FDM에서 관리하는 FTD에서 PBR을 사용하여 듀얼 활성 경로 기반 Site-to-Site VPN 구성

목차

소개

이 문서에서는 FDM에서 관리되는 FTD에서 PBR을 사용하여 듀얼 활성 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
- PBR(Policy Based Routing)에 대한 기본 이해
- IP SLA(Internet Protocol Service Level Agreement)의 기본 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

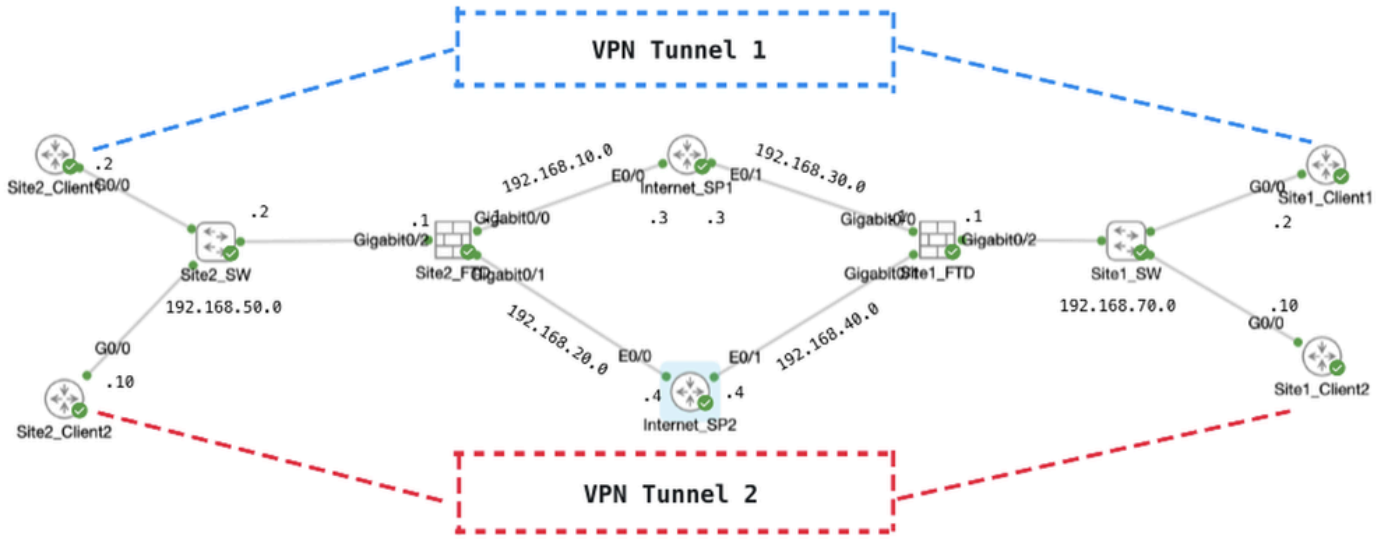
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 FTD에서 듀얼 액티브 경로 기반 사이트 대 사이트 VPN을 구성하는 방법에 대해 설명합니다. 이 예에서 Site1 및 Site2의 FTD는 두 ISP를 동시에 사용하여 사이트 대 사이트 VPN을 설정하는 듀얼 액티브 ISP 연결을 갖습니다. 기본적으로 VPN 트래픽은 ISP1(파란색 선)을 통해 터널 1을 통과합니다. 특정 호스트의 경우 트래픽이 ISP2를 통해 터널 2를 통과합니다(빨간색 선). ISP1에 중단이 발생하면 트래픽은 백업으로 ISP2로 전환됩니다. 반대로, ISP2에서 중단이 발생하면 트래픽은 백업으로 ISP1로 전환됩니다. 이 예에서는 PBR(Policy-Based Routing) 및 IP SLA(Internet Protocol Service Level Agreement)를 사용하여 이러한 요구 사항을 충족합니다.

구성

네트워크 다이어그램



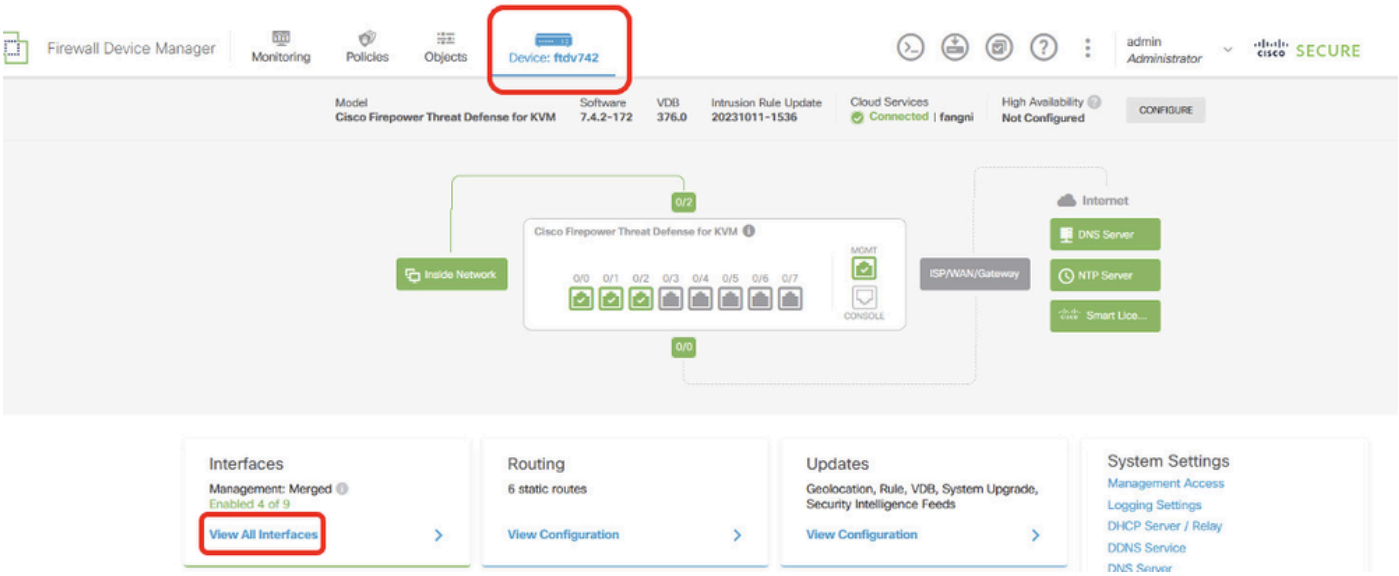
토폴로지

VPN의 컨피그레이션

노드 간 IP 상호 연결의 예비 컨피그레이션이 올바르게 완료되었는지 확인하는 것이 중요합니다. Site1 및 Site2의 클라이언트는 FTD 내부 IP 주소를 게이트웨이로 사용합니다.

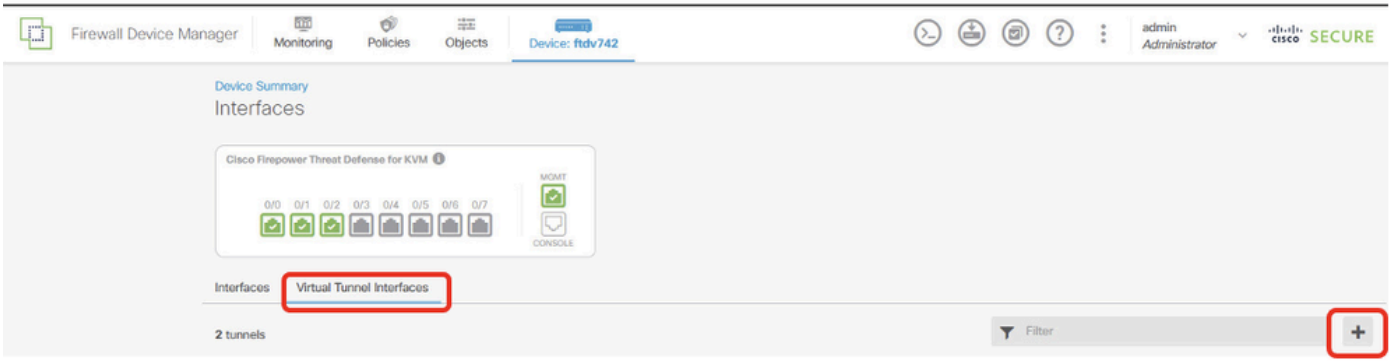
Site1 FTD VPN 컨피그레이션

1단계. ISP1 및 ISP2에 대한 가상 터널 인터페이스를 생성합니다. Site1 FTD의 FDM GUI에 로그인합니다. Device > Interfaces로 이동합니다. View All Interfaces를 클릭합니다.



Site1FTD_View_All_Interfaces

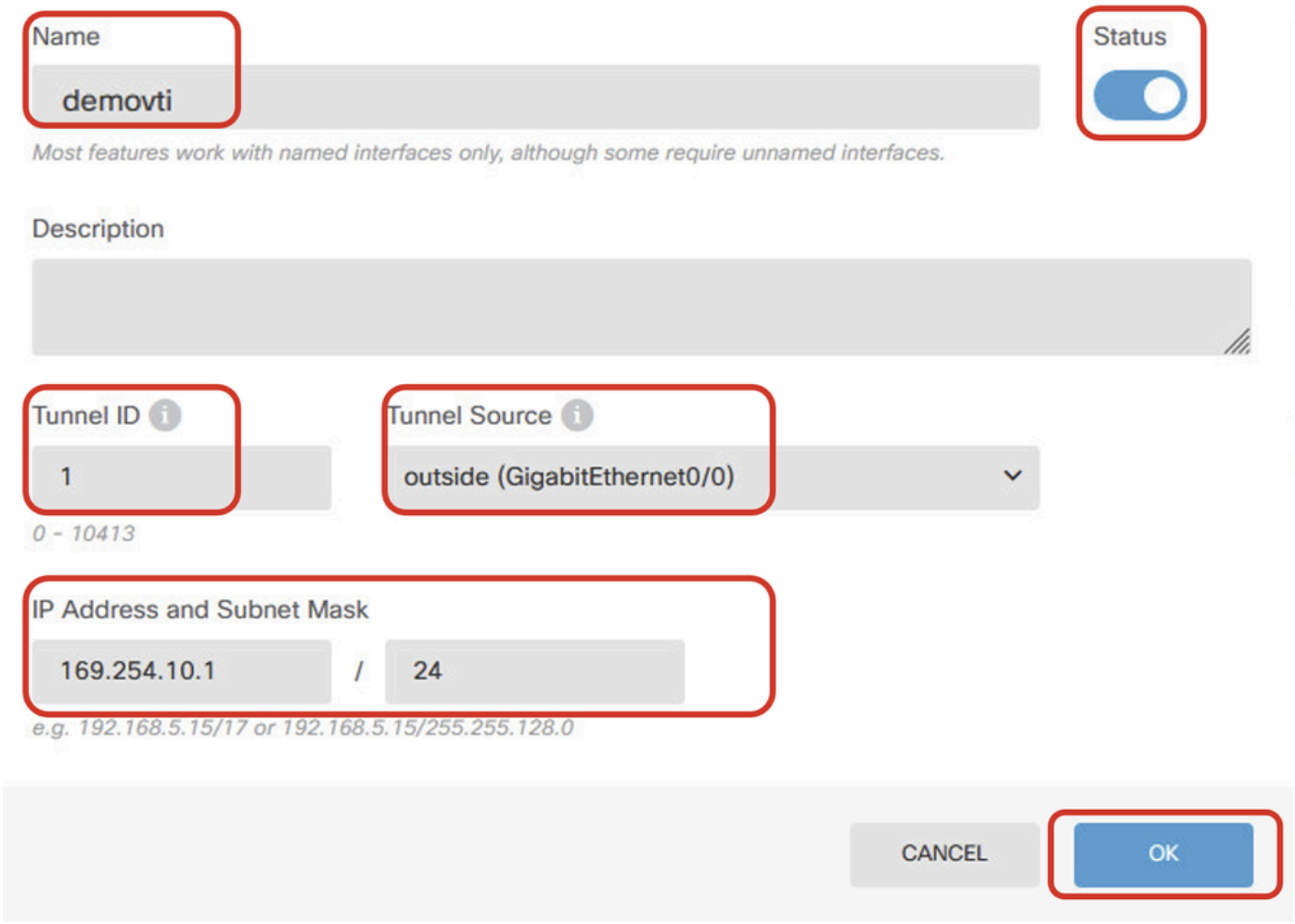
2단계. Virtual Tunnel Interfaces(가상 터널 인터페이스) 탭을 클릭한 다음 + 버튼을 클릭합니다.



Site1FTD_Create_VTI

3단계. VTI 세부사항에 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

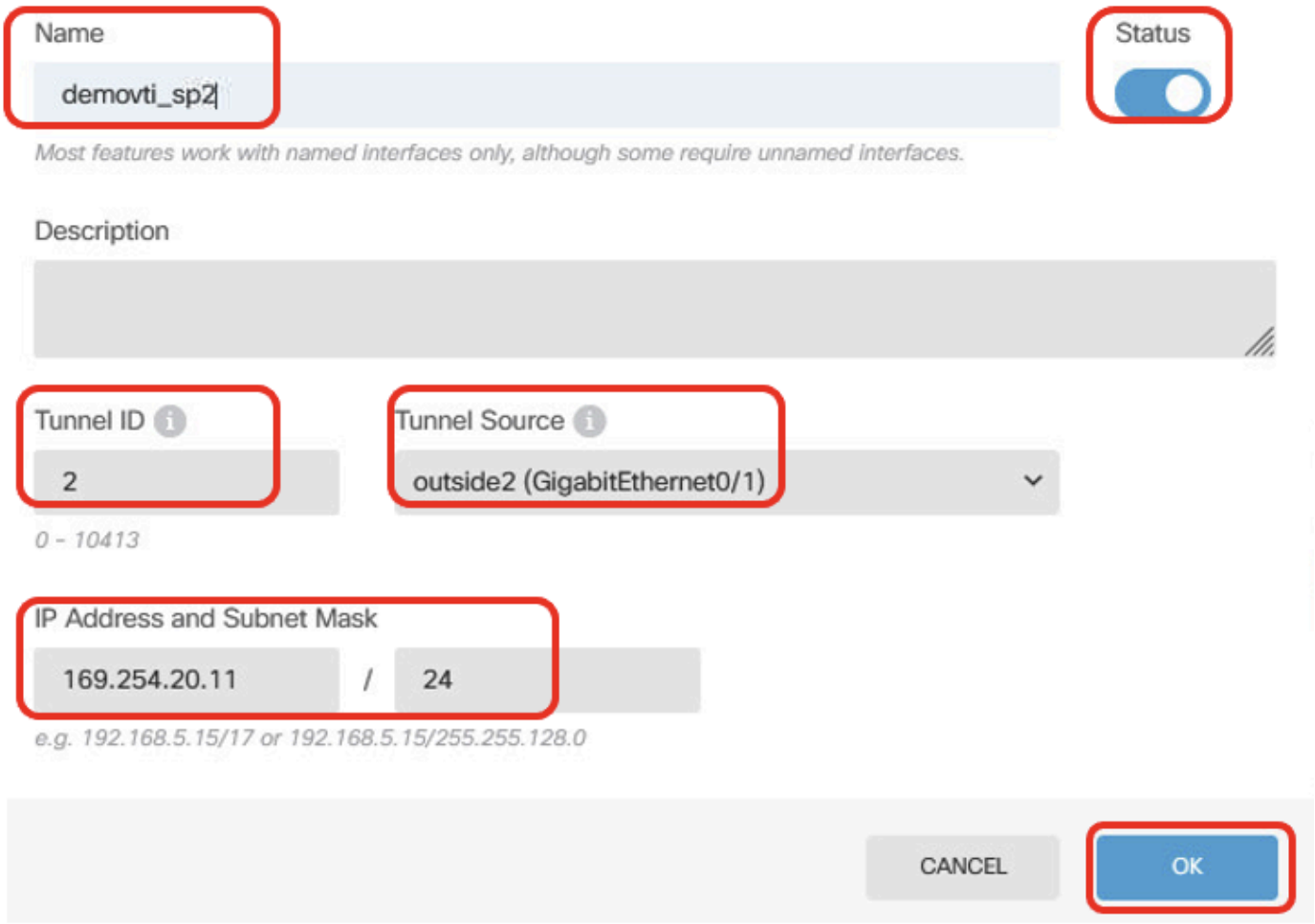
- 이름: 제거
- 터널 ID: 1
- 터널 원본: 외부(GigabitEthernet0/0)
- IP 주소 및 서브넷 마스크: 169.254.10.1/24
- 상태: Enabled(활성화됨) 위치에 있는 슬라이더를 클릭합니다.



Site1FTD_VTI_Details_Tunnel1_ISP1

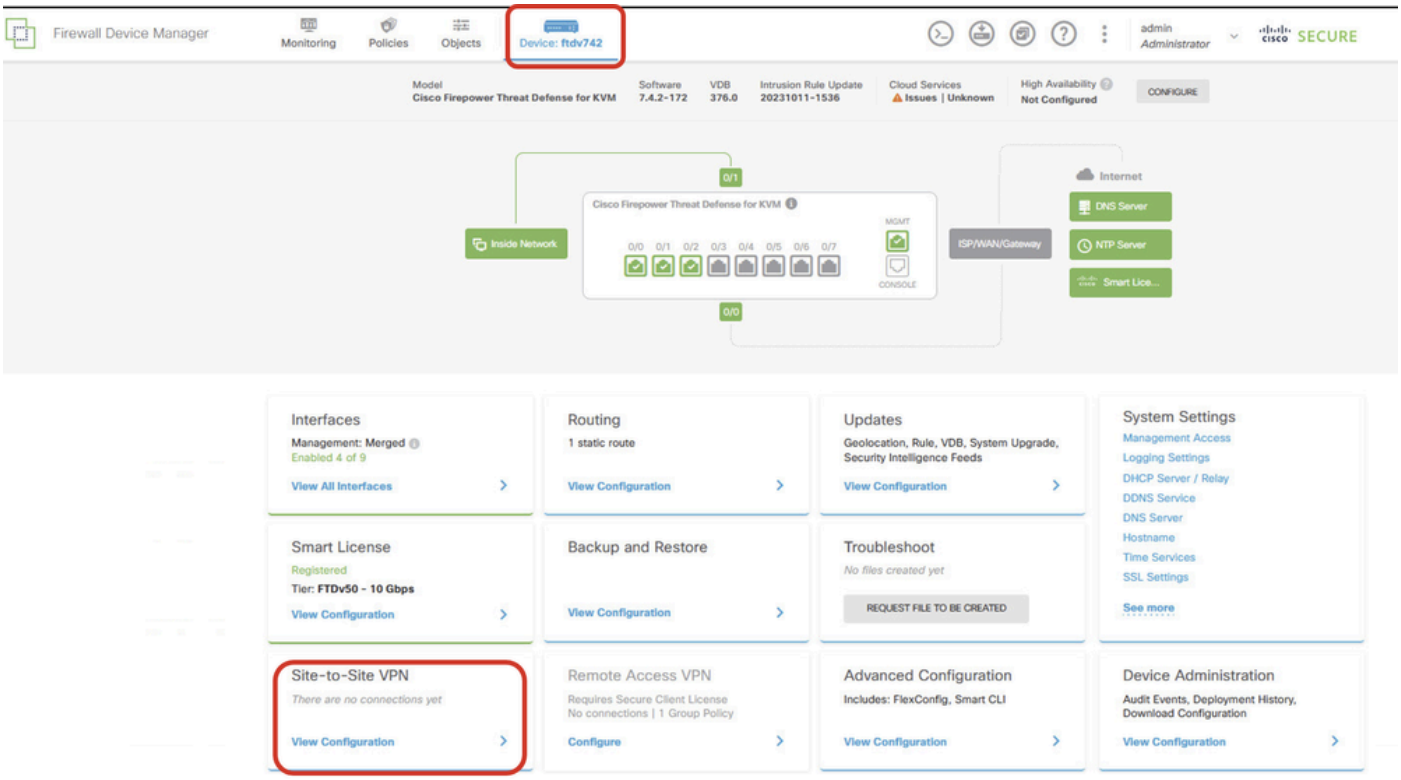
- 이름: 제거(_sp2)
- 터널 ID: 2

- 터널 원본: outside2(GigabitEthernet0/1)
- IP 주소 및 서브넷 마스크: 169.254.20.11/24
- 상태: Enabled(활성화됨) 위치에 있는 슬라이더를 클릭합니다.



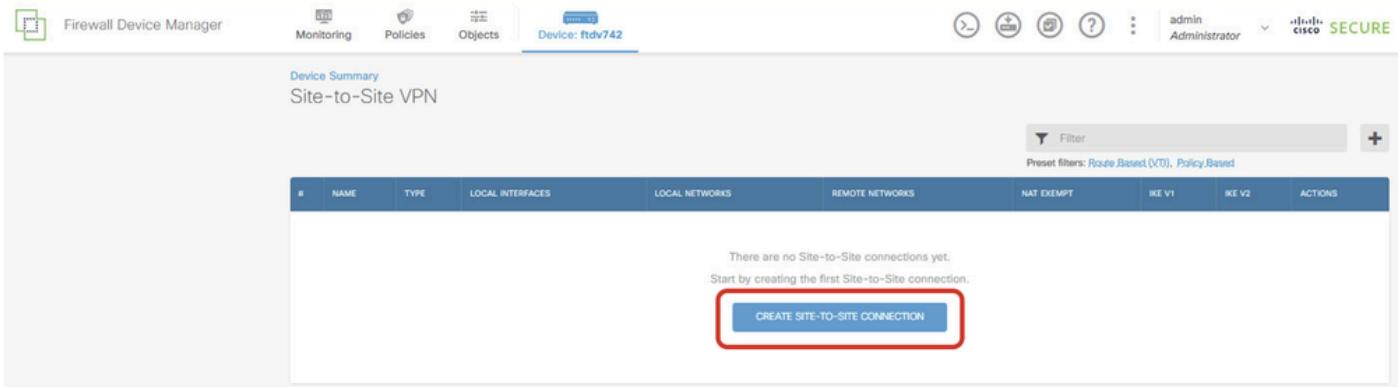
Site1FTD_VTI_Details_Tunnel2_ISP2

4단계. Device(디바이스) > Site-to-Site VPN으로 이동합니다. View Configuration(컨피그레이션 보기) 버튼을 클릭합니다.



Site1FTD_View_Site2Site_VPN

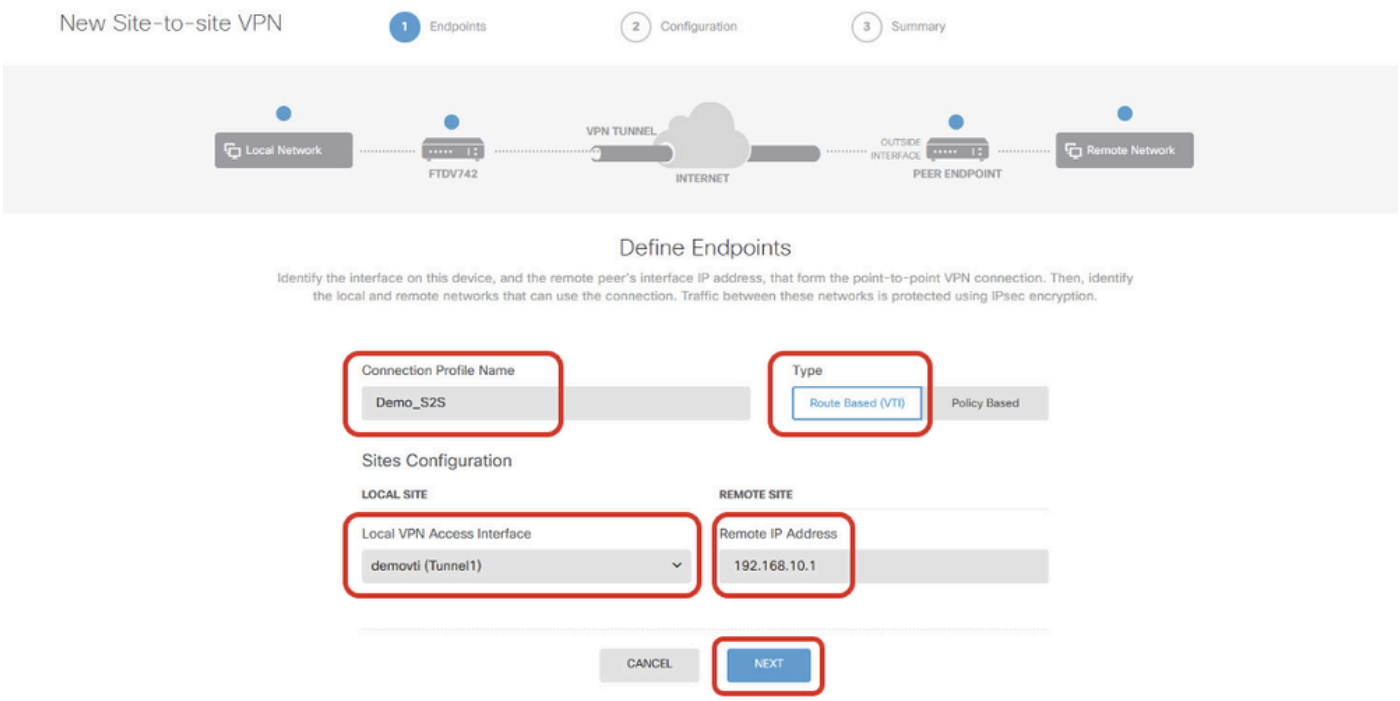
5단계. ISP1을 통해 새 Site-to-Site VPN을 만들기 시작합니다. CREATE SITE-TO-SITE CONNECTION(SITE-TO-SITE 연결 만들기) 버튼을 클릭하거나 + 버튼을 클릭합니다.



Site1FTD_Create_Site-to-Site_Connection

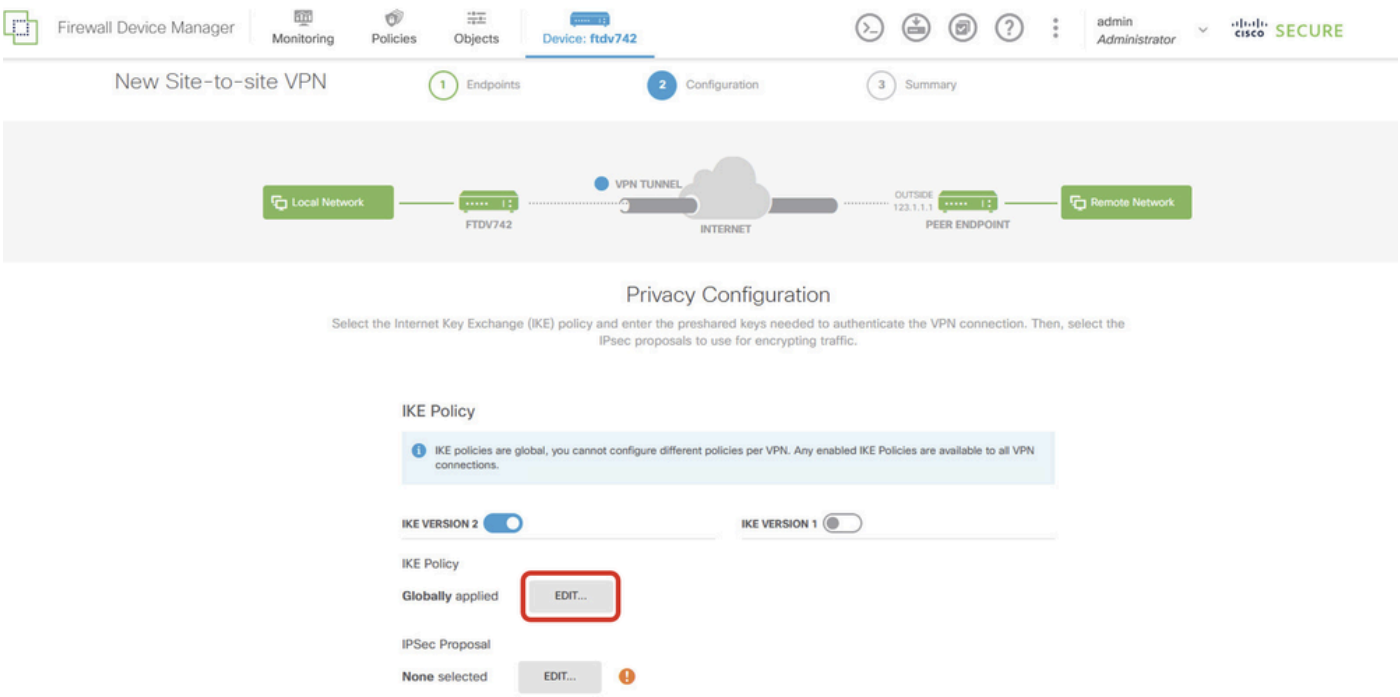
5.1단계. 엔드포인트에 필요한 정보를 제공합니다. Next(다음) 버튼을 클릭합니다.

- 연결 프로파일 이름: 데모_S2S
- 유형: 경로 기반(VTI)
- 로컬 VPN 액세스 인터페이스: demovti(3단계에서 생성됨)
- 원격 IP 주소: 192.168.10.1(Site2 FTD ISP1 IP 주소)



Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

5.2단계. IKE Policy(IKE 정책)로 이동합니다. Edit(편집) 버튼을 클릭합니다.

