FDM에서 관리하는 FTD에서 고정 경로를 사용하여 경로 기반 VPN 구성

목차

소개

이 문서에서는 FDM에서 관리하는 FTD에서 고정 경로 기반 사이트 대 사이트 VPN 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- VPN 터널의 작동 방식에 대한 기본 이해
- FDM(Firepower 장치 관리자) 탐색에 대한 사전 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

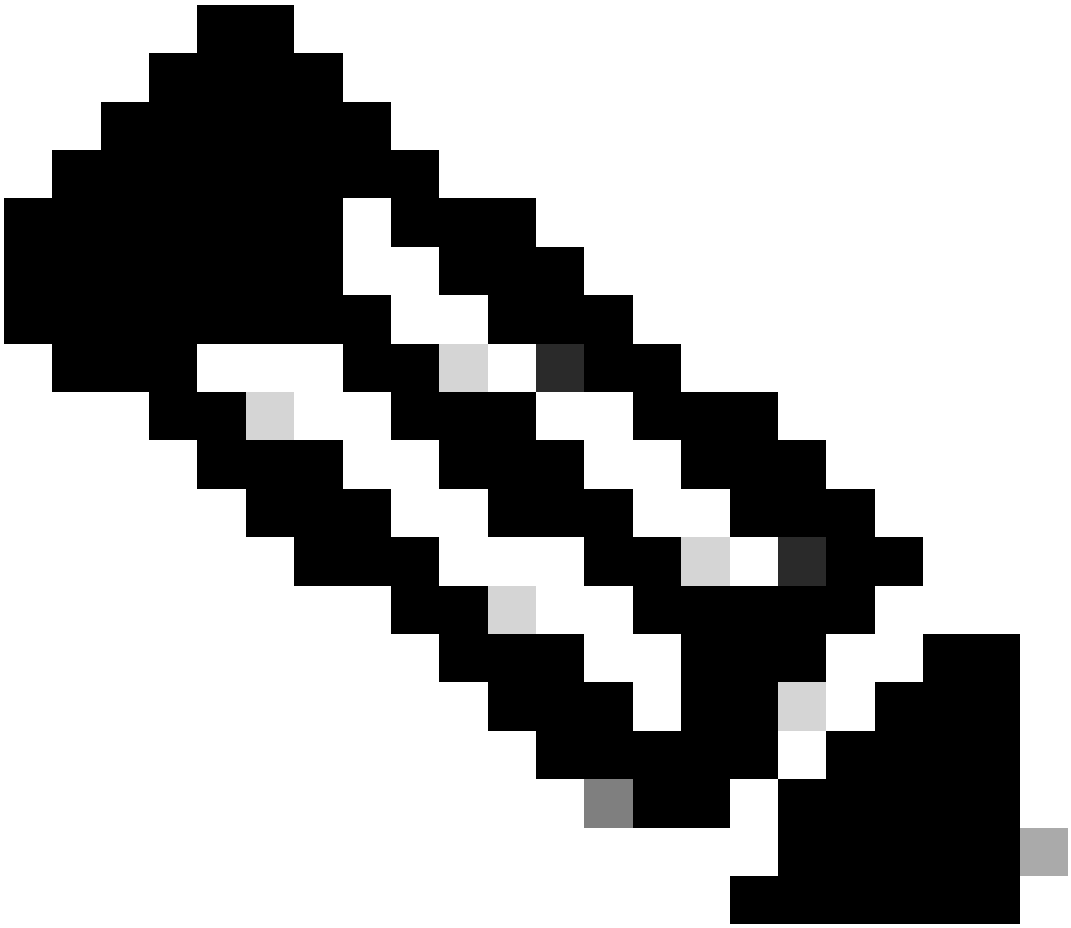
- Cisco FTD(Firepower Threat Defense) 버전 7.0은 FDM(Firepower Device Manager)에서 관리됩니다.

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

경로 기반 VPN을 사용하면 VPN 터널을 통해 보내거나 암호화할 흥미로운 트래픽을 결정할 수 있으며, 정책 기반 또는 암호화 맵 기반 VPN에서처럼 정책/액세스 목록 대신 트래픽 라우팅을 사용할 수 있습니다. 암호화 도메인은 IPsec 터널로 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPsec 로컬 및 원격 트래픽 선택기는 0.0.0.0/0.0.0.0으로 설정됩니다. 이는 IPsec 터널로 라우팅되는 모든 트래픽이 소스/대상 서브넷에 관계없이 암호화됨을 의미합니다.

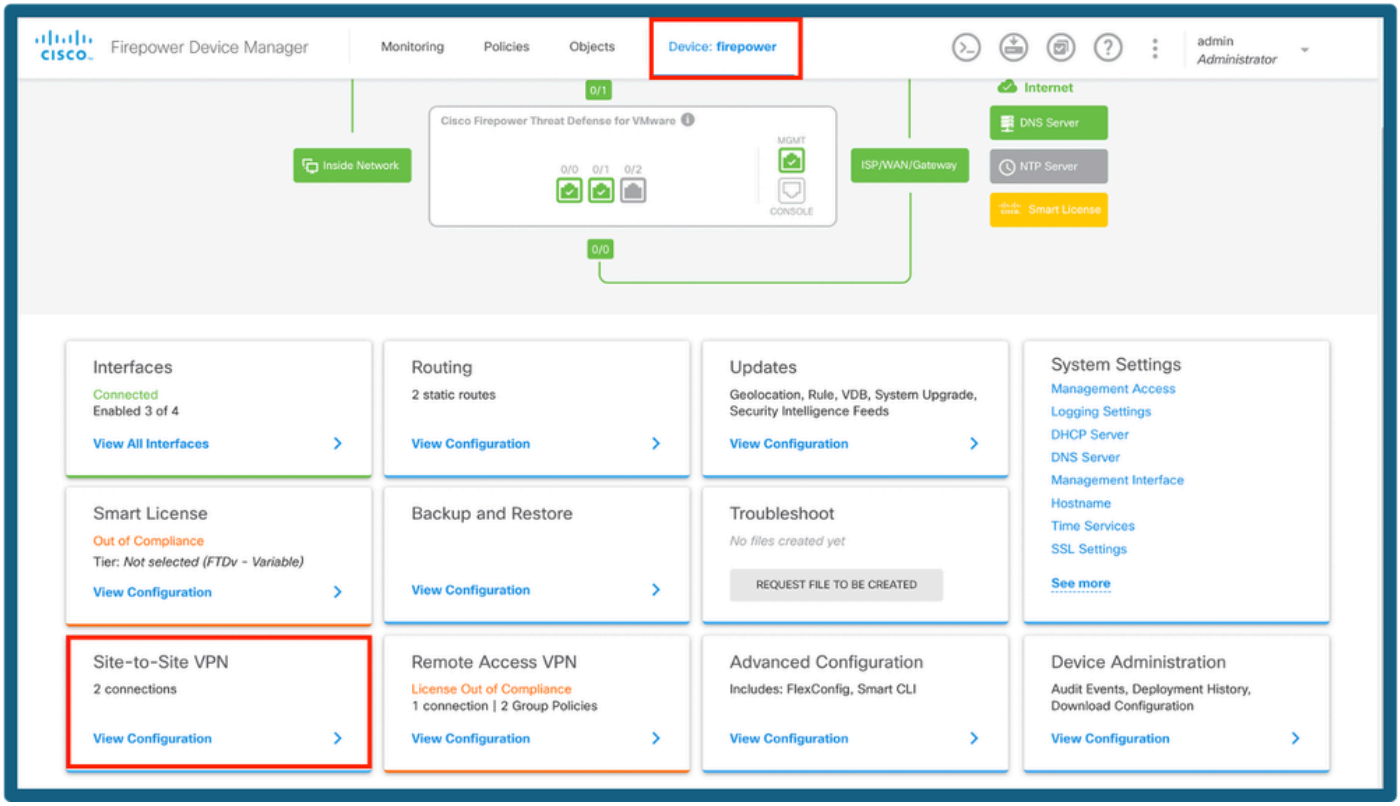
이 문서에서는 SVTI(Static Virtual Tunnel Interface) 컨피그레이션에 대해 중점적으로 설명합니다.



참고: 추가 라이선스가 필요하지 않으며, 경로 기반 VPN을 라이선스 및 평가 모드로 구성할 수 있습니다. 암호화 규정 준수(Export Controlled Features Enabled)가 없으면 DES만 암호화 알고리즘으로 사용할 수 있습니다.

FDM의 구성 단계

1단계. Device(디바이스) > Site To Site(사이트 대 사이트)로 이동합니다.



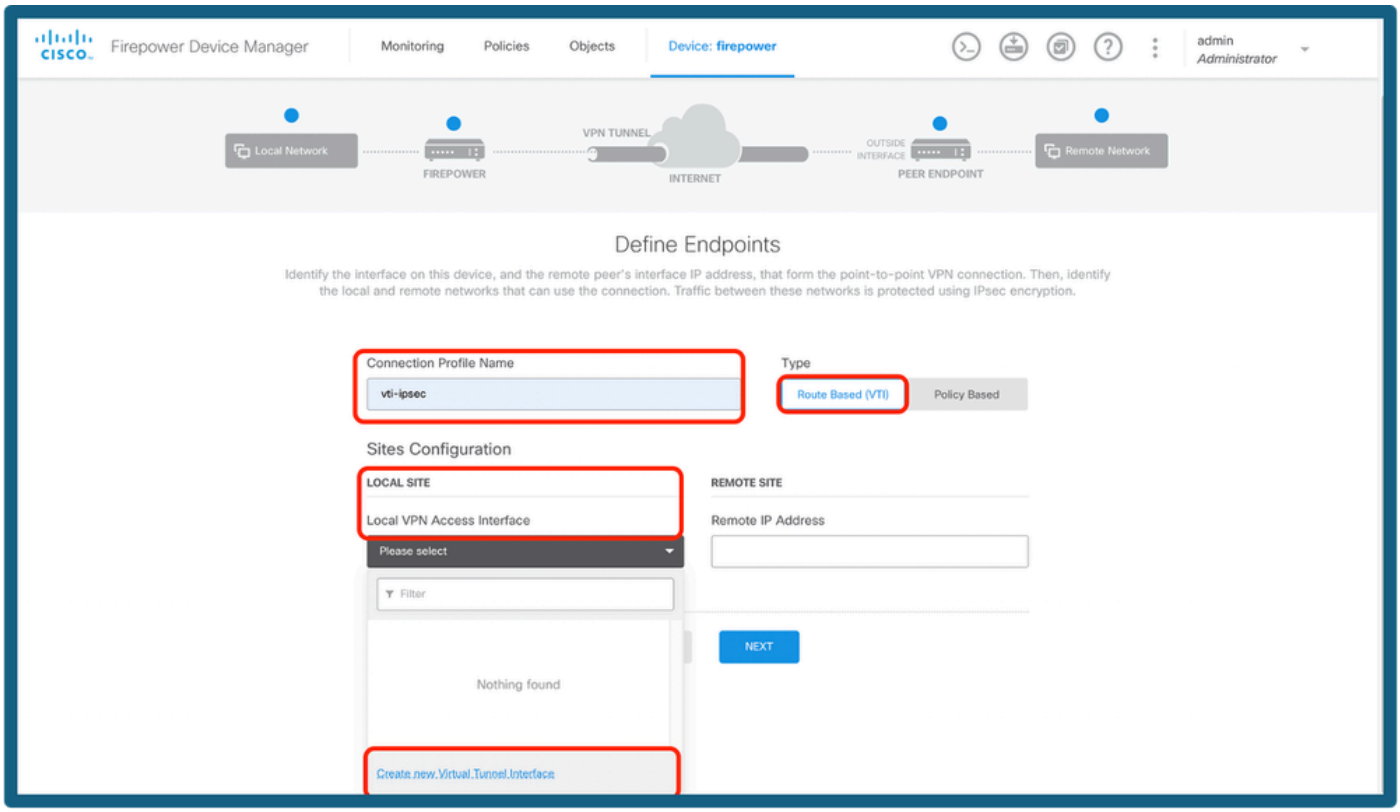
FDM 대시보드

2단계. + 아이콘을 클릭하여 사이트에 새 사이트를 추가합니다.

