# CD-FMC에서 관리하는 Azure FTD에서 중복 데이터 인터페이스 배포

## 목차

## 소개

이 문서에서는 이중화 관리자 액세스 데이터 인터페이스 기능을 사용하도록 cdFMC 관리 가상 FTD를 구성하는 단계에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Firewall 관리 센터
- Cisco Defense Orchestrator

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 클라우드 기반 방화벽 관리 센터
- Azure 클라우드에서 호스팅되는 Virtual Secure Firewall Threat Defense 버전 7.3.1입니다.

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.

### 관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- firepower Threat Defense 버전 7.3.0 이상을 실행할 수 있는 모든 물리적 어플라이언스

## 배경 정보

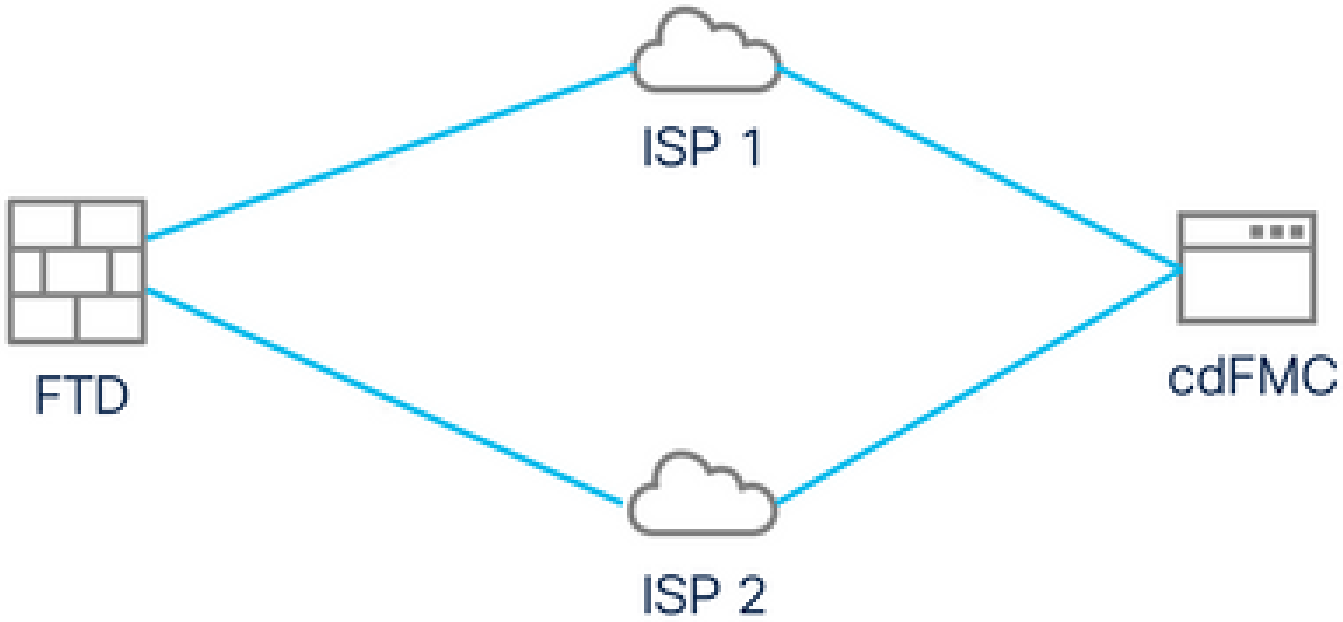
이 문서에서는 관리 목적으로 두 개의 데이터 인터페이스를 사용하도록 cdFMC 관리 vFTD를 구성하고 확인하는 단계를 보여줍니다. 이 기능은 고객이 제2 ISP를 사용하여 인터넷을 통해 FTD를 관

리하기 위해 제2 데이터 인터페이스가 필요한 경우에 유용합니다. 기본적으로 FTD는 두 인터페이스 간의 관리 트래픽에 대해 라운드 로빈 로드 밸런싱을 수행합니다. 이 문서에 설명된 대로 액티브/백업 구축으로 수정할 수 있습니다.

Secure Firewall Threat Defense 버전 7.3.0에는 관리용 이중 데이터 인터페이스 기능이 도입되었습니다. vFTD가 CDO 액세스를 위한 URL을 확인할 수 있는 이름 서버에 연결할 수 있다고 가정합니다.

# 설정

## 네트워크 다이어그램




네트워크 다이어그램

## 관리 액세스를 위한 데이터 인터페이스 구성

콘솔을 통해 디바이스에 로그인하고 configure network management-data-interface 명령을 사용하여 관리 액세스를 위한 데이터 인터페이스 중 하나를 구성합니다.

```
<#root>

>

configure network management-data-interface


Note: The Management default route will be changed to route through the data interfaces. If you are conn
interface with SSH, your connection may drop. You must reconnect using the console port.

Data interface to use for management:

GigabitEthernet0/0
```

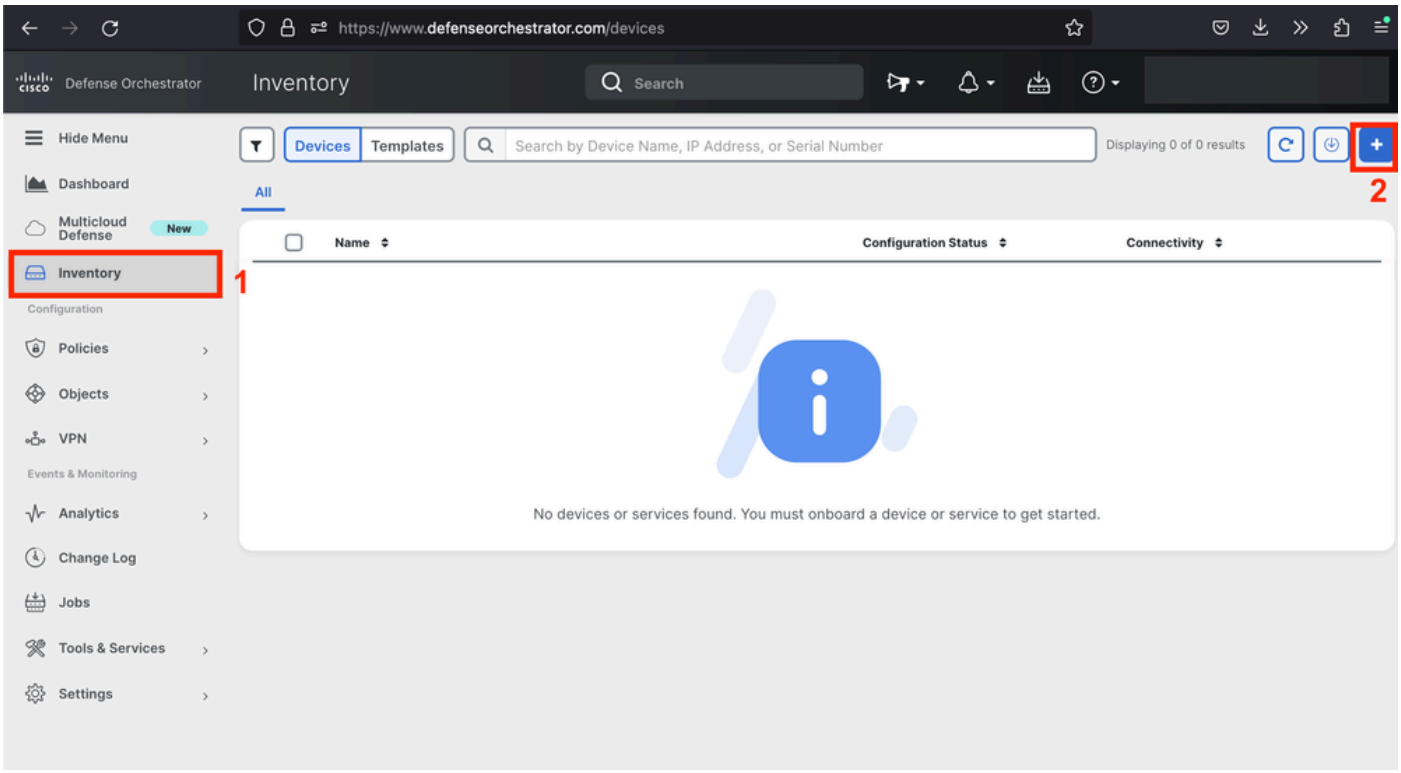
```
Specify a name for the interface [outside]:

outside-1

IP address (manual / dhcp) [dhcp]:

manual

IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

 255.255.255.0

Default Gateway:

10.6.2.1
```

원래 관리 인터페이스는 DHCP를 사용하도록 구성할 수 없습니다. show network 명령을 사용하여 이를 확인할 수 있습니다.

## CDO로 FTD 온보딩

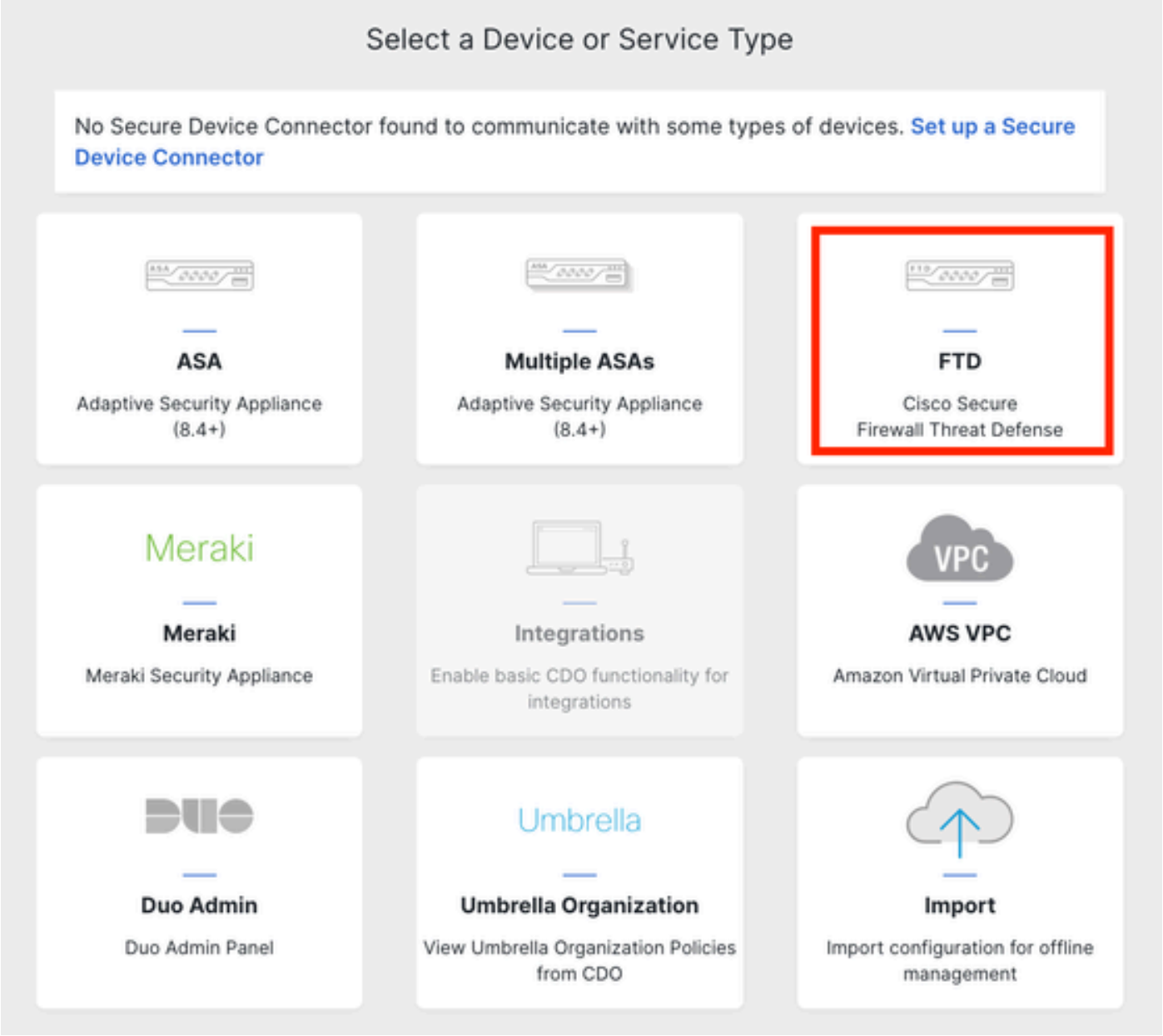
이 프로세스는 클라우드 제공 FMC에서 관리할 수 있도록 Azure FTD와 CDO를 온보딩합니다. 이 프로세스에서는 CLI 등록 키를 사용합니다. 이는 디바이스에 DHCP를 통해 할당된 IP 주소가 있는 경우에 유용합니다. 로그 터치 프로비저닝 및 일련 번호와 같은 다른 온보딩 방법은 Firepower 1000, Firepower 2100 또는 Secure Firewall 3100 플랫폼에서만 지원됩니다.

