BGP over routegebaseerde VPN op FTD beheerde switch met FDM

Inhoud

Inleiding

Dit document beschrijft het configureren van BGP via route-gebaseerde site-to-site VPN op FTDv beheerd door FirePower Device Manager (FDM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van VPN
- BGP-configuraties op FTDv
- Ervaring met FDM

Gebruikte componenten

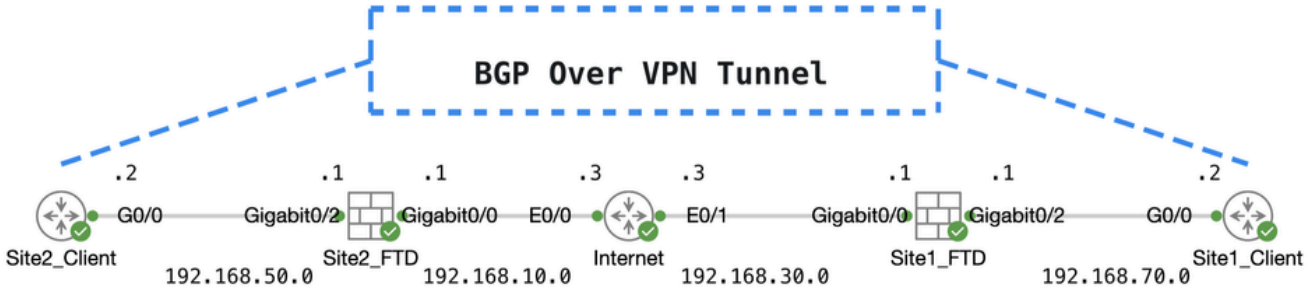
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTDv versie 7.4.2
- Cisco FDM versie 7.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram



Topo

Configuraties op VPN

Stap 1. Zorg ervoor dat de IP-interconnectiviteit tussen knooppunten gereed en stabiel is. De slimme licentie op FDM wordt met succes geregistreerd bij de smart account.

Stap 2. De gateway van Site1 Client is geconfigureerd met het binnenste IP-adres van Site1 FTD (192.168.70.1). De gateway van de Site2-client is geconfigureerd met het interne IP-adres van Site2 FTD (192.168.50.1). Zorg er ook voor dat de standaardroute op beide FTD's correct is geconfigureerd na FDM-initialisatie.

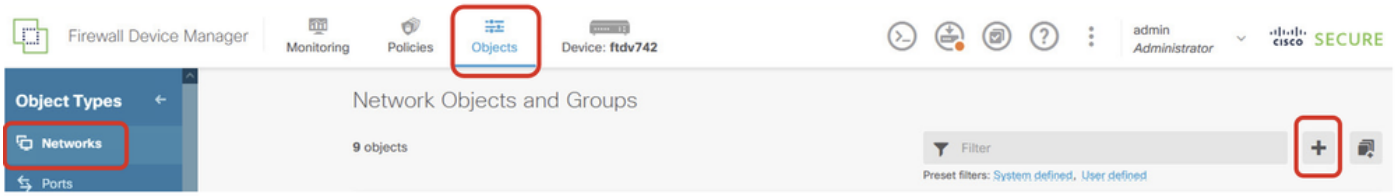
Meld u aan bij de GUI van elke FDM. Navigeer naarDevice > Routing. Klik op de knop .View Configuration Klik op het **Static Routing** tabblad om de standaard statische route te controleren.

Site1_FTD_Gateway

Site2_FTD_Gateway

Stap 3. Configureer route-gebaseerde site-to-site VPN. In dit voorbeeld, vorm eerst Site1 FTD.

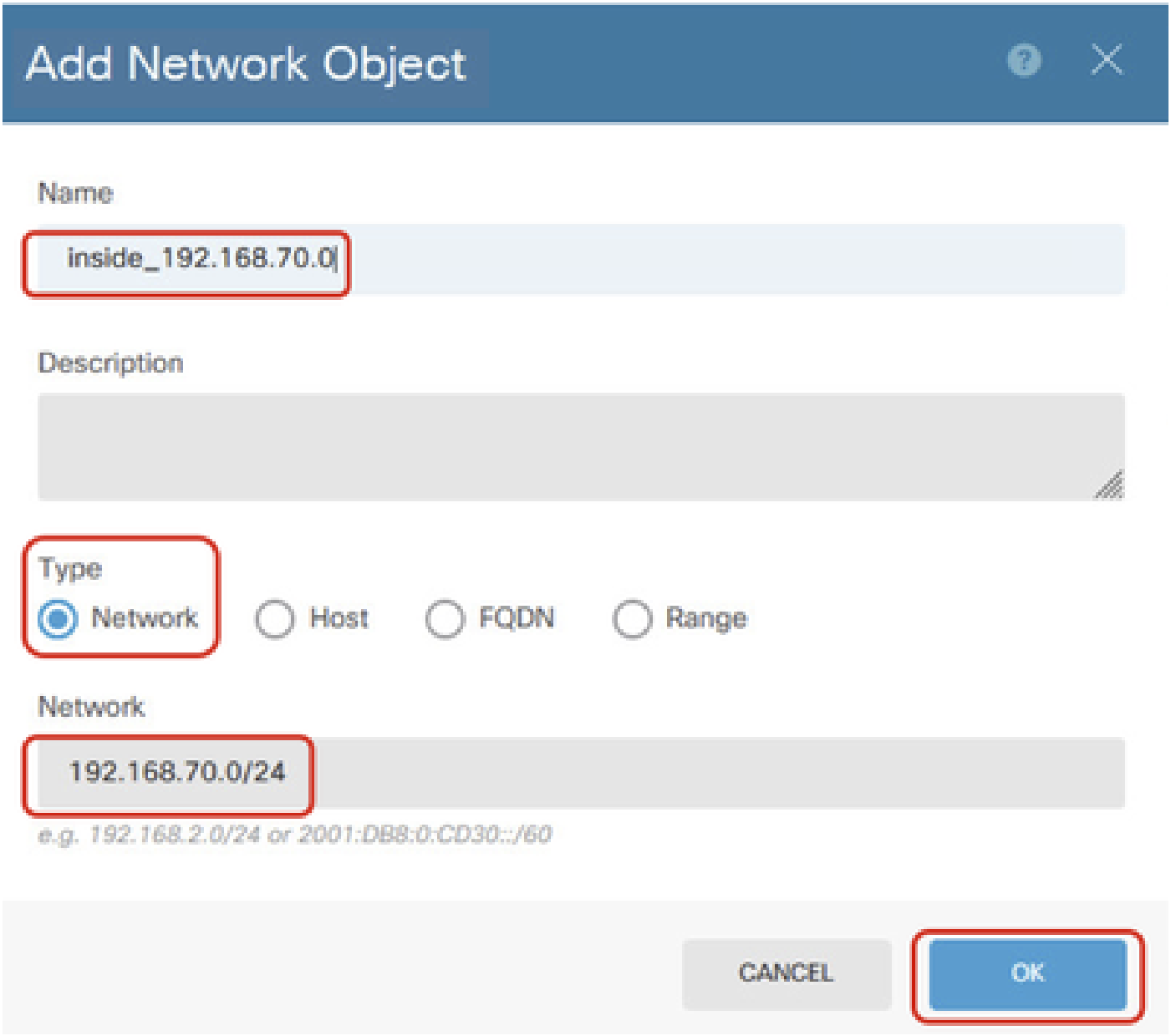
Stap 3.1. Aanmelden bij de FDM GUI van Site1 FTD. Maak een nieuw netwerkobject voor het interne netwerk van Site1 FTD. Navigeer naar **Objects** > **Networks**, klik op de knop +.



Maken_Netwerk_Object

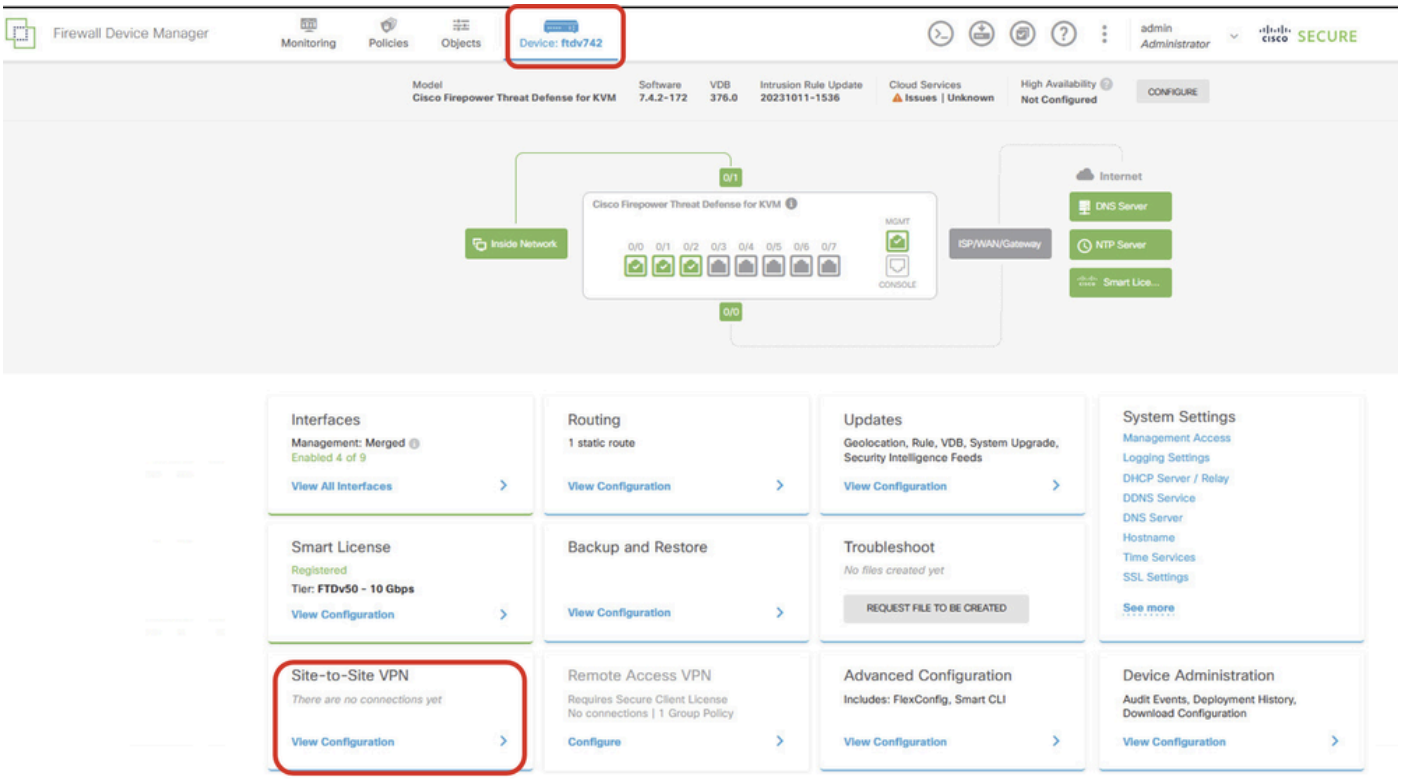
Stap 3.2. Verstrek de nodige informatie. Klik op de**OK** knop.

- Naam: inside_192.168.70.0
- Type: netwerk
- Netwerk: 192.168.70.0/24



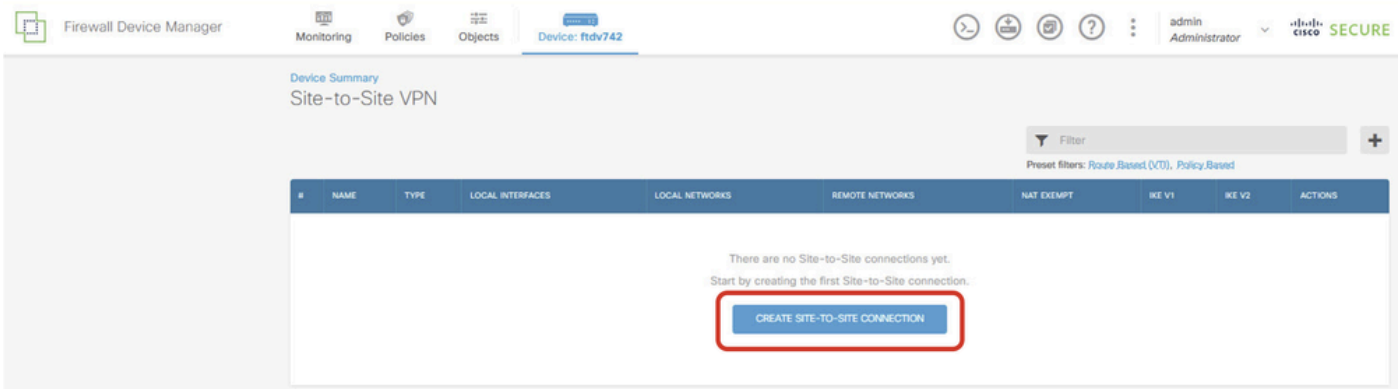
Site1_Binnen_Netwerk

Stap 3.3. Navigeer naar **Device > Site-to-Site VPN** . Klik op de knop .**View Configuration**



Site-to-Site VPN bekijken

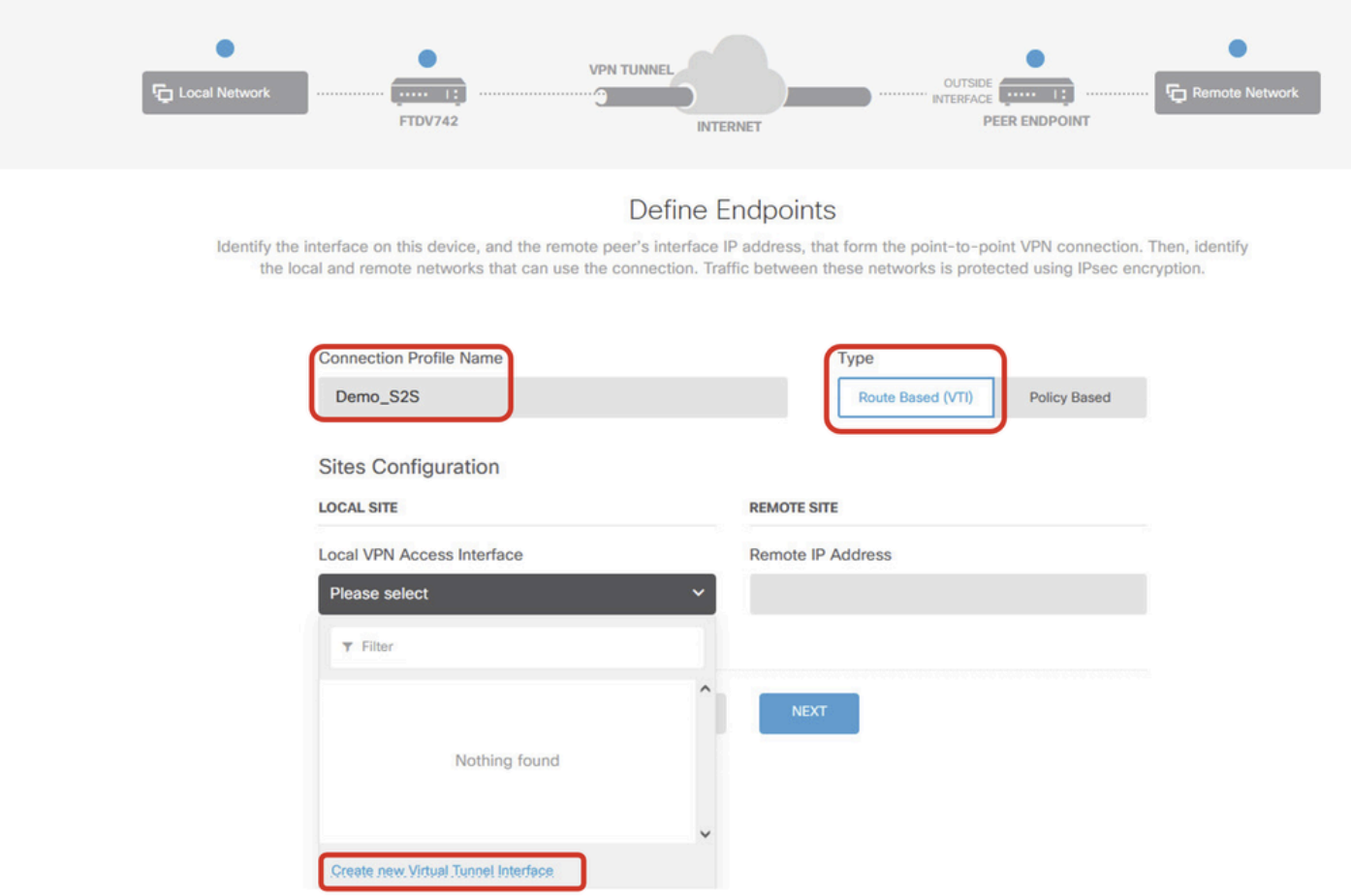
Stap 3.4. Start het maken van een nieuwe site-to-site VPN. Klik op de knop .**CREATE SITE-TO-SITE CONNECTION**



Create_Site-to-Site_Connection

Stap 3.5. Verstrek de nodige informatie.

