FDM에서 관리하는 FTD에서 경로 기반 VPN을 통한 BGP 구성

목차

소개

이 문서에서는 FDM(Firepower Device Manager)에서 관리되는 FTDv에서 경로 기반 사이트 대 사이트 VPN을 통한 BGP 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- VPN에 대한 기본 이해
- FTDv의 BGP 컨피그레이션
- FDM 사용 경험

사용되는 구성 요소

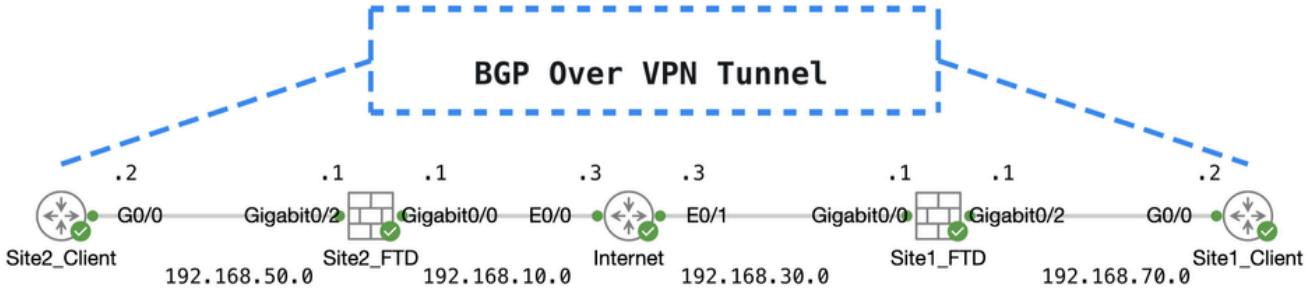
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 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.

구성

네트워크 다이어그램



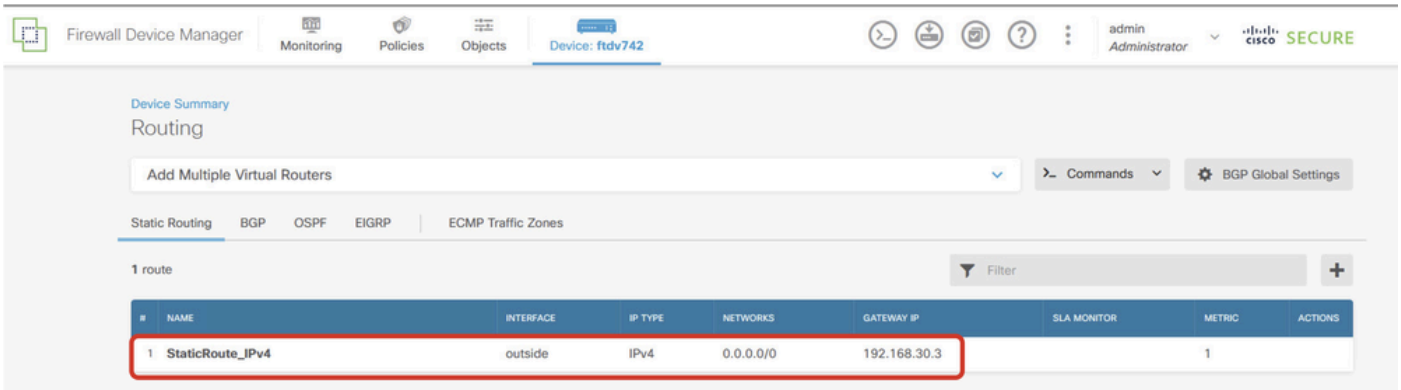
토포

VPN의 컨피그레이션

1단계. 노드 간의 IP 상호 연결이 준비되어 있고 안정적인지 확인합니다. FDM의 스마트 라이선스가 스마트 계정에 등록되었습니다.

2단계. Site1 클라이언트의 게이트웨이는 Site1 FTD(192.168.70.1)의 내부 IP 주소로 구성됩니다. Site2 클라이언트의 게이트웨이는 Site2 FTD(192.168.50.1)의 내부 IP 주소로 구성됩니다. 또한 FDM 초기화 후 두 FTD의 기본 경로가 올바르게 구성되었는지 확인합니다.

각 FDM의 GUI에 로그인합니다. 으로 이동합니다.Device > Routing 을 클릭합니다.View Configuration 기본 고정 경로를 **Static Routing** 확인하려면 탭을 클릭합니다.

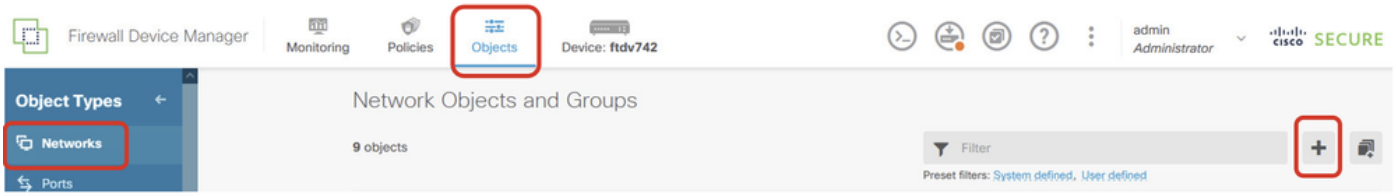


사이트1_FTD_게이트웨이

Site2_FTD_게이트웨이

3단계. 경로 기반 Site-to-Site VPN을 구성합니다. 이 예에서는 먼저 Site1 FTD를 구성합니다.

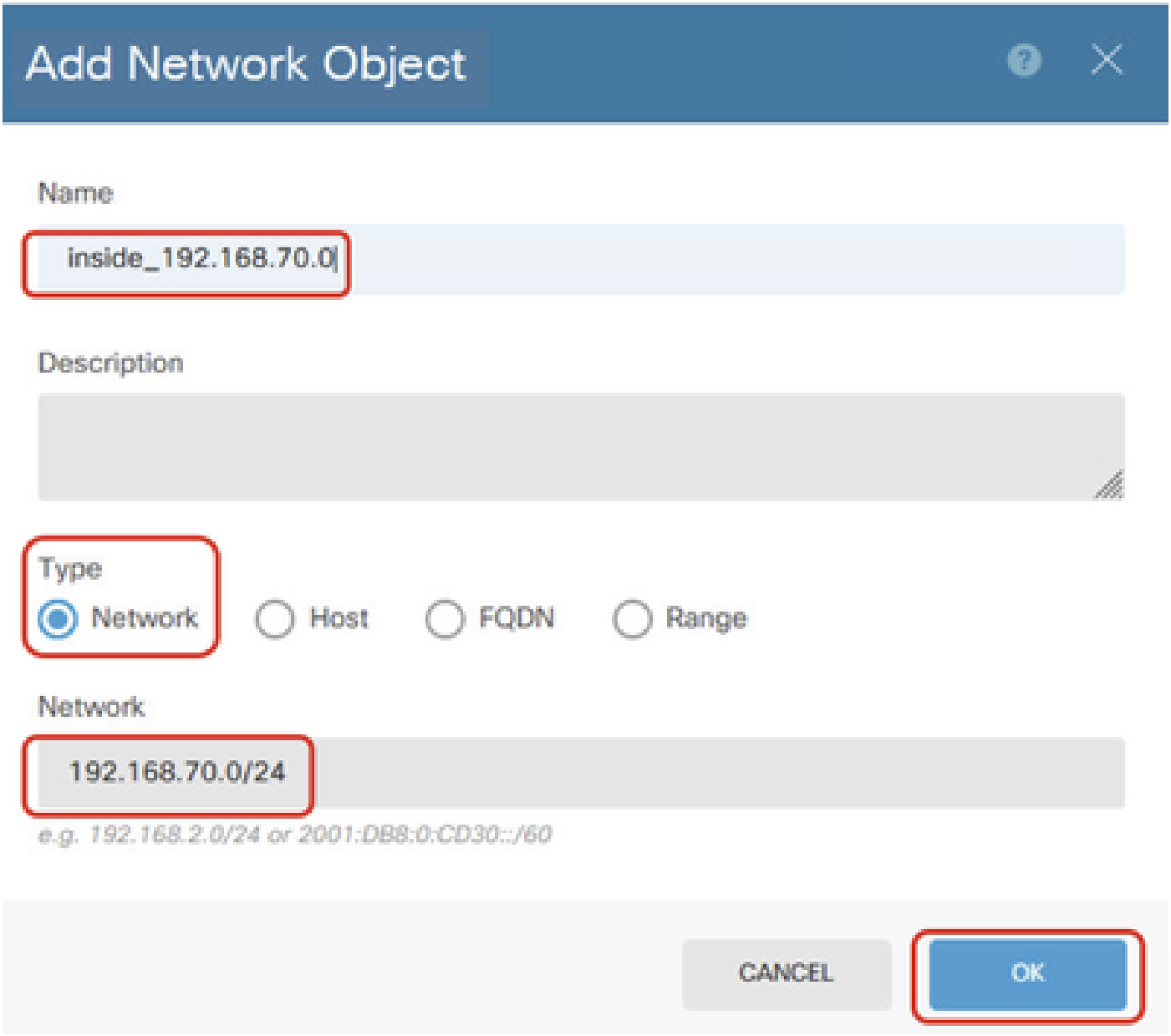
3.1단계. Site1 FTD의 FDM GUI에 로그인합니다. Site1 FTD의 내부 네트워크에 대한 새 네트워크 객체를 만듭니다. 로 **Objects** > **Networks**이동하고 + 버튼을 클릭합니다.



Create_Network_Object

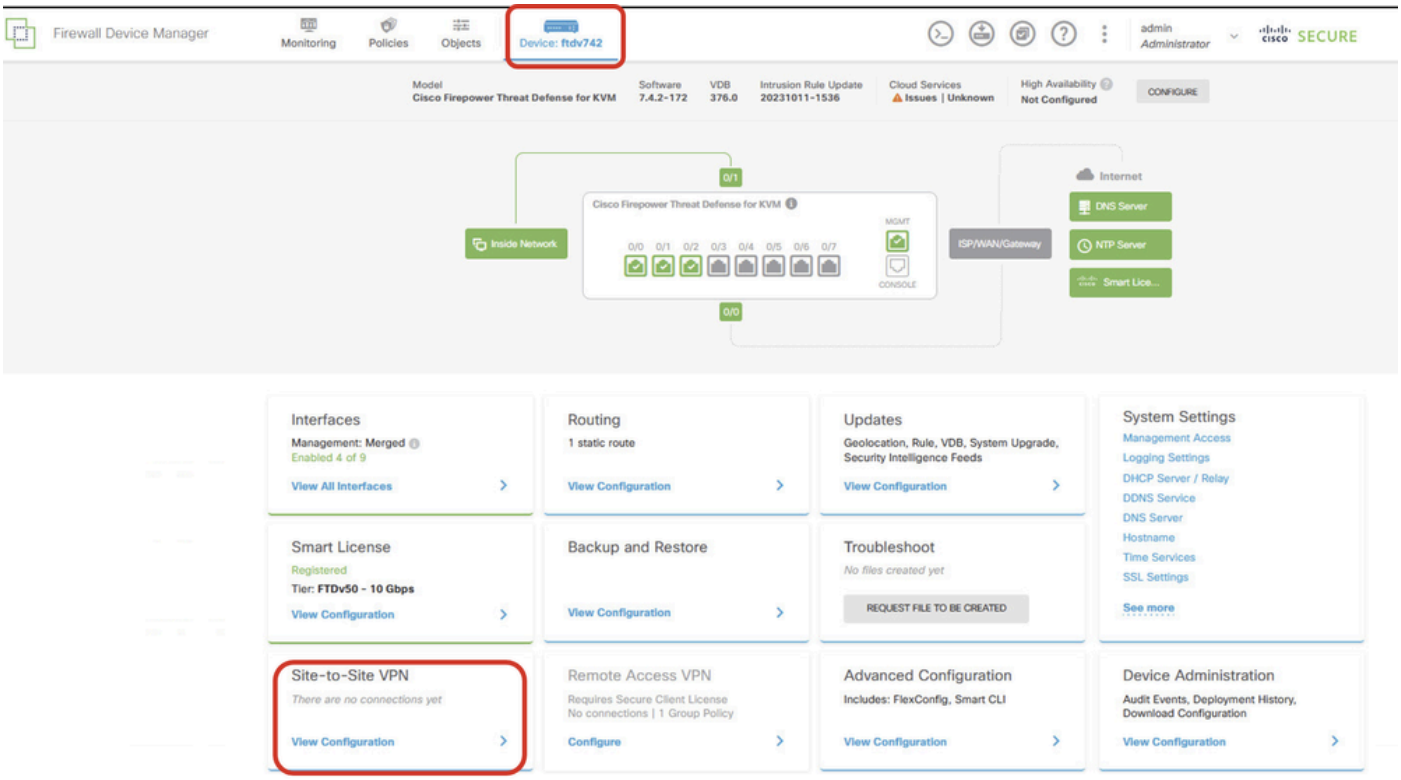
3.2단계. 필요한 정보를 제공합니다. 버튼을OK 클릭합니다.

