Configureer dubbele actieve route-gebaseerde site-to-site VPN met PBR op FTD die door FDM wordt beheerd

Inhoud

Inleiding

Dit document beschrijft hoe u dubbele actieve route-gebaseerde site-to-site VPN kunt configureren met PBR op FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van VPN
- Basis begrip van op beleid gebaseerde routing (PBR)
- Basiskennis van Internet Protocol Service Level Agreement (IP SLA)
- 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

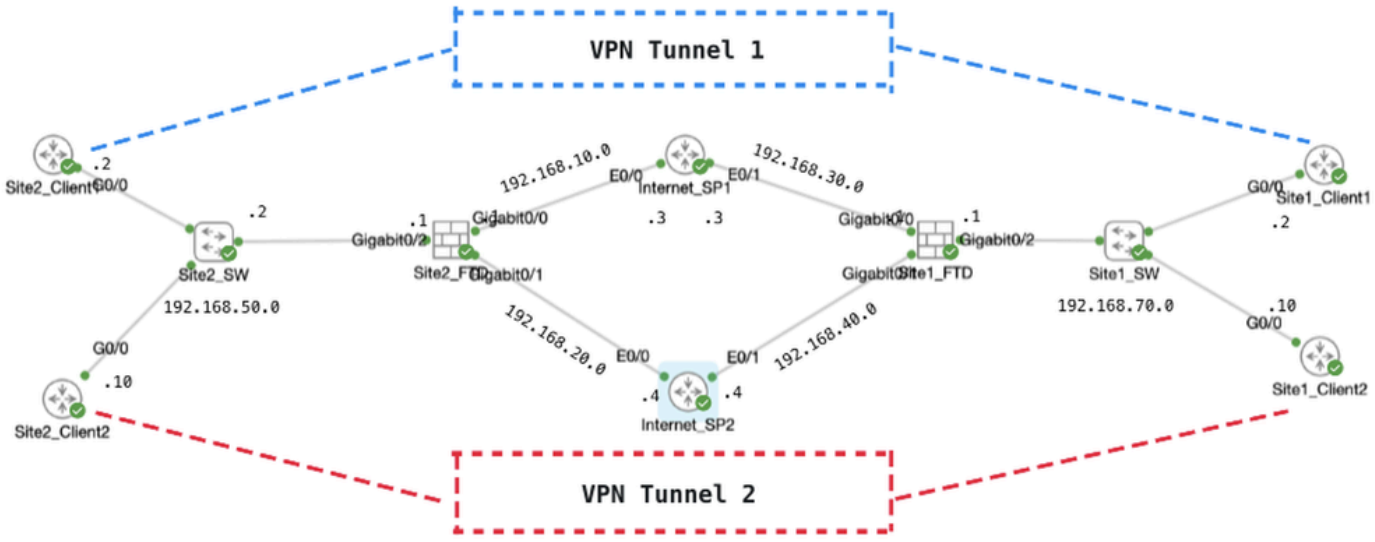
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document legt uit hoe u een dubbele actieve route-gebaseerde site-to-site VPN op FTD kunt configureren. In dit voorbeeld hebben FTDs op zowel Site1 als Site2 dubbele actieve ISP-verbindingen die de site-to-site VPN met beide ISPs tegelijk tot stand brengen. Standaard wordt Tunnel 1 van VPN-verkeer via ISP1 (blauwe lijn) verzonden. Voor specifieke hosts gaat het verkeer door Tunnel 2 via ISP2 (rode lijn). Als ISP1 een onderbreking ervaart, verkeers switches aan ISP2 als steun. Omgekeerd, als ISP2 een onderbreking ervaart, verkeers switches aan ISP1 als steun. Op beleid gebaseerde routing (PBR) en Internet Protocol Service Level Agreement (IP SLA) worden in dit voorbeeld gebruikt om aan deze vereisten te voldoen.