S2S 연결 추가

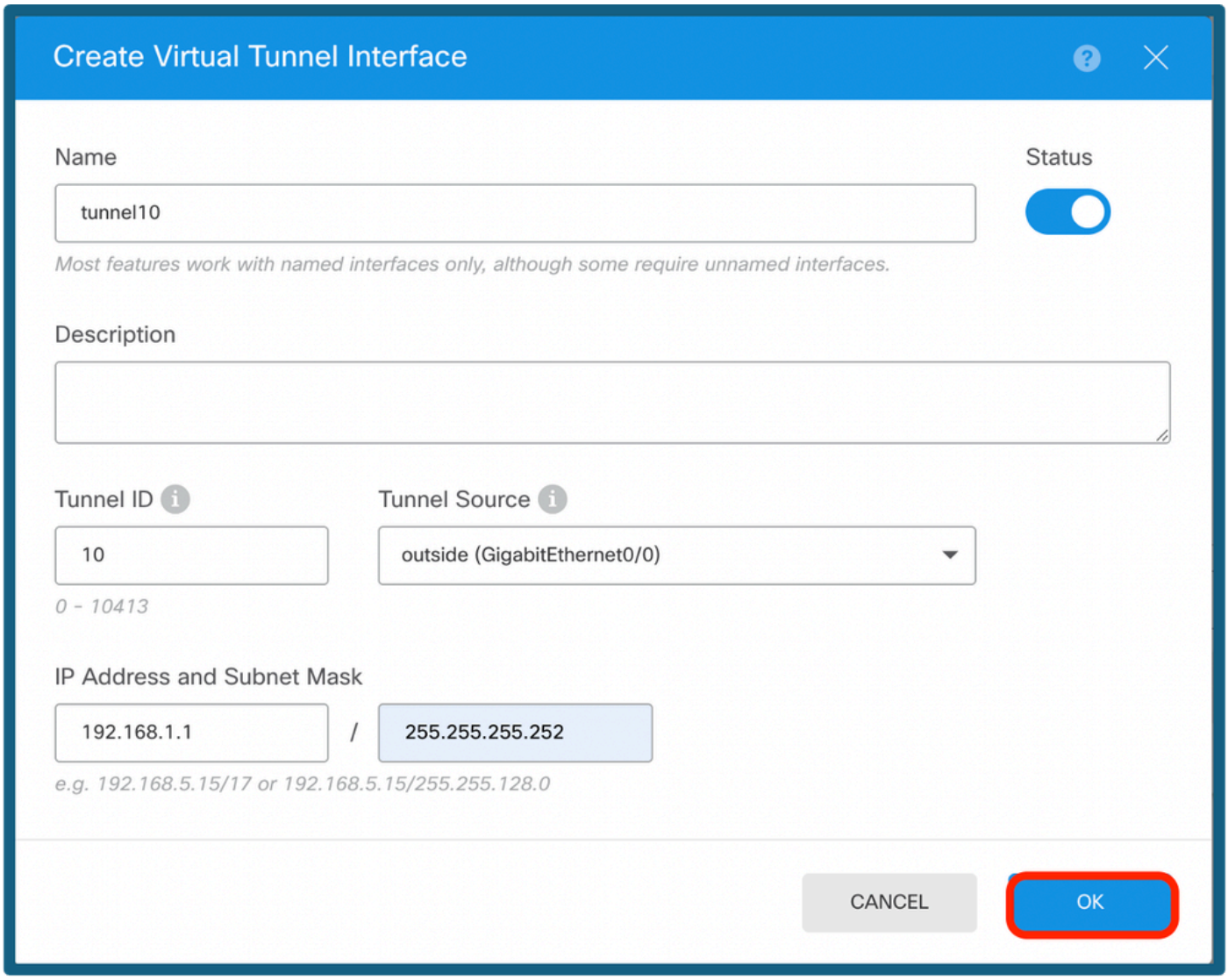
3단계. Topology Name(토폴로지 이름)을 제공하고 Type of VPN as Route Based (VTI)를 선택합니다.

Local VPN Access Interface(로컬 VPN 액세스 인터페이스)를 클릭한 다음 Create new Virtual Tunnel Interface(새 가상 터널 인터페이스 생성)를 클릭하거나 기존 목록에서 하나를 선택합니다.



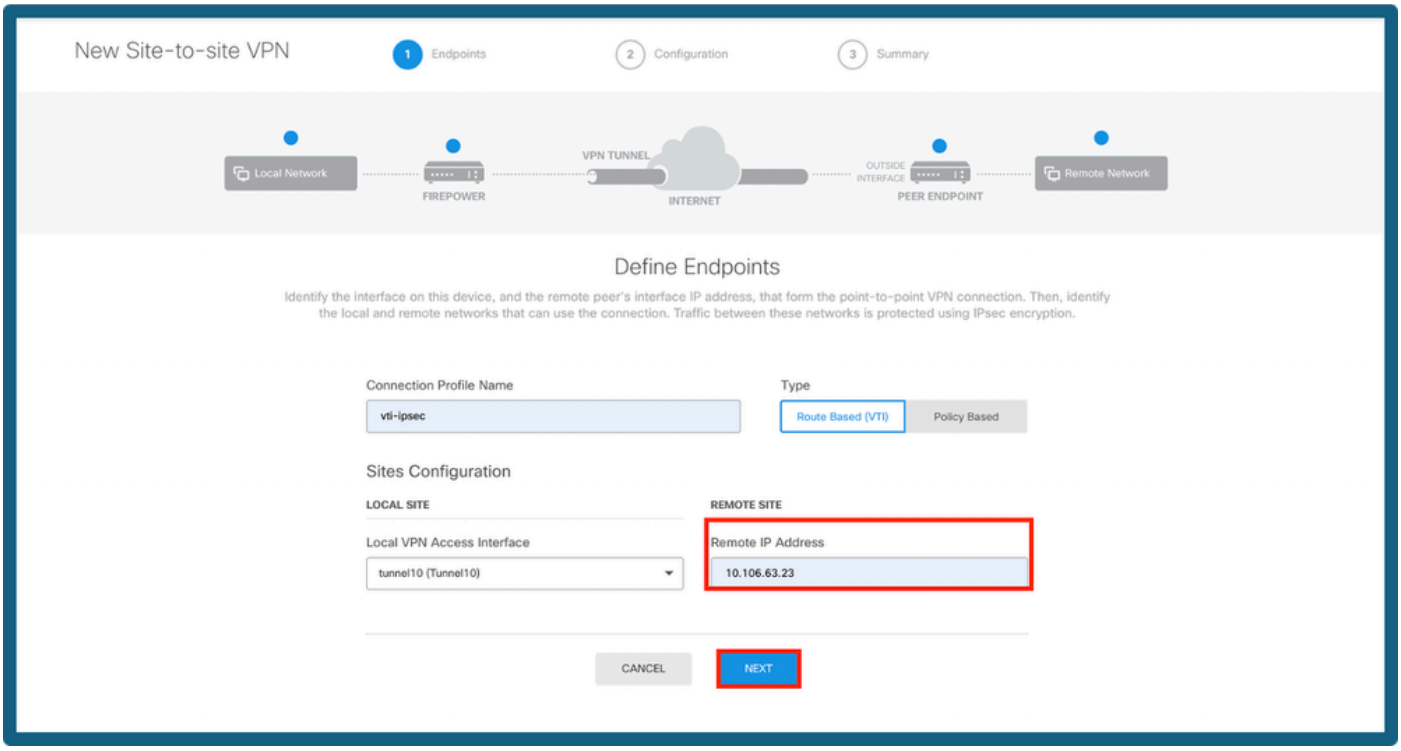
터널 인터페이스 추가

4단계. 새 가상 터널 인터페이스의 매개변수를 정의합니다. OK(확인)를 클릭합니다.



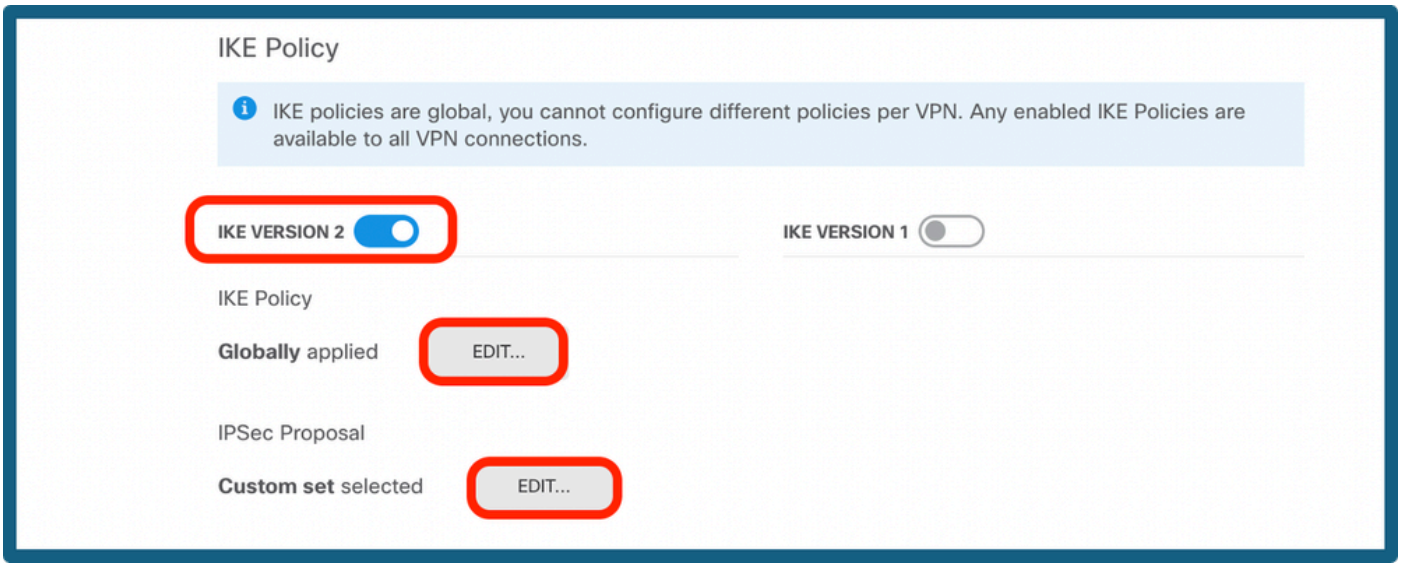
VTI 컨피그레이션

5단계. 새로 생성된 VTI 또는 가상 터널 인터페이스에 있는 VTI를 선택합니다. 원격 IP 주소를 제공합니다.