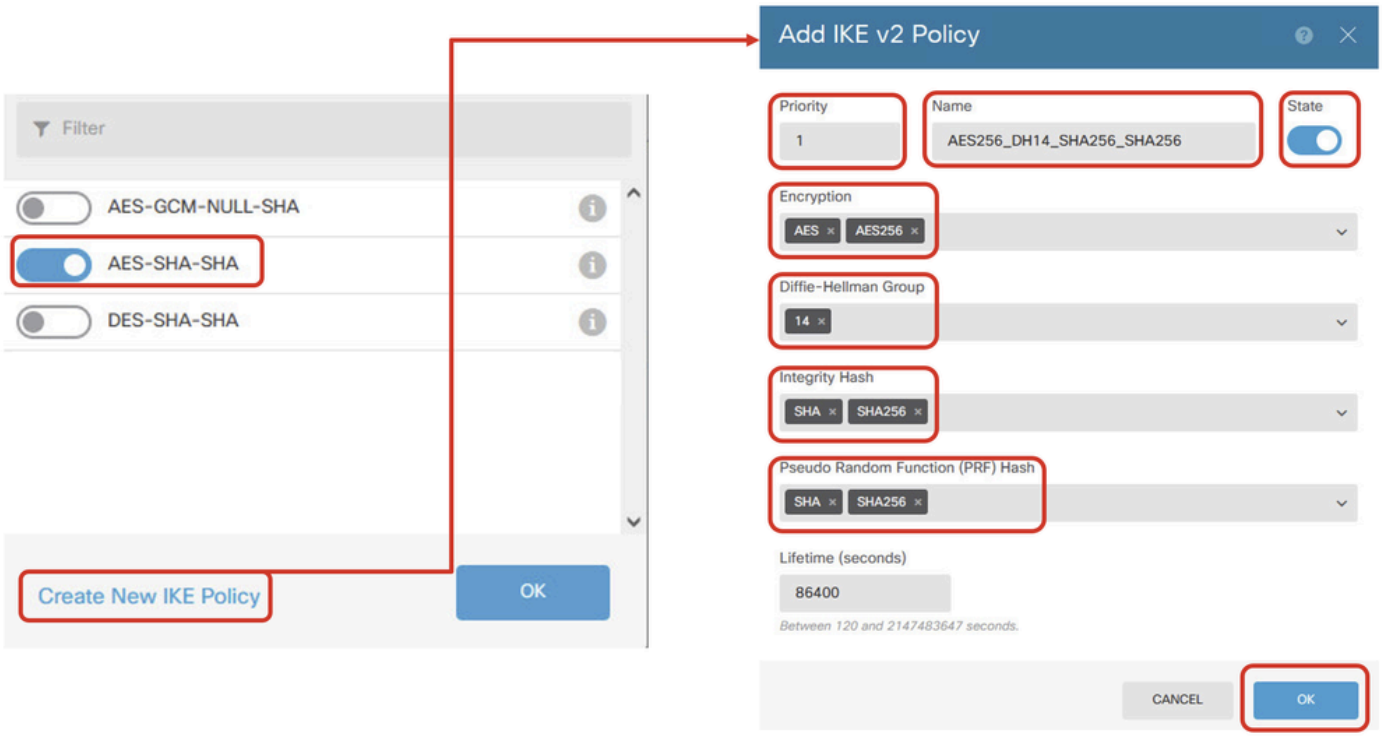


Site1FTD_Edit_IKE_Policy

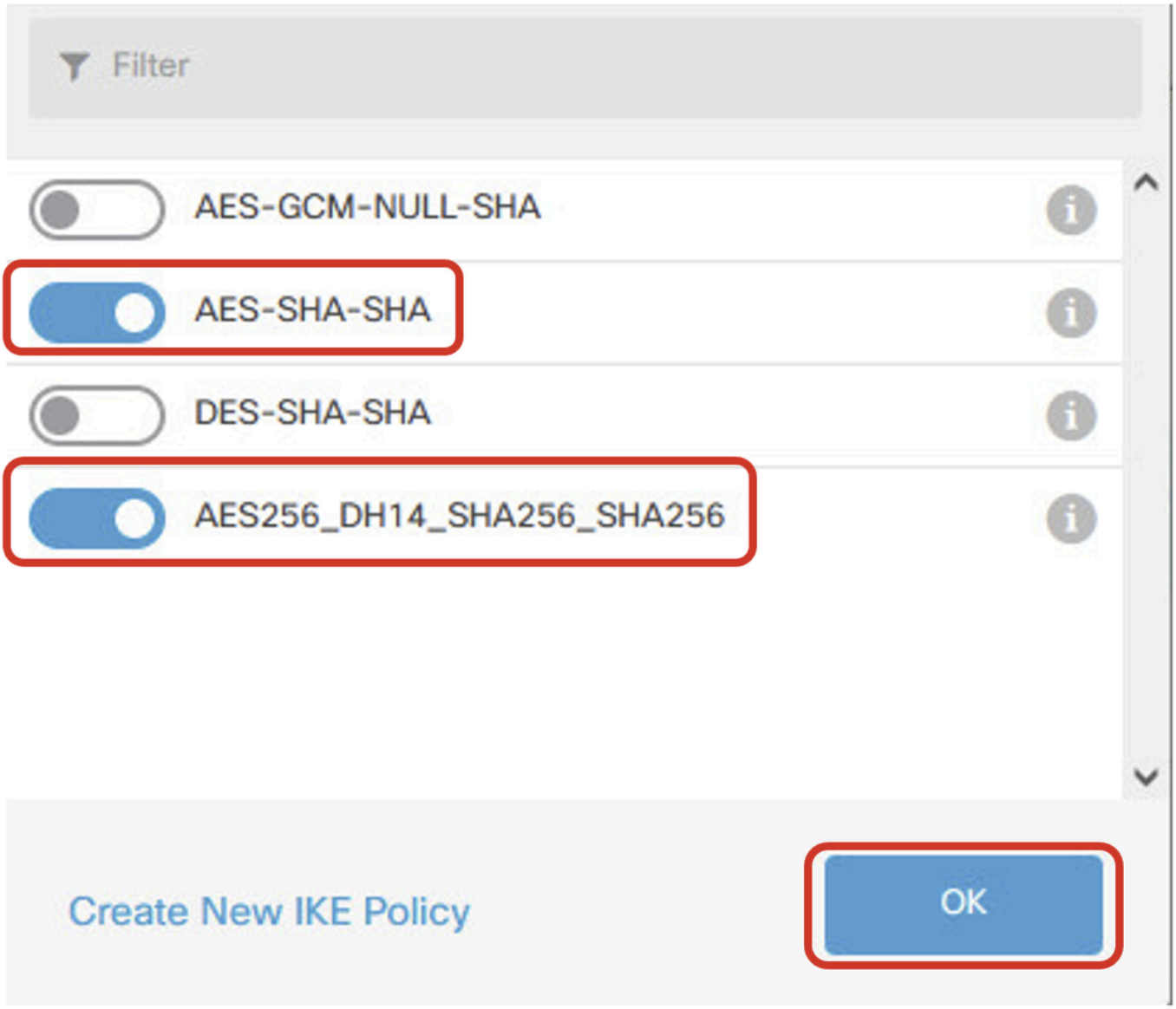
5.3단계. IKE 정책의 경우 미리 정의된 정책을 사용하거나 Create New IKE Policy(새 IKE 정책 생성)를 클릭하여 새 정책을 생성할 수 있습니다.

이 예에서는 기존 IKE 정책 AES-SHA-SHA를 토글하고 데모용으로 새 정책을 생성합니다. 저장하려면 OK(확인) 버튼을 클릭합니다.

- 이름: AES256_DH14_SHA256_SHA256
- 암호화: AES, AES256
- DH 그룹: 14
- 무결성 해시: SHA, SHA256
- PRF 해시: SHA, SHA256
- 수명: 86400(기본값)

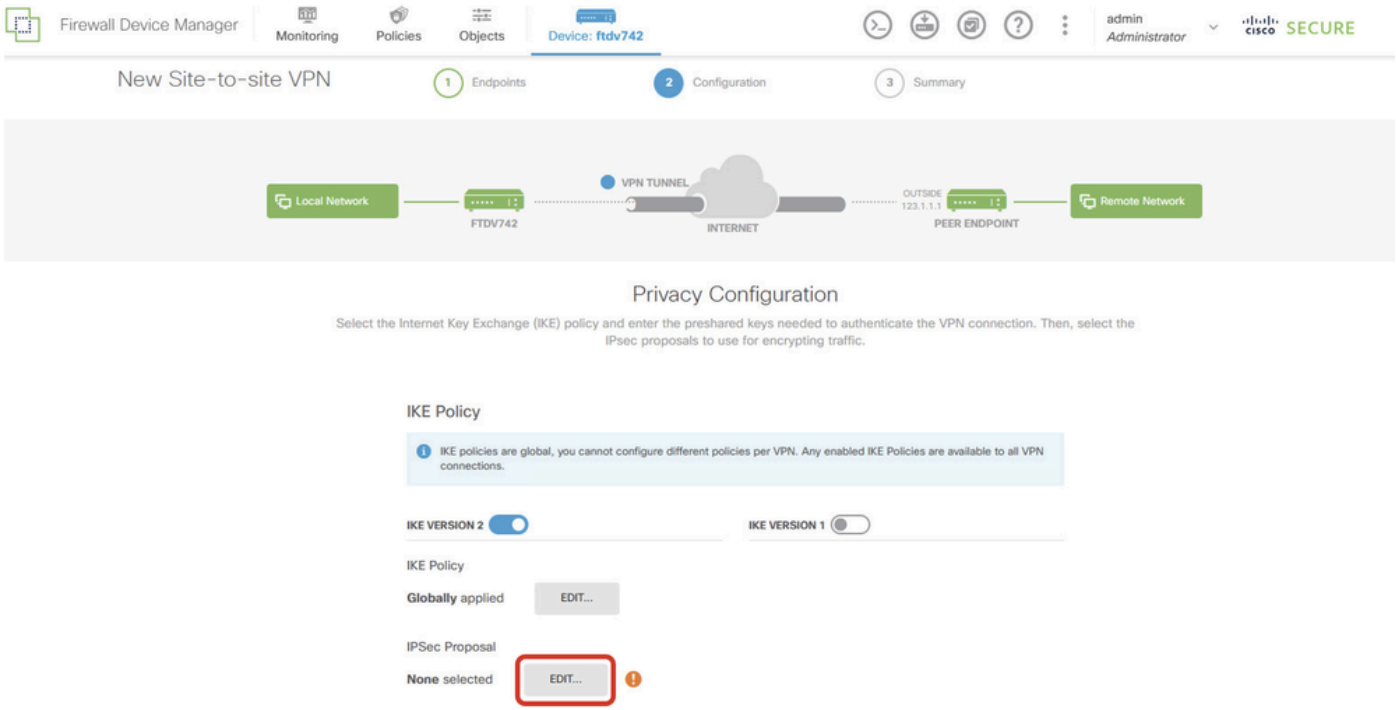


Site1FTD_Add_New_IKE_Policy



Site1FTD_Enable_New_IKE_Policy

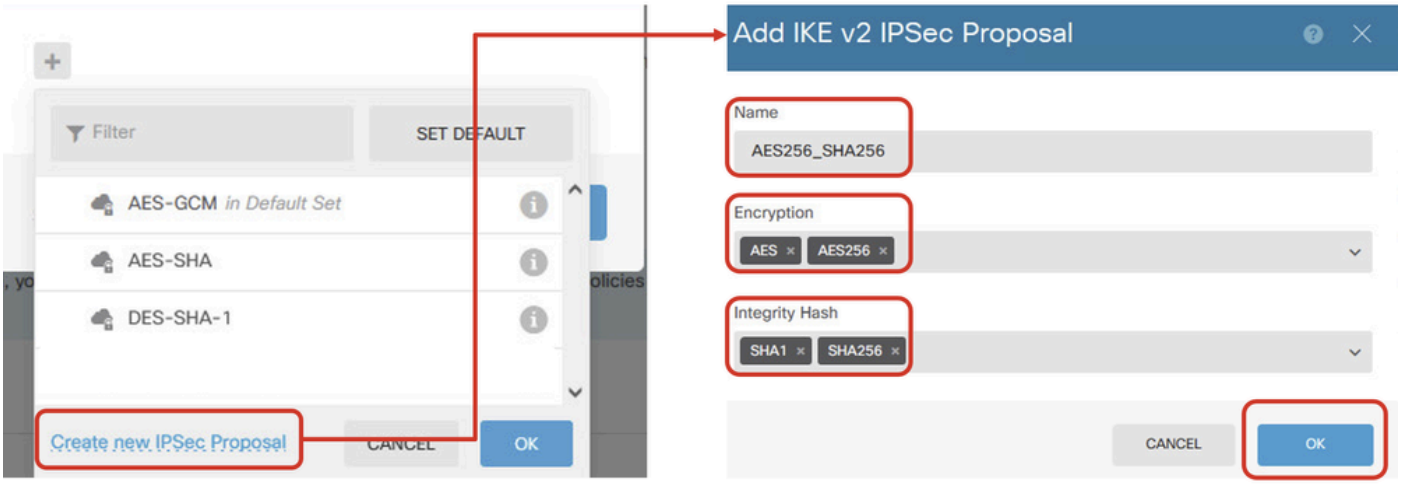
5.4단계. IPSec 제안으로 이동합니다. Edit(편집) 버튼을 클릭합니다.



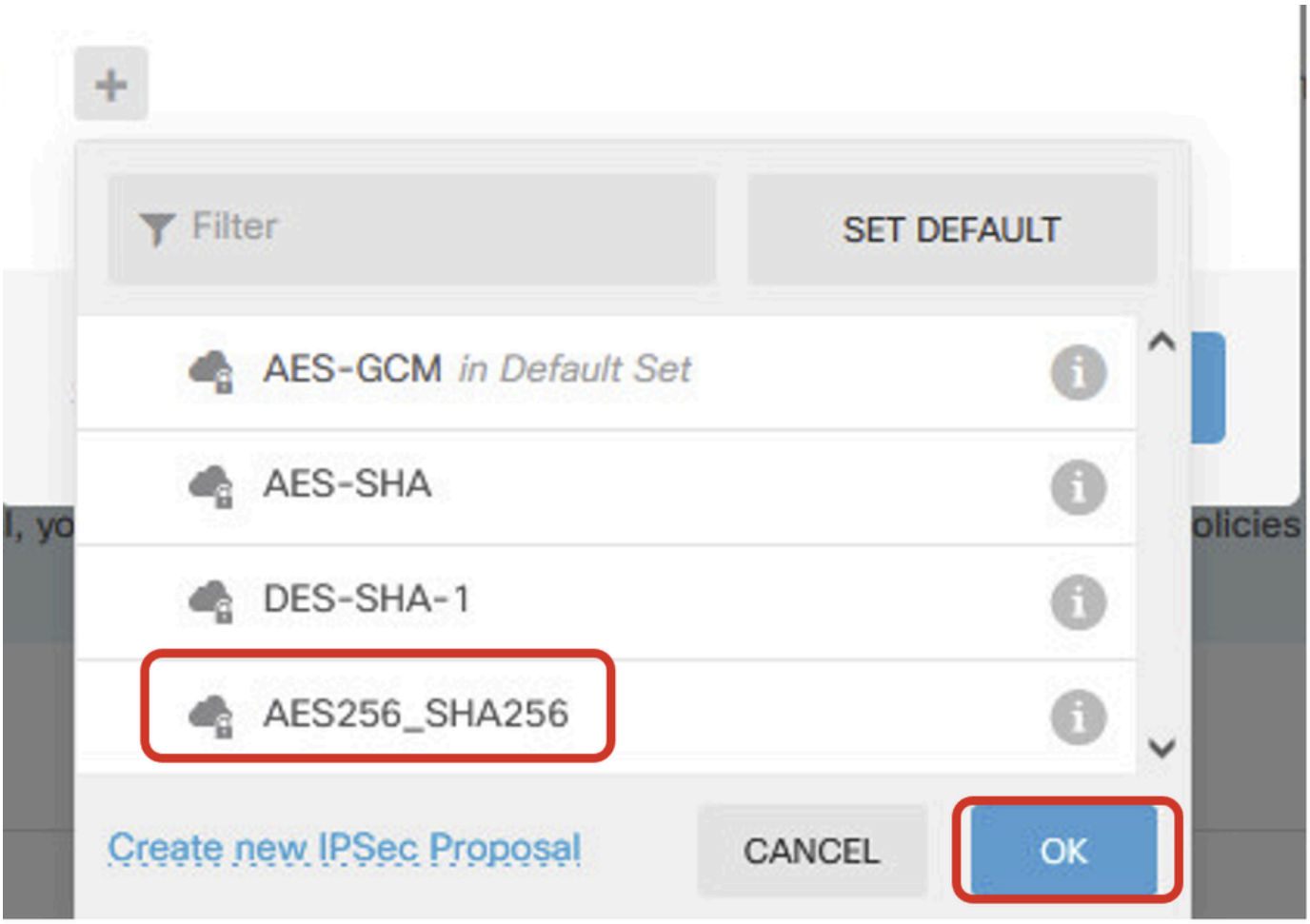
Site1FTD_Edit_IKE_Proposal

5.5단계. IPSec 제안의 경우 미리 정의된 것을 사용하거나 Create new IPSec Proposal(새 IPSec 제안 생성)을 클릭하여 새 제안서를 생성할 수 있습니다. 이 예에서는 데모용으로 새 버전을 만듭니다. 저장하려면 OK(확인) 버튼을 클릭합니다.

- 이름: AES256_SHA256
- 암호화: AES, AES256
- 무결성 해시: SHA1, SHA256



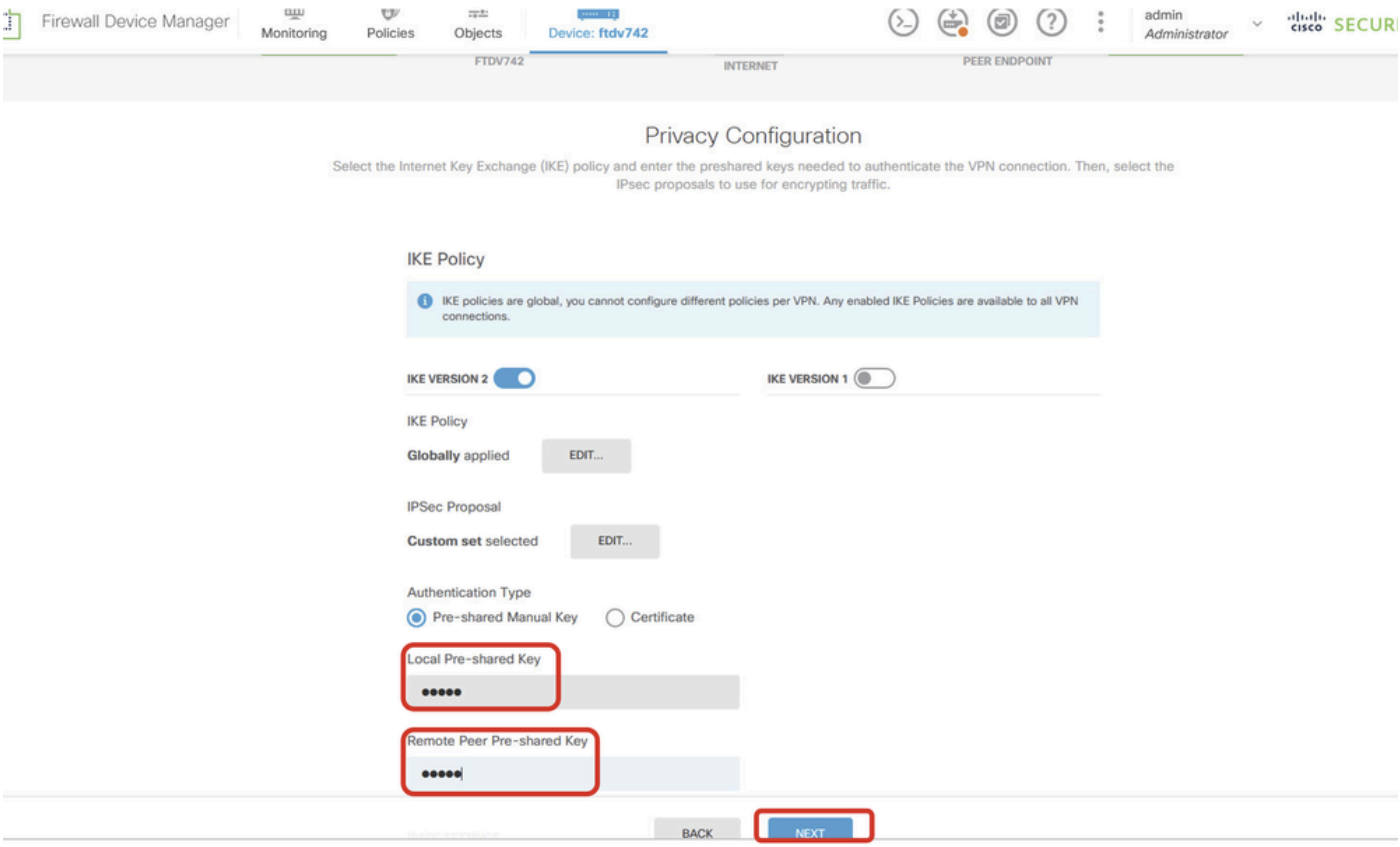
Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

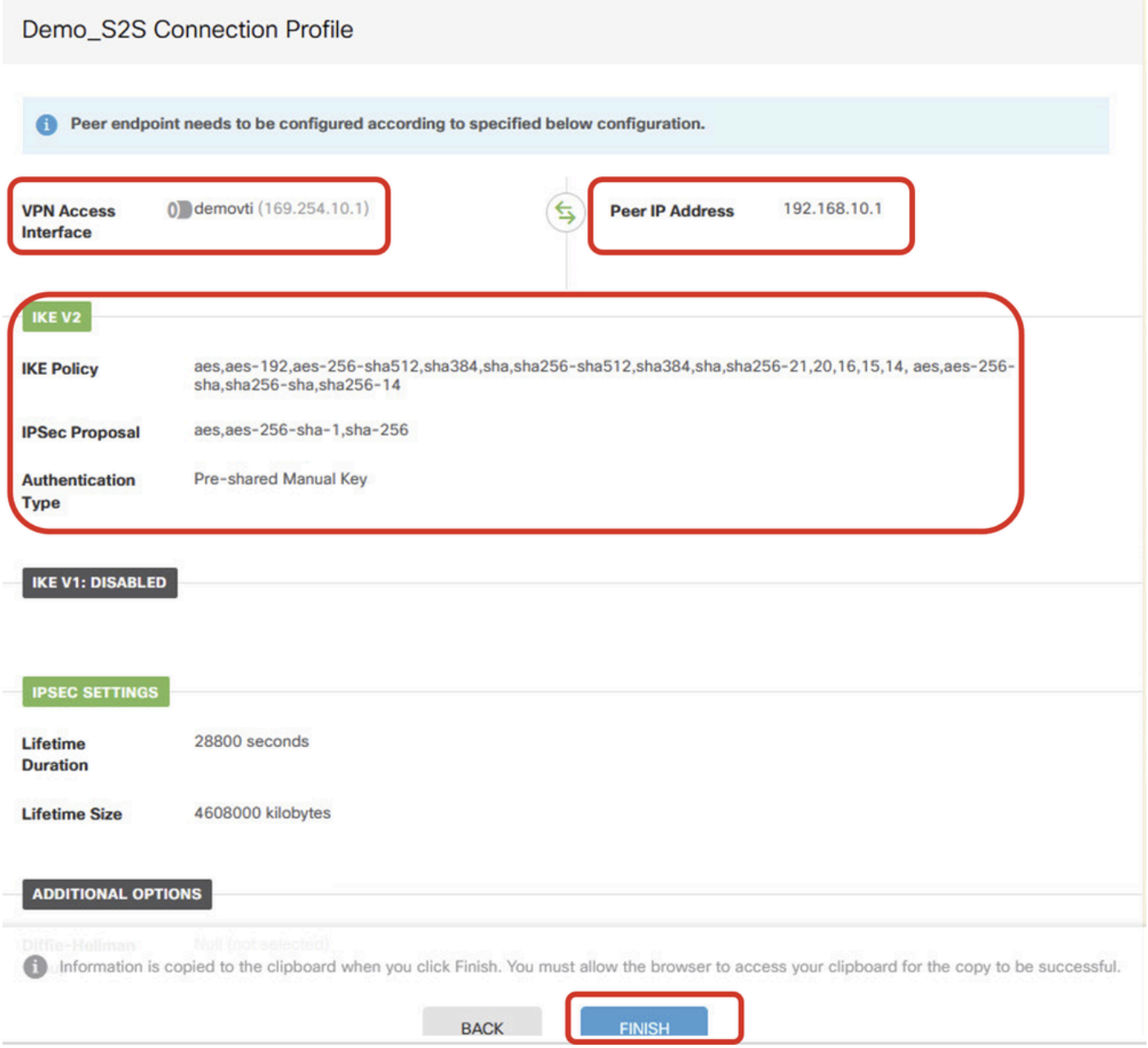
5.6단계. 페이지를 아래로 스크롤하여 사전 공유 키를 구성합니다. NextButton을 클릭합니다.

이 사전 공유 키를 기록해 두고 나중에 Site2 FTD에서 구성합니다.



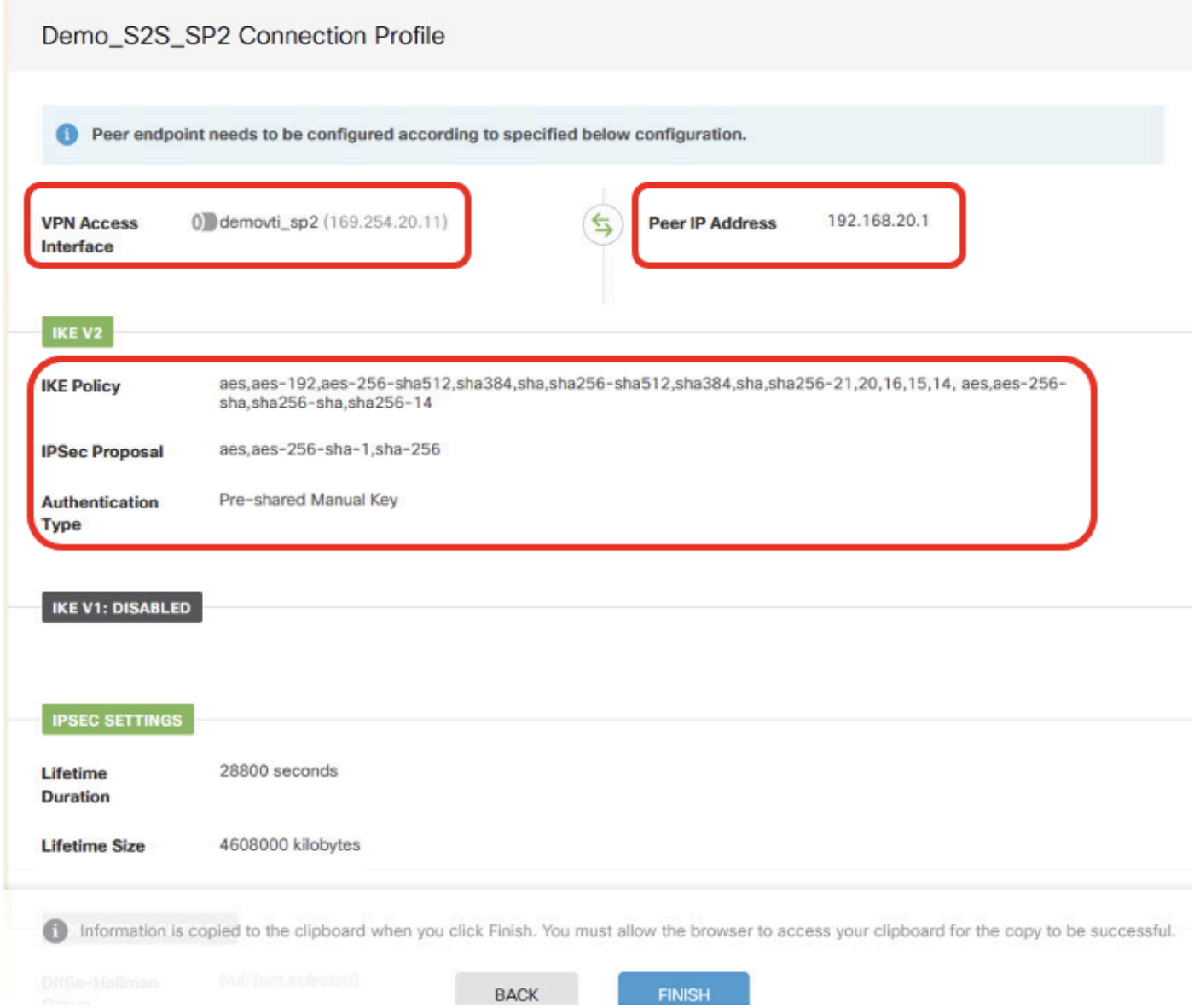
Site1FTD_Configure_Pre_Shared_Key

5.7단계. VPN 컨피그레이션을 검토합니다. 수정해야 할 사항이 있으면 BACK(뒤로) 버튼을 클릭합니다. 모든 것이 정상인 경우 FINISH(마침) 버튼을 클릭합니다.