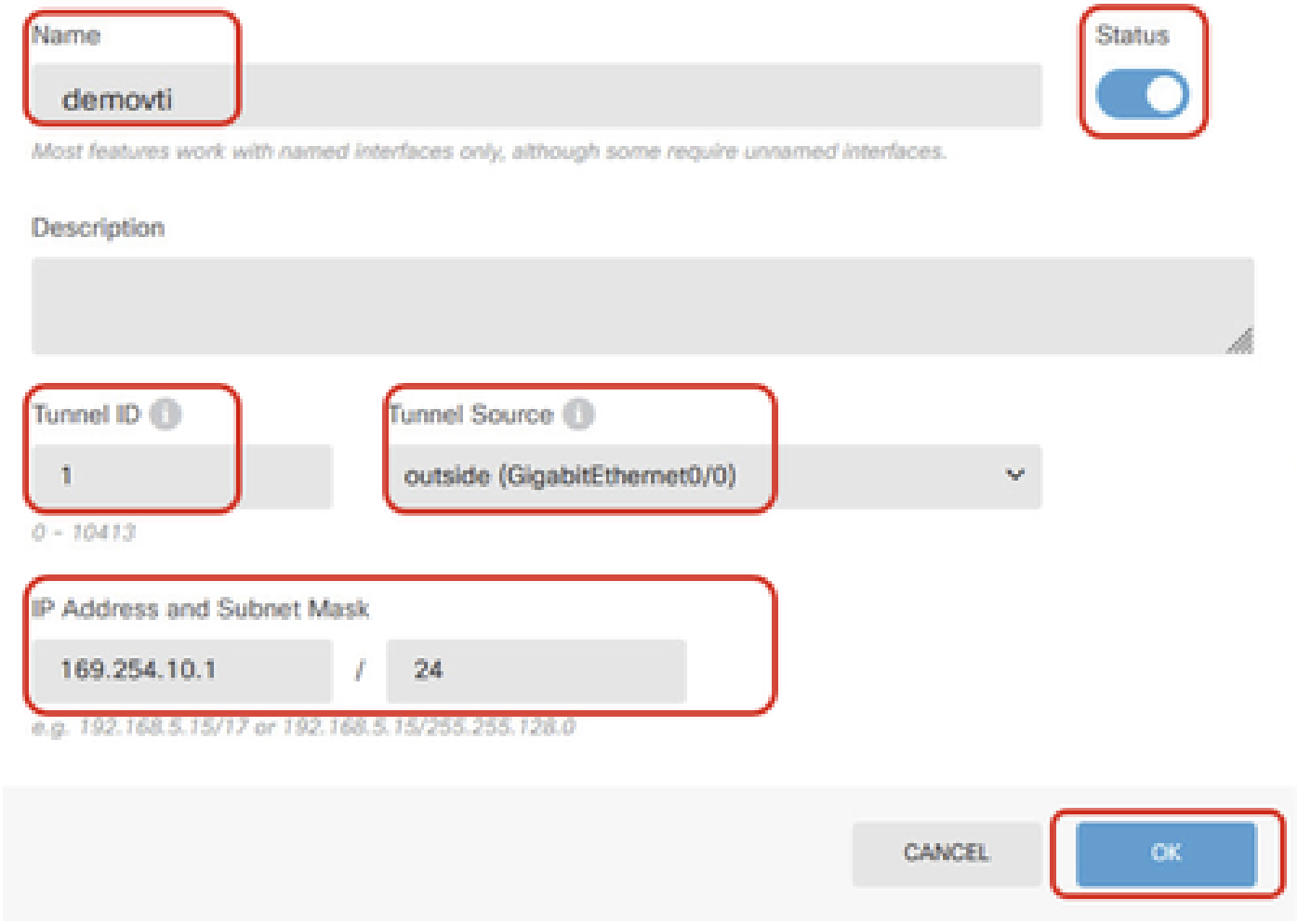
- Naam verbindingsprofiel: Demo_S2S
- Type: routegebaseerd (VTI)
- Lokale VPN-toegangsinterface: klik op de vervolgkeuzelijst en klik vervolgens op **Create new Virtual Tunnel Interface** .



Aanmaken_VTI_in_VPN_Wizard

Stap 3.6. Verstrek de nodige informatie om een nieuwe VTI te creëren. Klik op de knop OK.

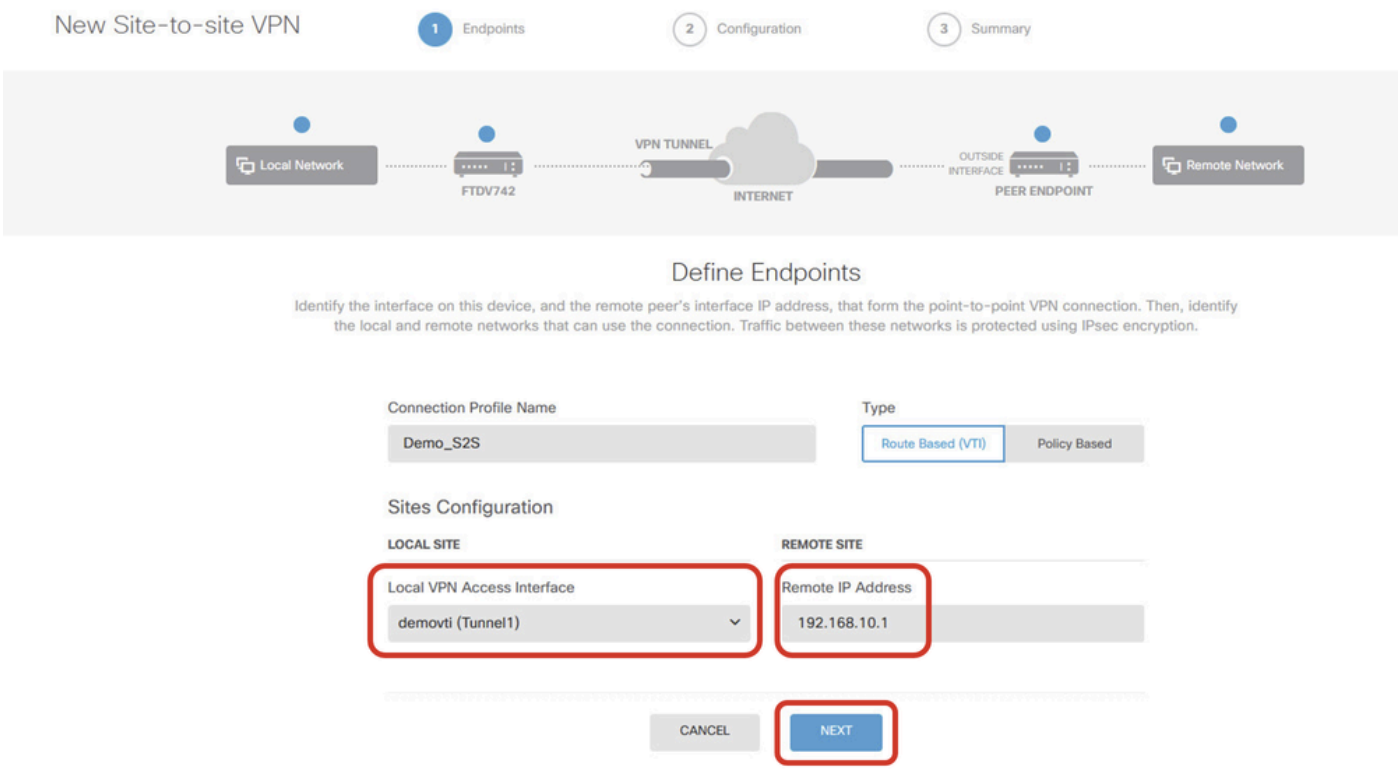
- Naam: demovti
- Tunnel-id: 1
- Tunnelbron: buiten (Gigabit Ethernet0/0)
- IP-adres en subnetmasker: 169.254.10.1/24
- Status: klik op de schuifschakelaar voor de ingeschakelde positie



Creëer_VTI_Details

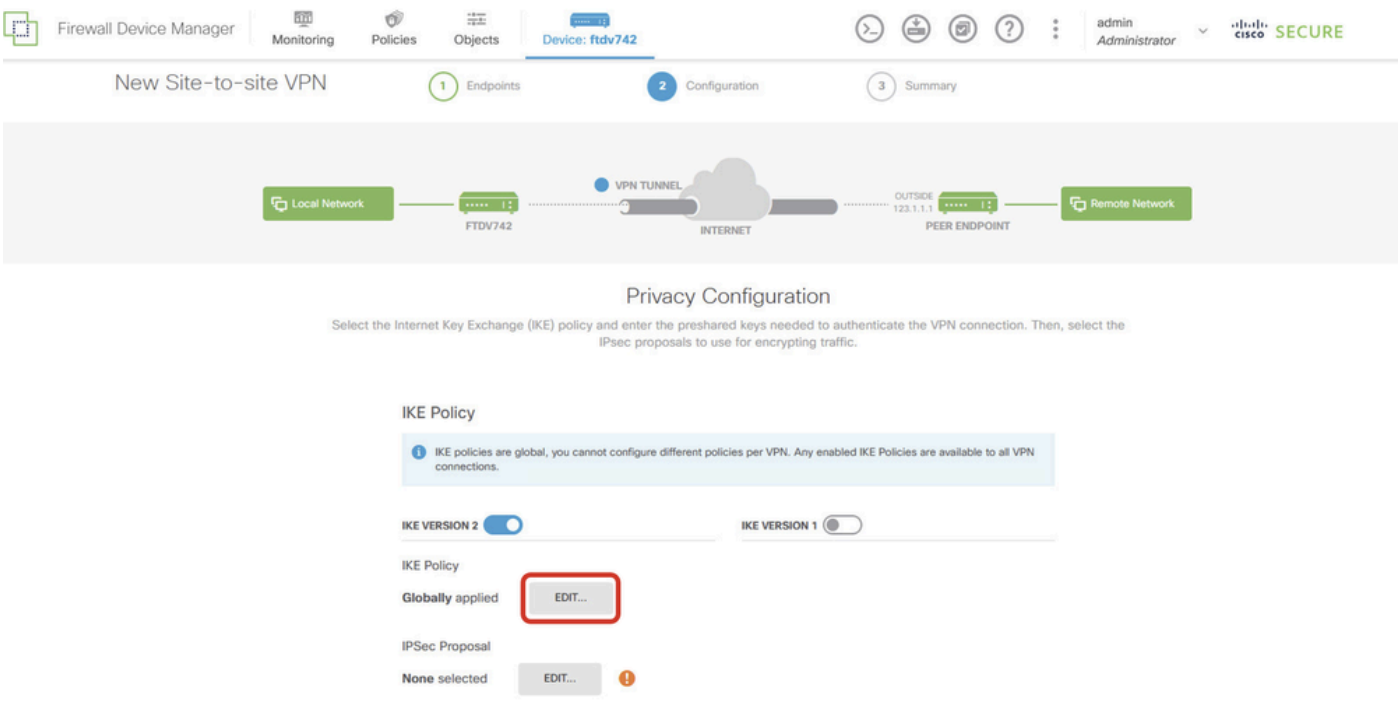
Stap 3.7. Blijf de nodige informatie verstrekken. Klik op de knop VOLGENDE.

- Lokale VPN-toegangsinterface: demovti (gemaakt in stap 3.6.)
- Remote IP-adres: 192.168.10.1



VPN_Wizard_Endpoints_Step1

Stap 3.8. Ga naar IKE-beleid. Klik op de knop BEWERKEN.



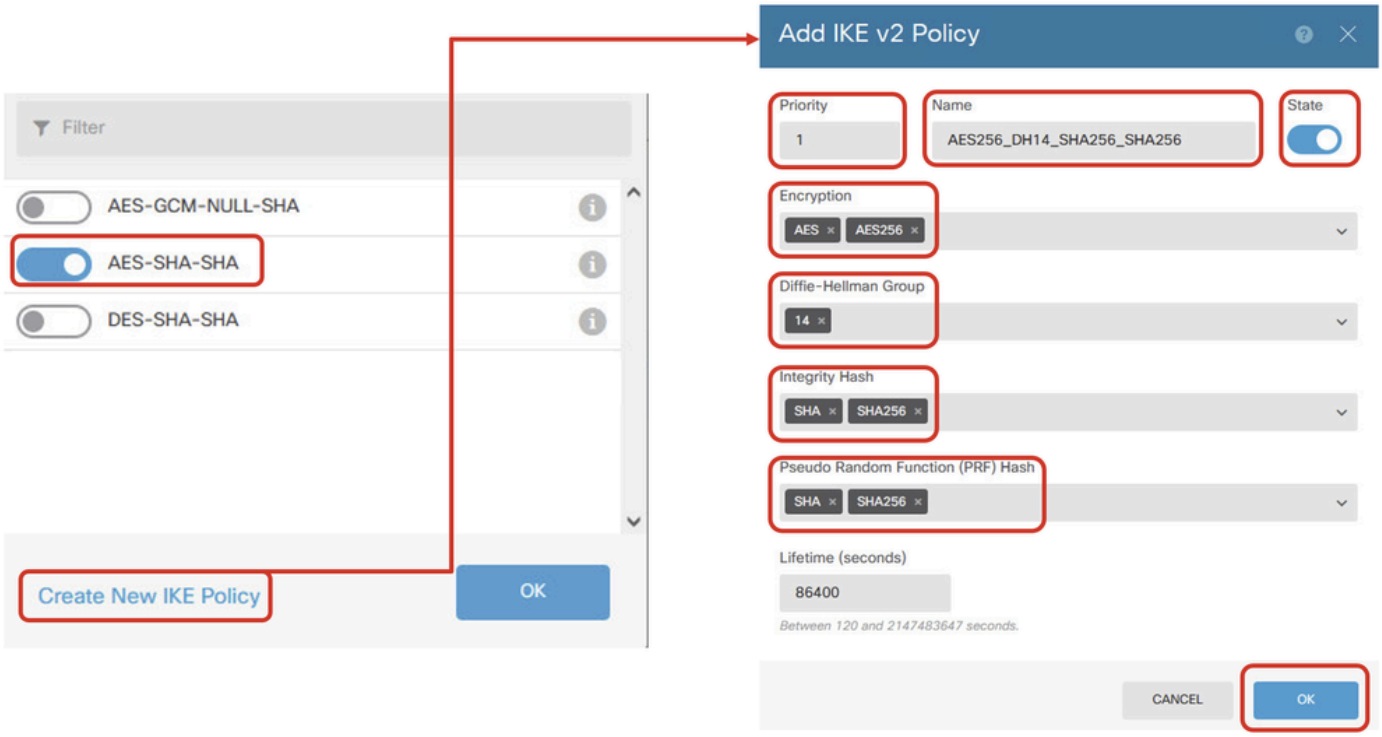
Bewerken_IKE_Policy

Stap 3.9. Voor het IKE-beleid kunt u een vooraf gedefinieerde gebruiken of een nieuwe maken door op Nieuw IKE-beleid maken te klikken.