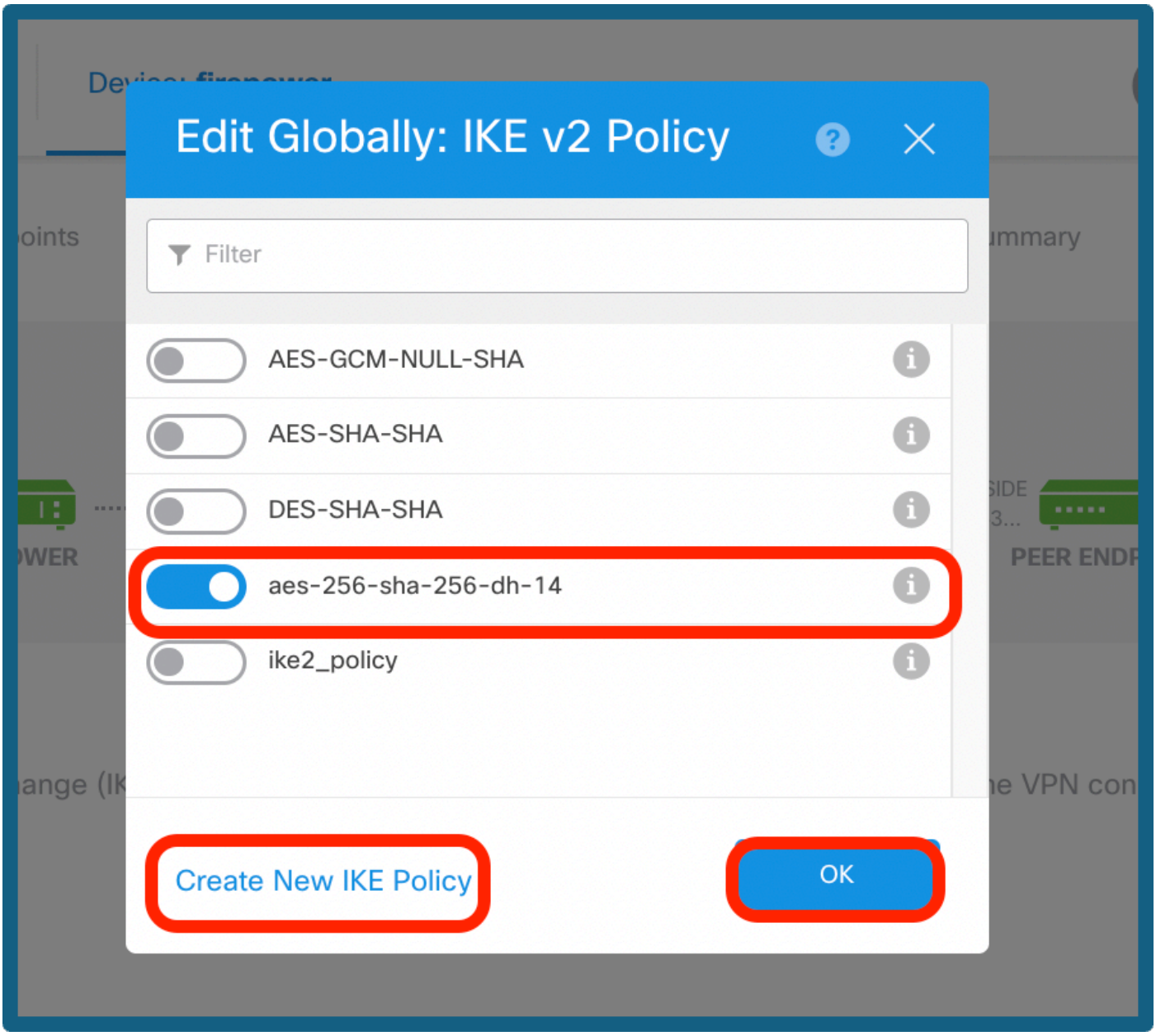
피어 IP 추가

6단계. IKE Version(IKE 버전)을 선택하고 Edit(편집) 버튼을 선택하여 이미지에 표시된 IKE 및 IPsec 매개변수를 설정합니다.

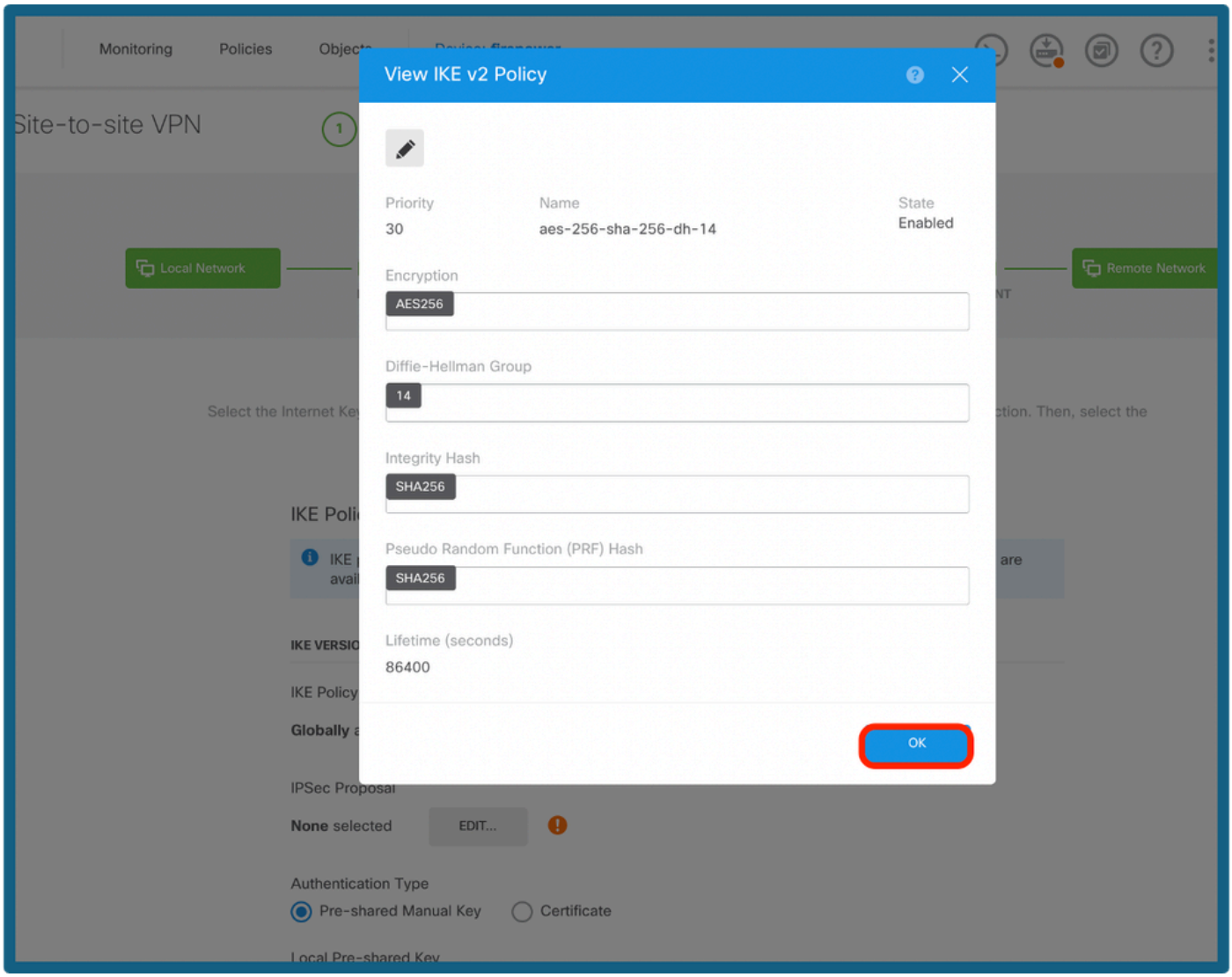


IKE 버전 구성

7a단계. 이미지에 표시된 대로 IKE Policy(IKE 정책) 버튼을 선택하고 확인 버튼 또는 Create New IKE Policy(새 IKE 정책 생성)를 클릭합니다.