1단계. CDO 포털에서 Inventory(인벤토리)로 이동한 다음 Onboard(온보드) 옵션을 클릭합니다.



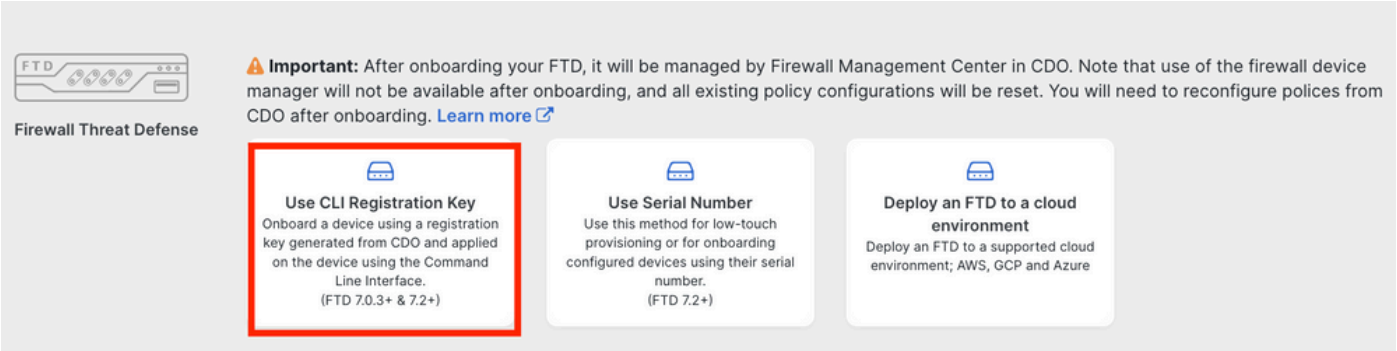

인벤토리 페이지

2단계. FTD 타일을 클릭합니다.



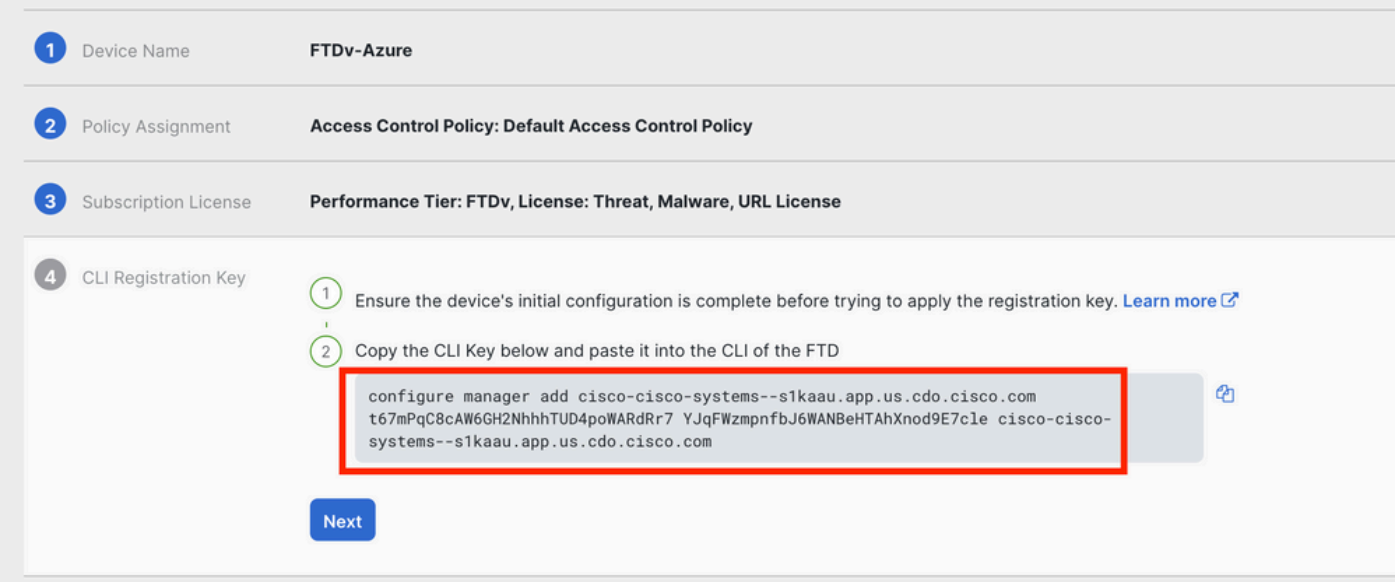

FTD 온보딩

3단계. Use CLI Registration key(CLI 등록 키 사용) 옵션을 선택합니다.

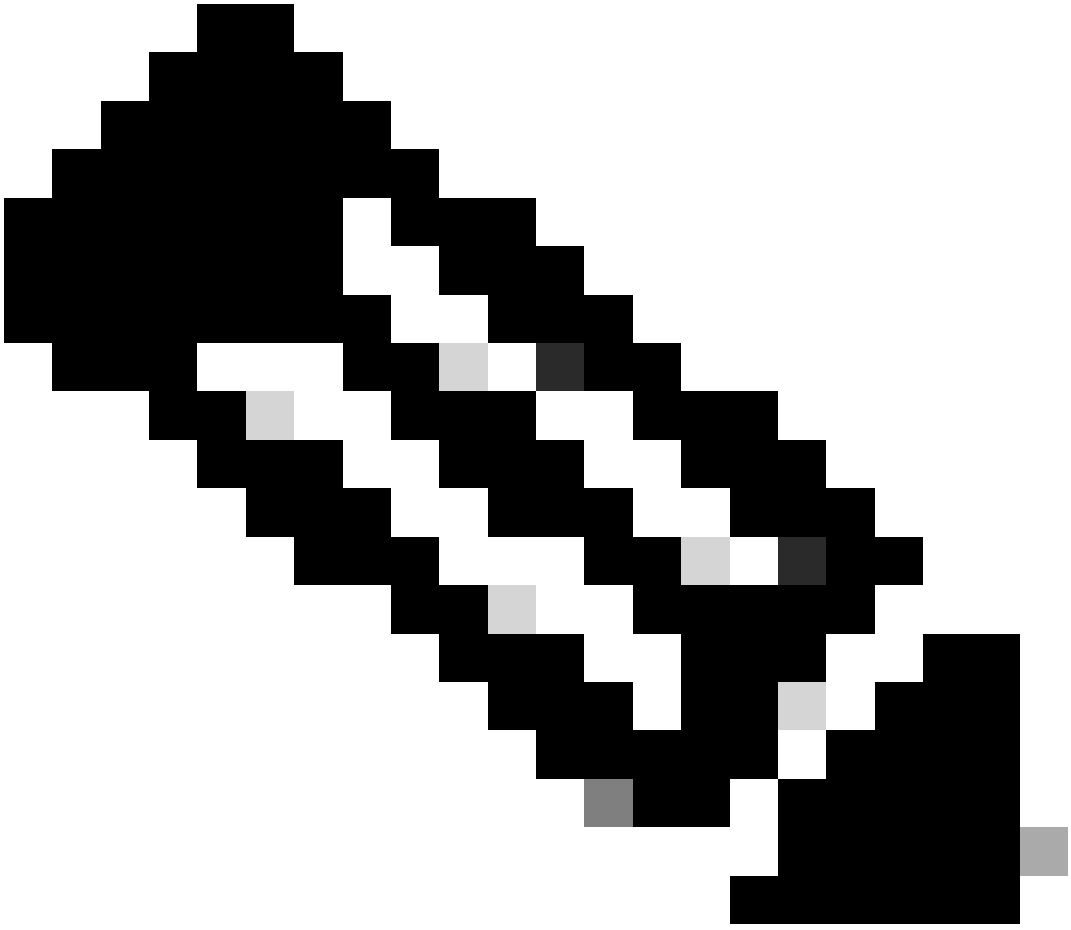



CLI 등록 키 사용

4단계. configure manager 명령에서 시작하여 CLI 키를 복사합니다.