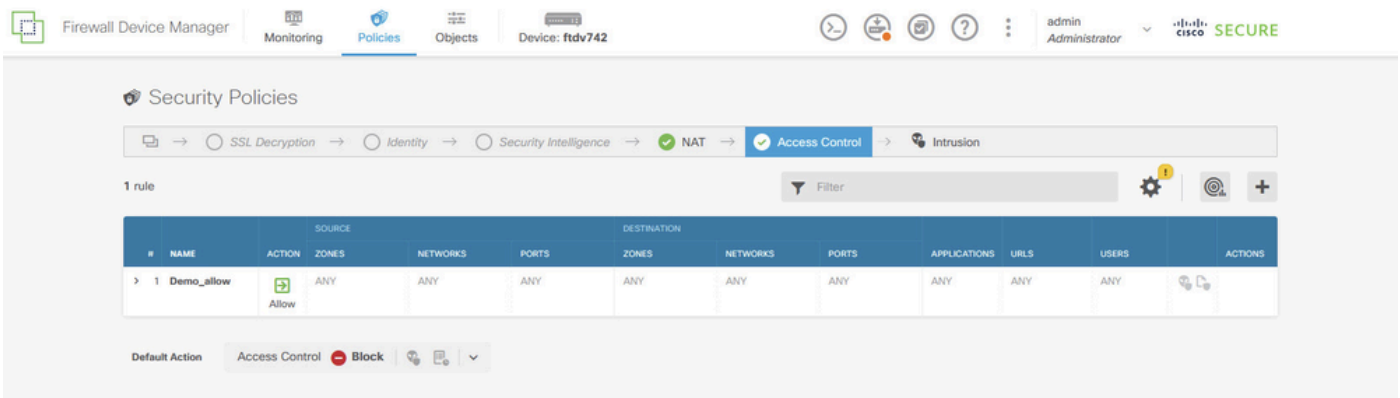
Site1FTD_ISP1_Review_VPN_Config_Summary

6단계. ISP2를 통해 새 Site-to-Site VPN을 생성하려면 5단계를 반복합니다.



Site1FTD_ISP2_Review_VPN_Config_Summary

7단계. 트래픽이 FTD를 통과하도록 허용하는 액세스 제어 규칙을 만듭니다. 이 예에서는 데모용으로 모두 허용합니다. 실제 요구 사항에 따라 정책을 수정합니다.



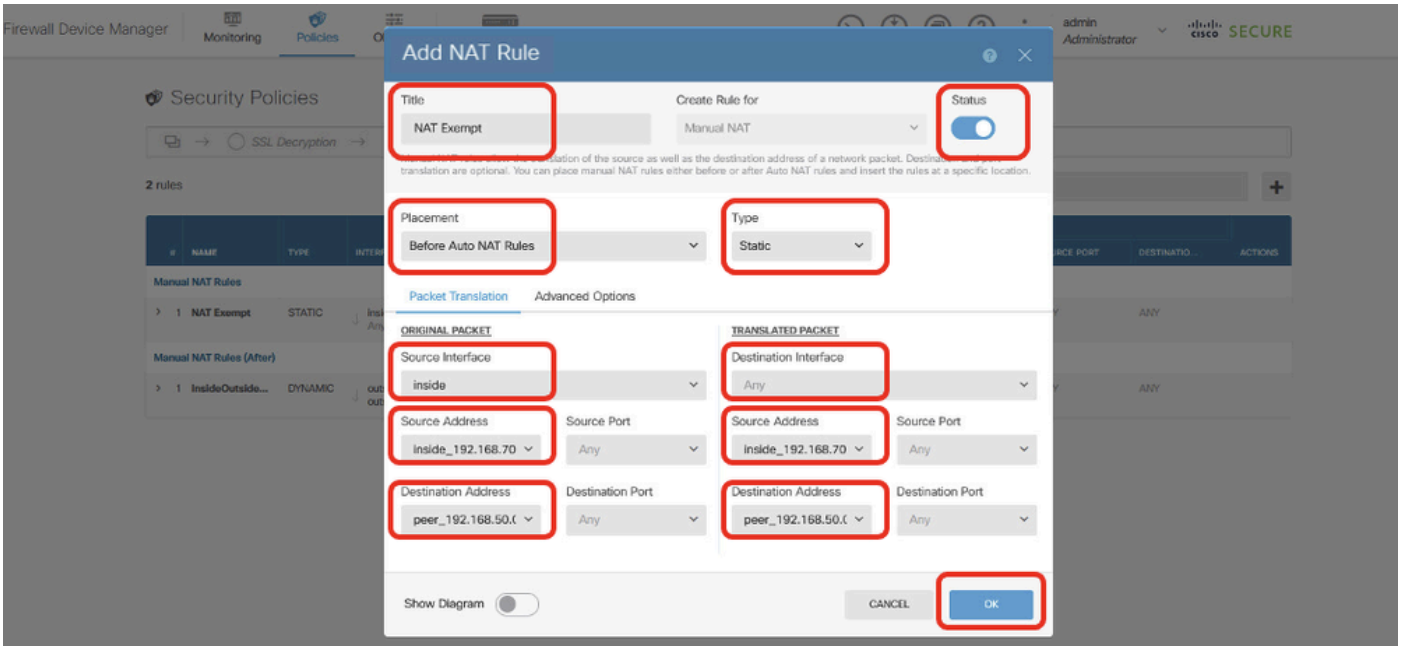
Site1FTD_Allow_Access_Control_Rule_Example

8단계. (선택 사항) 인터넷에 액세스하기 위해 클라이언트에 대해 구성된 동적 NAT가 있는 경우 FTD에서 클라이언트 트래픽에 대한 NAT 제외 규칙을 구성합니다.

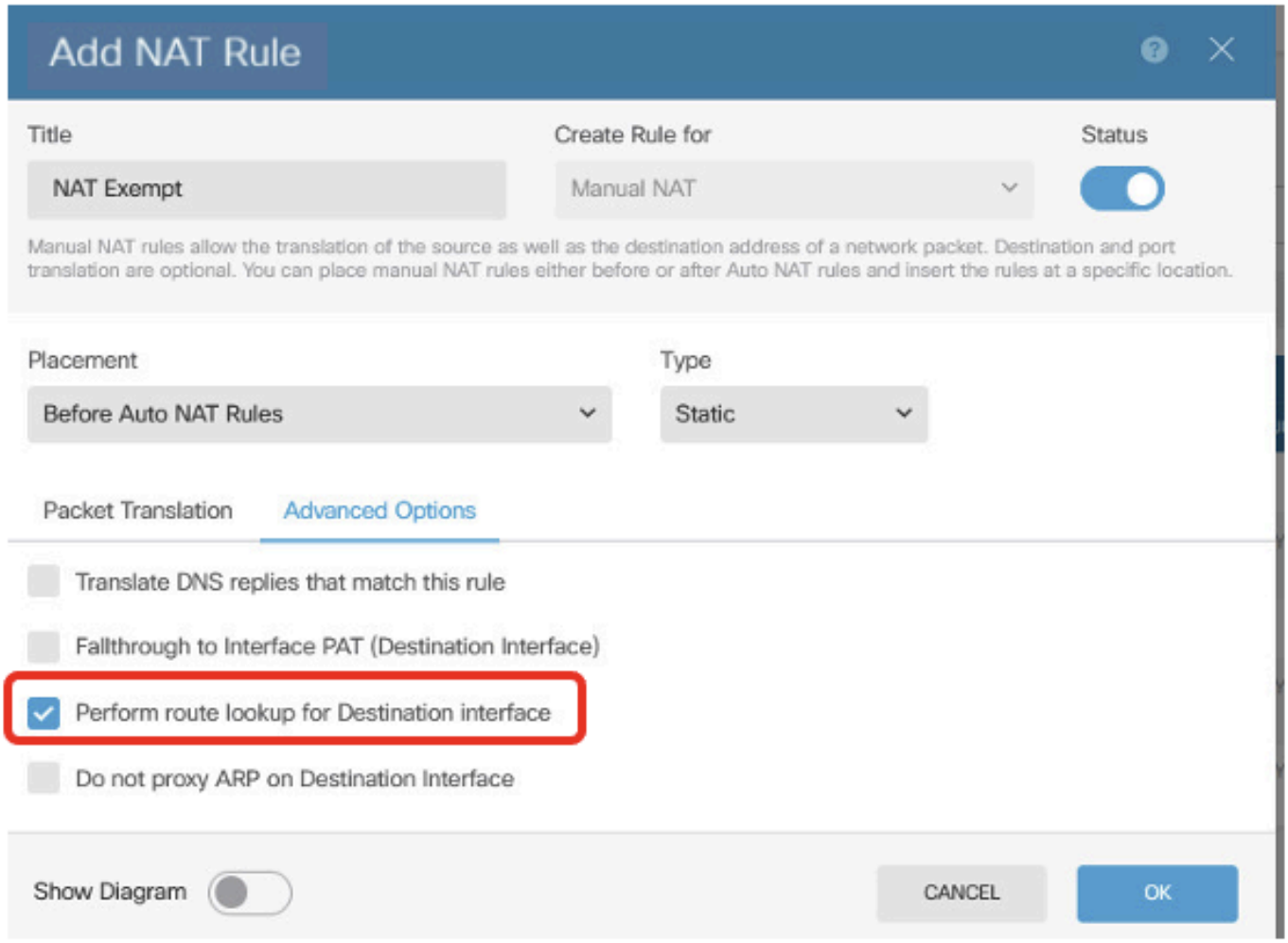
데모 목적을 위해 이 예에서는 클라이언트에 대해 동적 NAT가 구성되어 인터넷에 액세스합니다. 따라서 NAT 제외 규칙이 필요합니다.

Policies(정책) > NAT로 이동합니다. +단추를 클릭합니다. 세부 정보를 입력하고 OK(확인)를 클릭합니다.

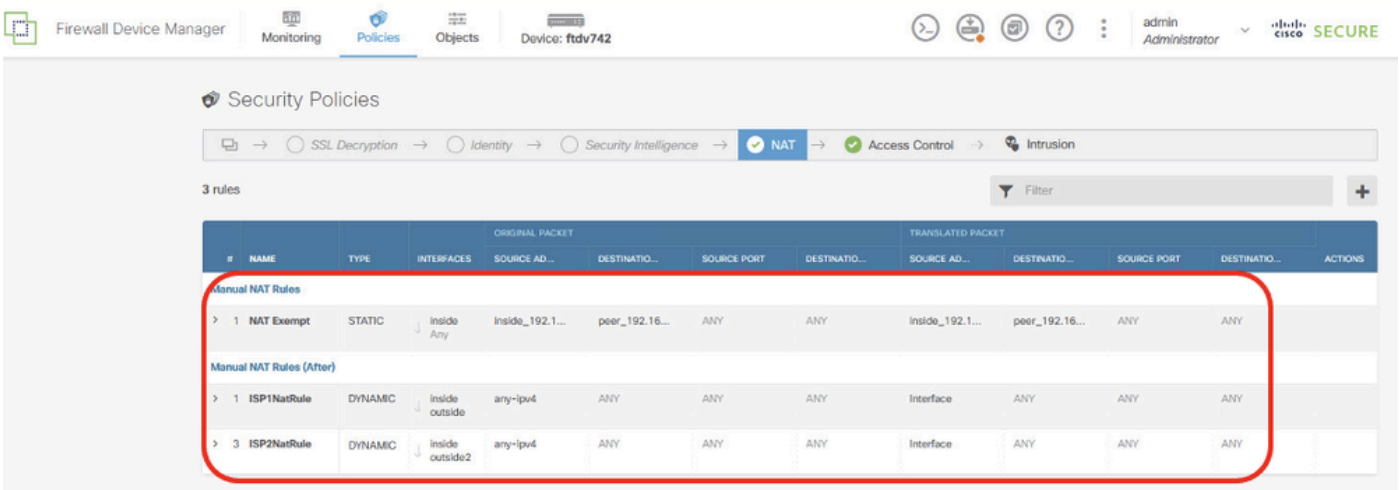
- 직함: NAT 제외
- 배치: 자동 NAT 규칙 이전
- 유형: 고정
- 소스 인터페이스: 내부
- 대상: 모두
- 원래 소스 주소: 192.168.70.0/24
- 변환된 소스 주소: 192.168.70.0/24
- 원래 대상 주소: 192.168.50.0/24
- 변환된 대상 주소: 192.168.50.0/24
- Route-Lookup 사용



Site1FTD_Nat_Exempt_Rule



Site1FTD_Nat_Exempt_Rule_2



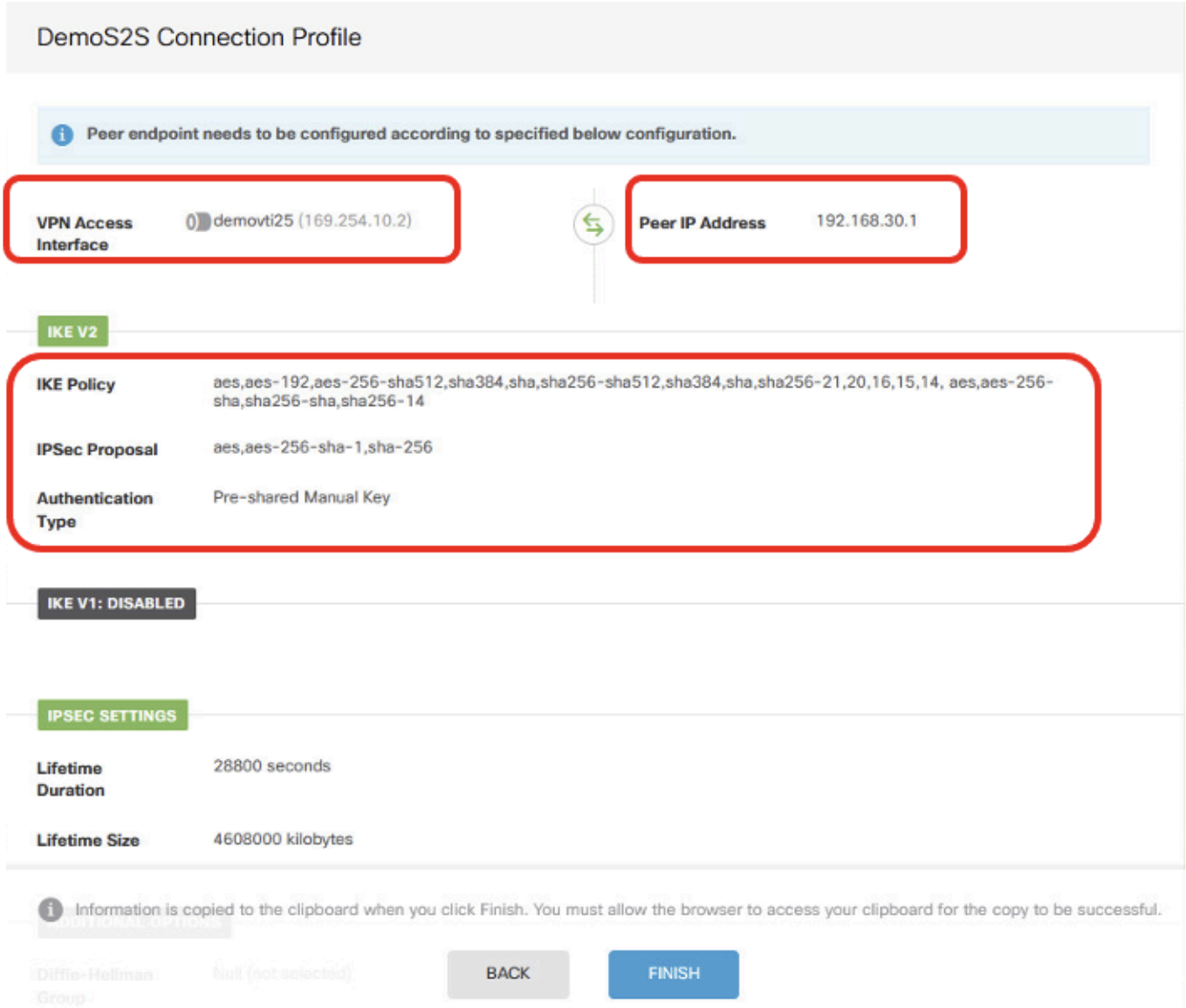
Site1FTD_Nat_Rule_Overview

9단계. 컨피그레이션 변경 사항을 구축합니다.

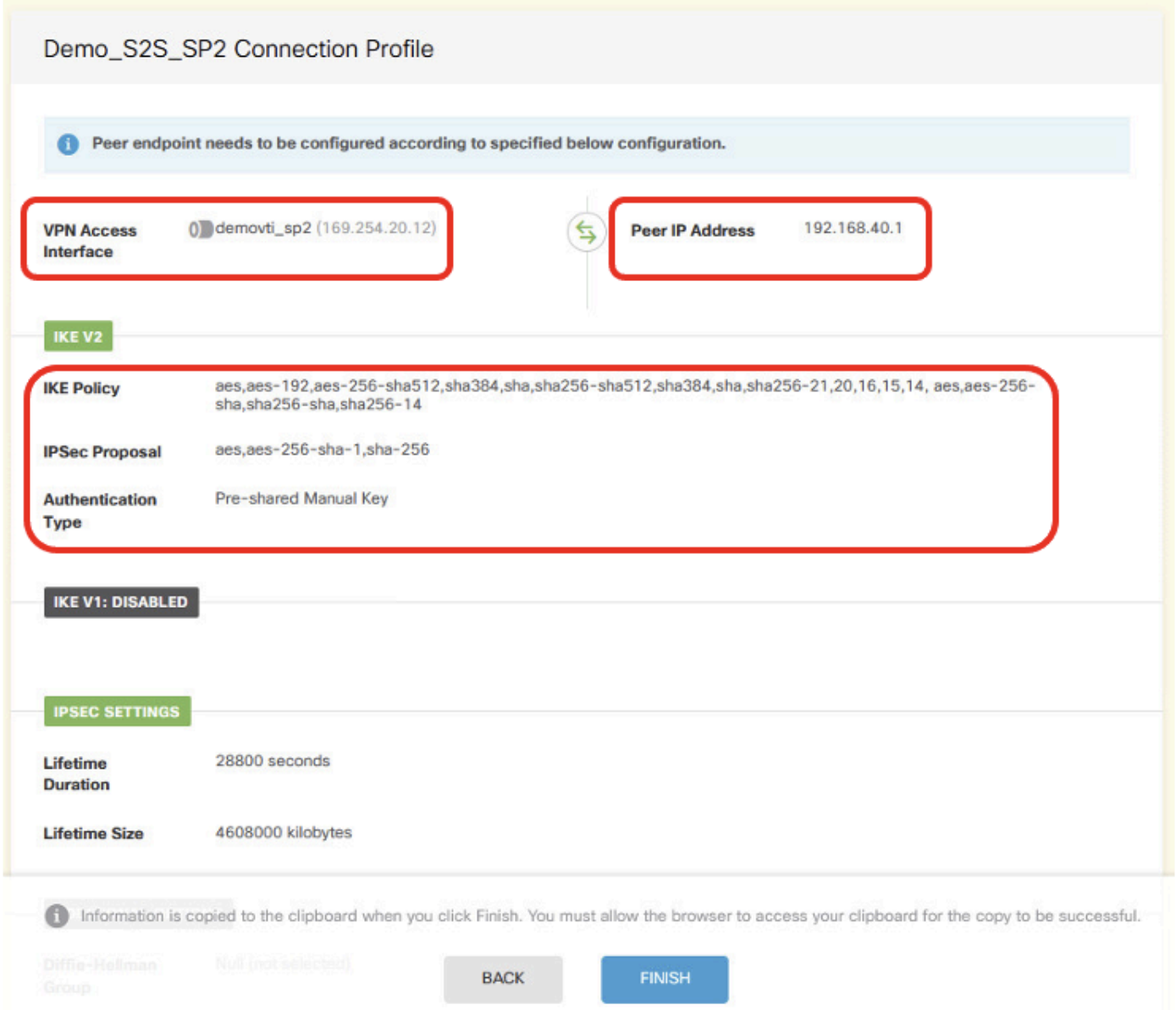
Site1FTD_Deployment_Changes

Site2 FTD VPN 컨피그레이션

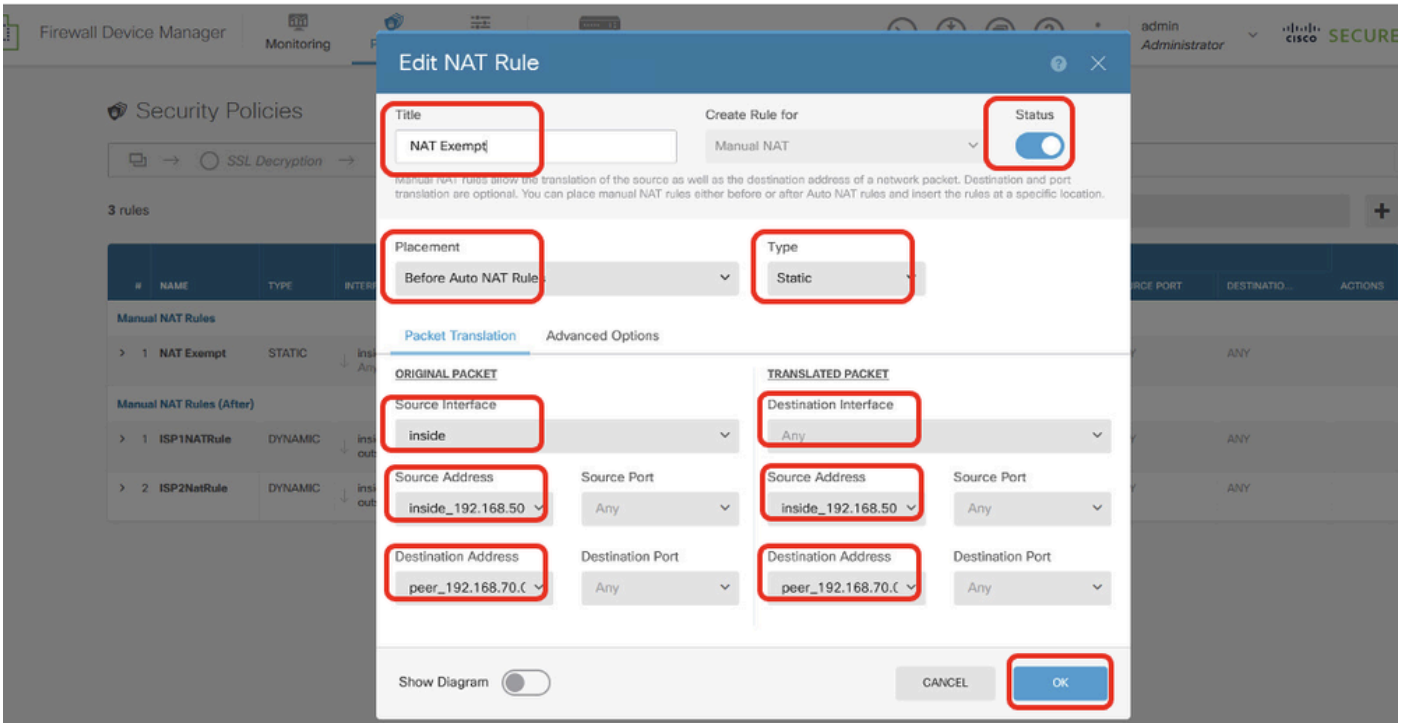
10단계. 사이트 2 FTD에 해당하는 매개변수를 사용하여 1단계부터 9단계까지 반복합니다.



Site2FTD_ISP1_Review_VPN_Config_요약



Site2FTD_ISP2_Review_VPN_Config_요약

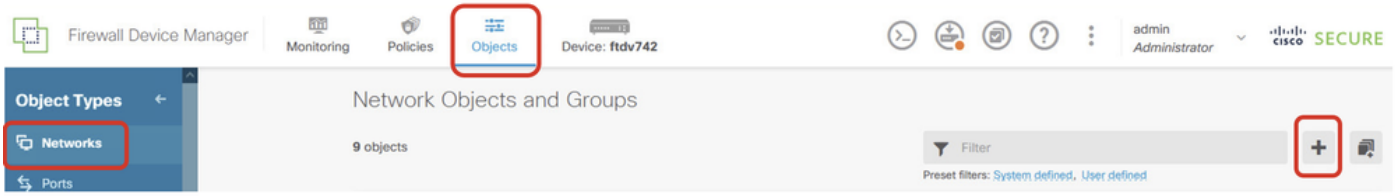


Site2FTD_Nat_Exempt_Rule

PBR의 컨피그레이션

Site1 FTD PBR 컨피그레이션

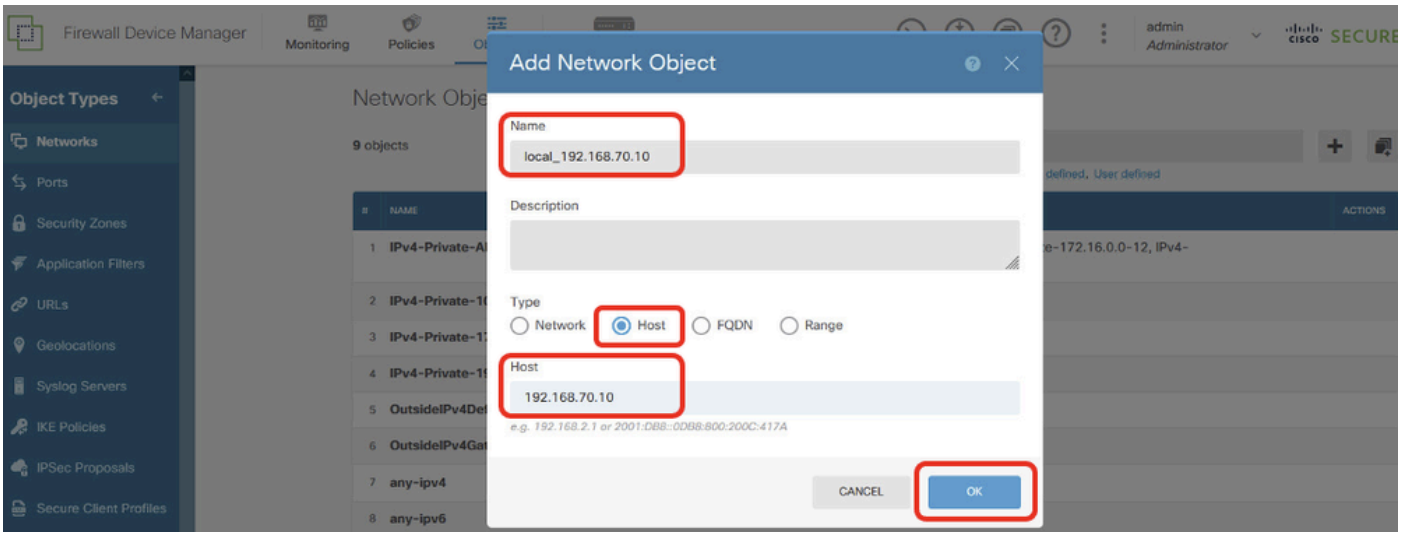
11단계. Site1 FTD에 대한 PBR 액세스 목록에서 사용할 새 네트워크 객체를 생성합니다. Objects > Networks로 이동하고 + 버튼을 클릭합니다.



Site1FTD_Create_Network_Object

11.1단계. Site1 Client2 IP 주소의 개체를 만듭니다. 필요한 정보를 제공하십시오. OK(확인) 버튼을 클릭합니다.

