Secure FMC를 사용하여 Secure FTD에서 VXLAN 인터페이스 구성

목차

소개

이 문서에서는 FMC(Secure Firewall Management Center)를 사용하여 FTD(Secure Firewall Threat Defense)에서 VXLAN 인터페이스를 구성하는 방법에 대해 설명합니다

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 기본 VLAN/VXLAN 개념
- 기본 네트워크 지식.
- 기본적인 Cisco Secure Management Center 환경
- 기본적인 Cisco Secure Firewall 위협 방어 환경

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 7.2.4 릴리스를 실행하는 Cisco FMCv(Secure Firewall Management Center Virtual) VMware
- 7.2.4 릴리스를 실행하는 Cisco FTDv(Secure Firewall Threat Defense Virtual Appliance) VMware.

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.

배경 정보

VXLAN(Virtual Extensible VLAN)은 기존 VLAN과 마찬가지로 이더넷 레이어 2 네트워크 서비스를 제공합니다. 가상 환경에서 VLAN 세그먼트에 대한 수요가 높기 때문에 VXLAN은 더 큰 확장성과 유연성을 제공하며 원래 레이어 2 프레임에 VXLAN 헤더가 추가된 다음 UDP-IP 패킷에 배치하는 MAC-in-UDP 캡슐화 방식을 정의합니다. 이 MAC-in-UDP 캡슐화를 통해 VXLAN은 레이어 3 네트워크를 통해 레이어 2 네트워크를 터널링합니다. VXLAN은 다음과 같은 이점을 제공합니다.

- 멀티테넌트 세그먼트에서 VLAN 유연성:
- 더 많은 L2(Layer 2) 세그먼트를 처리할 수 있는 뛰어난 확장성
- 네트워크 사용률 향상.

Cisco FTD(Secure Firewall Threat Defense)는 두 가지 유형의 VXLAN 캡슐화를 지원합니다.

- VXLAN(모든 보안 방화벽 위협 방어 모델에 사용)
- Geneve(Secure Firewall Threat Defense 가상 어플라이언스에 사용됨)

Amazon Web Services(AWS) 게이트웨이 로드 밸런서와 어플라이언스 간에 패킷을 투명하게 라우팅하고 추가 정보를 전송하려면 제네브 캡슐화가 필요합니다.

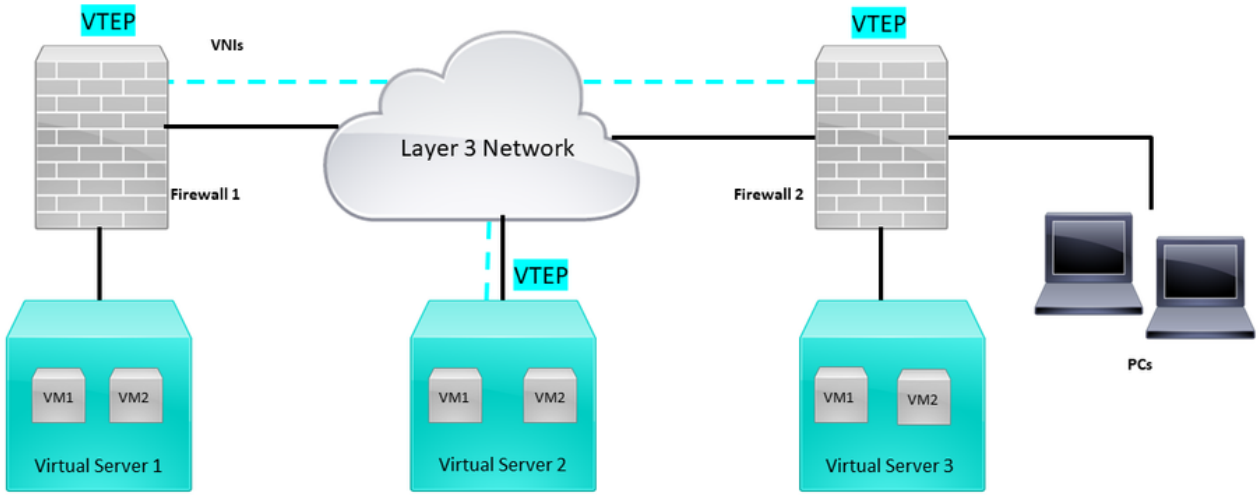
VXLAN은 VTEP(VXLAN Tunnel Endpoint)를 사용하여 테넌트의 엔드 디바이스를 VXLAN 세그먼트에 매핑하고 VXLAN 캡슐화 및 역캡슐화를 수행합니다. 각 VTEP에는 두 가지 인터페이스 유형이 있습니다. 보안 정책을 적용할 수 있는 VNI(VXLAN Network Identifier) 인터페이스라고 하는 하나 이상의 가상 인터페이스와 VTEP 간에 VNI 인터페이스가 터널링되는 VTEP 소스 인터페이스라고 하는 일반 인터페이스입니다. VTEP 소스 인터페이스는 VTEP-VTEP 통신을 위해 전송 IP 네트워크에 연결되며, VNI 인터페이스는 VLAN 인터페이스와 유사합니다. 태깅을 사용하여 지정된 물리적 인터페이스에서 네트워크 트래픽을 분리하는 가상 인터페이스입니다. 보안 정책은 각 VNI 인터페이스에 적용됩니다. 하나의 VTEP 인터페이스를 추가할 수 있으며 모든 VNI 인터페이스는 동일한 VTEP 인터페이스와 연결됩니다. AWS의 위협 방어 가상 클러스터링에는 예외가 있습니다.

위협 방어 기능은 세 가지 방법으로 캡슐화하고 캡슐화를 해제합니다.

- 위협 방어에 단일 피어 VTEP IP 주소를 정적으로 구성할 수 있습니다.
- 피어 VTEP IP 주소 그룹은 위협 방어에 정적으로 구성할 수 있습니다.
- 멀티캐스트 그룹은 각 VNI 인터페이스에서 구성할 수 있습니다.

이 문서에서는 2개의 피어 VTEP IP 주소 그룹을 정적으로 구성한 VXLAN 캡슐화를 위한 VXLAN 인터페이스에 대해 중점적으로 다룹니다. Geneve 인터페이스를 구성해야 하는 경우 AWS의 Geneve 인터페이스에 대한 공식 문서를 확인하거나 단일 피어 또는 멀티캐스트 그룹으로 VTEP를 구성하십시오. 단일 피어 또는 멀티캐스트 그룹 컨피그레이션 가이드를 사용하여 VTEP 인터페이스를 확인하십시오.

네트워크 다이어그램



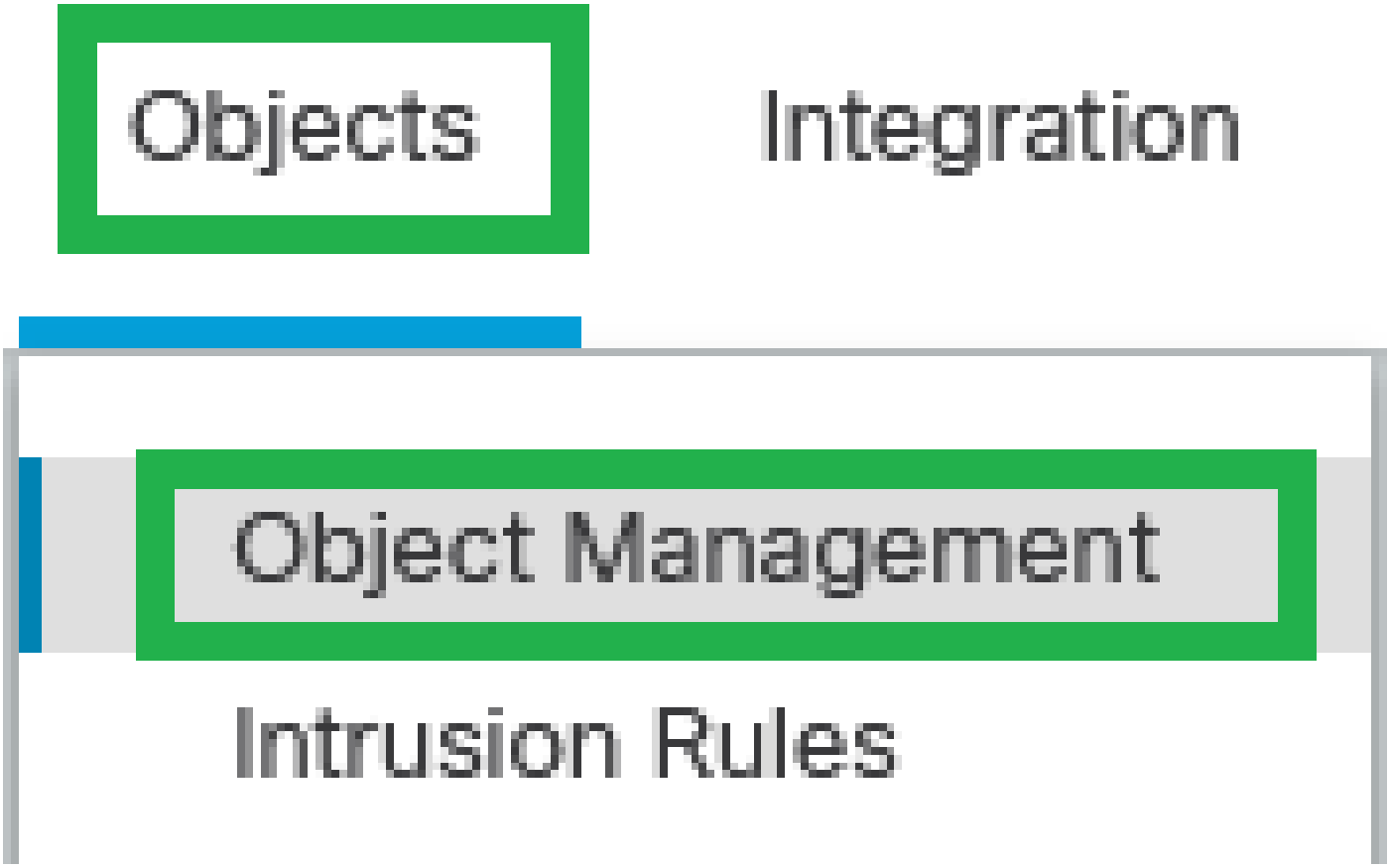
네트워크 토폴로지

configure 섹션에서는 언더레이 네트워크가 Secure Firewall Management Center를 통해 위협 방어에 이미 구성되어 있다고 가정합니다. 이 문서에서는 오버레이 네트워크 컨피그레이션을 중점적으로 다룹니다.