구성 관리자 명령 복사



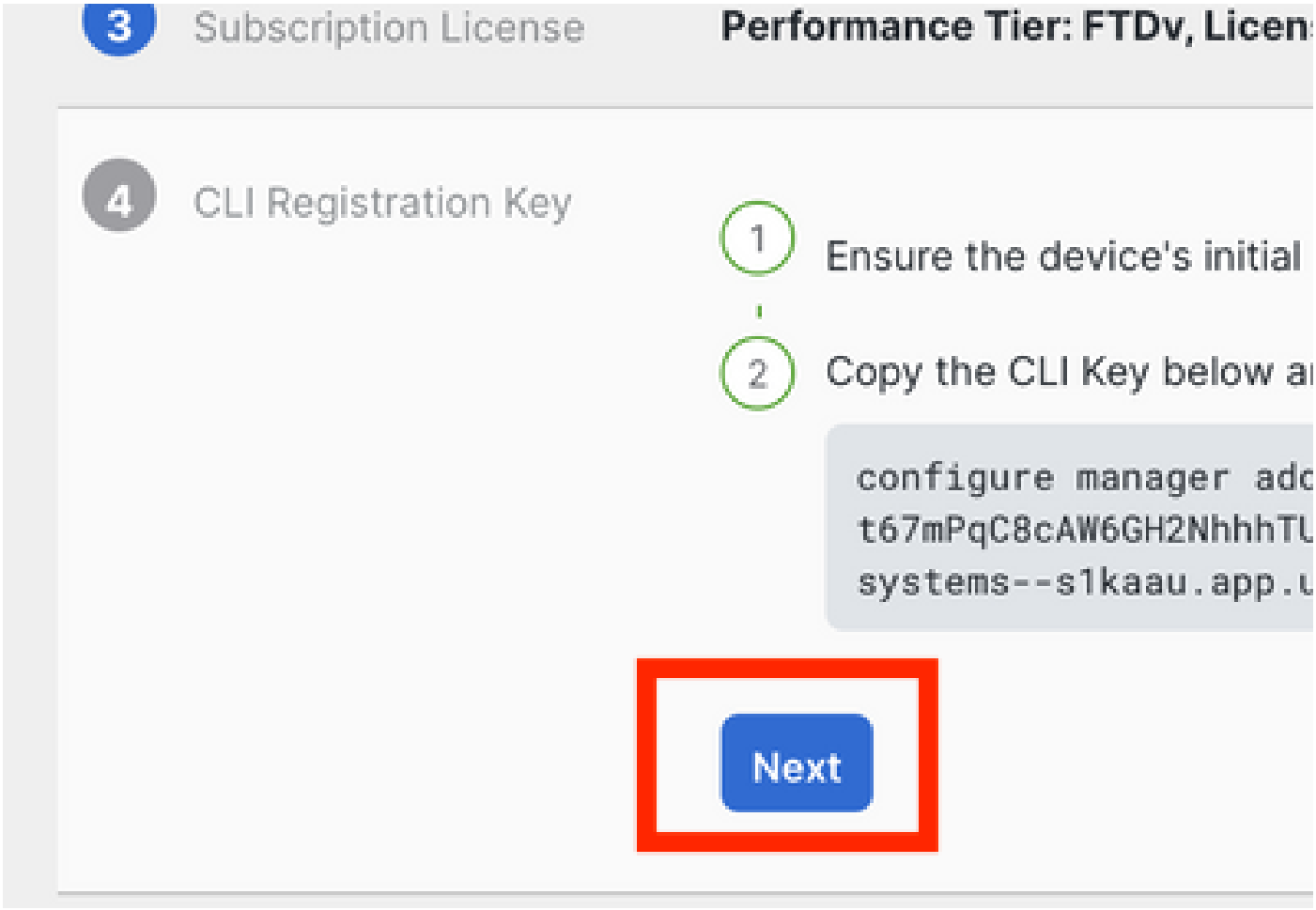
참고: CLI 키는 관리되는 디바이스가 NAT 디바이스 뒤에 있을 때 등록을 허용하도록 NAT-

ID를 구성할 수 있는 온프레미스 FMC를 사용하여 FTD를 등록하는 데 사용되는 형식과 일치합니다. configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>

5단계. FTD CLI에 명령을 붙여넣습니다. 다음 메시지가 성공적으로 전달된 경우 이 메시지를 수신해야 합니다.

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

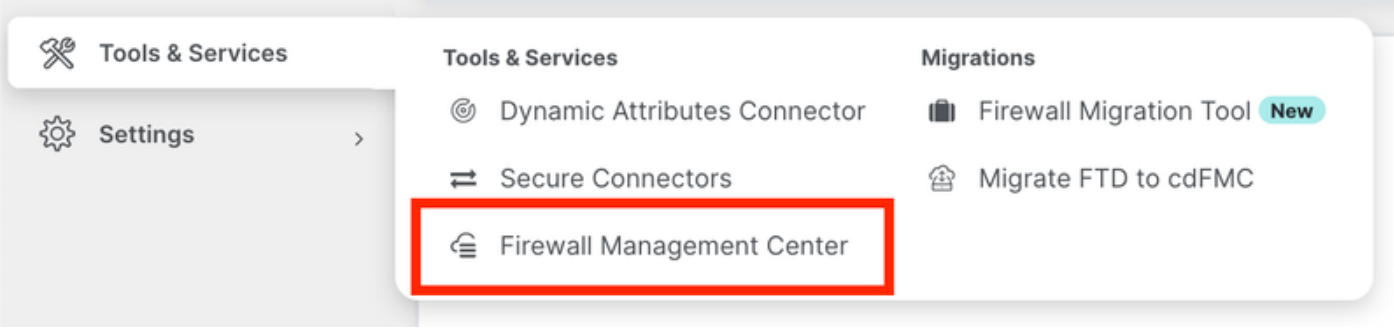
6단계. CDO로 돌아가 Next(다음)를 클릭합니다.




Next(다음)를 클릭합니다.

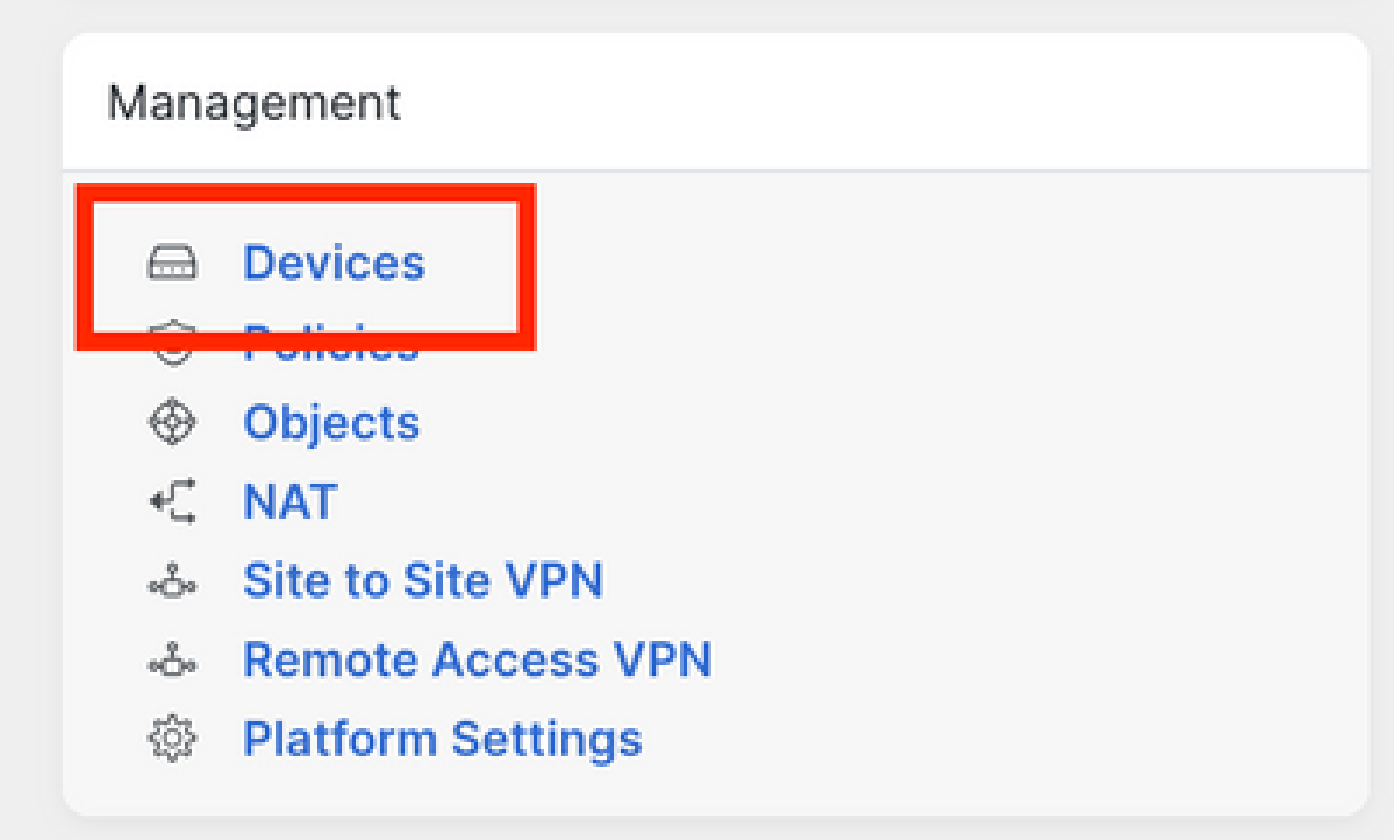
CDO는 등록 프로세스를 계속하며 완료하는 데 시간이 오래 걸린다는 메시지가 표시됩니다. Services(서비스) 페이지에서 Devices(디바이스) 링크를 클릭하여 등록 프로세스의 상태를 확인할 수 있습니다.

7단계. Tools & Services(툴 및 서비스) 페이지를 통해 FMC에 액세스합니다.



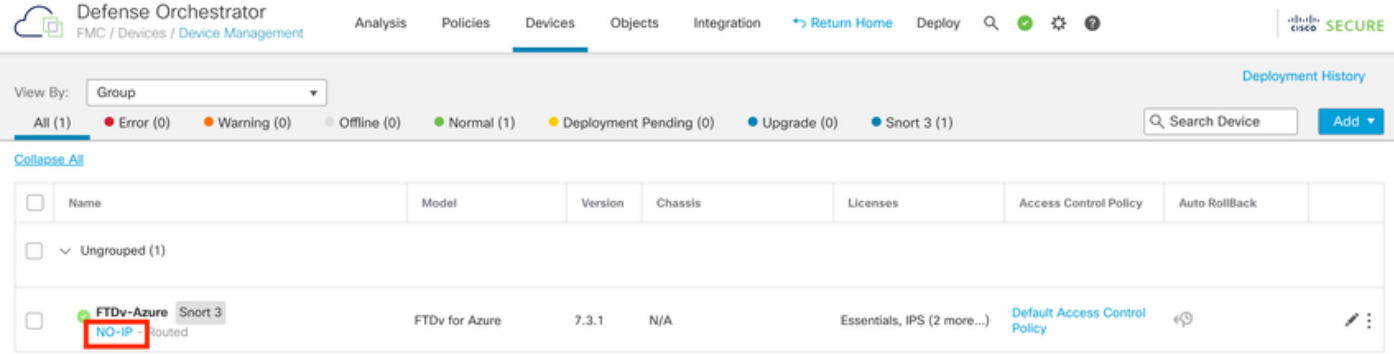

cdFMC 액세스

Devices(디바이스) 링크를 클릭합니다.




Devices를 클릭합니다.

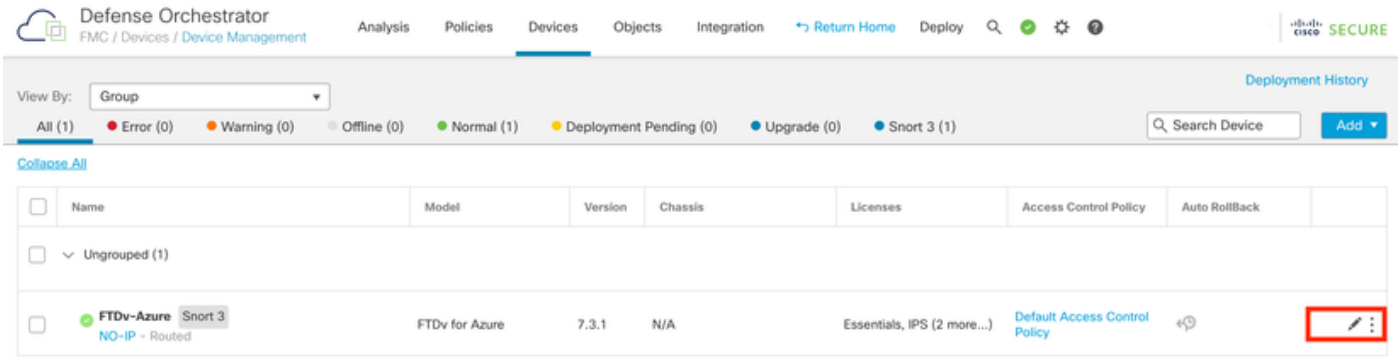
이제 FTD가 CDO에 온보딩되며 클라우드 제공 FMC에서 관리할 수 있습니다. 다음 그림에서는 디바이스 이름 아래에 NO-IP가 나열되어 있습니다. 이는 CLI 등록 키를 사용하는 온보딩 프로세스에서 필요합니다.