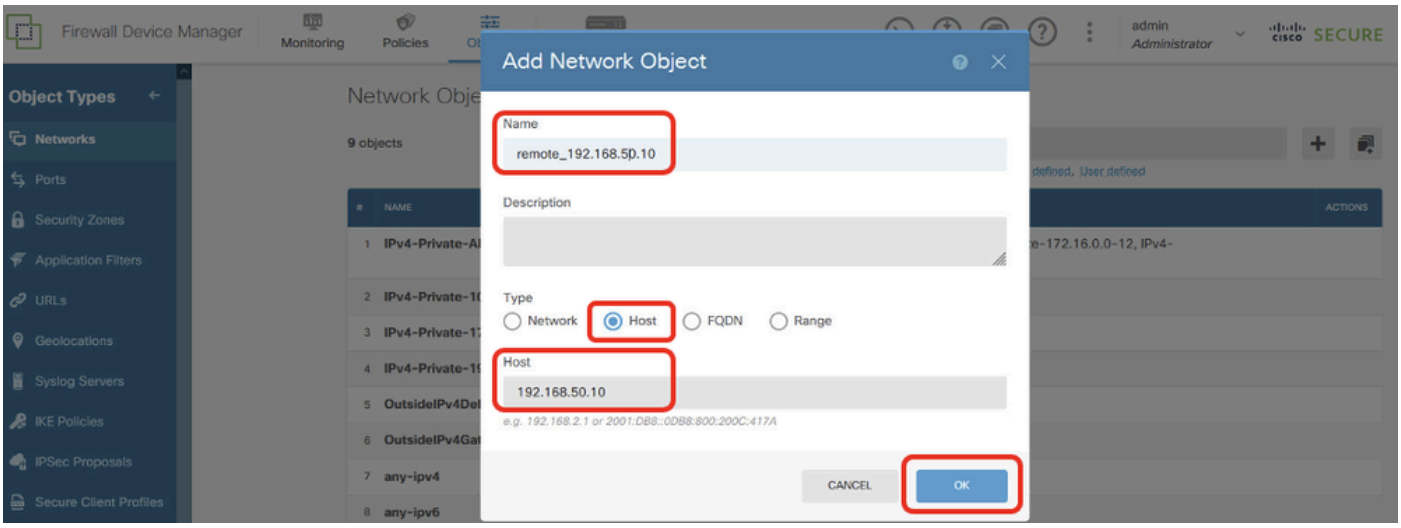
- 이름: local_192.168.70.10
- 유형: 호스트
- 호스트: 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

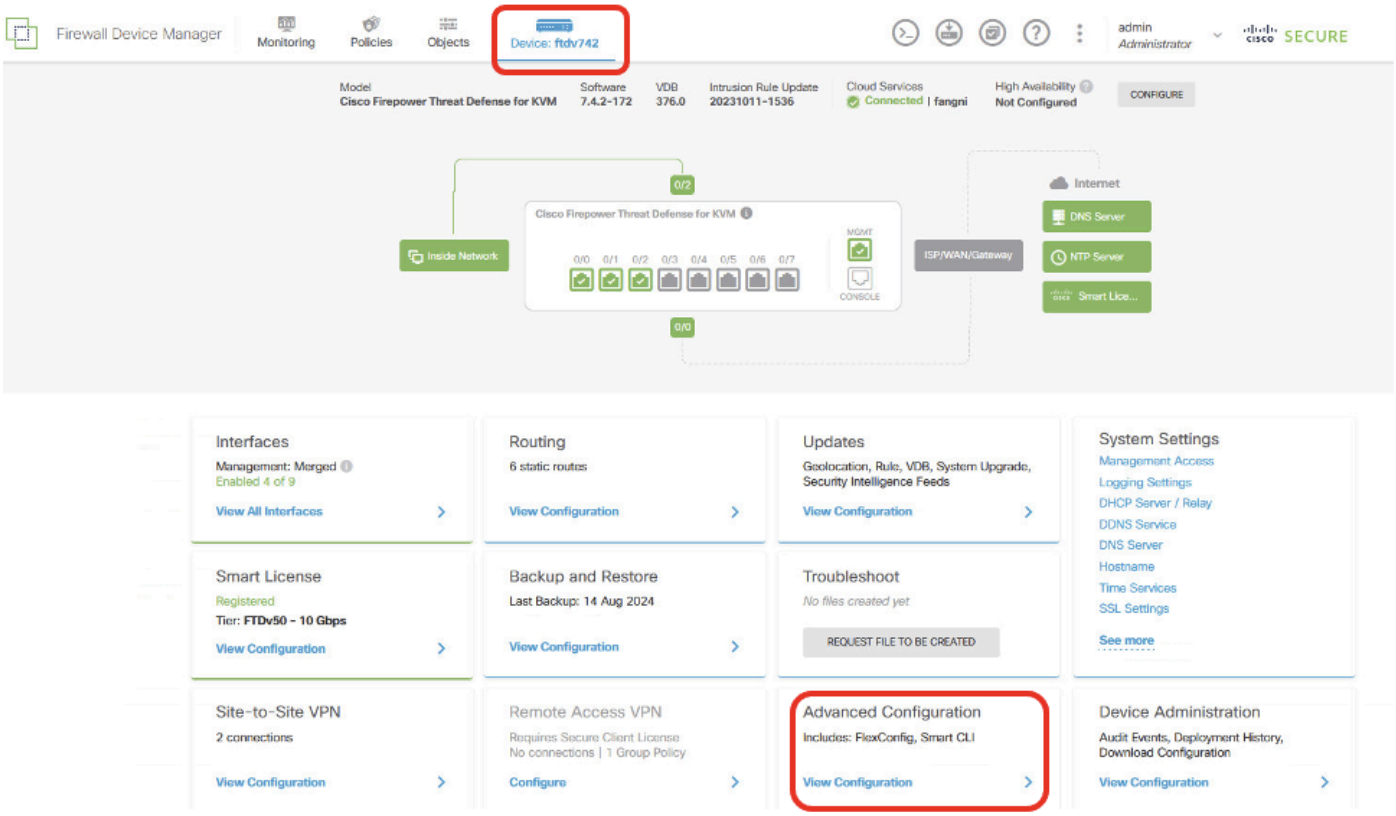
11.2단계. Site2 Client2 IP 주소의 개체를 만듭니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: remote_192.168.50.10
- 유형: 호스트
- 호스트: 192.168.50.10



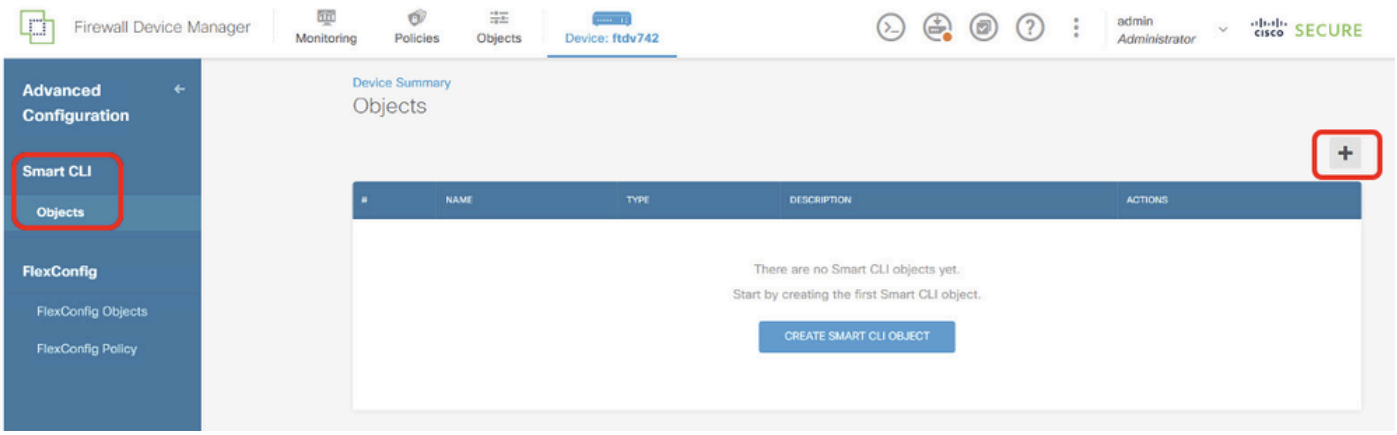
Site1FTD_PBR_RemoteObject

12단계. PBR에 대한 확장 액세스 목록을 생성합니다. Device(디바이스) > Advanced Configuration(고급 컨피그레이션)으로 이동합니다. View Configuration(컨피그레이션 보기)을 클릭합니다.



Site1FTD_View_Advanced_Configuration

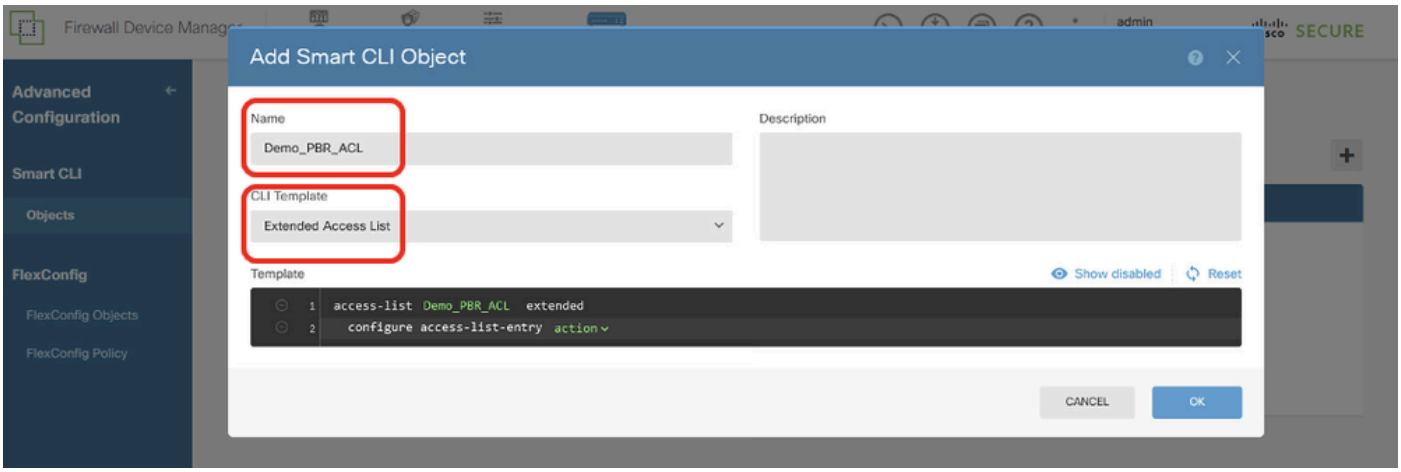
12.1단계. Smart CLI > Objects로 이동합니다. +단추를 클릭합니다.



Site1FTD_Add_SmartCLI_Object

12.2단계. 객체의 이름을 입력하고 CLI 템플릿을 선택합니다.

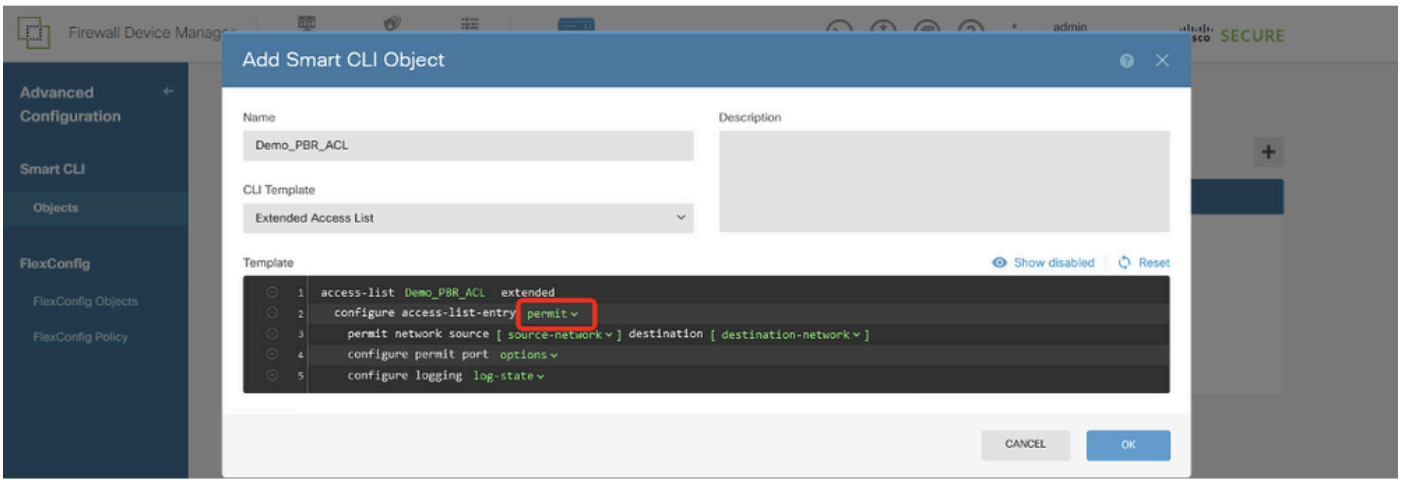
- 이름: 데모_PBR_ACL
- CLI 템플릿: 확장 액세스 목록



Site1FTD_Create_PBR_ACL_1

12.3단계. Template(템플릿)으로 이동하여 구성합니다. 저장하려면 OK 버튼을 클릭합니다.

행 2에서 작업을 클릭합니다. 허용을 선택합니다.

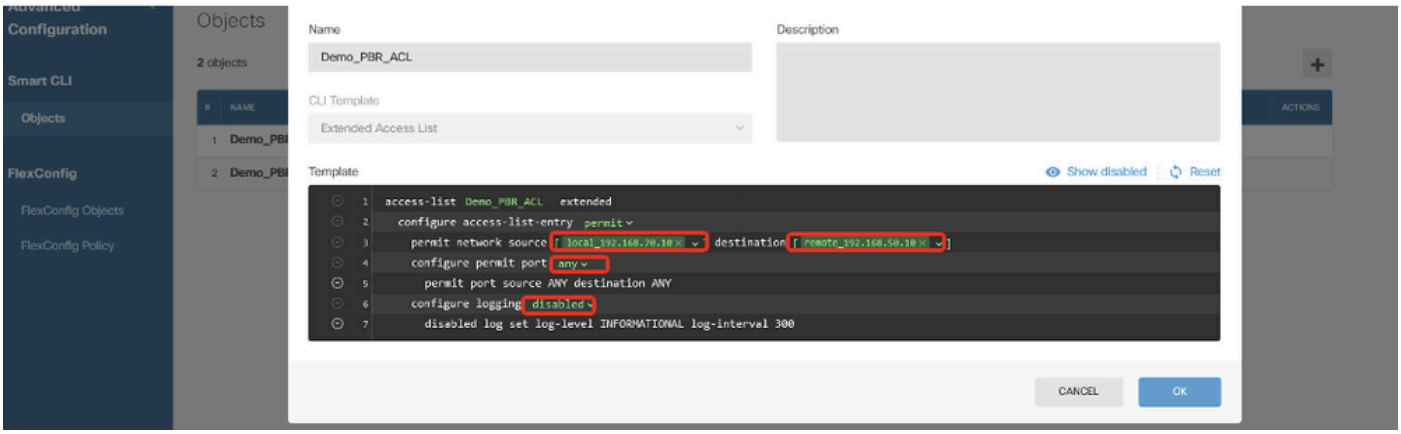


Site1FTD_Create_PBR_ACL_2

행 3에서 source-network를 클릭합니다. local_192.168.70.10을 선택합니다. destination-network를 누릅니다. remote_192.168.50.10을 선택합니다.

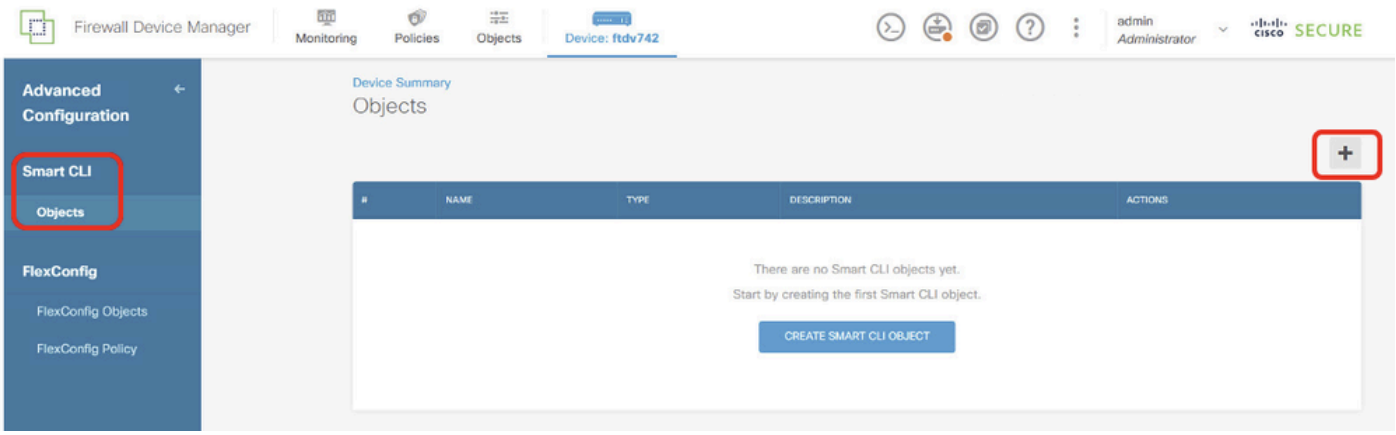
4번 행에서 옵션을 클릭하고 any를 선택합니다.

행 6에서 log-state를 클릭하고 disabled를 선택합니다.



Site1FTD_Create_PBR_ACL_3

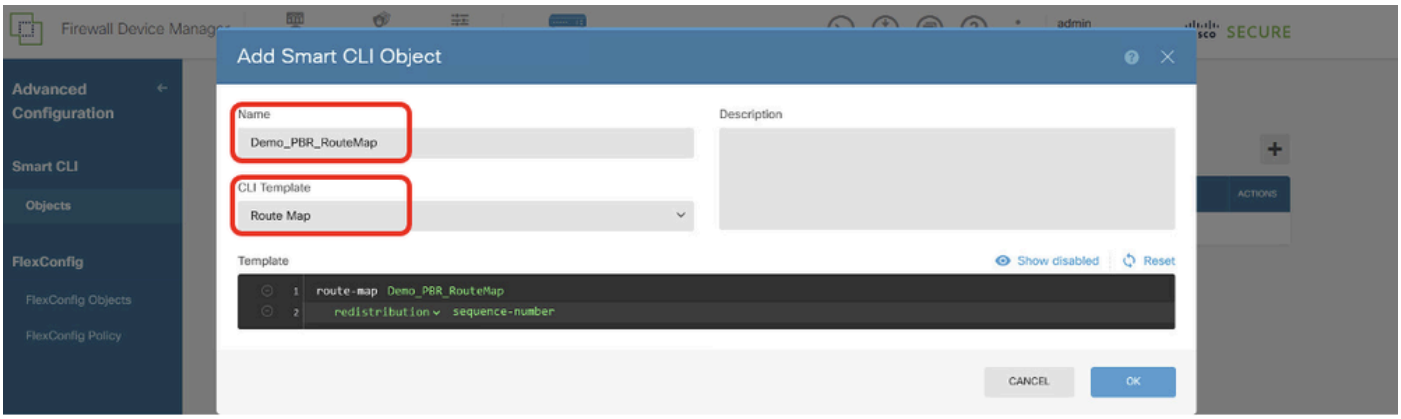
13단계. PBR에 대한 경로 맵을 만듭니다. Device(디바이스) > Advanced Configuration(고급 컨피그레이션) > Smart CLI > Objects(개체)로 이동합니다. +단추를 클릭합니다.



Site1FTD_Add_SmartCLI_Object

13.1단계. 객체의 이름을 입력하고 CLI 템플릿을 선택합니다.

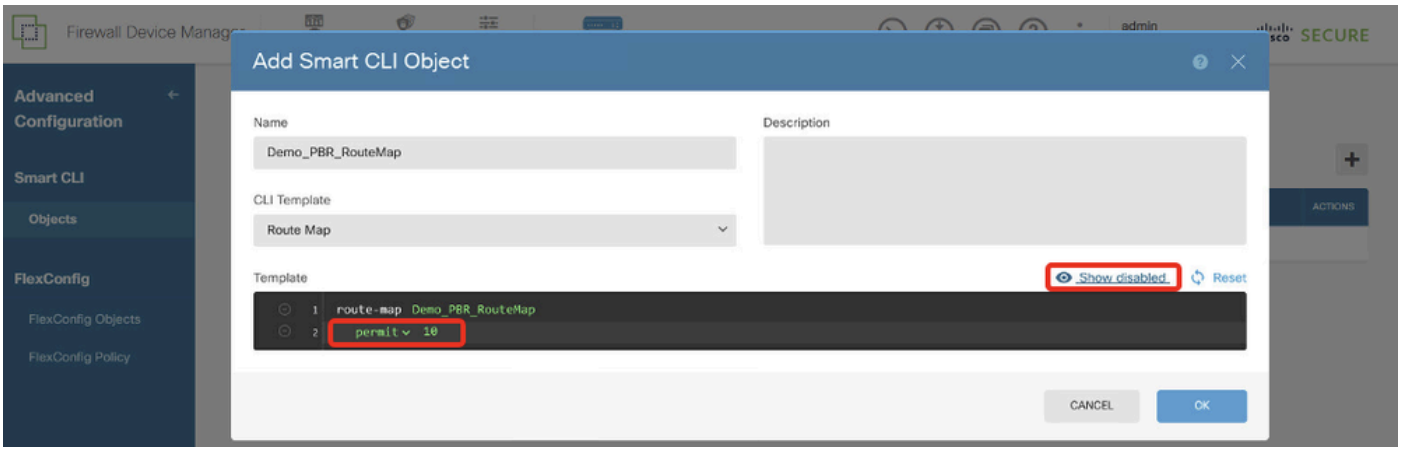
- 이름: Demo_PBR_RouteMap
- CLI 템플릿: 경로 지도



Site1FTD_Create_PBR_RouteMap_1

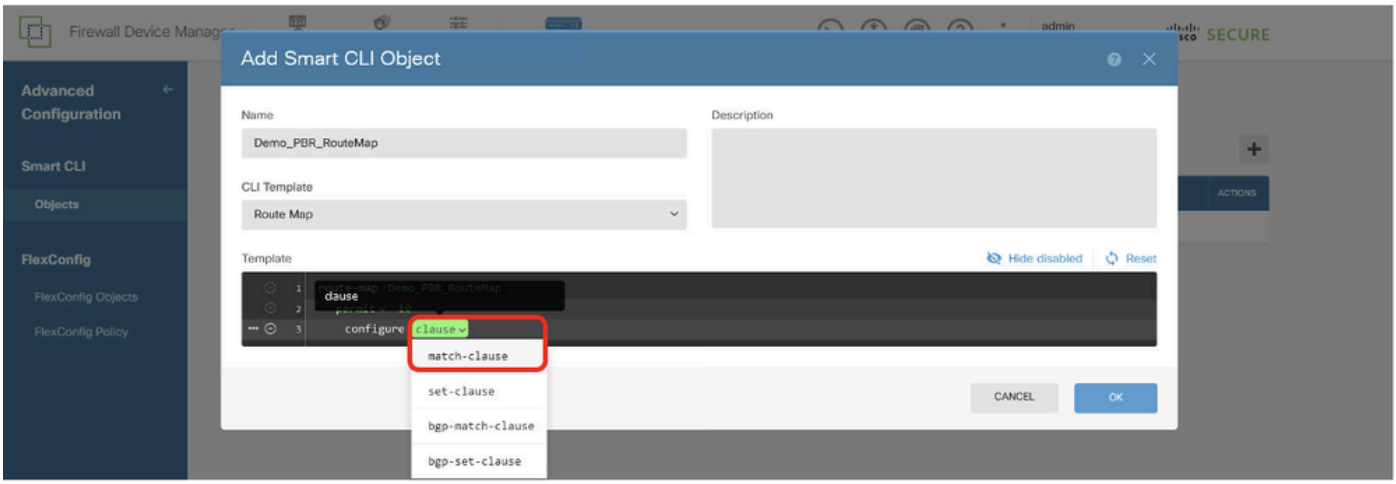
13.2단계. Template(템플릿)으로 이동하여 구성합니다. OK(확인) 버튼을 클릭하여 저장합니다.

행 2에서 재배포를 클릭합니다. 허용을 선택합니다. 시퀀스 번호, 수동 입력 10을 클릭합니다. 비활성 표시를 클릭합니다.



Site1FTD_Create_PBR_RouteMap_2

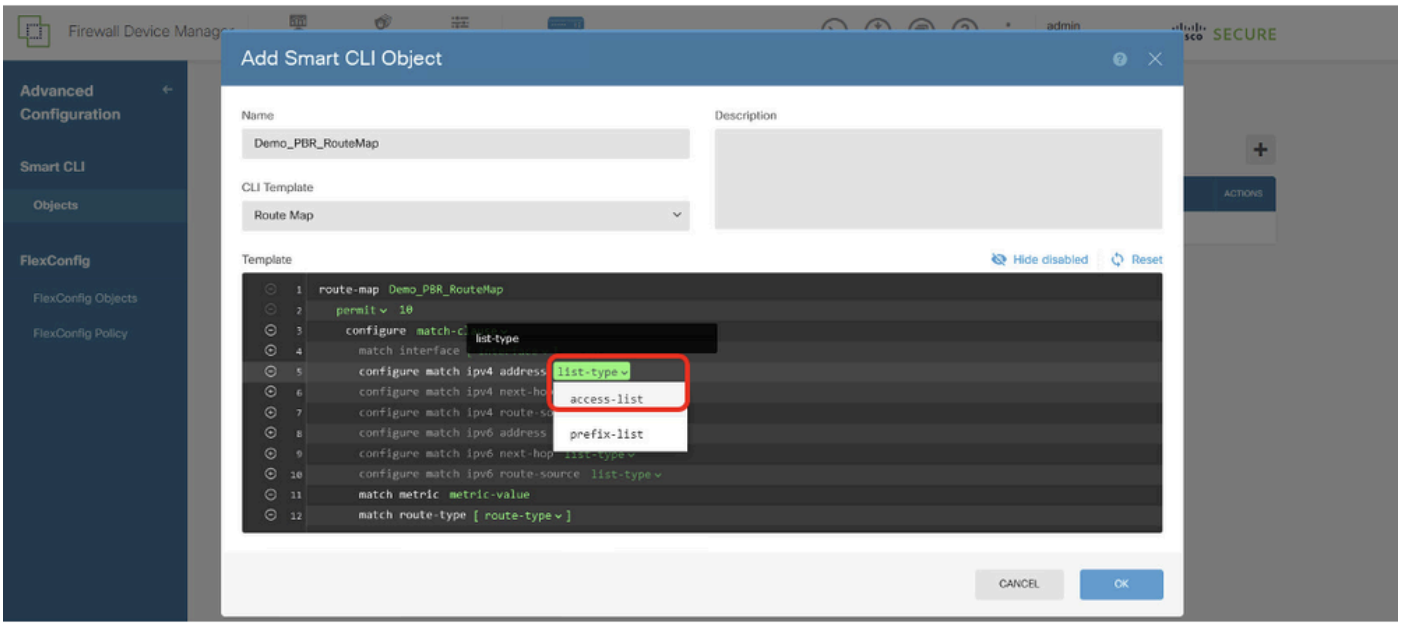
행 3에서 +를 클릭하여 행을 활성화합니다. 절을 클릭합니다. match-clause를 선택합니다.



Site1FTD_Create_PBR_RouteMap_3

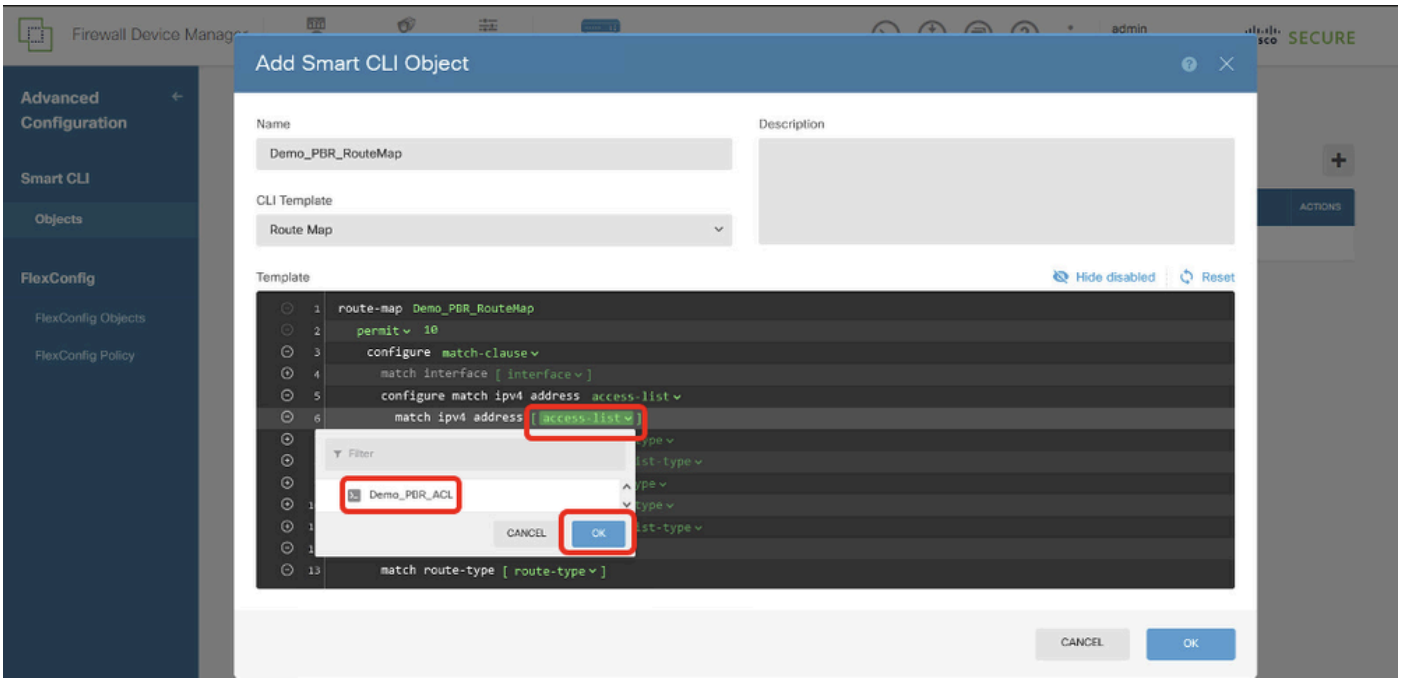
4번 행에서 -를 클릭하여 행을 비활성화합니다.

행 5에서 +를 클릭하여 행을 활성화합니다. list-type을 클릭합니다. access-list를 선택합니다.