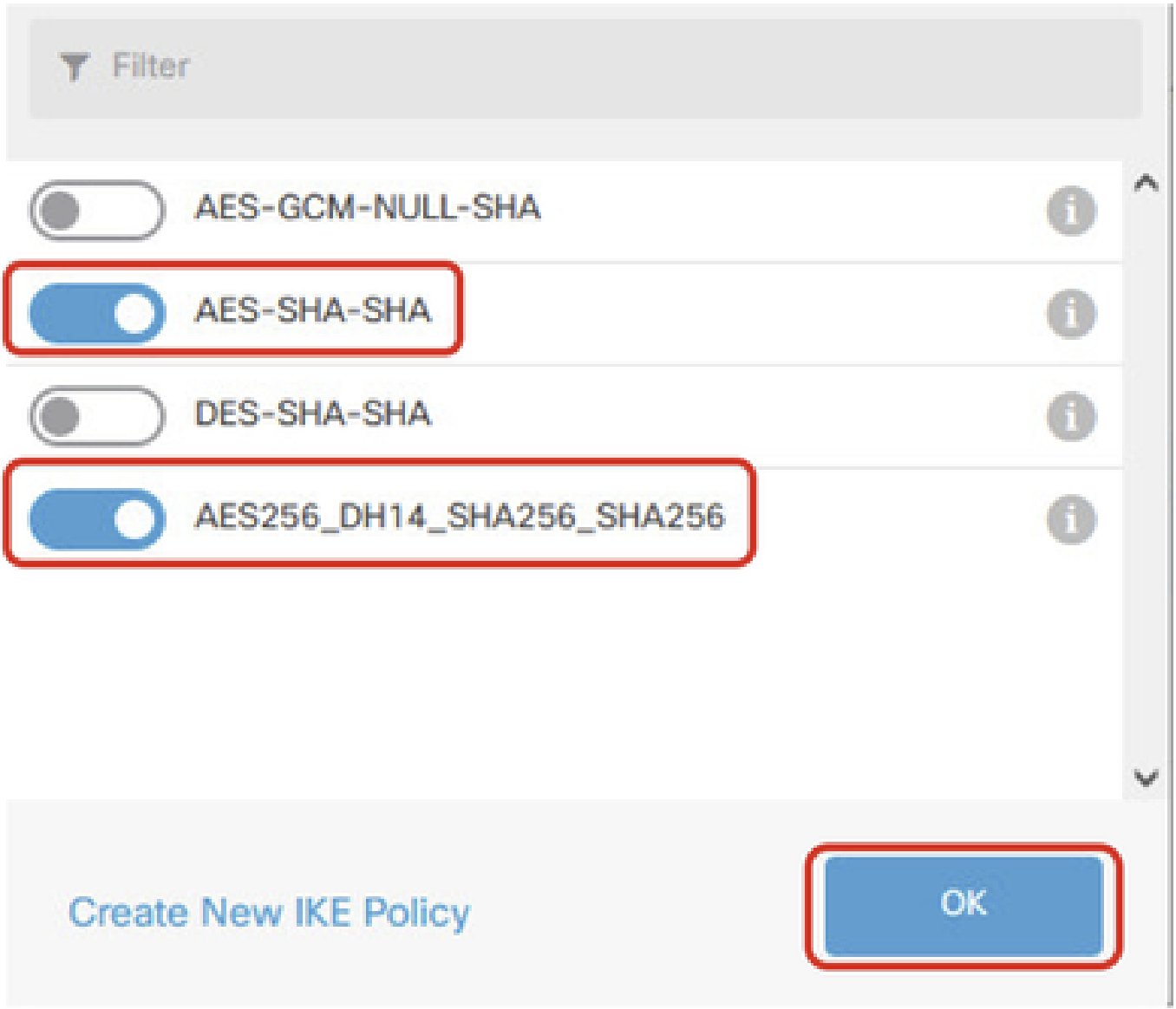
In dit voorbeeld, schakel een bestaand IKE-beleid AES-SHA-SHA en creëer ook een nieuwe voor

demo doeleinden. Klik op de knop OK om op te slaan.

- Naam: AES256_DH14_SHA256_SHA256
- Versleuteling: AES, AES256
- DH-groep: 14
- Integriteitshash: SHA, SHA256
- PRF-hash: SHA, SHA256
- Levensduur: 86400 (standaard)

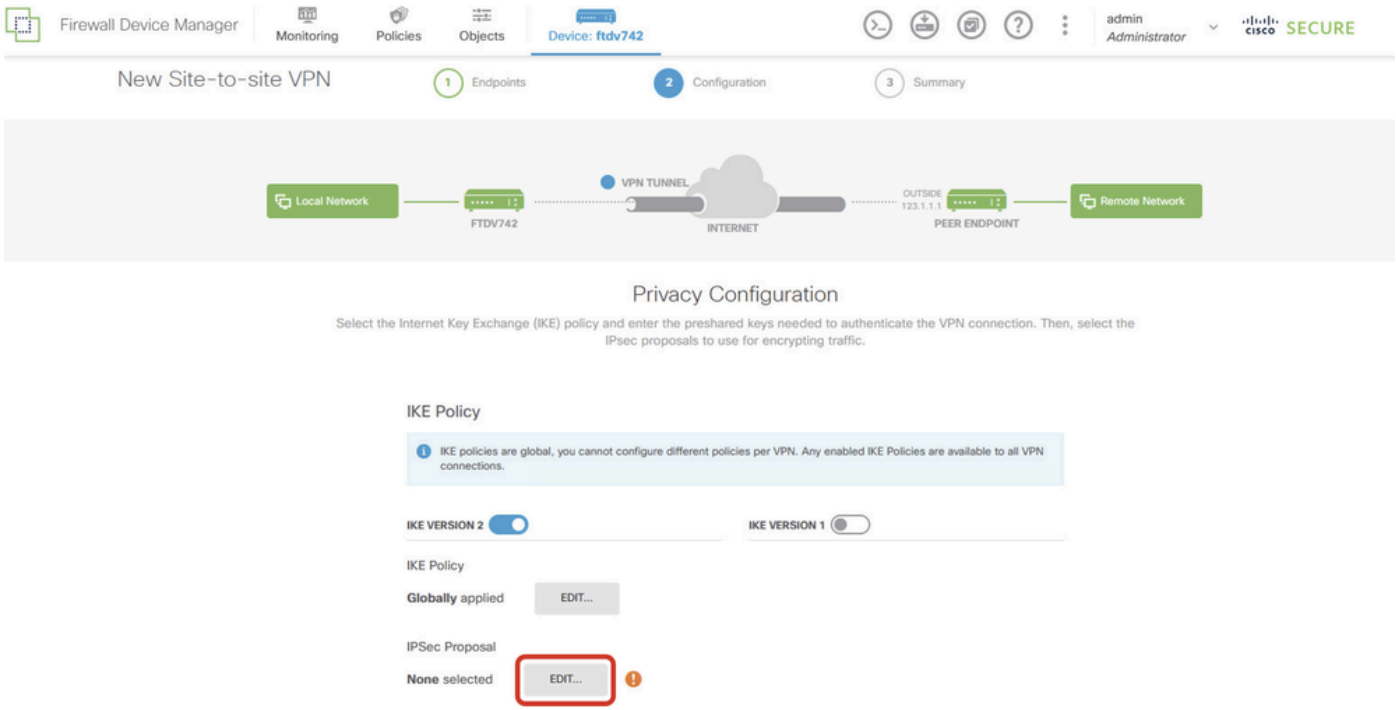


Add_New_IKE_Policy



Inschakelen_Nieuw_IKE_Beleid

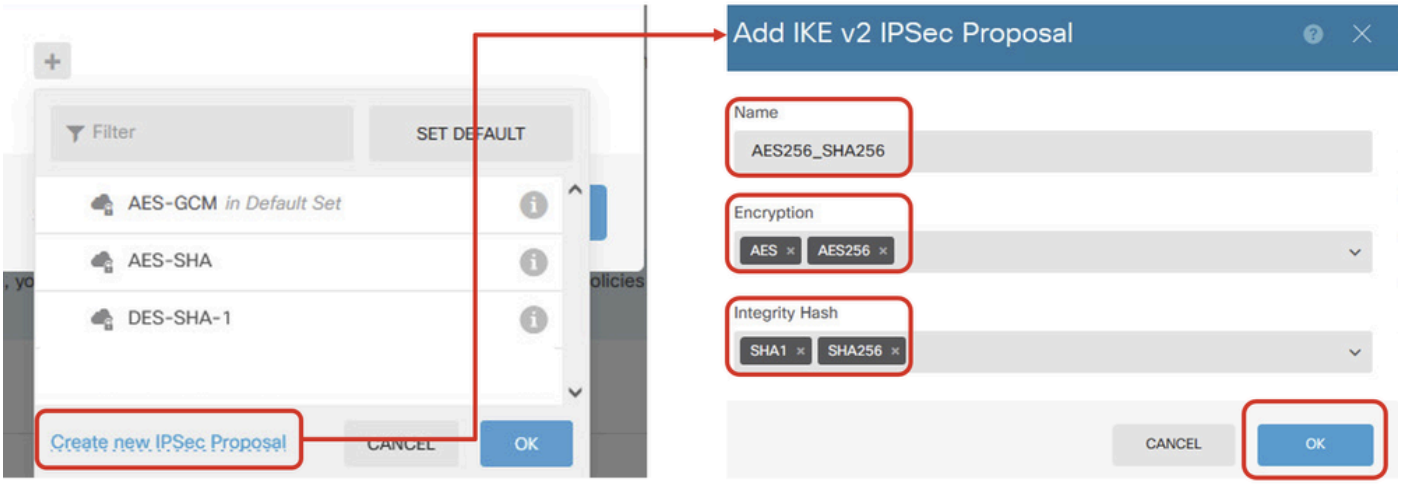
Stap 3.10. Ga naar het IPSec-voorstel. Klik op de knop BEWERKEN.



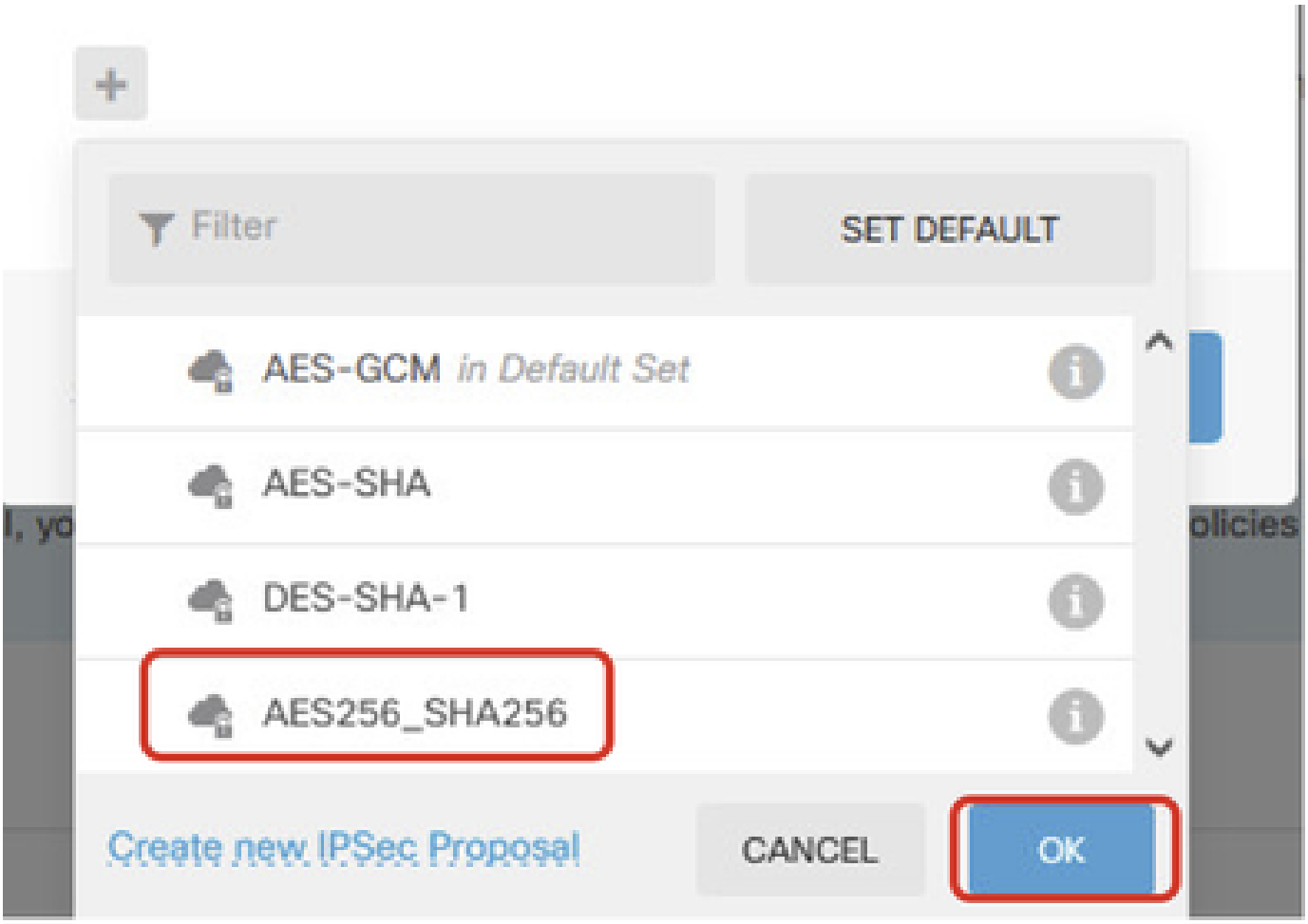
Bewerken_IKE_voorstel

Stap 3.11. Voor het IPSec-voorstel kunt u een vooraf gedefinieerde interface gebruiken of u kunt een nieuwe maken door op Nieuw IPSec-voorstel maken te klikken. In dit voorbeeld, maak een nieuwe voor demo doeleinden. Verstrek de nodige informatie. Klik op de knop OK om op te slaan.