# 관리자 액세스를 위한 이중화 데이터 인터페이스 구성

이 프로세스에서는 관리 액세스를 위해 두 번째 데이터 인터페이스를 할당합니다.

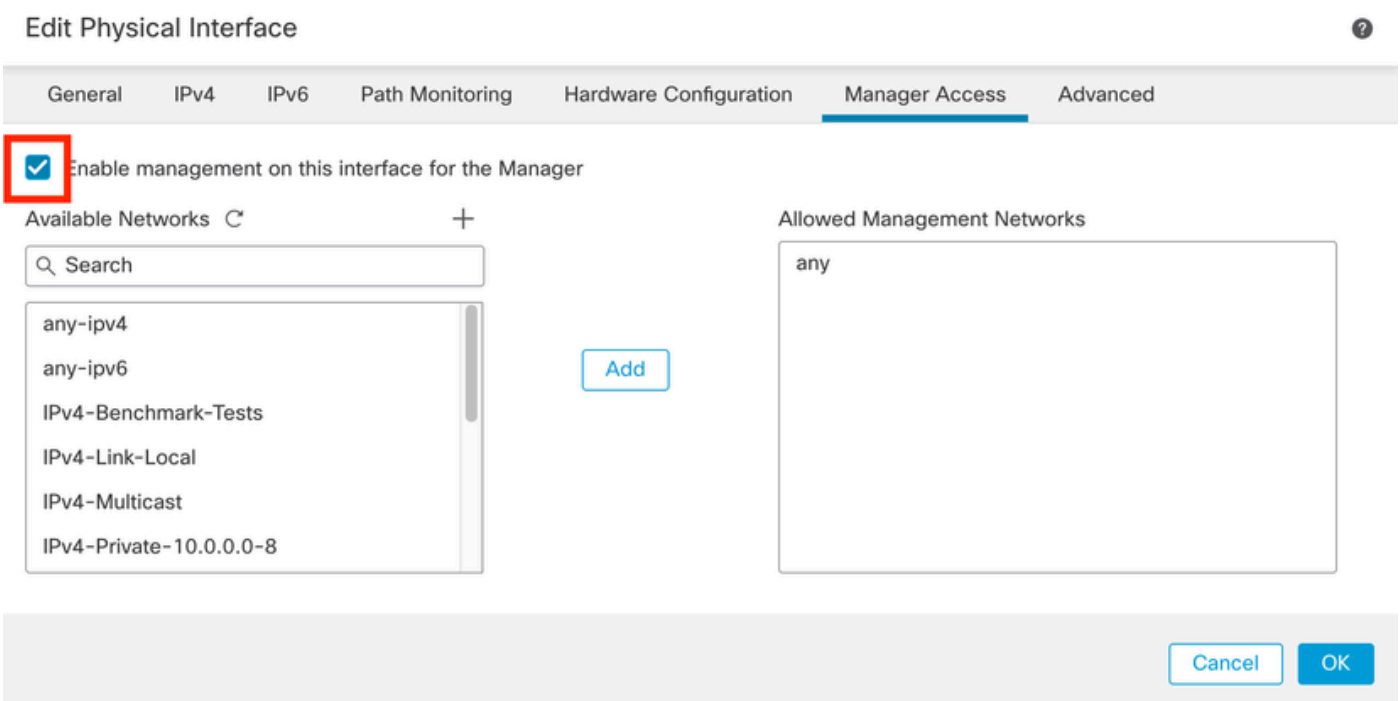
1단계. Devices(디바이스) 탭에서 연필 아이콘을 클릭하여 FTD 편집 모드에 액세스합니다.




FTD 편집

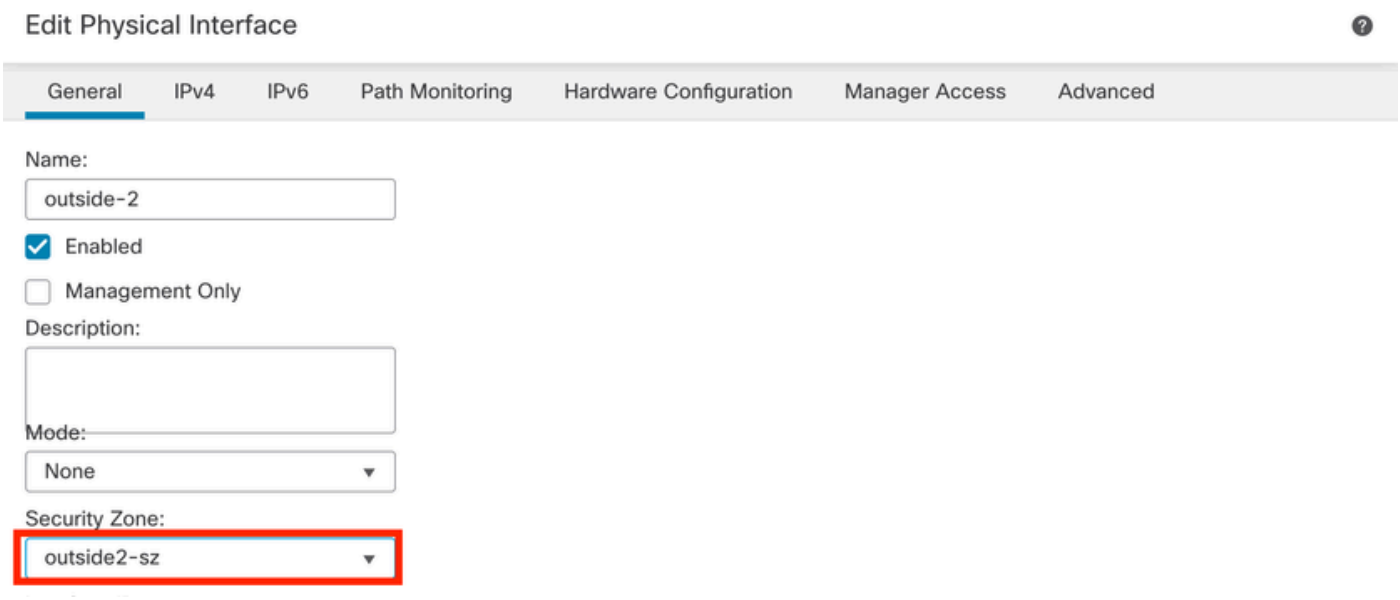
2단계. Interface 탭에서 이중화 관리 인터페이스로 할당할 인터페이스를 편집합니다. 이전에 구성하지 않은 경우 인터페이스 이름 및 IP 주소를 구성합니다.

3단계. Manager Access(관리자 액세스) 탭에서 Enable management on this interface for the manager(이 인터페이스에서 관리자 사용) 확인란을 활성화합니다.



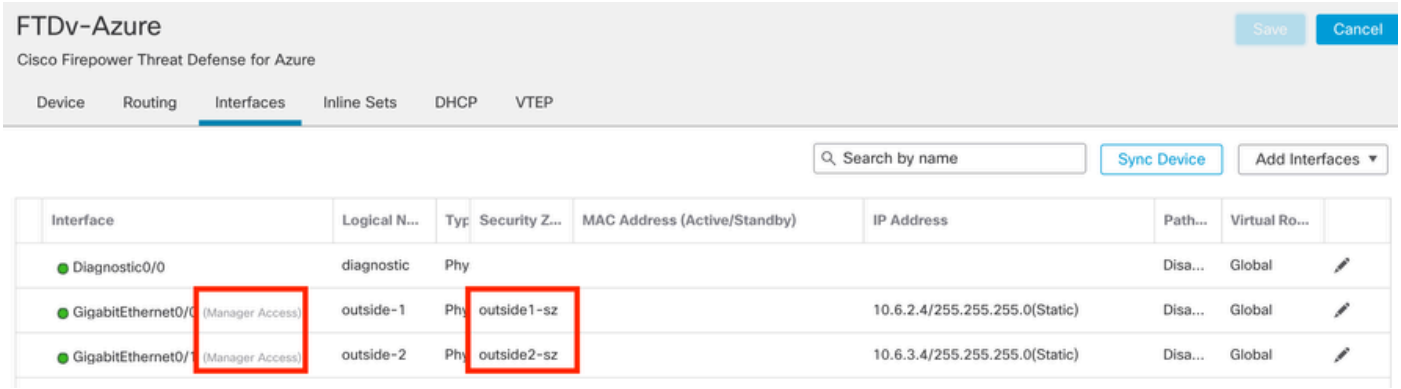

관리자 액세스 활성화

4단계. General(일반) 탭에서 인터페이스가 보안 영역에 할당되었는지 확인하고 OK(확인)를 클릭합니다.




이중화 데이터 인터페이스를 위한 보안 영역

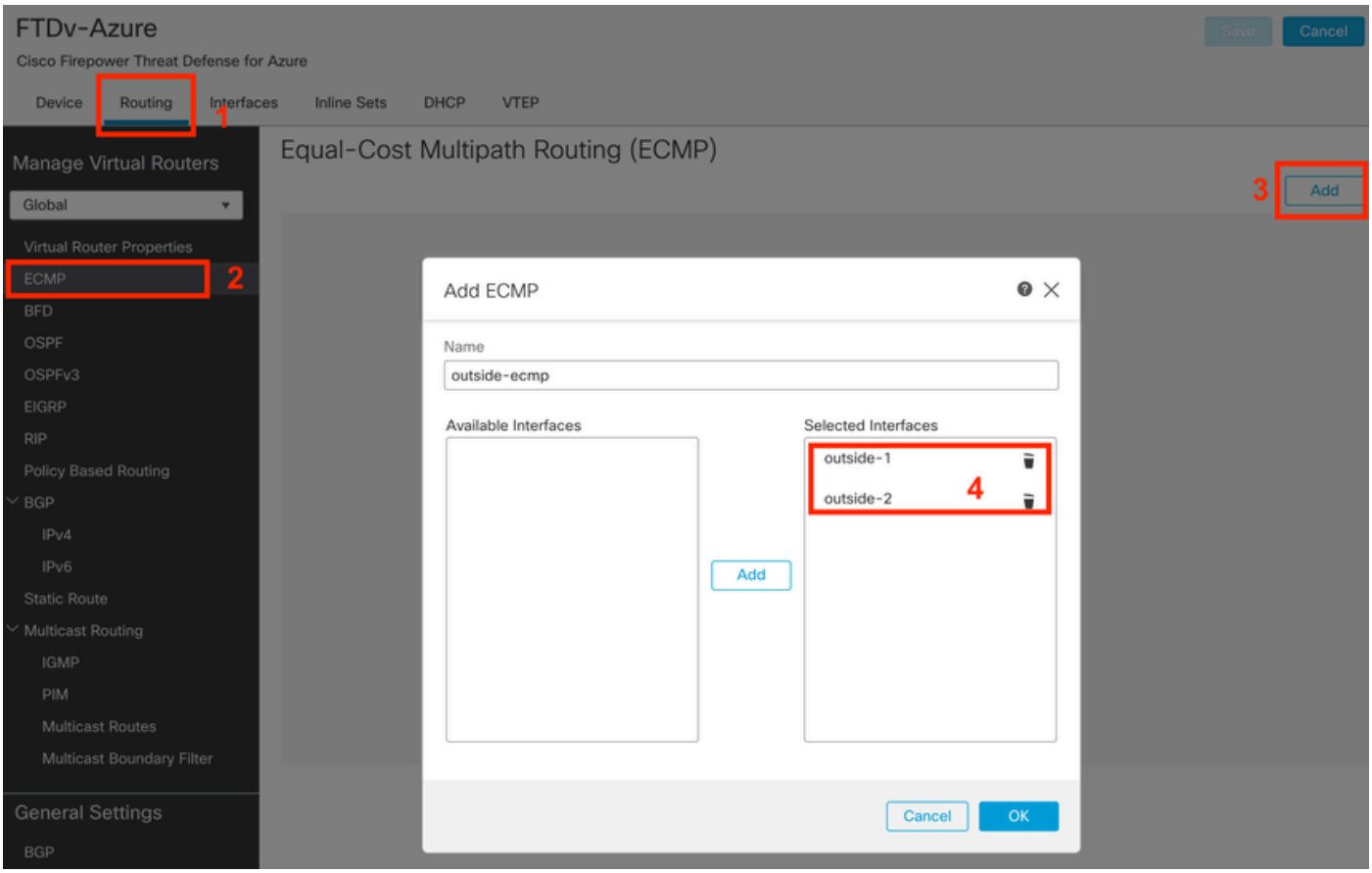
5단계. 이제 두 인터페이스에 모두 Manager Access 태그가 있습니다. 또한 기본 데이터 인터페이스가 다른 보안 영역에 할당되었는지 확인합니다.