- 이름: inside_192.168.70.0
- 유형: 네트워크
- 네트워크: 192.168.70.0/24



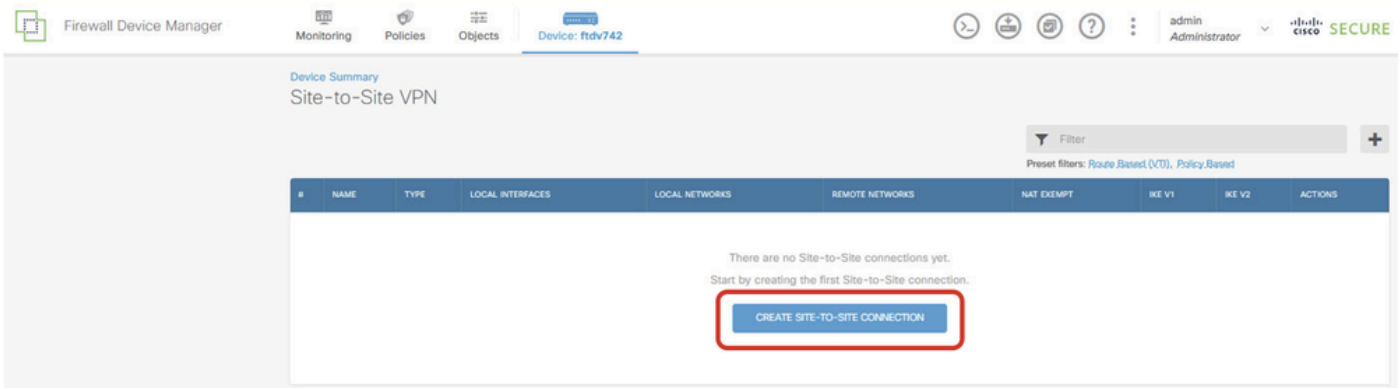
사이트1_내부_네트워크

3.3단계. 으로 이동합니다.**Device > Site-to-Site VPN** 을 클릭합니다.**View Configuration**



Site-to-Site VPN 보기

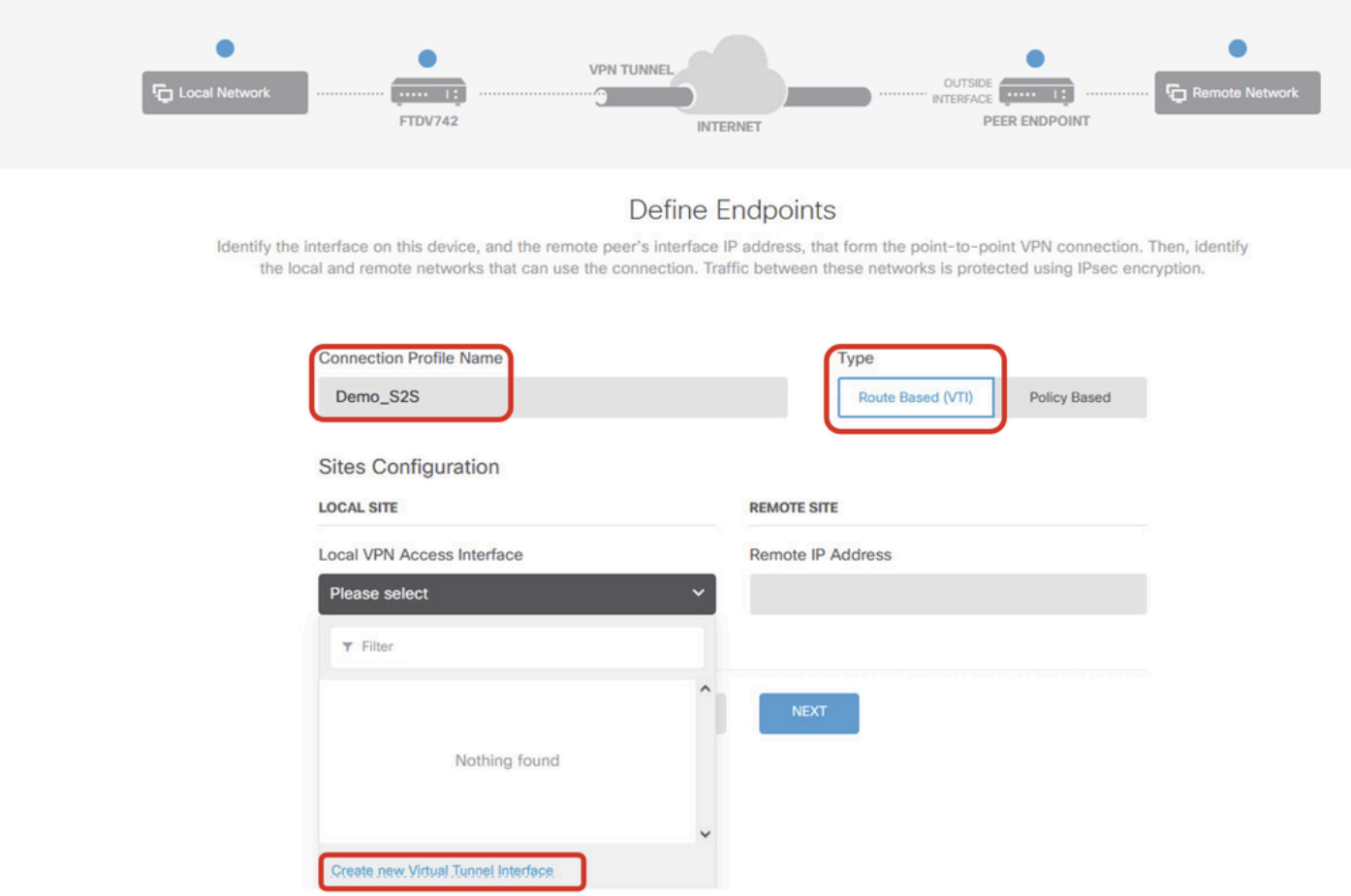
3.4단계. 새 Site-to-Site VPN 생성을 시작합니다. 을 클릭합니다.**CREATE SITE-TO-SITE CONNECTION**



Create_Site-Site_Connection

3.5단계. 필요한 정보를 제공합니다.

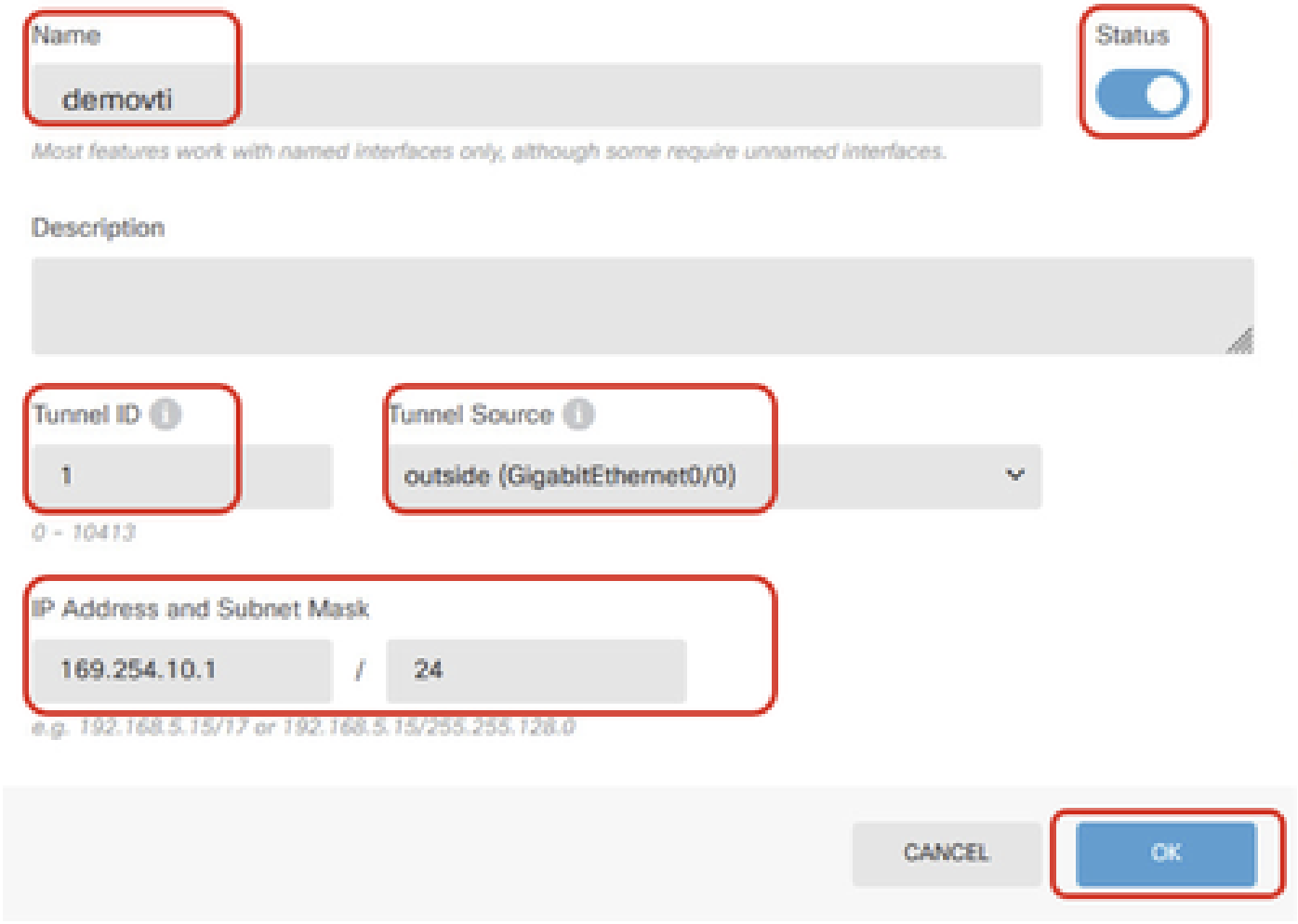
- 연결 프로파일 이름: Demo_S2S
- 유형: 경로 기반(VTI)
- Local VPN Access Interface(로컬 VPN 액세스 인터페이스): 드롭다운 목록을 클릭한 다음 을 **Create new Virtual Tunnel Interface** 클릭합니다.



Create_VTI_in_VPN_마법사

3.6단계. 새 VTI를 생성하기 위해 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

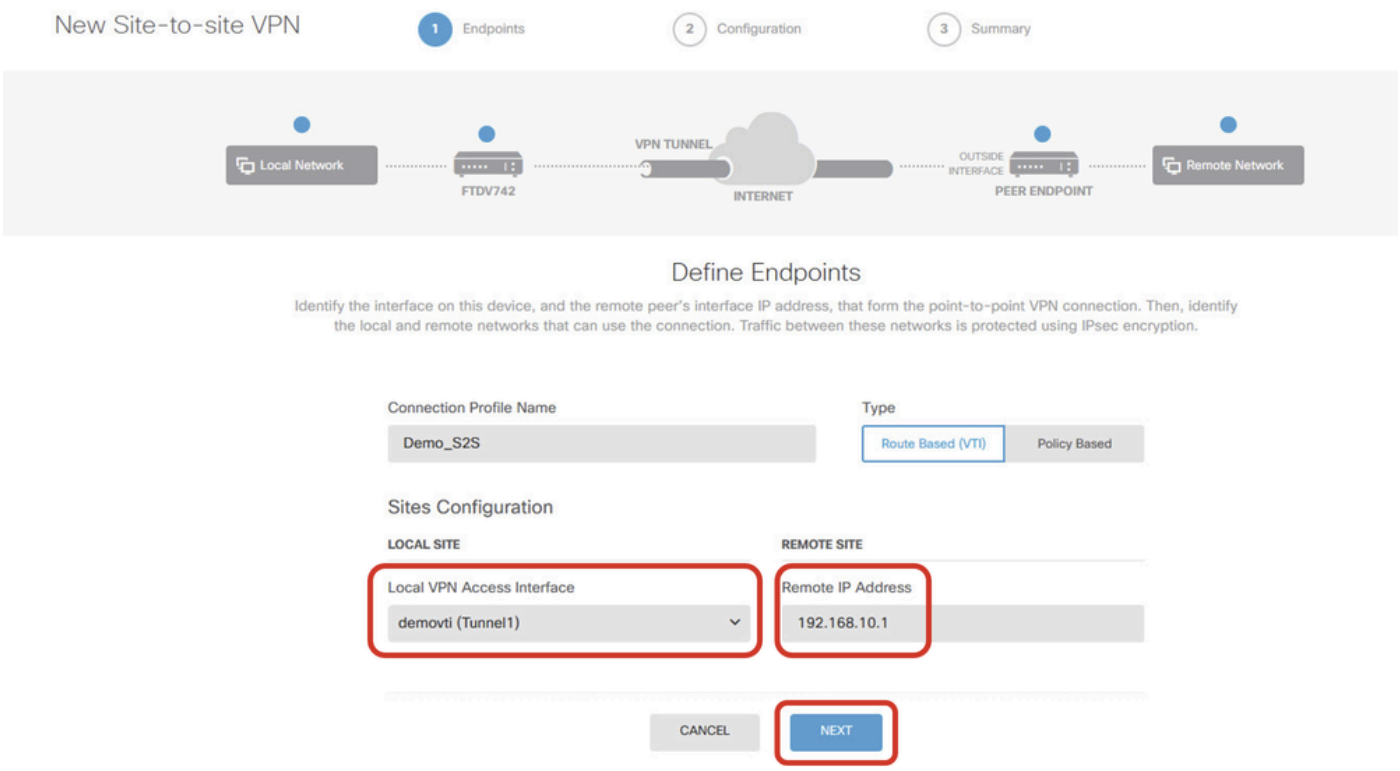
- Name(이름): demovti
- 터널 ID: 1
- 터널 소스: 외부(GigabitEthernet0/0)
- IP 주소 및 서브넷 마스크: 169.254.10.1/24
- 상태: Enabled(활성) 위치에 있는 슬라이더를 클릭합니다.



VTI_세부 정보 생성

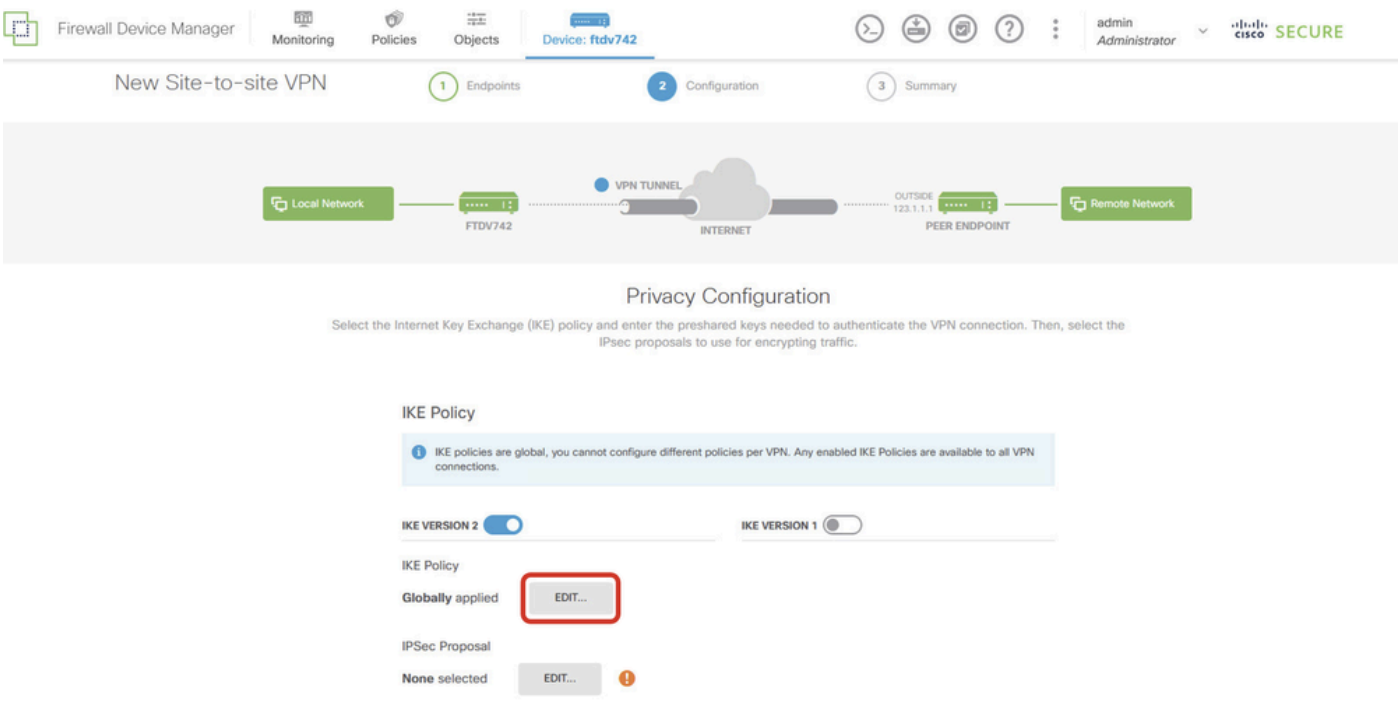
3.7단계. 필요한 정보를 계속 제공합니다. NEXT (다음) 버튼을 클릭합니다.

- 로컬 VPN 액세스 인터페이스: demovti(3.6단계에서 생성됨)
- 원격 IP 주소: 192.168.10.1



VPN_Wizard_Endpoint_Step1

3.8단계. IKE Policy(IKE 정책)로 이동합니다. EDIT(편집) 버튼을 클릭합니다.