- Naam: AES256_SHA256
- Versleuteling: AES, AES256
- Integriteitshash: SHA1, SHA256



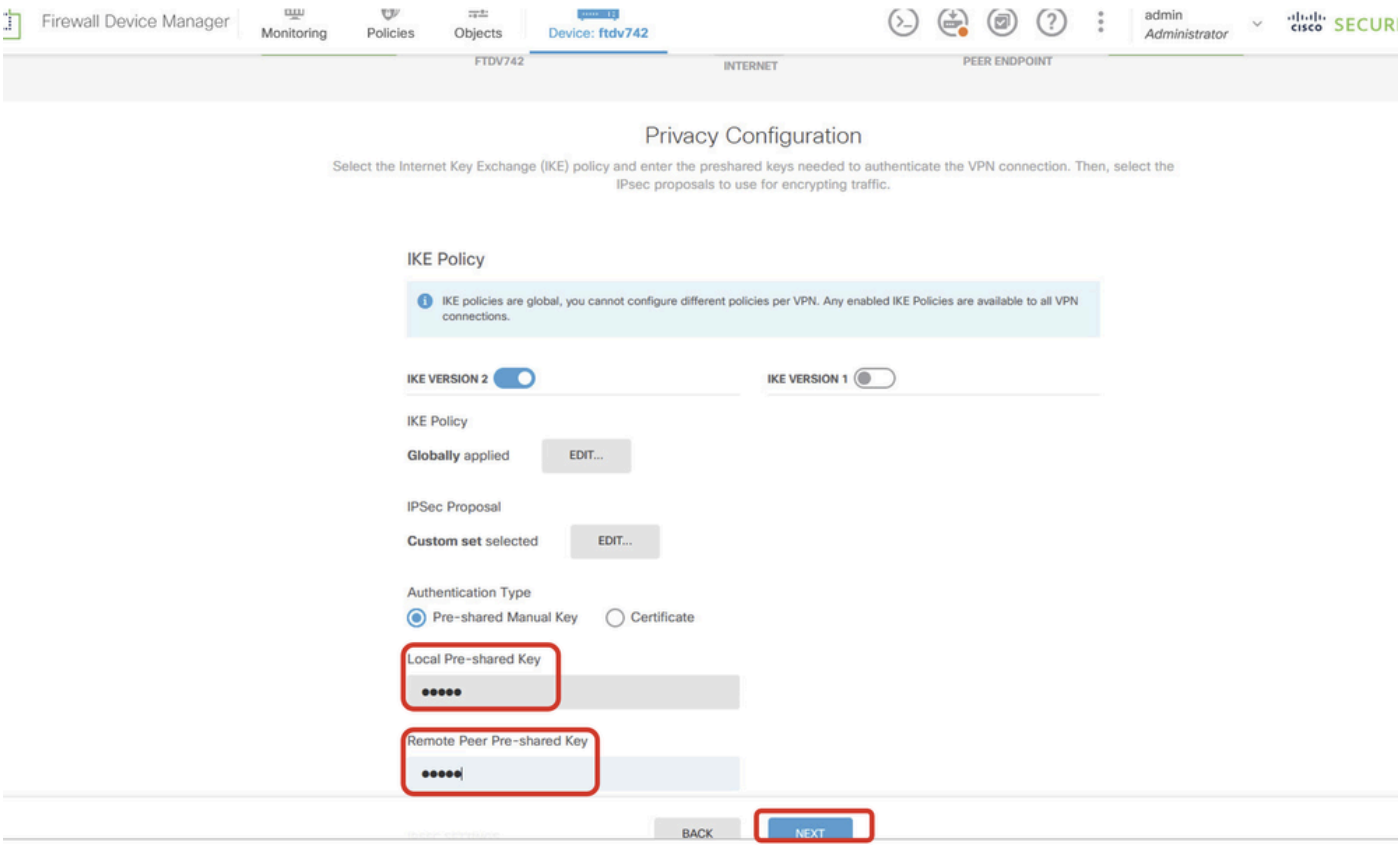
Add_New_IPSec_voorstel



Enable_New_IPSec_voorstel

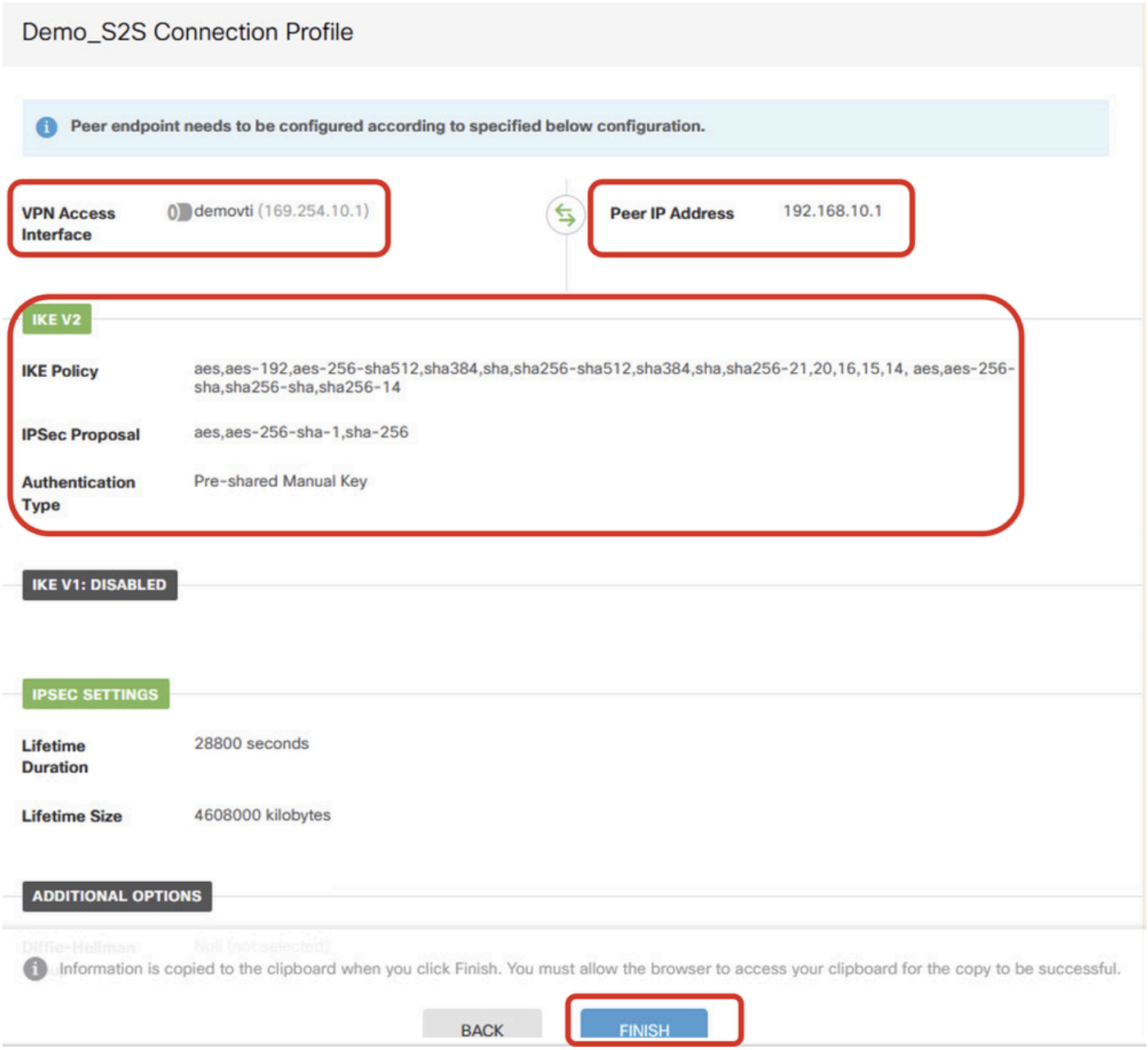
Stap 3.12. Configureer de voorgedeelde sleutel. Klik op de knop VOLGENDE.

Noteer deze vooraf gedeelde sleutel en configureer deze later op de Site2 FTD.



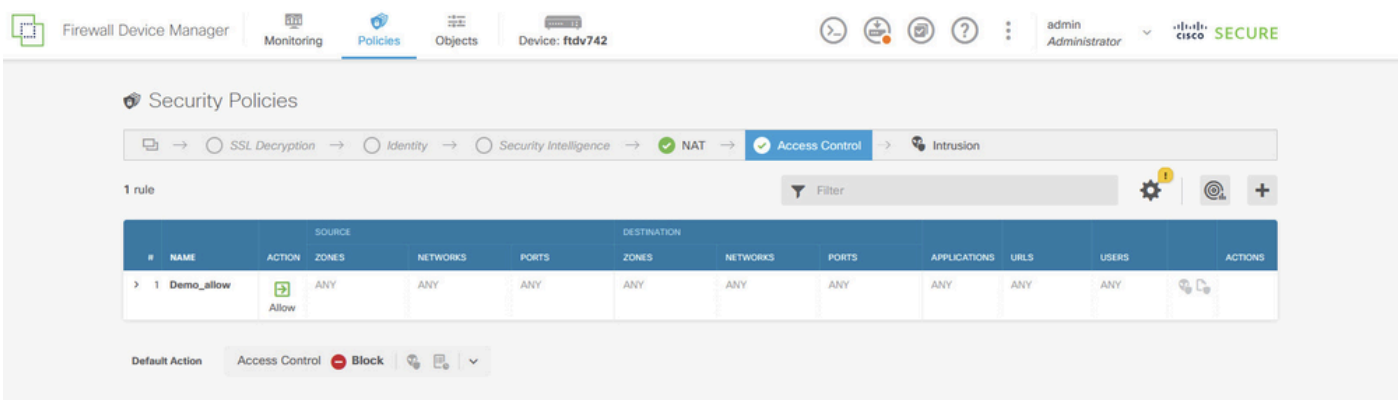
Configuratie_Vooraf_Gedeeld_Sleutel

Stap 3.13. Herzie de VPN-configuratie. Als er iets moet worden gewijzigd, klikt u op de knop TERUG. Als alles goed is, klikt u op de knop VOLTOOIEN.



VPN_Wizard_Compleet

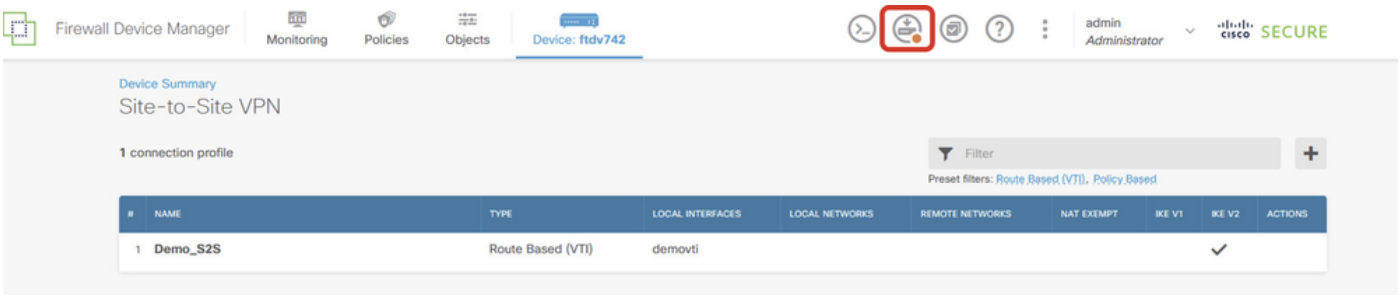
Stap 3.14. Maak een toegangscontroleregel om verkeer door de FTD te laten passeren. In dit voorbeeld, sta allen voor demodoeleinden toe. Wijzig uw beleid op basis van uw werkelijke behoeften.



Access_Control_Rule_Voorbeeld

Stap 3.15. (Optioneel) Configureer NAT-vrijstellingsregel voor het clientverkeer op FTD als dynamische NAT is geconfigureerd voor de client om toegang tot internet te krijgen. In dit voorbeeld is het niet nodig om een NAT-vrijgestelde regel te configureren omdat er op elke FTD geen dynamische NAT is geconfigureerd.

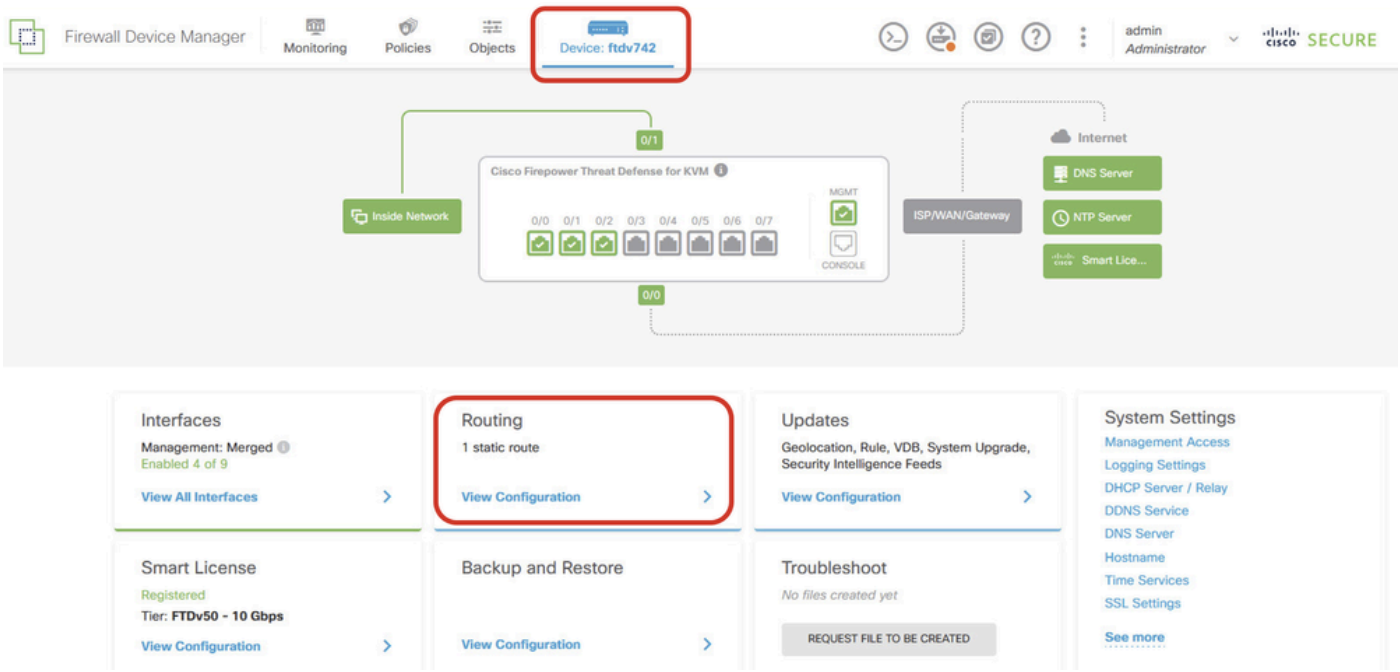
Stap 3.16. Stel de configuratieveranderingen op.