인터페이스 컨피그레이션 검토

다음 섹션에서는 CDO에 도달하기 위해 2개의 동일 비용 기본 경로를 구성하는 것을 의미하며, 각 경로는 독립적인 SLA 추적 프로세스에 의해 모니터링됩니다. SLA 추적은 모니터링되는 인터페이스를 사용하여 cdFMC와 통신할 수 있는 기능 경로가 있는지 확인합니다.

6단계. Routing(라우팅) 탭으로 이동하고 ECMP 메뉴에서 두 인터페이스가 모두 포함된 새 ECMP 영역을 생성합니다.

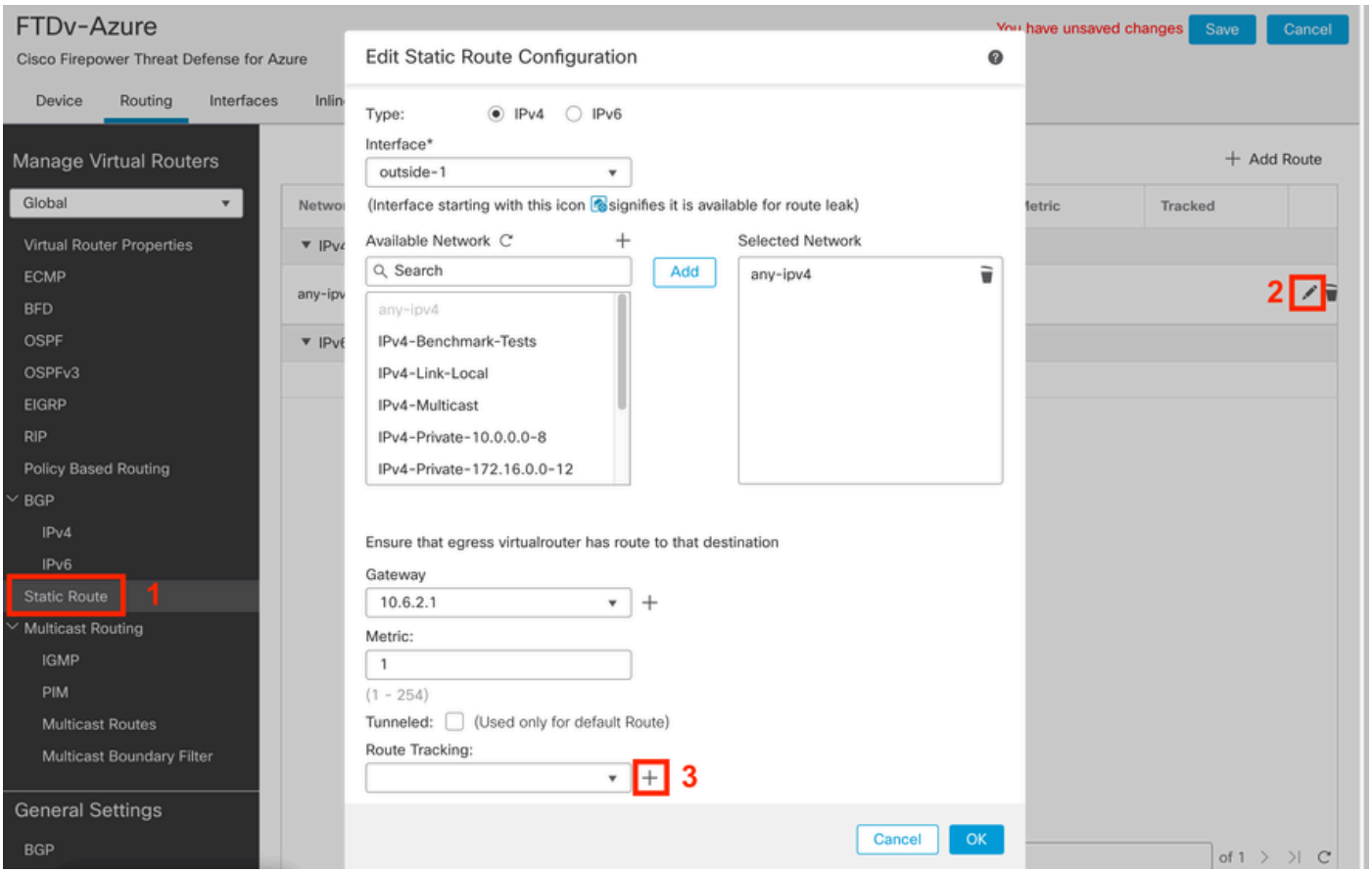



ECMP 영역 구성

OK(확인)와 Save(저장)를 클릭합니다.

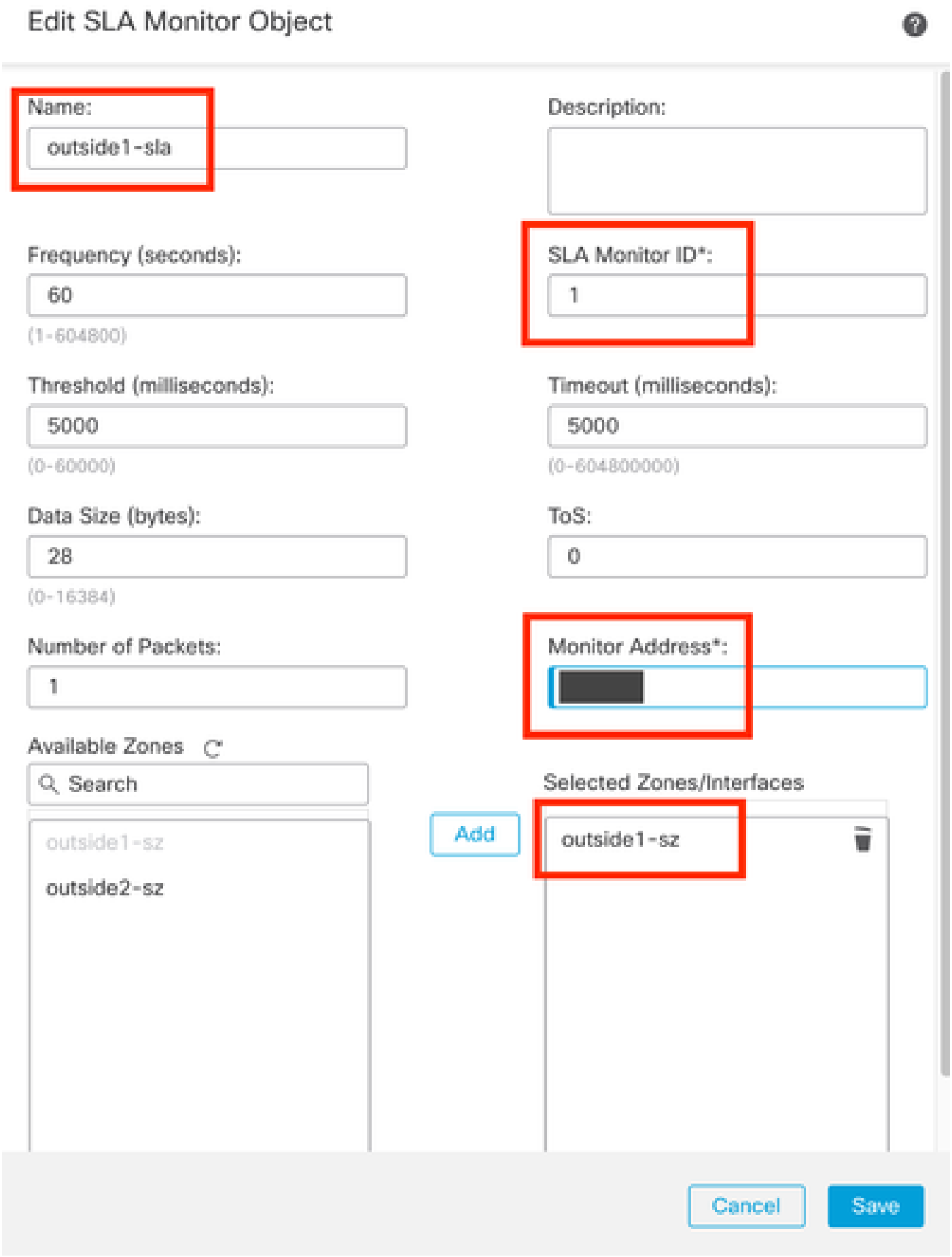
7단계. Routing(라우팅) 탭에서 Static Routes(고정 경로)로 이동합니다.

기본 경로를 수정하려면 연필 아이콘을 클릭합니다. 그런 다음 더하기 기호를 클릭하여 새 SLA 추적 객체를 추가합니다.