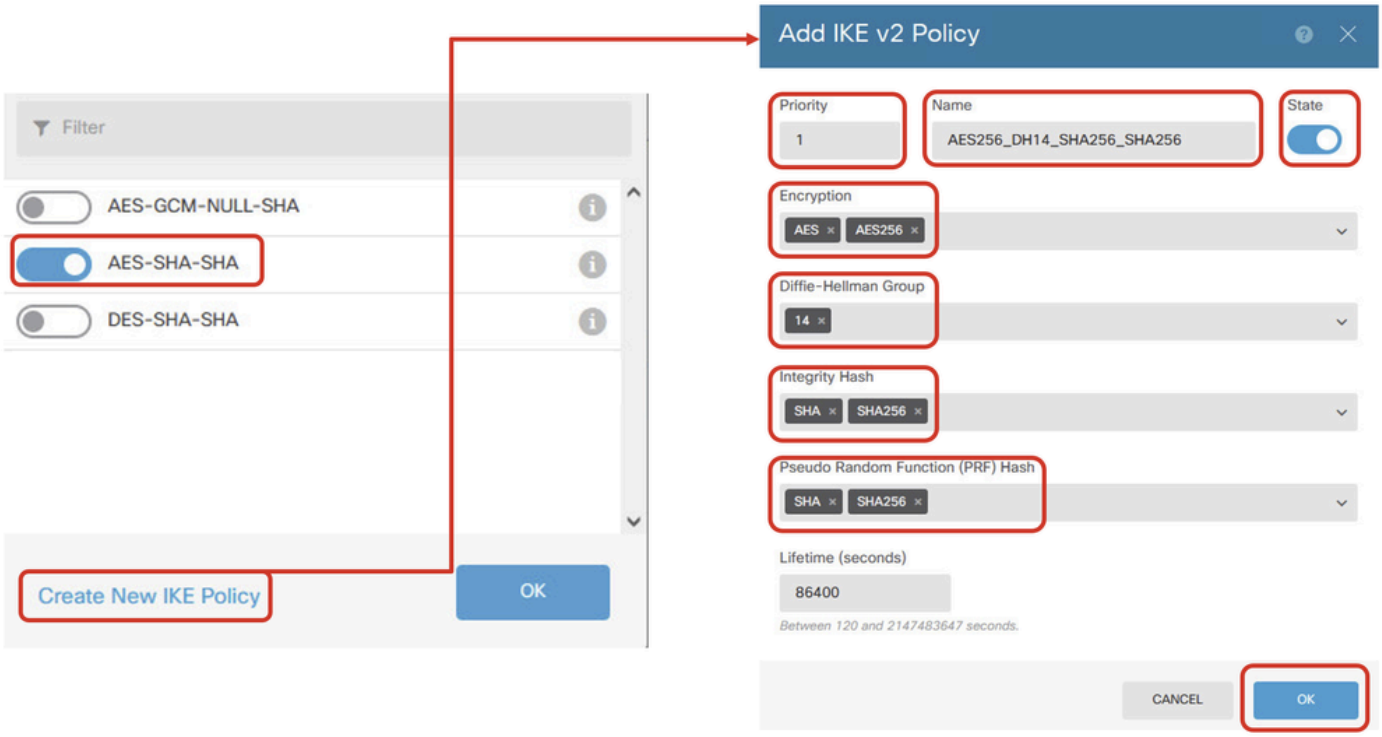
정책 수정(_I)

3.9단계. IKE 정책의 경우 미리 정의된 정책을 사용하거나 Create New IKE Policy(새 IKE 정책 생성)를 클릭하여 새 정책을 생성할 수 있습니다.

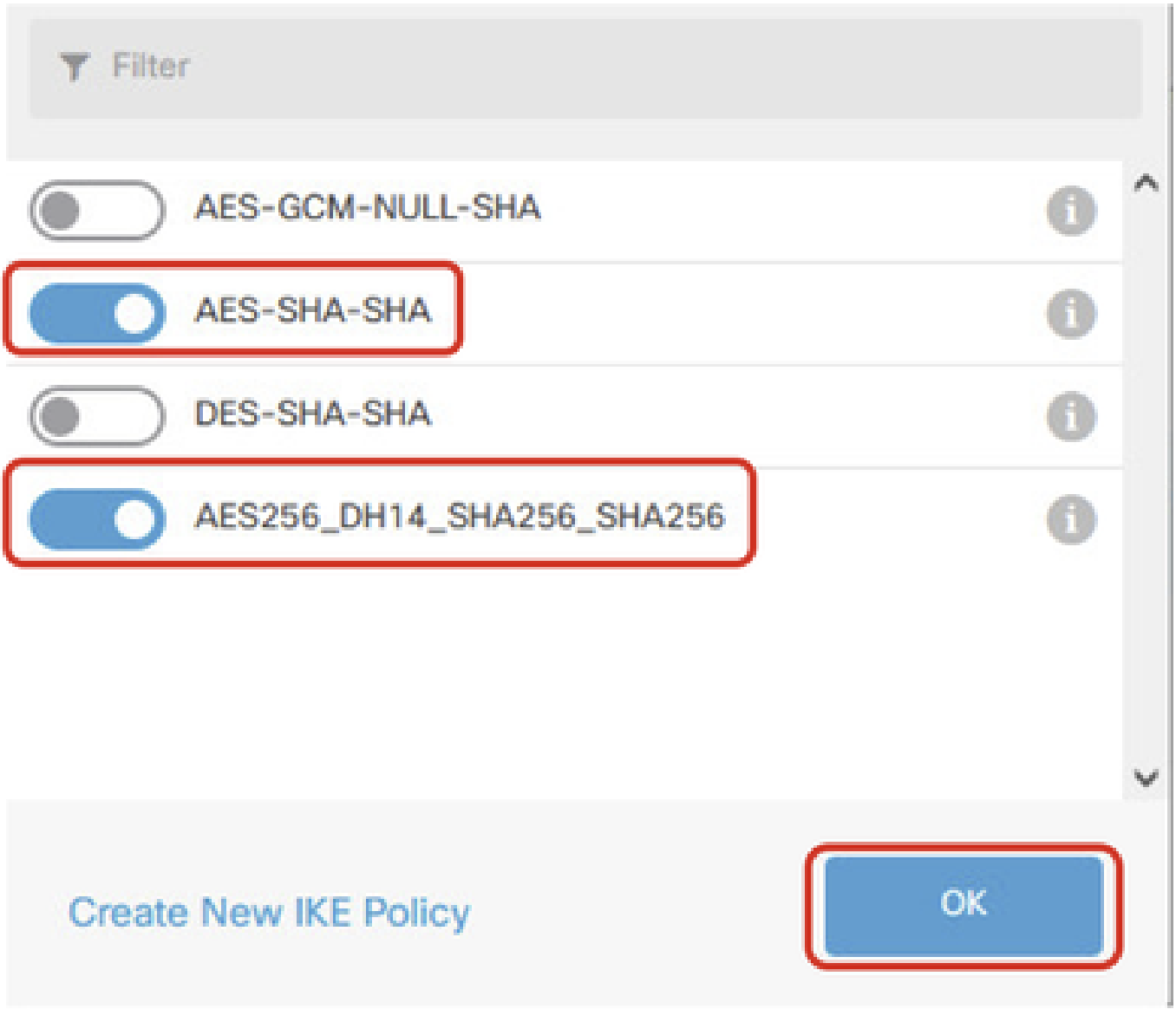
이 예에서는 기존 IKE 정책 AES-SHA-SHA를 토글하고 데모용으로 새 정책을 생성합니다. 저장하

려면 OK 버튼을 클릭합니다.

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

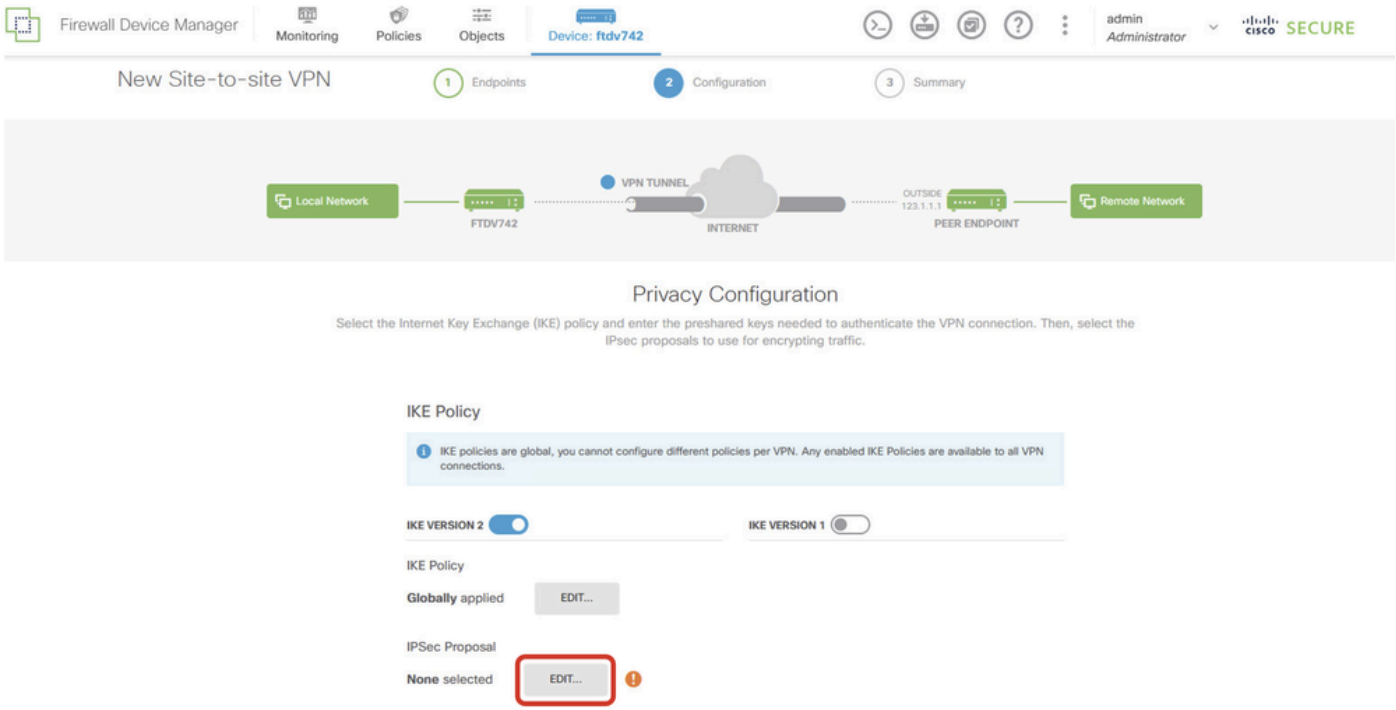


추가_새_IKE_정책



Enable_New_IKE_Policy

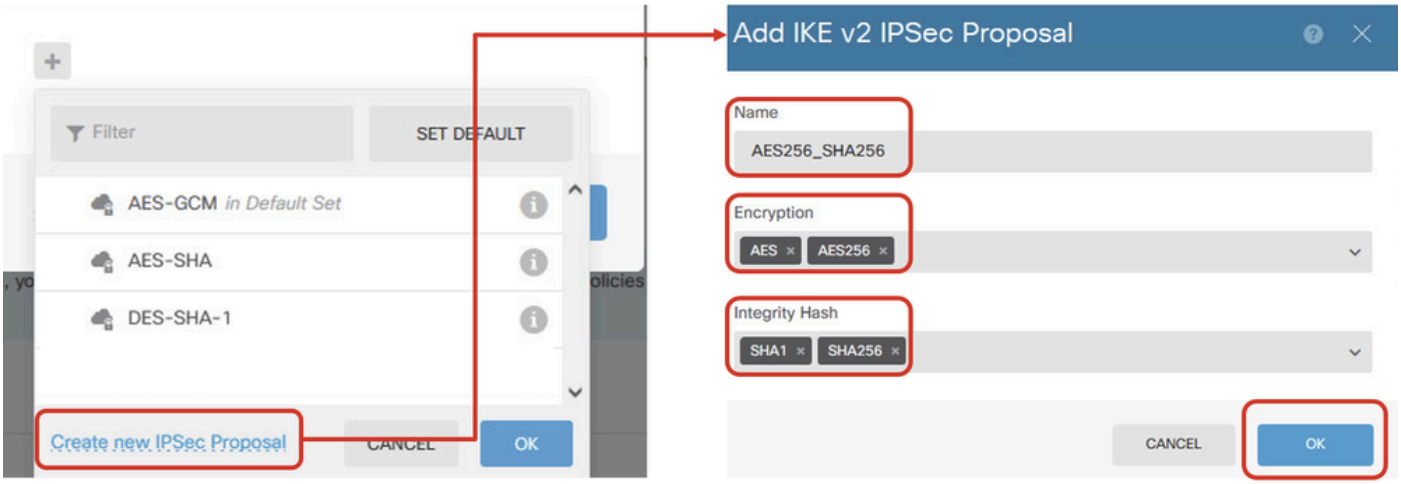
3.10단계. IPSec 제안으로 이동합니다. EDIT(편집) 버튼을 클릭합니다.



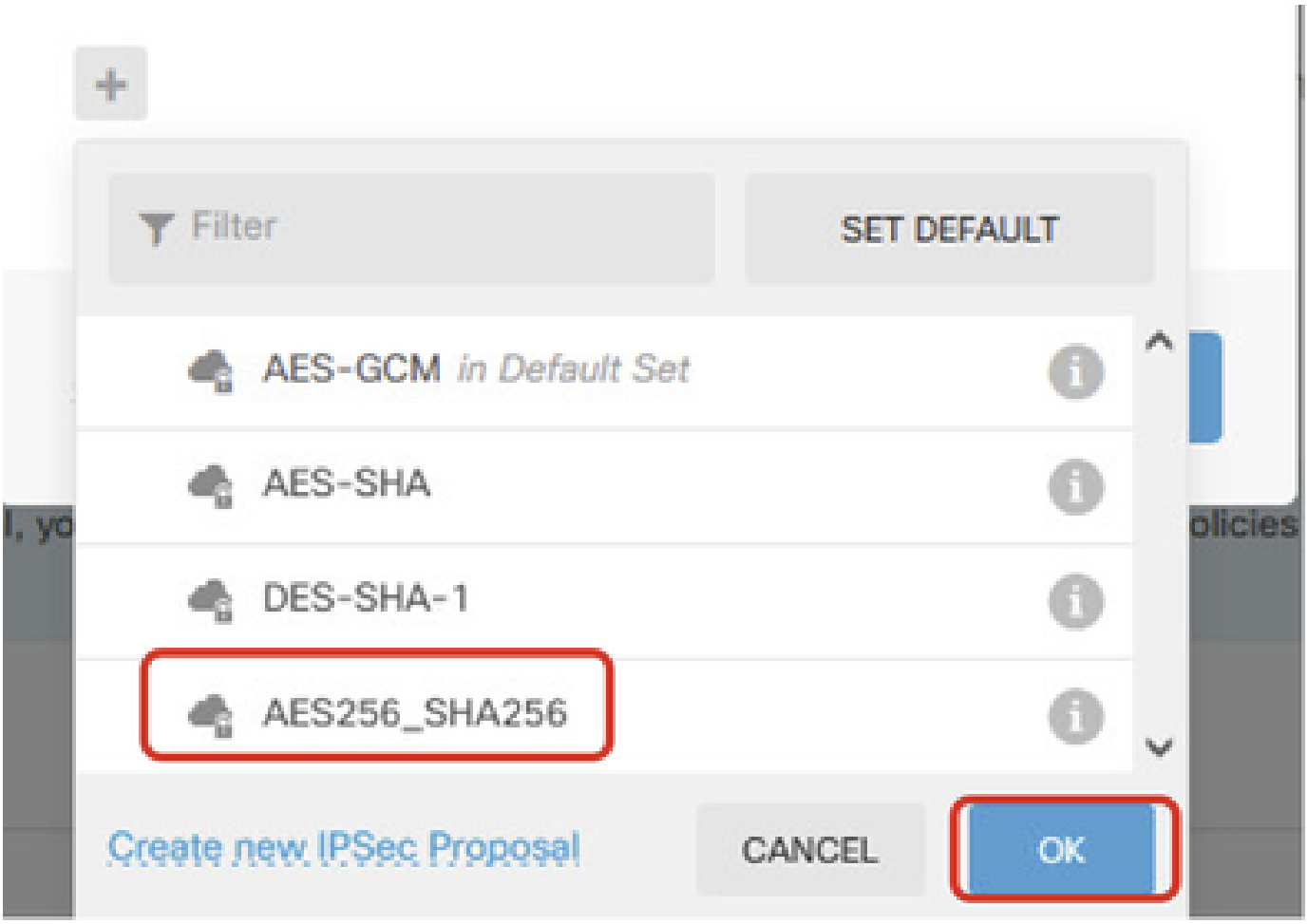
Edit_IKE_제안

3.11단계. IPSec 제안의 경우 미리 정의된 IPSec을 사용하거나 Create new IPSec Proposal(새 IPSec 제안 생성)을 클릭하여 새 제안서를 생성할 수 있습니다. 이 예에서는 데모용으로 새 버전을 만듭니다. 필요한 정보를 제공합니다. 저장하려면 OK 버튼을 클릭합니다.

