FDM에서 관리하는 FTD에서 VRF 인식 경로 기반 사이트 대 사이트 VPN 구성

목차

소개

이 문서에서는 FDM에서 관리되는 FTD에서 VRF 인식 경로 기반 사이트 대 사이트 VPN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- VPN에 대한 기본 이해
- VRF(Virtual Routing and Forwarding)에 대한 기본적인 이해
- FDM 사용 경험

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTDv 버전 7.4.2
- Cisco FDM 버전 7.4.2
- Cisco ASAv 버전 9.20.3

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.

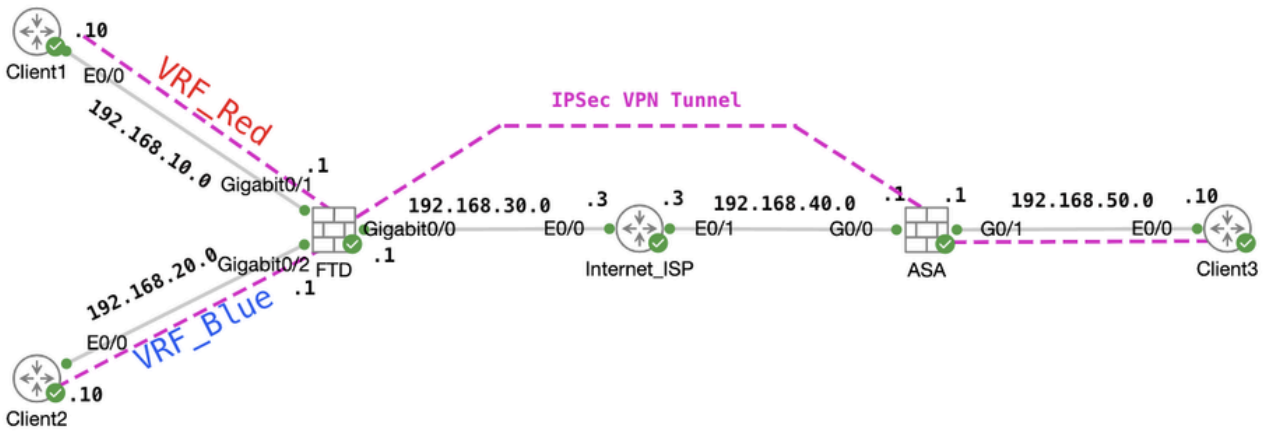
배경 정보

FDM(Firepower Device Manager)의 VRF(Virtual Routing and Forwarding)를 사용하면 단일 FTD(Firepower Threat Defense) 디바이스에서 여러 개의 격리 라우팅 인스턴스를 생성할 수 있습니다. 각 VRF 인스턴스는 자체 라우팅 테이블을 갖춘 별도의 가상 라우터로 작동하여 네트워크 트래픽을 논리적으로 분리하고 향상된 보안 및 트래픽 관리 기능을 제공합니다.

이 문서에서는 VRF 인식 IPSec VPN을 VTI와 함께 구성하는 방법에 대해 설명합니다. VRF Red 네트워크와 VRF Blue 네트워크는 FTD 뒤에 있습니다. VRF Red 네트워크의 Client1과 VRF Blue의 Client2는 IPSec VPN 터널을 통해 ASA 뒤에 있는 Client3과 통신합니다.

구성

네트워크 다이어그램

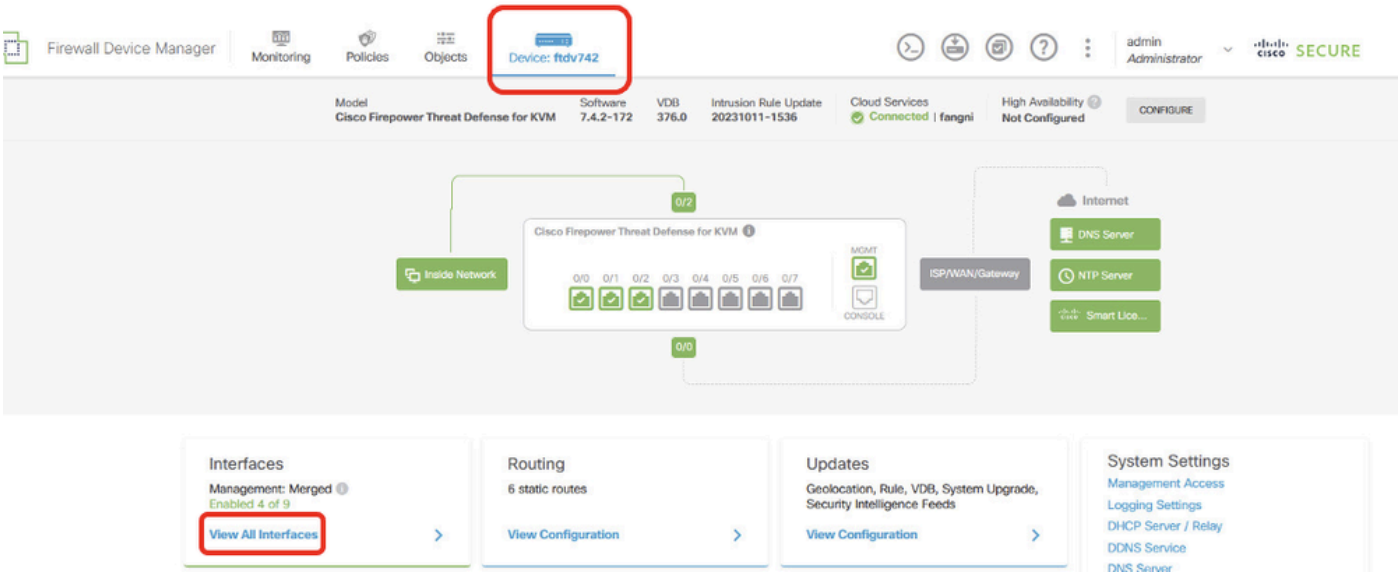


토폴로지

FTD 구성

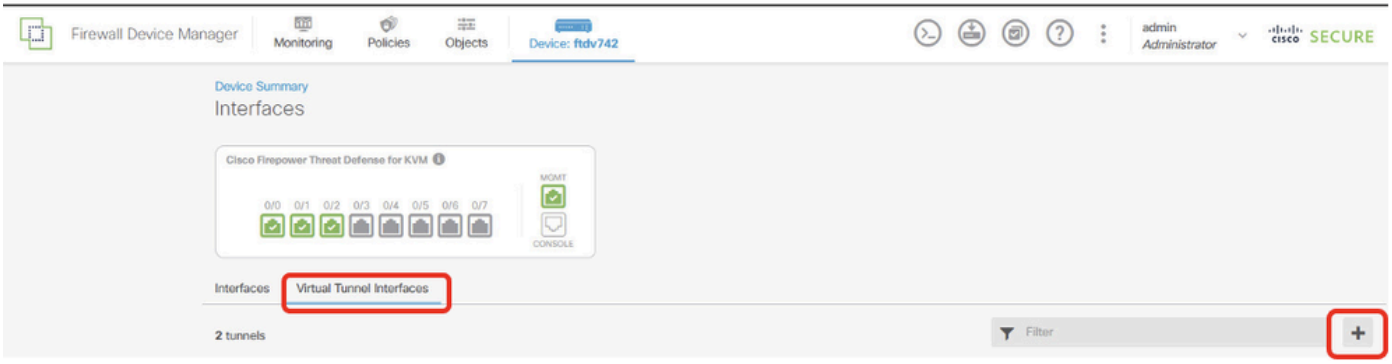
1단계. 노드 간 IP 상호 연결의 예비 컨피그레이션이 올바르게 완료되었는지 확인하는 것이 중요합니다. Client1 및 Client2는 FTD 내부 IP 주소를 게이트웨이로 사용합니다. Client3은 ASA 내부 IP 주소를 게이트웨이로 사용합니다.

2단계. 가상 터널 인터페이스를 생성합니다. FTD의 FDM GUI에 로그인합니다. Device > Interfaces로 이동합니다. View All Interfaces(모든 인터페이스 보기)를 클릭합니다.



FTD_View_Interface

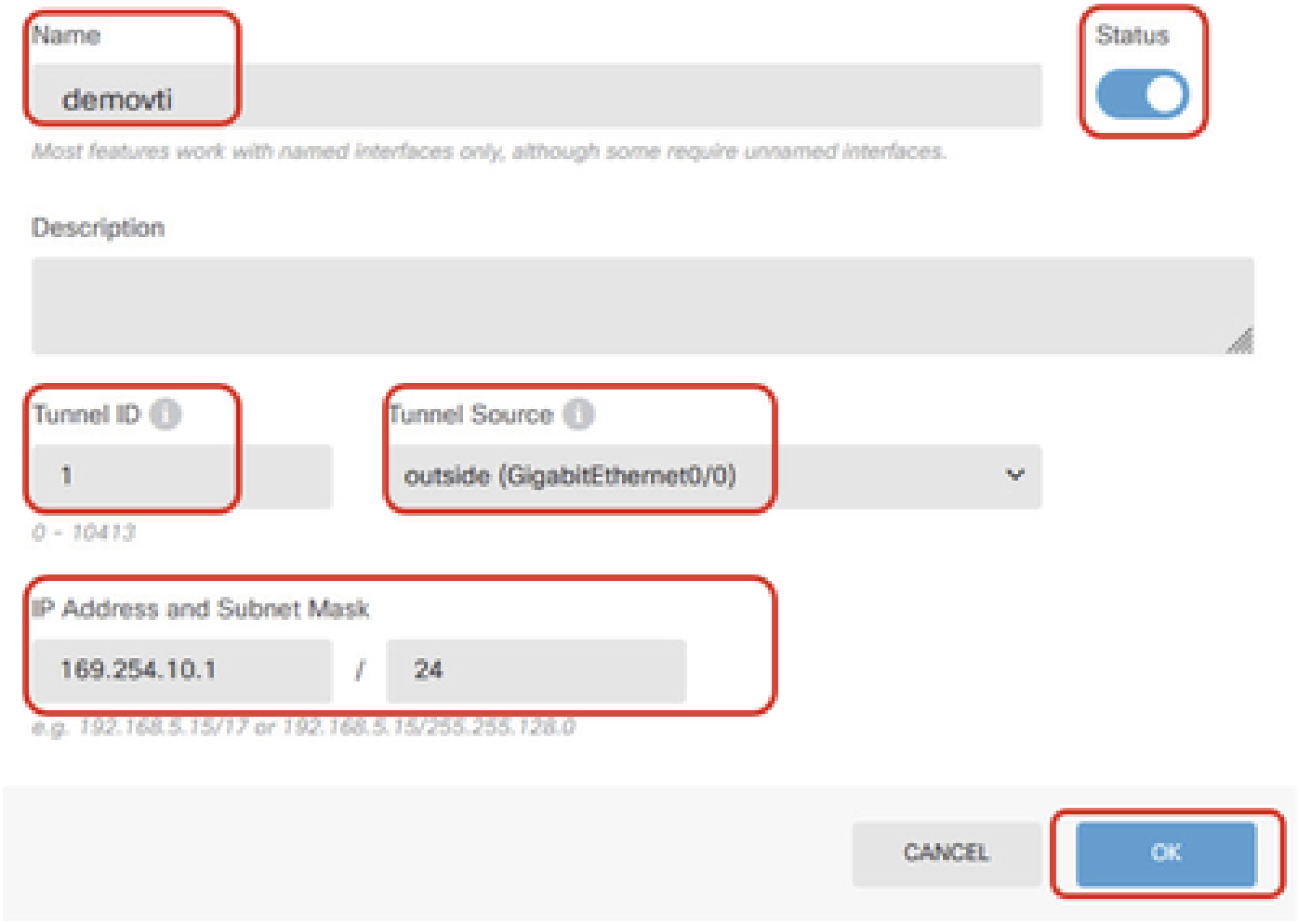
2.1단계. Virtual Tunnel Interfaces(가상 터널 인터페이스) 탭을 클릭합니다. +단추를 클릭합니다.