기본 경로를 편집하여 SLA 추적 추가

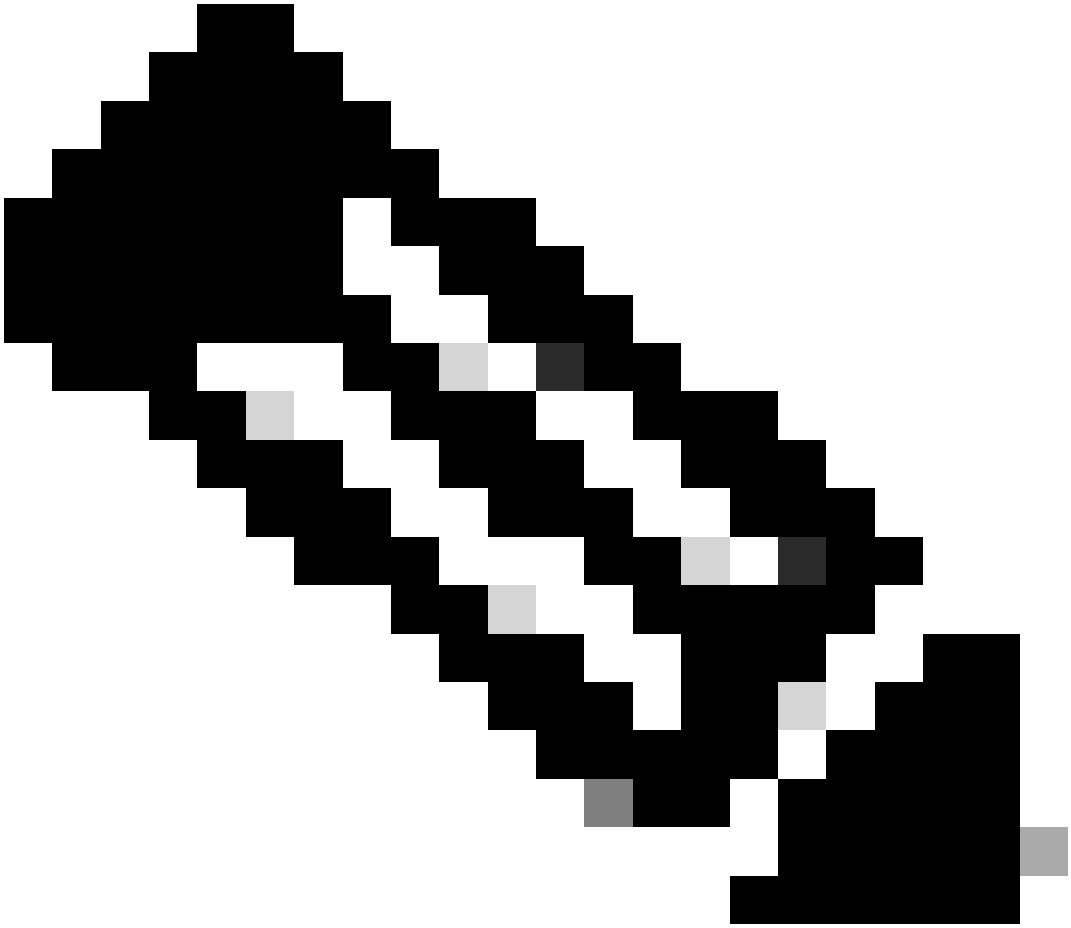
8단계. 기능 SLA 추적에 필요한 매개변수가 다음 이미지에서 강조 표시됩니다. 선택적으로, Number of Packets, Timeout, Frequency와 같은 다른 설정을 조정할 수 있습니다.




ISP 1에 대한 SLA 추적 구성

이 예에서는 Google DNS IP를 사용하여 outside1 인터페이스를 통해 인터넷(및 CDO)에 연결하기 위해 FTD 기능을 모니터링했습니다. 준비되면 확인을 클릭합니다.

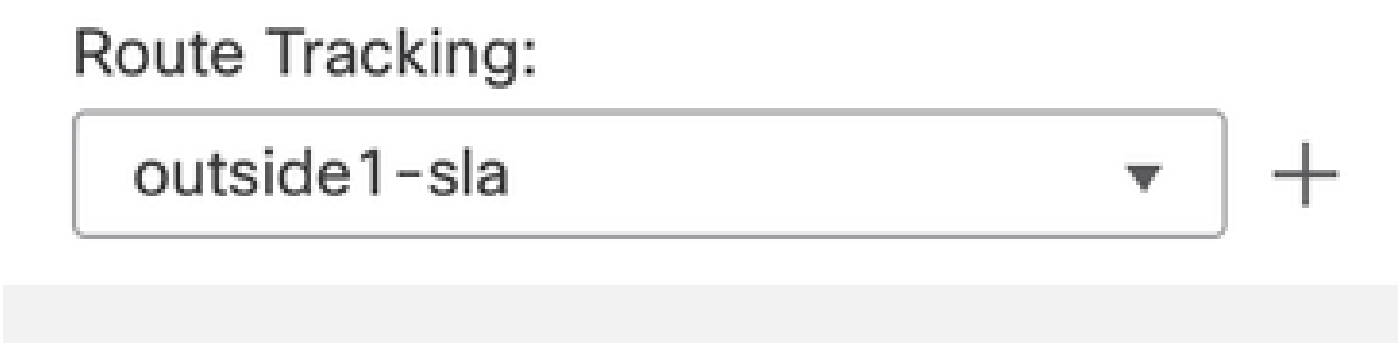
---



참고: FTD 외부 인터페이스에서 연결 가능한 것으로 이미 확인된 IP를 추적하고 있는지 확인하십시오. 연결할 수 없는 IP로 트랙을 구성하면 이 FTD에서 기본 경로가 중단된 다음 CDO와 통신할 수 없게 됩니다.

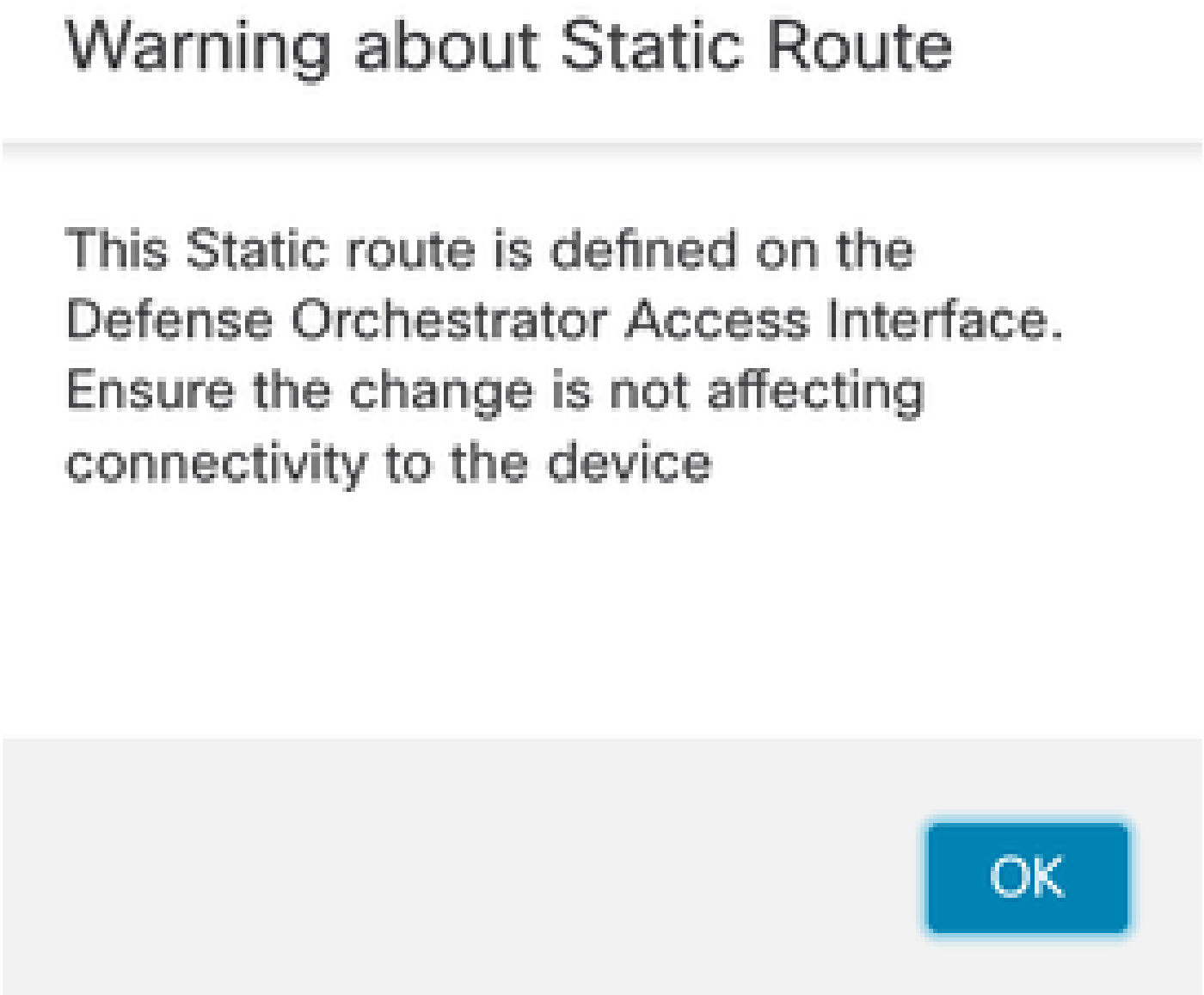
---

9단계. Save(저장)를 클릭하고 기본 인터페이스를 가리키는 경로에 새 SLA 추적이 할당되었는지 확인합니다.



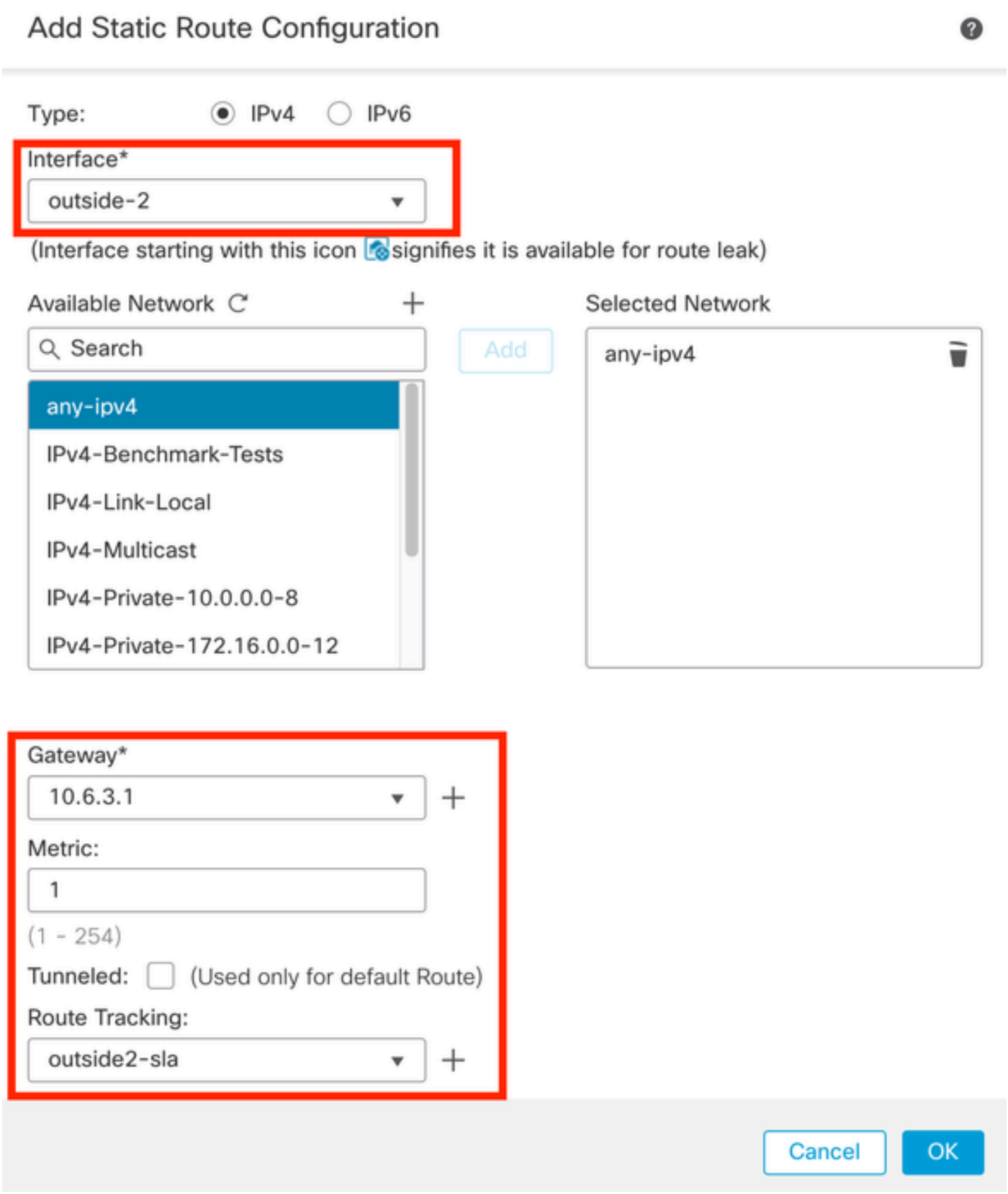

외부 1 SLA 추적

OK(확인)를 클릭하면 다음 WARNING(경고) 메시지가 포함된 팝업이 표시됩니다.