구성

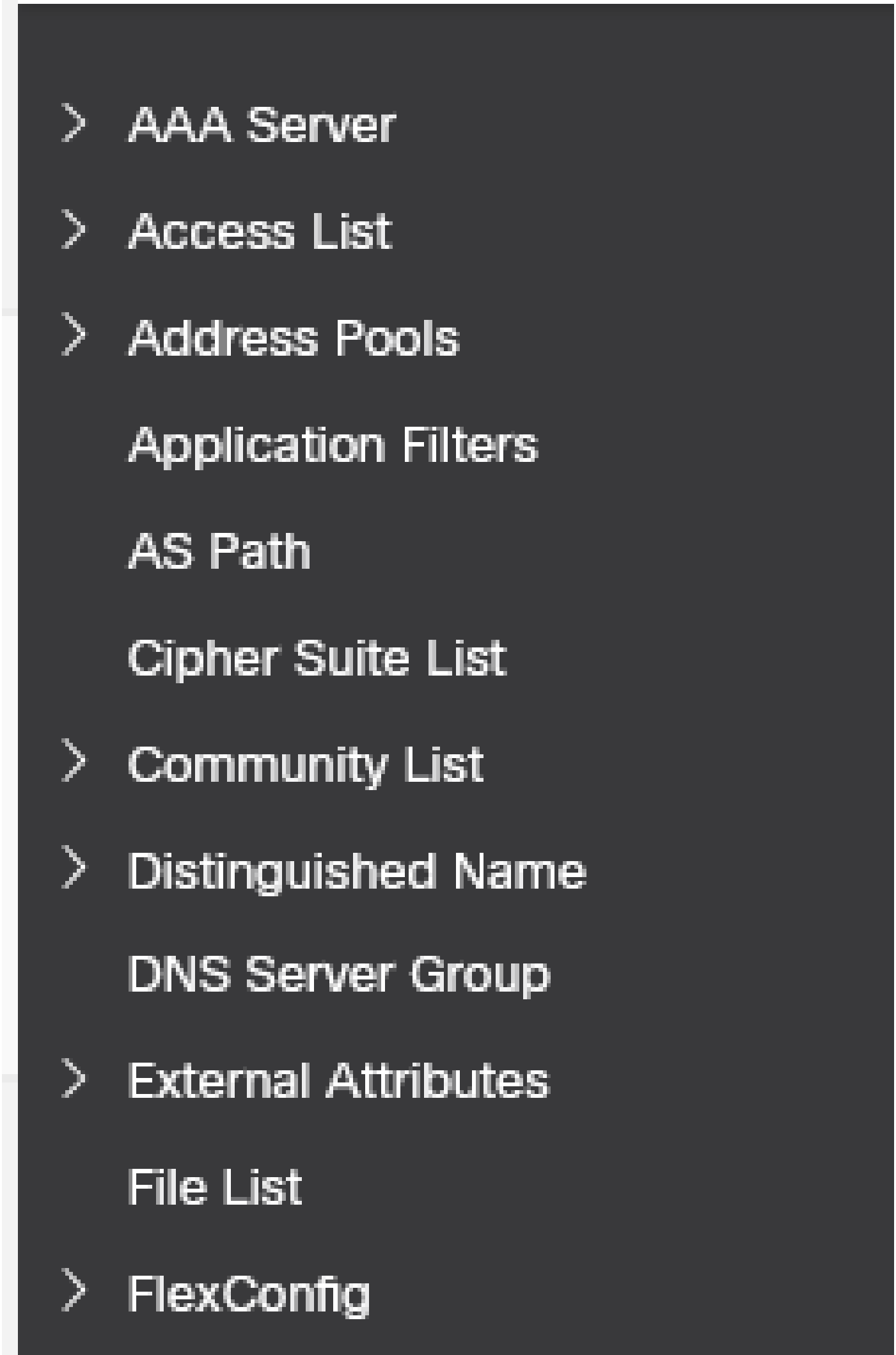
VTEP 피어 그룹 구성

1단계: Objects(개체) > Object Management(개체 관리)로 이동합니다.



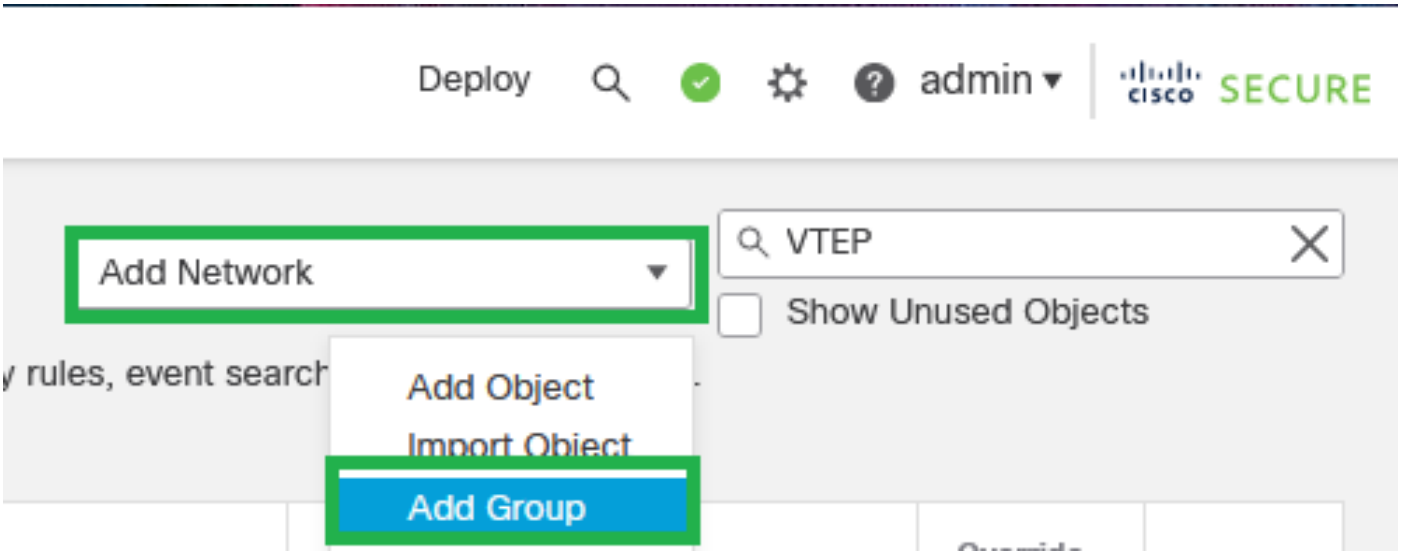
객체 - 객체 관리

2단계: 왼쪽 메뉴에서 Network(네트워크)를 클릭합니다.


AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig

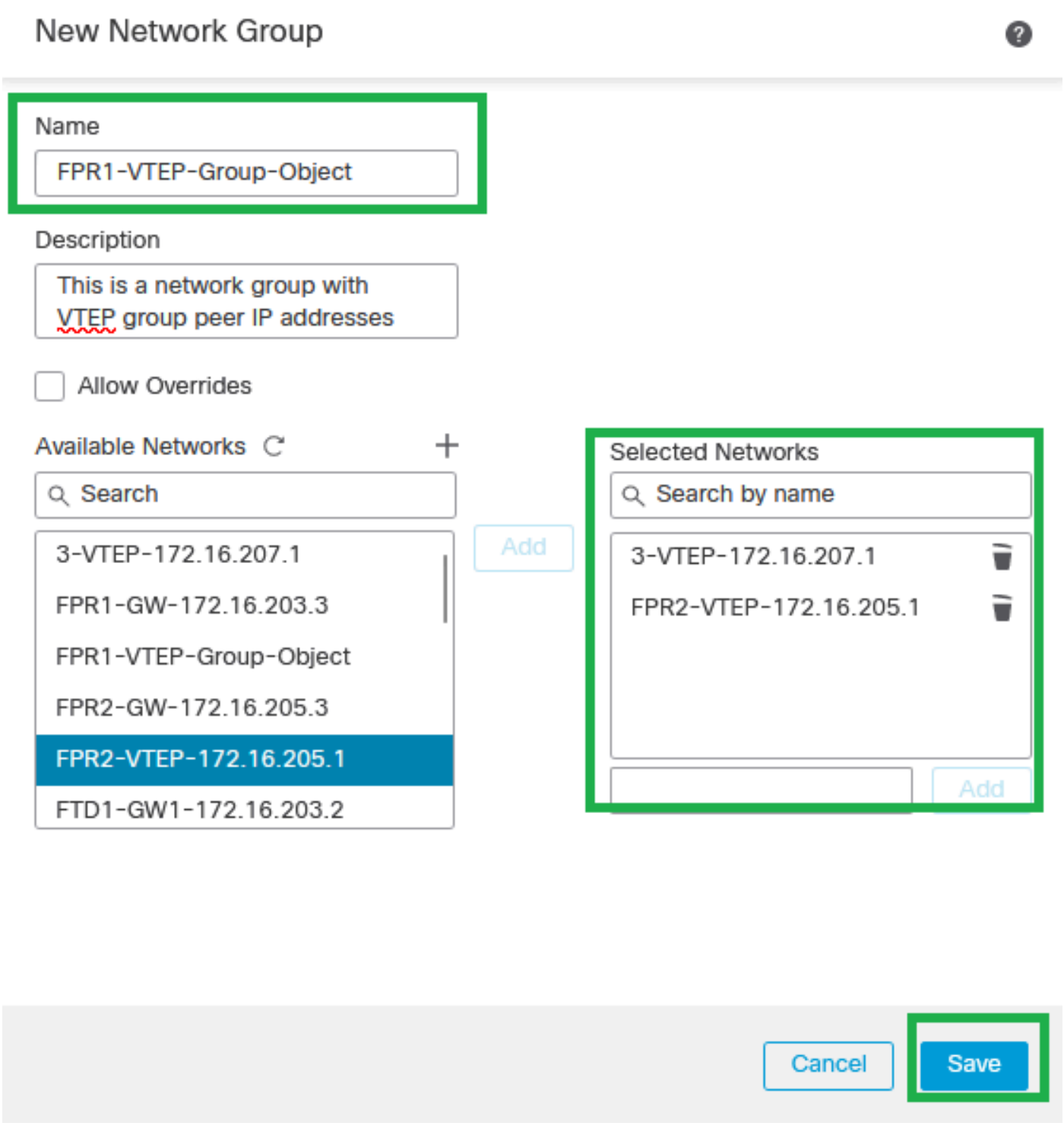
주소에 대해 더 많은 호스트 네트워크 개체를 구성합니다. 이 컨피그레이션 가이드에는 두 개의 객체가 있습니다.

5단계: Create Object Group(개체 그룹 생성)에서 Add Network(네트워크 추가) > Add Group(그룹 추가)을 클릭합니다.



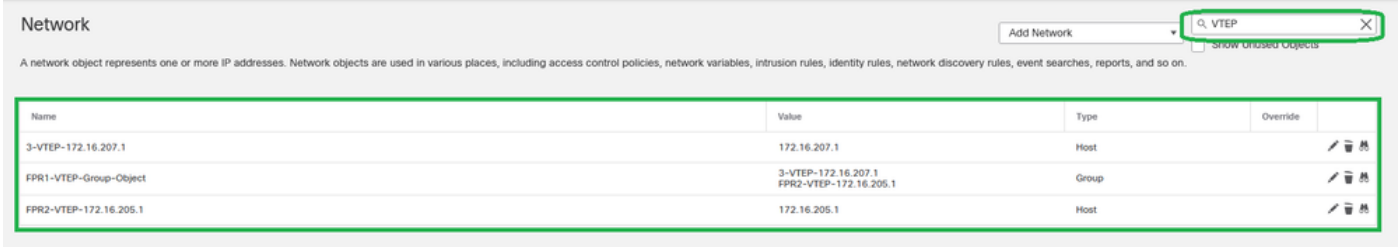
네트워크 추가 - 그룹 추가

6단계: 모든 VTEP 피어 IP 주소로 네트워크 개체 그룹을 만듭니다. 네트워크 그룹 이름을 설정하고 필요한 네트워크 객체 그룹을 선택한 다음 Save(저장)를 클릭합니다.



