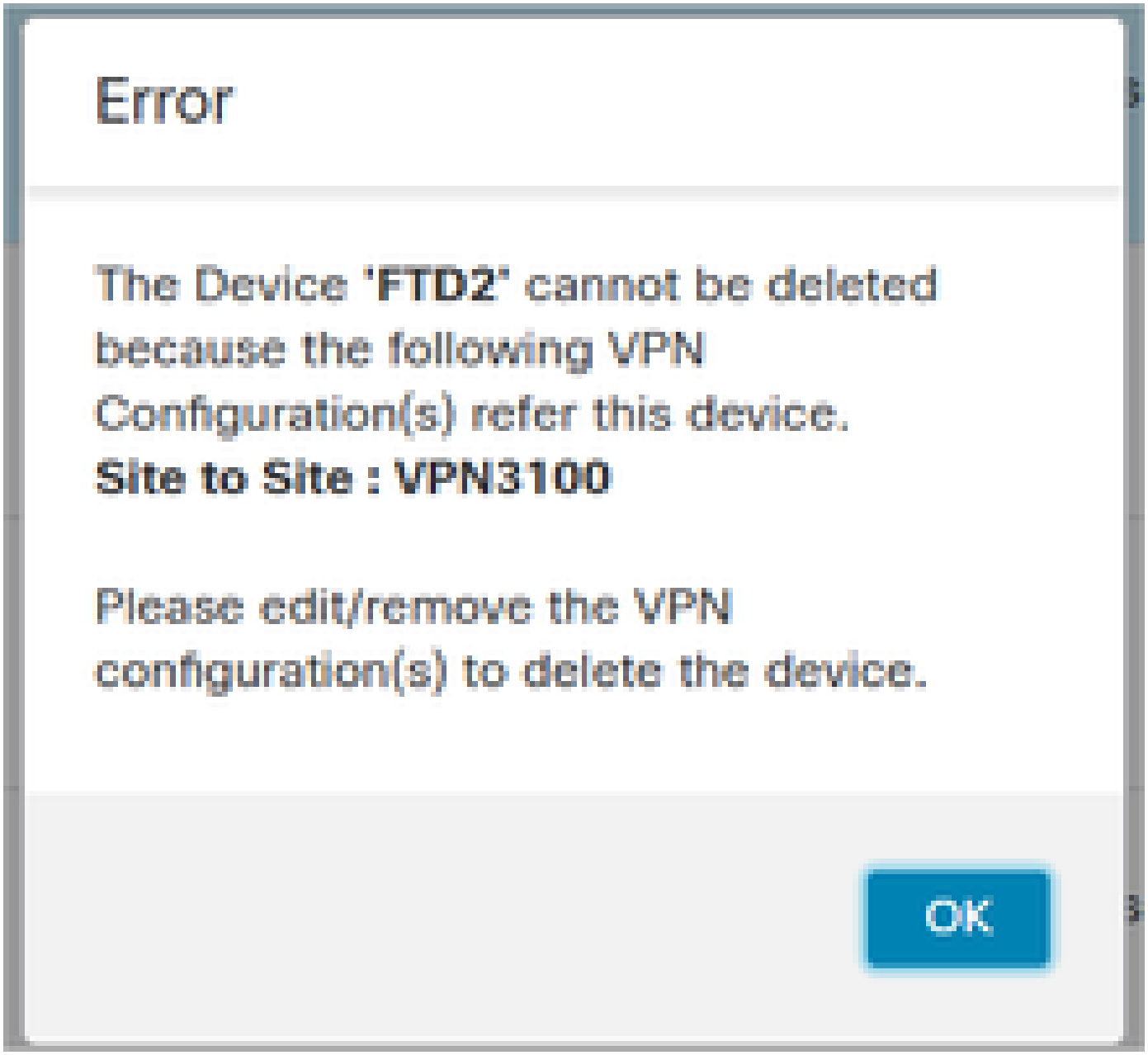
공격 전:


FTD1
FMC1
(source)
Traffic
mgmt IP
10.62.184.84
mgmt IP
10.62.184.121
Registration
Registration
mgmt IP
10.62.148.247
FMC1
(target)
mgmt IP
10.62.184.85
FTD2

이후:



FTD2에 연결된 VPN 컨피그레이션이 있는 경우 FTD를 삭제하기 전에 먼저 이를 제거해야 합니다. 이와 다른 경우 다음과 유사한 메시지가 표시됩니다.