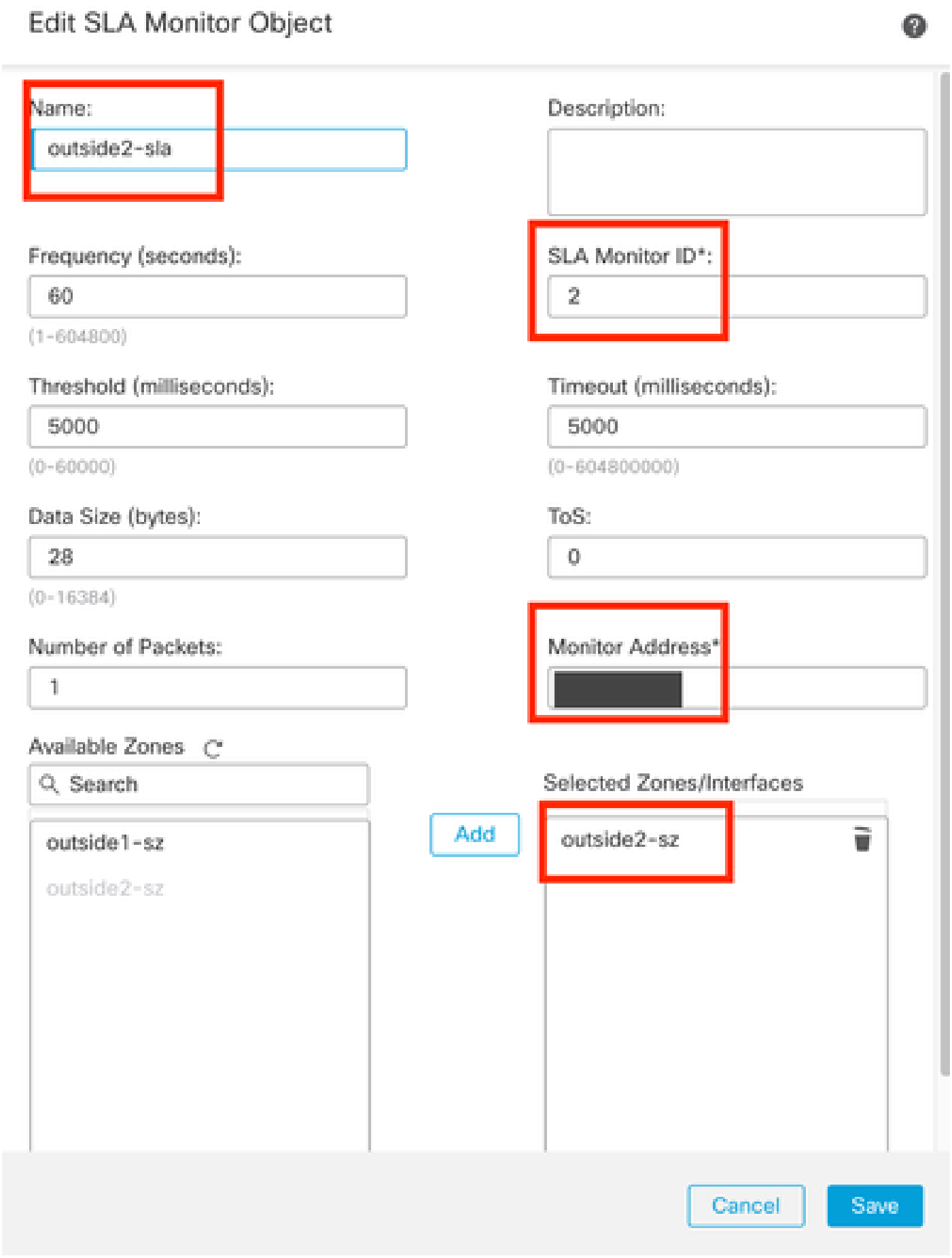



구성 경고

10단계. 이중화 데이터 인터페이스에 대한 새 경로를 추가하려면 Add Route(경로 추가) 옵션을 클릭합니다. 다음 이미지에서 경로의 메트릭 값이 동일하며, 또한 SLA 추적의 ID도 다릅니다.


Add Static Route Configuration
Type:
IPv4
IPv6
Interface*
outside-2
(Interface starting with this icon signifies it is available for route leak)
Available Network
Search
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12
Add
Selected Network
any-ipv4
Gateway*
10.6.3.1
Metric:
1
(1 - 254)
Tunneled:
(Used only for default Route)
Route Tracking:
outside2-sla
Cancel
OK

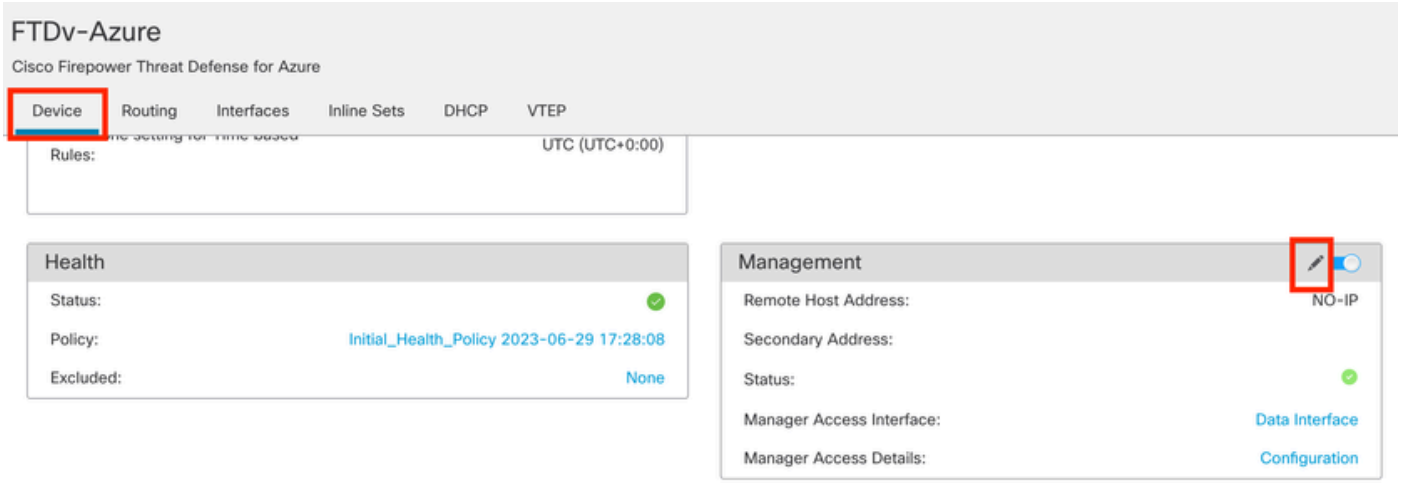
이중화 고정 경로 구성




이중화 데이터 인터페이스에 대한 추적 구성

저장을 클릭합니다.

11단계. 선택적으로, Device(디바이스) > Management(관리) 아래에서 보조 데이터 인터페이스 IP를 지정할 수 있습니다. 그러나 현재 온보딩 방법이 CLI 등록 키 프로세스를 사용했다는 점을 감안할 때 이 과정이 필요하지 않습니다.



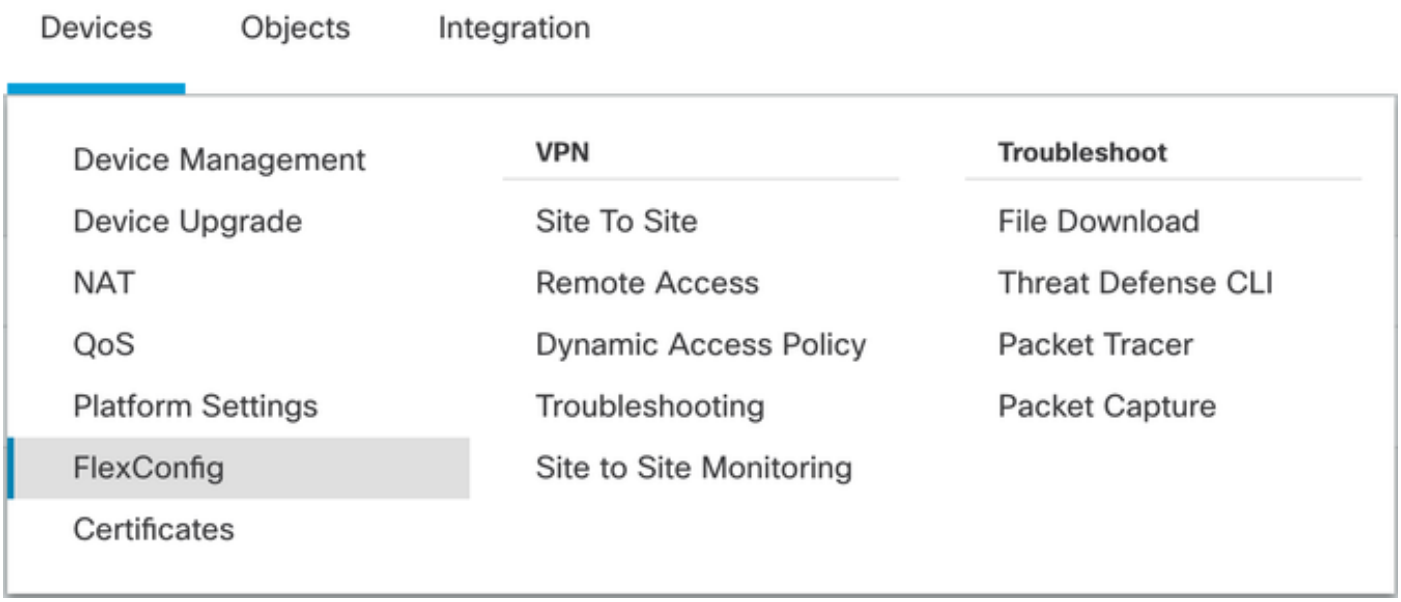

(선택 사항) Management(관리) 필드에서 중복 데이터 인터페이스에 대한 IP를 지정합니다

12단계. 변경 사항을 구축합니다.

## (선택 사항) 액티브/백업 인터페이스 모드에 대한 인터페이스 비용을 설정합니다.

기본적으로 데이터 인터페이스를 통한 이중화 관리에서는 라운드 로빈을 사용하여 두 인터페이스 간에 관리 트래픽을 분산합니다. 또는 한 WAN 링크의 대역폭이 다른 링크보다 높고 다른 링크가 백업으로 남아 있는 동안 이 링크를 기본 관리 링크로 선호할 경우 기본 링크에 1의 비용을 제공하고 백업 링크에 2의 비용을 제공할 수 있습니다. 다음 예에서는 인터페이스 GigabitEthernet0/0이 기본 WAN 링크로 유지되고 GigabitEthernet0/1은 백업 관리 링크로 사용됩니다.