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



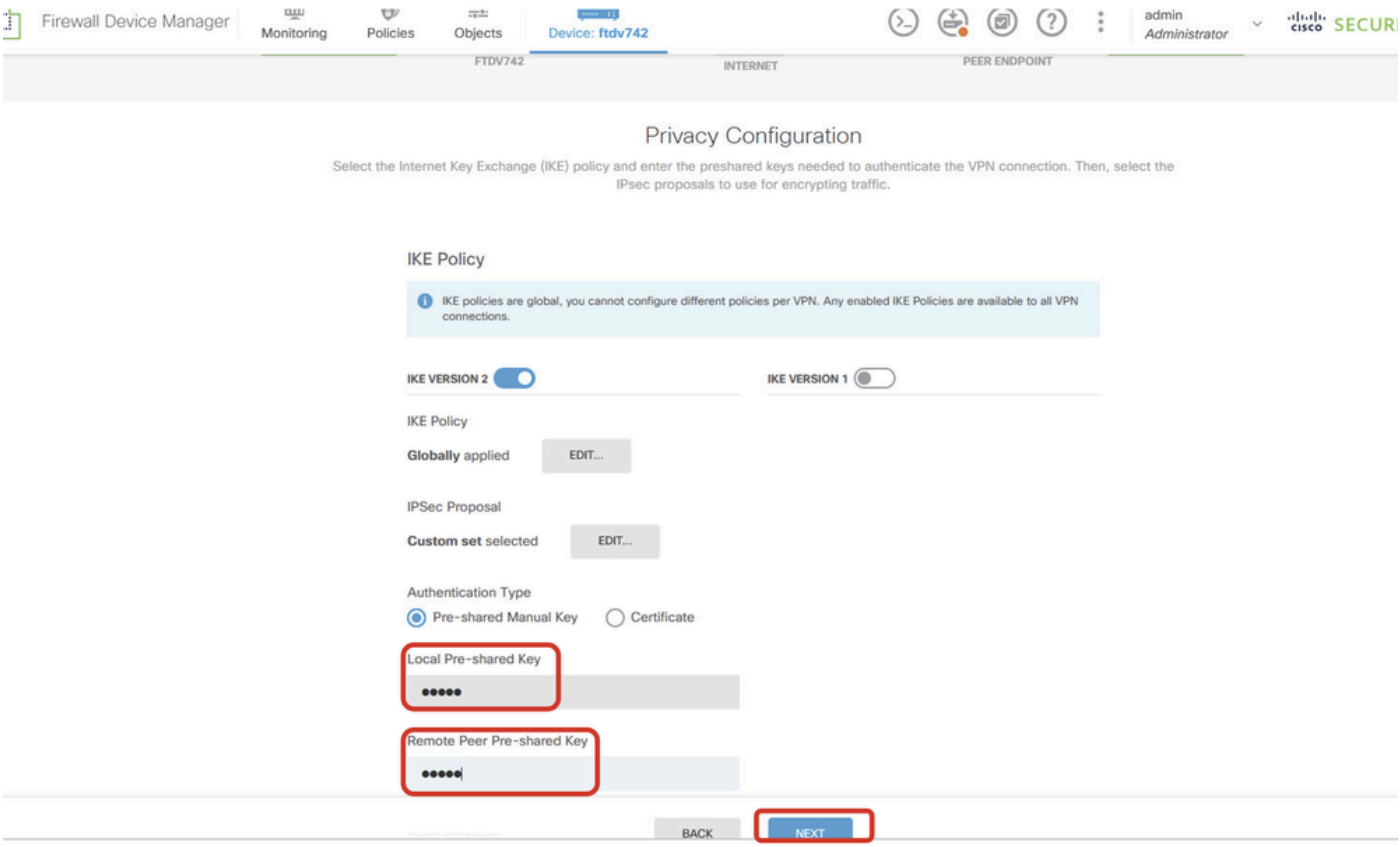
Add_New_IPSec_Proposal



Enable_New_IPSec_Proposal

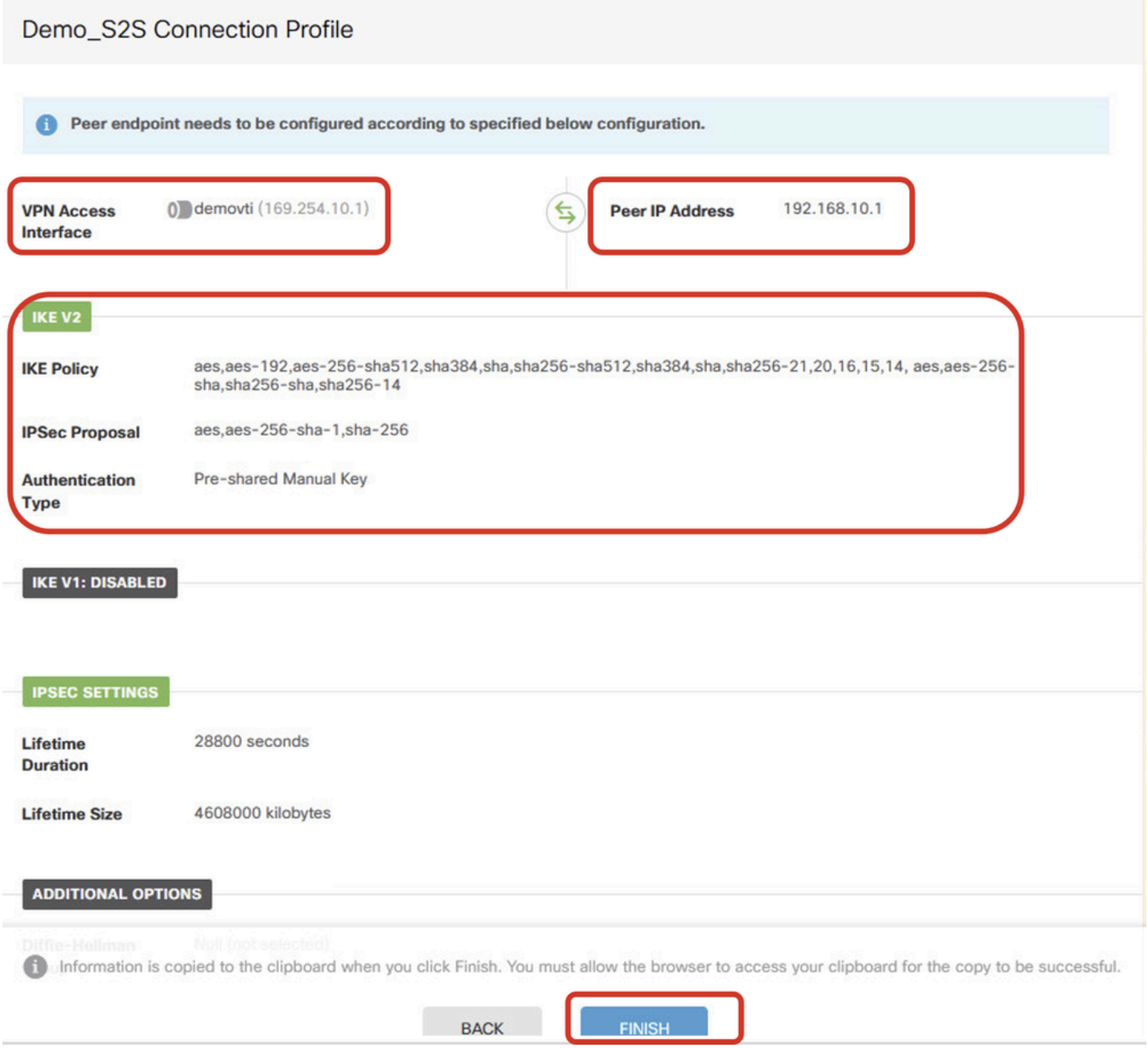
3.12단계. 사전 공유 키를 구성합니다. NEXT(다음) 버튼을 클릭합니다.

이 사전 공유 키를 기록해 두고 나중에 Site2 FTD에서 구성합니다.



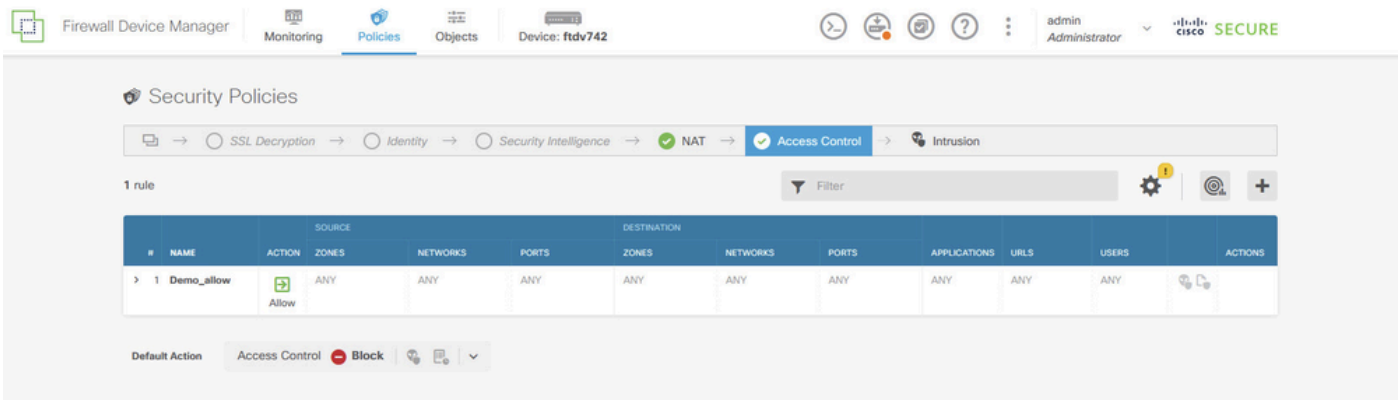
Configure_Pre_Shared_Key

3.13단계. VPN 컨피그레이션을 검토합니다. 수정해야 할 사항이 있으면 BACK(뒤로) 버튼을 클릭합니다. 모든 것이 정상인 경우 FINISH(마침) 버튼을 클릭합니다.



VPN_Wizard_Complete

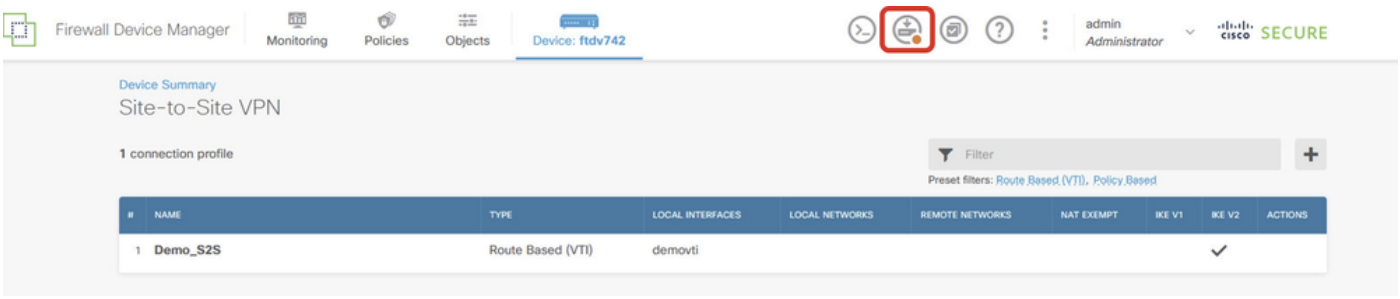
3.14단계. 트래픽이 FTD를 통과하도록 허용하는 액세스 제어 규칙을 생성합니다. 이 예에서는 데모용으로 모두 허용합니다. 실제 요구 사항에 따라 정책을 수정합니다.



액세스 제어 규칙 예

3.15단계(선택 사항) 인터넷에 액세스하기 위해 클라이언트에 대해 동적 NAT가 구성된 경우 FTD에서 클라이언트 트래픽에 대한 NAT 제외 규칙을 구성합니다. 이 예에서는 각 FTD에 동적 NAT가 구성되어 있지 않으므로 NAT-exempt 규칙을 구성할 필요가 없습니다.

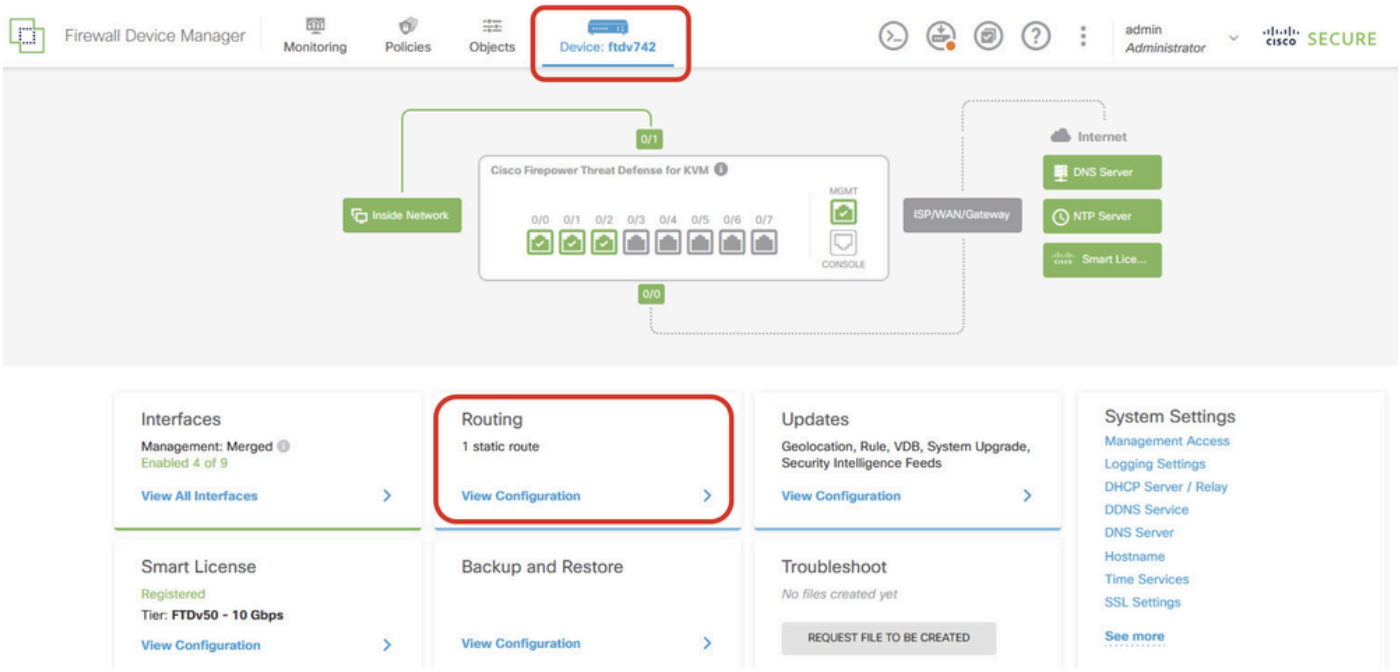
3.16단계. 컨피그레이션 변경 사항을 구축합니다.