Configureren

Netwerkdiagram



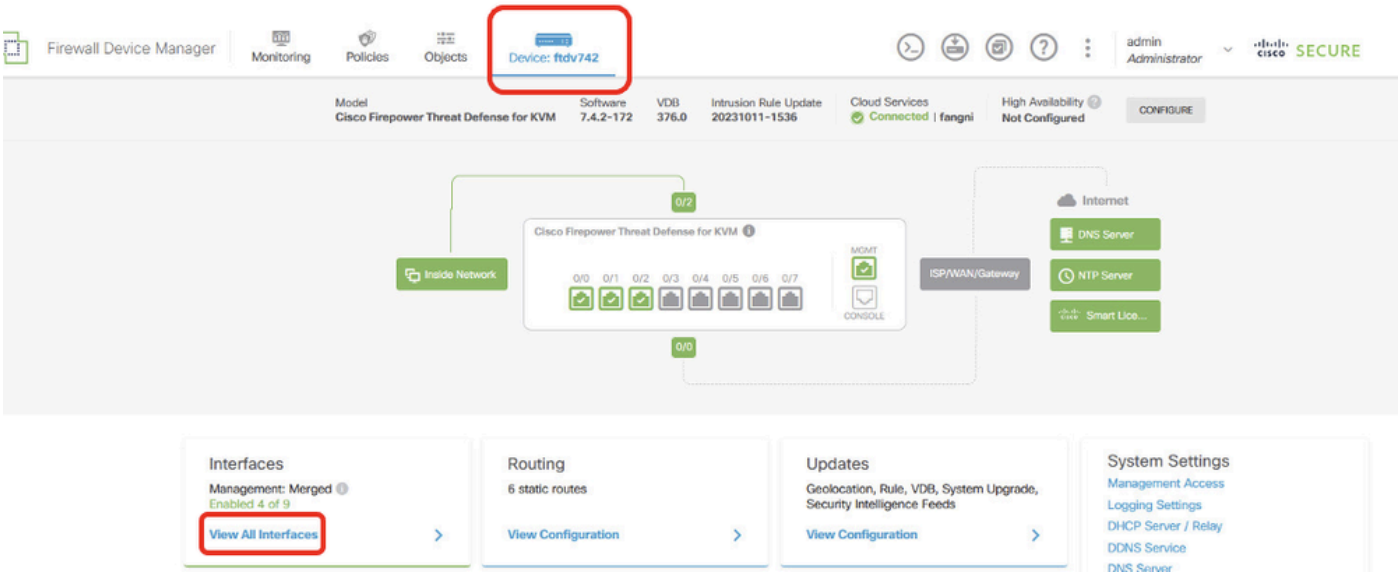
Topologie

Configuraties op VPN

Het is van essentieel belang ervoor te zorgen dat de voorlopige configuratie van IP-interconnectiviteit tussen knooppunten naar behoren is voltooid. De clients in zowel Site1 als Site2 zijn met FTD binnen IP adres als gateway.

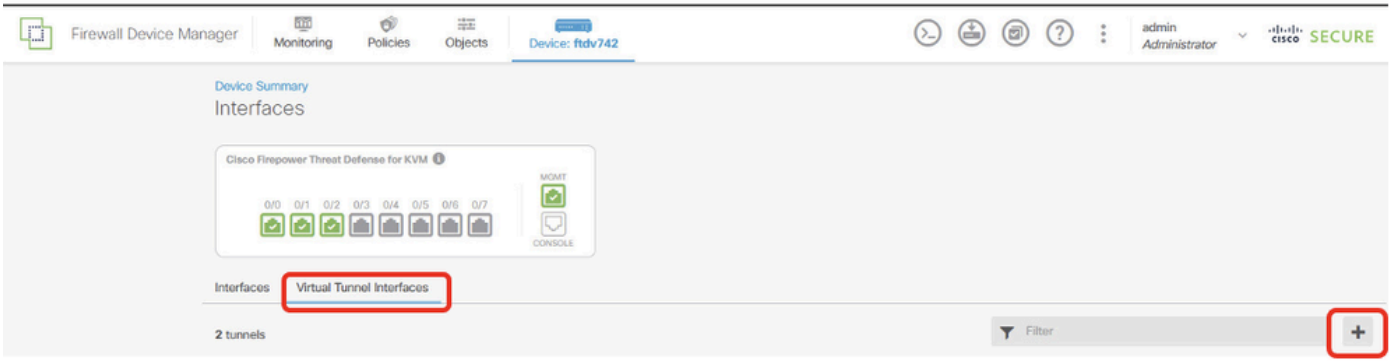
Configuratie van Site1 FTD VPN

Stap 1. Maak virtuele tunnelinterfaces voor ISP1 en ISP2. Login de FDM GUI van Site1 FTD. Navigeer naar Apparaat > Interfaces. Klik op Alle interfaces weergeven.