FTD_Create_VTI

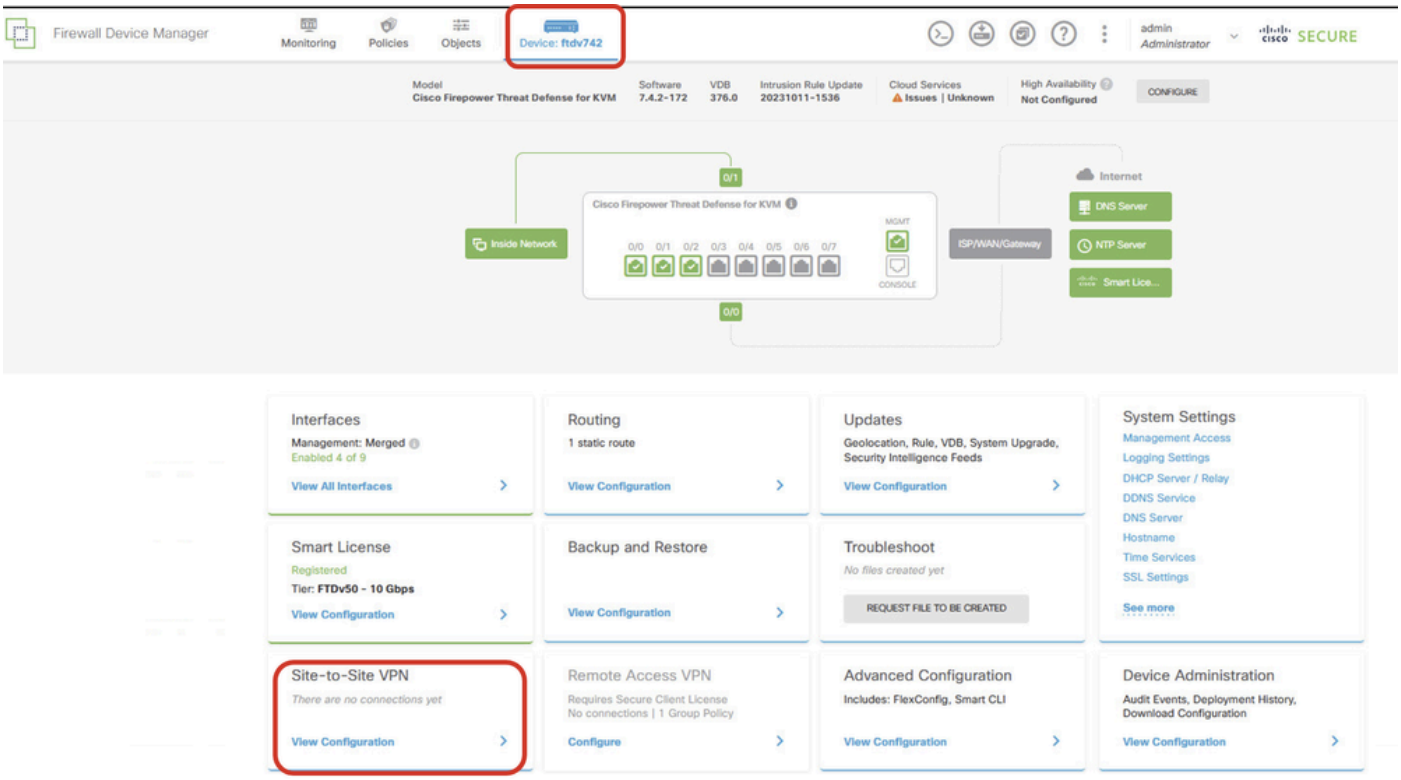
2.2단계. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: 제거
- 터널 ID: 1
- 터널 원본: 외부(GigabitEthernet0/0)
- IP 주소 및 서브넷 마스크: 169.254.10.1/24
- 상태: Enabled(활성화됨) 위치에 있는 슬라이더를 클릭합니다.



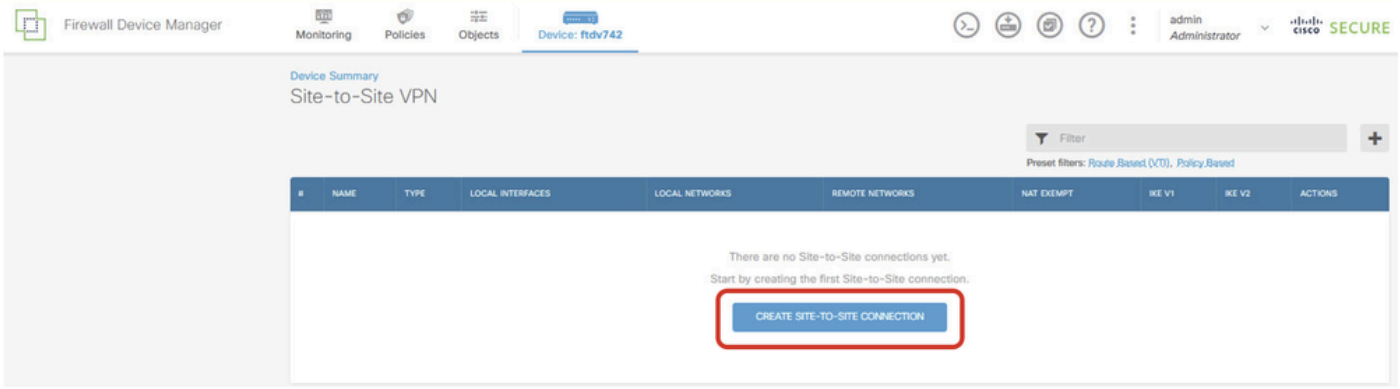
FTD_Create_VTI_Details

3단계. Device(디바이스) > Site-to-Site VPN(사이트 대 사이트 VPN)으로 이동합니다. View Configuration(컨피그레이션 보기) 버튼을 클릭합니다.



FTD_Site-to-Site_VPN_View_Configuration

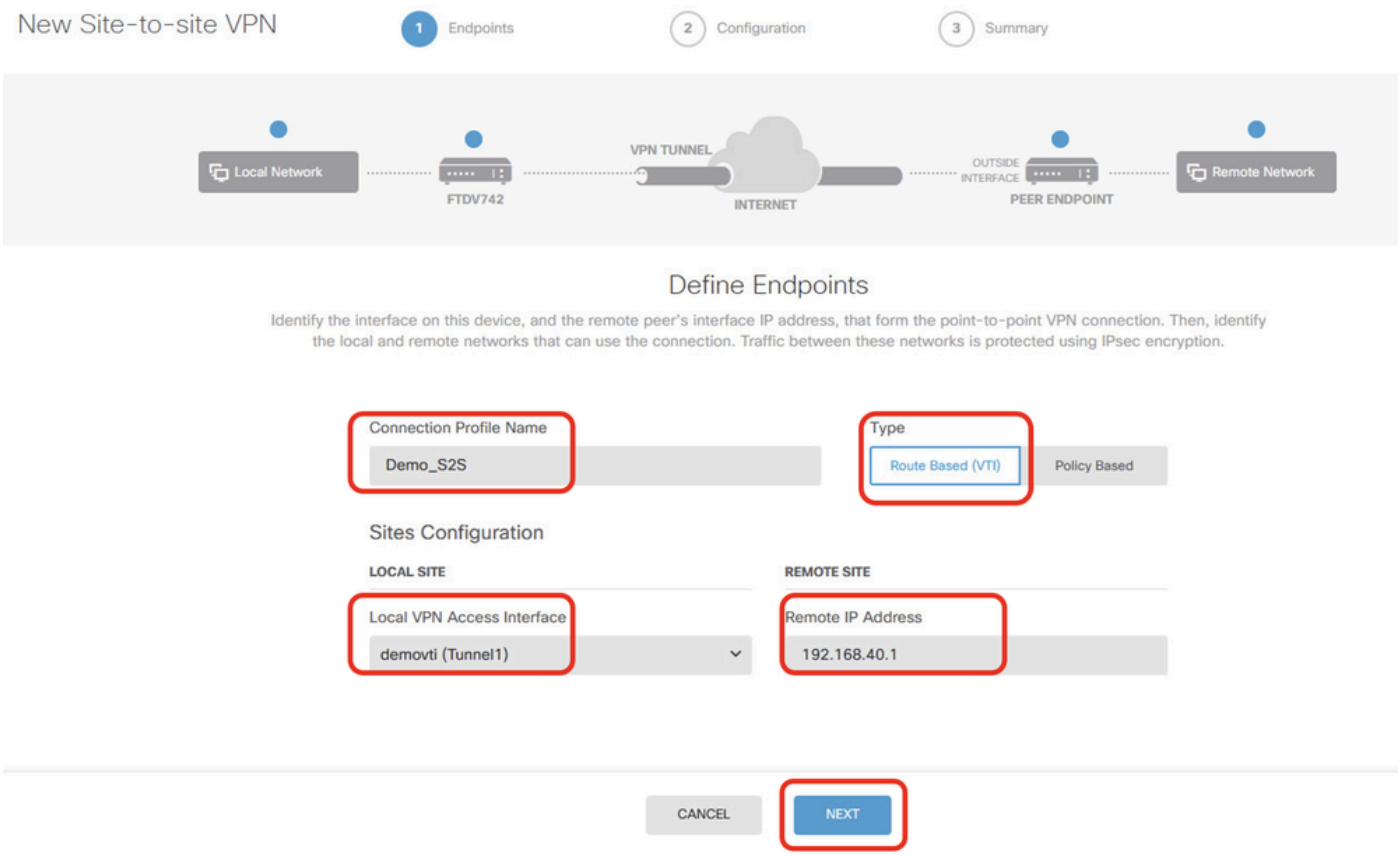
3.1단계. 새 Site-to-Site VPN 생성을 시작합니다. Create SITE-TO-SITE CONNECTION(사이트 대 사이트 연결 생성) 버튼을 클릭합니다. 또는 +단추를 클릭합니다.



FTD_Create_Site2Site_Connection

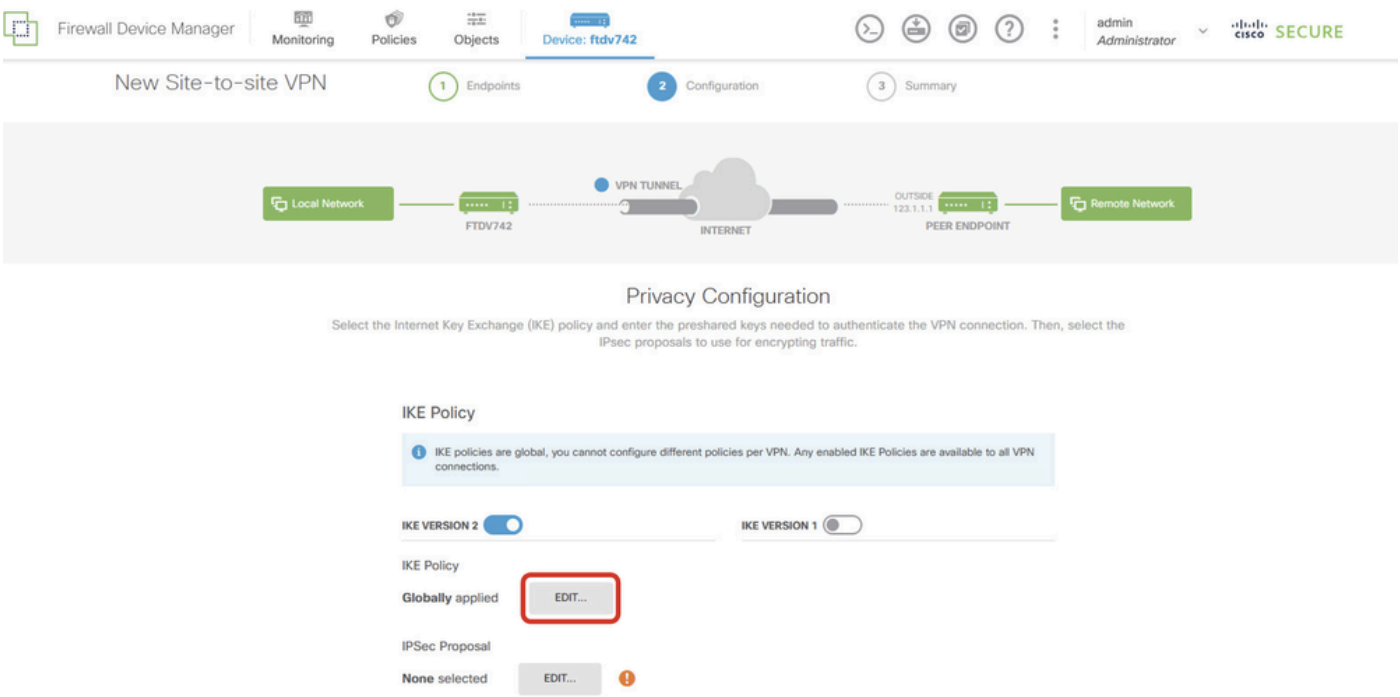
3.2단계. 제공 필요한 정보입니다. 다음 버튼을 클릭합니다.