CLI 확인:

```
<#root>

>

show managers


No managers configured.
```

FTD 컨피그레이션을 대상 FMC에 등록하기 전에 모두 삭제하는 것이 좋습니다. 이를 위해 방화벽 모드 간에 전환하는 것이 빠릅니다.

예를 들어 라우팅 모드가 있는 경우 투명 모드로 전환한 다음 다시 라우팅 모드로 전환합니다.

<#root>

>

configure firewall transparent

그리고

<#root>

>

configure firewall routed

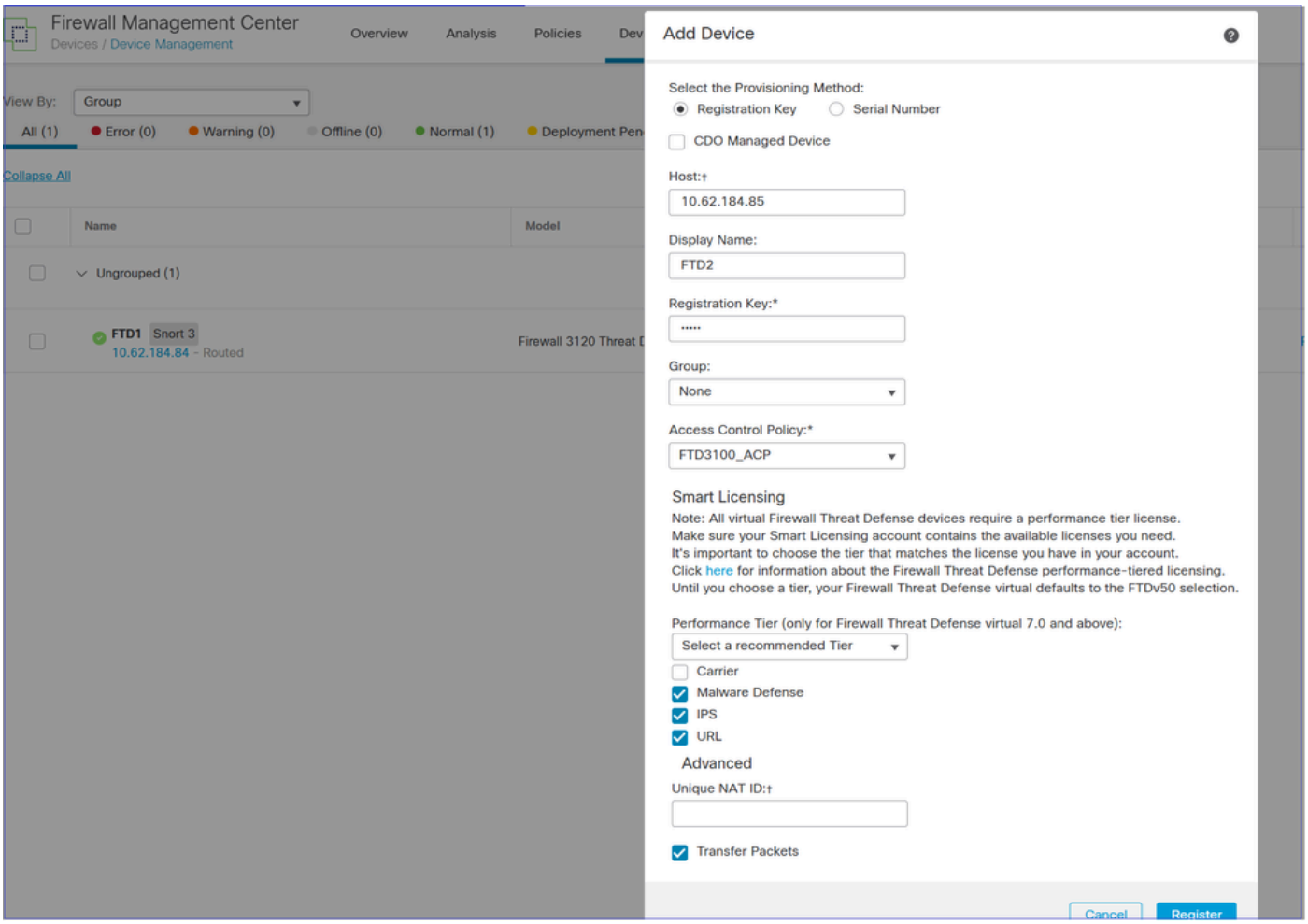
그런 다음 FMC2(대상 FMC)에 등록합니다.