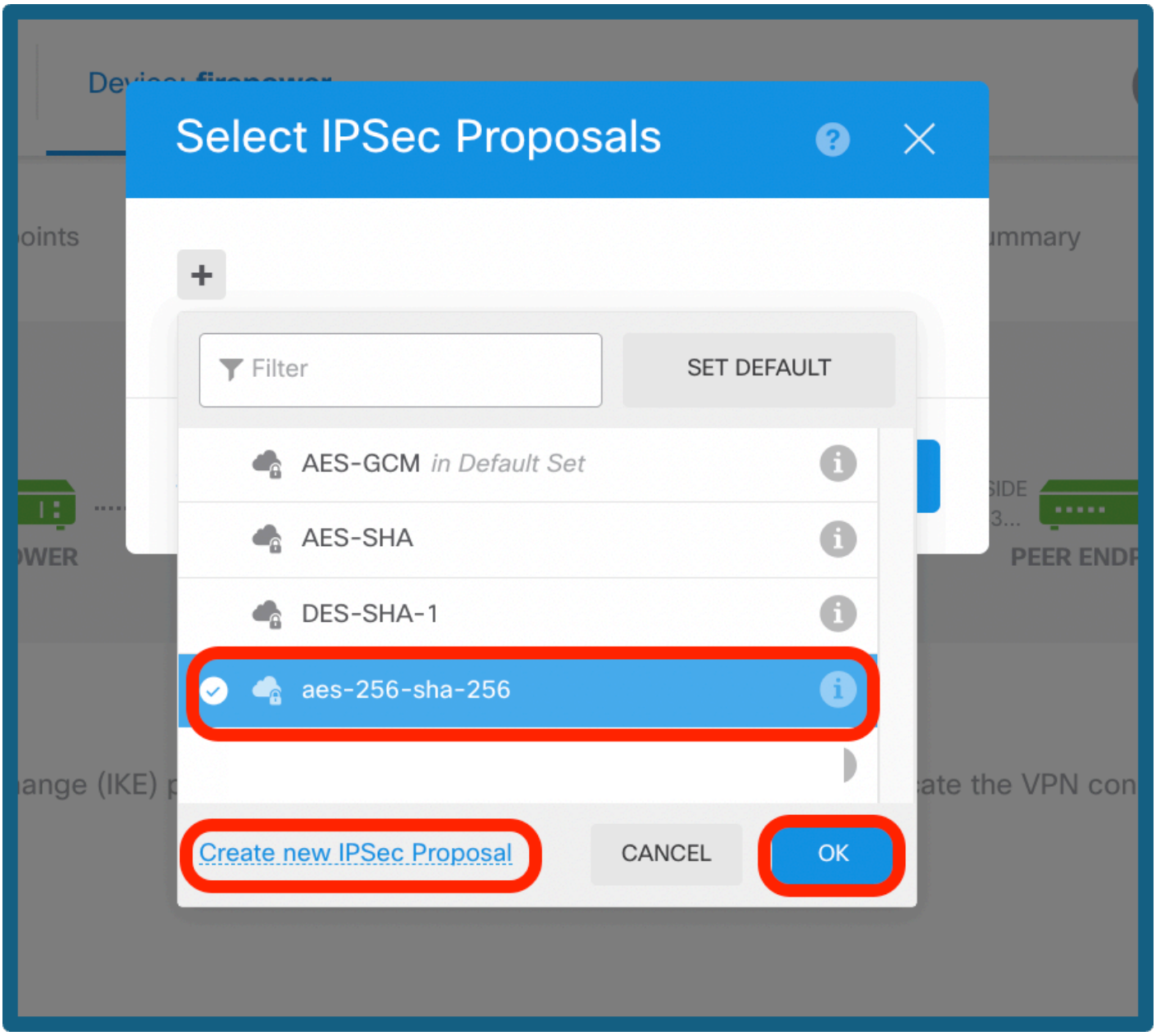

Edit Globally: IKE v2 Policy
Filter
AES-GCM-NULL-SHA
AES-SHA-SHA
DES-SHA-SHA
aes-256-sha-256-dh-14
ike2_policy
Create New IKE Policy
OK

IKE 정책 선택

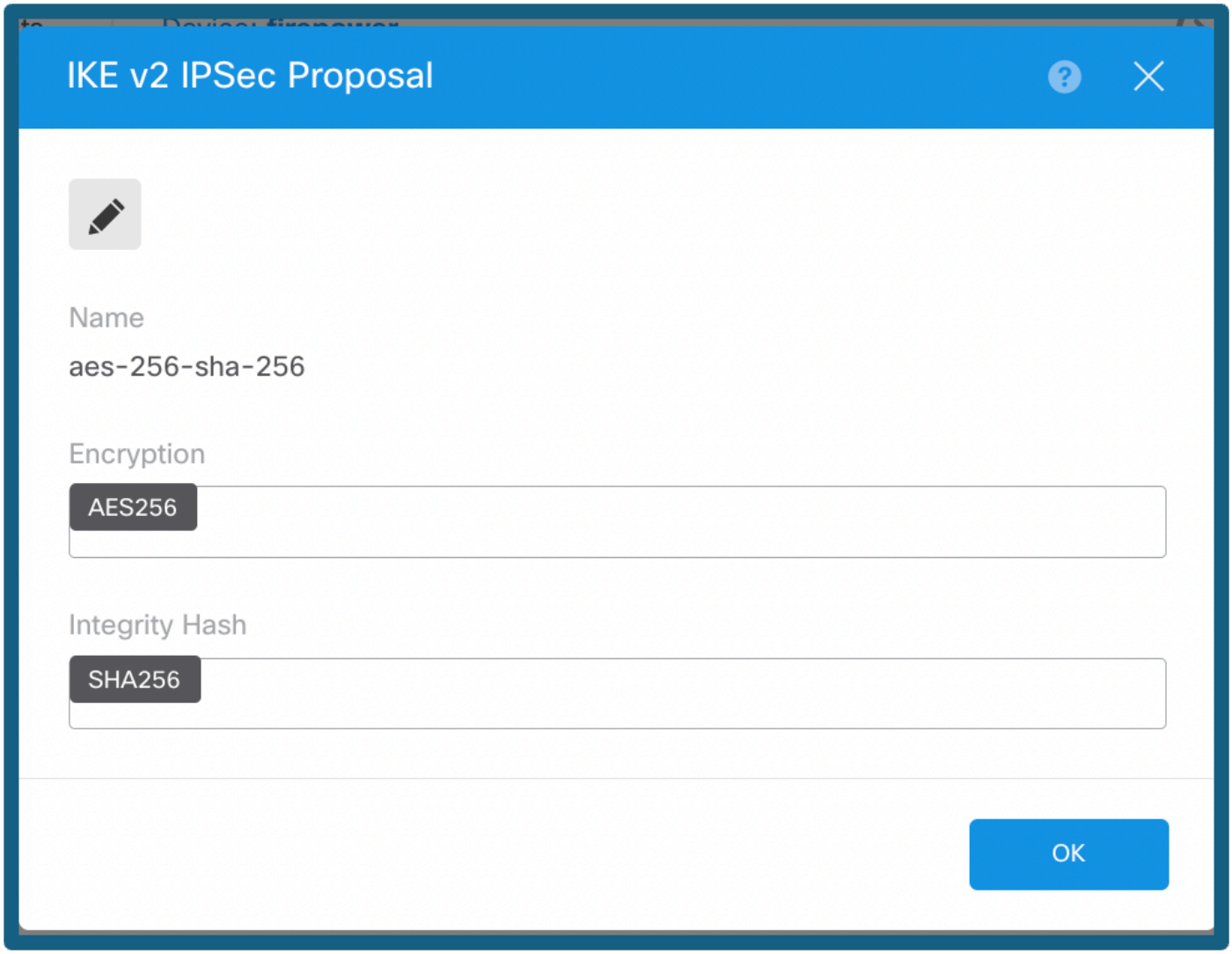


IKE 정책 구성

7b단계. 이미지에 표시된 대로 IPSec Policy(IPSec 정책) 버튼을 선택하고 ok(확인) 버튼 또는 Create New IPsec Proposal(새 IPsec 제안 생성)을 클릭합니다.


Select IPSec Proposals
Filter
SET DEFAULT
AES-GCM in Default Set
AES-SHA
DES-SHA-1
aes-256-sha-256
Create new IPSec Proposal
CANCEL
OK