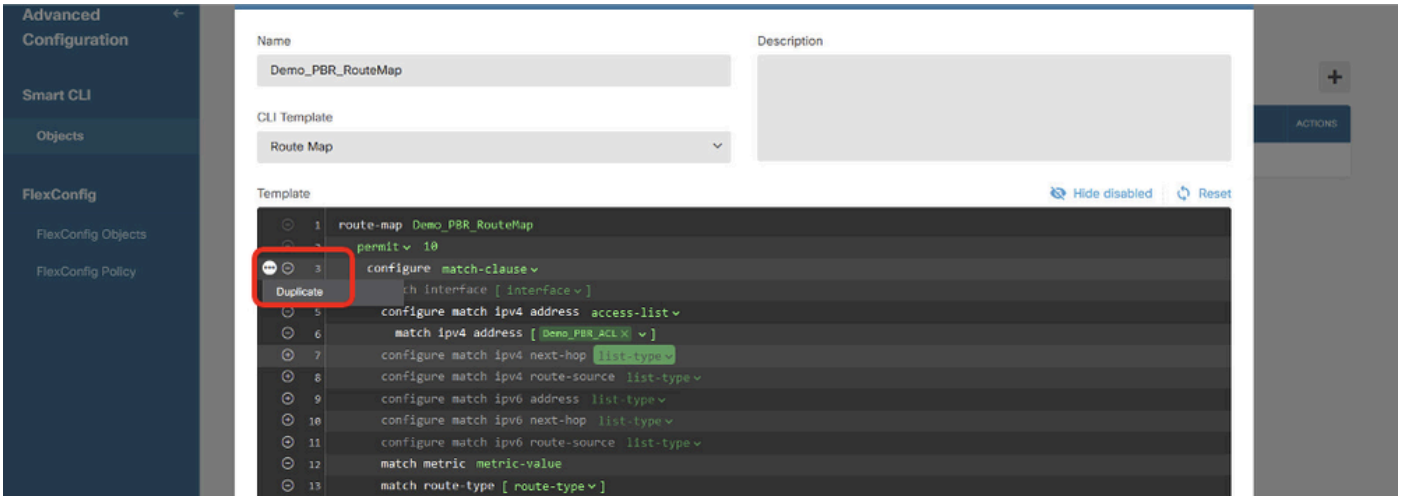
Site1FTD_Create_PBR_RouteMap_4

행 6에서 access-list를 클릭합니다. 12단계에서 생성한 ACL 이름을 선택합니다. 이 예에서는 Demo_PBR_ACL입니다.



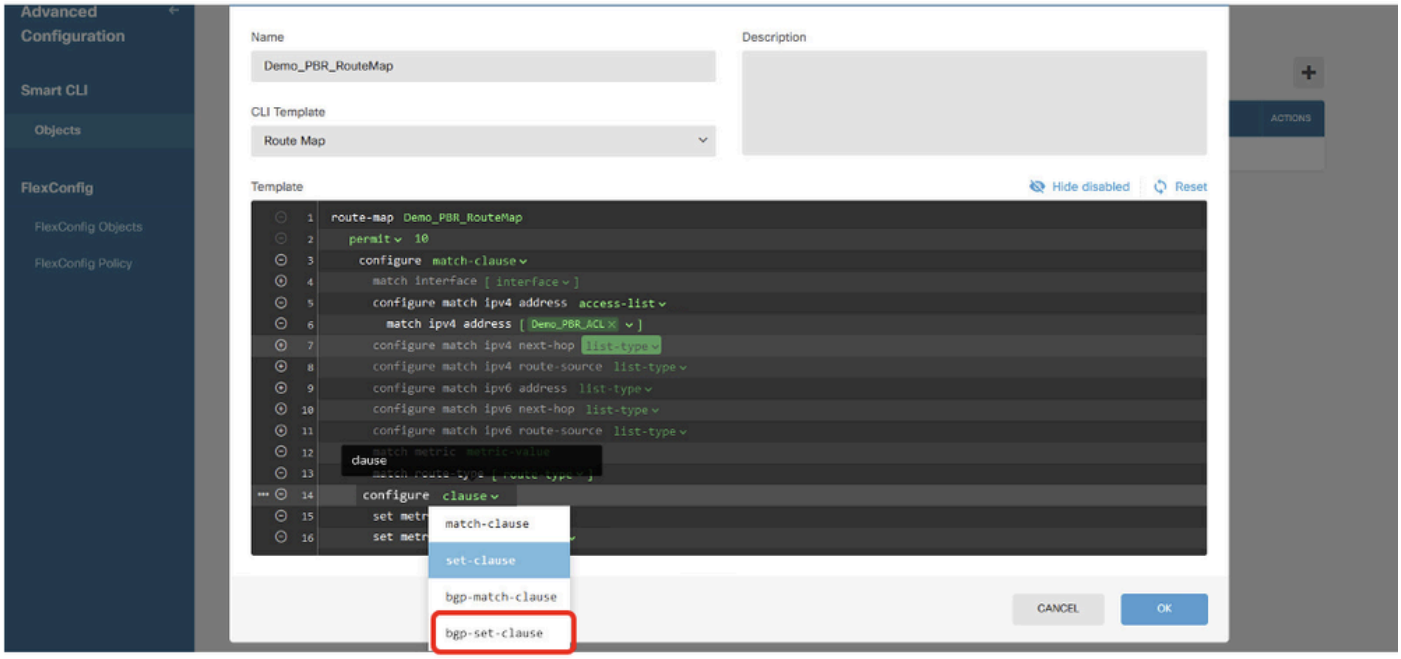
Site1FTD_Create_PBR_RouteMap_5

행 3으로 돌아갑니다. 옵션을 클릭하십시오. 버튼을 클릭하고 Duplicate(복제)를 선택합니다.



Site1FTD_Create_PBR_RouteMap_6

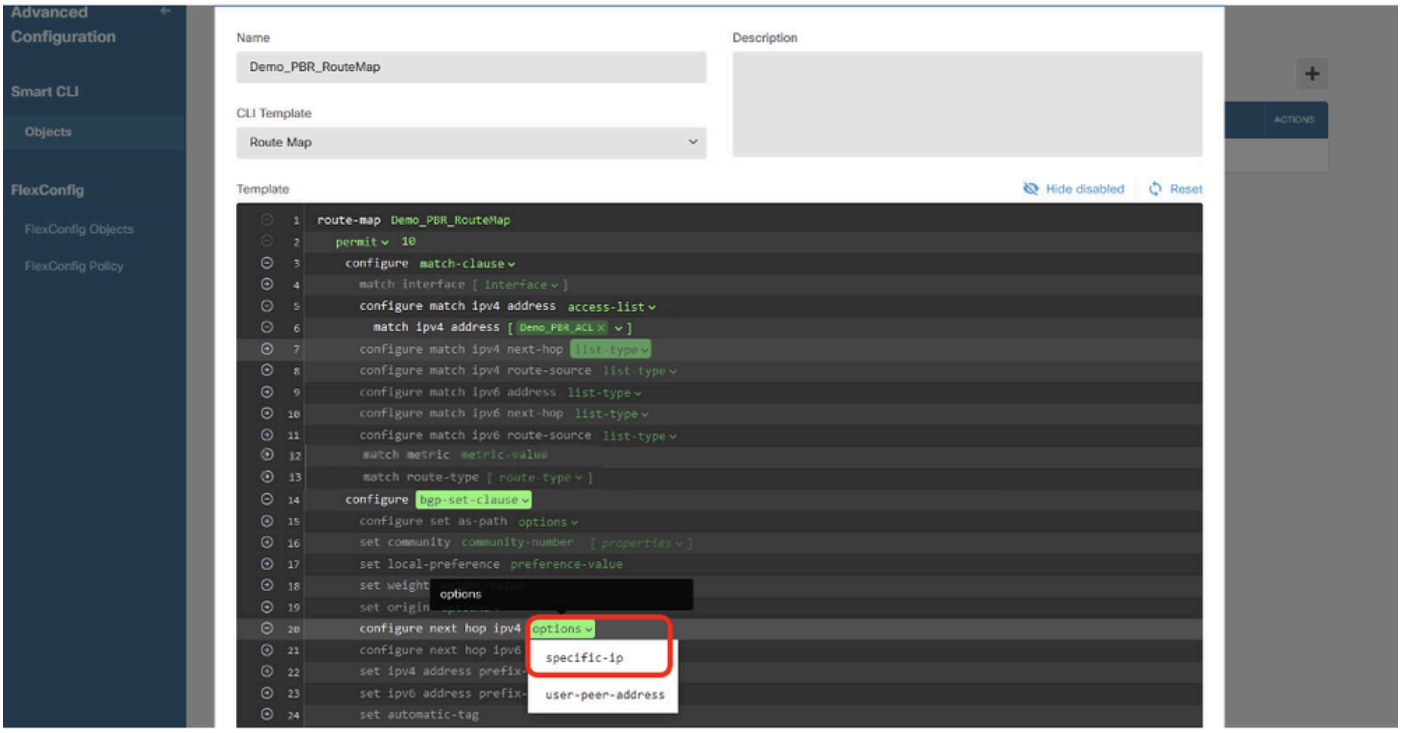
행 14에서 절을 클릭하고 bgp-set-clause를 선택합니다.



Site1FTD_Create_PBR_RouteMap_7

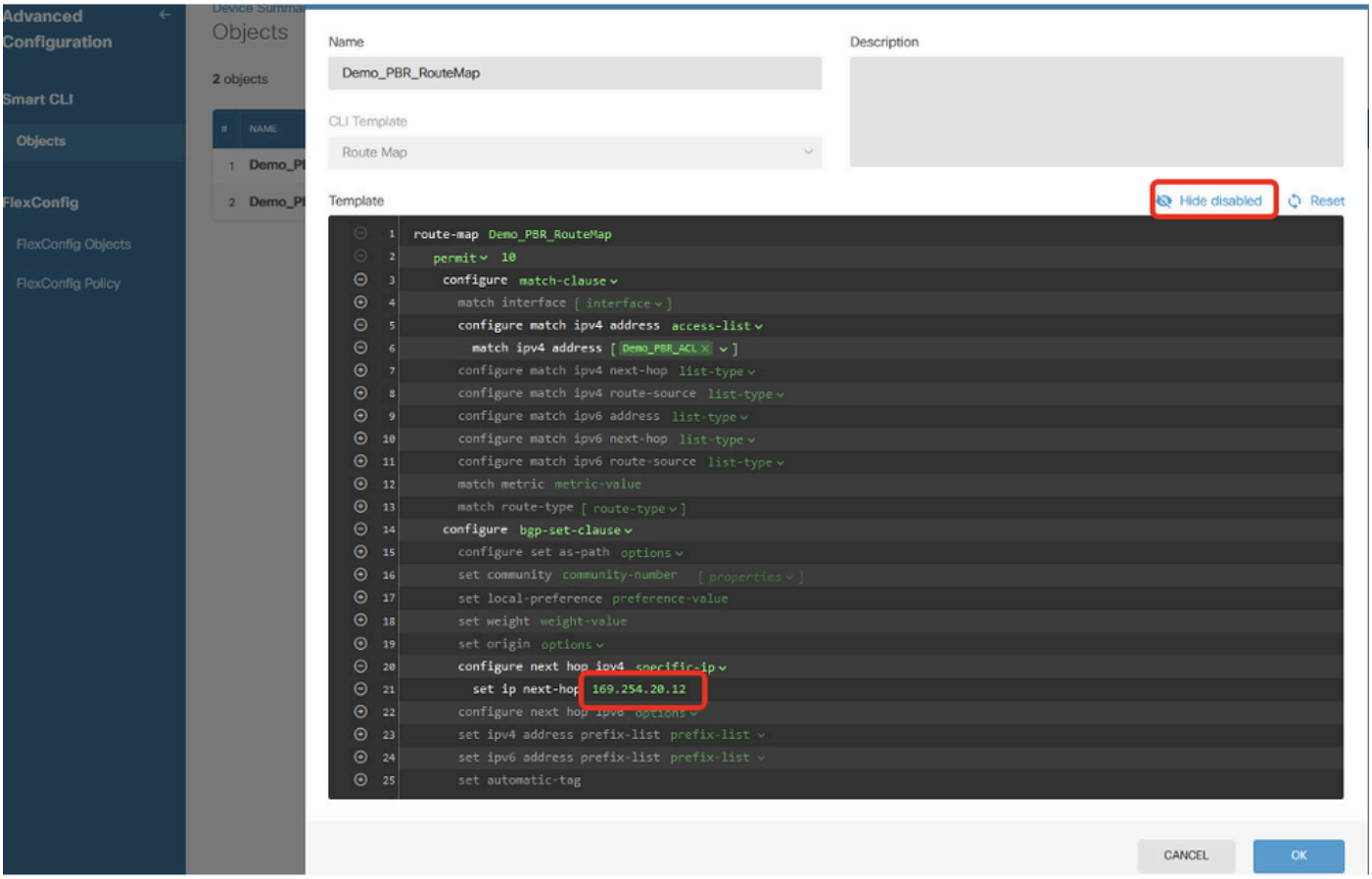
12, 13, 15, 16, 17, 18, 19, 21, 22, 23, 24번 행에서 버튼을 클릭하여 비활성화합니다.

행 20에서 options(옵션)를 클릭하고 specific-ip(특정 IP)를 선택합니다.



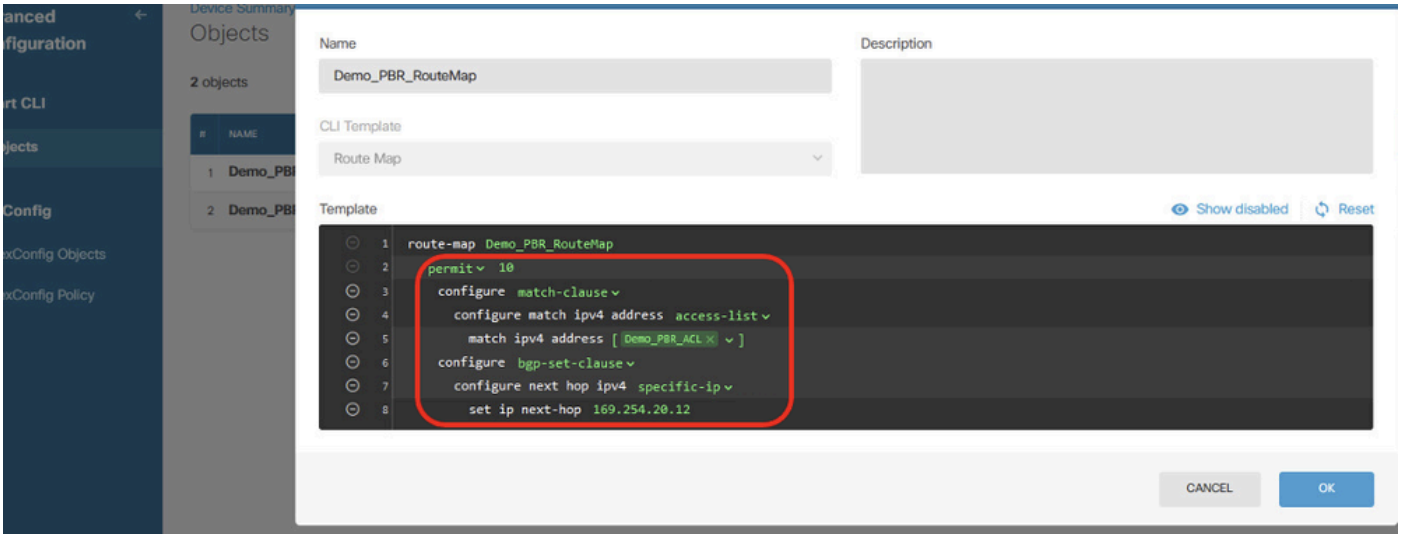
Site1FTD_Create_PBR_RouteMap_8

행 21에서 ip-address를 클릭합니다. 수동 입력 next-hop IP 주소. 이 예에서는 피어 Site2 FTD VTI tunnel2(169.254.20.12)의 IP 주소입니다. Hide disabled(비활성 숨기기)를 클릭합니다.



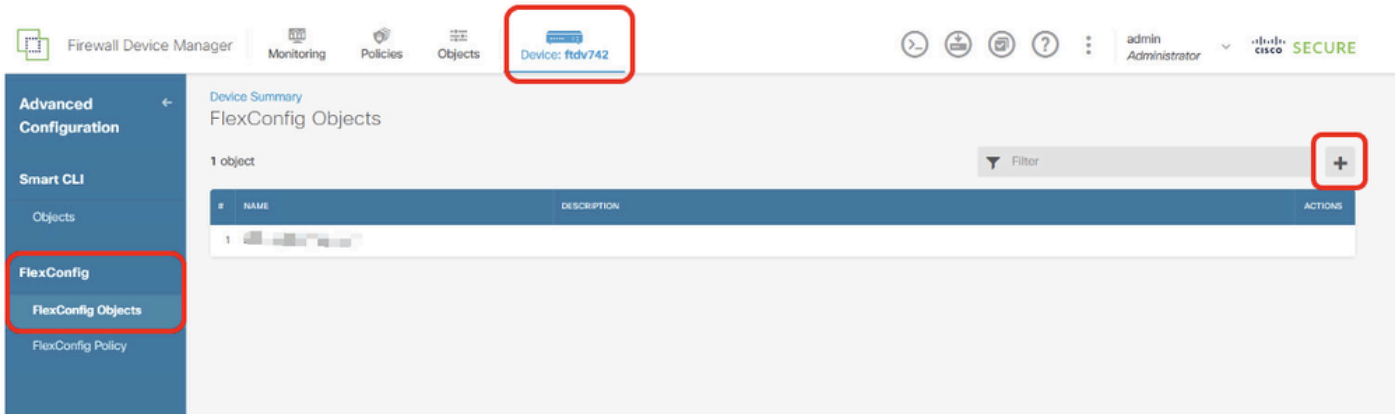
Site1FTD_Create_PBR_RouteMap_9

경로 맵의 컨피그레이션을 검토합니다.



Site1FTD_Create_PBR_RouteMap_10

14단계. PBR에 대한 FlexConfig 개체를 만듭니다. Device(디바이스) > Advanced Configuration(고급 컨피그레이션) > FlexConfig Objects(FlexConfig 개체)로 이동하고 + 버튼을 클릭합니다.



Site1FTD_Create_PBR_FlexObj_1

14.1단계. 객체의 이름을 입력합니다. 이 예에서는 Demo_PBR_FlexObj. 템플릿 및 부정 템플릿 편집기에서 명령줄을 입력합니다.

- 템플릿:

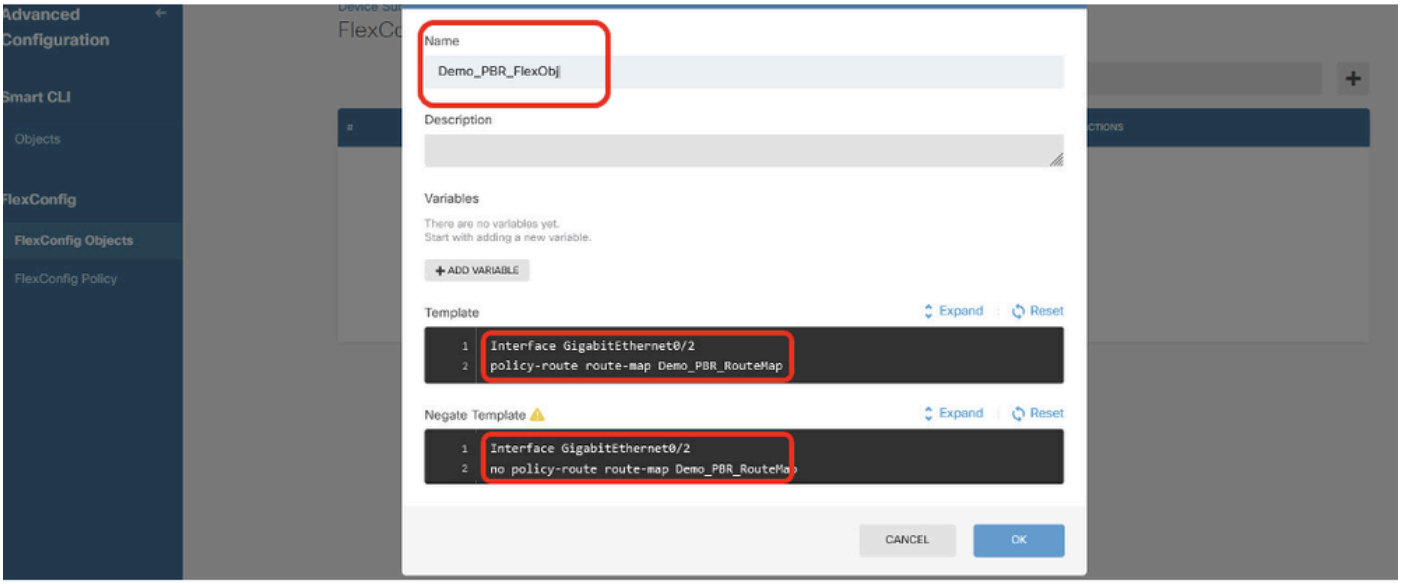
인터페이스 GigabitEthernet0/2

policy-route route-map Demo_PBR_RouteMap_Site2

- 부정 템플릿:

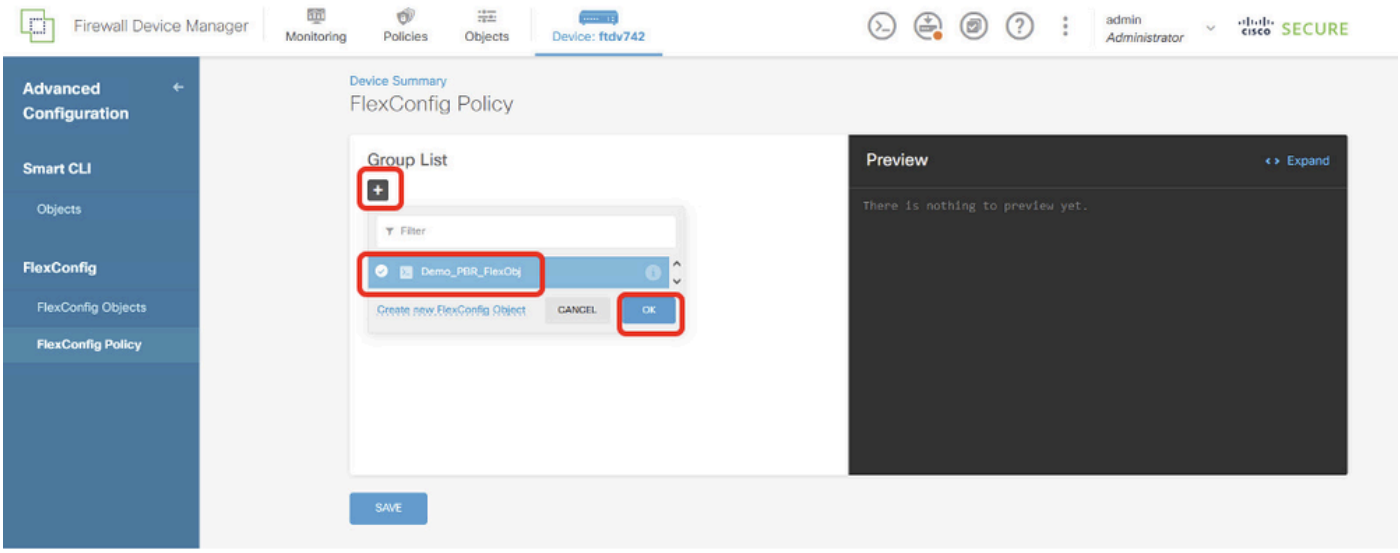
인터페이스 GigabitEthernet0/2

no policy-route route-map Demo_PBR_RouteMap_Site2



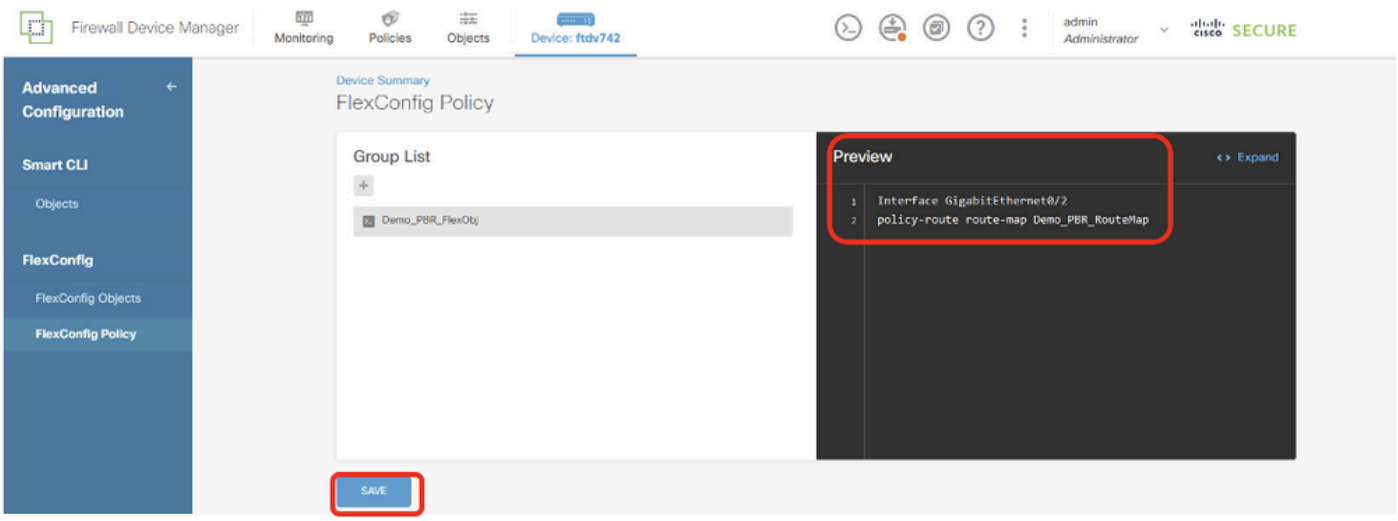
Site1FTD_Create_PBR_FlexObj_2

15단계. PBR에 대한 FlexConfig 정책을 생성합니다. Device(디바이스) > Advanced Configuration(고급 컨피그레이션) > FlexConfig Policy(FlexConfig 정책)로 이동합니다. +단추를 클릭합니다. 14단계에서 생성한 FlexConfig 개체 이름을 선택합니다. 확인 단추를 누릅니다.



Site1FTD_Create_PBR_FlexPolicy_1

15.1단계. Preview(미리 보기) 창에서 명령을 확인합니다. 좋으면 저장을 클릭합니다.



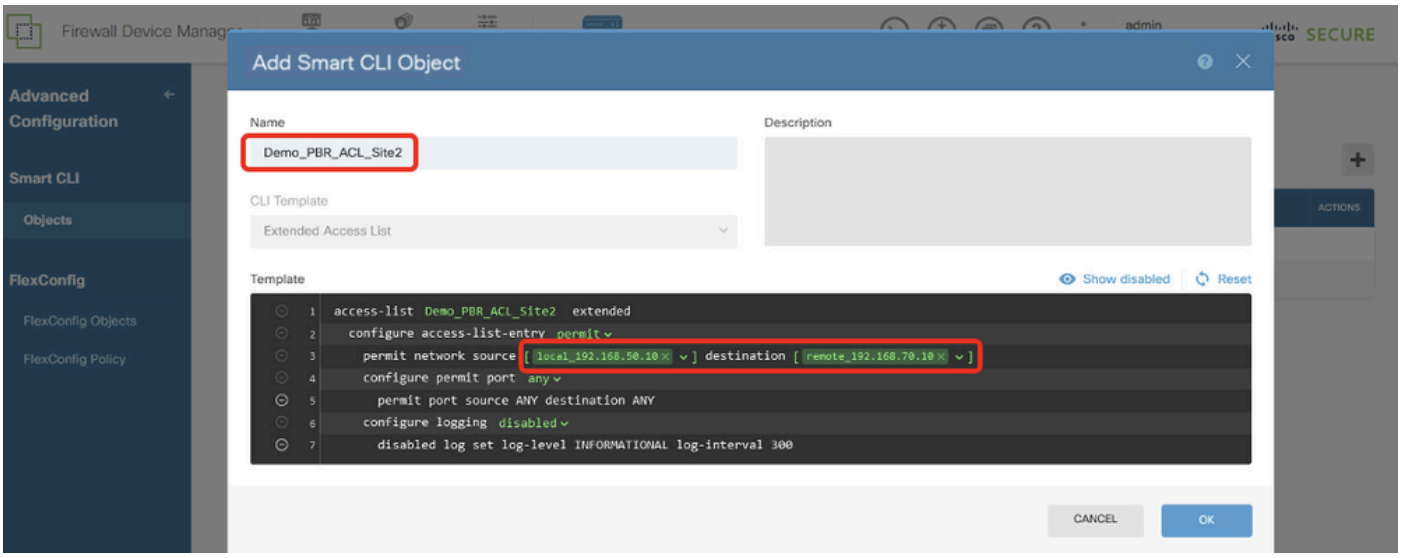
Site1FTD_Create_PBR_FlexPolicy_2

16단계. 구성 변경 사항을 배포합니다.