네트워크 개체 그룹 만들기

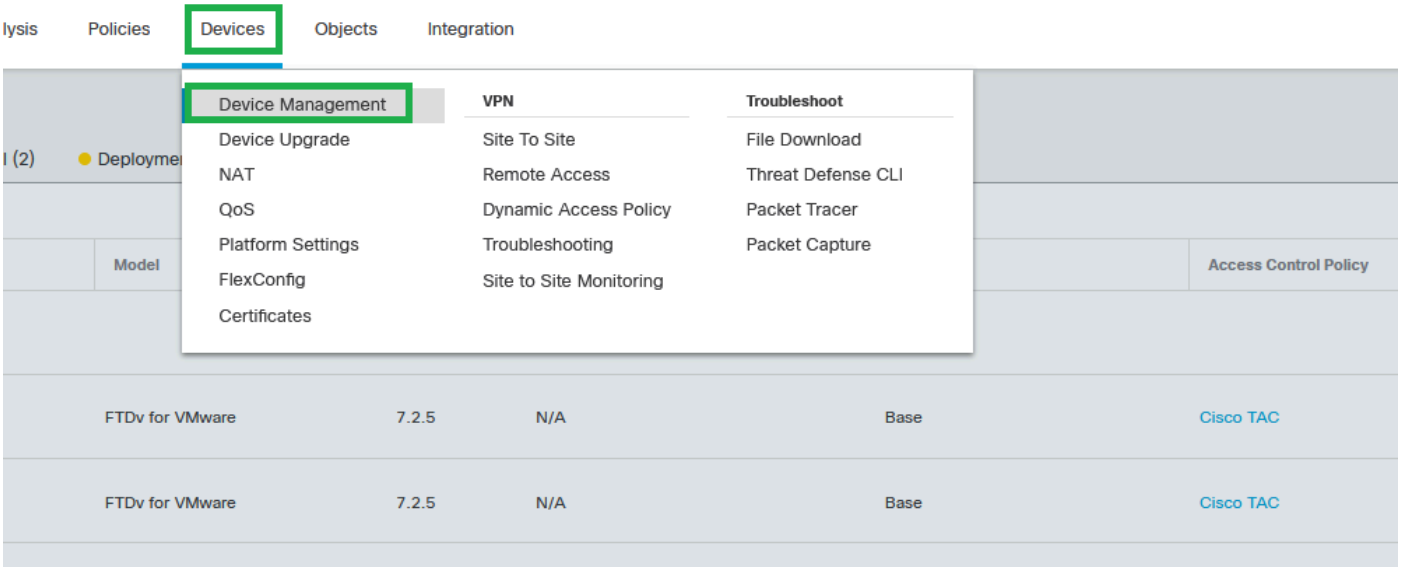
7단계: Network Object 필터에서 네트워크 개체 및 네트워크 개체 그룹을 검증합니다.



VTEP 개체 그룹 유효성 검사

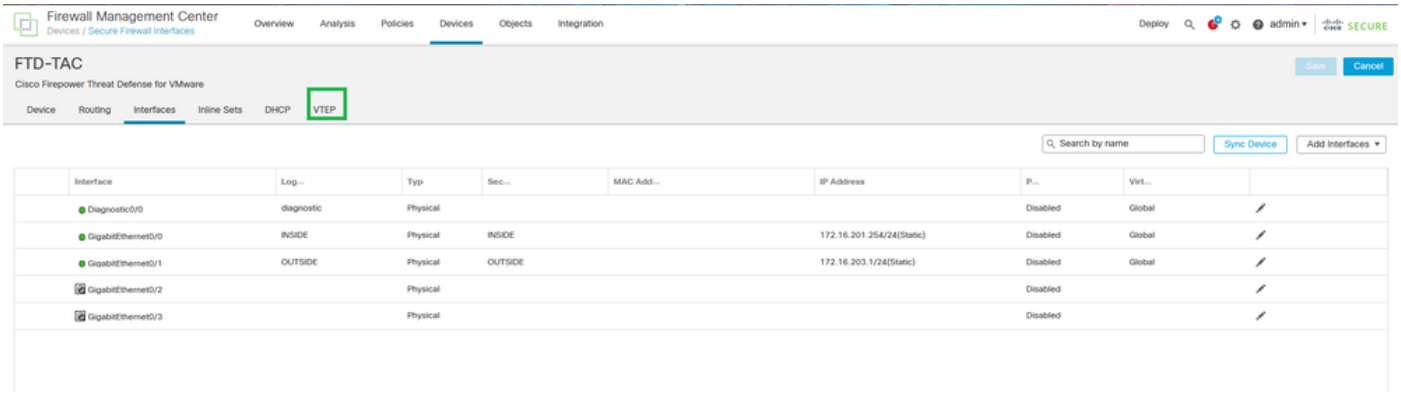
VTEP 소스 인터페이스 구성

1단계: Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 위협 방어를 수정합니다.



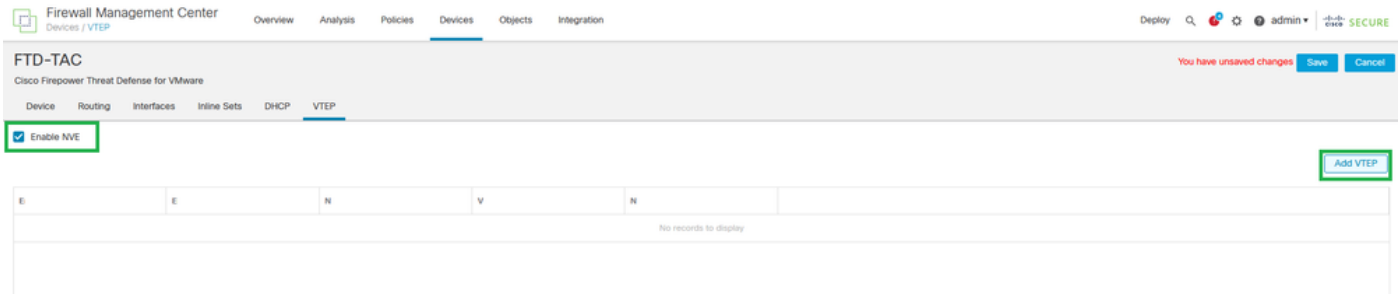
디바이스 - 디바이스 관리

2단계: VTEP 섹션으로 이동합니다.



VTEP 섹션

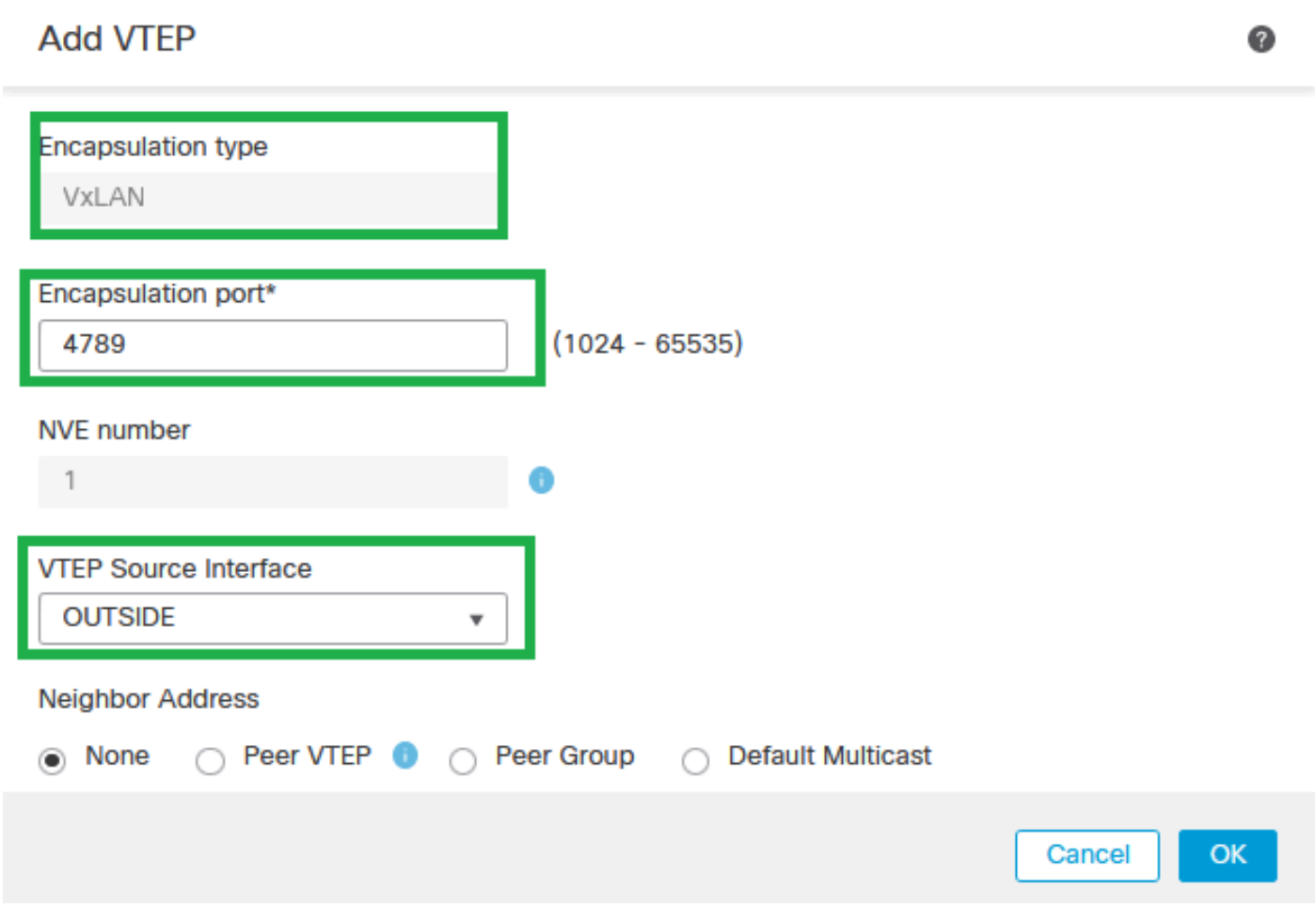
3단계: Enable VNE(VNE 활성화) 확인란을 선택하고 Add VTEP(VTEP 추가)를 클릭합니다.



NVE 활성화 및 VTEP 추가

4단계: Encapsulation(캡슐화) 유형으로 VxLAN을 선택하고 Encapsulation Port(캡슐화 포트) 값을

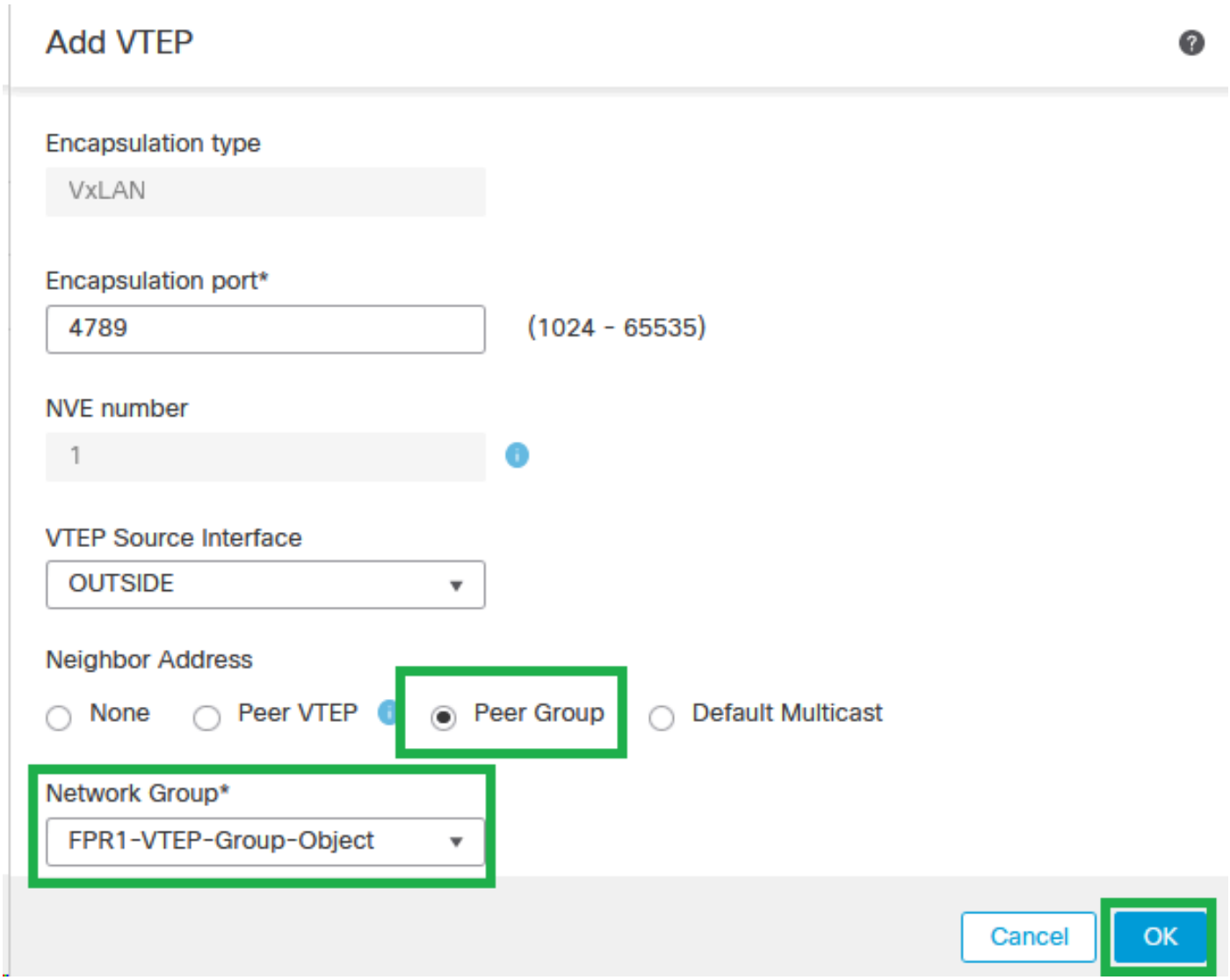
입력한 다음 이 위협 방어의 VTEP 소스에 사용되는 인터페이스를 선택합니다(이 컨피그레이션 가이드의 외부 인터페이스)