Implementatie_VPN_configuratie

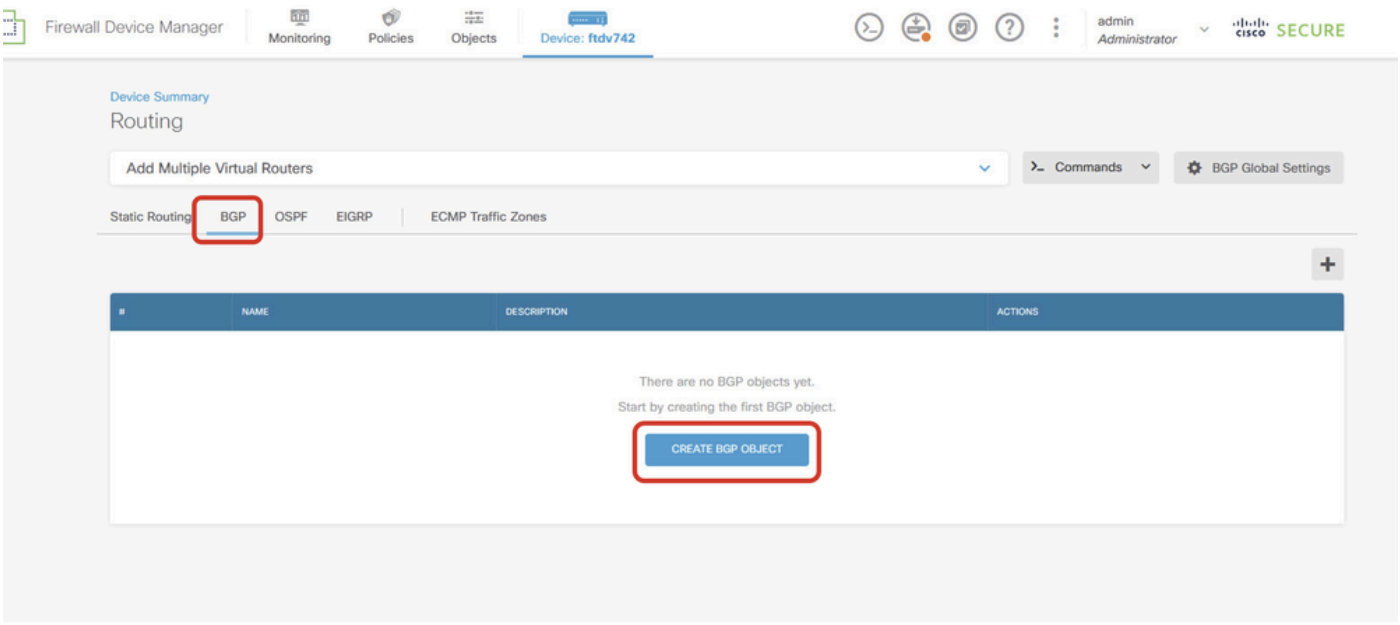
Configuraties op BGP

Stap 4. Navigeer naar apparaat > routing. Klik op Configuratie weergeven.



View_Routing_Configuration

Stap 5. Klik op het tabblad BGP en klik vervolgens op CREATE BGP OBJECT.



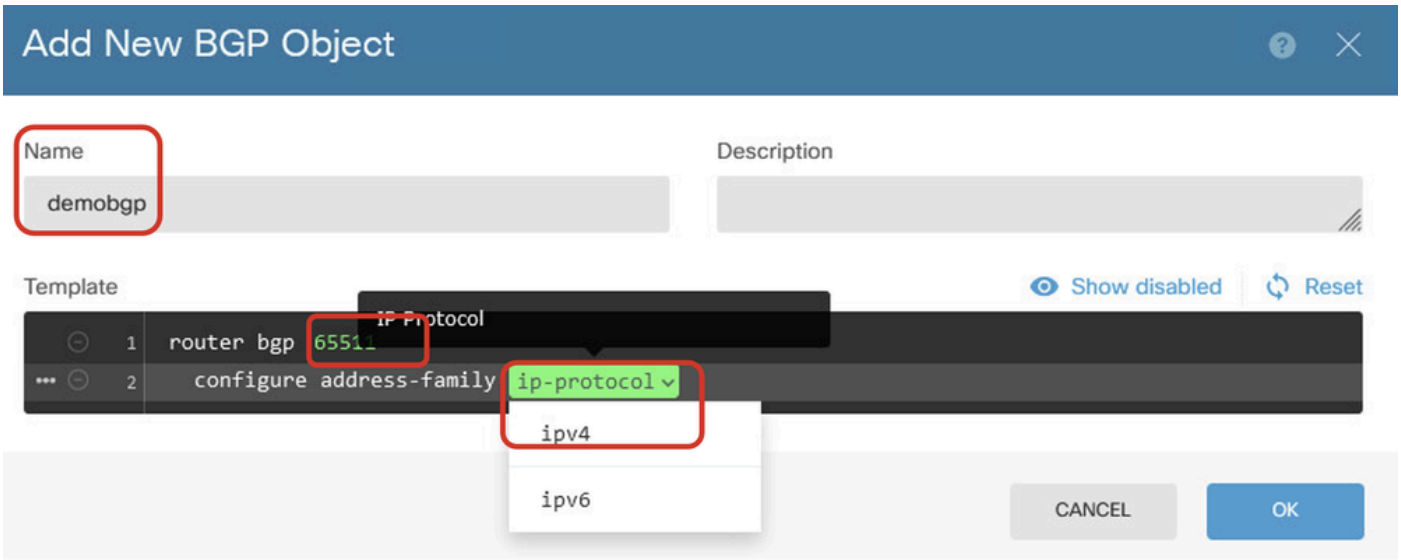
Maken_BGP_Object

Stap 6. Geef de naam van het object op. Navigeren naar Sjabloon en configureren. Klik op de knop OK om op te slaan.

Naam: demobgp

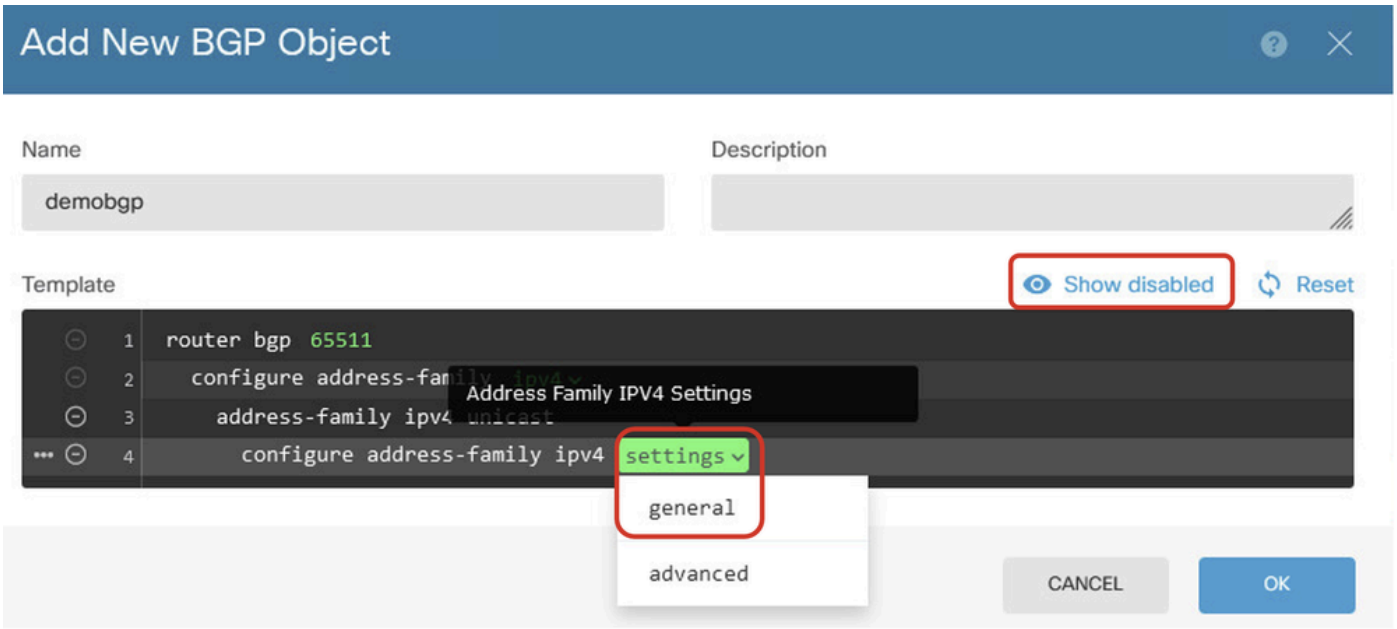
Lijn 1: Als nummer instellen. Klik op als nummer. Handmatige invoer lokaal AS-nummer. In dit voorbeeld, AS-nummer 65511 voor Site1 FTD.

Lijn 2: IP-protocol configureren. Klik op IP-protocol. Selecteer ipv4.



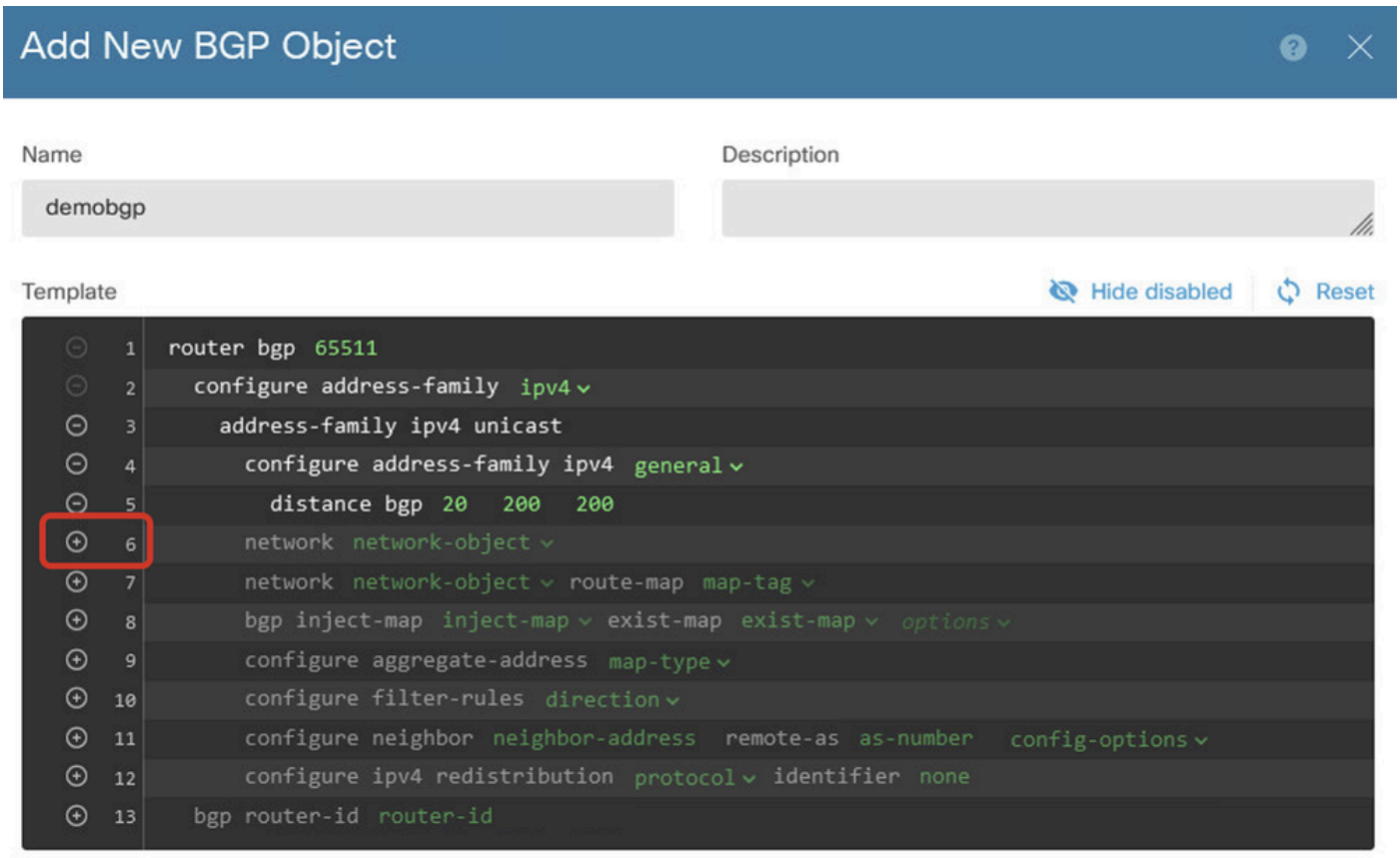
Maken_BGP_Object_ASNumber_Protocol

Lijn 4: Meer instellingen configureren. Klik op Instellingen, kies algemeen en klik vervolgens op Uitgeschakeld tonen.

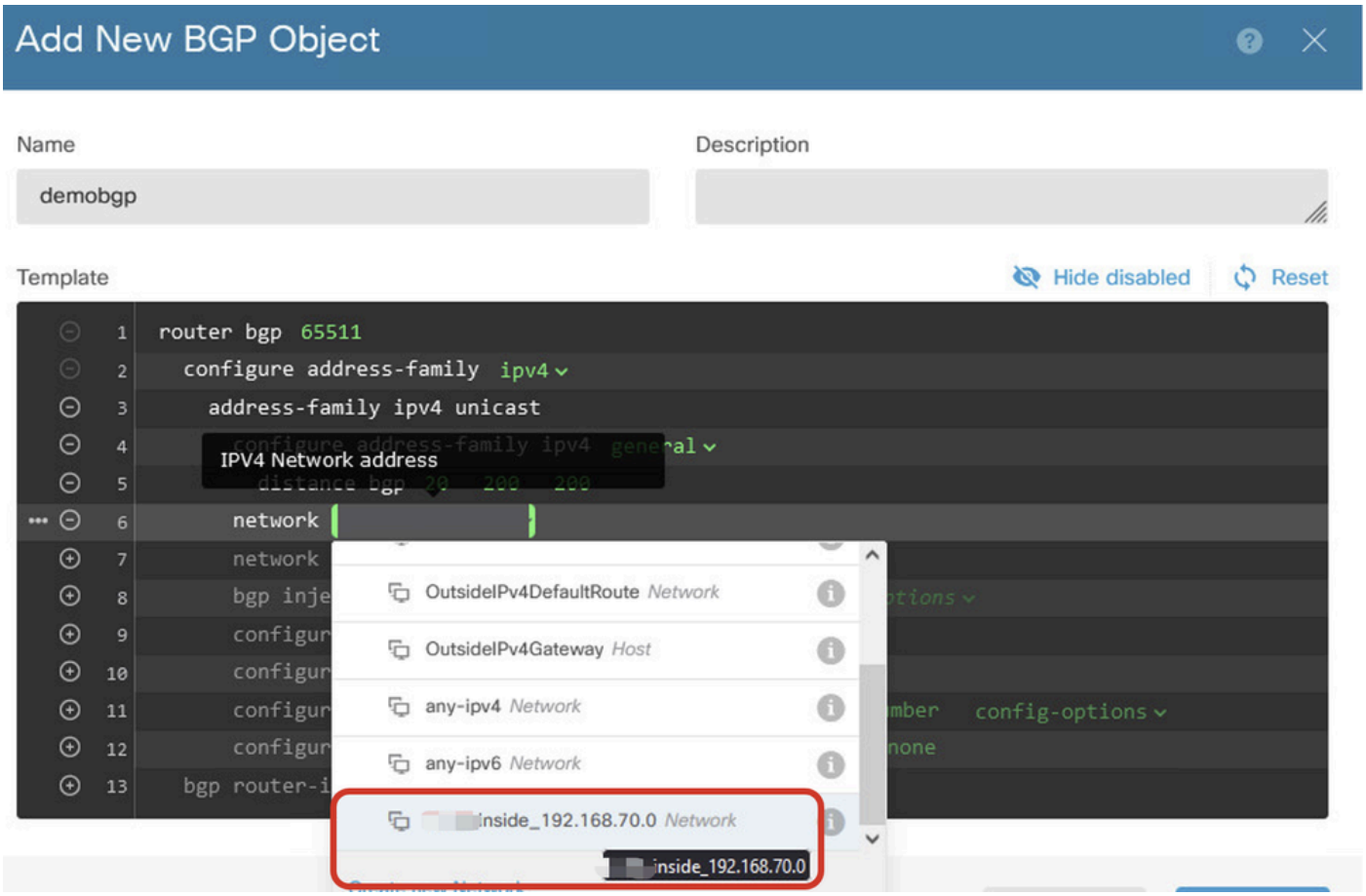


Creëer_BGP_Object_AddressSetting

Lijn 6: Klik op het pictogram + om de lijn in staat te stellen het BGP-netwerk te configureren. Klik op het netwerkobject. U kunt de bestaande beschikbare objecten zien en er een kiezen. Kies in dit voorbeeld de objectnaam inside_192.168.70.0 (gemaakt in Stap 3.2.).