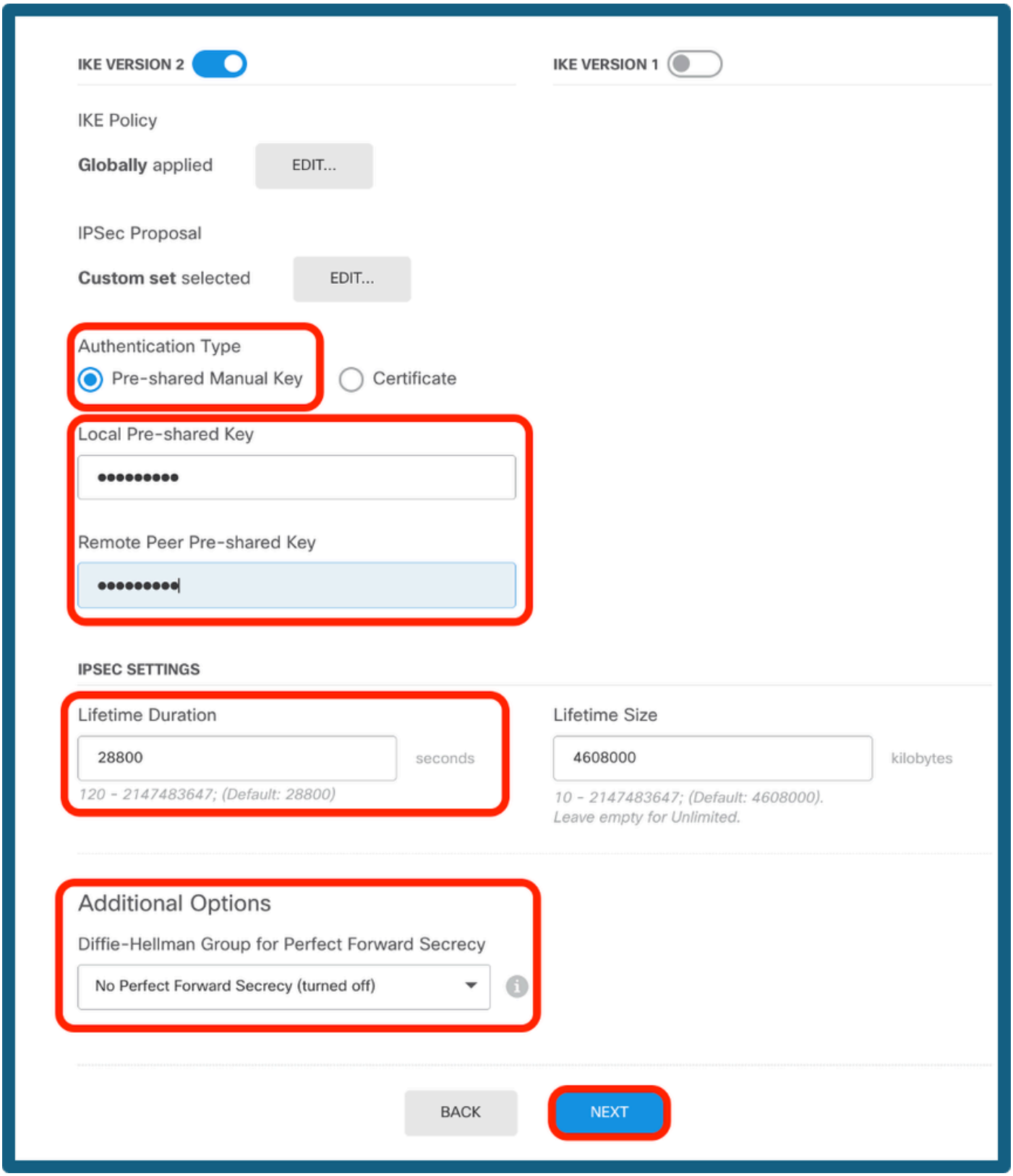
IPsec 제안 선택



IPsec 제안 구성

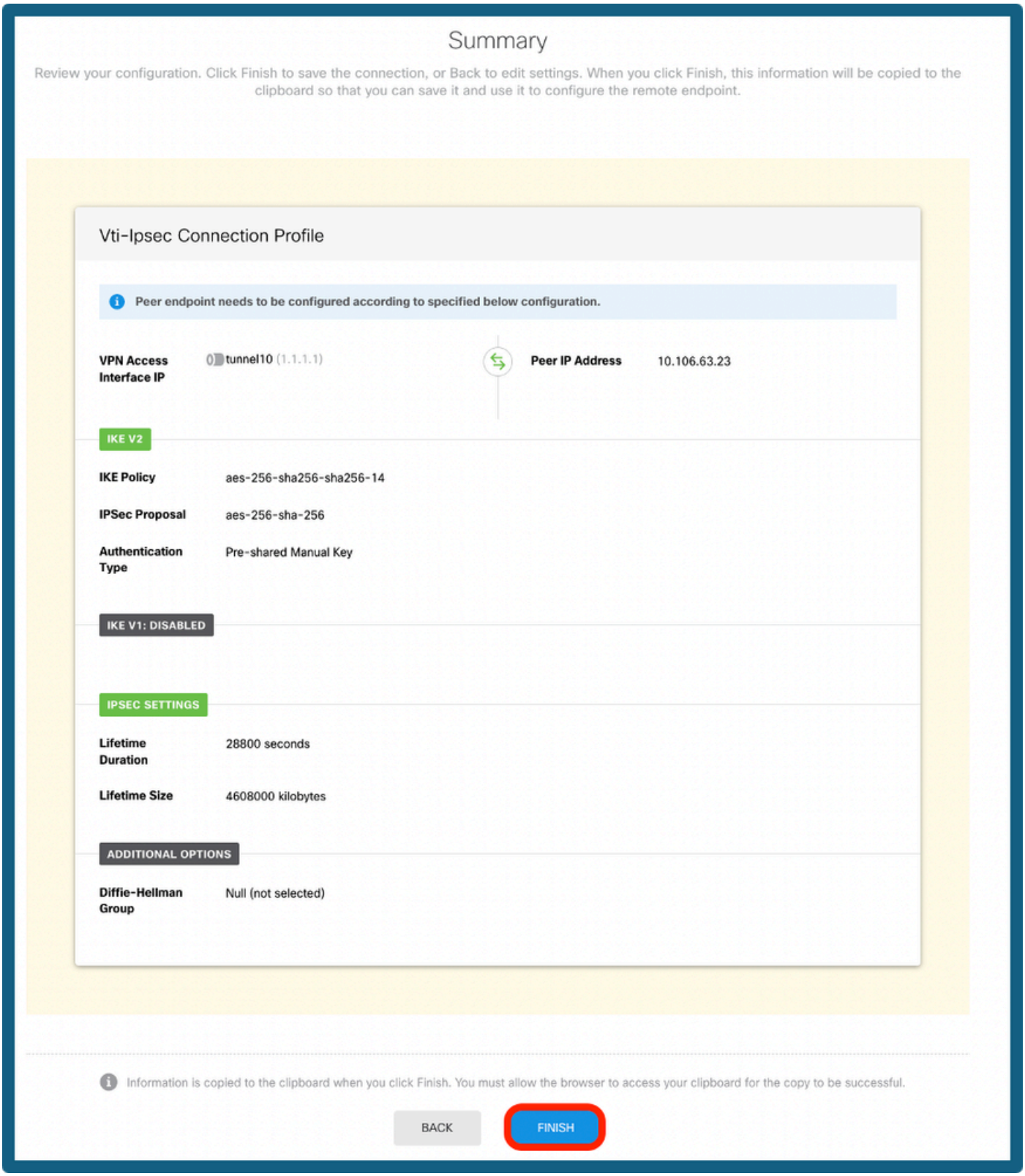
8a단계. 인증 유형을 선택합니다. 사전 공유 수동 키를 사용하는 경우 로컬 및 원격 사전 공유 키를 제공합니다.

8b단계. (선택 사항) Perfect Forward Secrecy 설정을 선택합니다. IPsec Lifetime Duration and Lifetime Size(IPsec 수명 기간 및 수명 크기)를 구성한 다음 Next(다음)를 클릭합니다.



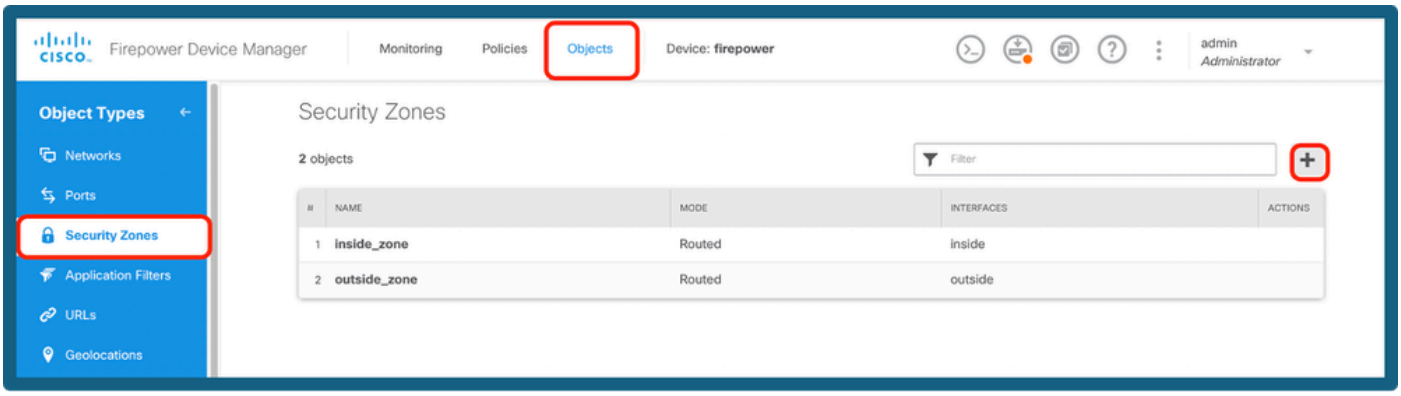
PSK 및 수명 컨피그레이션

9단계. 구성을 검토하고 Finish(마침)를 클릭합니다.



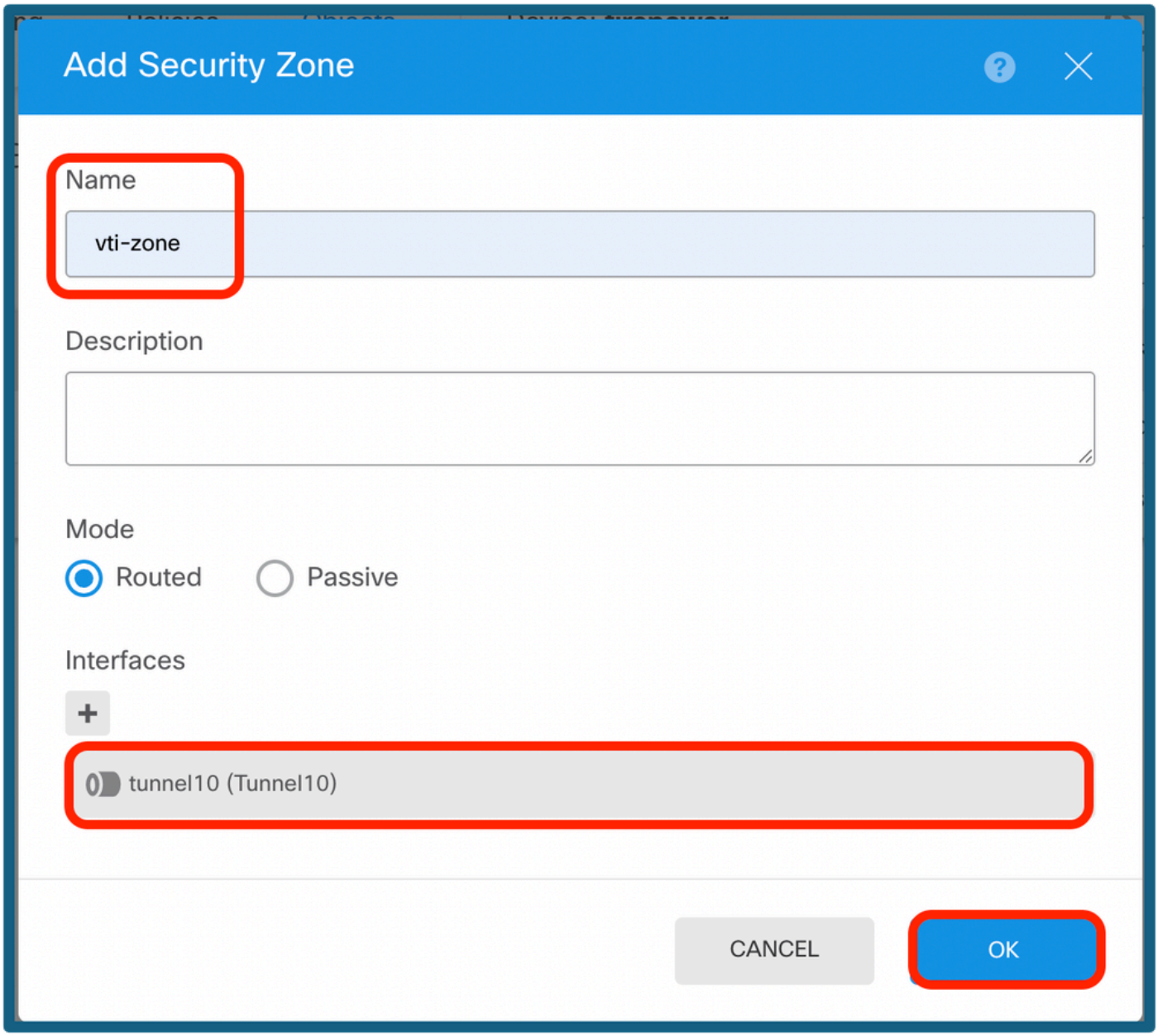
구성 요약

10a단계. Objects(개체) > Security Zones(보안 영역)로 이동한 다음 + 아이콘을 클릭합니다.