VTEP 추가

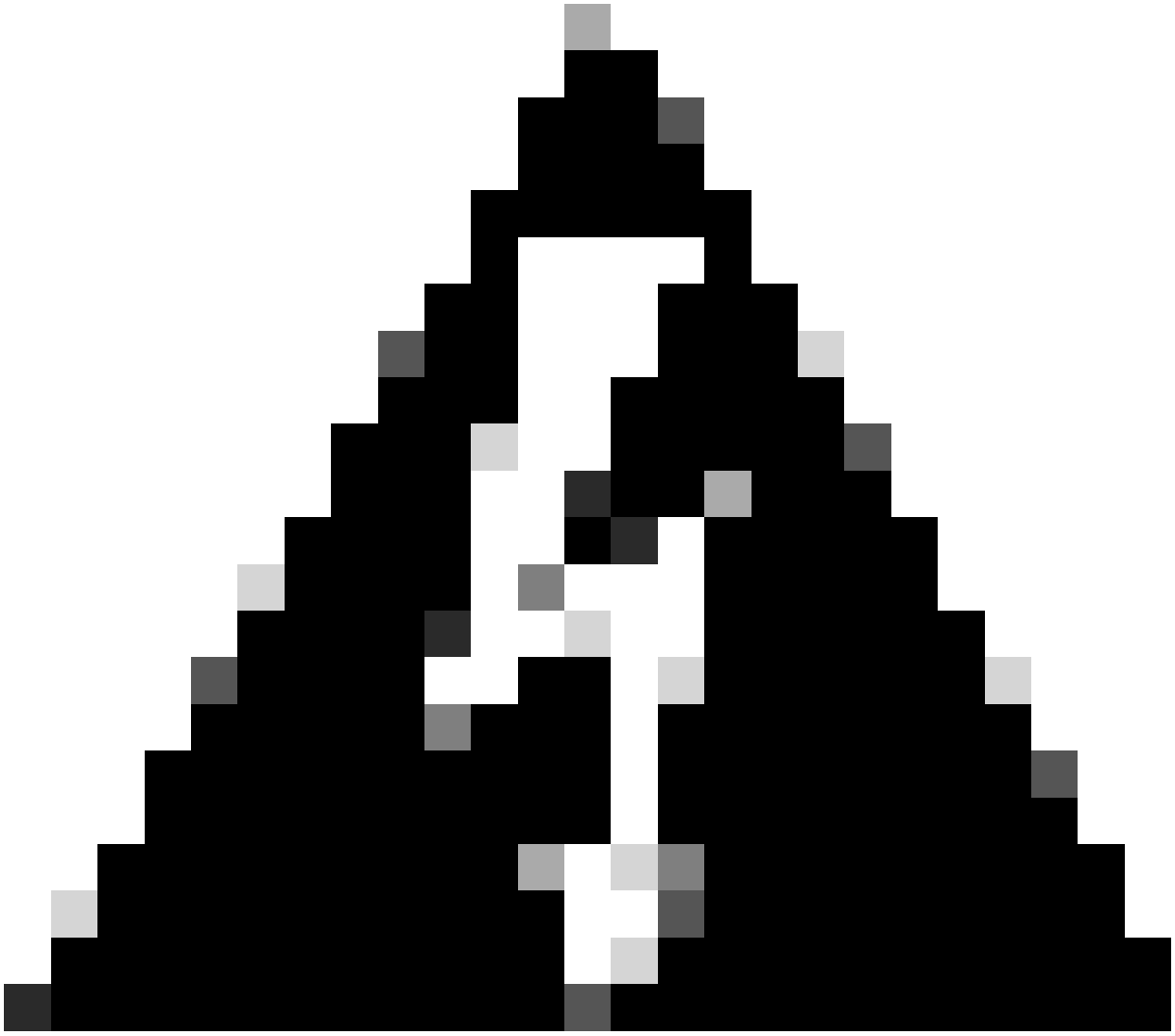
참고: VxLAN 캡슐화가 기본값입니다. AWS의 경우 VxLAN과 Geneve 중에서 선택할 수 있습니다. 기본값은 4789이며, 설계에 따라 1024~65535 범위 사이에서 Any Encapsulation Port(캡슐화 포트)를 선택할 수 있습니다.

5단계: Peer Group(피어 그룹)을 선택하고 이전 컨피그레이션 섹션에서 생성한 Network Object Group(네트워크 개체 그룹)을 선택한 다음 OK(확인)를 클릭합니다.



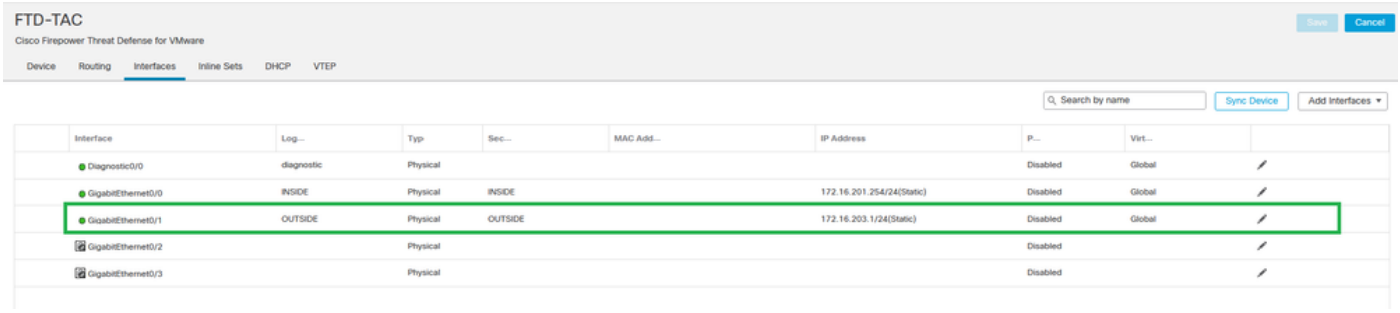
피어 그룹 - 네트워크 개체 그룹

6단계: 변경 사항을 저장합니다.



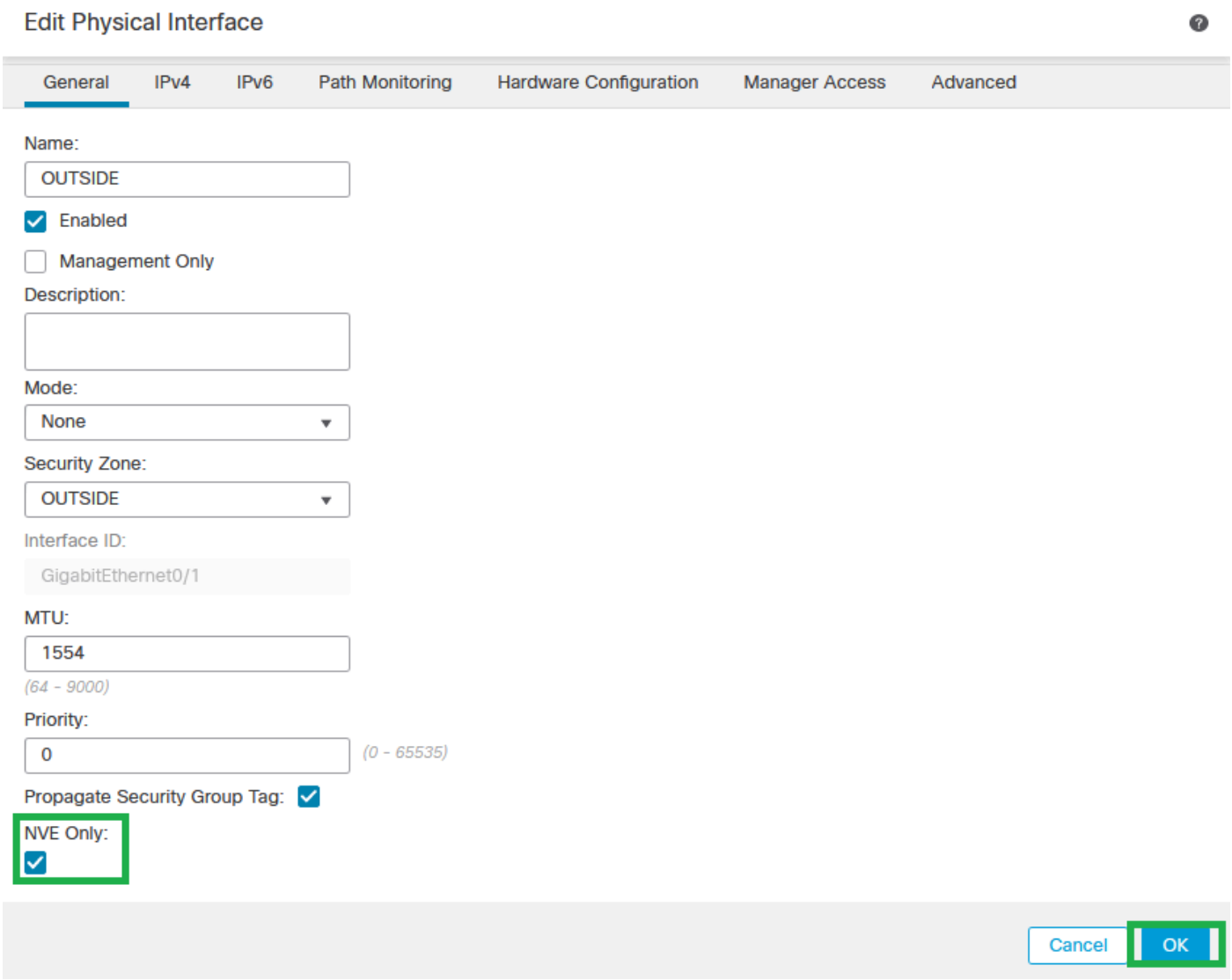
경고: 변경 사항이 저장되면 점보 프레임 변경 메시지가 나타나고, MTU가 VTEP로 할당된 인터페이스에서 1554로 변경되며, 언더레이 네트워크에서 동일한 MTU를 사용해야 합니다 .