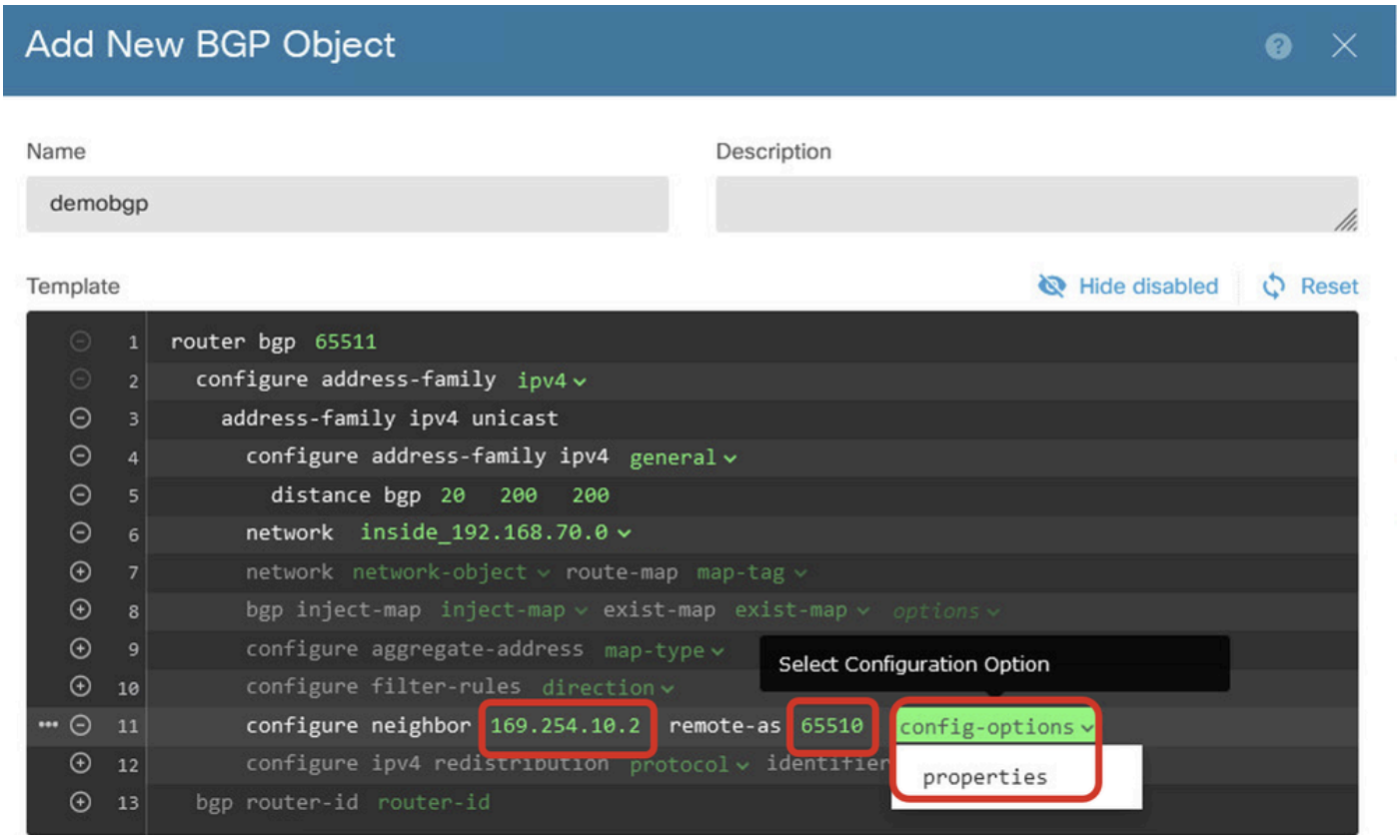


Aanmaken_BGP_Object_Add_Network



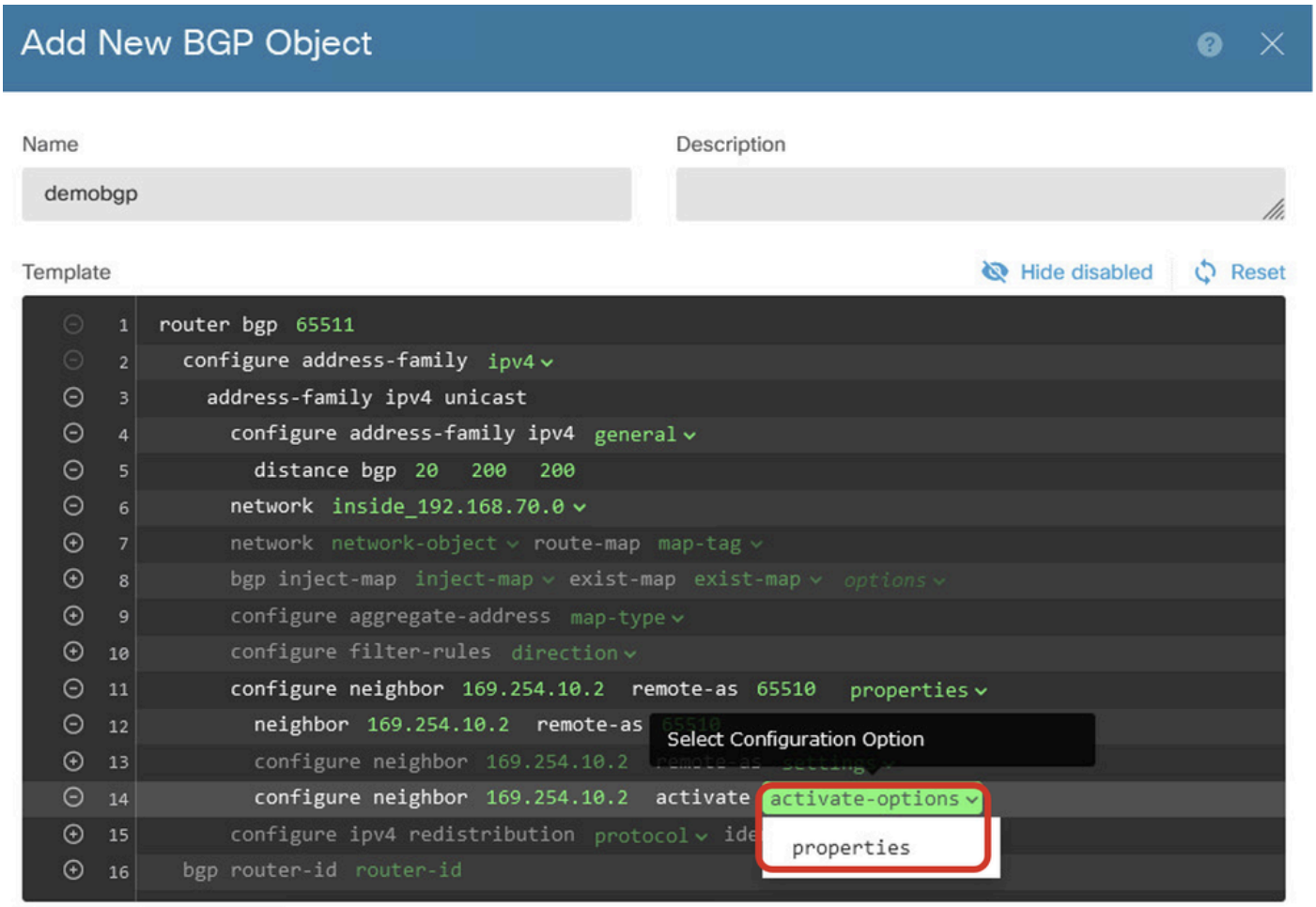
Maken_BGP_Object_Add_Network2

Lijn 11: Klik op het pictogram + om de lijn in staat te stellen om de BGP-buurinformatie te configureren. Klik op buuradres en voer handmatig het peer-BGP buuradres in. In dit voorbeeld is het 169.254.10.2 (VTI IP-adres van Site2 FTD). Klik op as-number en voer handmatig het peer AS-nummer in. In dit voorbeeld is 65510 voor Site2 FTD. Klik op Config-opties en kies eigenschappen.



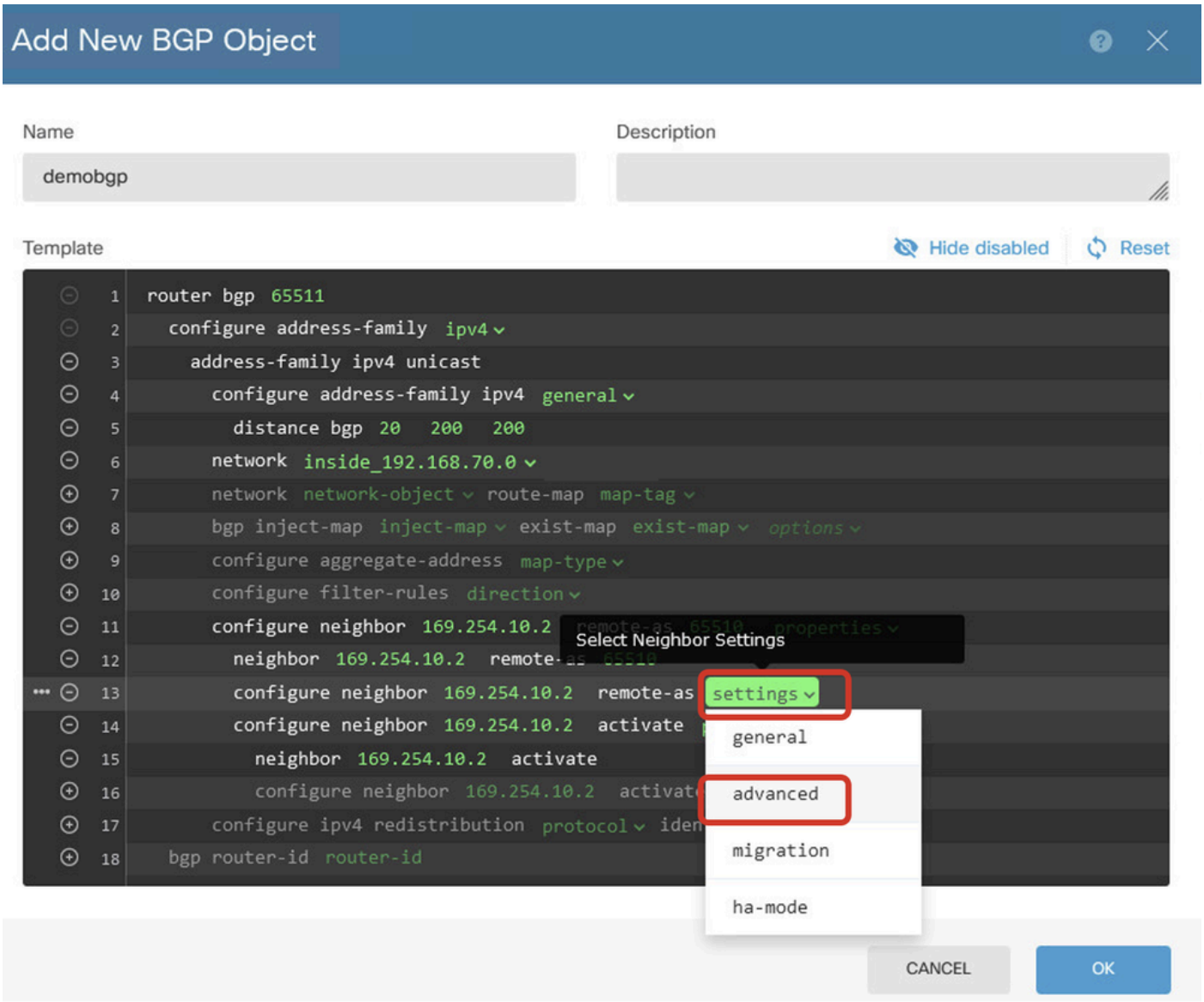
Creëer_BGP_Object_NeighbourSetting

Lijn 14: Klik op het pictogram + om de lijn in staat te stellen bepaalde eigenschappen van de buur te configureren. Klik op activeringsopties en kies eigenschappen.