구축_VPN_구성

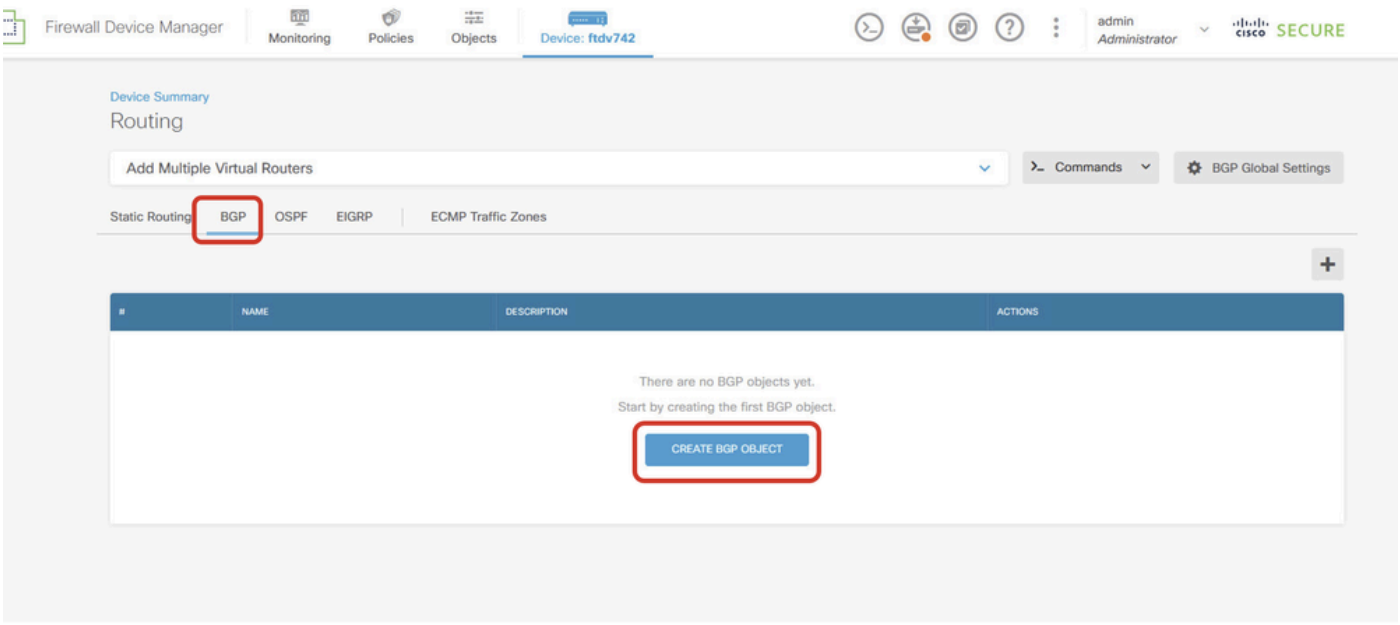
BGP의 컨피그레이션

4단계. Device(디바이스) > Routing(라우팅)으로 이동합니다. View Configuration(컨피그레이션 보기)을 클릭합니다.



보기_라우팅_구성

5단계. BGP 탭을 클릭한 다음 CREATE BGP OBJECT(BGP 개체 생성)를 클릭합니다.



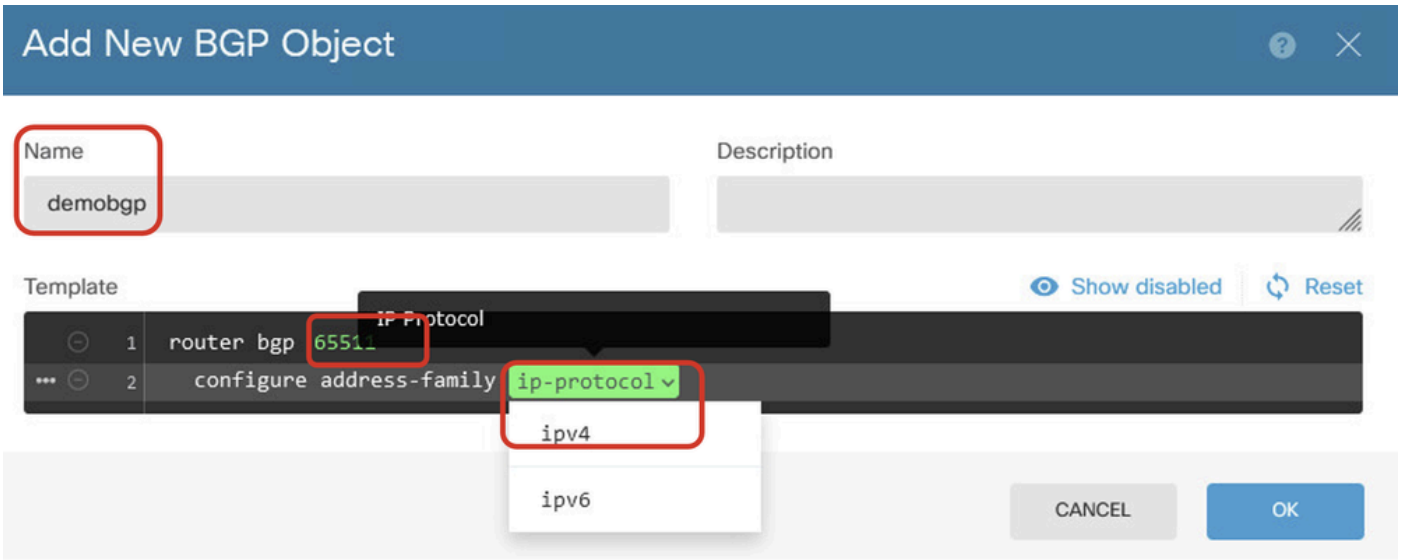
Create_BGP_Object

6단계. 객체의 이름을 제공합니다. Template(템플릿)으로 이동하여 구성합니다. 저장하려면 OK 버튼을 클릭합니다.

Name(이름): demobgp

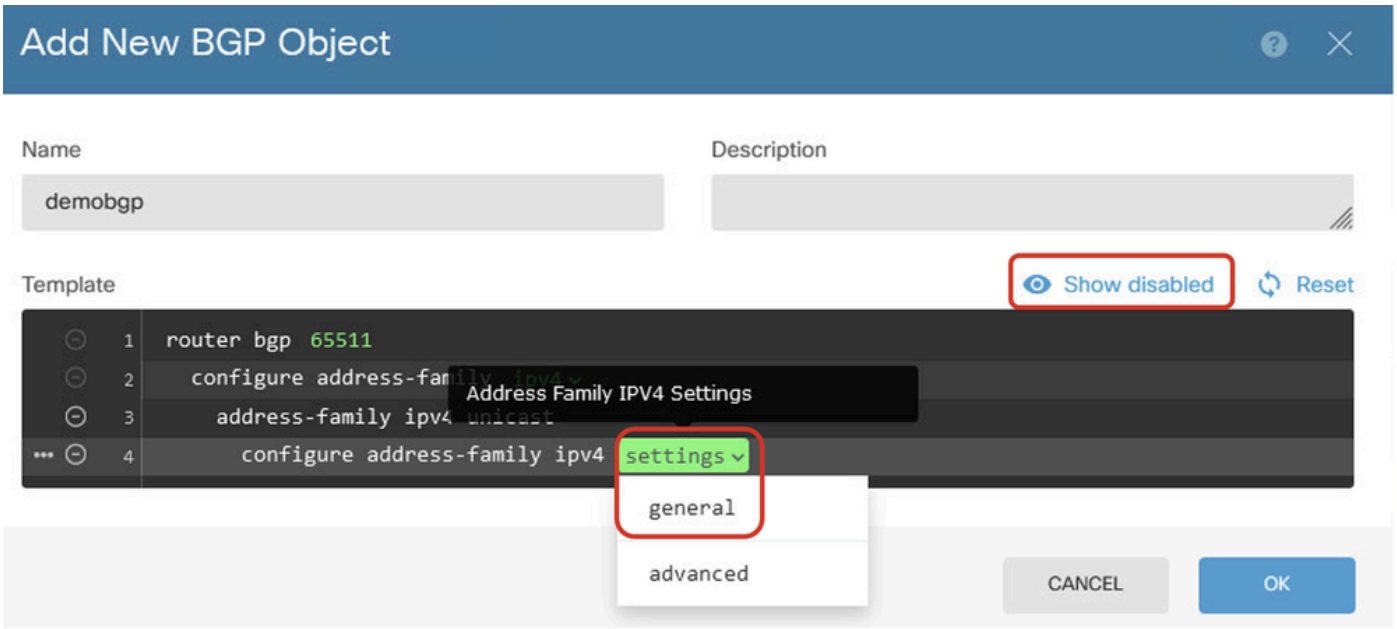
행 1: AS 번호를 구성합니다. as-number를 클릭합니다. 로컬 AS 번호를 수동으로 입력합니다. 이 예에서는 Site1 FTD에 대해 AS 번호가 65511.

행 2: IP 프로토콜을 구성합니다. ip-protocol을 클릭합니다. ipv4를 선택합니다.



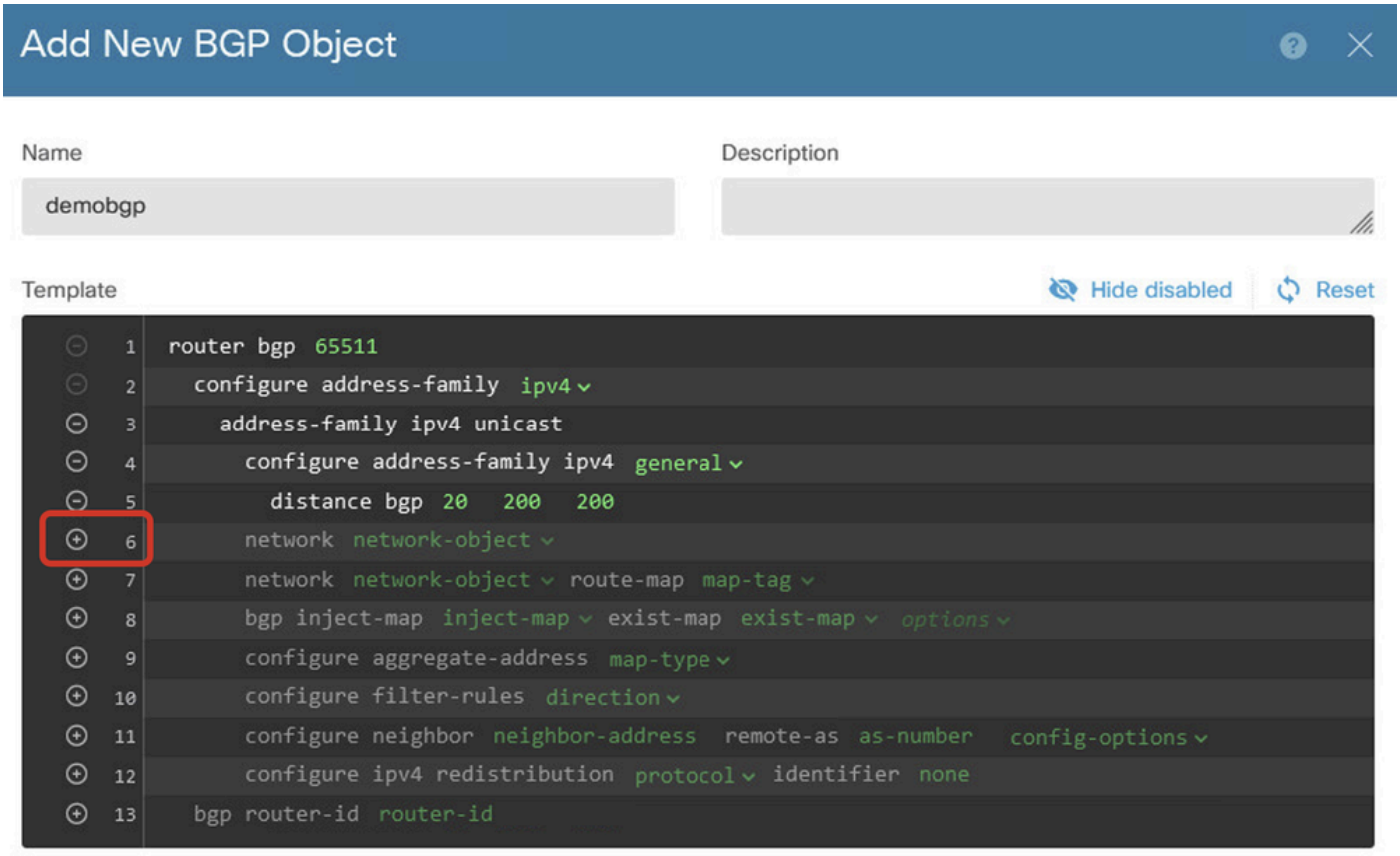
Create_BGP_Object_ASNumber_Protocol

행 4: 추가 설정을 구성합니다. Settings(설정)를 클릭하고 general(일반)을 선택한 다음 Show disabled(비활성 표시)를 클릭합니다.

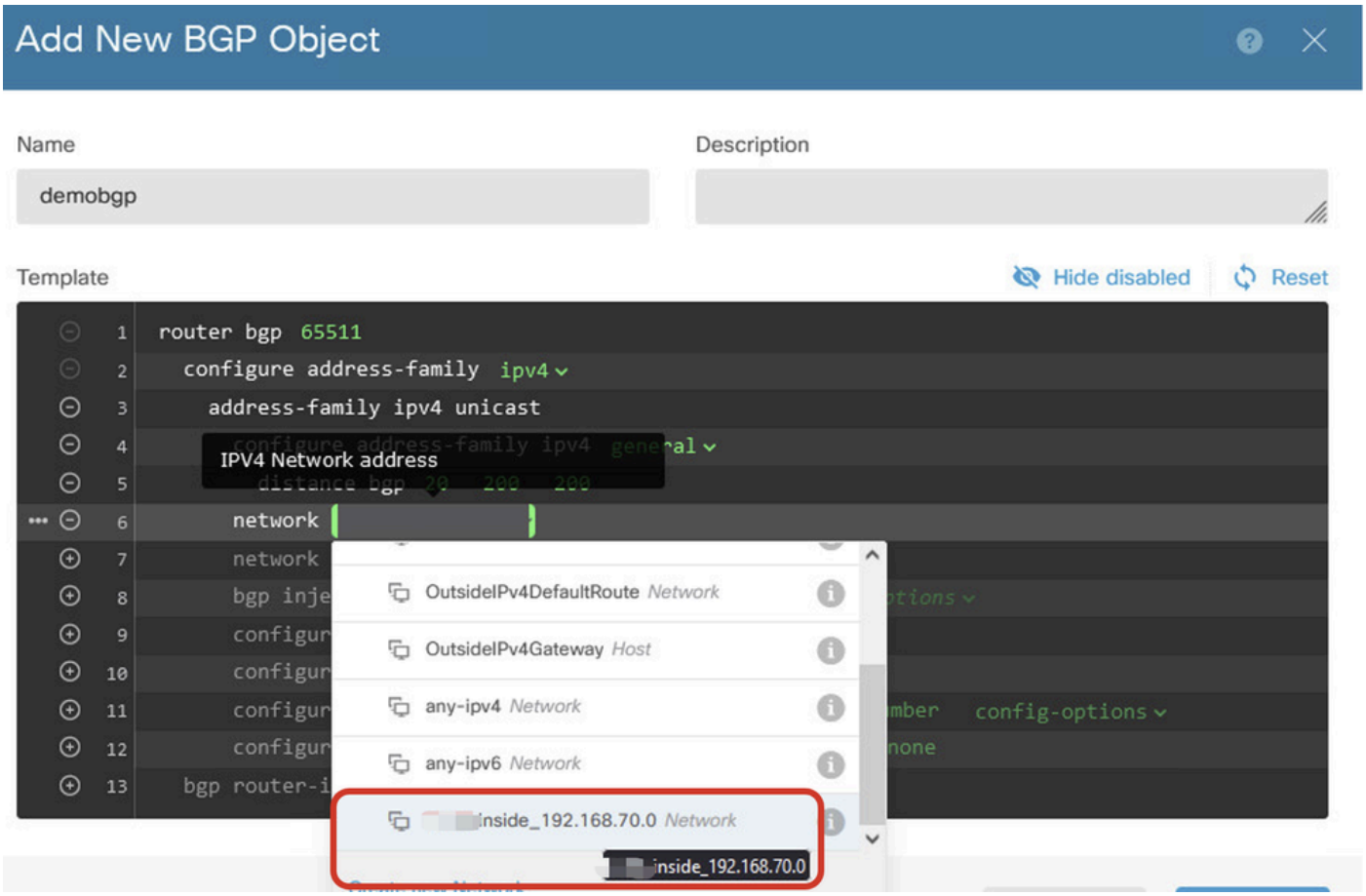


BGP_Object_AddressSetting 생성

행 6: BGP 네트워크를 구성하기 위해 행을 활성화하려면 + 아이콘을 클릭합니다. network-object를 클릭합니다. 사용 가능한 기존 객체를 보고 선택할 수 있습니다. 이 예에서는 inside_192.168.70.0(3.2단계에서 생성됨) 객체 이름을 선택합니다.