Site1FTD_View_All_Interfaces

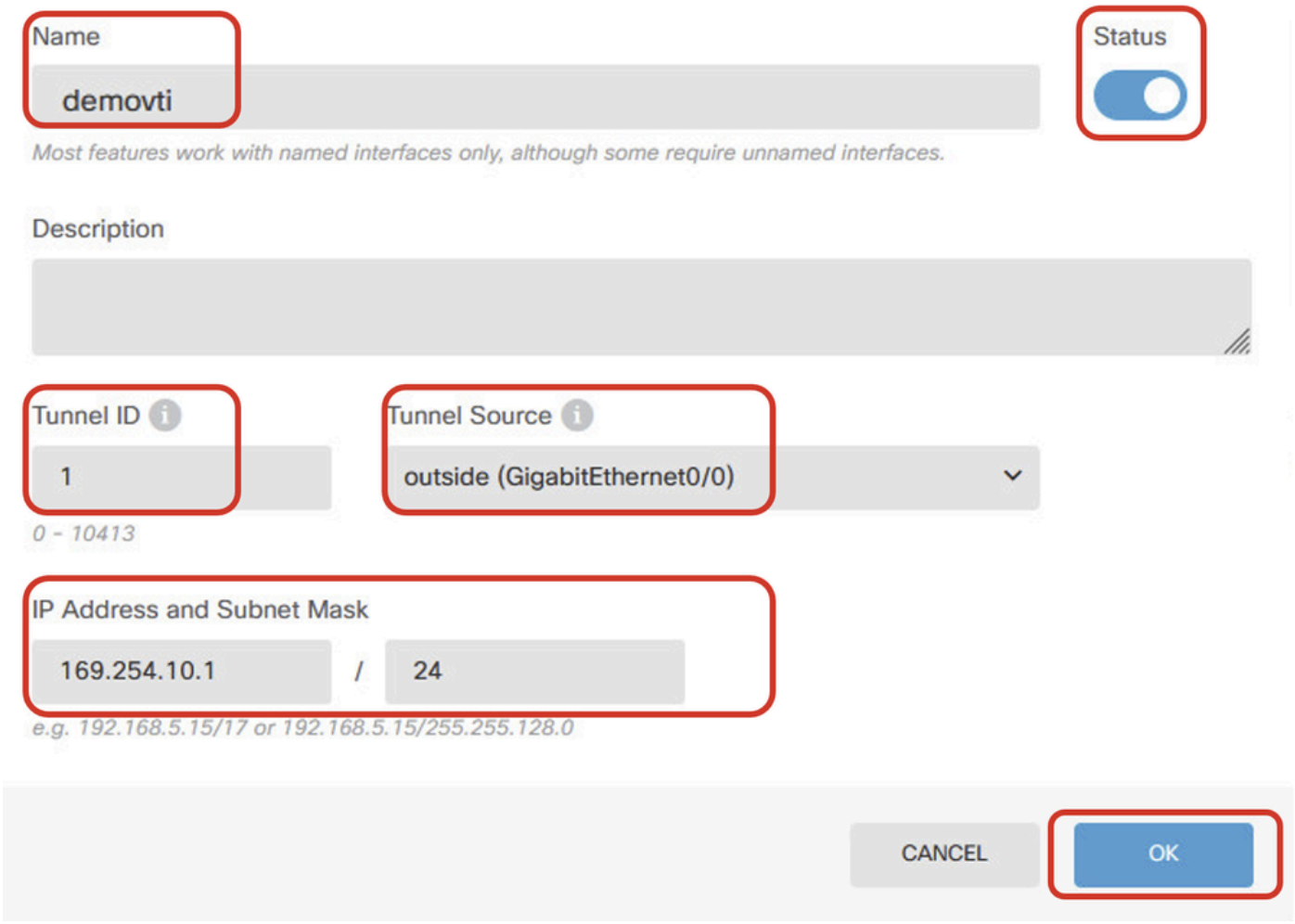
Stap 2. Klik op het tabblad Virtuele tunnelinterfaces en vervolgens op de knop +.



Site1FTD_Create_VTI

Stap 3. Verstrek de nodige informatie over de VTI-gegevens. Klik op de knop OK.