- 연결 프로파일 이름: 데모_S2S
- 유형: 경로 기반(VTI)
- 로컬 VPN 액세스 인터페이스: demovti(2단계에서 생성)
- 원격 IP 주소: 192.168.40.1(피어 ASA 외부 IP 주소)



FTD_사이트 대 사이트 VPN_엔드포인트

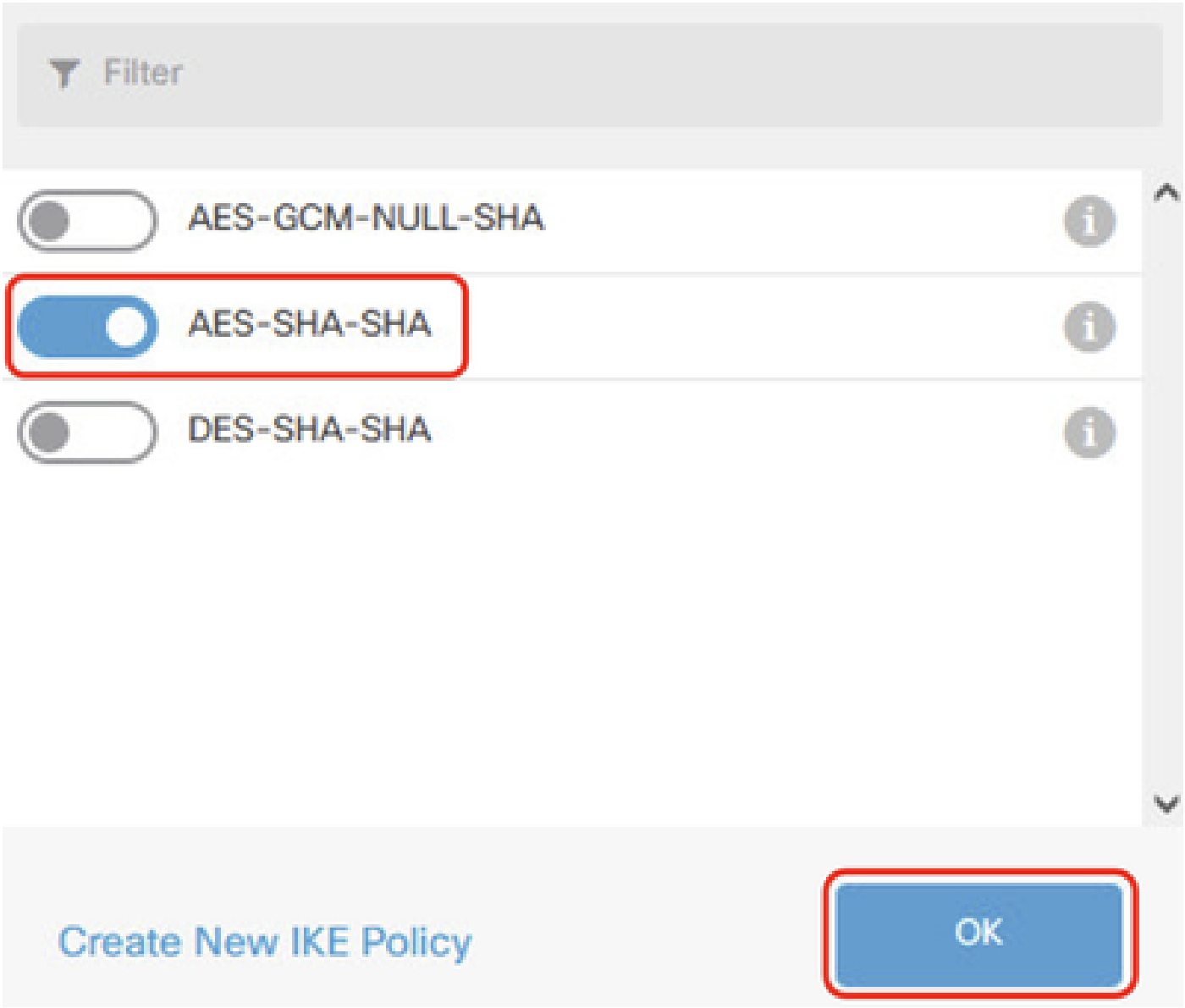
3.3단계. IKE Policy(IKE 정책)로 이동합니다. Edit(편집) 버튼을 클릭합니다.



FTD_Edit_IKE_Policy

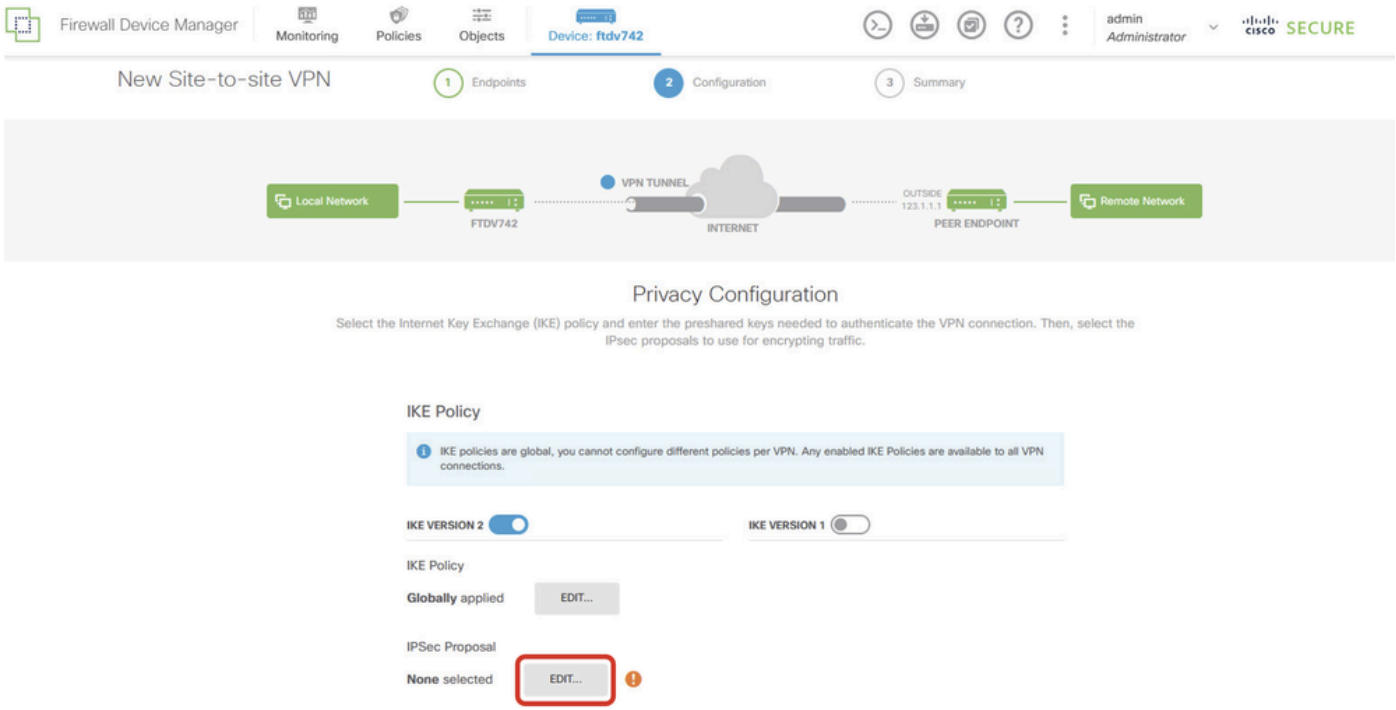
3.4단계. IKE 정책의 경우 미리 정의된 정책을 사용하거나 를 클릭하여 새 정책을 생성할 수 있습니다 새 IKE 정책 생성 .

이 예에서는 기존 IKE 정책 이름 AES-SHA-SHA를 토글합니다. OK(확인) 버튼을 클릭하여 저장합니다.



FTD_Enable_IKE_Policy

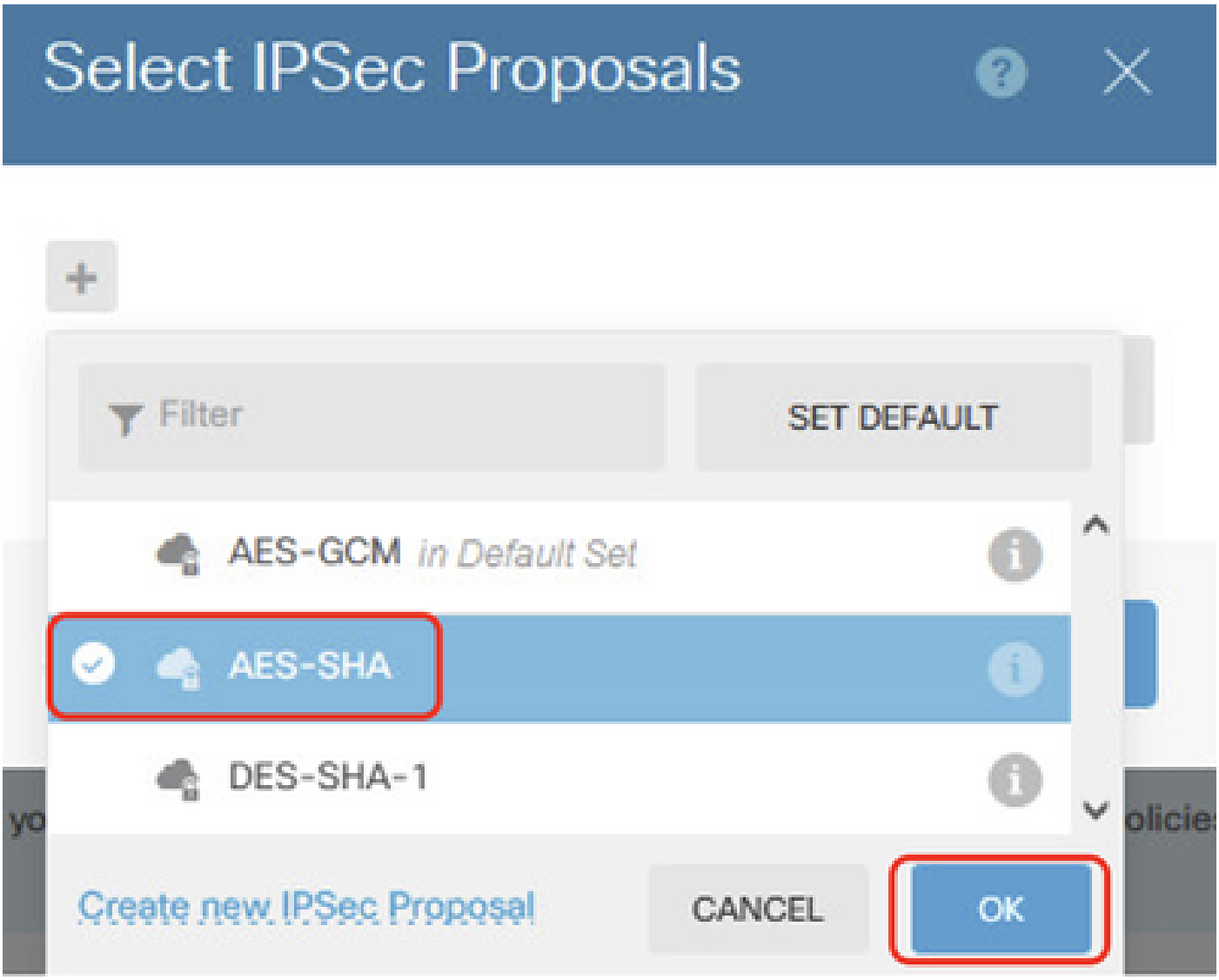
3.5단계. IPSec 제안으로 이동합니다. Edit(편집) 버튼을 클릭합니다.



FTD_Edit_IPSec_Proposal

3.6단계. IPSec 제안의 경우, 사전 정의된 것을 사용하거나 Create new IPSec Proposal(새 IPSec 제안 생성)을 클릭하여 새 제안서를 생성할 수 있습니다.

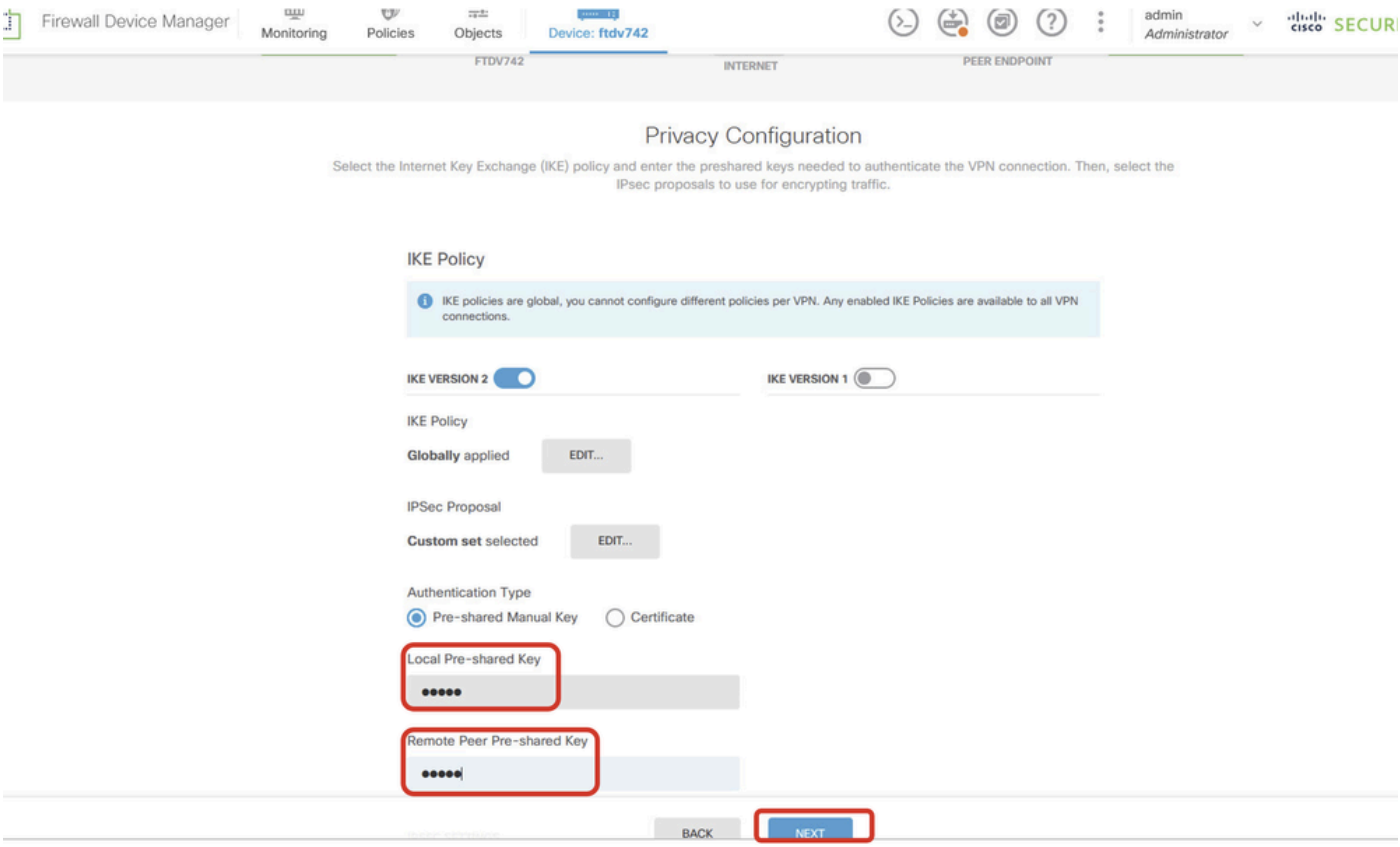
이 예에서는 기존 IPSec 제안 이름 AES-SHA를 토글합니다. 을 클릭합니다 확인 단추를 클릭하여 저장합니다.