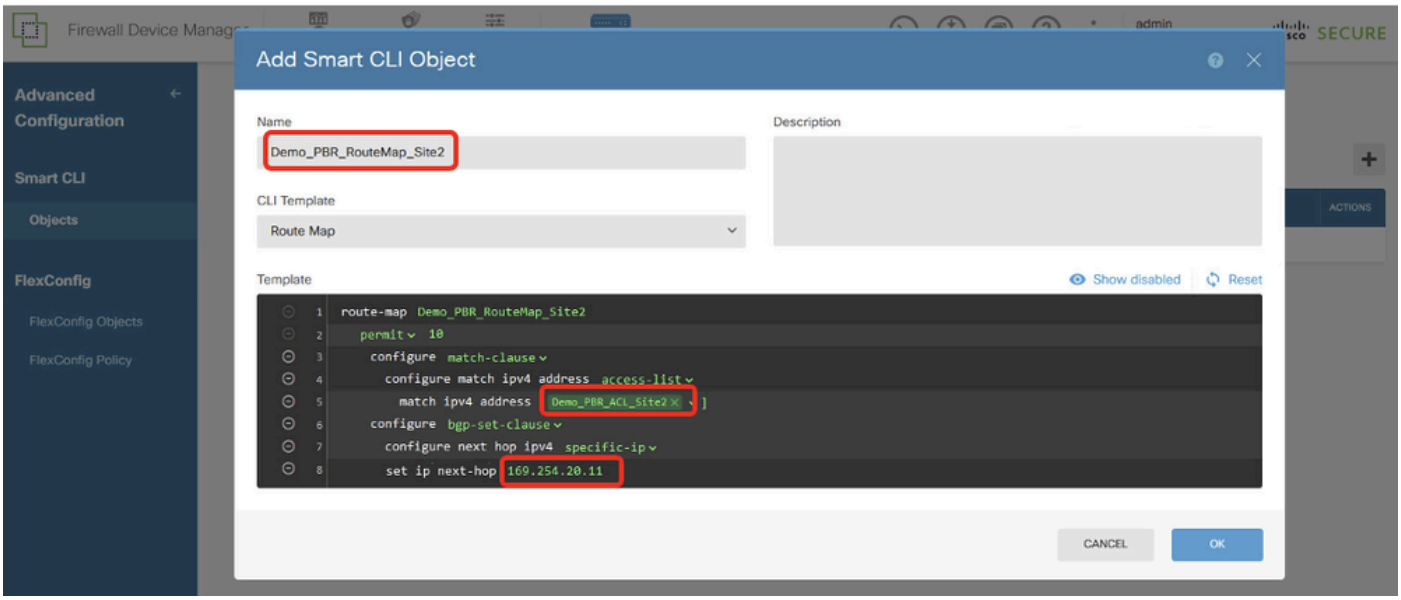
Site1FTD_Deployment_Changes

Site2 FTD PBR 컨피그레이션

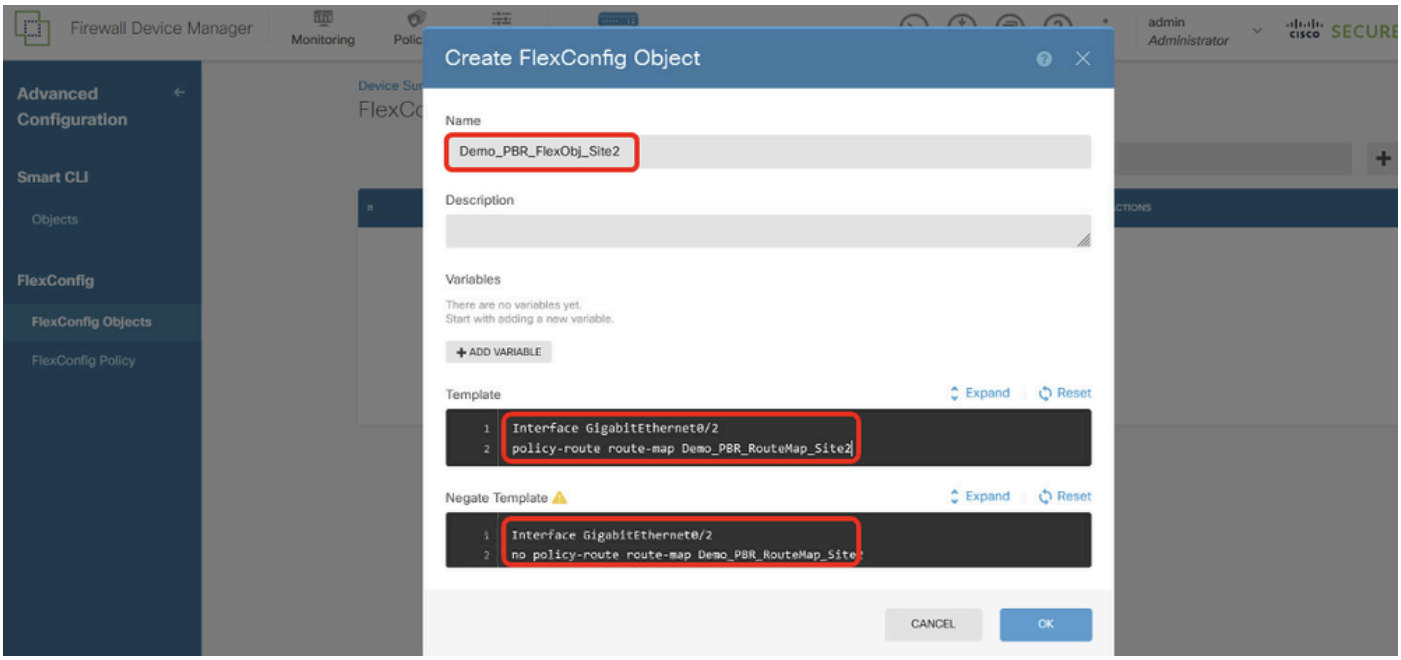
17단계. Site2 FTD에 해당하는 매개변수로 PBR을 생성하려면 11단계 - 16단계를 반복합니다.



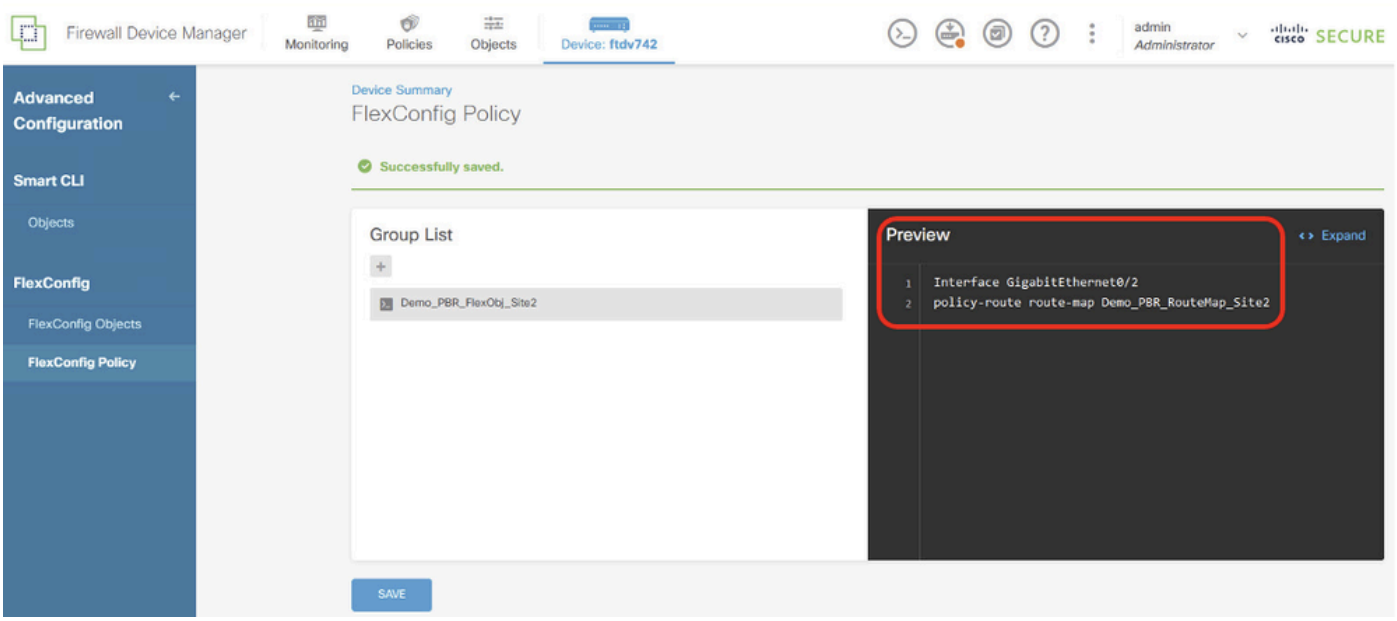
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

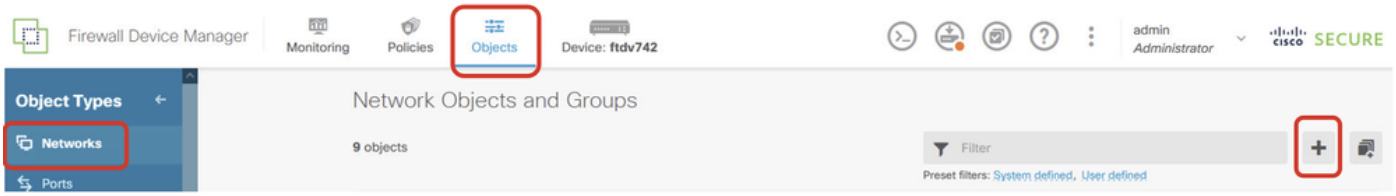


Site2FTD_Create_PBR_FlexPolicy

SLA 모니터의 컨피그레이션

Site1 FTD SLA 모니터 컨피그레이션

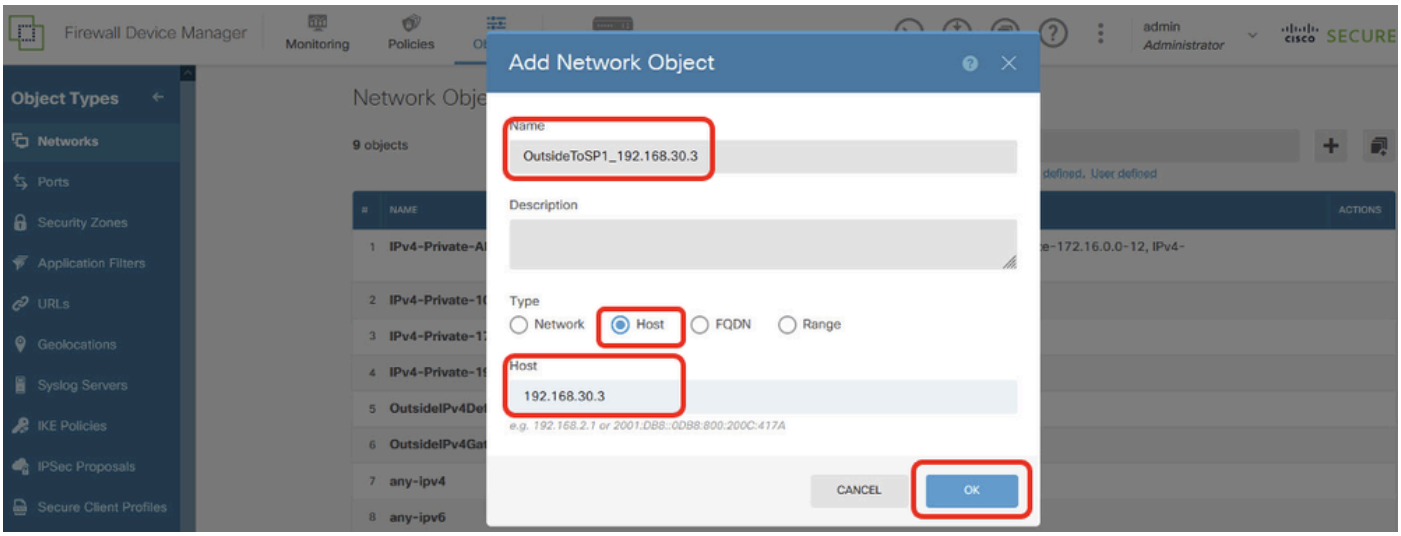
18단계. Site1 FTD에 대한 SLA 모니터에서 사용할 새 네트워크 객체를 생성합니다. Objects(객체) > Networks(네트워크)로 이동하고 + 버튼을 클릭합니다.



Site1FTD_Create_Network_Object

18.1단계. ISP1 게이트웨이 IP 주소에 대한 개체를 만듭니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

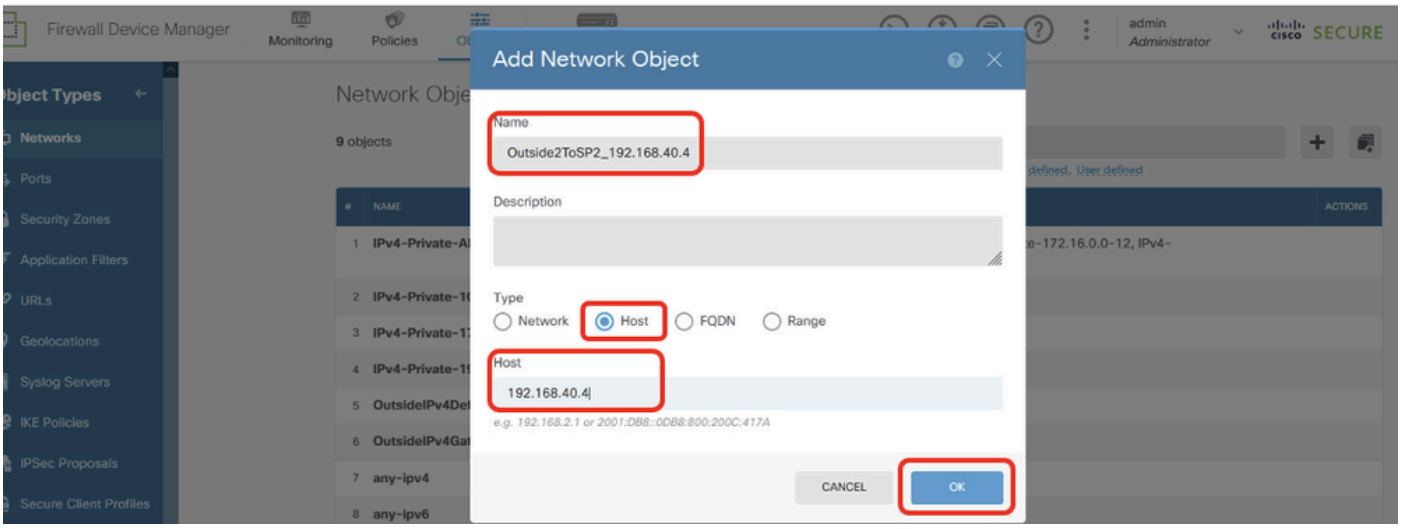
- 이름: 외부SP1_192.168.30.3
- 유형: 호스트
- 호스트: 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

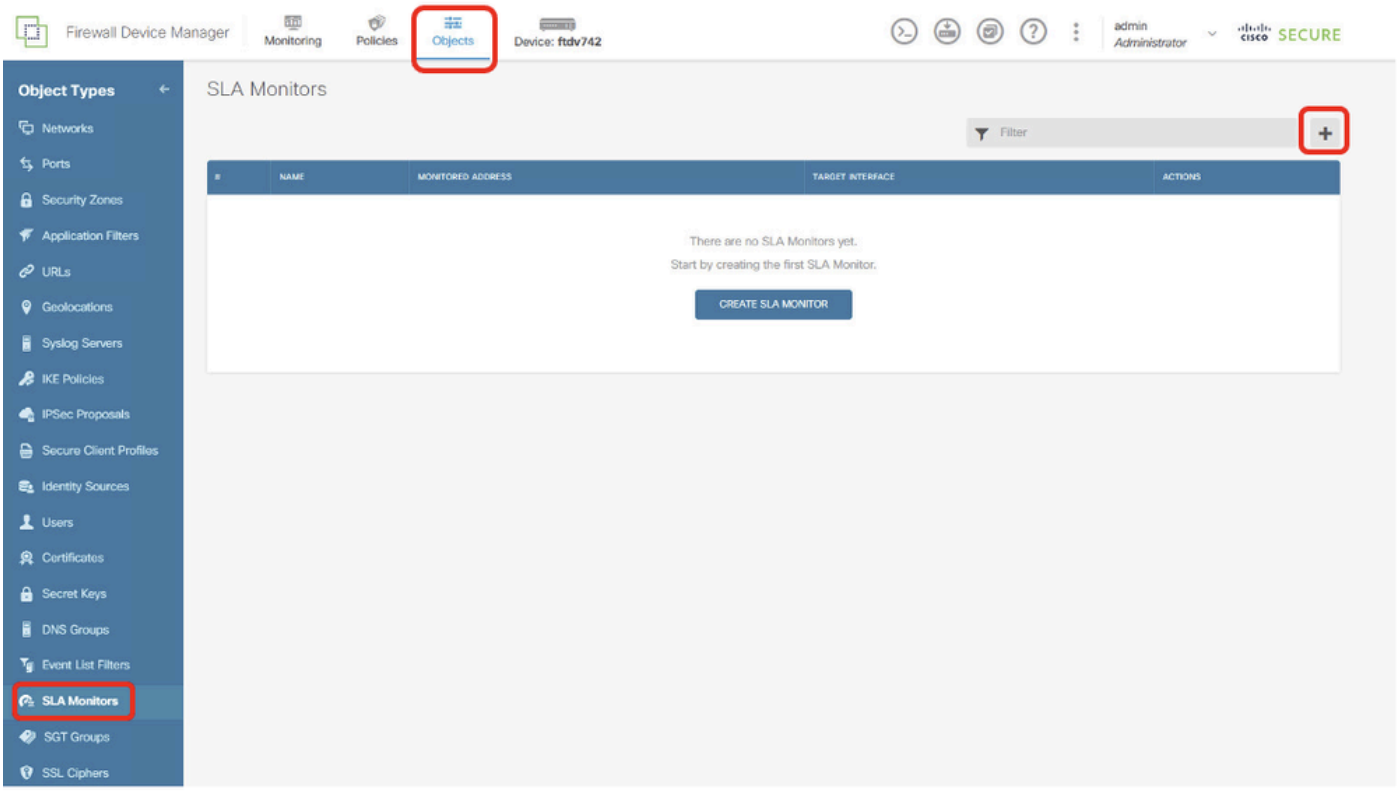
18.2단계. ISP2 게이트웨이 IP 주소에 대한 개체를 만듭니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: 외부2ToSP2_192.168.40.4
- 유형: 호스트
- 호스트: 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

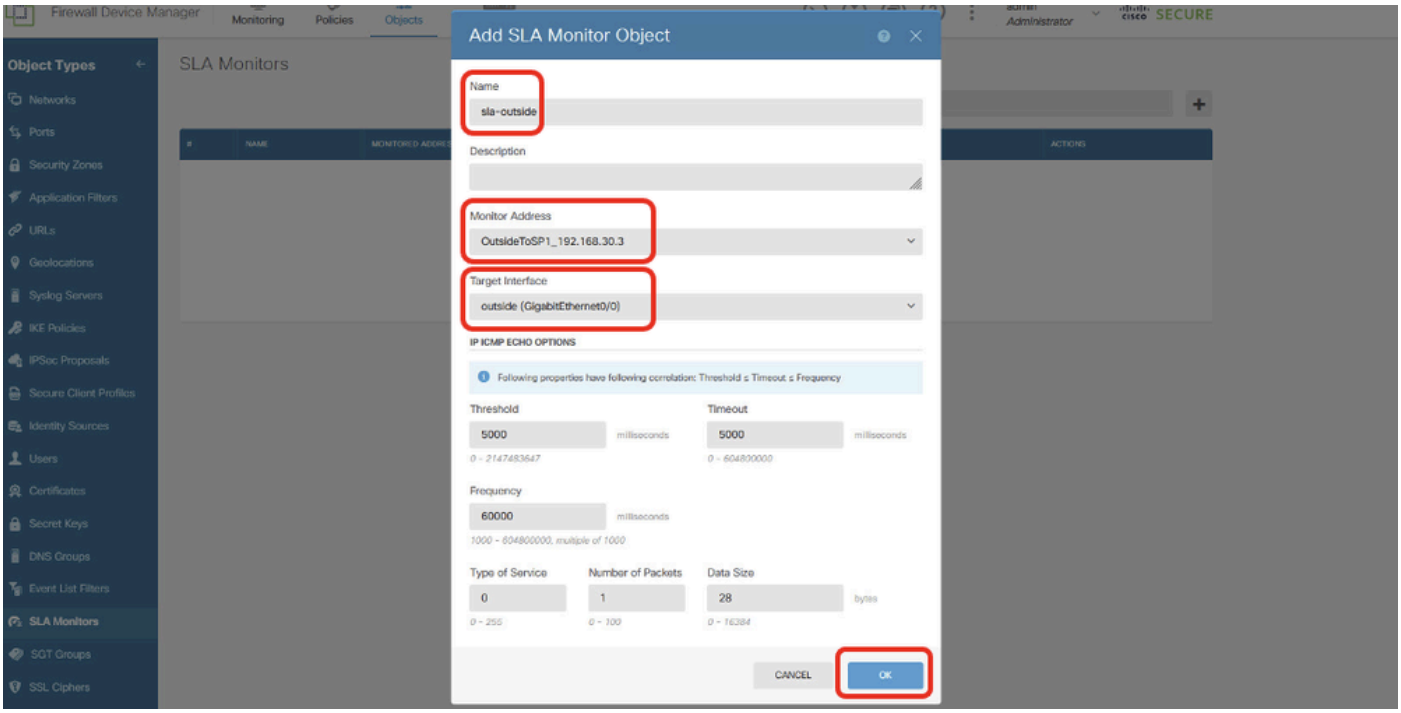
19단계. SLA 모니터를 생성합니다. Objects(개체) > Object Types(개체 유형) > SLA Monitors(SLA 모니터)로 이동합니다. 새 SLA 모니터를 생성하려면 + 버튼을 클릭합니다.



사이트1FTD_Create_SLAMonitor

19.1단계. Add SLA Monitor Object(SLA 모니터 개체 추가) 창에서 ISP1 게이트웨이에 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭하여 저장합니다.

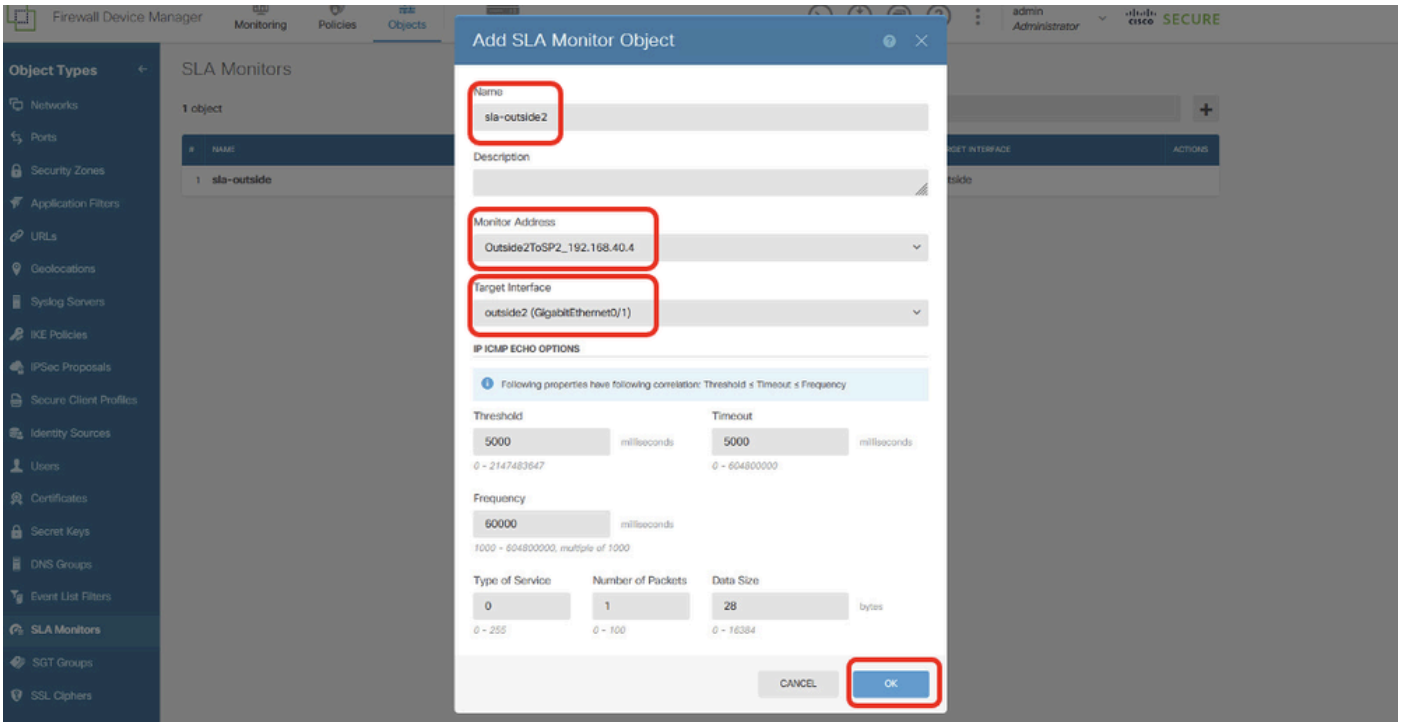
- 이름: sla 외부
- 모니터 주소: 외부SP1_192.168.30.3
- 대상 인터페이스: 외부(GigabitEthernet0/0)
- IP ICMP 에코 옵션: 기본값



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

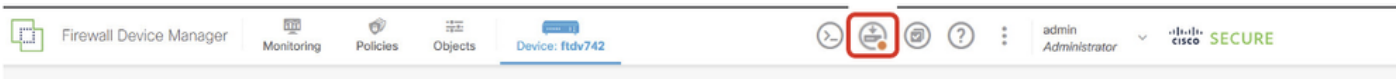
19.2단계. 계속해서 + 버튼을 클릭하여 ISP2 게이트웨이에 대한 새 SLA 모니터를 생성합니다. Add SLA Monitor Object(SLA 모니터 개체 추가) 창에서 ISP2 게이트웨이에 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭하여 저장합니다.

- 이름: sla 외부2
- 모니터 주소: 외부2ToSP2_192.168.40.4
- 대상 인터페이스: outside2(GigabitEthernet0/1)
- IP ICMP 에코 옵션: 기본값



Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

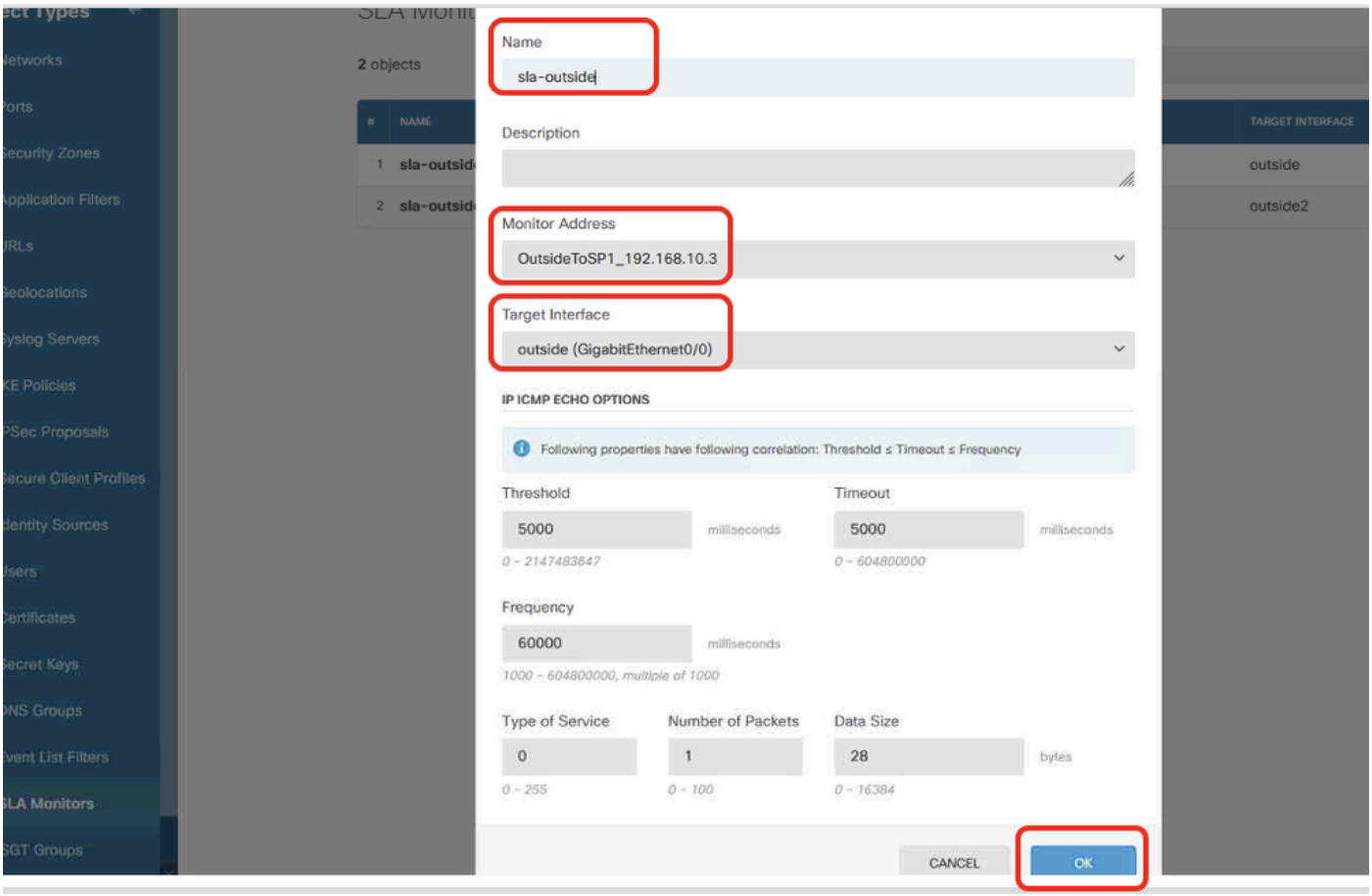
20단계. 구성 변경 사항을 배포합니다.