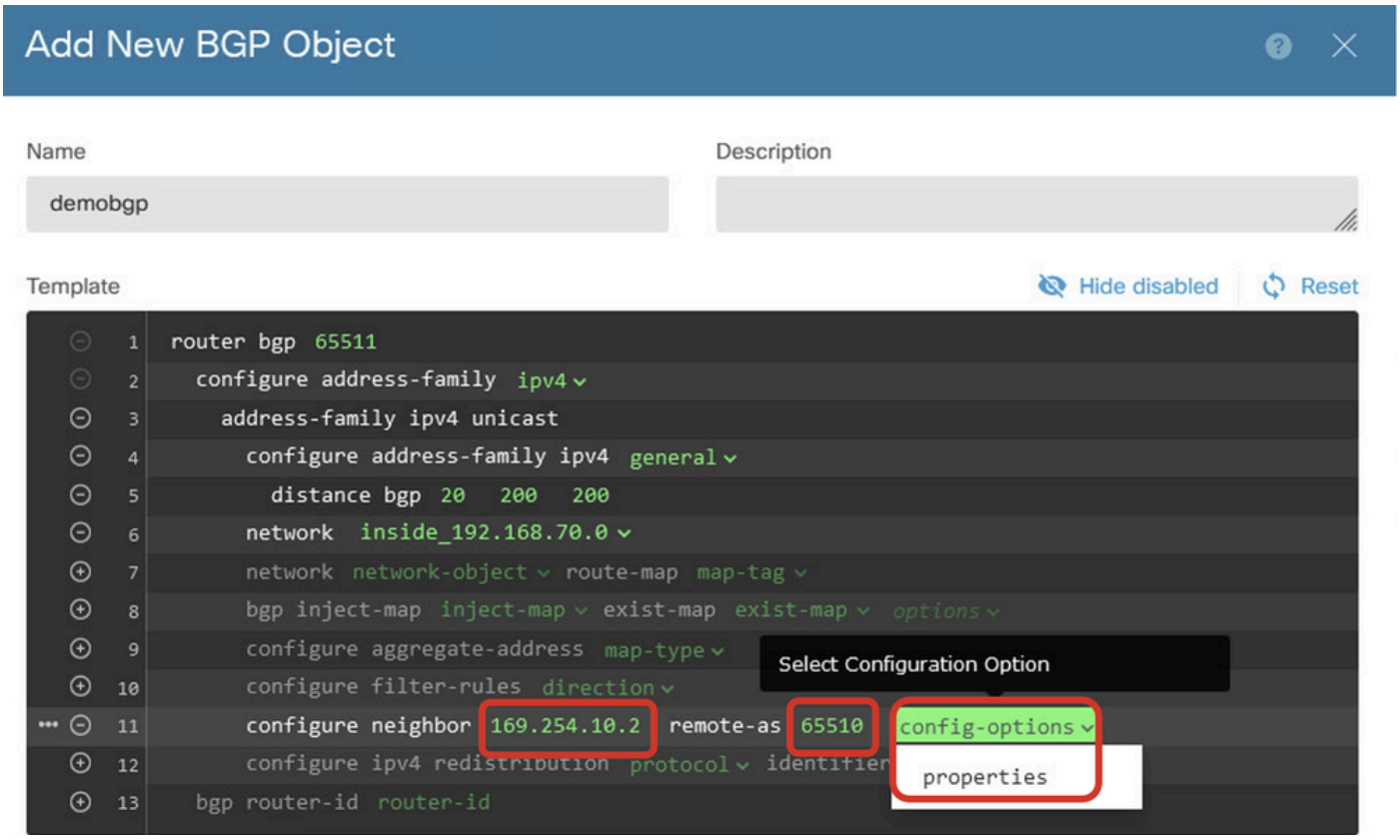


Create_BGP_Object_Add_Network



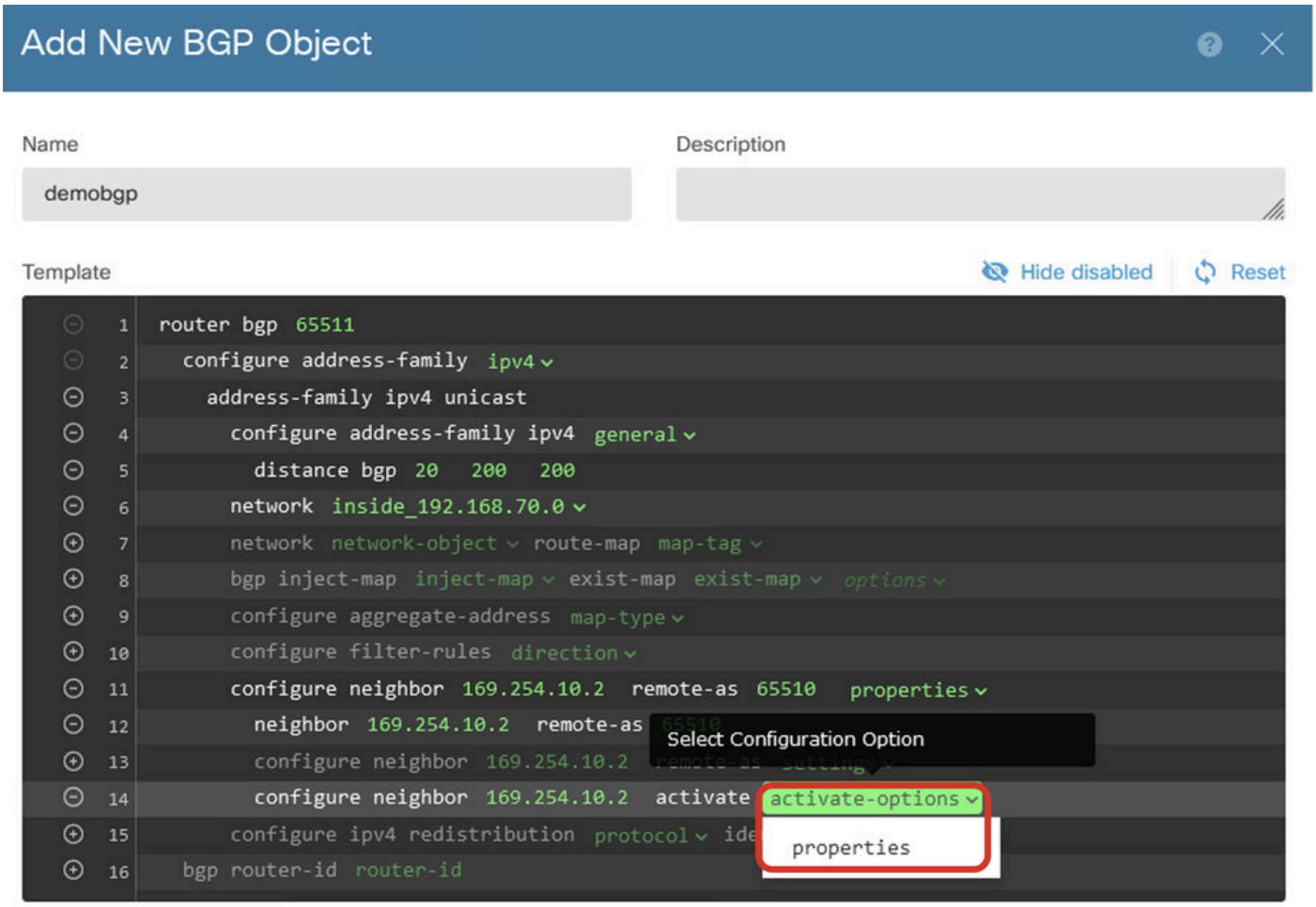
Create_BGP_Object_Add_Network2

행 11: BGP 네이버 관련 정보를 구성하도록 행을 활성화하려면 + 아이콘을 클릭합니다. neighbor-address를 클릭하고 피어 BGP 인접 디바이스 주소를 수동으로 입력합니다. 이 예에서는 169.254.10.2(Site2 FTD의 VTI IP 주소)입니다. as-number를 클릭하고 피어 AS 번호를 수동으로 입력합니다. 이 예에서65510 Site2 FTD를 위한 것입니다. config-options를 클릭하고 properties를 선택합니다.



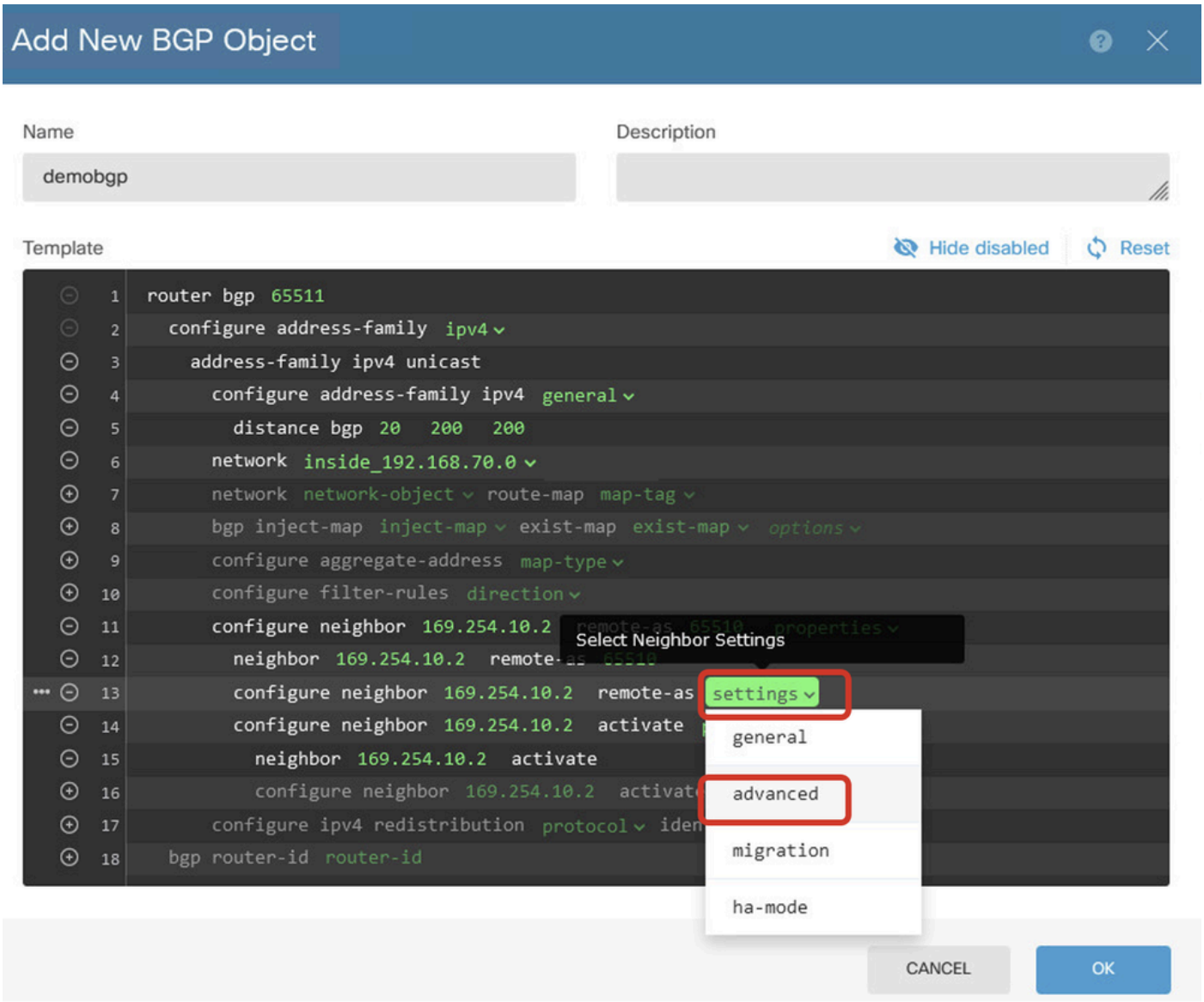
Create_BGP_Object_NeighborSetting

행 14: 인접 디바이스의 일부 속성을 구성하도록 라인을 활성화하려면 + 아이콘을 클릭합니다. activate-options를 클릭하고 properties를 선택합니다.