FTD_Enable_IPSec_Proposal

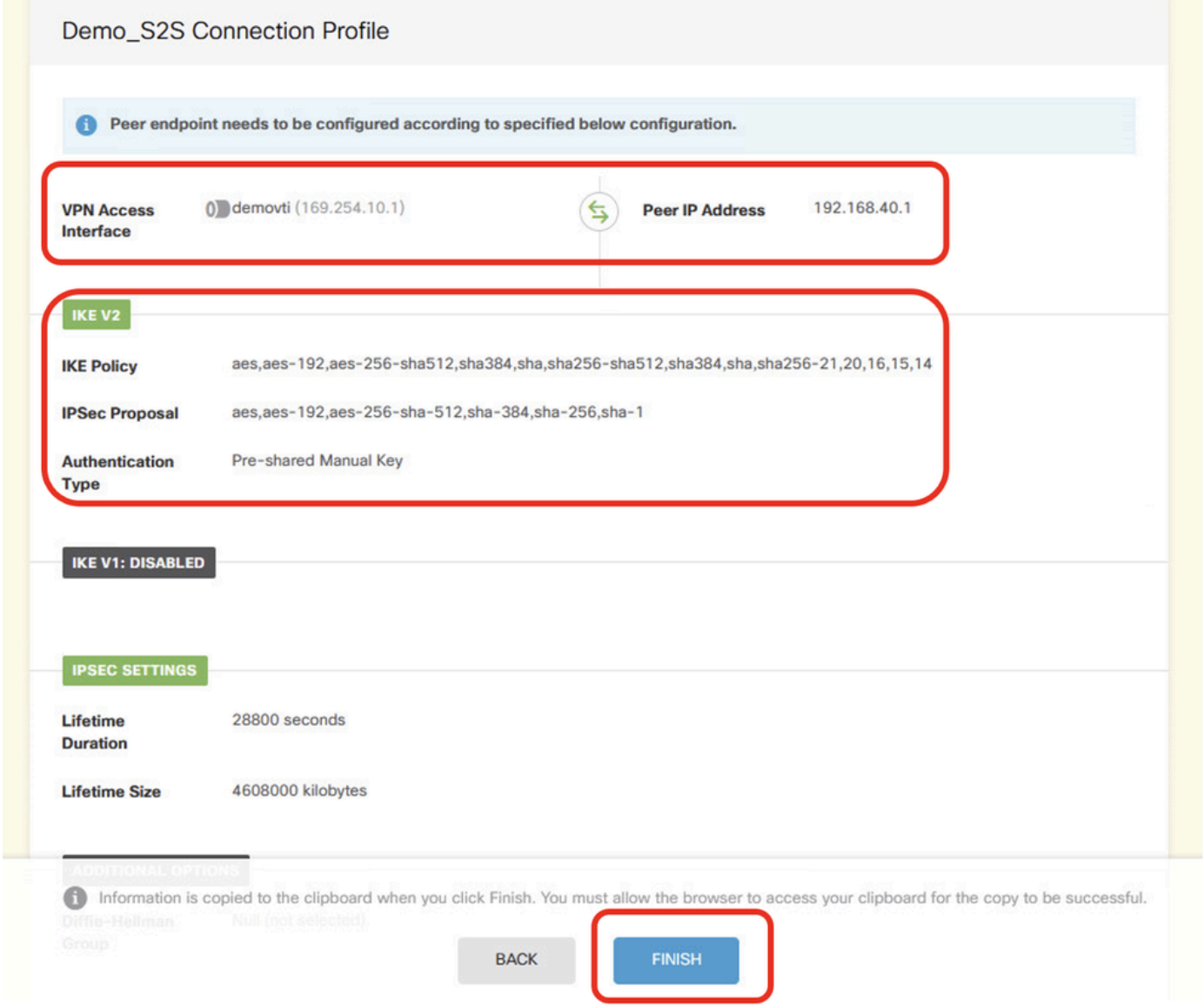
3.7단계. 페이지를 아래로 스크롤하여 사전 공유 키를 구성합니다. 다음 버튼을 클릭합니다.

이 사전 공유 키를 기록해 두었다가 나중에 ASA에서 구성합니다.



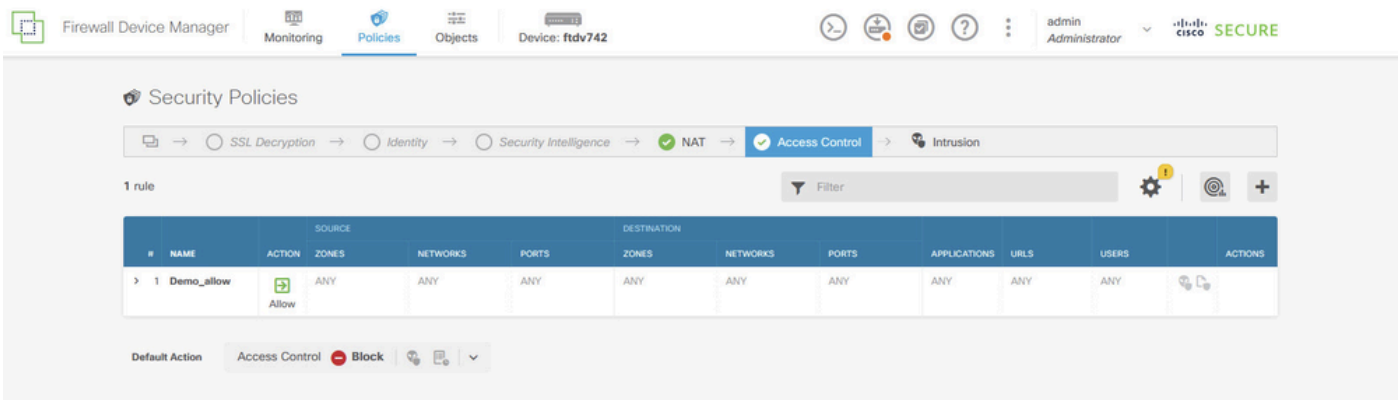
FTD_Configure_Pre_Shared_Key

3.8단계. VPN 컨피그레이션을 검토합니다. 수정해야 할 사항이 있으면 뒤로(BACK) 버튼을 클릭합니다. 모든 것이 정상인 경우 FINISH(마침) 버튼을 클릭합니다.



FTD_Review_VPN_구성

3.9단계. 트래픽이 FTD를 통과하도록 허용하는 액세스 제어 규칙을 생성합니다. 이 예에서는 데모용으로 모두 허용합니다. 실제 요구 사항에 따라 정책을 수정하십시오.

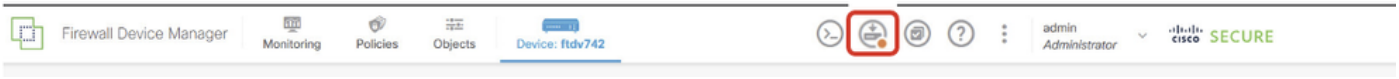


FTD_ACP_예

3.10단계(선택 사항) 클라이언트가 인터넷에 액세스하도록 구성된 동적 NAT가 있는 경우 FTD에서 클라이언트 트래픽에 대한 NAT 제외 규칙을 구성합니다. 이 예에서는 FTD에 구성된 동적 NAT가

없으므로 NAT 제외 규칙을 구성할 필요가 없습니다.

3.11단계. 컨피그레이션 변경 사항을 구축합니다.



FTD_구축_변경

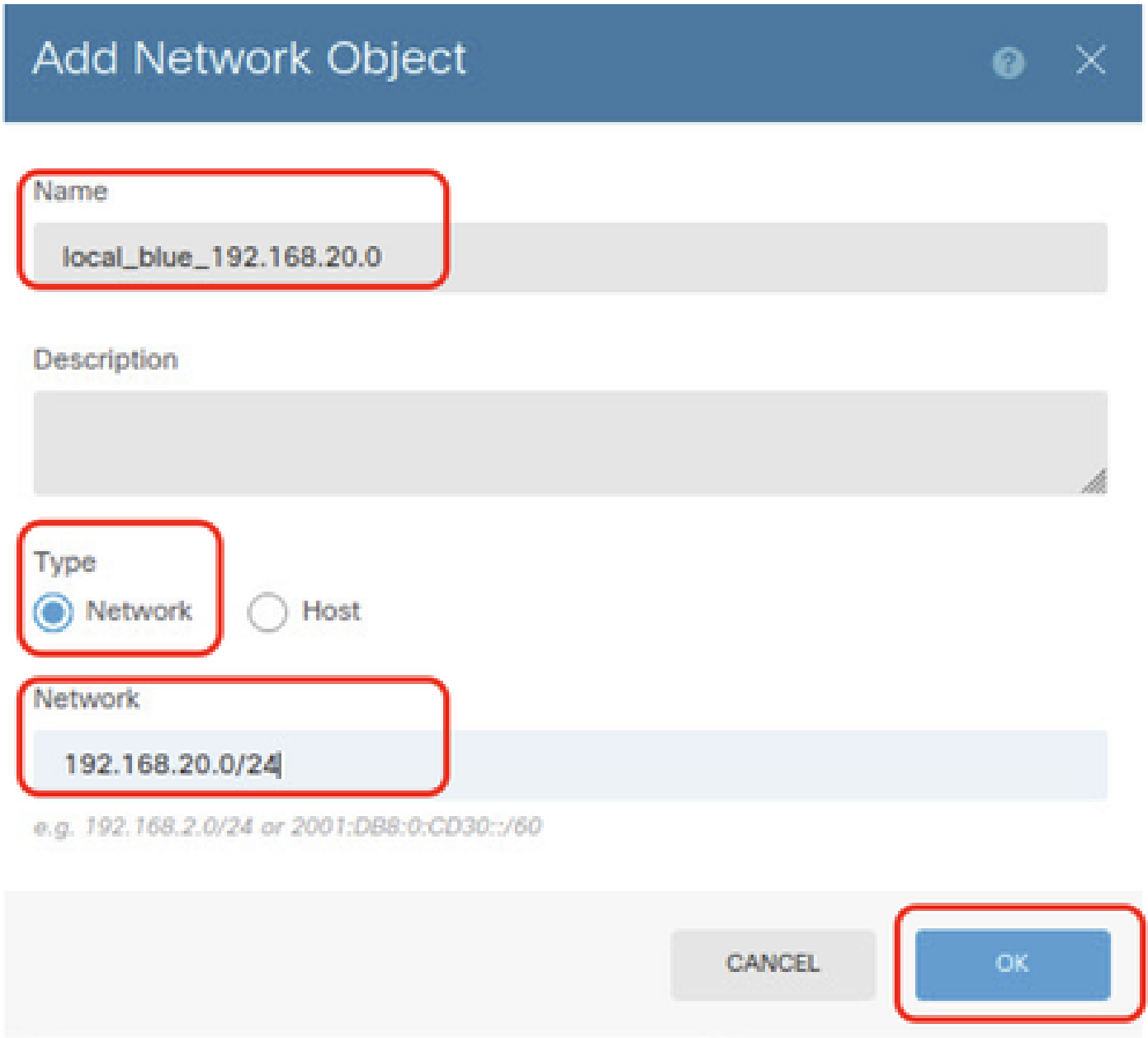
4단계. 가상 라우터 구성

4.1단계. 고정 경로에 대한 네트워크 객체를 생성합니다. Objects > Networks로 이동하여 +버튼을 클릭합니다.