7단계: Interfaces(인터페이스)를 클릭하고 VTEP 소스 인터페이스에 사용되는 인터페이스를 편집합니다. (이 컨피그레이션 가이드의 외부 인터페이스)

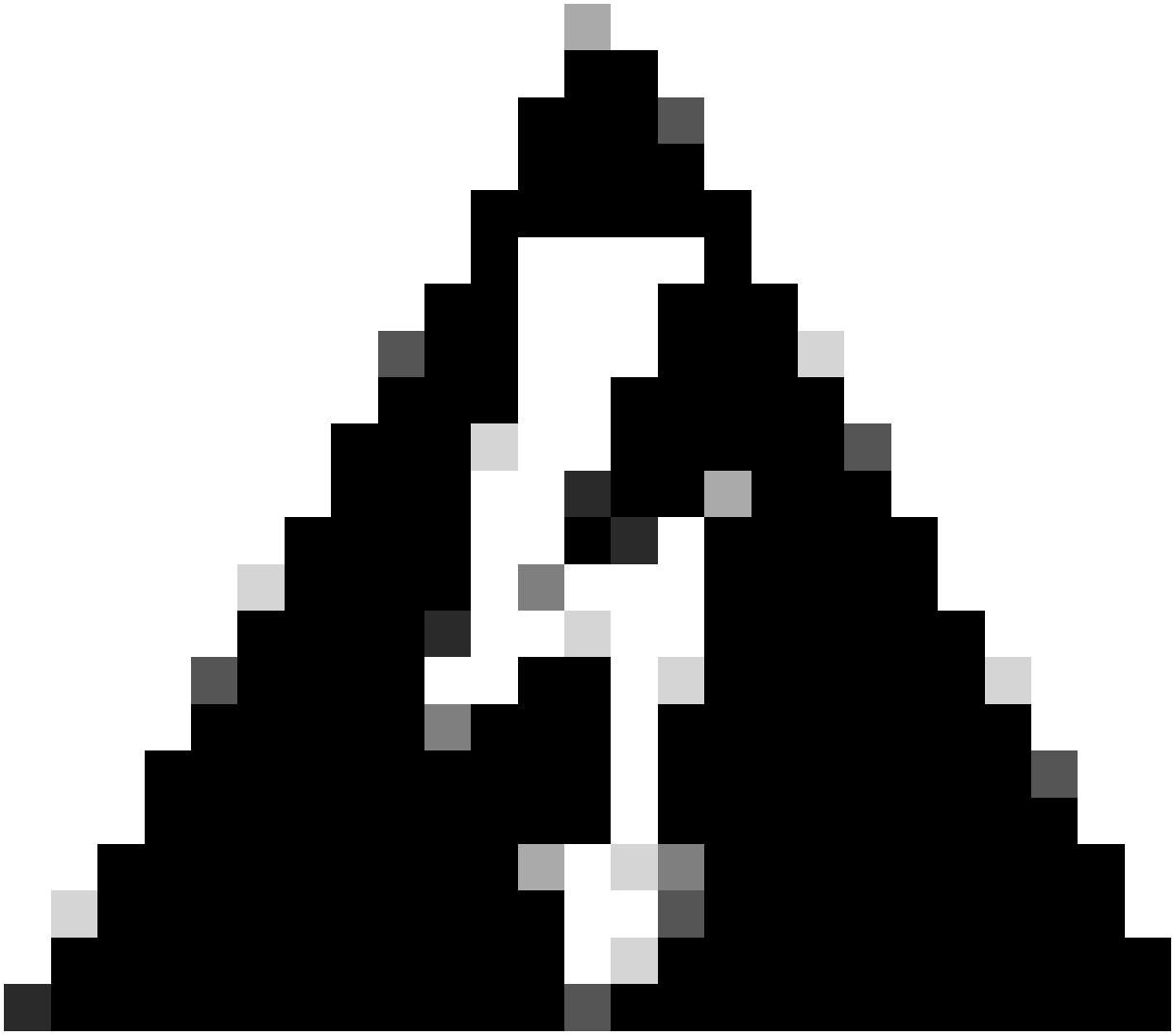


VTEP 소스 인터페이스로 외부

8단계(선택 사항): General(일반) 페이지에서 NVE Only(NVE만) 확인란을 선택한 다음 OK(확인)를 클릭합니다.



NVE 전용 컨피그레이션

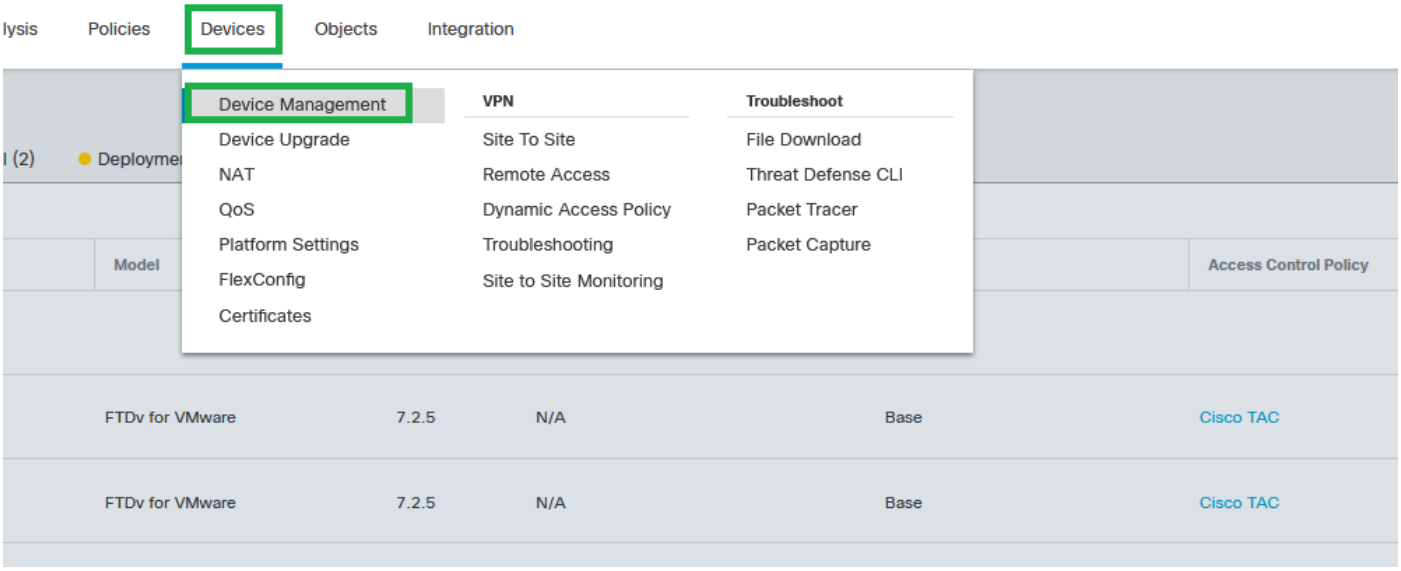


경고: 이 설정은 이 인터페이스에서 트래픽을 VXLAN 및 공통 관리 트래픽으로만 제한하는 라우팅된 모드에 대해 선택 사항입니다. 이 설정은 투명 방화벽 모드에 대해 자동으로 활성화됩니다.

9단계: 변경 사항을 저장합니다.

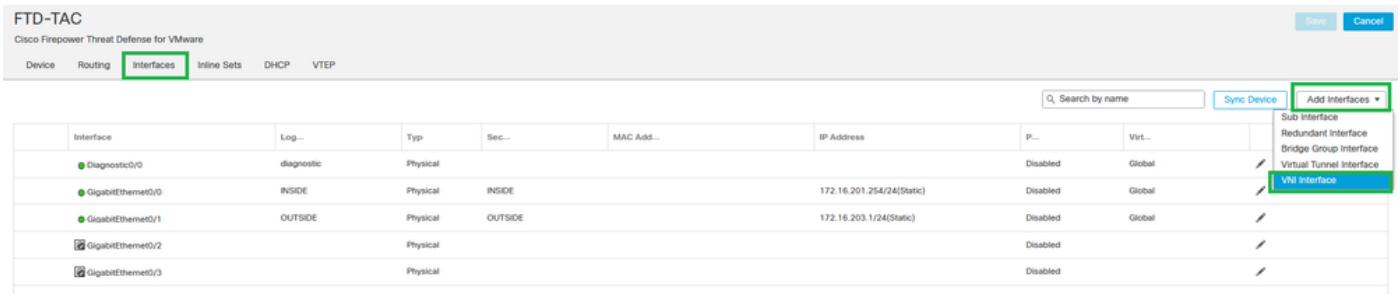
VTEP VNI 인터페이스 구성

1단계: Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 위협 방어를 수정합니다.



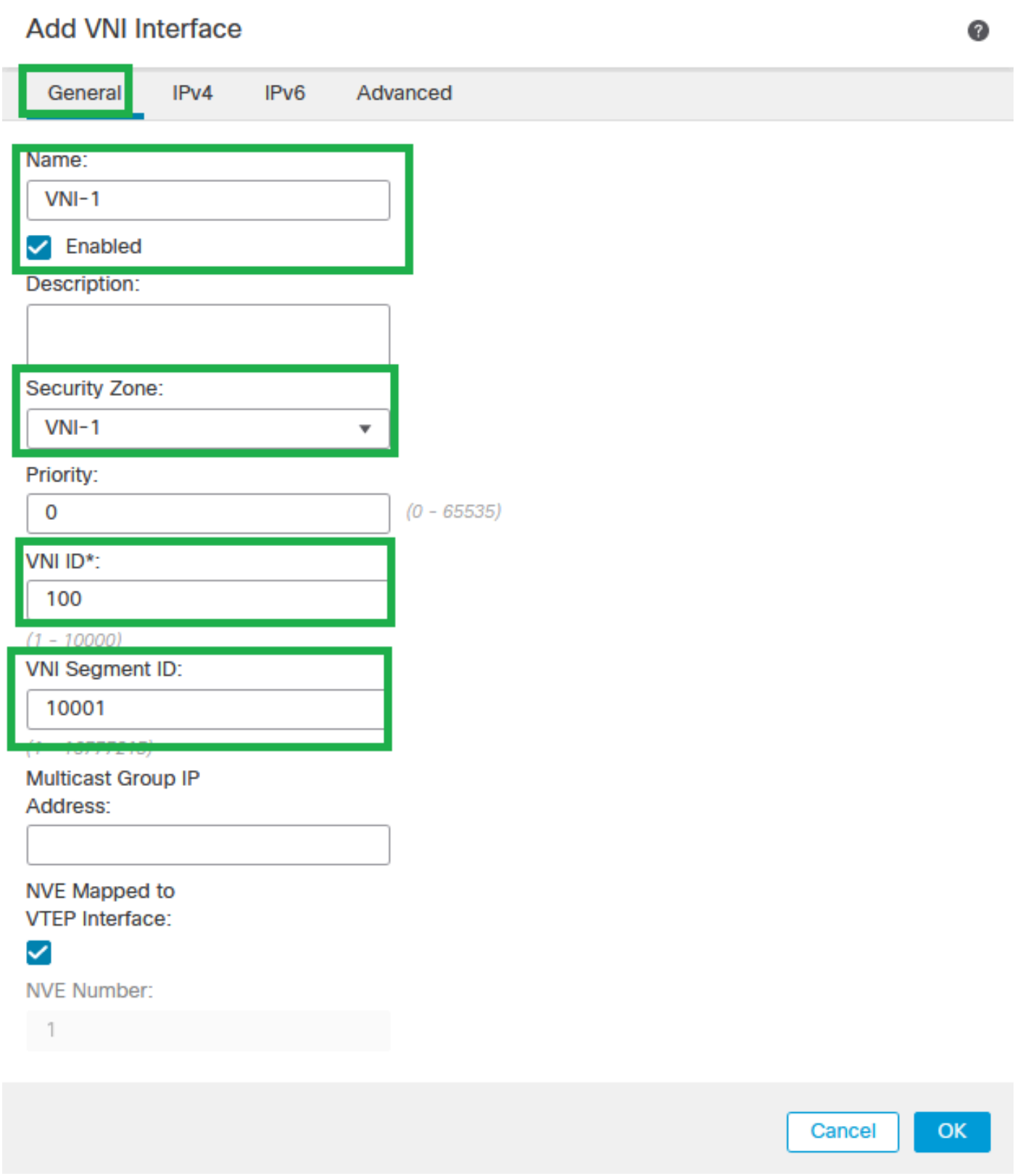
디바이스 - 디바이스 관리

2단계: Interfaces(인터페이스) 섹션에서 Add Interfaces(인터페이스 추가) > VNI Interfaces(VNI 인터페이스)를 클릭합니다.