<#root>

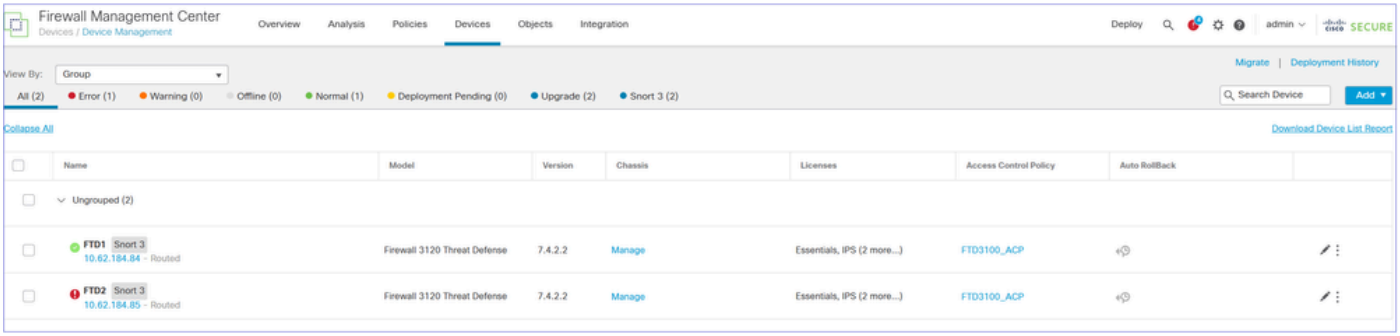
>

configure manager add 10.62.148.247 cisco

```
Manager 10.62.148.247 successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```



결과:

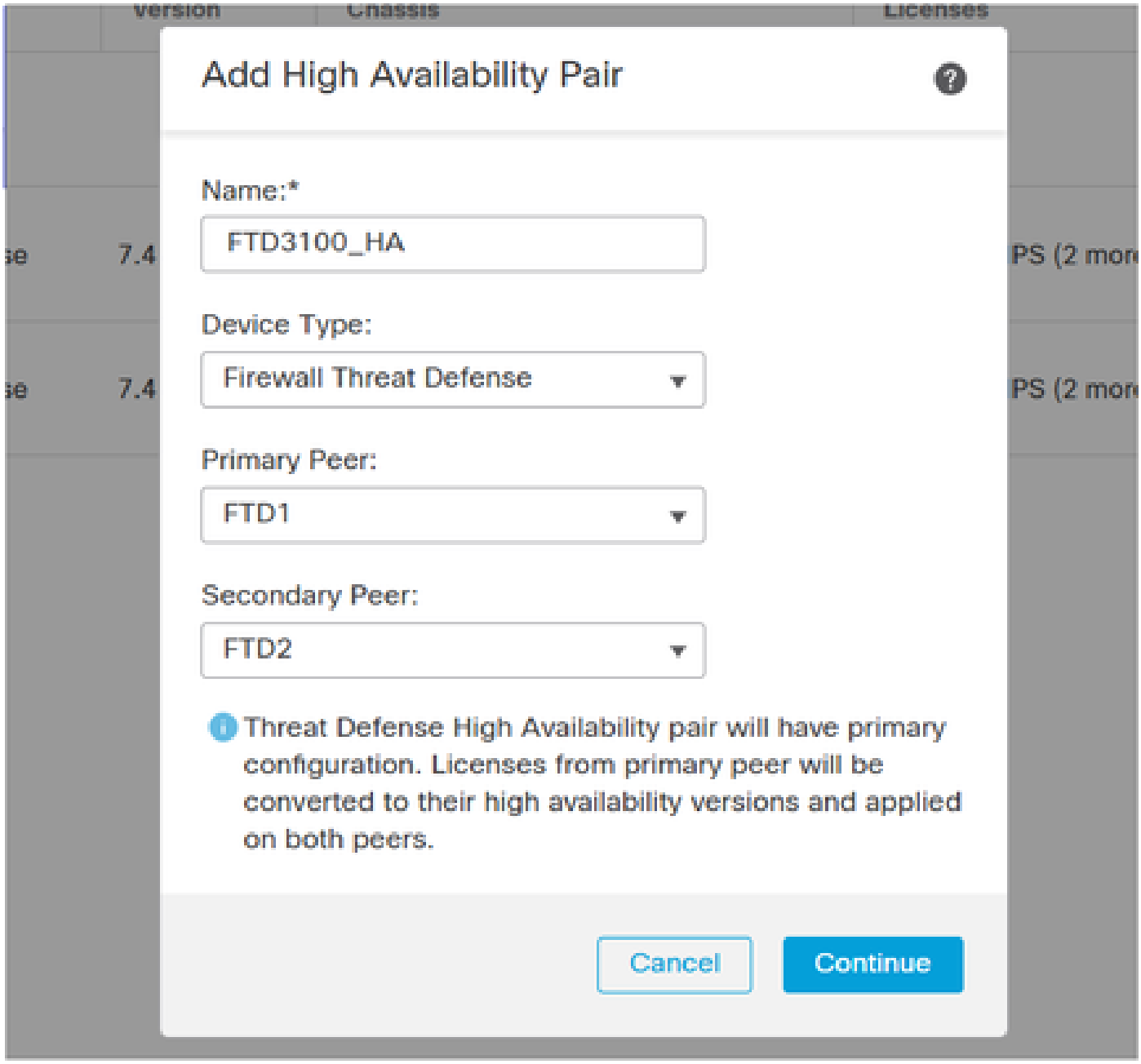


14단계. FTD HA 다시 구성

참고: 이 작업(HA 관련 작업)도 MW 중에 수행해야 합니다. HA 협상 중에 데이터 인터페이스가 다운된 후 1분 동안 트래픽 중단이 발생합니다.

대상 FMC에서 Devices(디바이스) > Device Management(디바이스 관리) 및 Add(추가) > High Availability(고가용성)로 이동합니다.

⚠ 주의: 트래픽을 처리하는 FTD(이 시나리오에서는 FTD1)를 기본 피어로 선택해야 합니다.



모니터링되는 인터페이스, 대기 IP, 가상 MAC 주소 등을 포함한 HA 설정을 재구성합니다.

FTD1 CLI에서 확인:

```
<#root>

FTD3100-3#

show failover | include host

        This host: Primary - Active
        Other host: Secondary - Standby Ready
```

FTD2 CLI에서 확인:

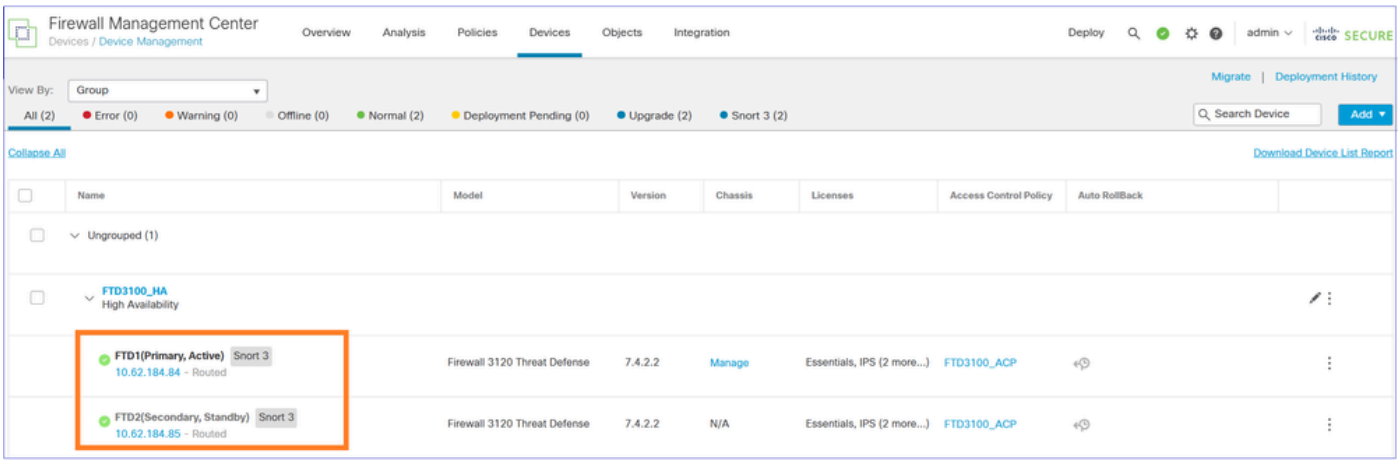
<#root>

FTD3100-3#

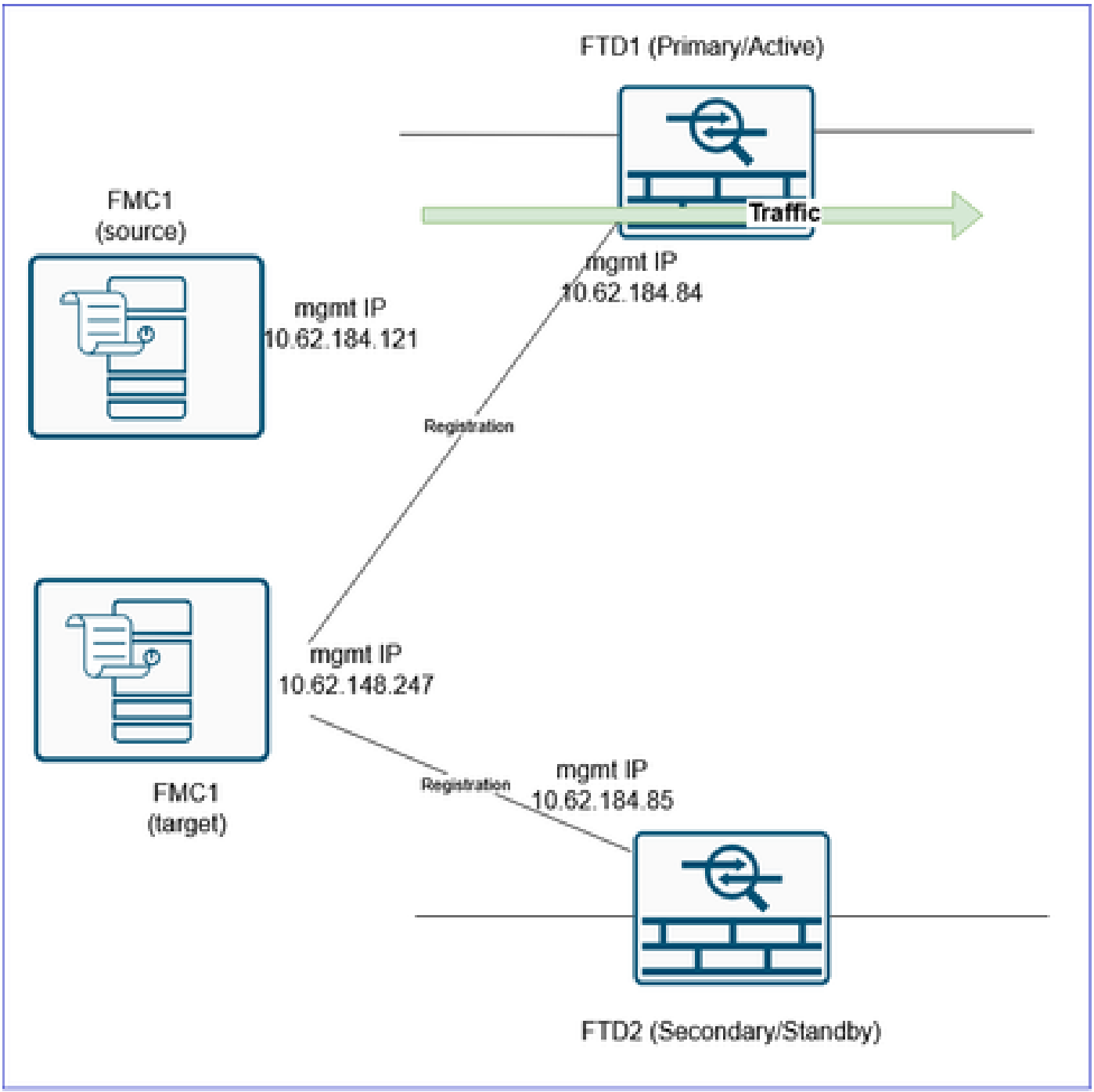
show failover | include host

```
        This host: Secondary - Standby Ready
        Other host: Primary - Active
```

FMC UI 확인:



마지막으로, FTD2 디바이스의 데이터 인터페이스를 다시 시작합니다.



참조

- 디바이스 컨피그레이션 내보내기 및 가져오기
- 고가용성 쌍 추가
- 한 FMC에서 다른 FMC로 FTD 마이그레이션

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.