FTD_Create_NetObjects

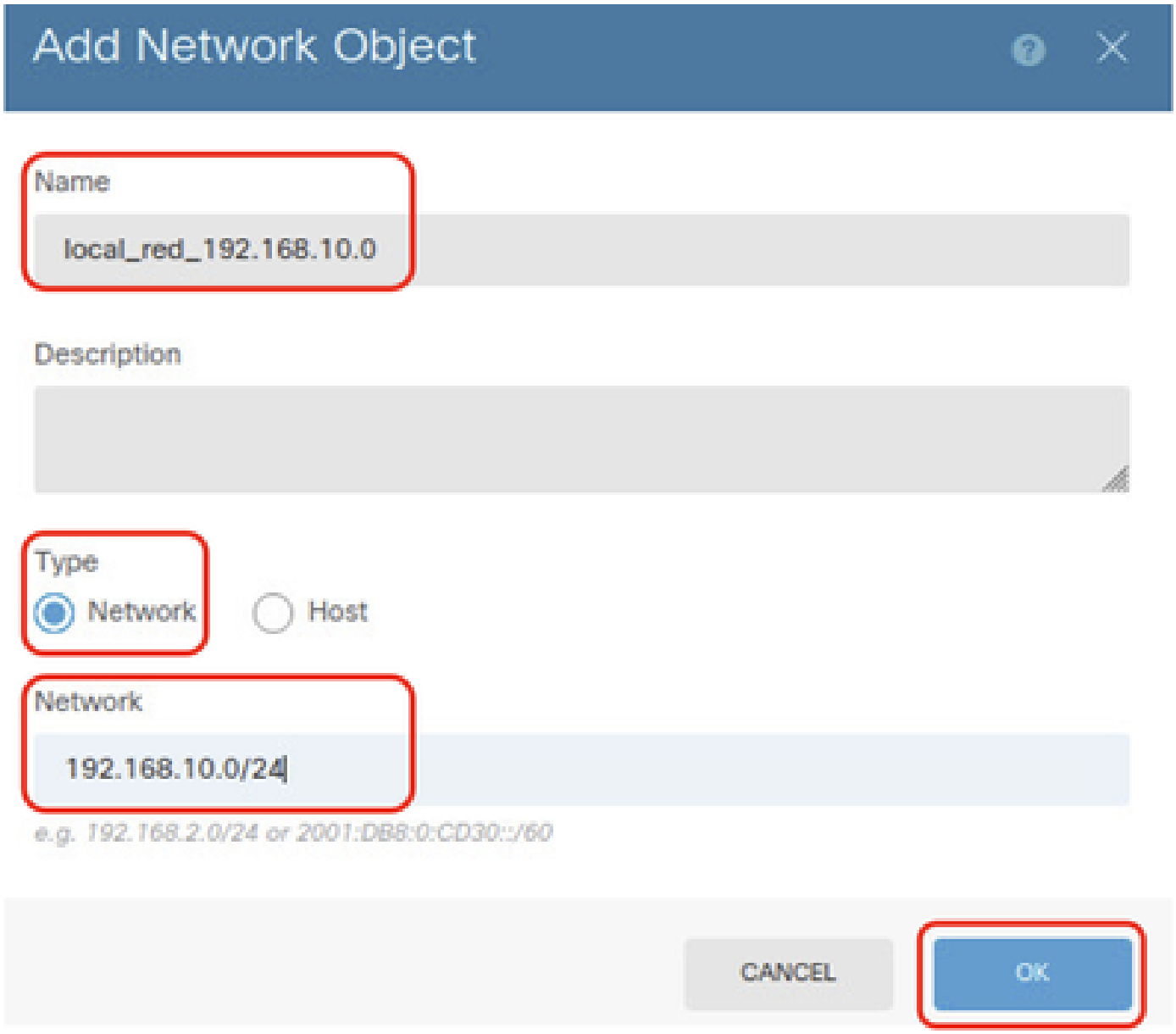
4.2단계. 각 네트워크 개체에 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: local_blue_192.168.20.0
- 유형: 네트워크
- 네트워크: 192.168.20.0/24



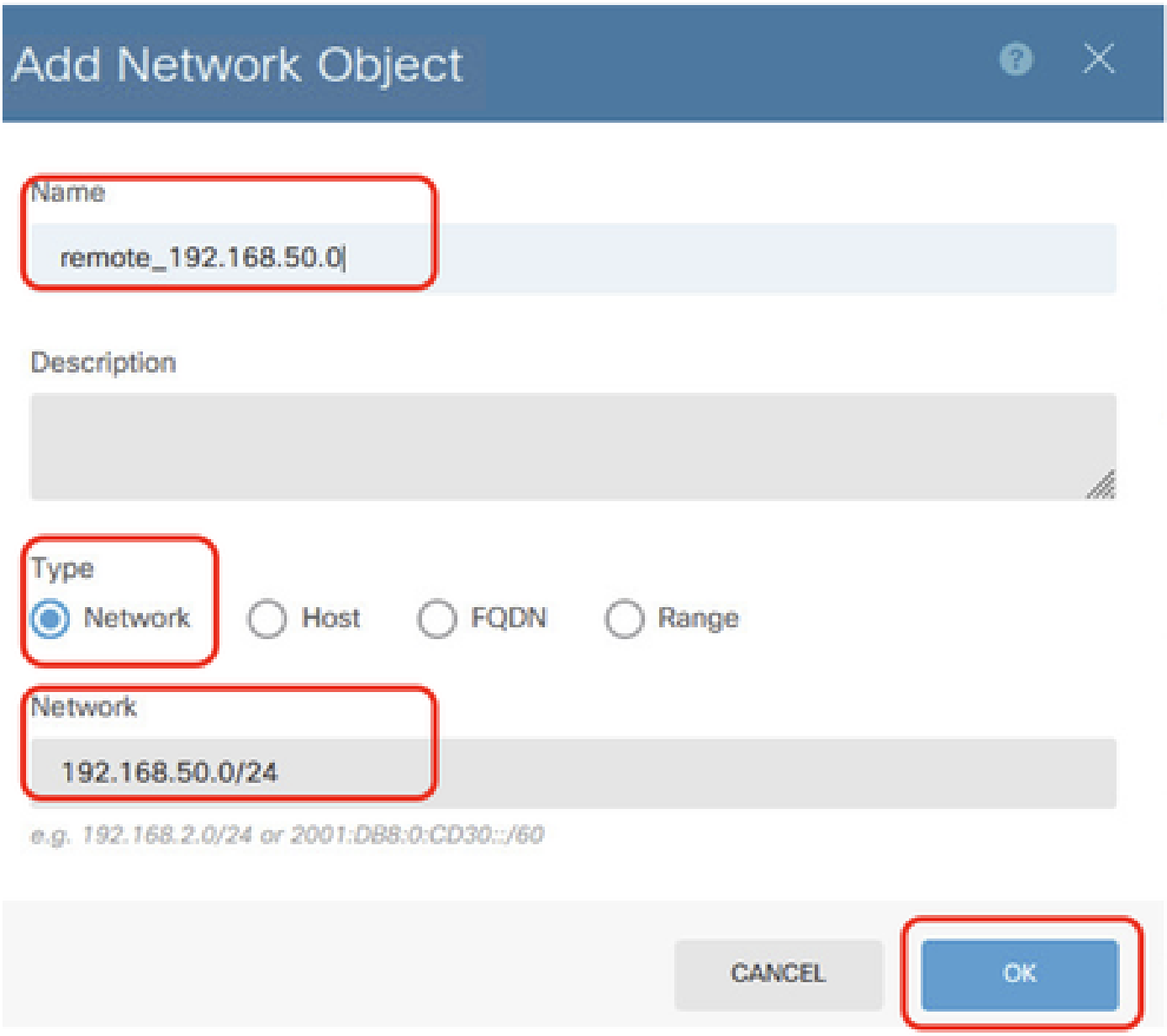
FTD_VRF_Blue_Network

- 이름: local_red_192.168.10.0
- 유형: 네트워크
- 네트워크: 192.168.10.0/24



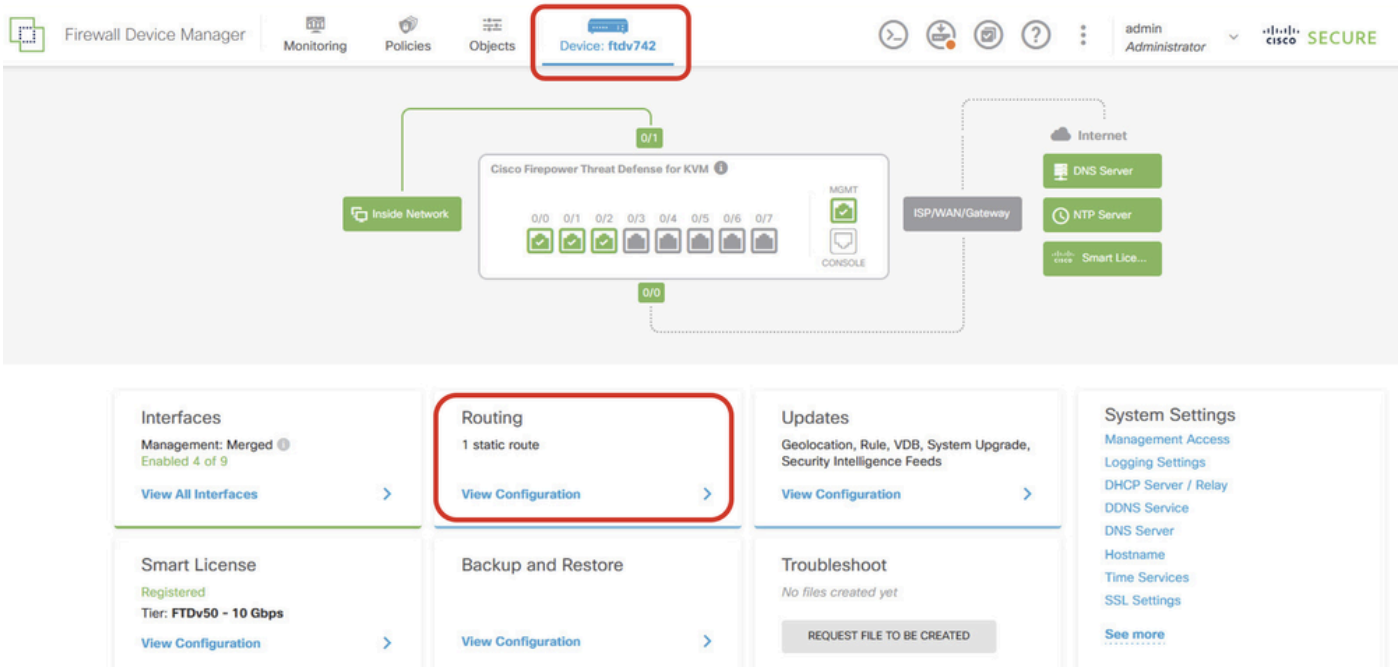
FTD_VRF_Red_Network

- 이름: remote_192.168.50.0
- 유형: 네트워크
- 네트워크: 192.168.50.0/24



FTD_원격_네트워크

4.3단계. 첫 번째 가상 라우터를 생성합니다. Device(디바이스) > Routing(라우팅)으로 이동합니다. View Configuration(컨피그레이션 보기)을 클릭합니다.



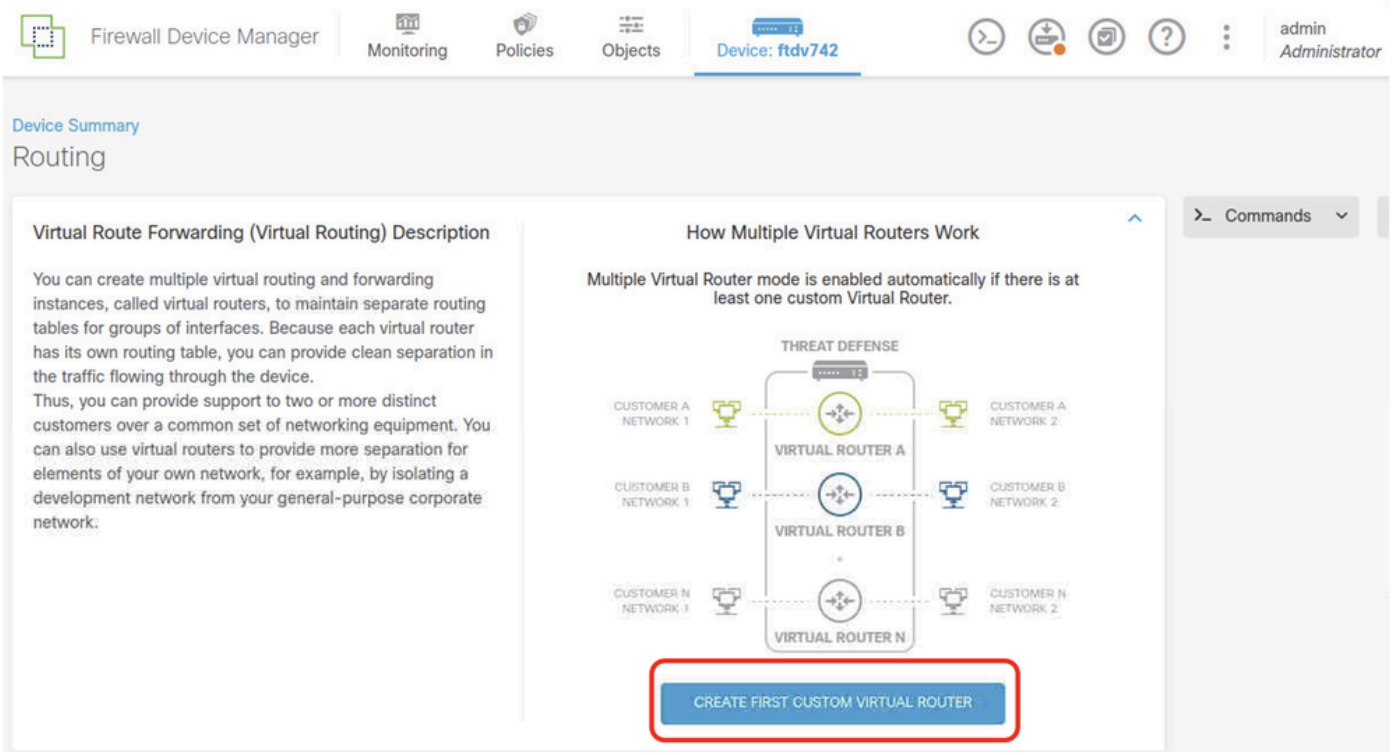
FTD_View_Routing_Configuration

4.4단계. Add Multiple Virtual Routers(여러 가상 라우터 추가)를 클릭합니다.