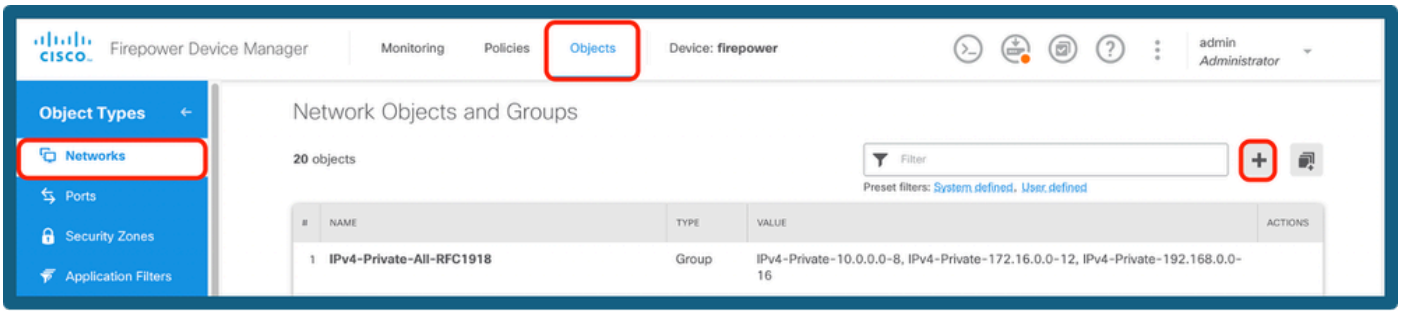
보안 영역 추가

10b단계. 영역을 생성하고 아래에 표시된 대로 VTI 인터페이스를 선택합니다.



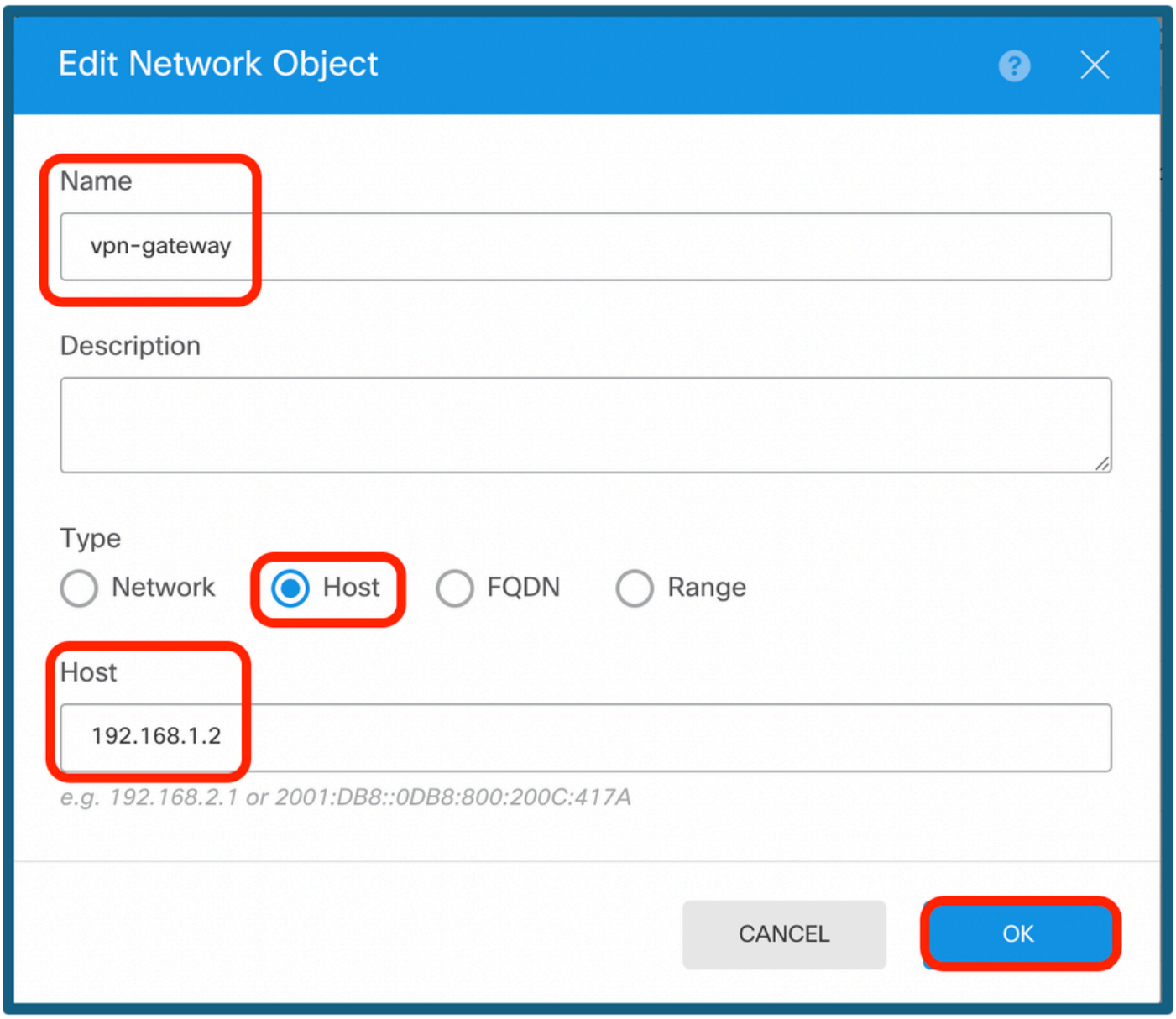
보안 영역 구성

11a단계. Objects(개체) > Networks(네트워크)로 이동하여 + 아이콘을 클릭합니다.



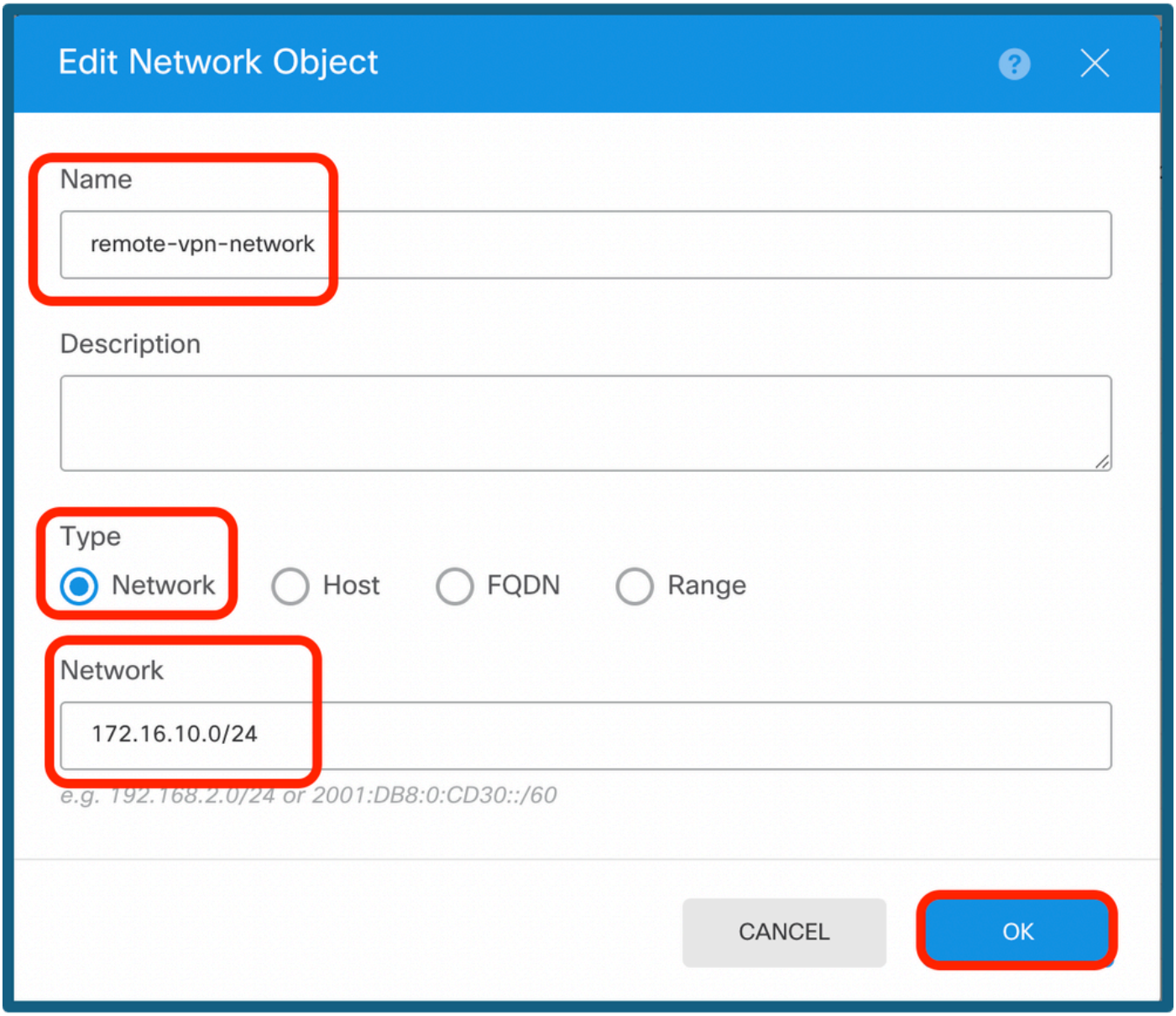
네트워크 개체 추가

11b단계. 호스트 객체를 추가하고 피어 엔드용 터널 ip를 사용하여 게이트웨이를 생성합니다.