1. Devices(디바이스) > FlexConfig 링크로 이동하여 flexConfig 정책을 생성합니다. FTD에 이미 flexConfig 정책이 구성되어 할당되어 있는 경우 이를 수정합니다.

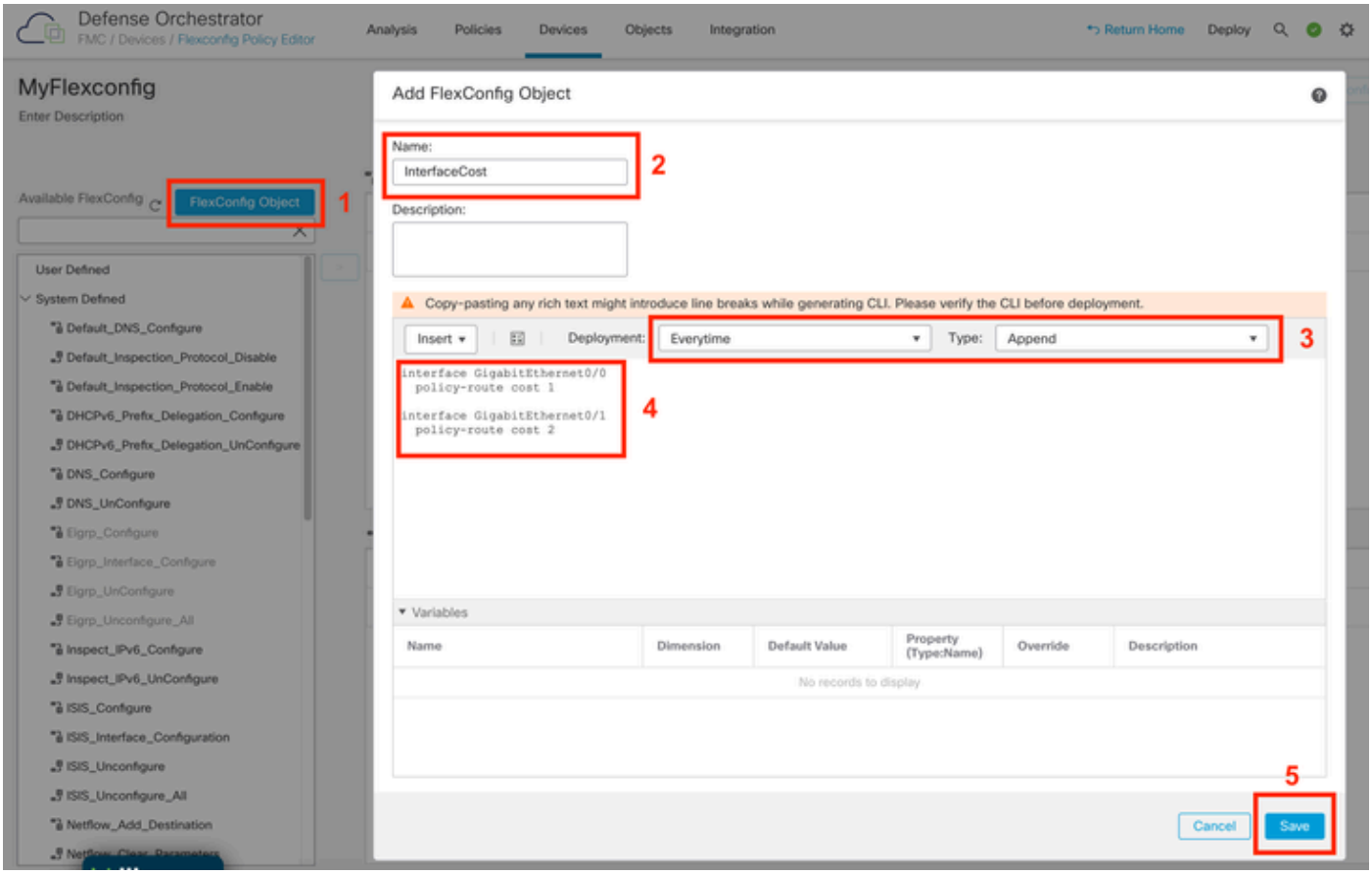


FlexConfig 메뉴 액세스

2. 새 FlexConfig 개체를 만듭니다.

- FlexConfig 개체의 이름을 지정합니다.
- Deployment(구축) 및 Type(유형) 섹션에서 Everytime(매번) 및 Append(추가)를 각각 선택합니다.
- 이미지 22에 표시된 대로 다음 명령을 사용하여 인터페이스의 비용을 설정합니다.
- 저장을 클릭합니다.

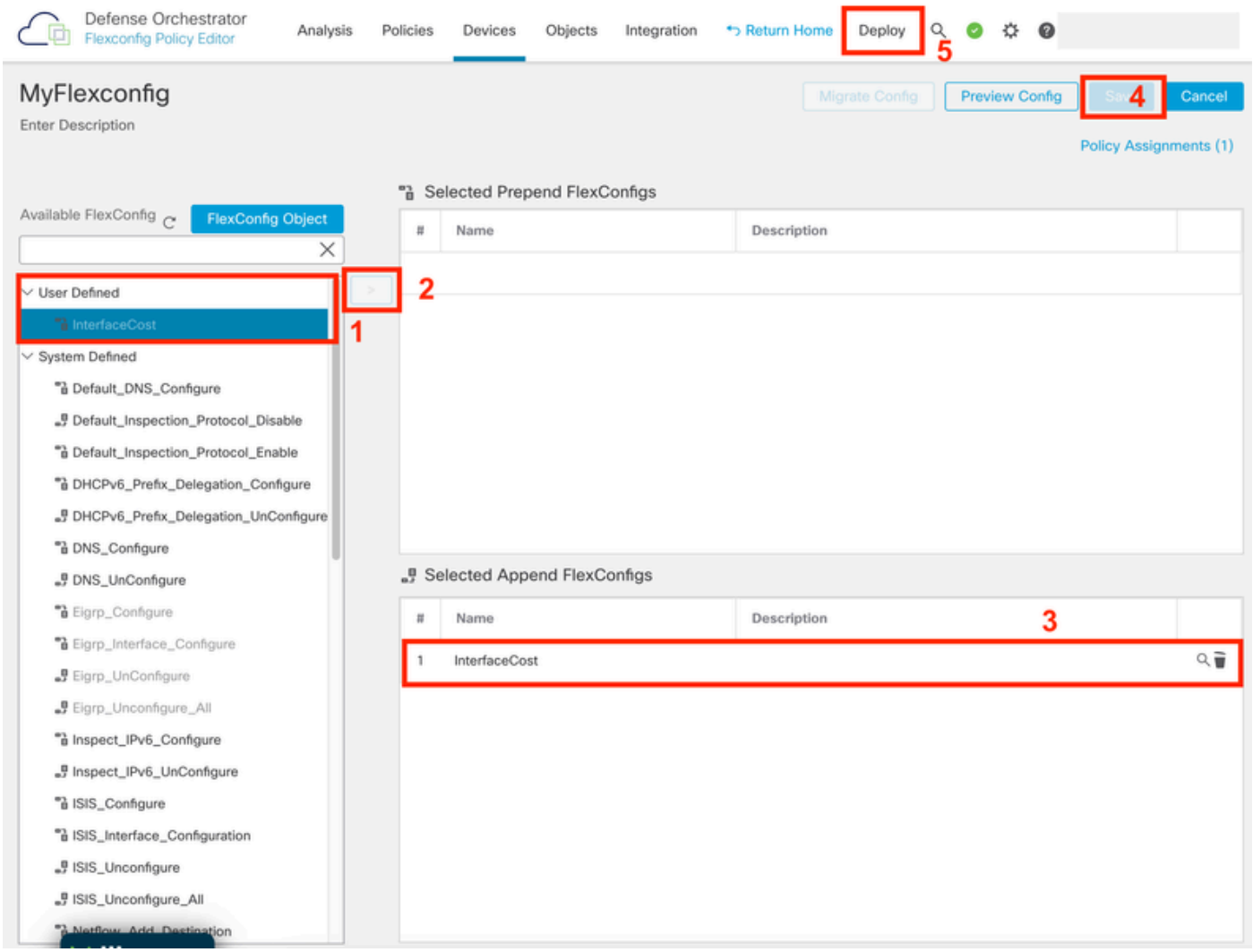
```
<#root>
interface GigabitEthernet0/0

  policy-route cost 1

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.
interface GigabitEthernet0/1

  policy-route cost 2

<=== Cost 2 sets this interface as a backup interface.
```



Flexconfig 객체 추가

3. 최근 생성된 객체를 선택하고 그림에 표시된 대로 선택된 가변 구성 추가 섹션에 추가합니다. 변

경 사항을 저장하고 컨피그레이션을 구축합니다.




Flexconfig 정책에 객체 할당

4. 변경사항을 배치합니다.

# 다음을 확인합니다.

1. 확인하려면 show network 명령을 사용합니다. 이중화 관리 인터페이스에 대한 새 인스턴스가 구성됩니다.

```
> show network

<<---------- output omitted for brevity ---------->>

======================[ eth0 ]======================
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
```

```
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.0.4
Netmask : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration : Disabled

===============[ Proxy Information ]================
State : Disabled
Authentication : Disabled
. . .

===============[ GigabitEthernet0/0 ]===============
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled

===============[ GigabitEthernet0/1 ]===============
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled
```

2. 인터페이스가 이제 sftunnel 도메인의 일부가 되었습니다. show sftunnel 인터페이스 및 show running-config sftunnel 명령을 사용하여 이를 확인할 수 있습니다.

```
<#root>

>

show sftunnel interfaces


Physical Interface Name of the Interface
GigabitEthernet0/0 outside-1
GigabitEthernet0/1 outside-2

>

show running-config sftunnel
```

```
sftunnel interface outside-2
sftunnel interface outside-1
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. 정책 기반 경로의 철자가 자동으로 지정됩니다. 인터페이스 비용을 지정하지 않은 경우 adaptive-interface 옵션은 두 인터페이스 간의 관리 트래픽을 로드 밸런싱하도록 라운드 로빈 프로세싱을 설정합니다.

```
<#root>

>

show running-config route-map


!
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2

>

show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392


access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. show running-config interface <interface> 명령을 사용하여 인터페이스 설정을 확인합니다.

```
<#root>

>

 show running-config interface GigabitEthernet 0/0


!
interface GigabitEthernet0/0
nameif outside-1
security-level 0
zone-member outside-ecmp
ip address 10.6.2.4 255.255.255.0
policy-route cost 1

>

show running-config interface GigabitEthernet 0/1


!
interface GigabitEthernet0/1
nameif outside-2
security-level 0
zone-member outside-ecmp
```

```
ip address 10.6.3.4 255.255.255.0
policy-route cost 2
```

일부 추가 명령을 사용하여 구성된 경로의 추적을 확인할 수 있습니다.

<#root>

>

**show track**

```
Track 1
Response Time Reporter 2 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 10
Tracked by:
STATIC-IP-ROUTING 0
Track 2
Response Time Reporter 1 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
STATIC-IP-ROUTING 0
```

>

**show route**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.6.3.1 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
                   [1/0] via 10.6.2.1, outside-1
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

# 관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Defense Orchestrator에서 클라우드 기반 방화벽 관리 센터를 통해 방화벽 위협 방어 관리

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.