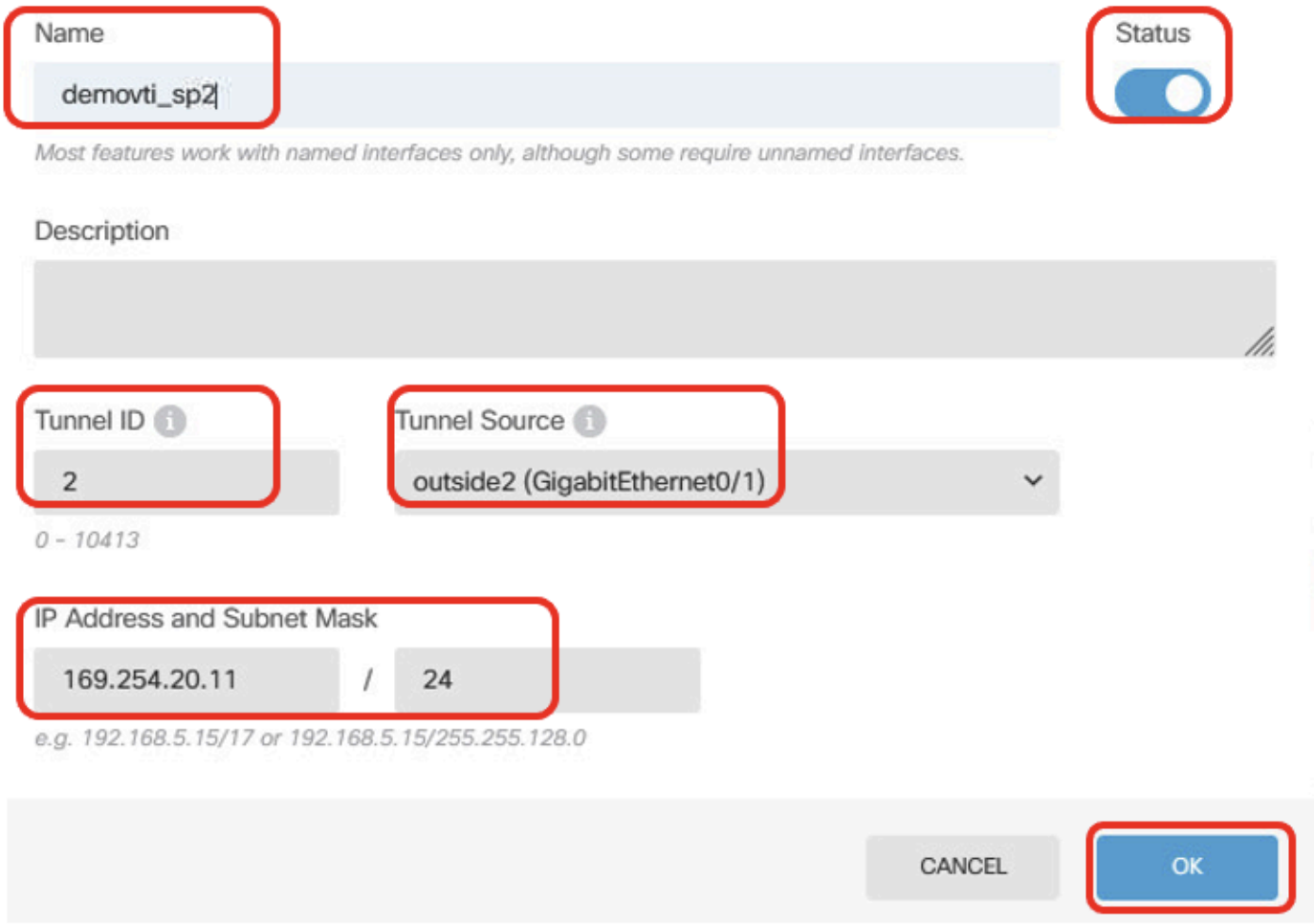
- Naam: demovti
- Tunnel-ID: 1
- Tunnelbron: buiten (Gigabit Ethernet0/0)
- IP-adres en subnetmasker: 169.254.10.1/24
- Status: klik op de schuifschakelaar om de positie Ingeschakeld te selecteren