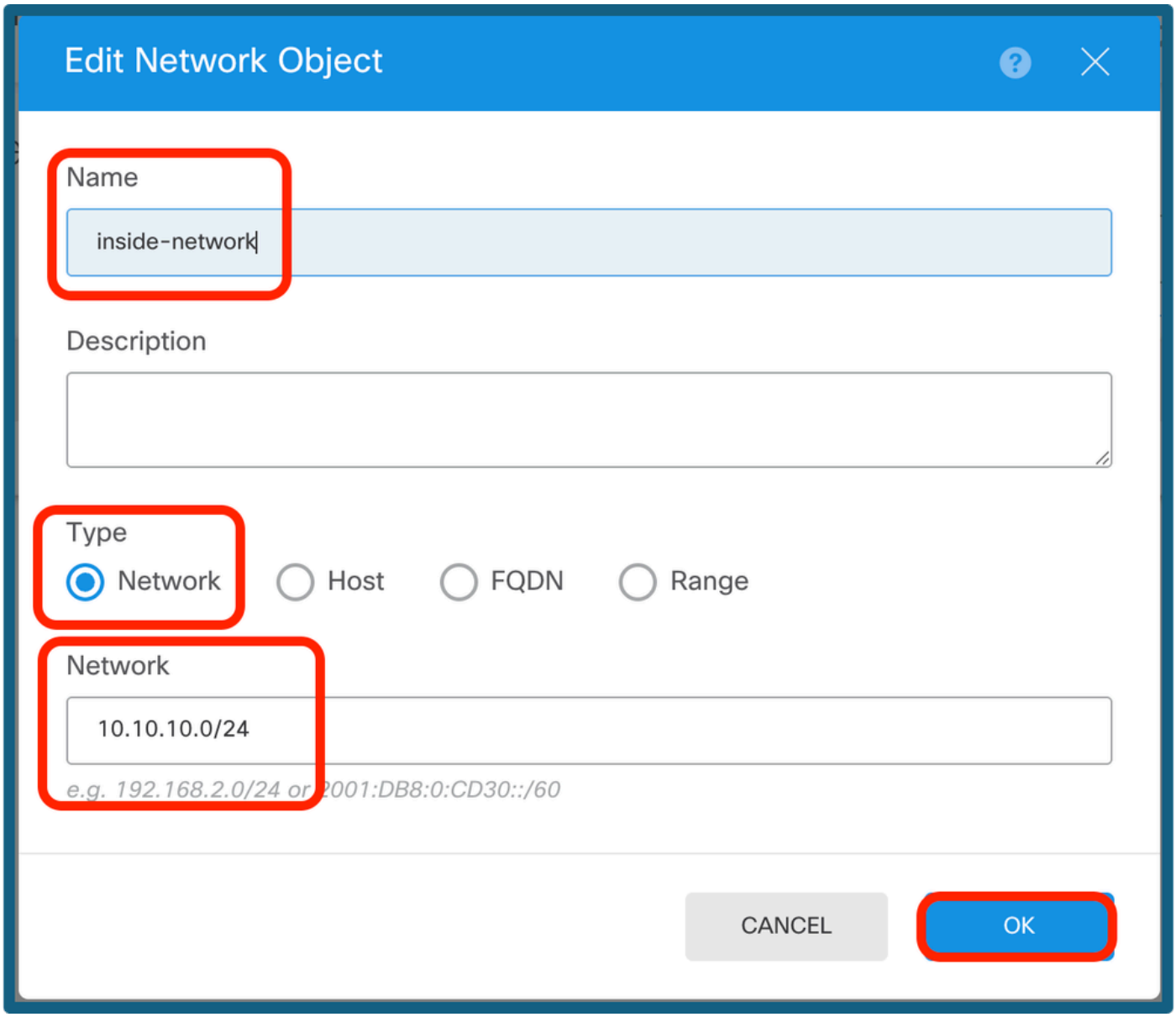


VPN 게이트웨이 구성

11c단계. 원격 서브넷 및 로컬 서브넷을 추가합니다.

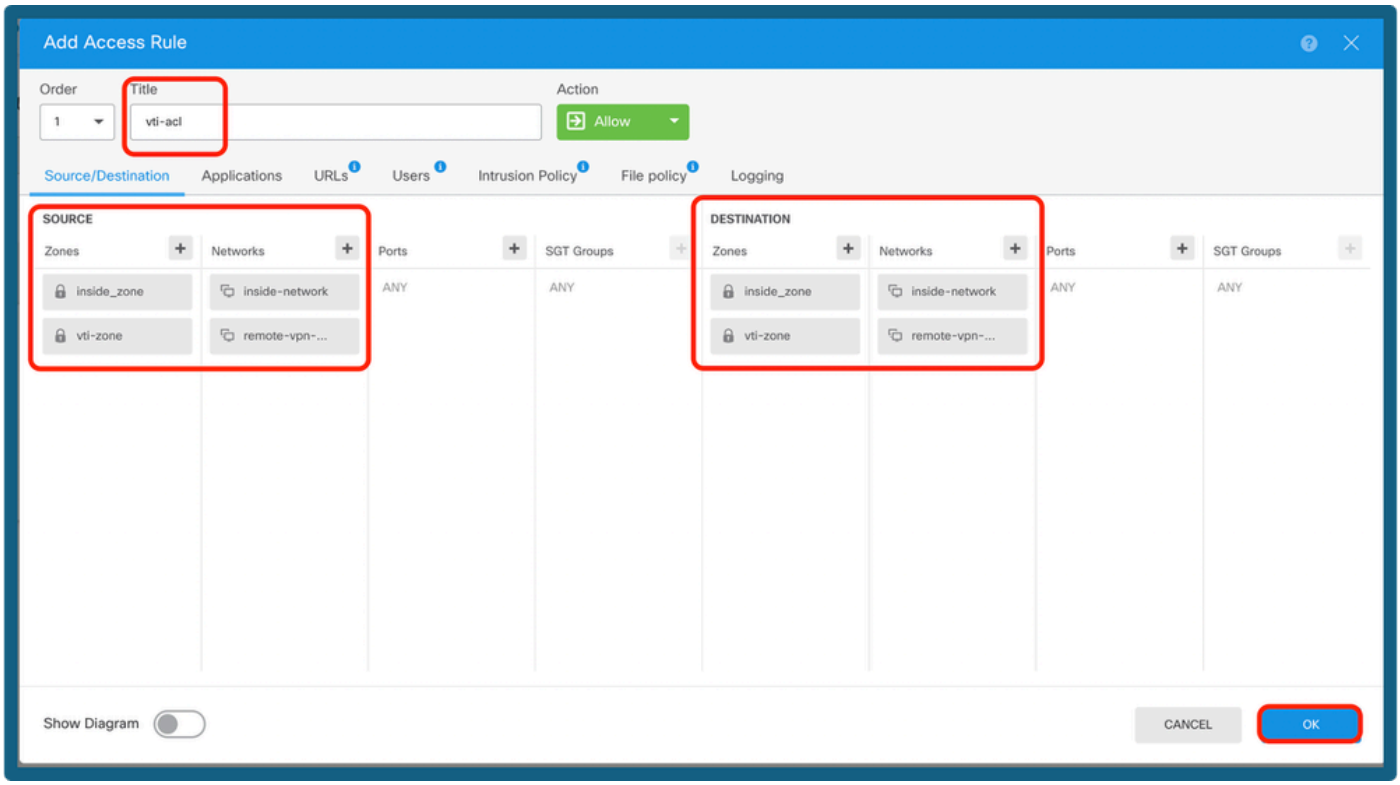

Edit Network Object
Name
remote-vpn-network
Description
Type
Network
Host
FQDN
Range
Network
172.16.10.0/24
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60
CANCEL
OK

원격 IP 컨피그레이션



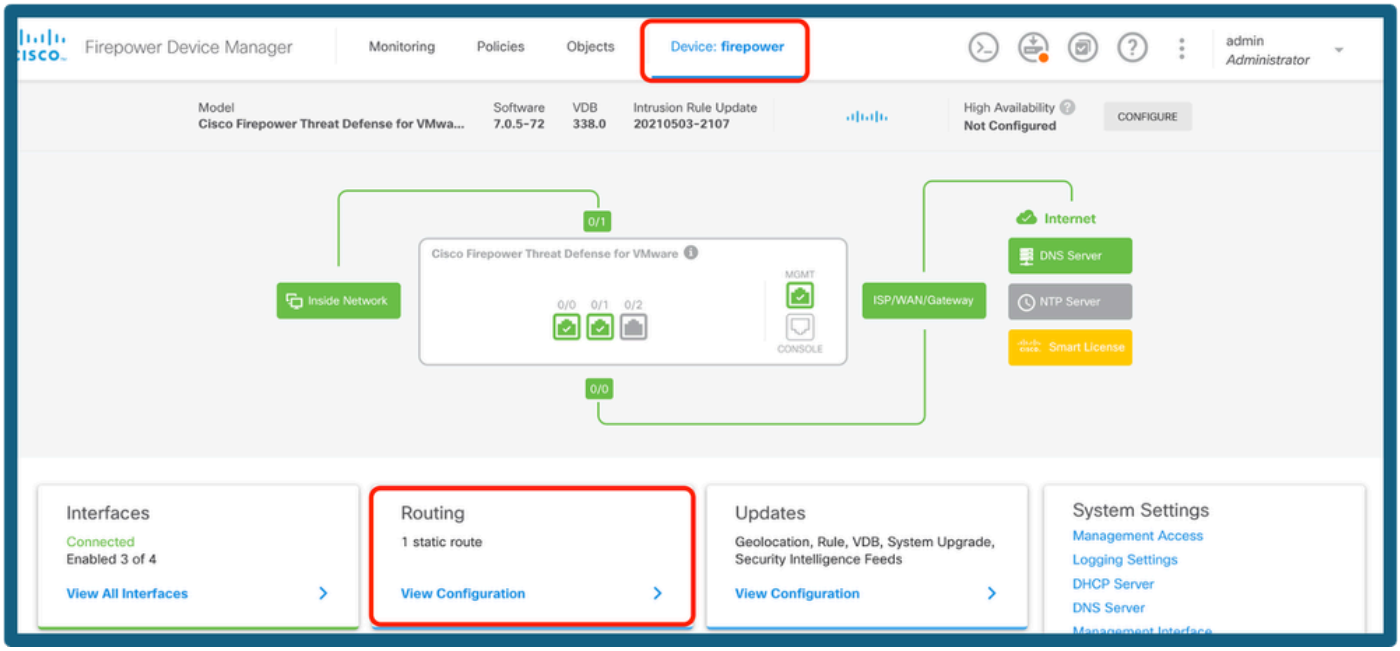
로컬 IP 컨피그레이션

12단계. Device(디바이스) > Policies(정책)로 이동하고 Access Control Policy(액세스 제어 정책)를 구성합니다.