참고: 외부 인터페이스를 통과하는 고정 경로는 FDM 초기화 중에 이미 구성되어 있습니다. 없는 경우 수동으로 구성하십시오.

FTD_Add_First_Virtual_Router1

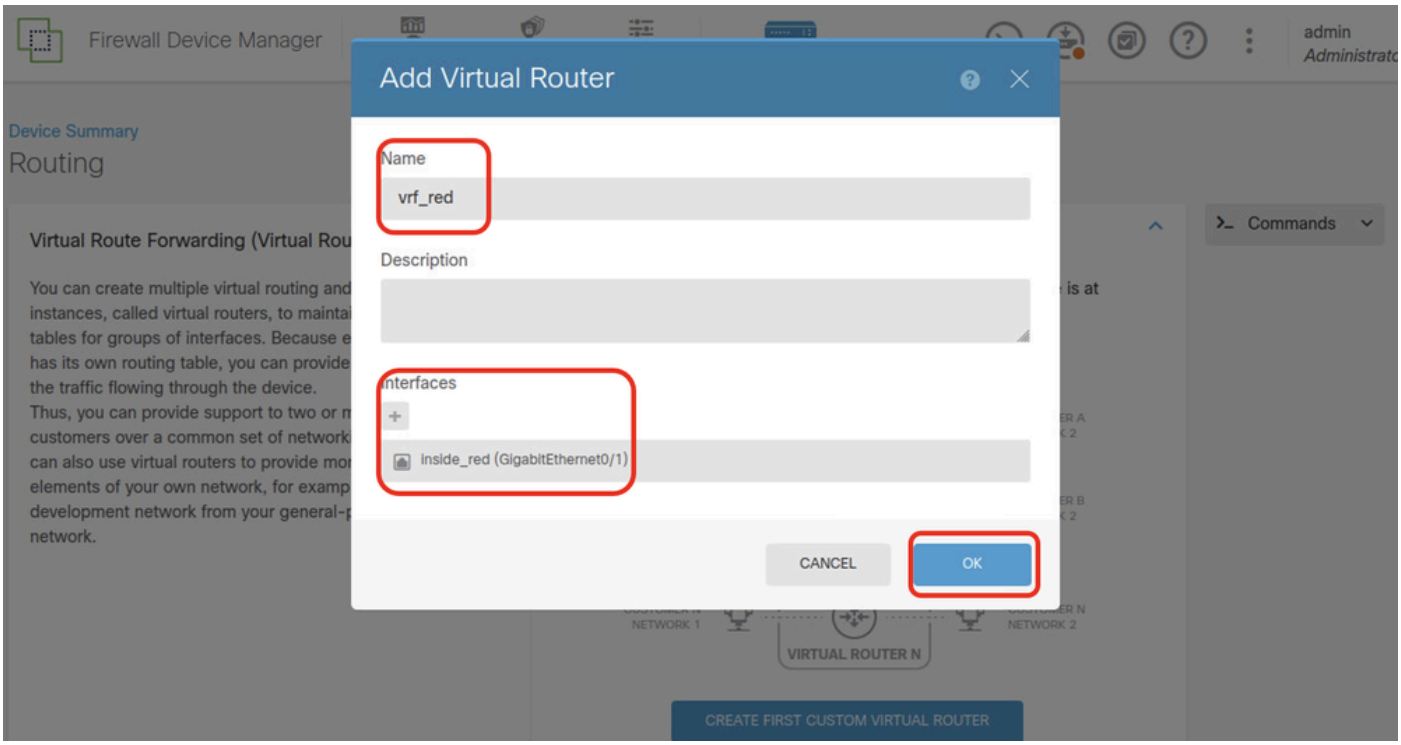
4.5단계. CREATE FIRST CUSTOM VIRTUAL ROUTER를 클릭합니다.



FTD_Add_First_Virtual_Router2

4.6단계. 첫 번째 가상 라우터에 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다. 가상 라우터를 처음 생성한 후에는 vrf 이름 Global이 자동으로 표시됩니다.

- 이름: vrf_빨강
- 인터페이스: inside_red(GigabitEthernet0/1)



FTD_Add_First_Virtual_Router3

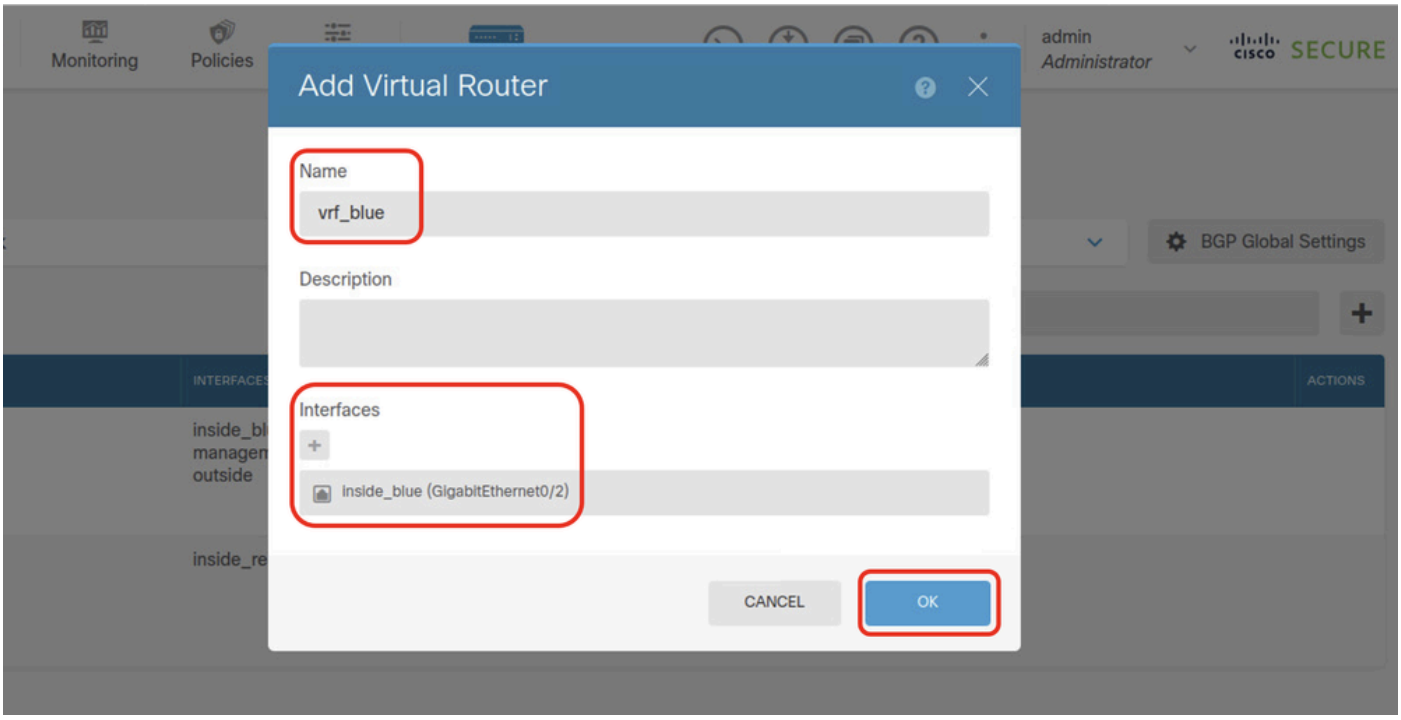
4.7단계. 두 번째 가상 라우터를 생성합니다. Device(디바이스) > Routing(라우팅)으로 이동합니다.

View Configuration(컨피그레이션 보기)을 클릭합니다. +단추를 클릭합니다.

FTD_Add_Second_Virtual_Router

4.8단계. 두 번째 가상 라우터에 필요한 정보를 제공합니다. OK(확인) 버튼 클릭

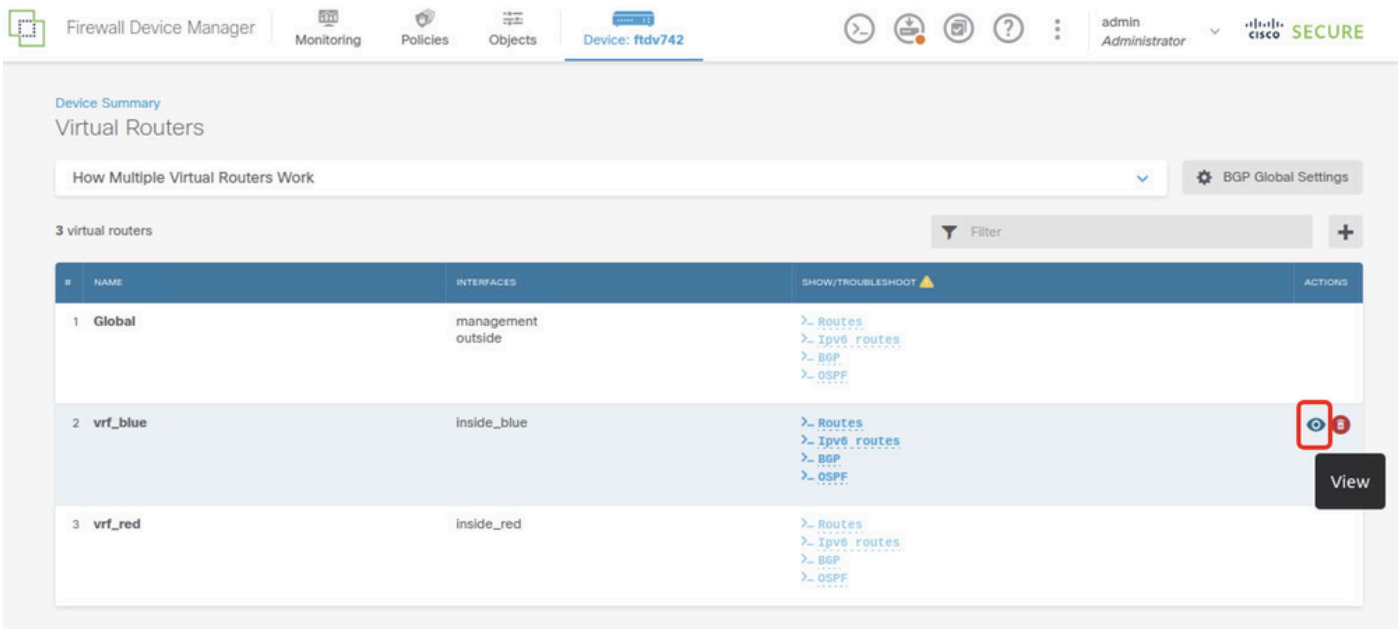
- 이름: vrf_blue
- 인터페이스: inside_blue(GigabitEthernet0/2)



FTD_Add_Second_Virtual_Router2

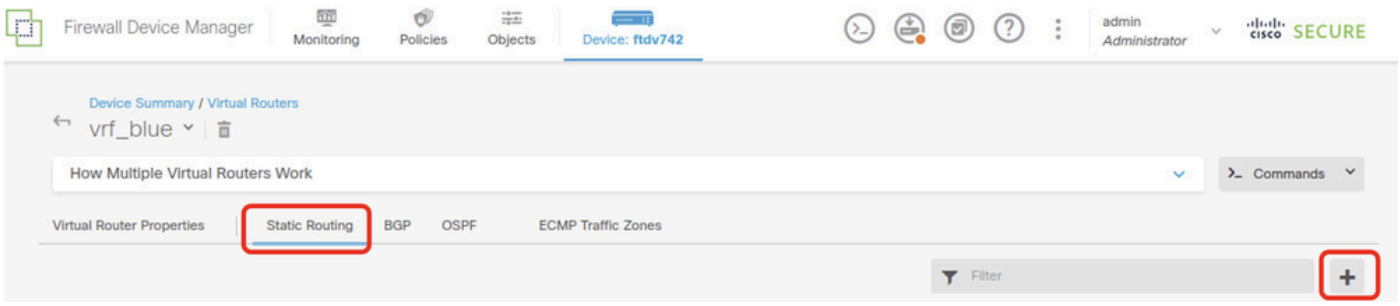
5단계. vrf_blue에서 전역으로 경로 누수를 생성합니다. 이 경로는 192.168.20.0/24 네트워크의 엔드포인트가 사이트 간 VPN 터널을 통과하는 연결을 시작할 수 있도록 합니다. 이 예에서 원격 엔드포인트는 192.168.50.0/24 네트워크를 보호하고 있습니다.