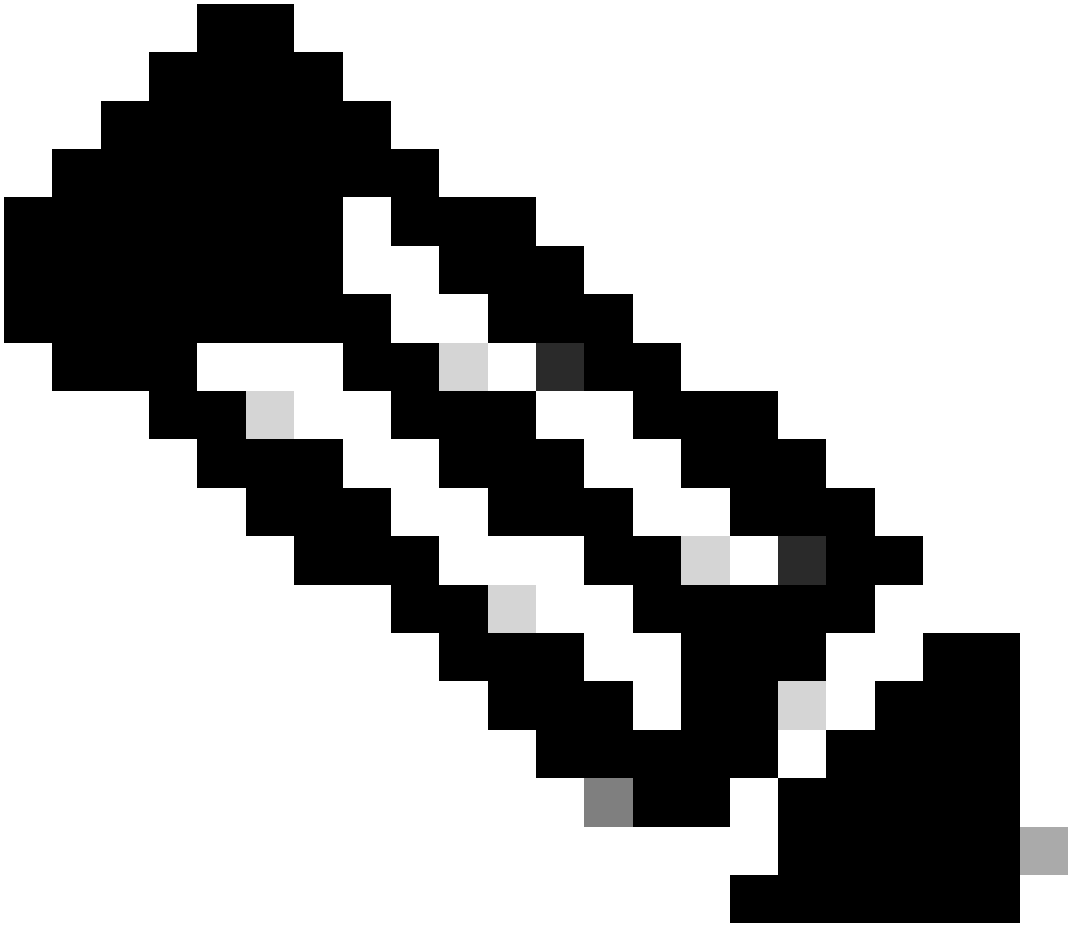


인터페이스 - 인터페이스 추가 - VNI 인터페이스

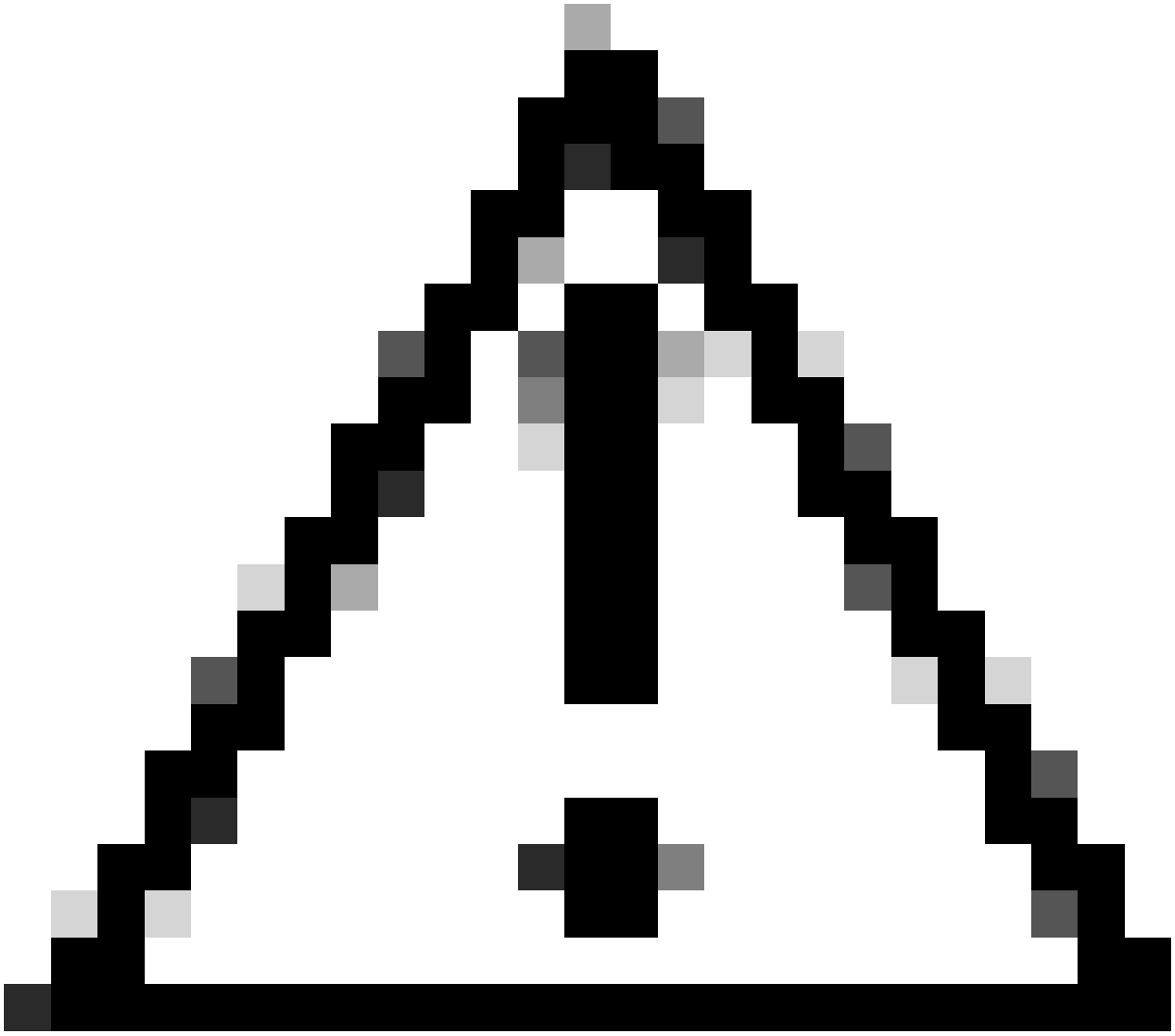
3단계: General(일반) 섹션에서 이름, 설명, Security Zone(보안 영역), VNI ID 및 VNI Segment ID를 사용하여 VNI 인터페이스를 설정합니다.


Add VNI Interface
General
IPv4
IPv6
Advanced
Name:
VNI-1
Enabled
Description:
Security Zone:
VNI-1
Priority:
0
(0 - 65535)
VNI ID*:
100
(1 - 10000)
VNI Segment ID:
10001
Multicast Group IP Address:
NVE Mapped to VTEP Interface:
NVE Number:
1
Cancel
OK

VNI 인터페이스 추가

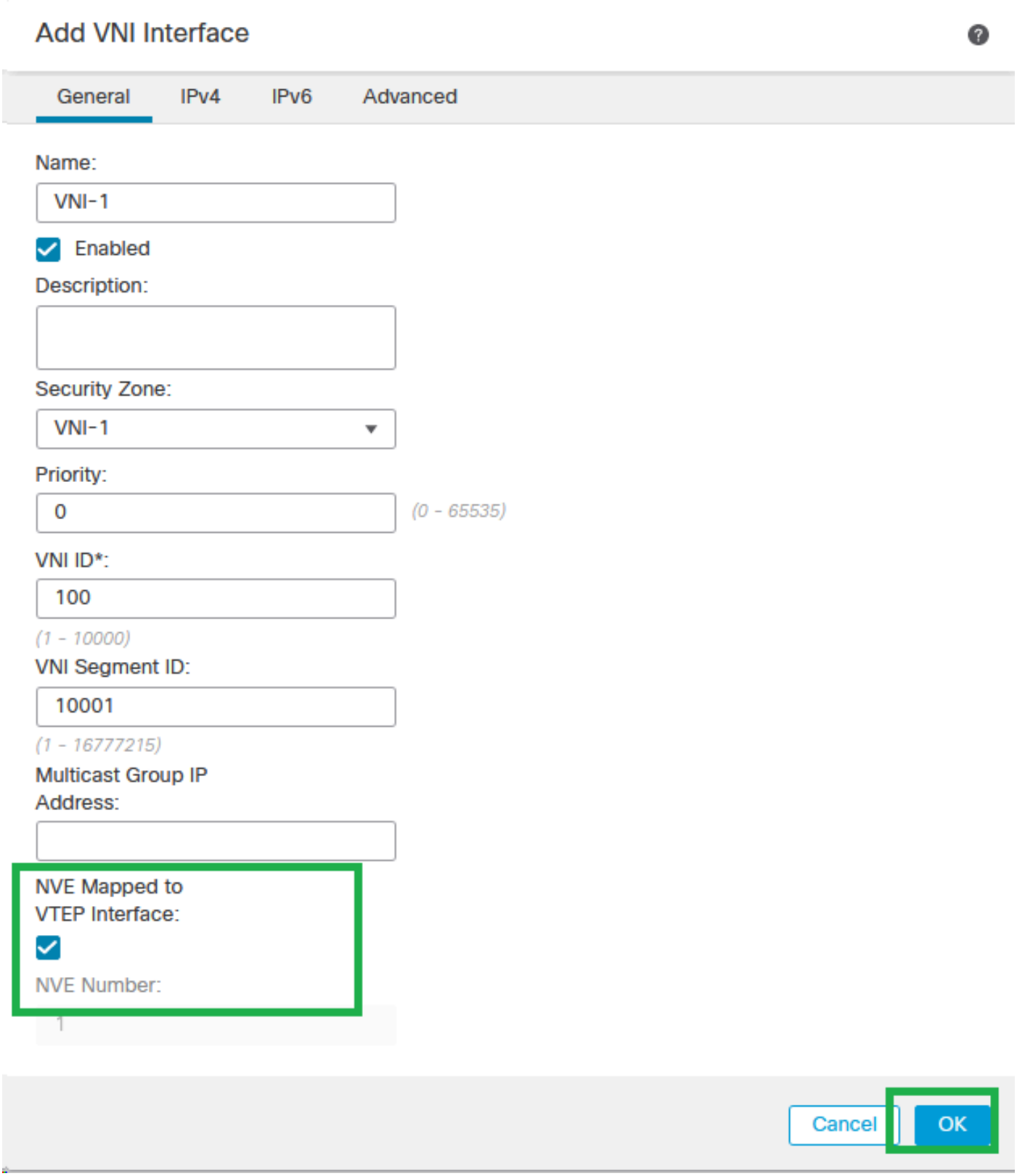


참고: VNI ID는 1에서 10000 사이로 구성되고 VNI 세그먼트 ID는 1에서 16777215 사이로 구성됩니다(세그먼트 ID는 VXLAN 태깅에 사용됨).