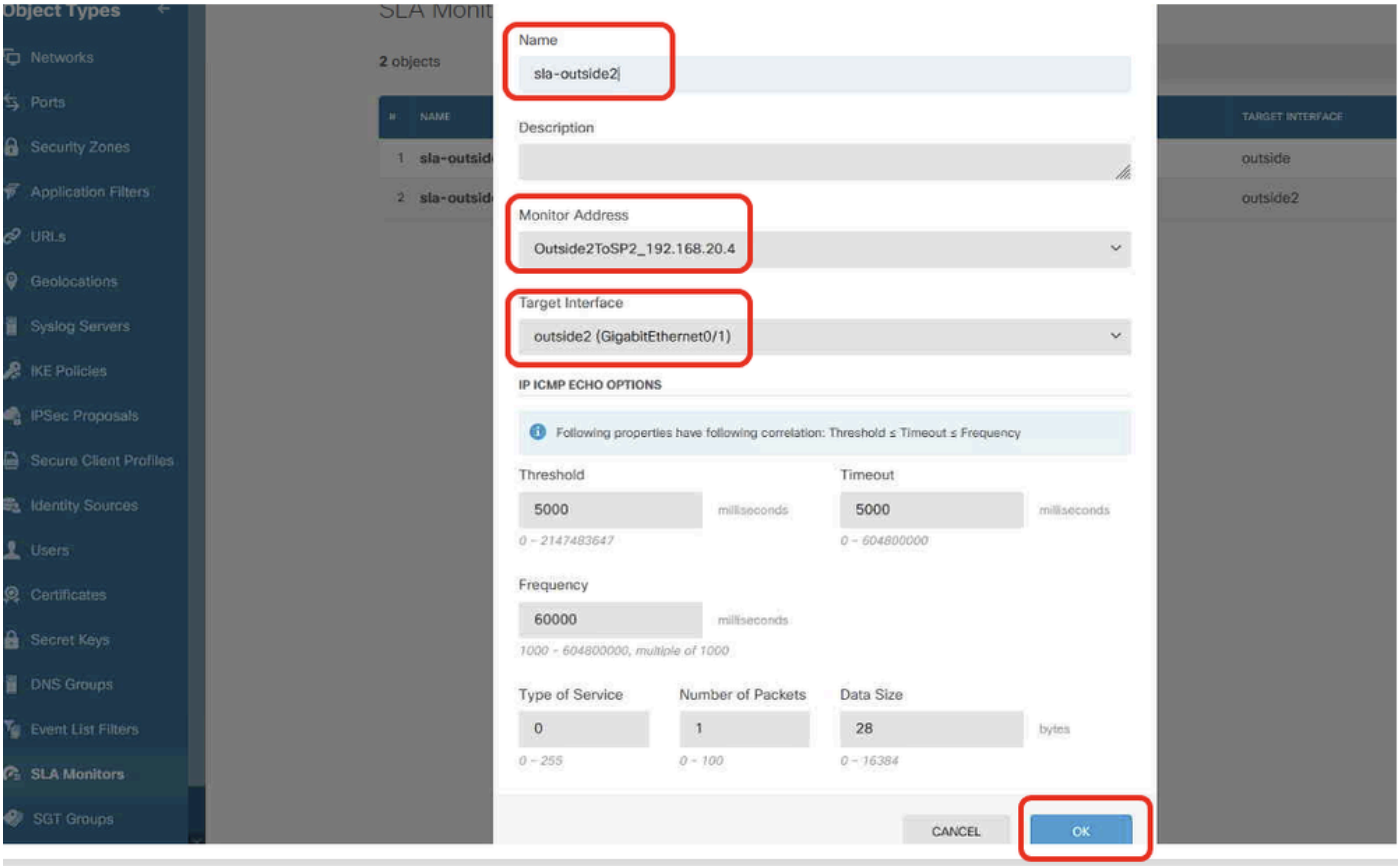
Site1FTD_Deployment_Changes

Site2 FTD SLA 모니터 컨피그레이션

21단계. 18단계 ~ 20단계를 반복합니다. Site2 FTD에서 해당 매개변수를 사용하여 SLA 모니터를 생성합니다.



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

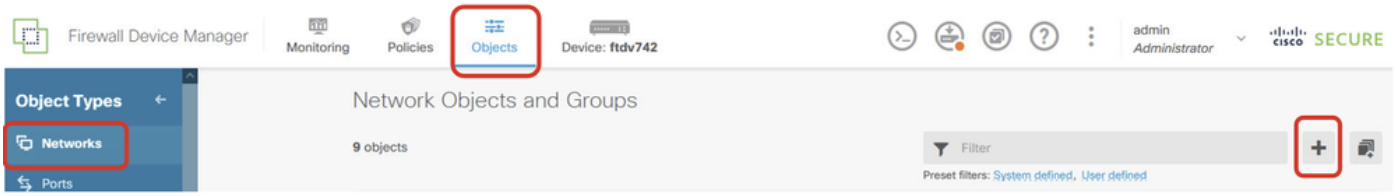


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

고정 경로의 컨피그레이션

Site1 FTD 정적 경로 컨피그레이션

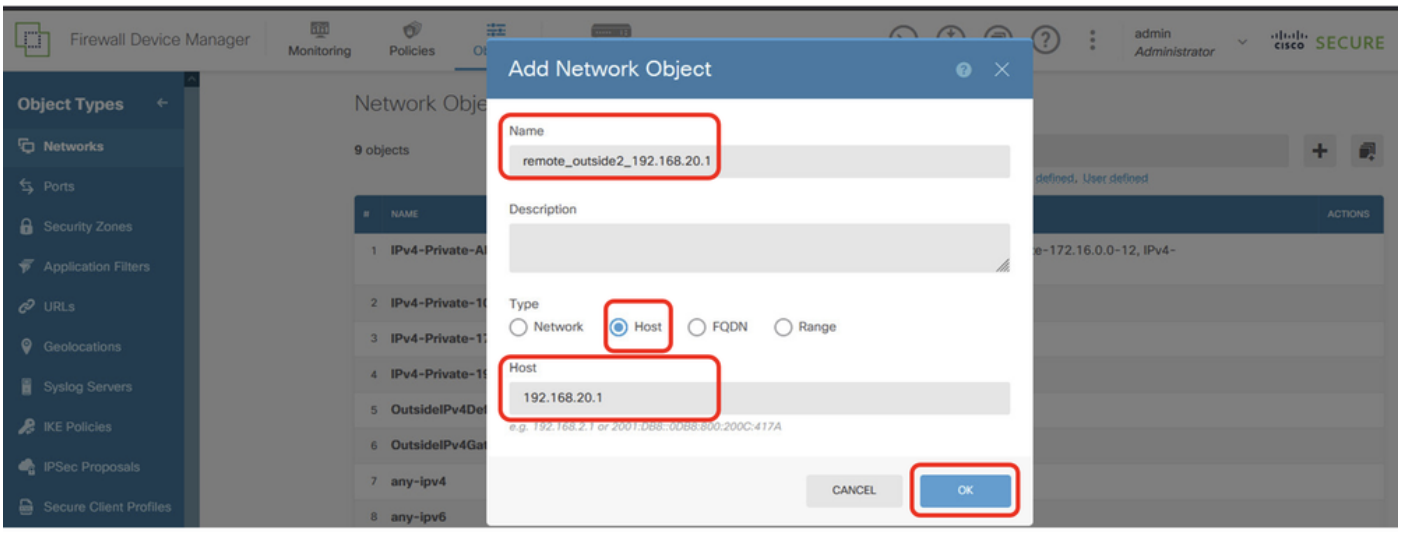
22단계. Site1 FTD에 대한 고정 경로에서 사용할 새 네트워크 객체를 생성합니다. Objects > Networks로 이동하고 + 버튼을 클릭합니다.



Site1FTD_Create_Obj

22.1단계. 피어 Site2 FTD의 outside2 IP 주소에 대한 개체를 만듭니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

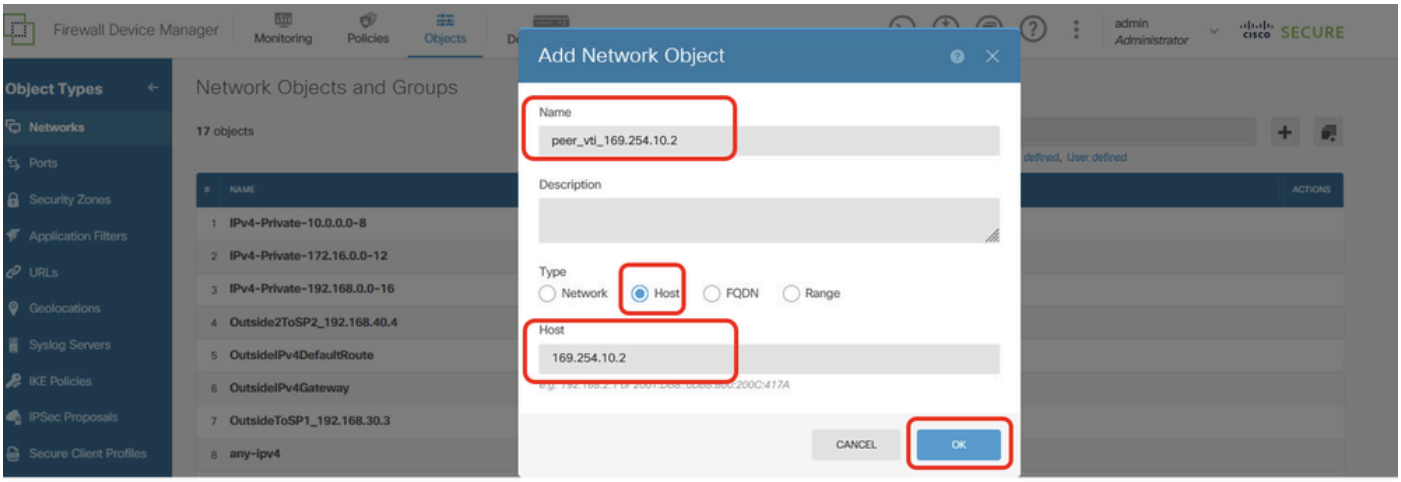
- 이름: remote_outside2_192.168.20.1
- 유형: 호스트
- 네트워크: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

22.2단계. 피어 Site2 FTD의 VTI Tunnel1 IP 주소에 대한 개체를 만듭니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

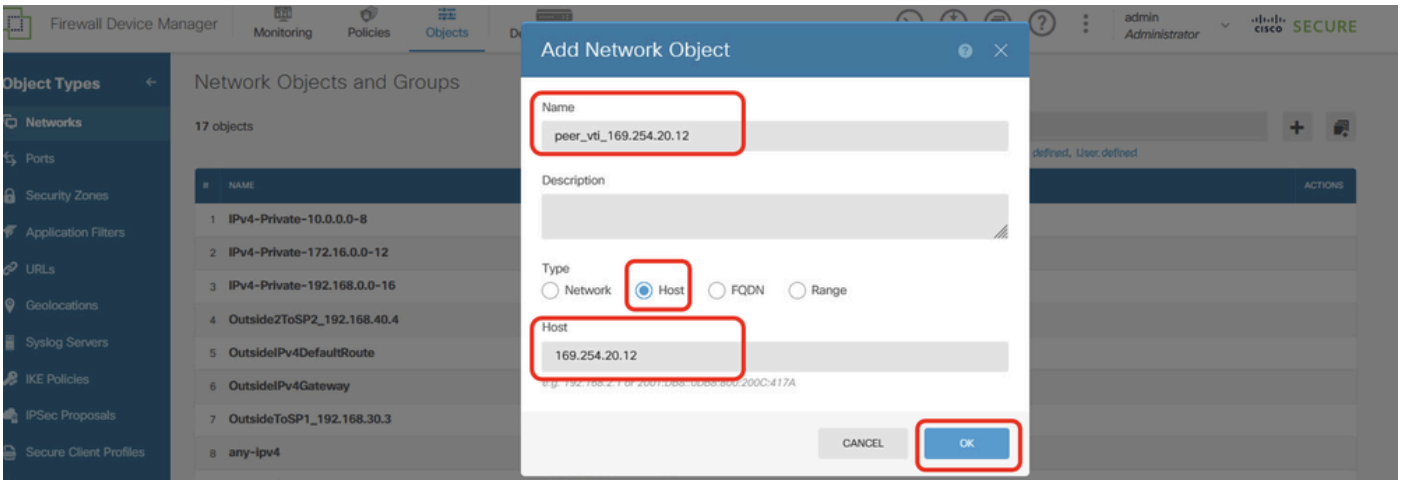
- 이름: peer_vti_169.254.10.2
- 유형: 호스트
- 네트워크:169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

22.3단계. 피어 Site2 FTD의 VTI Tunnel2 IP 주소에 대한 개체를 만듭니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

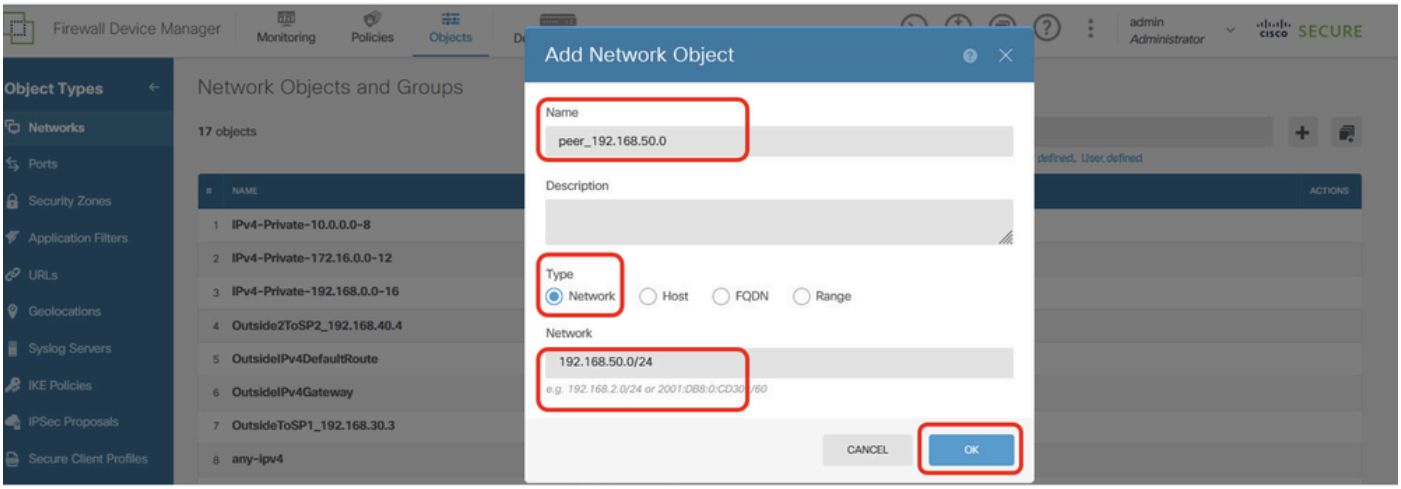
- 이름: peer_vti_169.254.20.12
- 유형: 호스트
- 네트워크:169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

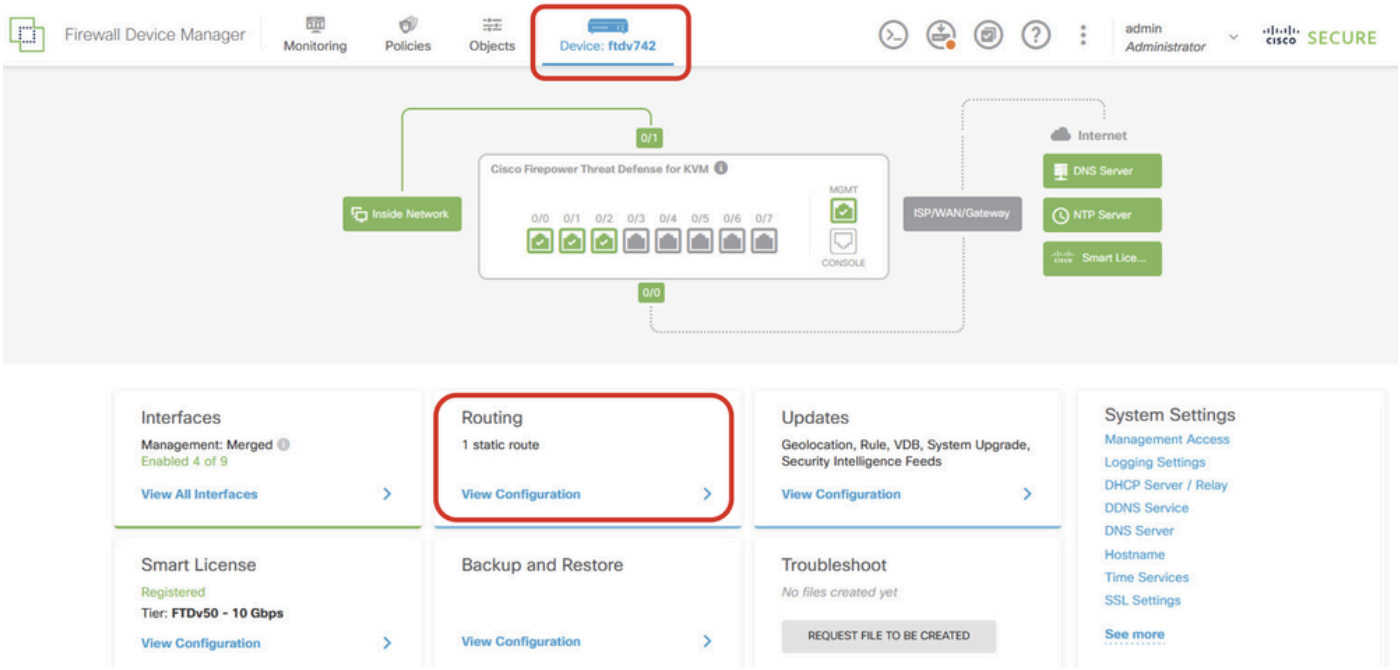
22.4단계. 피어 Site2 FTD의 내부 네트워크에 대한 개체를 만듭니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

- 이름: peer_192.168.50.0
- 유형: 네트워크
- 네트워크:192.168.50.0/24

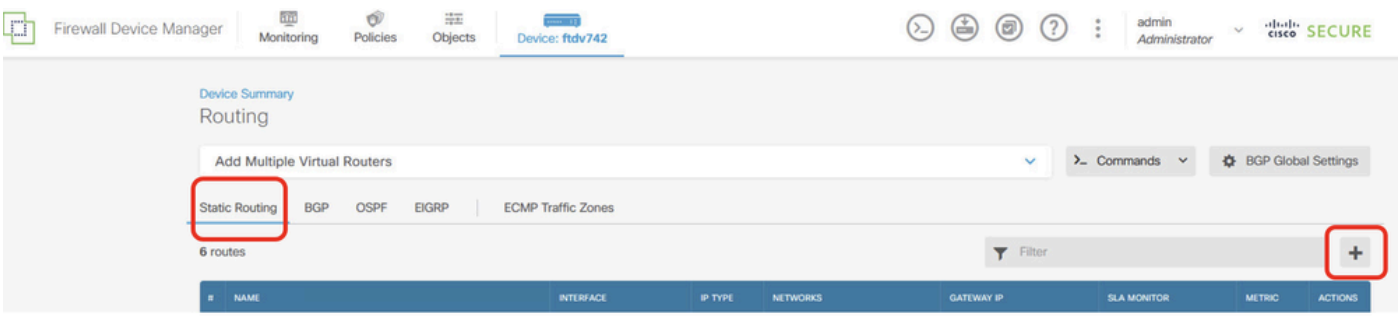


Site1FTD_Create_NetObj_StaticRoute_4

23단계. 장치 > 공정순서로 이동합니다. View Configuration(컨피그레이션 보기)을 클릭합니다. Static Routing 탭을 클릭합니다. 새 고정 경로를 추가하려면 + 버튼을 클릭합니다.



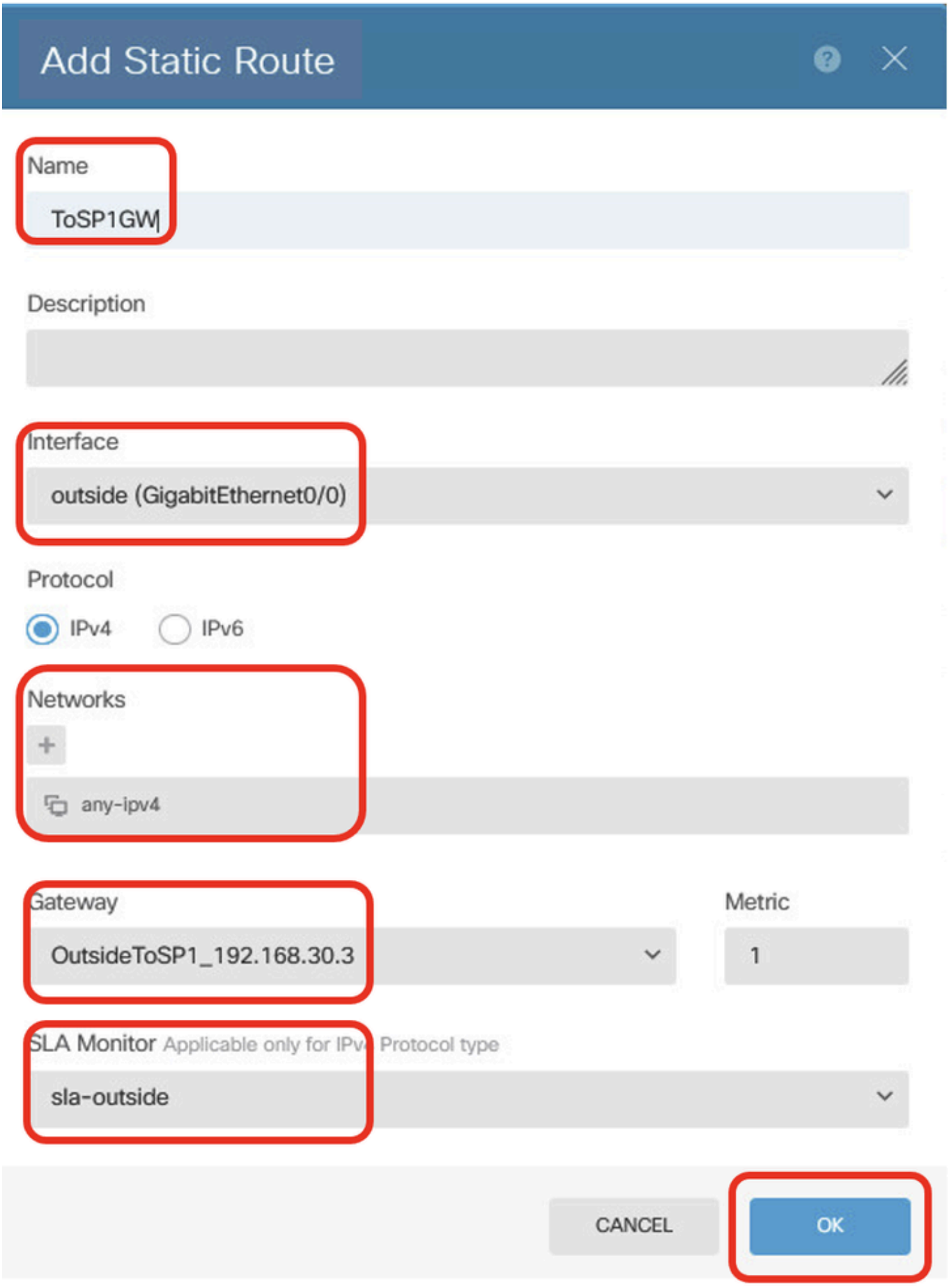
Site1FTD_View_Route_Configuration



Site1FTD_Add_Static_Route

23.1단계. SLA 모니터링이 포함된 ISP1 게이트웨이를 사용하여 기본 경로를 생성합니다. ISP1 게이트웨이가 중단되면 트래픽은 ISP2를 통해 백업 기본 경로로 전환됩니다. ISP1이 복구되면 트래픽은 ISP1을 사용하도록 되돌아갑니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭하여 저장합니다.

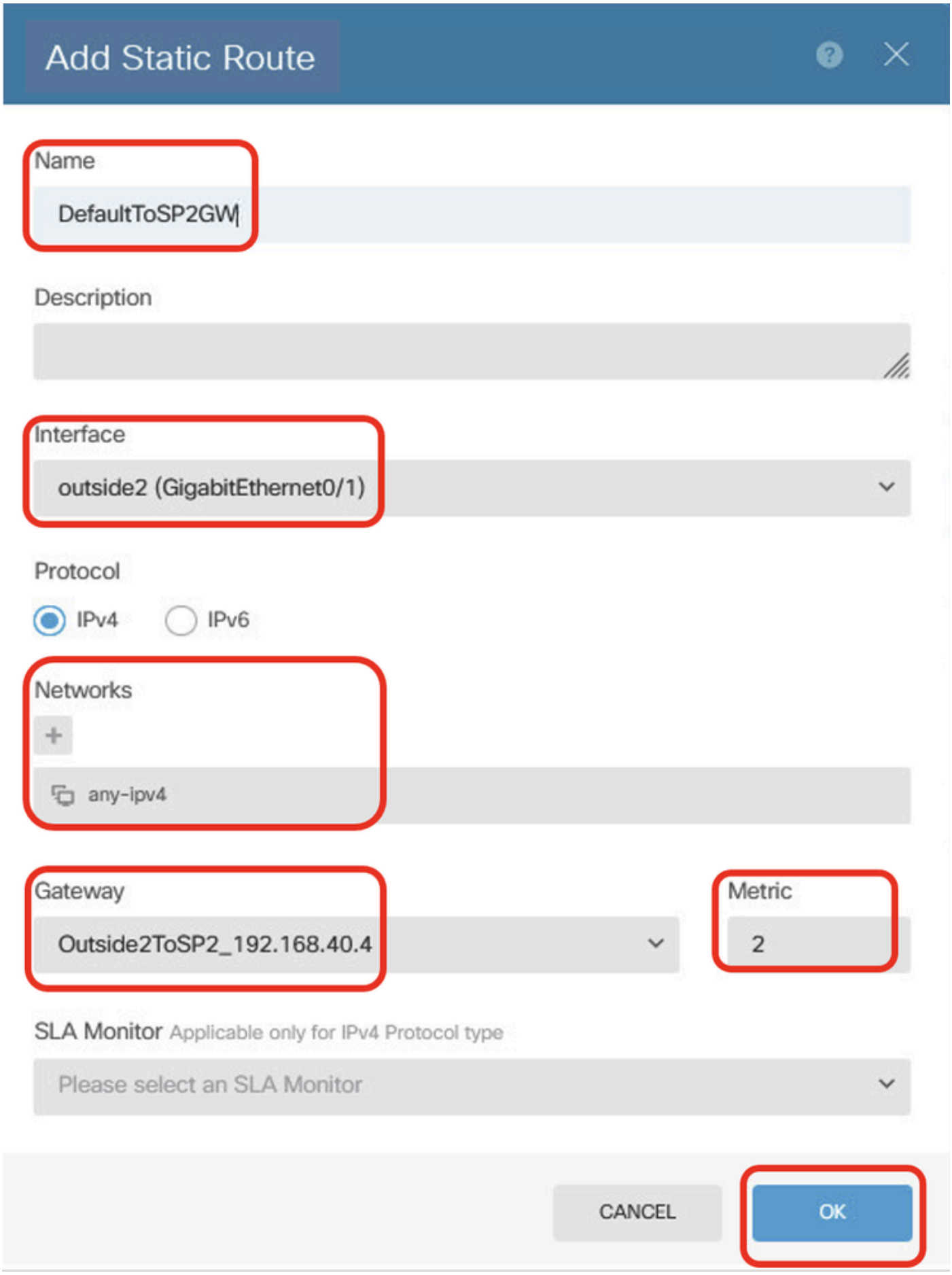
- 이름: 대상SP1GW
- 인터페이스: 외부(GigabitEthernet0/0)
- 프로토콜: IPv4
- 네트워크: any-ipv4
- 게이트웨이: 외부SP1_192.168.30.3
- 메트릭: 1
- SLA 모니터: sla 외부



Site1FTD_Create_StaticRoute_1

23.2단계. 게이트웨이 ISP2 게이트웨이를 통해 백업 기본 경로를 생성합니다. 메트릭은 1보다 커야 합니다. 이 예에서 메트릭은 2입니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭하여 저장합니다.