Device(디바이스) > Routing(라우팅)으로 이동합니다. 구성 보기를 누릅니다. 보기 아이콘을 누릅니다. 가상 라우터 vrf_blue에 대한 Action(작업) 셀.



FTD_뷰_VRF_블루

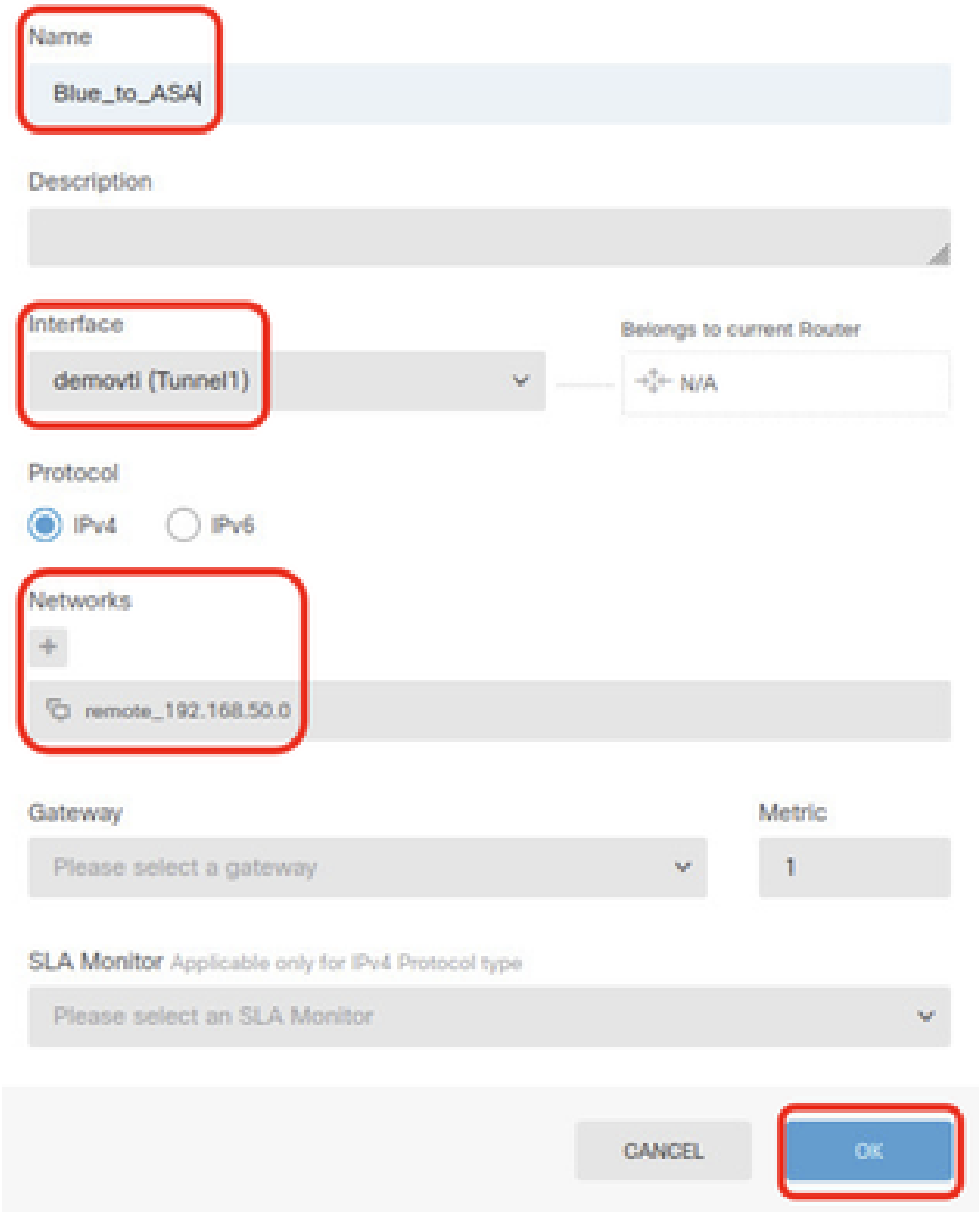
5.1단계. Static Routing(정적 라우팅) 탭을 클릭합니다. +단추를 클릭합니다.



FTD_Create_Static_Route_VRF_Blue

5.2단계. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: 블루_투_ASA
- 인터페이스: demovti(터널1)
- 네트워크: remote_192.168.50.0
- 게이트웨이: 이 항목은 비워 둡니다.

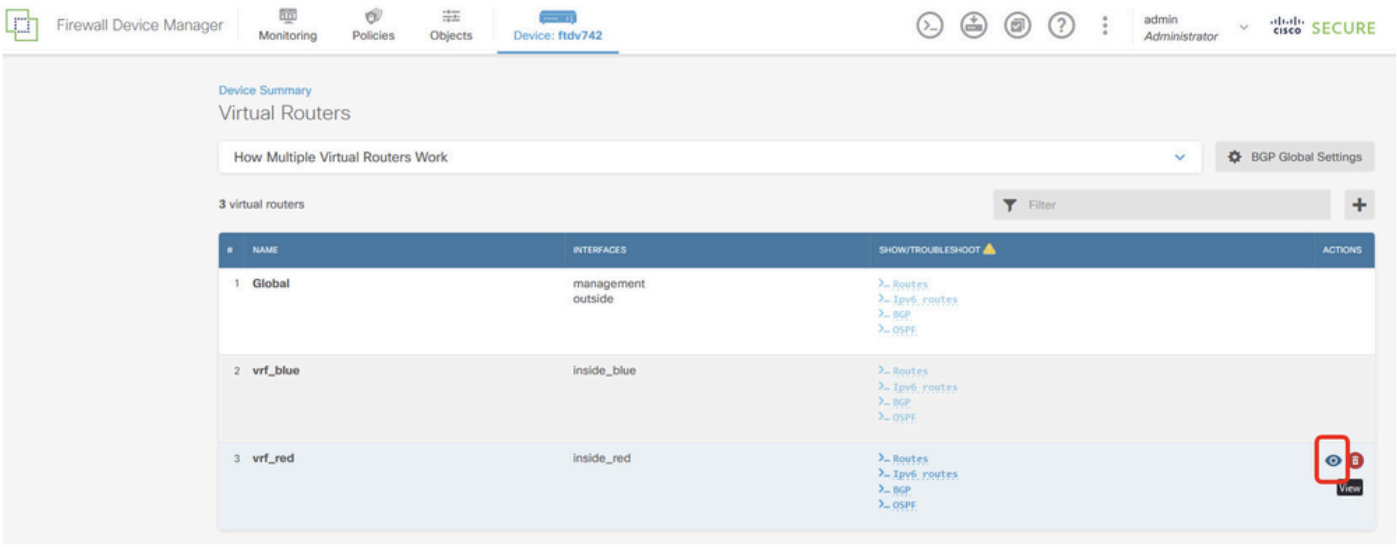


FTD_Create_Static_Route_VRF_Blue_Details

6단계. vrf_red에서 전역으로 경로 누수를 생성합니다. 이 경로는 192.168.10.0/24 네트워크의 엔드포인트가 사이트 간 VPN 터널을 통과하는 연결을 시작할 수 있도록 합니다. 이 예에서 원격 엔드포

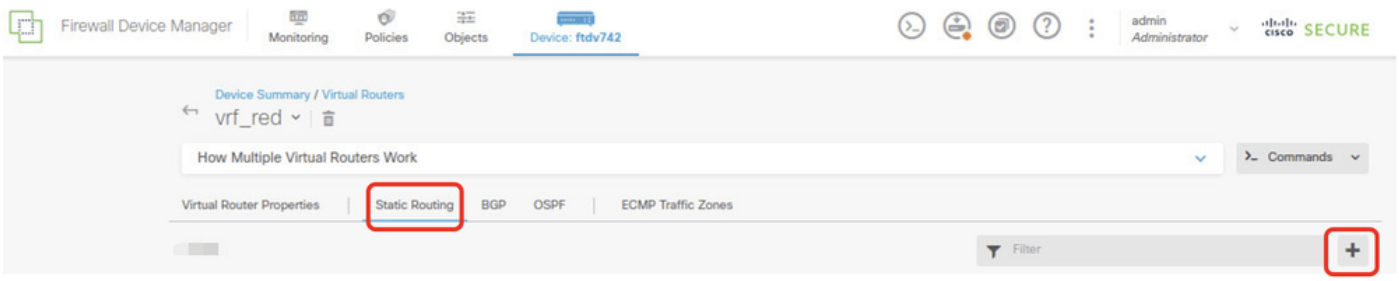
인트는 192.168.50.0/24 네트워크를 보호하고 있습니다.

Device(디바이스) > Routing(라우팅)으로 이동합니다. 구성 보기를 누릅니다. 보기 아이콘을 누릅니다. 가상 라우터 vrf_red에 대한 Action(작업) 셀.



FTD_뷰_VRF_레드

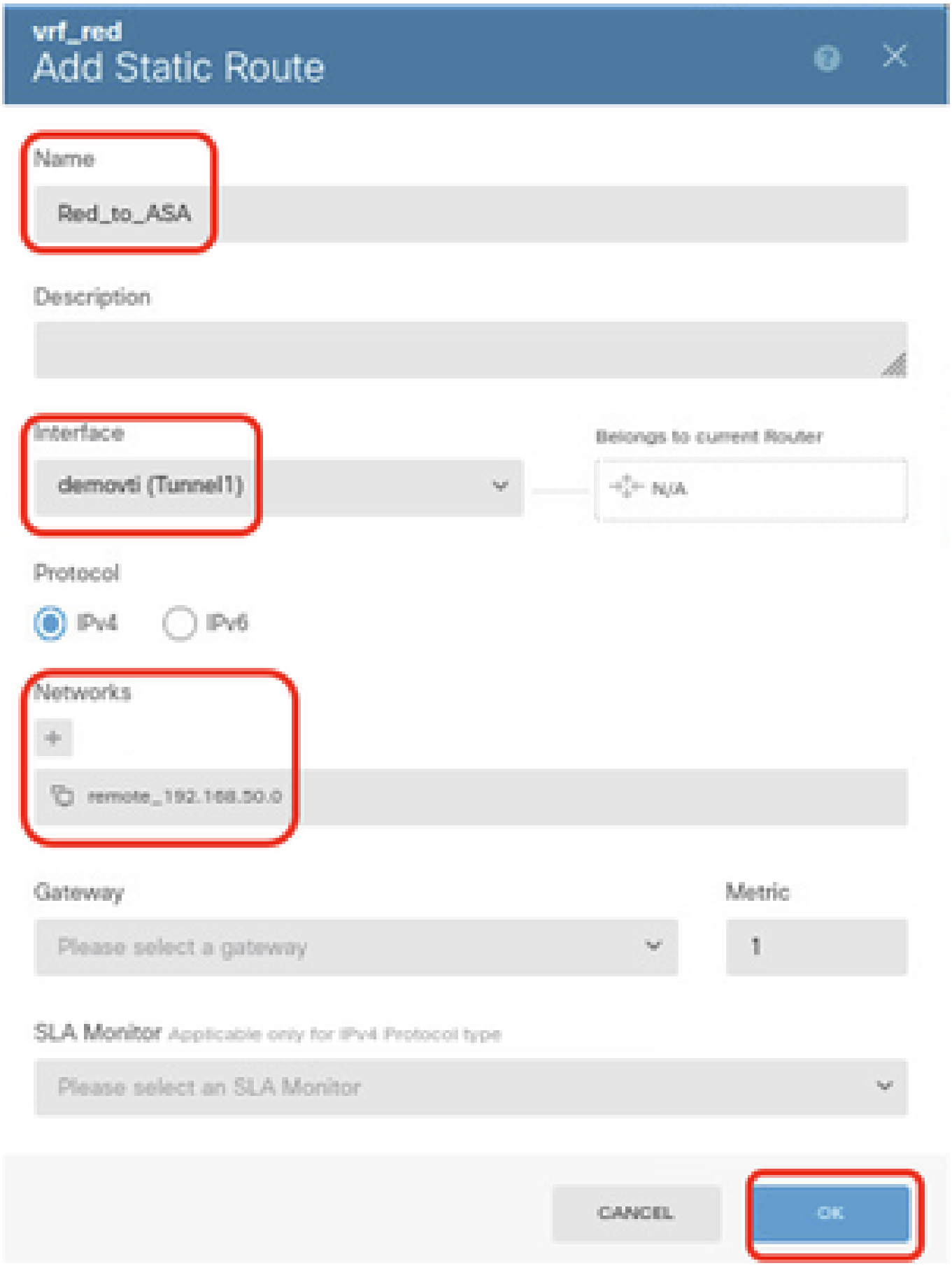
6.1단계. Static Routing(정적 라우팅) 탭을 클릭합니다. +단추를 클릭합니다.



FTD_Create_Static_Route_VRF_Red

6.2단계. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: Red_to_ASA
- 인터페이스: demovti(터널1)
- 네트워크: remote_192.168.50.0
- 게이트웨이: 이 항목은 비워 둡니다.