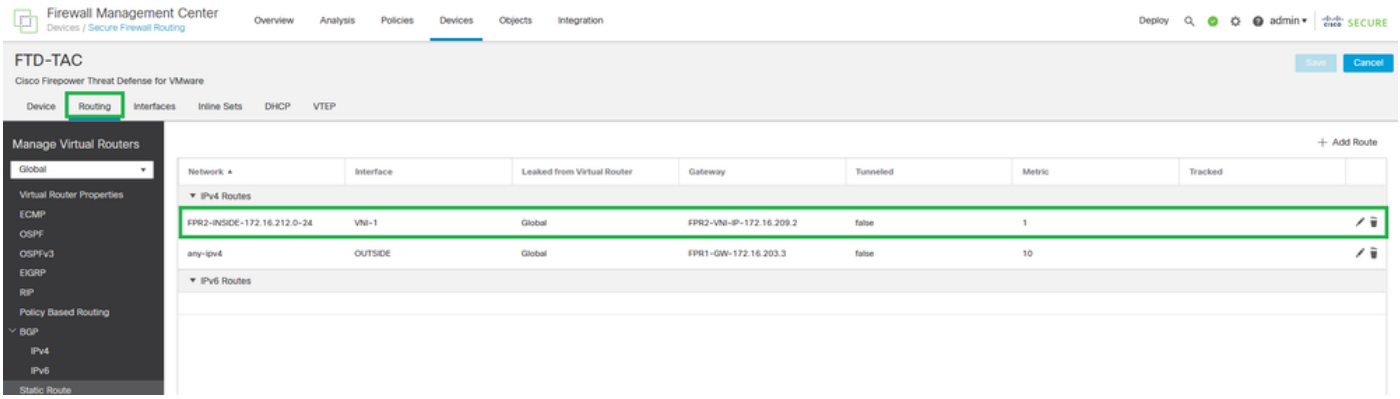
주의: 멀티캐스트 그룹이 VNI 인터페이스에 구성되지 않은 경우 VTEP 소스 인터페이스 컨피그레이션의 기본 그룹이 사용 가능한 경우 사용됩니다. VTEP 소스 인터페이스에 대해 VTEP 피어 IP를 수동으로 설정하는 경우 VNI 인터페이스에 대한 멀티캐스트 그룹을 지정할 수 없습니다.

3단계: NVE Mapped to VTEP Interface(VTEP 인터페이스에 매핑된 NVE) 확인란을 선택하고 OK(확인)를 클릭합니다.

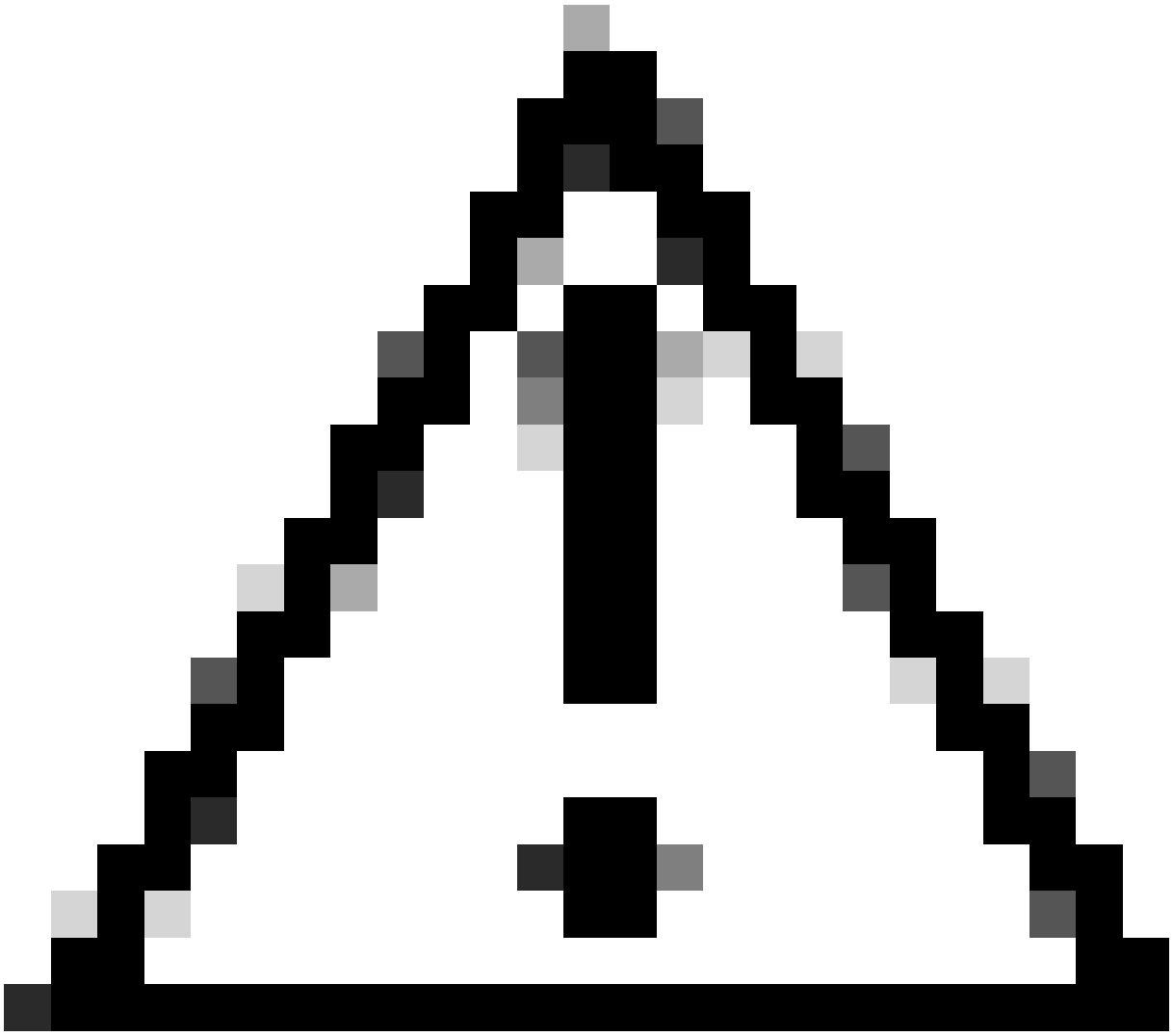


VTEP 인터페이스에 매핑된 NVE

4단계: VXLAN용 목적지 네트워크를 VNI 피어 인터페이스에 광고하도록 고정 경로를 구성합니다. Routing(라우팅) > Static Route(고정 경로)로 이동합니다.

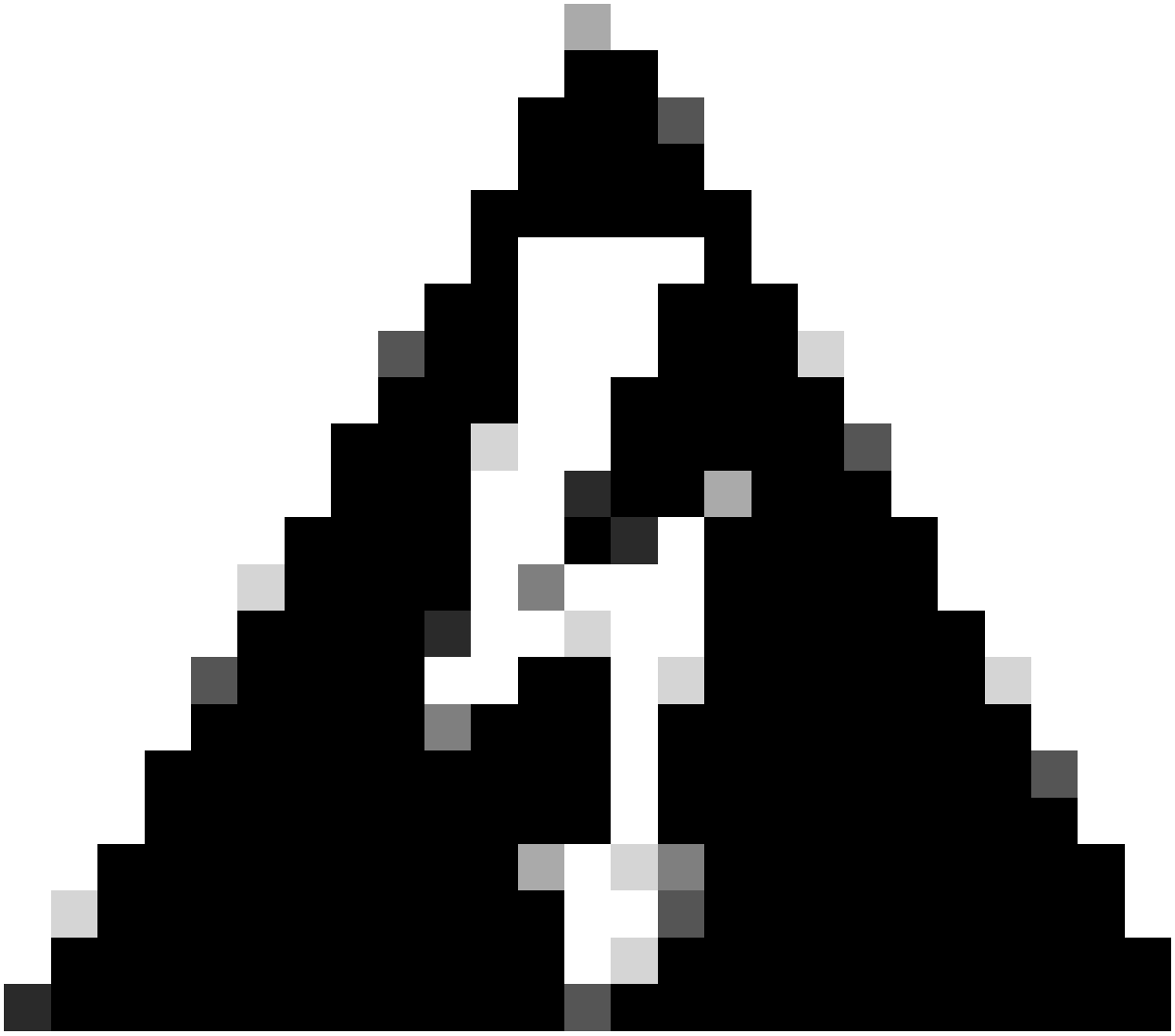


고정 경로 컨피그레이션



주의: VXLAN에 대한 대상 네트워크는 피어 VNI 인터페이스를 통해 전송해야 합니다. 모든 VNI 인터페이스는 동일한 브로드캐스트 도메인(논리 세그먼트)에 있어야 합니다.

5단계: 변경 사항을 저장하고 구축합니다.



경고: 구축 전에 검증 경고가 표시될 수 있습니다. 물리적 VTEP 소스 인터페이스에서 VTEP 피어 IP 주소에 연결할 수 있는지 확인하십시오.

다음을 확인합니다.