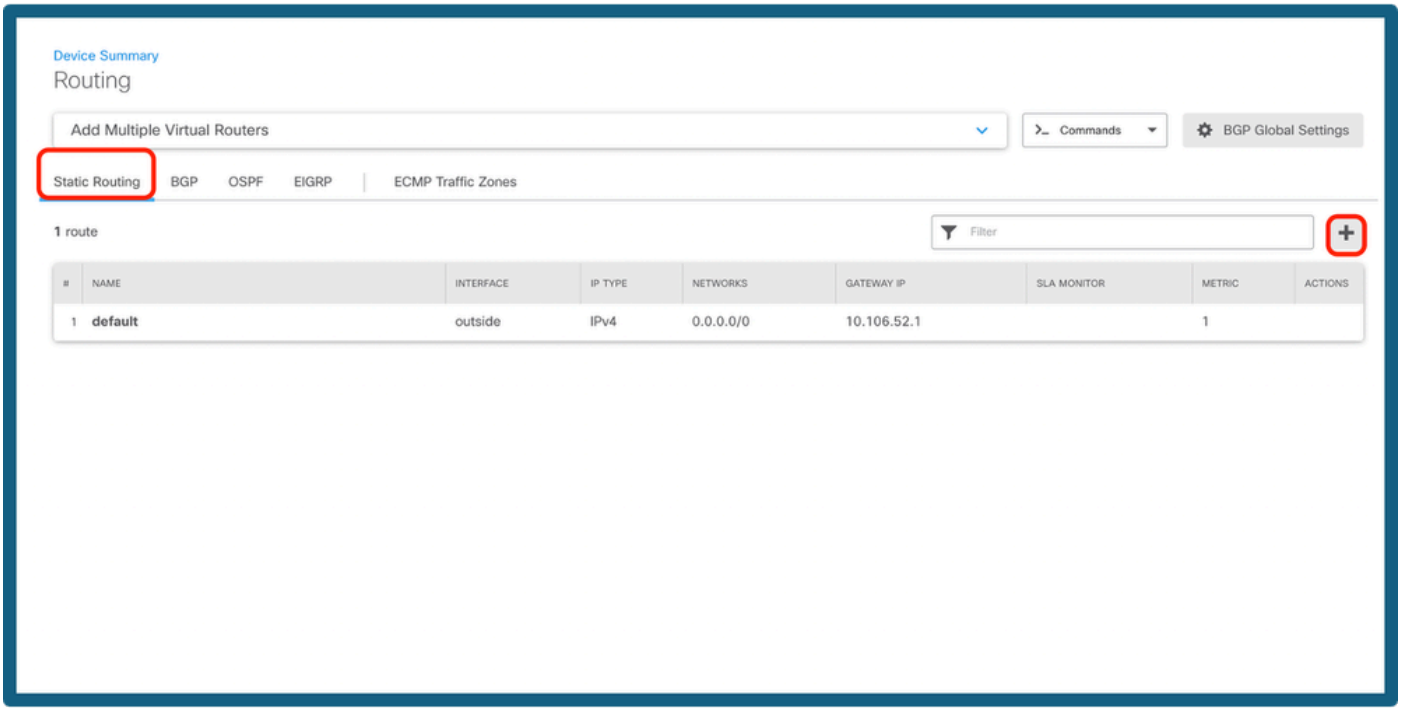
액세스 제어 정책 추가

13a단계. VTI 터널을 통해 라우팅을 추가합니다. Device(디바이스) > Routing(라우팅)으로 이동합니다.



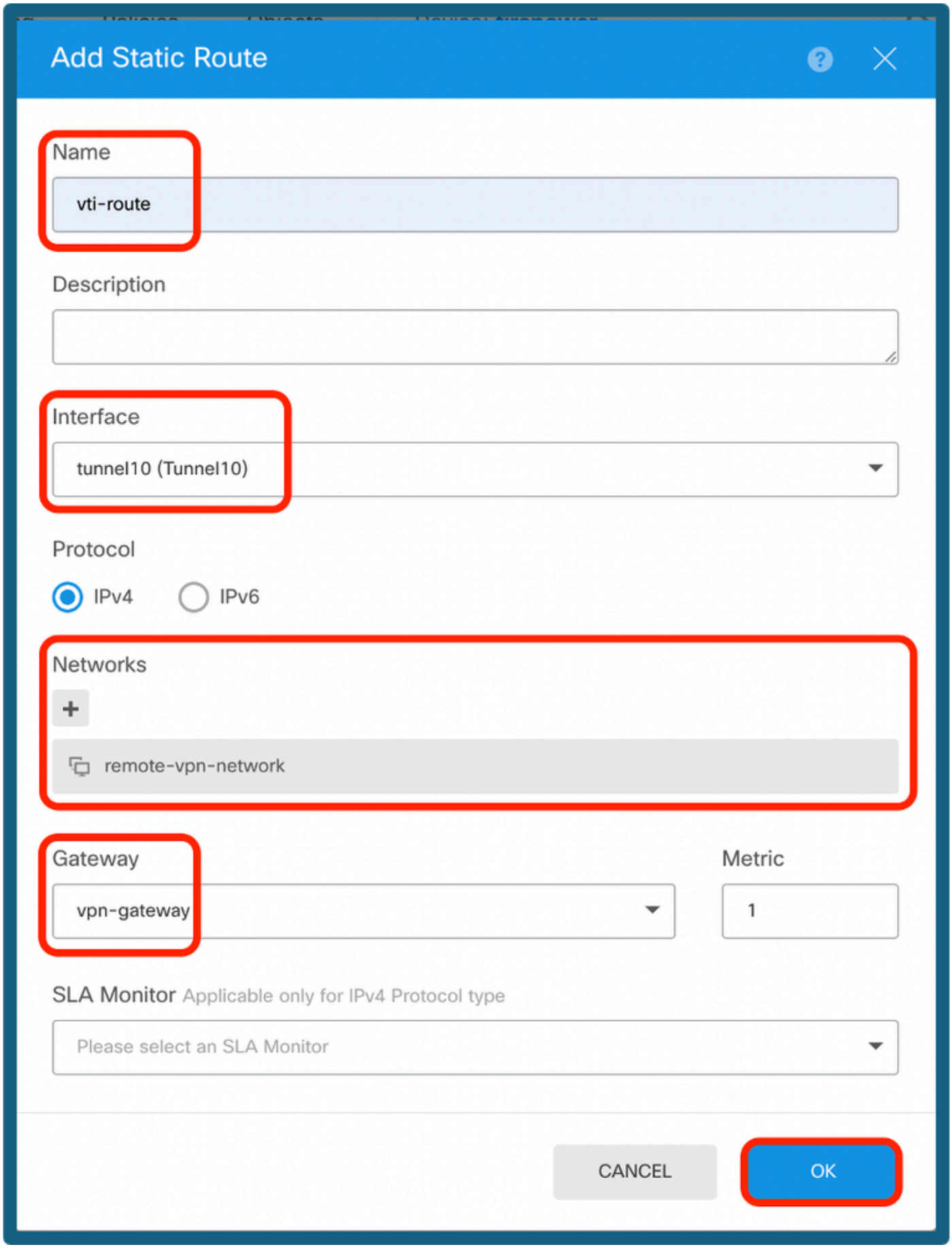
라우팅 선택

13b단계. Routing(라우팅) 탭에서 Static Route(고정 경로)로 이동합니다. +아이콘을 클릭합니다.



경로 추가

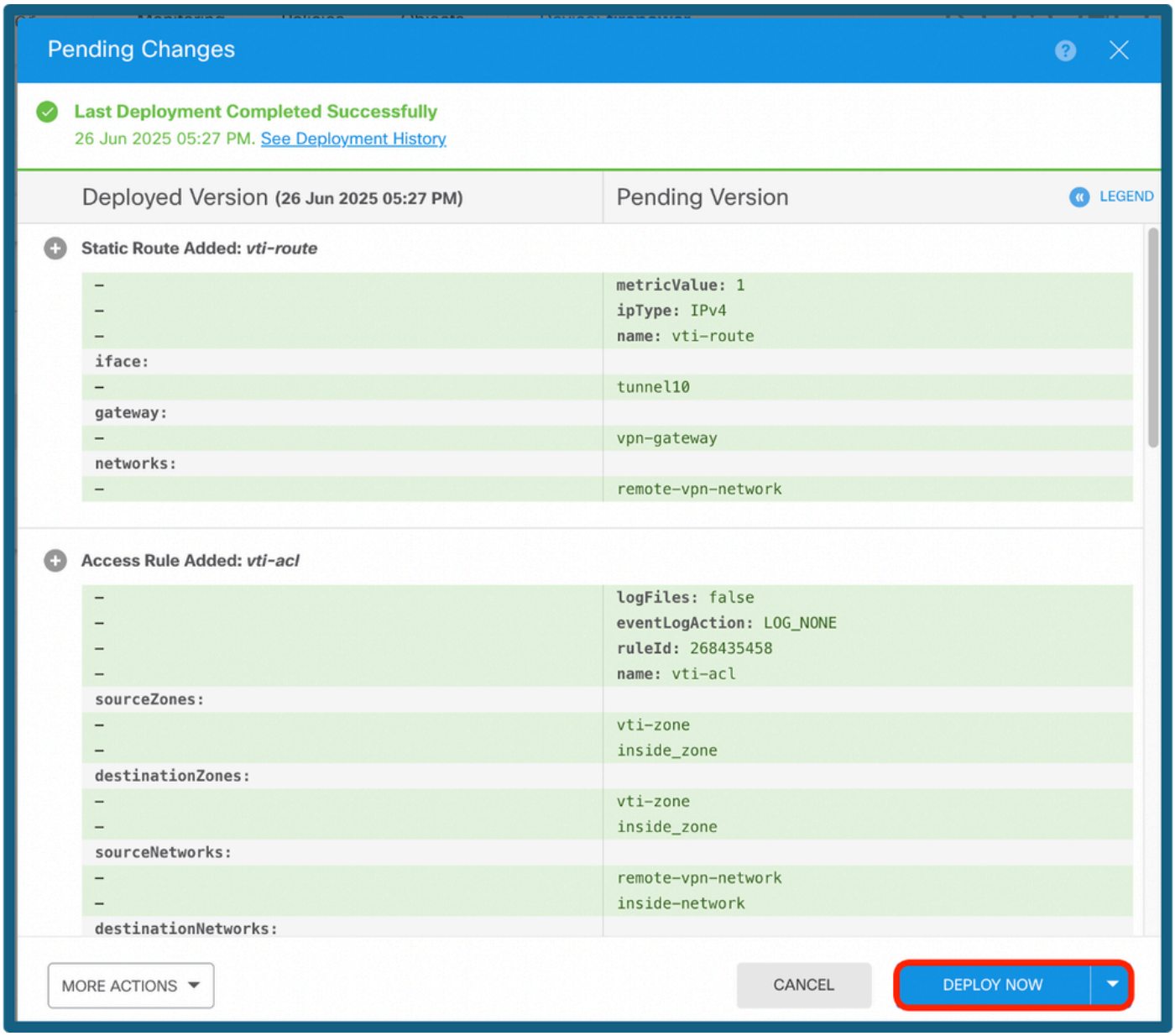
13c단계. 인터페이스를 제공하고, 네트워크를 선택하고, 게이트웨이를 제공합니다. OK(확인)를 클릭합니다.



고정 경로 구성

14단계. Deploy(구축)로 이동합니다. 변경 사항을 검토한 다음 Deploy Now(지금 구축)를 클릭합니

다.



컨피그레이션 구축

다음을 확인합니다.

구축이 완료되면 다음 명령을 사용하여 CLI에서 터널 상태를 확인할 수 있습니다.

1. show crypto ikev2 sa
2. show crypto ipsec sa <peer-ip>

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                   Remote                                  Status         Role
3294213359 10.106.52.222/500                      10.106.63.23/500                        READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/141 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x26a14554/0xd5db88bc
> show crypto ipsec sa
interface: tunnel10
    Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 10.106.63.23
```

Show 명령

관련 정보

FDM에서 관리하는 FTD의 Site-to-Site VPN에 대한 자세한 내용은 여기에서 전체 구성 가이드를 참조하십시오.

[FTD Managed by FDM 컨피그레이션 가이드]

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.