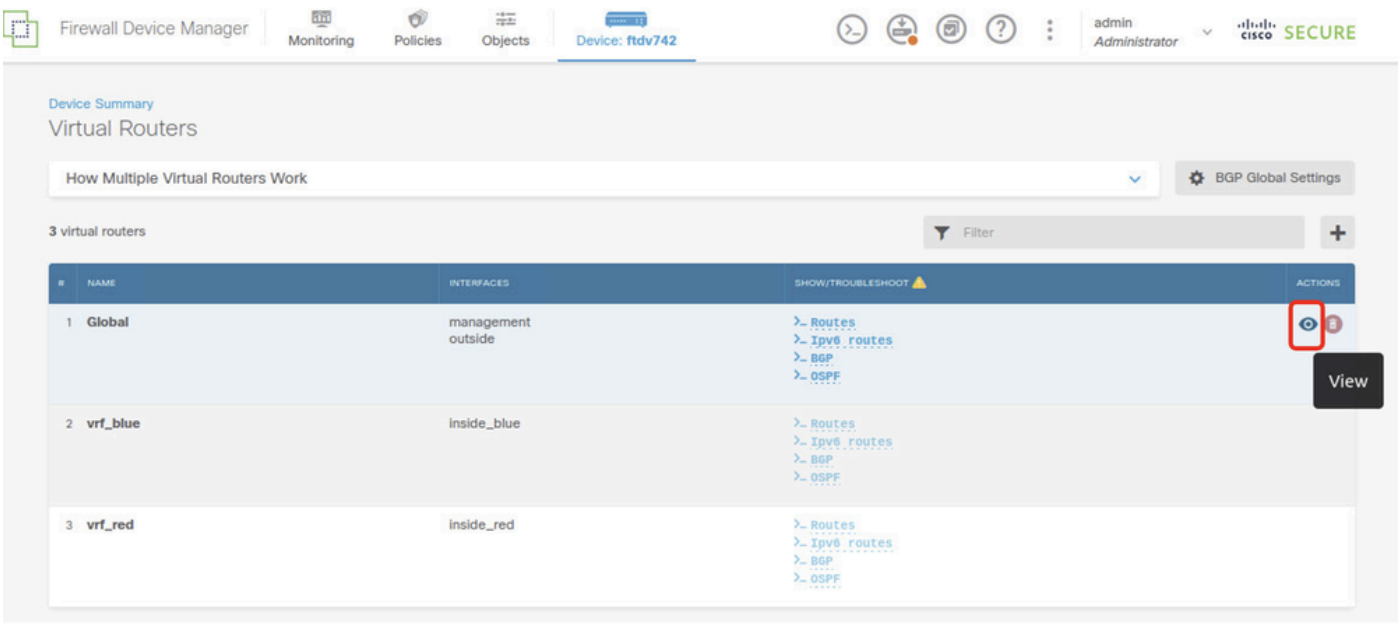


FTD_Create_Static_Route_VRF_Red_Details

7단계. Global에서 가상 라우터로의 경로 유출 생성 이 경로를 통해 사이트 대 사이트 VPN의 원격 끝점으로 보호되는 엔드포인트가 vrf_red 가상 라우터의 192.168.10.0/24 네트워크 및 vrf_blue 가상

라우터의 192.168.20.0/24 네트워크에 액세스할 수 있습니다.

Device(디바이스) > Routing(라우팅)으로 이동합니다. 구성 보기를 누릅니다. 전역 가상 라우터에 대한 작업 셀에서 보기 아이콘을 누릅니다.



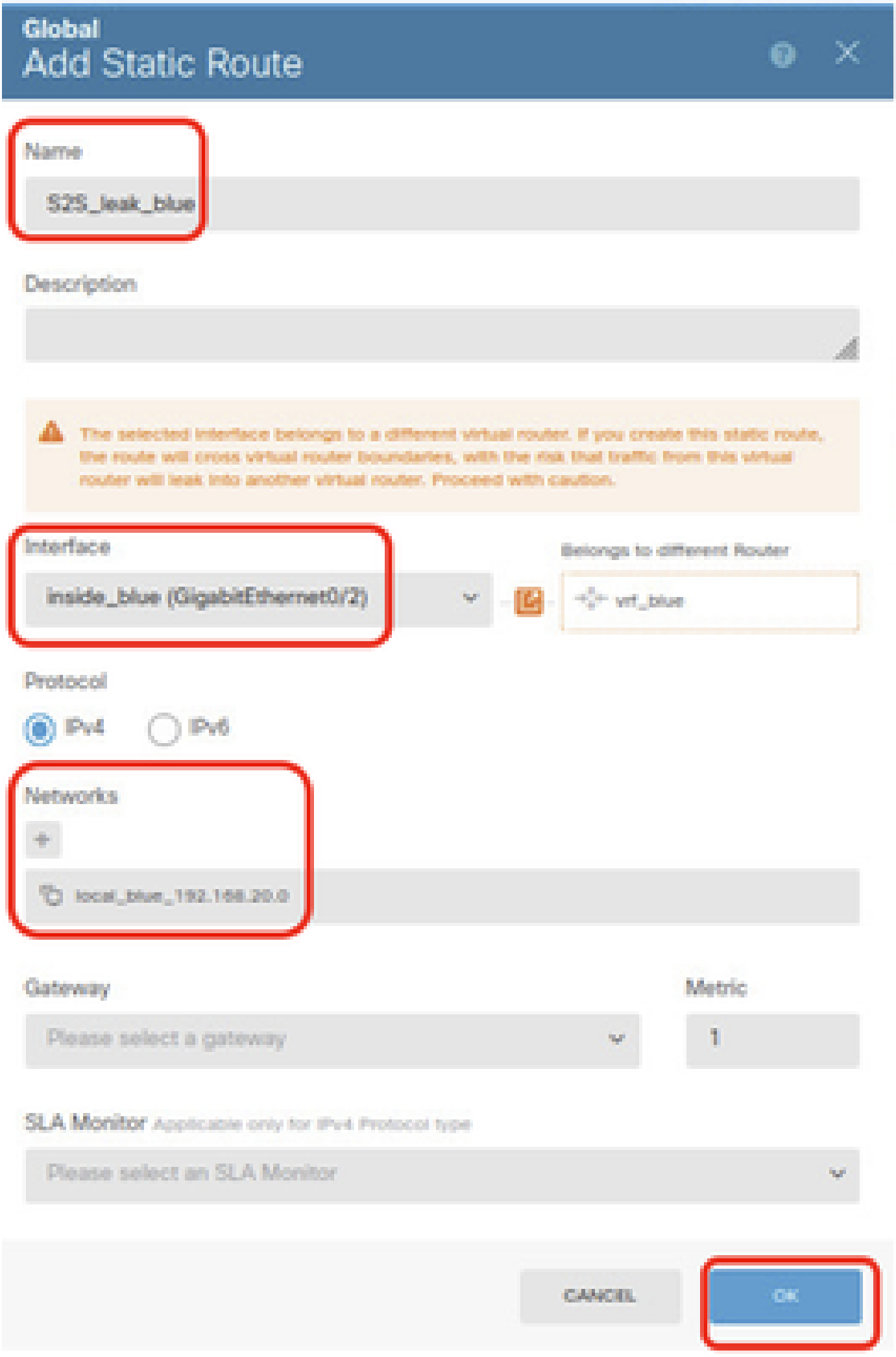
FTD_View_VRF_Global

7.1단계. Static Routing(정적 라우팅) 탭을 클릭합니다. +단추를 클릭합니다.

FTD_Create_Static_Route_VRF_Global

7.2단계. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: S2S_leak_blue
- 인터페이스: inside_blue(GigabitEthernet0/2)
- 네트워크: local_blue_192.168.20.0
- 게이트웨이: 이 항목은 비워 둡니다.


Global
Add Static Route
Name
S2S_leak_blue
Description
The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.
Interface
inside_blue (GigabitEthernet0/2)
Belongs to different Router
vrf_blue
Protocol
IPv4
IPv6
Networks
local_blue_192.168.20.0
Gateway
Please select a gateway
Metric
1
SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor
CANCEL
OK

```
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 21 20 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

10단계. FTD에 구성된 것과 동일한 매개변수를 정의하는 IKEv2 ipsec-proposal을 생성합니다.

```
<#root>

crypto ipsec ikev2 ipsec-proposal

AES-SHA


 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

11단계. ipsec 프로필, 참조 ipsec-proposal이 10단계에서 생성되었습니다.

```
<#root>

crypto ipsec profile

demo_ipsec_profile


 set ikev2 ipsec-proposal

AES-SHA


 set security-association lifetime kilobytes 4608000
 set security-association lifetime seconds 28800
```

12단계. IKEv2 프로토콜을 허용하는 그룹 정책을 생성합니다.

```
<#root>

group-policy

demo_gp_192.168.30.1

 internal
group-policy demo_gp_192.168.30.1 attributes
 vpn-tunnel-protocol ikev2
```

13단계. 12단계에서 생성한 그룹 정책을 참조하여 피어 FTD 외부 IP 주소에 대한 터널 그룹을 생성합니다. ftd(3.7단계에서 생성)와 동일한 사전 공유 키 구성

<#root>

```
tunnel-group 192.168.30.1 type ipsec-l2l
tunnel-group 192.168.30.1 general-attributes
 default-group-policy
```

demo_gp_192.168.30.1

```
tunnel-group 192.168.30.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

14단계. 외부 인터페이스에서 IKEv2를 활성화합니다.

```
crypto ikev2 enable outside
```

15단계. 가상 터널을 생성합니다.

<#root>

```
interface Tunnel1
 nameif demovti_asa
 ip address 169.254.10.2 255.255.255.0
 tunnel source interface outside
 tunnel destination 192.168.30.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile
```

demo_ipsec_profile

16단계. 고정 경로를 생성합니다.

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. 콘솔 또는 SSH를 통해 FTD 및 ASA의 CLI로 이동하여 show crypto ikev2 sa 및 show crypto ipsec sa 명령을 통해 1단계 및 2단계의 VPN 상태를 확인합니다.

FTD:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv742#
ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
 32157565 192.168.30.1/500                                      192.168.40.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/67986 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: 0x4cf55637/0xa493cc83

ftdv742# show crypto ipsec sa
interface: demovti
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1

      Protected vrf (ivrf): Global
      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: 192.168.40.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: A493CC83
      current inbound spi : 4CF55637

    inbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16867)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
```

```
      spi: 0xA493CC83 (2761149571)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4285440/16867)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

ASA:

```
ASA9203# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
 26025779 192.168.40.1/500                               192.168.30.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/68112 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: 0xa493cc83/0x4cf55637
ASA9203#
ASA9203# show cry
ASA9203# show crypto ipsec sa
interface: demovti_asa
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1

      Protected vrf (ivrf): Global
      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: 192.168.30.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 4CF55637
      current inbound spi : A493CC83

    inbound esp sas:
      spi: 0xA493CC83 (2761149571)
         SA State: active
```

```
        transform: esp-aes-256 esp-sha-512-hmac no compression
        in use settings ={L2L, Tunnel, IKEv2, VTI, }
        slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
        sa timing: remaining key lifetime (kB/sec): (4101120/16804)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
    outbound esp sas:
      spi: 0x4CF55637 (1291146807)
        SA State: active
        transform: esp-aes-256 esp-sha-512-hmac no compression
        in use settings ={L2L, Tunnel, IKEv2, VTI, }
        slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
        sa timing: remaining key lifetime (kB/sec): (4055040/16804)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

2단계. FTD에서 VRF 및 전역 경로를 확인합니다.

```
ftdv742# 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 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
SI       192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI       192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside


ftdv742# show route vrf vrf_blue


Routing Table: vrf_blue
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 not set

C        192.168.20.0 255.255.255.0 is directly connected, inside_blue
```

```
L        192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti


ftdv742# show route vrf vrf_red


Routing Table: vrf_red
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 not set

C        192.168.10.0 255.255.255.0 is directly connected, inside_red
L        192.168.10.1 255.255.255.255 is directly connected, inside_red
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

3단계. ping 테스트를 확인합니다.

ping하기 전에 show crypto ipsec sa의 카운터를 확인하십시오 | inc 인터페이스:|encap|decap on FTD.

이 예에서 Tunnel1은 캡슐화 및 캡슐화 해제에 대해 모두 30개의 패킷을 표시합니다.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

Client1 Client3에 대해 ping을 수행했습니다.

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

Client2에서 Client3에 ping을 수행했습니다.

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

카운터 확인 암호화 ipsec sa 표시 | inc 인터페이스:|encap|decap FTD에서 ping에 성공했습니다.

이 예에서 Tunnel1은 성공적인 ping 후 캡슐화와 캡슐화 해제에 모두 40개의 패킷을 표시합니다. 또한 두 카운터가 모두 10개 패킷 증가하여 10개의 ping 에코 요청과 일치했으며, 이는 ping 트래픽이 IPSec 터널을 성공적으로 통과했음을 나타냅니다.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
      #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

이러한 debug 명령을 사용하여 VPN 섹션의 문제를 해결할 수 있습니다.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

이러한 debug 명령을 사용하여 경로 섹션의 문제를 해결할 수 있습니다.

```
debug ip routing
```

참조

Cisco Secure Firewall Device Manager 컨피그레이션 가이드, 버전 7.4

Cisco Secure Firewall ASA VPN CLI 구성 가이드, 9.20

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.