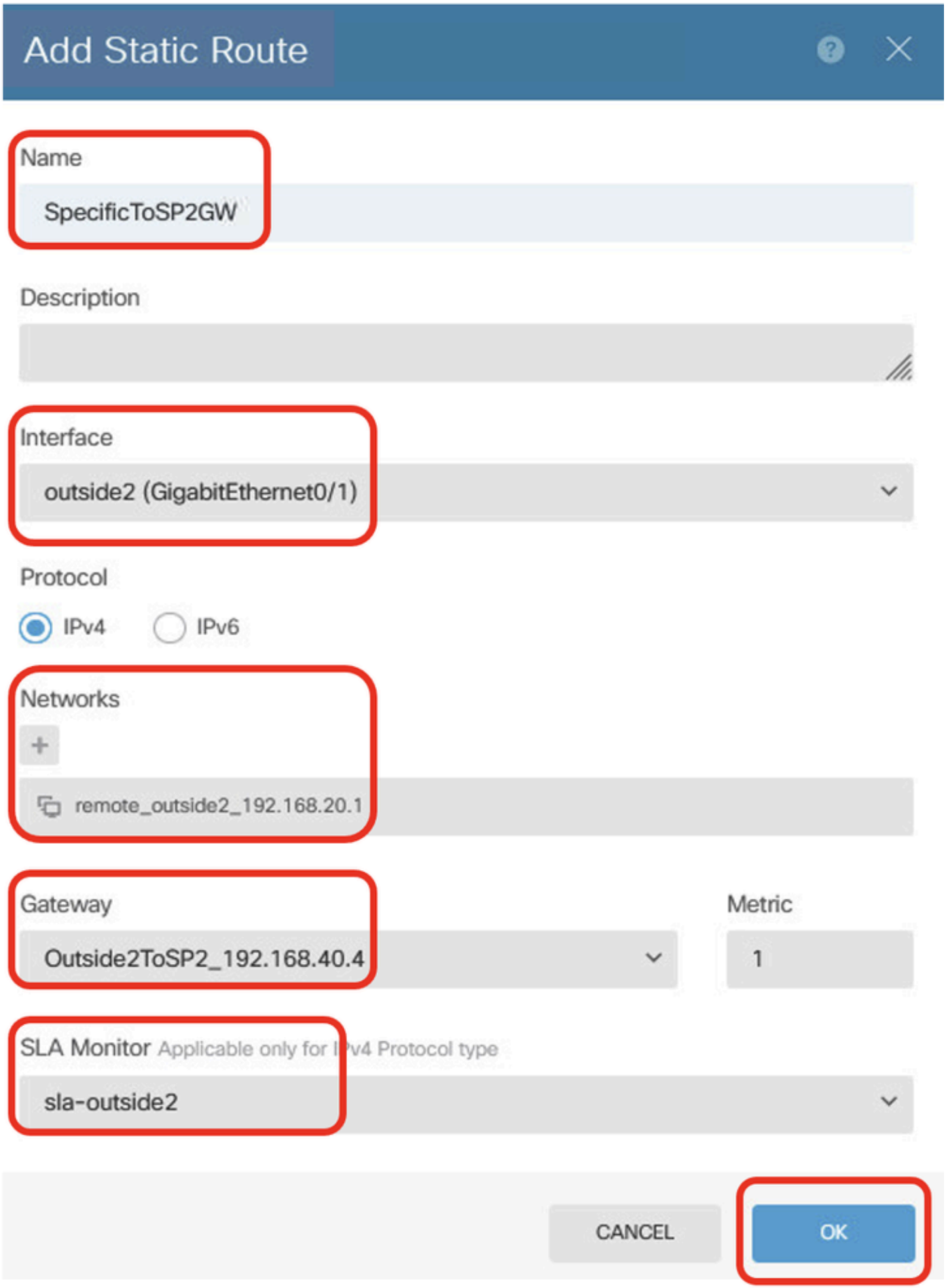
- 이름: 기본값SP2GW
- 인터페이스: outside2(GigabitEthernet0/1)
- 프로토콜: IPv4
- 네트워크: any-ipv4
- 게이트웨이: 외부2ToSP2_192.168.40.4
- 메트릭: 2



Site1FTD_Create_StaticRoute_2

23.3단계. Site2 FTD의 outside2로 VPN을 설정하는 데 사용되는 SLA 모니터링과 함께 ISP2 게이트웨이를 통해 피어 Site2 FTD의 outside2 IP 주소로 대상 트래픽의 고정 경로를 생성합니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭하여 저장합니다.

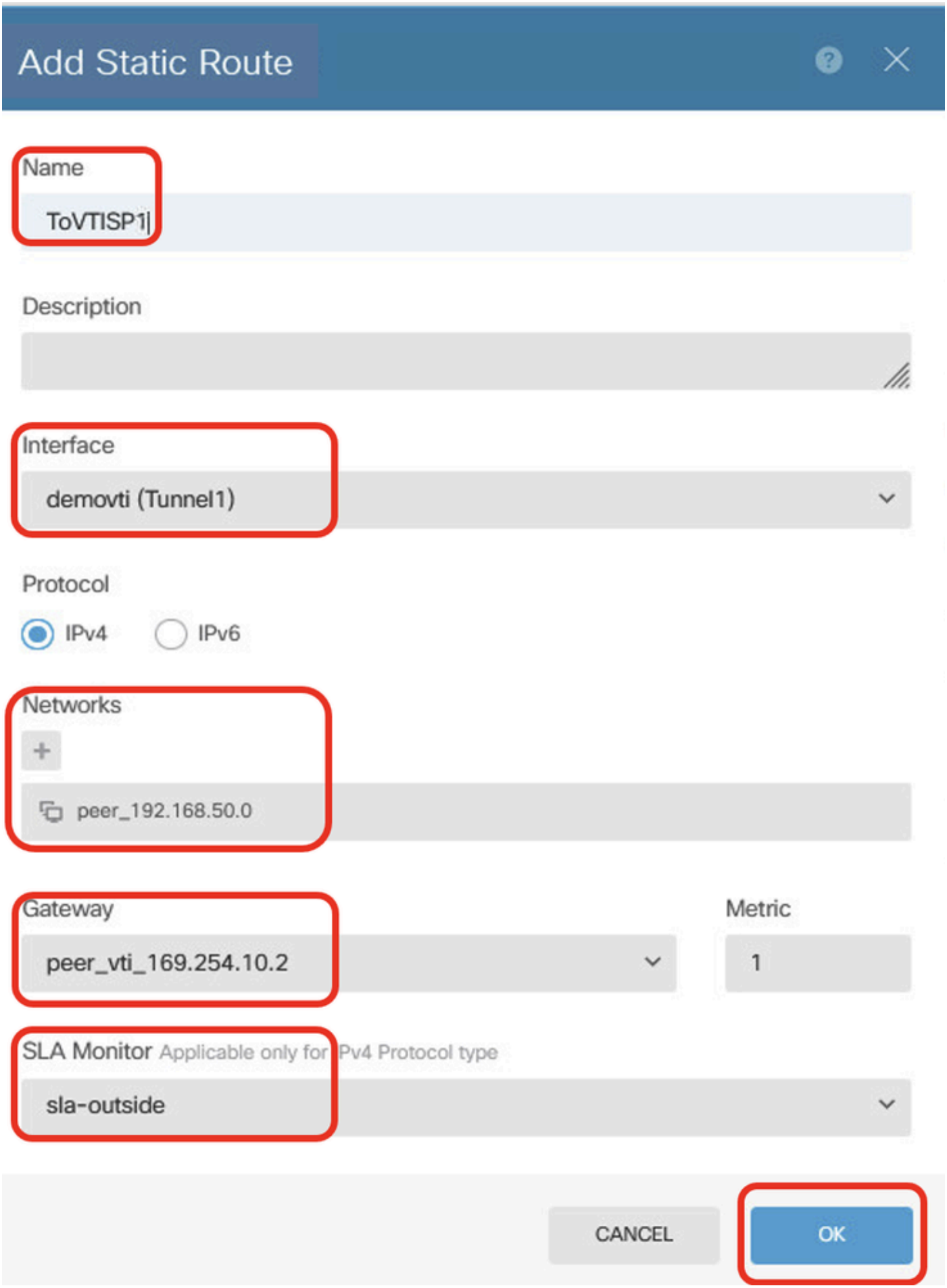
- 이름: 특정SP2GW
- 인터페이스: outside2(GigabitEthernet0/1)
- 프로토콜: IPv4
- 네트워크: remote_outside2_192.168.20.1
- 게이트웨이: 외부2ToSP2_192.168.40.4
- 메트릭: 1
- SLA 모니터: sla 외부2



Site1FTD_Create_StaticRoute_3

23.4단계. 게이트웨이로서 Site2 FTD의 피어 VTI 터널 1을 통해 피어 Site2 FTD의 내부 네트워크에 대한 대상 트래픽에 대한 고정 경로를 생성합니다. 터널 1을 통해 클라이언트 트래픽을 암호화하기 위한 SLA 모니터링을 사용합니다. ISP1 게이트웨이가 중단이 발생하면 VPN 트래픽은 ISP2의 VTI 터널 2로 전환됩니다. ISP1이 복구되면 트래픽은 ISP1의 VTI 터널 1로 되돌아갑니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭하여 저장합니다.

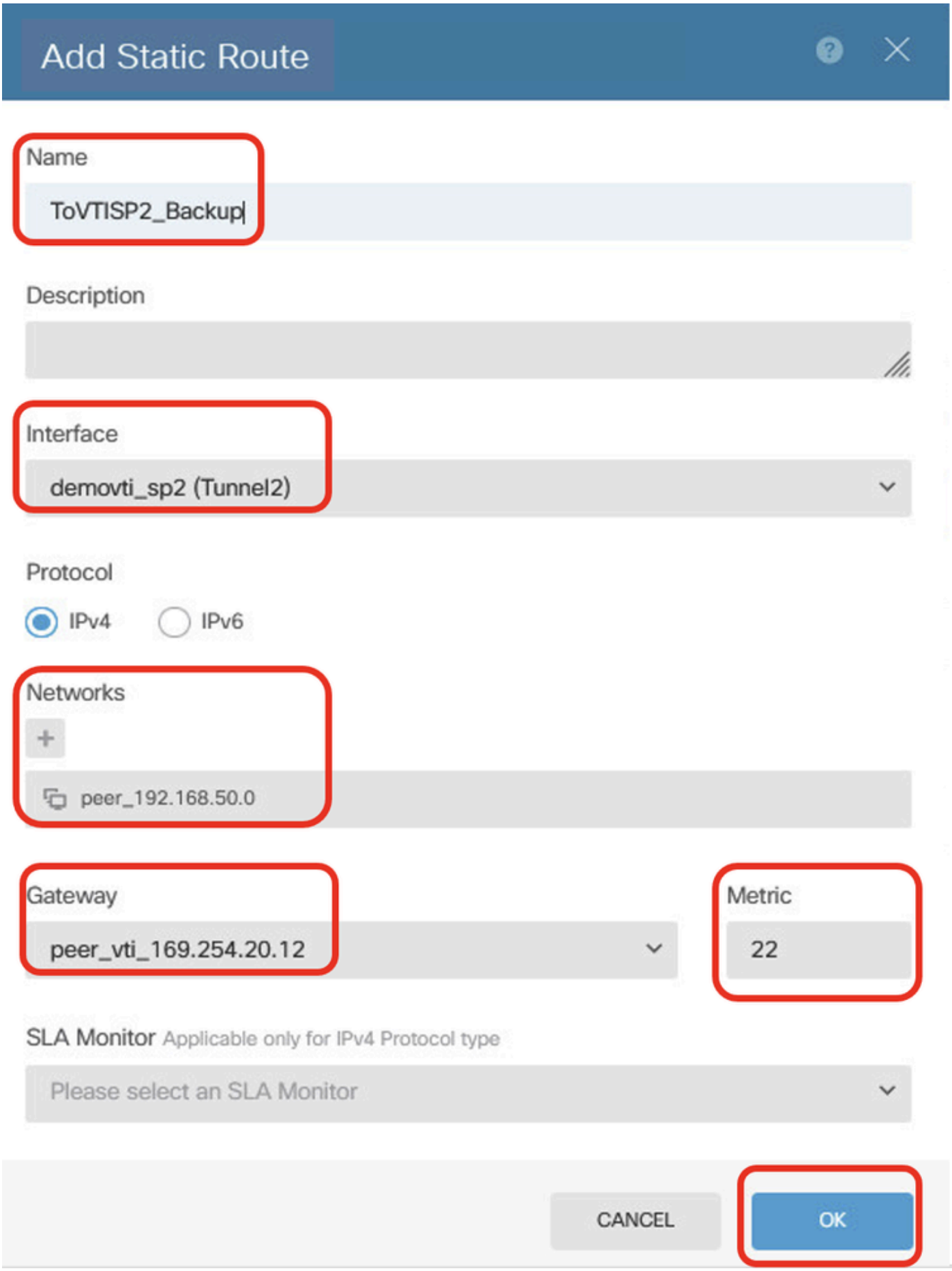
- 이름: ToVTISP1
- 인터페이스: demovti(터널1)
- 프로토콜: IPv4
- 네트워크: peer_192.168.50.0
- 게이트웨이: peer_vti_169.254.10.2
- 메트릭: 1
- SLA 모니터: sla 외부



Site1FTD_Create_StaticRoute_4

23.5단계. 터널 2를 통해 클라이언트 트래픽을 암호화하는 데 사용되는 게이트웨이로서 Site2 FTD의 피어 VTI 터널 2를 통해 피어 Site2 FTD의 내부 네트워크로 대상 트래픽에 대한 백업 고정 경로를 생성합니다. 메트릭을 1보다 큰 값으로 설정합니다. 이 예에서 메트릭은 22입니다. 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭하여 저장합니다.

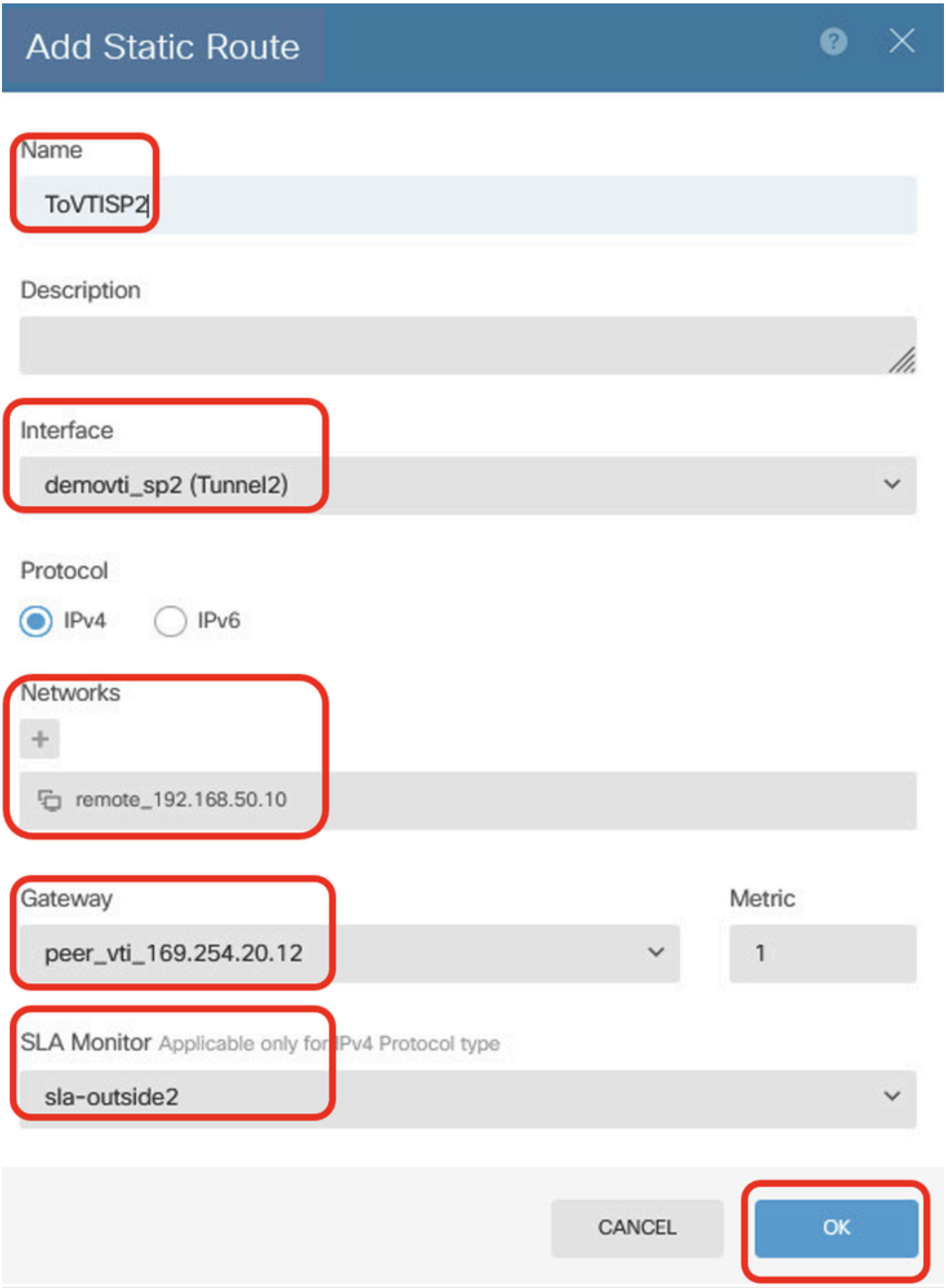
- 이름: ToVTISP2_백업
- 인터페이스: demovti_sp2(터널2)
- 프로토콜: IPv4
- 네트워크: peer_192.168.50.0
- 게이트웨이: peer_vti_169.254.20.12
- 메트릭: 22



Site1FTD_Create_StaticRoute_5

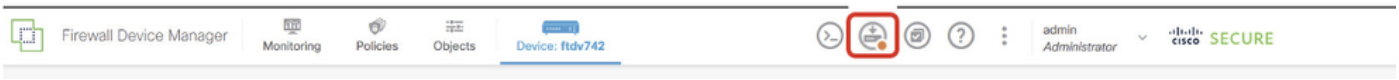
23.6단계. PBR 트래픽에 대한 고정 경로를 생성합니다. SLA 모니터링과 함께 게이트웨이로서의 Site2 FTD의 피어 VTI 터널 2를 통해 Site2 Client2에 대한 대상 트래픽입니다. 필요한 정보를 제공하십시오. OK(확인) 버튼을 클릭하여 저장합니다.

- 이름: ToVTISP2
- 인터페이스: demovti_sp2(터널2)
- 프로토콜: IPv4
- 네트워크: remote_192.168.50.10
- 게이트웨이: peer_vti_169.254.20.12
- 메트릭: 1
- SLA 모니터: sla 외부2



Site1FTD_Create_StaticRoute_6

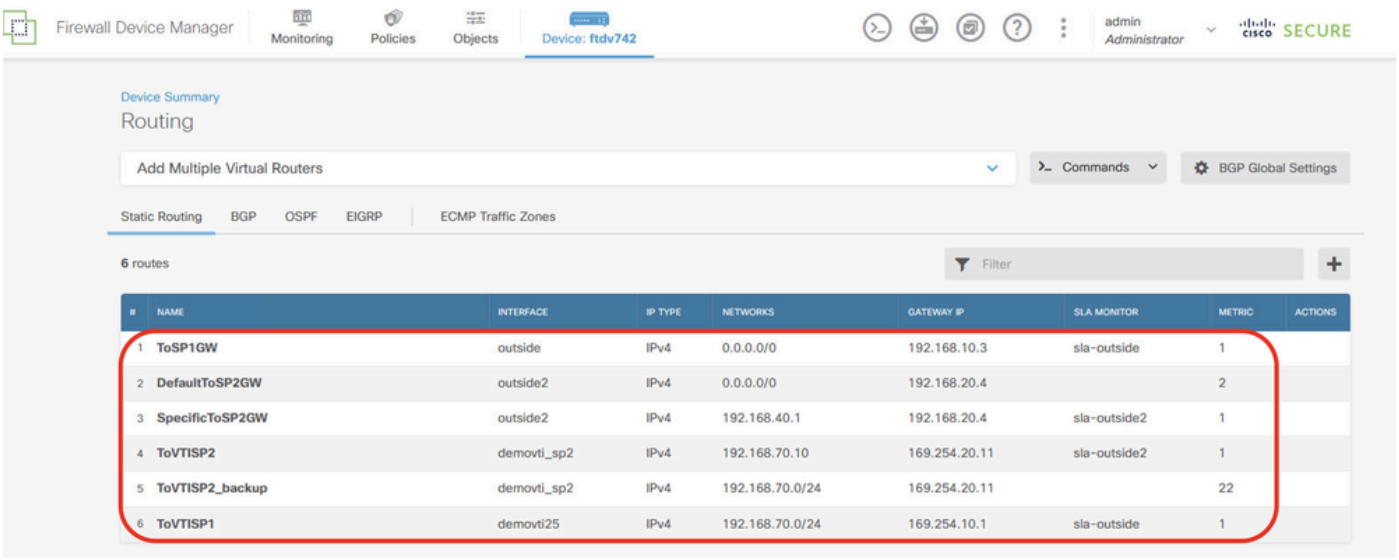
24단계. 컨피그레이션 변경 사항을 구축합니다.



Site1FTD_Deployment_Changes

Site2 FTD 정적 경로 컨피그레이션

25단계. Site2 FTD에 대한 해당 매개변수로 고정 경로를 생성하려면 22~24단계를 반복합니다.



Site2FTD_Create_StaticRoute

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오. 콘솔 또는 SSH를 통해 Site1 FTD 및 Site2 FTD의 CLI로 이동합니다.

ISP1 및 ISP2 모두 정상 작동

VPN

```
//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1072332533 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
1045734377 192.168.40.1/500                                192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
499259237 192.168.10.1/500                                192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
477599833 192.168.20.1/500                                192.168.40.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607
```

경로

```
// Site1 FTD:

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
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA 모니터

```
// Site1 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
```

```
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:


ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900

Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
```

```
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

// Site2 FTD:

```
ftdv742#  show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
```

```
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100

Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Ping 테스트

시나리오 1. Site1 Client1 Site2 Client1에 ping합니다.

ping하기 전에 show crypto ipsec sa의 카운터를 확인하십시오. | inc 인터페이스:|encap|decap on Site1 FTD.

이 예에서 Tunnel1은 캡슐화를 위해 1497개의 패킷을, 역캡슐화를 위해 1498개의 패킷을 보여줍니다.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
      #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
```

```
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 Site2 Client1에 대해 ping을 수행했습니다.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

show crypto ipsec sa의 카운터를 확인합니다. | inc 인터페이스:|encap|decap on Site1 FTD after ping successfully.

이 예에서 터널 1은 캡슐화를 위한 1502개의 패킷과 캡슐화를 위한 1503개의 패킷을 보여주며, 두 카운터는 모두 5개 패킷씩 증가하여 5개의 ping 에코 요청과 일치합니다. 이는 Site1 Client1에서 Site2 Client1로의 ping이 ISP1 터널 1을 통해 라우팅됨을 나타냅니다. 터널 2에서는 캡슐화 또는 캡슐화 해제 카운터가 증가하지 않았으므로 이 트래픽에 사용되고 있지 않음을 확인합니다.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
      #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

시나리오 2. Site1 Client2 Site2 Client2에 ping합니다.

ping하기 전에 show crypto ipsec sa의 카운터를 확인하십시오. | inc 인터페이스:|encap|decap on Site1 FTD.

이 예에서 Tunnel2는 캡슐화를 위해 21개의 패킷을, 캡슐화를 위해 20개의 패킷을 보여줍니다.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
```

```
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2 Site2 Client2에 대해 ping을 수행했습니다.

```
Site1_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 = 4/39/87 ms
```

show crypto ipsec sa의 카운터를 확인합니다. | inc 인터페이스:|encap|decap on Site1 FTD after ping successfully.

이 예에서 Tunnel 2는 캡슐화를 위한 26개 패킷과 캡슐화를 위한 25개 패킷을 보여주며, 두 카운터는 모두 5개 패킷 증가하여 5개의 ping 에코 요청과 일치합니다. 이는 Site1 Client2에서 Site2 Client2로의 ping이 ISP2 터널 2를 통해 라우팅됨을 나타냅니다. 터널 1에서는 캡슐화 또는 캡슐화 해제 카운터가 증가하지 않았으므로 이 트래픽에 사용되고 있지 않음을 확인합니다.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP1이 정상적으로 작동하는 동안 ISP1이 중단 경험

이 예에서는 ISP1에서 인터페이스 E0/1을 수동으로 종료하여 중단이 발생한 ISP1을 시뮬레이션합니다.

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
```

```
Internet_SP1(config)#
```

VPN

터널 1이(가) 다운되었습니다. IKEV2 SA에서는 Tunnel2만 활성화됩니다.

```
// Site1 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.1, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.30.1
    Destination IP address: 192.168.10.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d


ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
1045734377 192.168.40.1/500                                      192.168.20.1/500                    G
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.2, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.10.1
    Destination IP address: 192.168.30.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
477599833 192.168.20.1/500                                      192.168.40.1/500                    G
```

```
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

경로

경로 테이블에서 백업 경로가 적용됩니다.

```
// Site1 FTD:

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 192.168.40.4 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
```

```
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA 모니터

Site1 FTD에서 SLA 모니터는 ISP1에 대한 항목 번호 855903900 시간 초과(대상 주소는 192.168.30.3)를 표시합니다.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000

Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

ftdv742# show track
Track 1
```

```
  Response Time Reporter 855903900 reachability
  Reachability is Down
  7 changes, last change 00:11:03
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Up
  4 changes, last change 13:15:11
  Latest operation return code: OK
  Latest RTT (millisecs) 140
  Tracked by:
    STATIC-IP-ROUTING 0
```

Ping 테스트

ping하기 전에 show crypto ipsec sa의 카운터를 확인하십시오. | inc 인터페이스:|encap|decap on Site1 FTD.

이 예에서 Tunnel2는 캡슐화를 위해 36개의 패킷을, 역캡슐화를 위해 35개의 패킷을 보여줍니다.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
      #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 Site2 Client1에 대해 ping을 수행했습니다.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

Site1 Client2 Site2 Client2에 대해 ping을 수행했습니다.

```
Site1_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 = 34/56/87 ms
```

show crypto ipsec sa의 카운터를 확인합니다. | inc 인터페이스:|encap|ping에 성공한 후 사이트1 FTD에서 decap

이 예에서 터널 2는 캡슐화를 위한 46개 패킷과 캡슐화를 위한 45개 패킷을 보여주며, 두 카운터는 모두 10개 패킷 증가하여 10개의 ping 에코 요청과 일치합니다. 이는 ping 패킷이 ISP2 터널 2를 통해 라우팅됨을 나타냅니다.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
      #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP1이 정상적으로 작동하는 동안 ISP2에서 중단 경험

이 예에서는 ISP2에서 인터페이스 E0/1을 수동으로 종료하여 중단이 발생한 ISP2를 시뮬레이션합니다.

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

터널 2가 다운되었습니다. IKEV2 SA에서는 Tunnel1만 활성화됩니다.

```
// Site1 FTD:

ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.40.1
    Destination IP address: 192.168.20.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:
```

```
Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1375077093 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc
```

```
// Site2 FTD:

ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.12, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.20.1
    Destination IP address: 192.168.40.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1025640731 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

경로

경로 테이블에서 PBR 트래픽에 대해 ISP2 관련 경로가 비활성화되었습니다.

```
// Site1 FTD:

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
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside
```

```
// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

SLA 모니터

Site1 FTD에서 SLA 모니터는 ISP2에 대한 항목 번호 188426425 시간 초과(대상 주소는 192.168.40.4)를 표시합니다.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
```

```
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100


ftdv742#  show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Up
  8 changes, last change 00:14:37
  Latest operation return code: OK
  Latest RTT (millisecs) 60
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Down
  5 changes, last change 00:09:30
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

Ping 테스트

ping하기 전에 show crypto ipsec sa의 카운터를 확인하십시오. | inc 인터페이스:|encap|decap on Site1 FTD.

이 예에서 Tunnel 1은 캡슐화를 위해 74개의 패킷을, 역캡슐화를 위해 73개의 패킷을 보여줍니다.

```
// Site1 FTD:
```

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
      #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 Site2 Client1에 대해 ping을 수행했습니다.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

Site1 Client2 Site2 Client2에 대해 ping을 수행했습니다.

```
Site1_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 = 6/58/143 ms
```

show crypto ipsec sa의 카운터를 확인합니다. | inc 인터페이스:|encap|decap을 Site1 FTD에서 ping했습니다.

이 예에서 Tunnel 1은 캡슐화를 위한 84개 패킷과 캡슐화를 위한 83개 패킷을 보여주며, 두 카운터는 모두 10개 패킷 증가하여 10개의 ping 에코 요청과 일치합니다. 이는 ping 패킷이 ISP1 터널 1을 통해 라우팅됨을 나타냅니다.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
      #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
      #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 PBR 섹션의 문제를 해결할 수 있습니다.

```
debug policy-route
```

이러한 debug 명령을 사용하여 SLA Monitor 섹션의 문제를 해결할 수 있습니다.

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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.