Site1FTD_VTI_Details_Tunnel1_ISP1

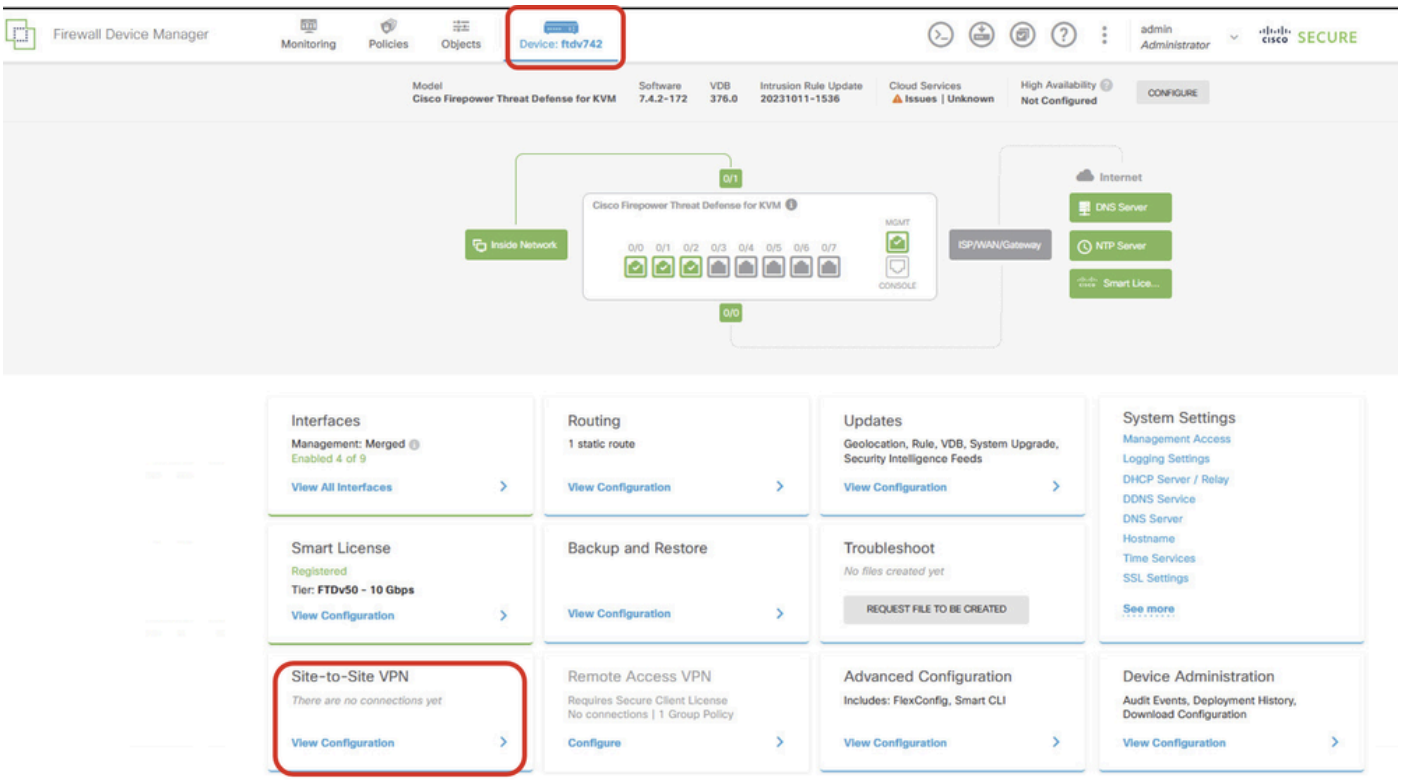
- Naam: demovti_sp2
- Tunnel-ID: 2

- Tunnelbron: buiten2 (Gigabit Ethernet0/1)
- IP-adres en subnetmasker: 169.254.20.11/24
- Status: klik op de schuifschakelaar om de positie Ingeschakeld te selecteren