NVE 컨피그레이션을 확인합니다.

```
firepower# show running-config nve
nve 1
encapsulation vxlan
source-interface OUTSIDE
peer-group FPR1-VTEP-Group-Object
```

```
firepower# show nve 1
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
```

```
IP address 172.16.203.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
1309 packets input, 128170 bytes
2009 packets output, 230006 bytes
142 packets dropped
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Configured static peer group VTEPs:
IP address 172.16.205.1 MAC address 0050.56b3.c30a (learned)
IP address 172.16.207.1 MAC address 0050.56b3.c30a (learned)
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 172.16.205.1
IP address 172.16.207.1
Number of VNIs attached to nve 1: 1
VNIs attached:
vni 100: proxy off, segment-id 10001, mcast-group none
NVE proxy single-arm channel is off.
```

```
firepower# show nve 1 summary
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Number of discovered peer VTEPs: 2
Number of VNIs attached to nve 1: 1
NVE proxy single-arm channel is off.
```

VNI 인터페이스 컨피그레이션을 확인합니다.

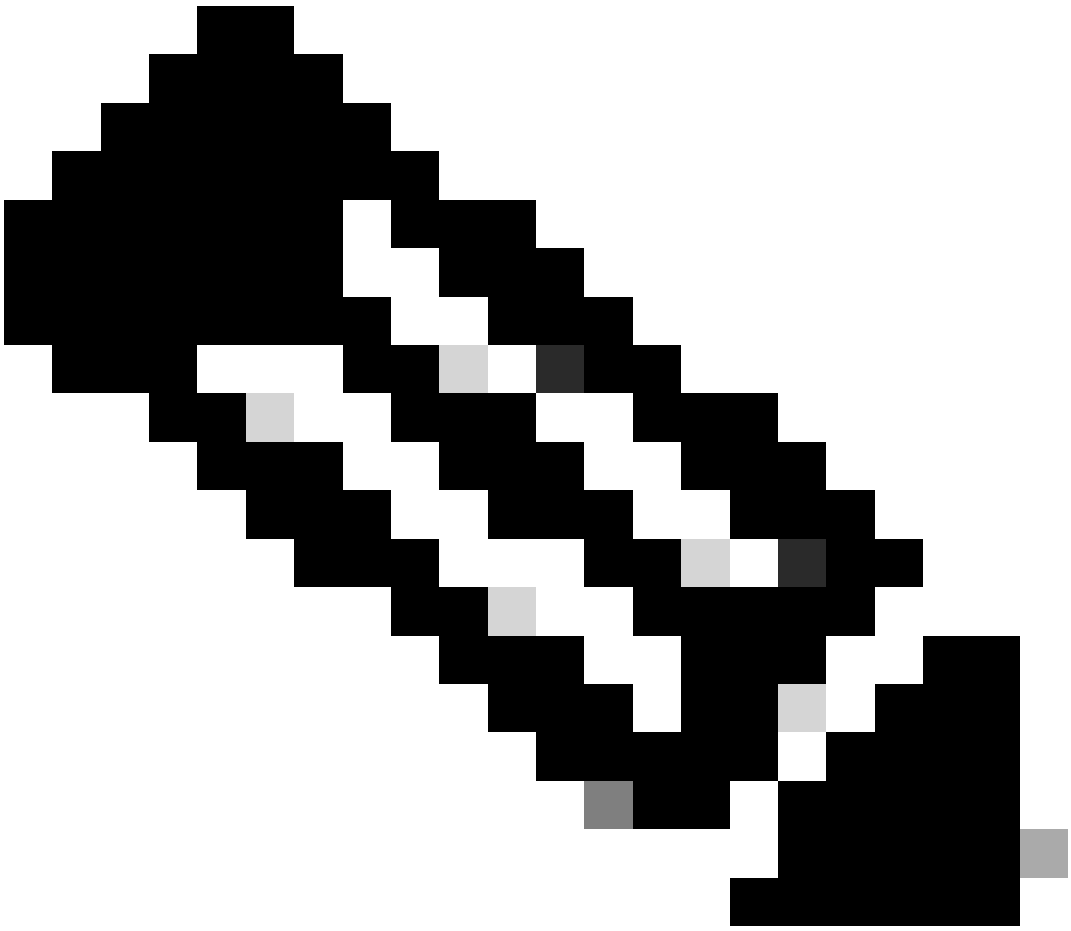
```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

VTEP 인터페이스에서 MTU 컨피그레이션을 확인합니다.

```
firepower# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0050.56b3.26b8, MTU 1554
IP address 172.16.203.1, subnet mask 255.255.255.0
---
[Output omitted]
```

대상 네트워크에 대한 고정 경로 컨피그레이션을 확인합니다.

```
firepower# show run route
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.203.3 10
route VNI-1 172.16.212.0 255.255.255.0 172.16.209.2 1
route VNI-1 172.16.215.0 255.255.255.0 172.16.209.3 1
```



참고: 모든 피어의 VNI 인터페이스가 동일한 브로드캐스트 도메인에 구성되어 있는지 확인합니다.

문제 해결

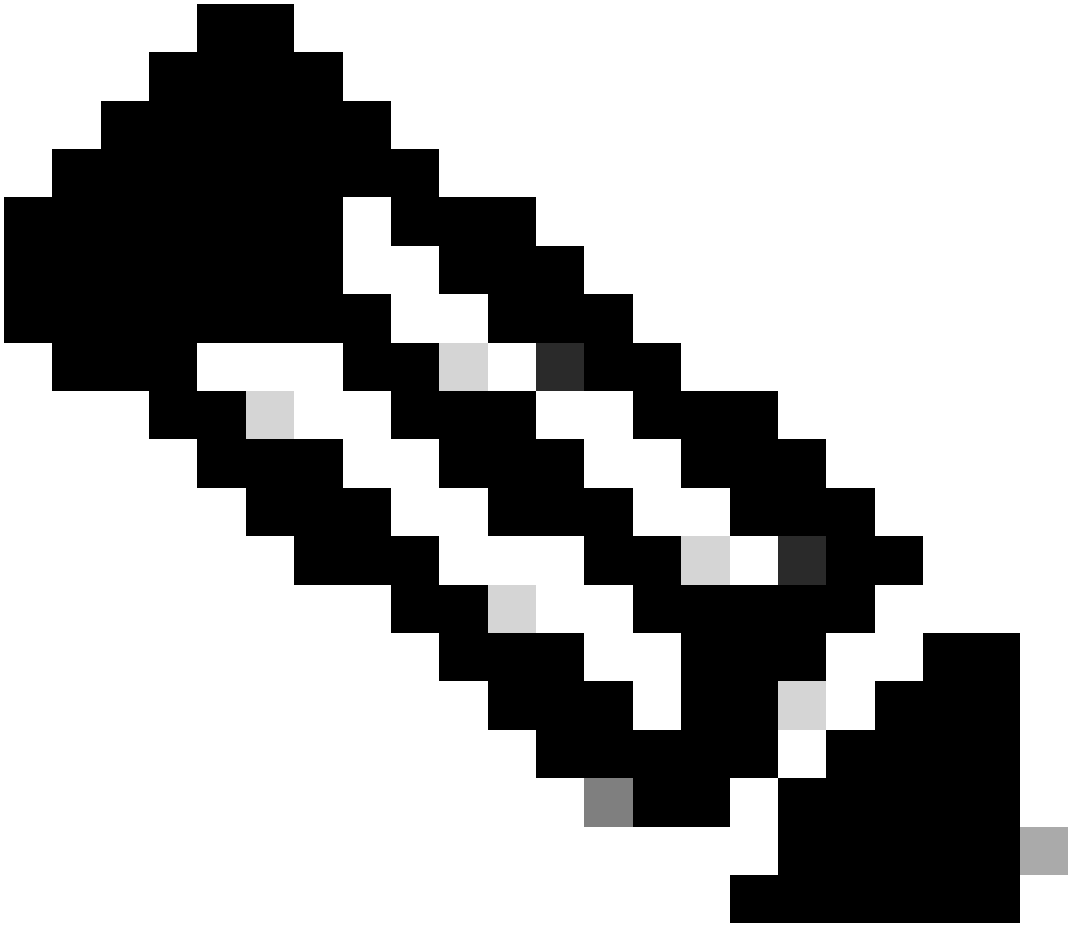
VTEP 피어와의 연결을 확인합니다.

피어 1:

```
firepower# ping 172.16.205.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.205.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

피어 2:

```
firepower# ping 172.16.207.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.207.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



참고: VTEP 피어 연결 문제는 보안 FMC에서 구축 실패를 생성할 수 있습니다. 모든 VTEP 피어 컨피그레이션에 대한 연결을 유지합니다.

VNI 피어와의 연결을 확인합니다.

.

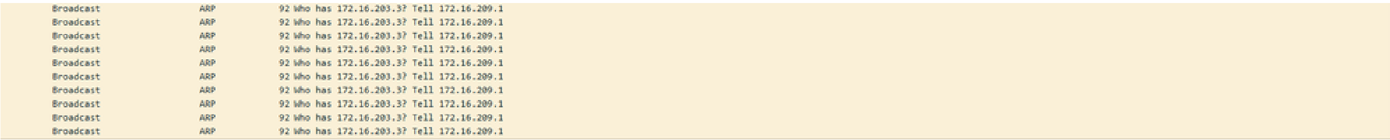
피어 1:

```
firepower# ping 172.16.209.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

피어 2:

```
firepower# ping 172.16.209.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

때로는 잘못된 고정 경로가 구성되어 ARP 불완전 출력을 생성할 수 있습니다. VTEP 인터페이스에서 VXLAN 패킷에 대한 캡처를 구성하고 pcap 형식으로 다운로드합니다. 모든 패킷 분석기 툴을 사용하면 경로에 문제가 있는지 확인할 수 있습니다. VNI 피어 IP 주소를 게이트웨이로 사용해야 합니다.



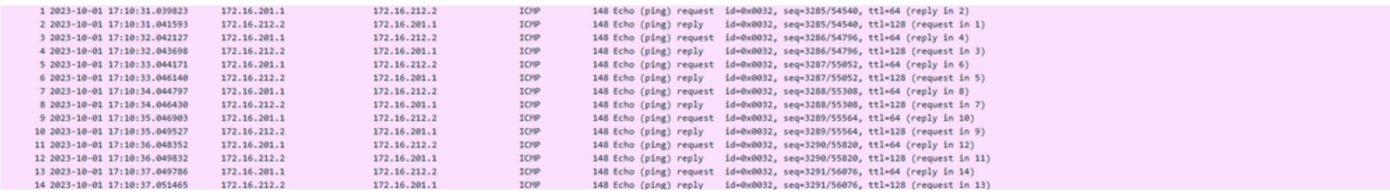
라우팅 문제

방화벽 삭제 시 Secure FTD에서 ASP 삭제 캡처를 구성하려면 show asp drop 명령을 사용하여 ASP 삭제 카운터를 확인합니다. 분석을 위해 Cisco TAC에 문의하십시오.

VNI/VTEP 인터페이스에서 VXLAN UDP 트래픽을 허용하도록 액세스 제어 정책 규칙을 구성해야 합니다.

VXLAN 패킷이 프래그먼트화될 수 있는 경우도 있습니다. 프래그먼트화를 방지하기 위해 MTU를 언더레이 네트워크에서 점보 프레임으로 변경해야 합니다.

Ingress/VTEP 인터페이스에서 캡처를 구성하고 분석을 위해 .pcap 형식으로 캡처를 다운로드합니다. 패킷은 VTEP 인터페이스에 VXLAN 헤더를 포함해야 합니다.



VXLAN 헤더로 Ping 캡처

VXLAN 헤더

관련 정보

- VXLAN 인터페이스 구성
- VXLAN 활용 사례
- VXLAN 패킷 처리
- VTEP 소스 인터페이스 구성
- VNI 인터페이스 구성
- Cisco 기술 지원 및 다운로드

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.