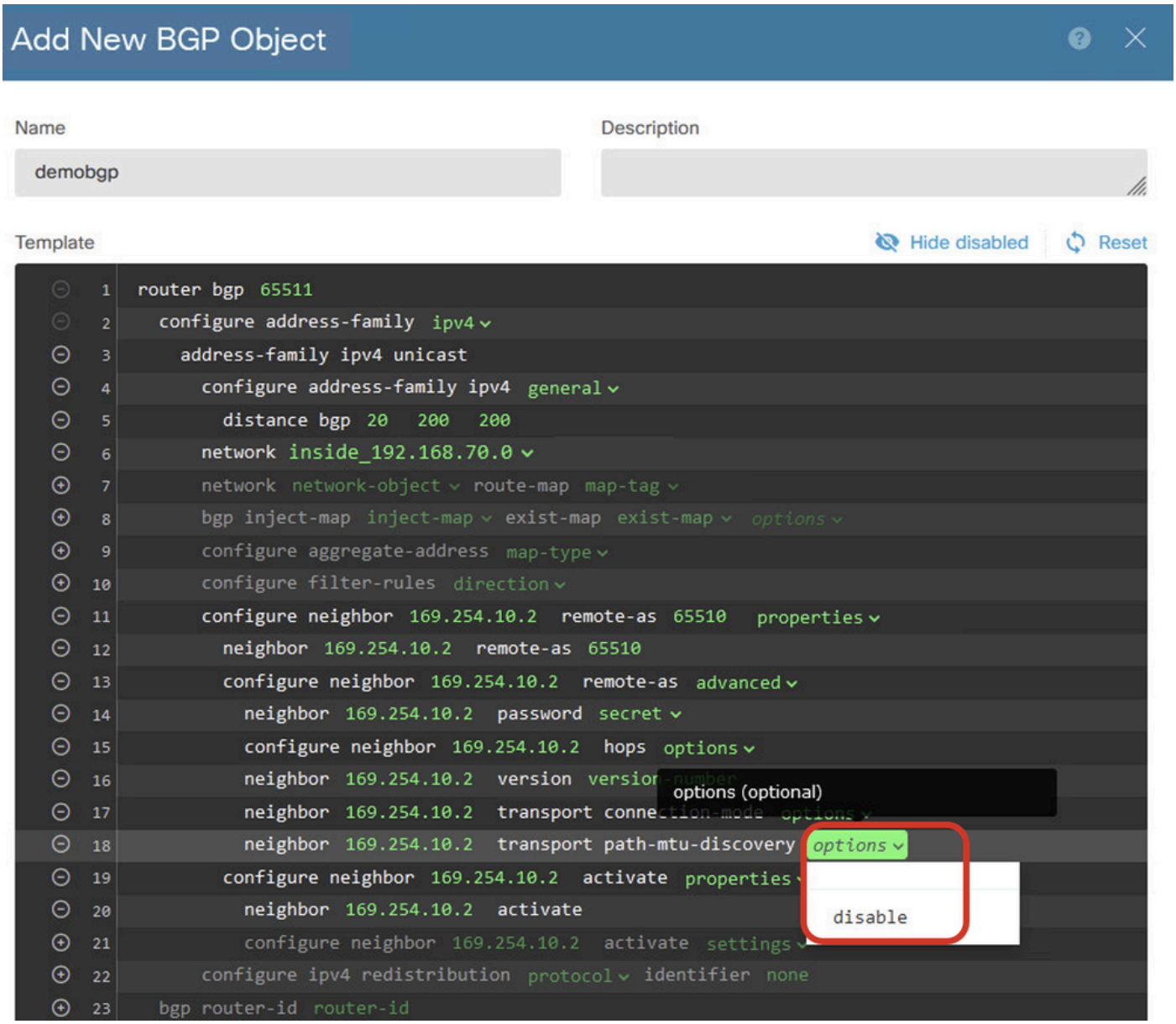
Create_BGP_Object_NeighborSetting_Properties

행 13: + 아이콘을 클릭하여 고급 옵션을 표시하도록 행을 활성화합니다. 설정을 클릭하고 고급을 선택합니다.



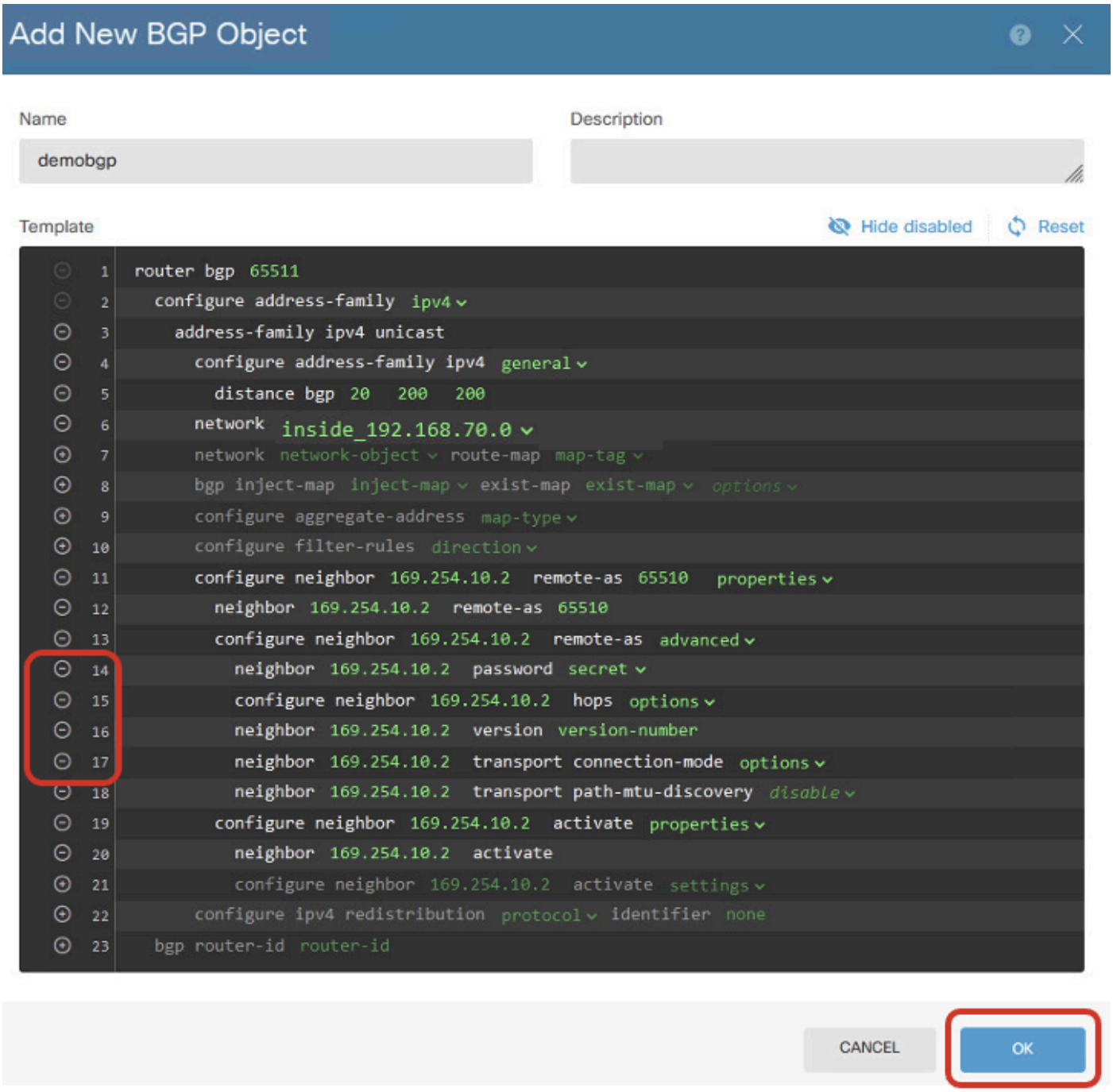
Create_BGP_Object_NeighborSetting_Properties_Advanced

행 18: 경로 MTU 검색을 비활성화하려면 옵션을 클릭하고 비활성화를 선택합니다.



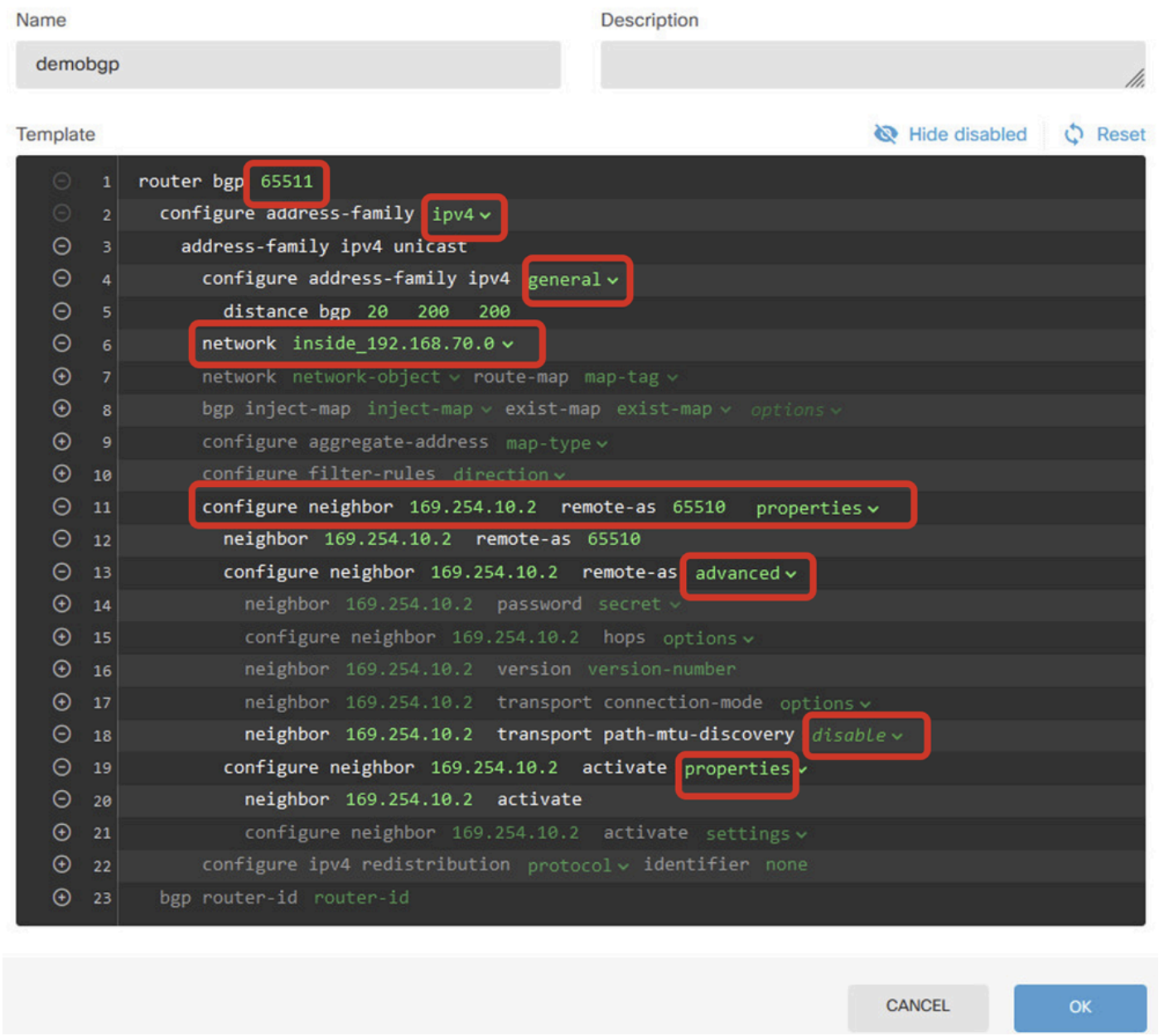
Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

행 14, 15, 16, 17: 라인을 비활성화하려면 - 버튼을 클릭합니다. 그런 다음 OK(확인) 버튼을 클릭하여 BGP 객체를 저장합니다.



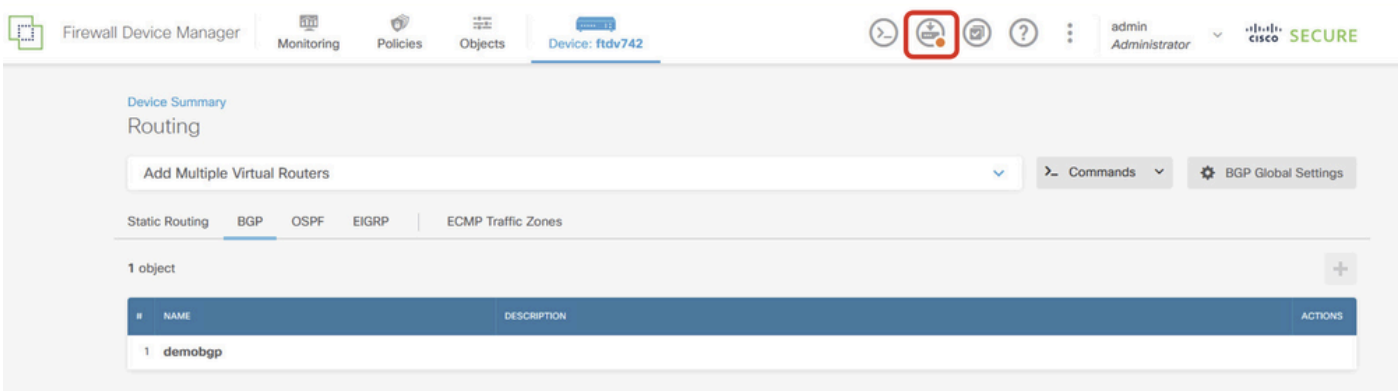
Create_BGP_Object_DisableLines

이 예에서는 BGP 설정에 대한 개요입니다. 실제 요구 사항에 따라 다른 BGP 설정을 구성할 수 있습니다.



BGP_Object_Final_Overview 생성

7단계. BGP 컨피그레이션 변경 사항을 구축합니다.



Deploy_BGP_Configuration

8단계. 이제 Site1 FTD에 대한 컨피그레이션이 완료되었습니다.

Site2 FTD VPN 및 BGP를 구성하려면 Site2 FTD의 해당 매개변수를 사용하여 3~7단계를 반복합니다.

CLI에서 Site1 FTD 및 Site2 FTD의 구성 개요

사이트 1 FTD	사이트 2 FTD
NGFW 버전 7.4.2 인터페이스 GigabitEthernet0/0 nameif 외부 cts 설명서 propagate sgt preserve-untag policy static sgt disabled trusted 보안 수준 0 ip 주소 192.168.30.1 255.255.255.0 인터페이스 GigabitEthernet0/2 nameif 내부 보안 수준 0 ip 주소 192.168.70.1 255.255.255.0 인터페이스 터널 1 nameif demvti ip 주소 169.254.10.1 255.255.255.0 터널 소스 인터페이스 외부 터널 대상 192.168.10.1 터널 모드 ipsec ipv4 터널 보호 ipsec 프로필 ipsec_profile|e4084d322d 개체 네트워크 외부IPv4게이트웨이 호스트 192.168.30.3 object network inside_192.168.70.0 서브넷 192.168.70.0 255.255.255.0 액세스 그룹 NGFW_ONBOX_ACL 전역 access-list NGFW_ONBOX_ACL remark rule-id 268435457: 액세스 정책: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule 액세스 목록 NGFW_ONBOX_ACL 고급 신뢰 개체 그룹 |acSvcg-268435457 ifc 내부 모든 규칙 ID 외부 모든 ifc 268435457 이벤트 로그 모두 access-list NGFW_ONBOX_ACL remark rule-id 268435458: 액세스 정책: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458:	NGFW 버전 7.4.2 인터페이스 GigabitEthernet0/0 nameif 외부 cts 설명서 propagate sgt preserve-untag policy static sgt disabled trusted 보안 수준 0 ip 주소 192.168.10.1 255.255.255.0 인터페이스 GigabitEthernet0/2 nameif 내부 보안 수준 0 ip 주소 192.168.50.1 255.255.255.0 인터페이스 터널 1 nameif devti25 ip 주소 169.254.10.2 255.255.255.0 터널 소스 인터페이스 외부 터널 대상 192.168.30.1 터널 모드 ipsec ipv4 터널 보호 ipsec 프로필 ipsec_profile|e4084d322d 개체 네트워크 외부IPv4게이트웨이 호스트 192.168.10.3 object network inside_192.168.50.0 서브넷 192.168.50.0 255.255.255.0 액세스 그룹 NGFW_ONBOX_ACL 전역 access-list NGFW_ONBOX_ACL remark rule-id 268435457: 액세스 정책: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule 액세스 목록 NGFW_ONBOX_ACL 고급 신뢰 개체 그룹 |acSvcg-268435457 ifc 내부 모든 규칙 ID 외부 모든 ifc 268435457 이벤트 로그 모두 access-list NGFW_ONBOX_ACL remark rule-id 268435458: 액세스 정책: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow

L5 RULE: Demo_allow 액세스 목록 NGFW_ONBOX_ACL 고급 허용 개체 그룹 |acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: 액세스 정책: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any rule-id 1 라우터 bgp 65511 bgp 로그 인접 디바이스 변경 bgp router-id vrf auto-assign 주소군 ipv4 유니캐스트 neighbor 169.254.10.2 remote-as 65510 네이버 169.254.10.2 전송 경로 mtu 검색 비활성화 네이버 169.254.10.2 활성화 네트워크 192.168.70.0 자동 요약 없음 동기화 안 함 출구 주소군 경로 외부 0.0.0.0 0.0.0 192.168.30.3 1 crypto ipsec ikev2 ipsec-proposal AES256_SHA256 프로토콜 esp 암호화 aes-256 aes 프로토콜 esp 무결성 sha-256 sha-1 암호화 ipsec 프로필 ipsec_profile|e4084d322d ikev2 ipsec-proposal AES256_SHA256 설정 보안 연결 수명 킬로바이트 4608000 설정 security-association lifetime seconds 28800 설정 암호화 ipsec 보안 연결 pmtu-에이징 무한 crypto ikev2 정책 1 암호화 aes-256 aes 무결성 sha256 sha 그룹 14 prf sha256 sha 수명 초 86400 crypto ikev2 정책 20 암호화 aes-256 aes-192 aes 무결성 sha512 sha384 sha256 sha 그룹 21 20 16 15 14	액세스 목록 NGFW_ONBOX_ACL 고급 허용 개체 그룹 |acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: 액세스 정책: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any rule-id 1 라우터 bgp 65510 bgp 로그 인접 디바이스 변경 bgp router-id vrf auto-assign 주소군 ipv4 유니캐스트 neighbor 169.254.10.1 remote-as 65511 네이버 169.254.10.1 전송 경로 mtu 검색 비활성화 네이버 169.254.10.1 활성화 네트워크 192.168.50.0 자동 요약 없음 동기화 안 함 출구 주소군 경로 외부 0.0.0.0 0.0.0 192.168.10.3 1 crypto ipsec ikev2 ipsec-proposal AES256_SHA256 프로토콜 esp 암호화 aes-256 aes 프로토콜 esp 무결성 sha-256 sha-1 암호화 ipsec 프로필 ipsec_profile|e4084d322d ikev2 ipsec-proposal AES256_SHA256 설정 보안 연결 수명 킬로바이트 4608000 설정 security-association lifetime seconds 28800 설정 암호화 ipsec 보안 연결 pmtu-에이징 무한 crypto ikev2 정책 1 암호화 aes-256 aes 무결성 sha256 sha 그룹 14 prf sha256 sha 수명 초 86400 crypto ikev2 정책 20 암호화 aes-256 aes-192 aes 무결성 sha512 sha384 sha256 sha 그룹 21 20 16 15 14

prf sha512 sha384 sha256 sha 수명 초 86400 crypto ikev2 enable outside 그룹 정책 |s2sGP|192.168.10.1 내부 그룹 정책 |s2sGP|192.168.10.1 특성 vpn-tunnel-protocol ikev2 tunnel-group 192.168.10.1 type ipsec-l2l 터널 그룹 192.168.10.1 일반 특성 기본 그룹 정책 |s2sGP|192.168.10.1 터널 그룹 192.168.10.1 ipsec 특성 ikev2 원격 인증 사전 공유 키 ***** ikev2 로컬 인증 사전 공유 키 *****	prf sha512 sha384 sha256 sha 수명 초 86400 crypto ikev2 enable outside 그룹 정책 |s2sGP|192.168.30.1 내부 그룹 정책 |s2sGP|192.168.30.1 특성 vpn-tunnel-protocol ikev2 tunnel-group 192.168.30.1 type ipsec-l2l 터널 그룹 192.168.30.1 일반 특성 기본 그룹 정책 |s2sGP|192.168.30.1 터널 그룹 192.168.30.1 ipsec 특성 ikev2 원격 인증 사전 공유 키 ***** ikev2 로컬 인증 사전 공유 키 *****

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

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

사이트 1 FTD	사이트 2 FTD
ftdv742# show crypto ikev2 sa IKEv2 SA: Session-id:134, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id 로컬 원격 fvrf/ivrf 상태 역할 563984431 192.168.30.1/500 192.168.10.1/500 Global/Global READY RESPONSE 암호화: AES-CBC, 키 크기: 256, 해시: SHA256, DH Grp:14, 인증 기호: PSK, 인증 확인: PSK 수명/활성 시간: 86400/5145초 하위 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	ftdv742# show crypto ikev2 sa IKEv2 SA: Session-id:13, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id 로컬 원격 fvrf/ivrf 상태 역할 339797985 192.168.10.1/500 192.168.30.1/500 전역/전역 준비 개시자 암호화: AES-CBC, 키 크기: 256, 해시: SHA256, DH Grp:14, 인증 기호: PSK, 인증 확인: PSK 수명/활성 시간: 86400/74099초 하위 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 인/아웃: 0xb7b5b38b/0xf0c4239d

ESP spi in/out: 0xf0c4239d/0xb7b5b38b	
ftdv742# show crypto ipsec sa 인터페이스: demovti 암호화 맵 태그: __vti-crypto-map-Tunnel1-0-1, 시퀀스 번호: 65280, 로컬 주소: 192.168.30.1 보호된 vrf(ivrf): 전역 로컬 id(addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) 원격 id(addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1 #pkts 캡슐화: 5720, #pkts 암호화: 5720, #pkts 다이제스트: 5720 #pkts decaps: 5717, #pkts decrypt: 5717, #pkts verify: 5717 #pkts 압축: 0, 압축 #pkts: 0 #pkts 않음: 5720, #pkts 구성 요소 실패: 0, #pkts 압축 해제 실패: 0 #pre-frag 성공: 0, #pre-frag 실패: 0, #fragments 생성: 0 #PMTUs 전송: 0, #PMTUs rcvd: 0, #decapsulated reassembly가 필요한 frgs: 0 #TFC 수신: 0, #TFC: 0 #Valid ICMP 오류: 0, #Invalid ICMP 오류: 0 #send 오류: 0, #recv 오류: 0 로컬 암호화 종료: 192.168.30.1/500, 원격 암호화 종료: 192.168.10.1/500 경로 mtu 1500, ipsec 오버헤드 78(44), 미디어 mtu 1500 남은 PMTU 시간(초): 0, DF 정책: copy-df ICMP 오류 검증: 비활성화됨, TFC 패킷: 비활성화됨 현재 아웃바운드 spi: B7B5B38B 현재 인바운드 spi: F0C4239D 인바운드 esp sas: spi: 0xF0C4239D(4039386013) SA 상태: 활성 변환: esp-aes-256 esp-sha-256-hmac 압축 안 함 사용 설정 ={L2L, Tunnel, IKEv2, VTI, }	ftdv742# show crypto ipsec sa 인터페이스: demovti25 암호화 맵 태그: __vti-crypto-map-Tunnel1-0-1, 시퀀스 번호: 65280, 로컬 주소: 192.168.10.1 보호된 vrf(ivrf): 전역 로컬 id(addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) 원격 id(addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1 #pkts 캡슐화: 5721, #pkts 암호화: 5721, #pkts 다이제스트: 5721 #pkts decaps: 5721, #pkts decrypt: 5721, #pkts verify: 5721 #pkts 압축: 0, 압축 #pkts: 0 #pkts 않음: 5721, #pkts 구성 요소 실패: 0, #pkts 압축 해제 실패: 0 #pre-frag 성공: 0, #pre-frag 실패: 0, #fragments 생성: 0 #PMTUs 전송: 0, #PMTUs rcvd: 0, #decapsulated reassembly가 필요한 frgs: 0 #TFC 수신: 0, #TFC: 0 #Valid ICMP 오류: 0, #Invalid ICMP 오류: 0 #send 오류: 0, #recv 오류: 0 로컬 암호화 종료: 192.168.10.1/500, 원격 암호화 종료: 192.168.30.1/500 경로 mtu 1500, ipsec 오버헤드 78(44), 미디어 mtu 1500 남은 PMTU 시간(초): 0, DF 정책: copy-df ICMP 오류 검증: 비활성화됨, TFC 패킷: 비활성화됨 현재 아웃바운드 spi: F0C4239D 현재 인바운드 spi: B7B5B38B 인바운드 esp sas: spi: 0xB7B5B38B(3082138507) SA 상태: 활성 변환: esp-aes-256 esp-sha-256-hmac 압축 안 함 사용 설정 ={L2L, Tunnel, IKEv2, VTI, }

슬롯: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa 타이밍: 남은 키 수명(kB/초): (4285389/3722) IV 크기: 16바이트 재생 감지 지원: Y 재전송 방지 비트맵: 0xFFFFFF 0xFFFFFFFF 아웃바운드 esp sas: spi: 0xB7B5B38B(3082138507) SA 상태: 활성 변환: esp-aes-256 esp-sha-256-hmac 압축 안 함 사용 설정 ={L2L, Tunnel, IKEv2, VTI, } 슬롯: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa 타이밍: 남은 키 수명(kB/초): (4147149/3722) IV 크기: 16바이트 재생 감지 지원: Y 재전송 방지 비트맵: 0x00000000 0x00000001	슬롯: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa 타이밍: 남은 키 수명(kB/초): (3962829/3626) IV 크기: 16바이트 재생 감지 지원: Y 재전송 방지 비트맵: 0xFFFFFF 0xFFFFFFFF 아웃바운드 esp sas: spi: 0xF0C4239D(4039386013) SA 상태: 활성 변환: esp-aes-256 esp-sha-256-hmac 압축 안 함 사용 설정 ={L2L, Tunnel, IKEv2, VTI, } 슬롯: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa 타이밍: 남은 키 수명(kB/초): (4101069/3626) IV 크기: 16바이트 재생 감지 지원: Y 재전송 방지 비트맵: 0x00000000 0x00000001

2단계. 콘솔 또는 SSH를 통해 각 FTD의 CLI로 이동하여 show bgp neighbors 및 show route bgp 명령을 사용하여 BGP 상태를 확인합니다.

사이트 1 FTD	사이트 2 FTD
ftdv742# show bgp neighbors BGP 인접 디바이스가 169.254.10.2, vrf single_vf, 원격 AS 65510, 외부 링크 BGP 버전 4, 원격 라우터 ID 192.168.50.1 BGP 상태 = Established, 최대 1d20h 마지막 읽기 00:00:25, 마지막 쓰기 00:00:45, 보류 시간은 180, keepalive 간격은 60초입니다. 네이버 세션: 1 활성, 다중 세션 지원 안 함(사용 안 함) 네이버 기능: 경로 새로 고침: 알림 및 수신(신규) 4옥텟 ASN 기능: 알림 및 수신 주소군 IPv4 유니캐스트: 알림 및 수신 멀티세션 기능: 메시지 통계: InQ 깊이는 0 OutQ 깊이가 0입니다. 보낸 수신	ftdv742# show bgp neighbors BGP 인접 디바이스는 169.254.10.1, vrf single_vf, 원격 AS 65511, 외부 링크 BGP 버전 4, 원격 라우터 ID 192.168.70.1 BGP 상태 = Established, 최대 1d20h 마지막 읽기 00:00:11, 마지막 쓰기 00:00:52, 대기 시간은 180, keepalive 간격은 60초입니다. 네이버 세션: 1 활성, 다중 세션 지원 안 함(사용 안 함) 네이버 기능: 경로 새로 고침: 알림 및 수신(신규) 4옥텟 ASN 기능: 알림 및 수신 주소군 IPv4 유니캐스트: 알림 및 수신 멀티세션 기능: 메시지 통계: InQ 깊이는 0 OutQ 깊이가 0입니다. 보낸 수신

열기: 1 1 알림: 0 0 업데이트: 2 2 킵얼라이브: 2423 2427 경로 새로 고침: 0 0 합계: 2426 2430 광고 실행 간의 기본 최소 시간은 30초입니다. 주소군의 경우: IPv4 유니캐스트 세션: 169.254.10.2 BGP 테이블 버전 3, 인접 디바이스 버전 3/0 출력 대기열 크기: 0 색인 1 업데이트 그룹 구성원 1개 보낸 수신 접두사 활동: ---- ---- Prefixes Current(현재 접두사): 1 1(80바이트 사용) 접두사 합계: 1 1 암시적 철회: 0 0 명시적 철회: 0 0 최상의 경로로 사용: 해당 사항 없음 1 다중 경로로 사용: n/a 0 아웃바운드 인바운드 로컬 정책 거부된 접두사: -------- ------- 이 피어의 최상의 경로: 1 n/a 합계: 1 0 전송된 업데이트의 NLRI 수: 최대 1, 최소 0 주소 추적이 활성화되어 있으며 RIB에는 169.254.10.2에 대한 경로가 있습니다. 연결 설정 1, 끊김 0 마지막 재설정 안 함 Transport(tcp) path-mtu-discovery가 비활성화되었습니다. Graceful-Restart가 비활성화됨	열기: 1 1 알림: 0 0 업데이트: 2 2 킵얼라이브: 2424 2421 경로 새로 고침: 0 0 합계: 2427 2424 광고 실행 간의 기본 최소 시간은 30초입니다. 주소군의 경우: IPv4 유니캐스트 세션: 169.254.10.1 BGP 테이블 버전 9, 인접 디바이스 버전 9/0 출력 대기열 크기: 0 색인 4 4 업데이트 그룹 구성원 보낸 수신 접두사 활동: ---- ---- Prefixes Current(현재 접두사): 1 1(80바이트 사용) 접두사 합계: 1 1 암시적 철회: 0 0 명시적 철회: 0 0 최상의 경로로 사용: 해당 사항 없음 1 다중 경로로 사용: n/a 0 아웃바운드 인바운드 로컬 정책 거부된 접두사: -------- ------- 이 피어의 최상의 경로: 1 n/a 합계: 1 0 전송된 업데이트의 NLRI 수: 최대 1, 최소 0 주소 추적이 활성화되어 있으며 RIB에는 169.254.10.1에 대한 경로가 있습니다. 연결 설정 4, 끊김 3 세션 1의 인터페이스 플랩으로 인한 마지막 재설정 1d21h Transport(tcp) path-mtu-discovery가 비활성화되었습니다. Graceful-Restart가 비활성화됨
ftdv742# 경로 bgp 표시 코드: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간 N1 - OSPF NSSA 외부 유형 1, N2 - OSPF	ftdv742# 경로 bgp 표시 코드: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간 N1 - OSPF NSSA 외부 유형 1, N2 - OSPF

NSSA 외부 유형 2 E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, V - VPN i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2 ia - IS-IS inter area, * - 후보 기본값, U - 사용자 별 고정 경로 o - ODR, P - 정기적으로 다운로드되는 고정 경로, + - 복제된 경로 SI - 정적 InterVRF, BI - BGP InterVRF 최종 목적지의 게이트웨이는 192.168.30.3에서 네트워크 0.0.0.0으로 B 169.254.10.2, 1d20h를 통해 192.168.50.0 255.255.255.0 [20/0]	NSSA 외부 유형 2 E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, V - VPN i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2 ia - IS-IS inter area, * - 후보 기본값, U - 사용자 별 고정 경로 o - ODR, P - 정기적으로 다운로드되는 고정 경로, + - 복제된 경로 SI - 정적 InterVRF, BI - BGP InterVRF 최종 목적지의 게이트웨이는 192.168.10.3에서 네트워크 0.0.0.0으로 B 169.254.10.1, 1d20h를 통해 192.168.70.0 255.255.255.0 [20/0]

3단계. Site1 클라이언트와 Site2 클라이언트가 성공적으로 서로 ping했습니다.

사이트 1 클라이언트:

```
Site1_Client#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 = 31/56/90 ms
```

사이트 2 클라이언트:

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

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 BGP 섹션의 문제를 해결할 수 있습니다.

```
ftdv742# debug ip bgp ?

A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range      BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpnv4      Address family
vpnv6      Address family
vrf        VRF scope
<cr>
```

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.