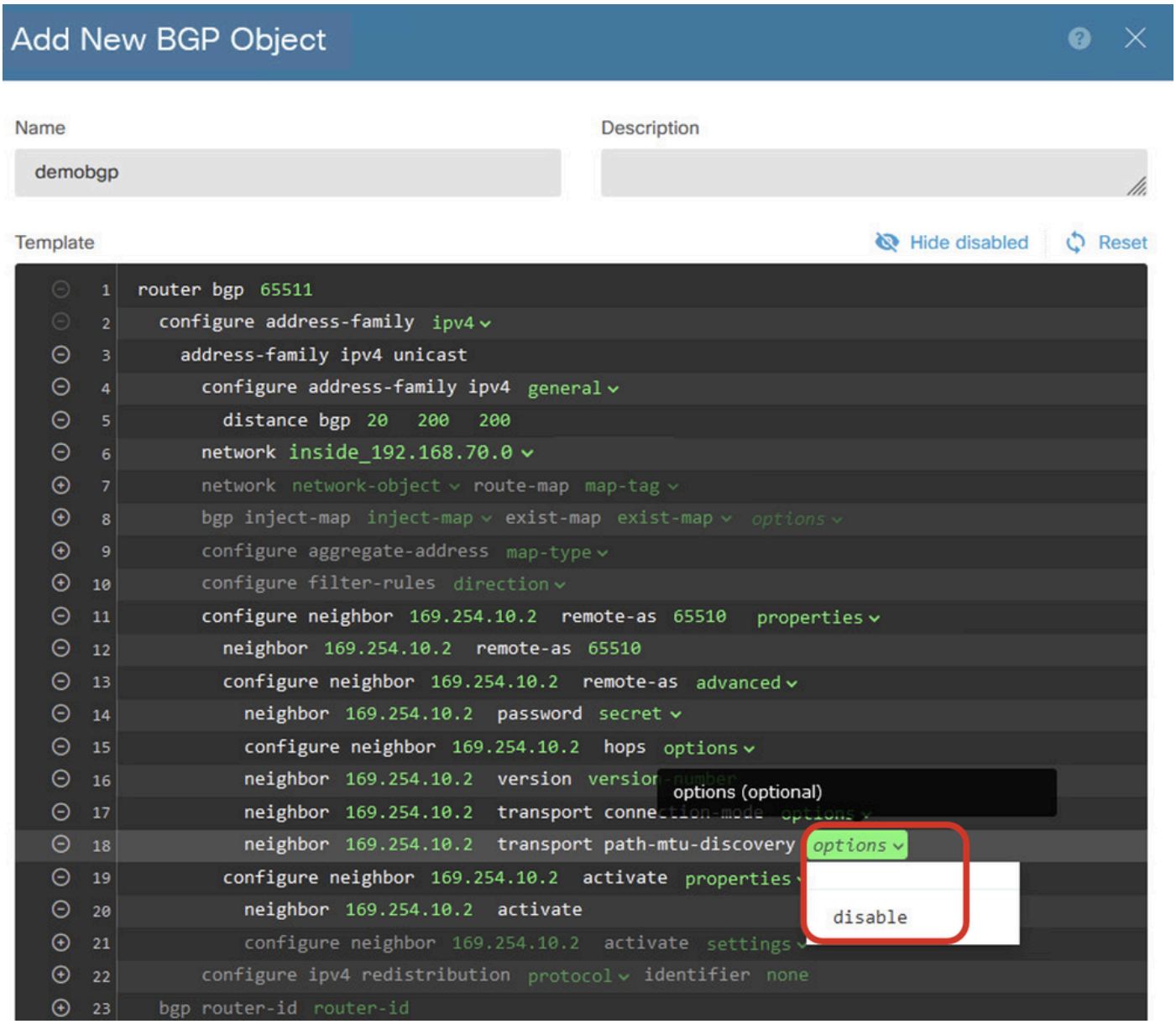
Maken_BGP_Object_NeighborSetting_Properties

Lijn 13: Klik op het pictogram + om de lijn in staat te stellen geavanceerde opties weer te geven. Klik op Instellingen en kies Geavanceerd.



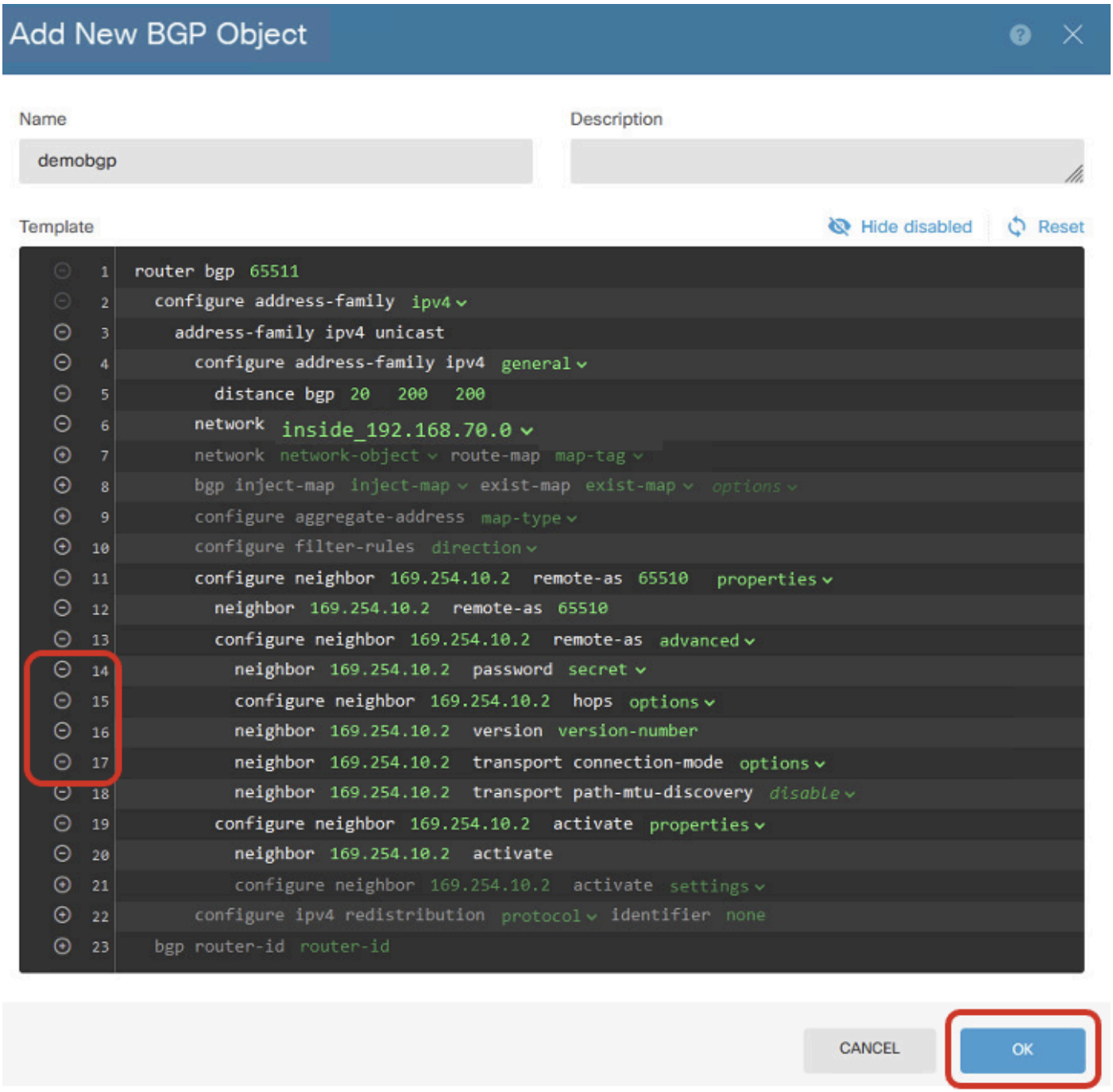
Maken_BGP_Object_NeighborSetting_Properties_Advanced

Lijn 18: Klik op opties en kies uitschakelen om MTU-detectie van pad uit te schakelen.



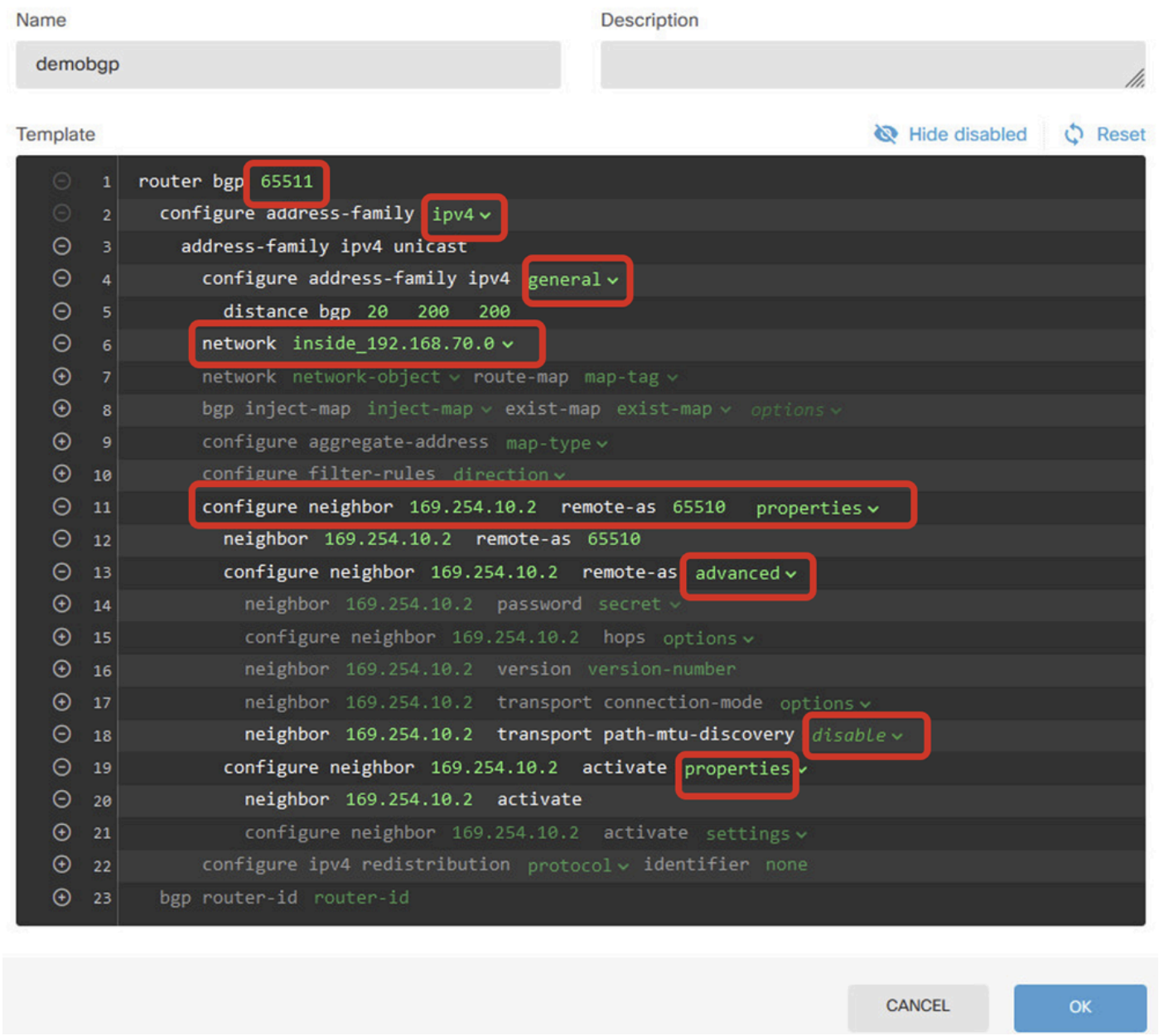
Maken_BGP_Object_NeighborSetting_Properties_Advanced_PMD

Lijn 14, 15, 16, 17: Klik op de -toets om de lijnen uit te schakelen. Klik vervolgens op de knop OK om het BGP-object op te slaan.



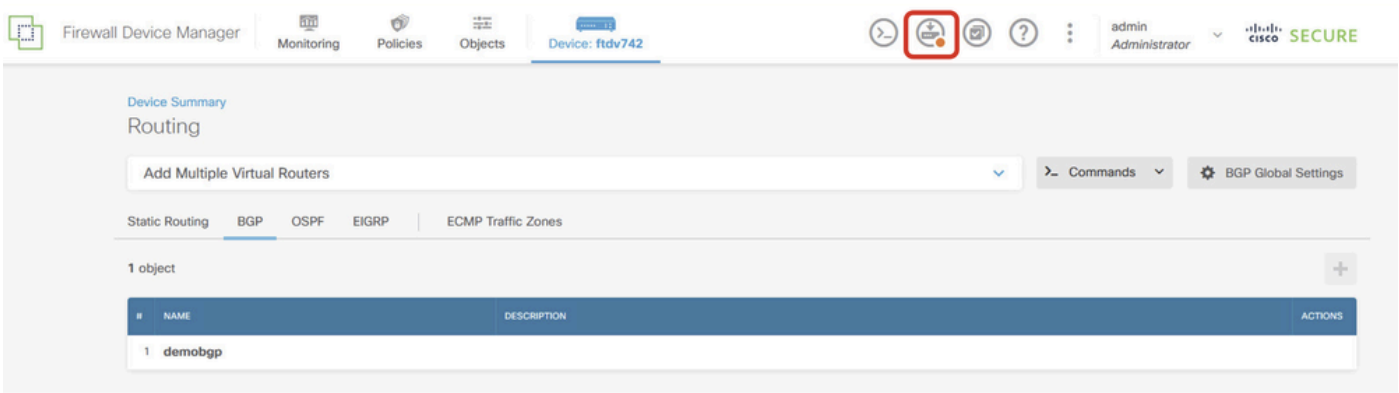
Creëer_BGP_Object_DisableLines

Dit is een overzicht van de BGP-instelling in dit voorbeeld. U kunt de andere BGP-instellingen configureren op basis van uw werkelijke behoeften.



Maken_BGP_Object_Final_Overview

Stap 7. Implementeer de BGP-configuratiewijzigingen.



Implementatie_BGP_configuratie

Stap 8. De configuratie voor Site1 FTD is nu voltooid.

Herhaal stap 3 tot en met stap 7 om Site2 FTD VPN en BGP te configureren met de bijbehorende parameters van Site2 FTD.

Configuratieoverzicht van Site1 FTD en Site2 FTD in CLI.

Site1 FTD	Site2 FTD
NGFW versie 7.4.2 interface Gigabit Ethernet0/0 nameif buiten cts-handleiding propagate sgt-conservatie-untag beleid statisch zicht uitgeschakeld vertrouwd veiligheidsniveau 0 IP-adres 192.168.30.1 255.255.255.0 interface Gigabit Ethernet0/2 nameif inside veiligheidsniveau 0 IP-adres 192.168.70.1 255.255.255.0 interfacetunnel 1 nameif demovti IP-adres 169.254.10.1 255.255.255.0 tunnelbroninterface buiten tunnelbestemming 192.168.10.1 tunnelmodus ipsec ipv4 tunnelbeveiliging ipsec-profiel ipsec_profile|e4084d322d objectnetwerk OutsideIPv4Gateway host 192.168.30.3 objectnetwerk inside_192.168.70.0 subnetnummer 192.168.70.0 255.255.255.0 algemene toegangsgroep NGFW_ONBOX_ACL toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: L5 REGEL: Inside_Outside_Rule access-list NGFW_ONBOX_ACL geavanceerde trust object-groep |acSvcg-268435457 ifc in elke ifc buiten elk regel-id 268435457 gebeurtenislogboek, beide toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435458: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id	NGFW versie 7.4.2 interface Gigabit Ethernet0/0 nameif buiten cts-handleiding propagate sgt-conservatie-untag beleid statisch zicht uitgeschakeld vertrouwd veiligheidsniveau 0 IP-adres 192.168.10.1 255.255.255.0 interface Gigabit Ethernet0/2 nameif inside veiligheidsniveau 0 IP-adres 192 168 50 1255 255 255 00 interfacetunnel 1 nameif-demovti25 IP-adres 169.254.10.2 255.255.255.0 tunnelbroninterface buiten tunnelbestemming 192.168.30.1 tunnelmodus ipsec ipv4 tunnelbeveiliging ipsec-profiel ipsec_profile|e4084d322d objectnetwerk OutsideIPv4Gateway host 192.168.10.3 objectnetwerk inside_192.168.50.0 subnetnummer 192.168.50.0 255.255.255.0 algemene toegangsgroep NGFW_ONBOX_ACL toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: L5 REGEL: Inside_Outside_Rule access-list NGFW_ONBOX_ACL geavanceerde trust object-groep |acSvcg-268435457 ifc in elke ifc buiten elk regel-id 268435457 gebeurtenislogboek, beide toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435458: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435458: L5 REGEL: Demo_allow

268435458: L5 REGEL: Demo_allow	
toegangslijst NGFW_ONBOX_ACL geavanceerde	toegangslijst NGFW_ONBOX_ACL geavanceerde
vergunningsobject-groep |acSvcg-268435458 elk regel-id	vergunningsobject-groep |acSvcg-268435458 elk regel-id
268435458-gebeurtenislogboek, zowel	268435458-gebeurtenislogboek, zowel
toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1:	toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1:
TOEGANGSBELEID: NGFW_Access_Policy	TOEGANGSBELEID: NGFW_Access_Policy
toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1: L5	toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1: L5
REGEL: DefaultActionRule	REGEL: DefaultActionRule
toegangslijst Geavanceerd NGFW_ONBOX_ACL	toegangslijst Geavanceerd NGFW_ONBOX_ACL
ontkennen ip elke regel-id 1	ontkennen ip elke regel-id 1
router bgp 65511	router bgp 65510
bgp log-buurwijzigingen	bgp log-buurwijzigingen
bgp router-id vrf automatisch toewijzen	bgp router-id vrf automatisch toewijzen
IPv4-unicast voor adresfamilie	IPv4-unicast voor adresfamilie
buur 169.254.10.2 op afstand 65510	buur 169.254.10.1 op afstand 65511
buur 169.254.10.2 transportpad-mtu-discovery uitschakelen	buur 169.254.10.1 transportpad-mtu-discovery uitschakelen
buur 169.254.10.2 activeren	buur 169.254.10.1 activeren
netwerk 192.168.70.0	netwerk 192.168.50.0
geen automatische samenvatting	geen automatische samenvatting
geen synchronisatie	geen synchronisatie
exit-address-family	exit-address-family
route buiten 0.0.0.0 0.0.0 192.168.30.3 1	route buiten 0.0.0.0 0.0.0 192.168.10.3 1
crypto ipsec ikev2 ipsec-voorstel AES256_SHA256	crypto ipsec ikev2 ipsec-voorstel AES256_SHA256
ESP-encryptie protocol aes-256 aes	ESP-encryptie protocol aes-256 aes
protocol ESP-integriteit sha-256 sha-1	protocol ESP-integriteit sha-256 sha-1
crypto ipsec-profiel ipsec_profile|e4084d322d	crypto ipsec-profiel ipsec_profile|e4084d322d
set ikev2 ipsec-voorstel AES256_SHA256	set ikev2 ipsec-voorstel AES256_SHA256
instellen security-associatie-levensduur kilobytes 4608000	instellen security-associatie-levensduur kilobytes 4608000
instellen security-associatielevensduur seconden 28800	instellen security-associatielevensduur seconden 28800
crypto ipsec security-association pmtu-aging oneindig	crypto ipsec security-association pmtu-aging oneindig
crypto ikev2-beleid 1	crypto ikev2-beleid 1
encryptie aes-256 aes	encryptie aes-256 aes
integriteit sha256 sha	integriteit sha256 sha
groep 14	groep 14
prf sha256 sha	prf sha256 sha
levenslange 86400	levenslange 86400
crypto ikev2-beleid 20	crypto ikev2-beleid 20
encryptie aes-256 aes-192 aes	encryptie aes-256 aes-192 aes
integriteit sha512 sha384 sha256 sha	integriteit sha512 sha384 sha256 sha
groep 21 20 16 15 14	groep 21 20 16 15 14

prf sha512 sha384 sha256 sha levenslange 86400 crypto ikev2 activeren buiten groepsbeleid |s2sGP|192.168.10.1 intern groepsbeleid |s2sGP|192.168.10.1 eigenschappen VPN-tunnelprotocol ikev2 tunnelgroep 192.168.10.1 type ipsec-l2l tunnelgroep 192.168.10.1 algemene kenmerken standaardgroepsbeleid |s2sGP|192.168.10.1 tunnel-groep 192.168.10.1 ipsec-eigenschappen ikev2-***** voor verificatie op afstand vooraf met gedeelde sleutel ikev2-***** voor lokale verificatie met gedeelde sleutel	prf sha512 sha384 sha256 sha levenslange 86400 crypto ikev2 activeren buiten groepsbeleid |s2sGP|192.168.30.1 intern groepsbeleid |s2sGP|192.168.30.1 eigenschappen VPN-tunnelprotocol ikev2 tunnel-groep 192.168.30.1 type ipsec-l2l tunnelgroep 192.168.30.1 algemene kenmerken standaardgroepsbeleid |s2sGP|192.168.30.1 tunnel-groep 192.168.30.1 ipsec-eigenschappen ikev2-***** voor verificatie op afstand vooraf met gedeelde sleutel ikev2-***** voor lokale verificatie met gedeelde sleutel

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Stap 1. Navigeer naar de CLI van elk FTD via console of SSH om de VPN-status van fase 1 en fase 2 te verifiëren via de opdrachten tonen crypto ikev2 sa en tonen crypto ipsec sa.

Site1 FTD	Site2 FTD
ftdv742# toont crypto ikev2 sa IKEv2 SA's: Session-id:134, status:UP-ACTIVE, IKE-telling:1, KINDERTELLING:1 Tunnel-id lokale externe FVRF/ivrf-statusrol 563984431 192.168.30.1/500 192.168.10.1/500 Global/Global Ready-responder Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Leven/actieve tijd: 86400/5145 sec Kinderslot: lokale keuzeschakelaar 0.0.0.0/0 - 25.255.255.255/65535 externe selector 0.0.0.0/0 - 25.255.255.255/65535	ftdv742# toont crypto ikev2 sa IKEv2 SA's: Session-id:13, status:UP-ACTIVE, IKE-telling:1, KINDERTELLING:1 Tunnel-id lokale externe FVRF/ivrf-statusrol 339797985 192.168.10.1/500 192.168.30.1/500 Initiator voor wereldwijde/wereldwijde voorbereiding Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Leven/actieve tijd: 86400/74099 sec Kinderslot: lokale keuzeschakelaar 0.0.0.0/0 - 25.255.255.255/65535 externe selector 0.0.0.0/0 - 25.255.255.255/65535 ESP spi in/uit: 0xb7b5b38b/0xf0c4239d

ESP spi in/uit: 0xf0c4239d/0xb7b5b38b	
ftdv742# toont crypto ipsec sa interface: demovti Crypto map tag: __vti-crypto-map-Tunnel1-0-1, volgnummer: 65280, lokaal adres: 192.168.30.1 Protected vrf (ivrf): Wereldwijd lokaal nummer (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) afstandsbediening (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1 #pkts encaps: 5720, #pkts versleutelen: 5720, #pkts overzicht: 5720 #pkts decaps: 5717, #pkts decrypt: 5717, #pkts verifieer: 5717 #pkts gecomprimeerd: 0, #pkts gedecompresseerd: 0 #pkts niet gecomprimeerd: 5720, #pkts comp mislukt: 0, #pkts decomp mislukt: 0 #pre-frag successen: 0, #pre-frag mislukkingen: 0, #fragments gecreëerd: 0 #PMTUs verzonden: 0, #PMTUs rcvd: 0, #decapsulated eieren die hermontage nodig hebben: 0 #TFC rcvd: 0, #TFC verzonden: 0 #Valid ICMP-fouten rcvd: 0, #Invalid ICMP-fouten rcvd: 0 #send fouten: 0, #recv fouten: 0 lokale crypto-endpt: 192.168.30.1/500, externe crypto-endpt: 192.168.10.1/500 pad mtu 1500, ipsec overhead 78(44), media mtu 1500 PMTU tijd resterend (sec): 0, DF-beleid: copy-df ICMP-foutvalidatie: uitgeschakeld, TFC-pakketten: uitgeschakeld huidige uitgaande spi: B7B5B38B huidige inkomende spi: F0C4239D inkomende esp sas: Centrifugeren: 0xF0C4239D (4039386013)	ftdv742# toont crypto ipsec sa interface: demovti25 Crypto map tag: __vti-crypto-map-Tunnel1-0-1, volgnummer: 65280, lokaal adres: 192.168.10.1 Protected vrf (ivrf): Wereldwijd lokaal nummer (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) afstandsbediening (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1 #pkts encaps: 5721, #pkts versleutelen: 5721, #pkts overzicht: 5721 #pkts decaps: 5721, #pkts decrypt: 5721, #pkts verifieer: 5721 #pkts gecomprimeerd: 0, #pkts gedecompresseerd: 0 #pkts niet gecomprimeerd: 5721, #pkts comp mislukt: 0, #pkts decomp mislukt: 0 #pre-frag successen: 0, #pre-frag mislukkingen: 0, #fragments gecreëerd: 0 #PMTUs verzonden: 0, #PMTUs rcvd: 0, #decapsulated eieren die hermontage nodig hebben: 0 #TFC rcvd: 0, #TFC verzonden: 0 #Valid ICMP-fouten rcvd: 0, #Invalid ICMP-fouten rcvd: 0 #send fouten: 0, #recv fouten: 0 lokale crypto-endpt: 192.168.10.1/500, externe crypto-endpt: 192.168.30.1/500 pad mtu 1500, ipsec overhead 78(44), media mtu 1500 PMTU tijd resterend (sec): 0, DF-beleid: copy-df ICMP-foutvalidatie: uitgeschakeld, TFC-pakketten: uitgeschakeld huidige uitgaande spi: F0C4239D actuele inkomende spi: B7B5B38B inkomende esp sas: SPI: 0xB7B5B38B (3082138507)

SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen ={L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (4285389/3722) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0xFFFFFF 0xFFFF uitgaande bse: SPI: 0xB7B5B38B (3082138507) SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen ={L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (4147149/3722) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0x00000000 0x00000001	SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen ={L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (3962829/3626) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0xFFFFFF 0xFFFF uitgaande bse: Centrifugeren: 0xF0C4239D (4039386013) SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen ={L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (4101069/3626) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0x00000000 0x00000001

Stap 2. Navigeer naar de CLI van elk FTD via console of SSH om de BGP status te verifiëren met behulp van de opdrachten tonen bgp buren en tonen route bgp.

Site1 FTD	Site2 FTD
ftdv742# toont bgp-buren BGP-buur is 169.254.10.2, vrf single_vf, extern AS-65510, externe link BGP versie 4, externe router-ID 192.168.50.1 BGP-status = ingesteld, tot 1 d20 uur Laatste gelezen 00:00:25, laatste schrijven 00:00:45, de tijd van de greep is 180, keepalive interval is 60 seconden Buursessies: 1 actief, is niet geschikt voor meerdere sessies (uitgeschakeld)	ftdv742# toont bgp-buren BGP-buur is 169.254.10.1, vrf single_vf, extern AS-65511, externe link BGP versie 4, externe router-ID 192.168.70.1 BGP-status = ingesteld, tot 1 d20 uur Laatste gelezen 00:00:11, laatste schrijven 00:00:52, de tijd van de greep is 180, keepalive interval is 60 seconden Buursessies: 1 actief, is niet geschikt voor meerdere sessies (uitgeschakeld)

Buurmogelijkheden: Routevernieuwing: geadverteerd en ontvangen(nieuw) Vier-octetten ASN Capability: geadverteerd en ontvangen IPv4 Unicast-adresfamilie: geadverteerd en ontvangen Multisessievermogen: Berichtstatistieken: InQ diepte is 0 OutQ-diepte is 0 Verzonden RCVD Opent: 1 1 Kennisgevingen: 0 0 Updates: 2.2 Keepalives: 2423 2427 Routevernieuwing: 0,0 Totaal: 2426 2430 De minimale tijd tussen het maken van een advertentie is 30 seconden. Voor adresfamilie: IPv4 Unicast Sessie: 169.254.10.2 BGP-tabelversie 3, buurversie 3/0 Grootte van uitvoerwachtrij : 0 Indexnummer 1 1 lid van de updategroep Verzonden RCVD Prefixactiviteit: ---- ---- Huidige prefixes: 1 1 (gebruikt 80 bytes) Totaal: 1 1 Stilzwijgende intrekking: 0 0 Expliciet terugtrekken: 0 0 Gebruikt als beste pad: n.v.t. 1 Gebruikt als multipath: n/a 0 Uitgaand inkomend Prefixes bij lokaal beleid geweigerd: -------- ------- Bestpath van deze peer: 1 n/a Totaal: 1 0 Aantal NLRI's in de verstuurde update: max 1, min 0 Het bijhouden van adressen is ingeschakeld, de RIB heeft een route naar 169.254.10.2	Buurmogelijkheden: Routevernieuwing: geadverteerd en ontvangen(nieuw) Vier-octetten ASN Capability: geadverteerd en ontvangen IPv4 Unicast-adresfamilie: geadverteerd en ontvangen Multisessievermogen: Berichtstatistieken: InQ diepte is 0 OutQ-diepte is 0 Verzonden RCVD Opent: 1 1 Kennisgevingen: 0 0 Updates: 2.2 Keepalives: 2424 2421 Routevernieuwing: 0,0 Totaal: 2427 2424 De minimale tijd tussen het maken van een advertentie is 30 seconden. Voor adresfamilie: IPv4 Unicast Sessie: 169 254 10.1 BGP-tabelversie 9, buurversie 9/0 Grootte van uitvoerwachtrij : 0 Indexnummer 4 4 update-groep lid Verzonden RCVD Prefixactiviteit: ---- ---- Huidige prefixes: 1 1 (gebruikt 80 bytes) Totaal: 1 1 Stilzwijgende intrekking: 0 0 Expliciet terugtrekken: 0 0 Gebruikt als beste pad: n.v.t. 1 Gebruikt als multipath: n/a 0 Uitgaand inkomend Prefixes bij lokaal beleid geweigerd: -------- ------- Bestpath van deze peer: 1 n/a Totaal: 1 0 Aantal NLRI's in de verstuurde update: max 1, min 0 Het bijhouden van adressen is ingeschakeld, de RIB heeft een route naar 169.254.10.1

Aansluitingen vastgelegd 1; gevallen 0 Laatste reset nooit Transport (TCP) pad-mtu-detectie is uitgeschakeld Naadloze herstart is uitgeschakeld	Aansluitingen vastgelegd 4; gevallen 3 Laatst gereset 1d21h, vanwege interfaceklep van sessie 1 Transport (TCP) pad-mtu-detectie is uitgeschakeld Naadloze herstart is uitgeschakeld
ftdv742# toont route bgp Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2 E1 - OSPF extern type 1, E2 - OSPF extern type 2, V - VPN i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2 ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker o - ODR, P - periodieke gedownloade statische route, + - replicated route SI - Statische InterVRF, BI - BGP InterVRF Gateway of last resort is 192.168.30.3 naar netwerk 0.0.0.0 B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h	ftdv742# toont route bgp Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2 E1 - OSPF extern type 1, E2 - OSPF extern type 2, V - VPN i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2 ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker o - ODR, P - periodieke gedownloade statische route, + - replicated route SI - Statische InterVRF, BI - BGP InterVRF Gateway of last resort is 192.168.10.3 naar netwerk 0.0.0.0 B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h

Stap 3. Site1-client en Site2-client pingen elkaar met succes.

Site1-client:

```
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
```

Site2-client:

```
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
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

U kunt deze debug-opdrachten gebruiken om de VPN-sectie probleemoplossing te bieden.

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

U kunt deze debug commando's gebruiken om de BGP sectie op te lossen.

```
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>
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.