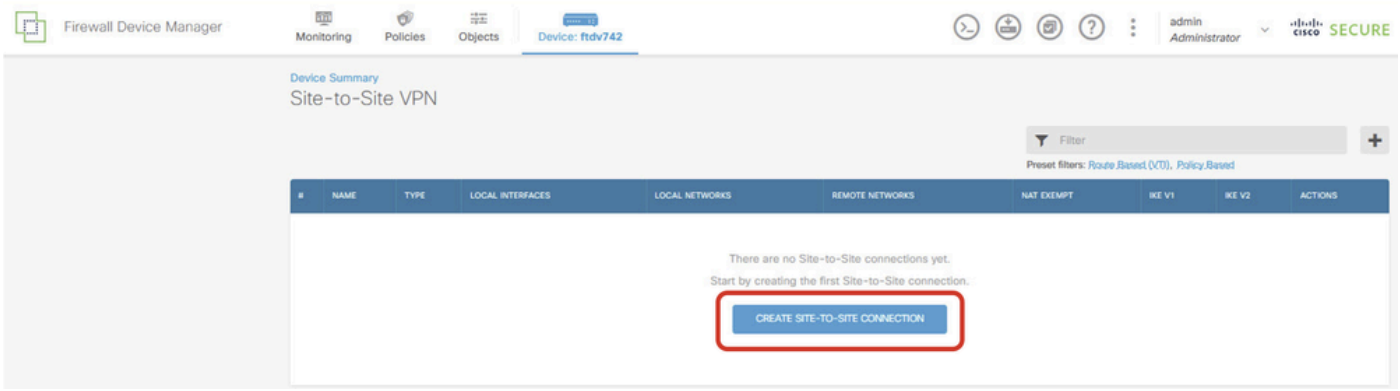
Site1FTD_VTI_Details_Tunnel2_ISP2

Stap 4. Navigeer naar apparaat > Site-to-Site VPN. Klik op de knop Configuratie bekijken.



Site1FTD_View_Site2Site_VPN

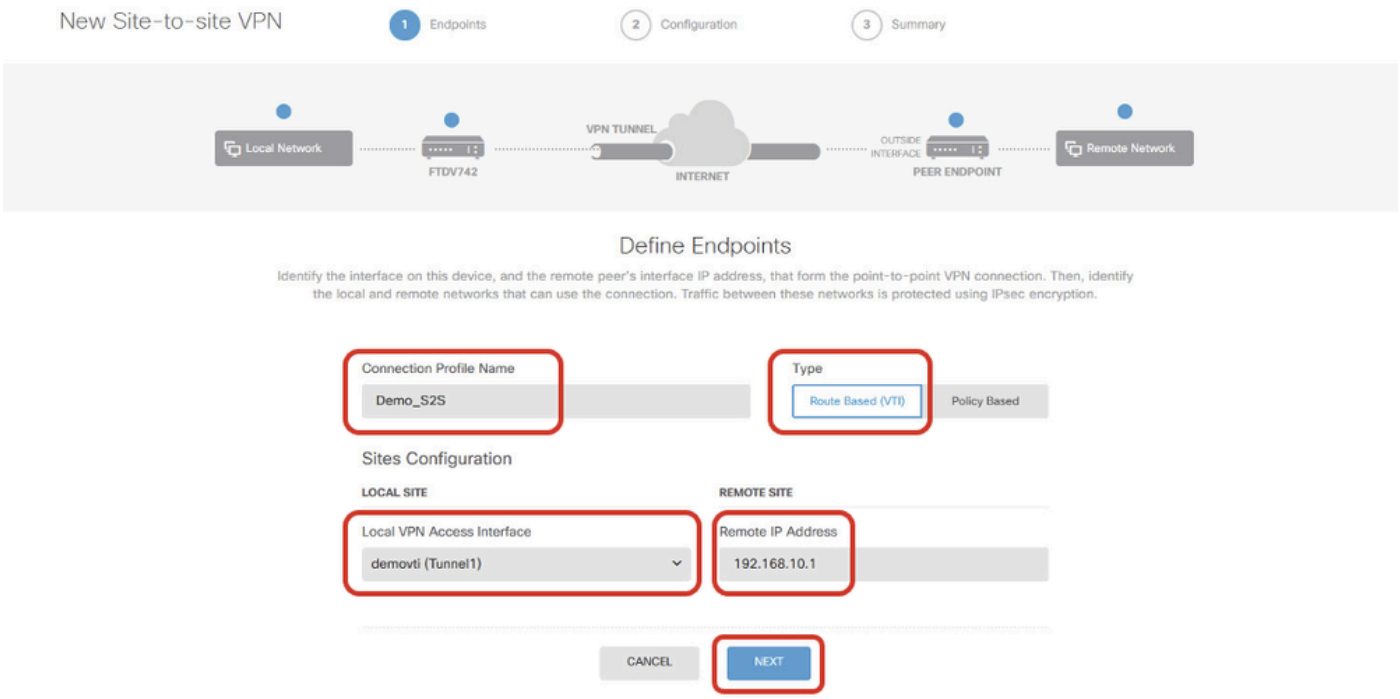
Stap 5. Start het maken van nieuwe site-to-site VPN via ISP1. Klik op CREATE SITE-TO-SITE CONNECTION knop of klik op de + knop.



Site1FTD_Create_Site-to-Site_Connection

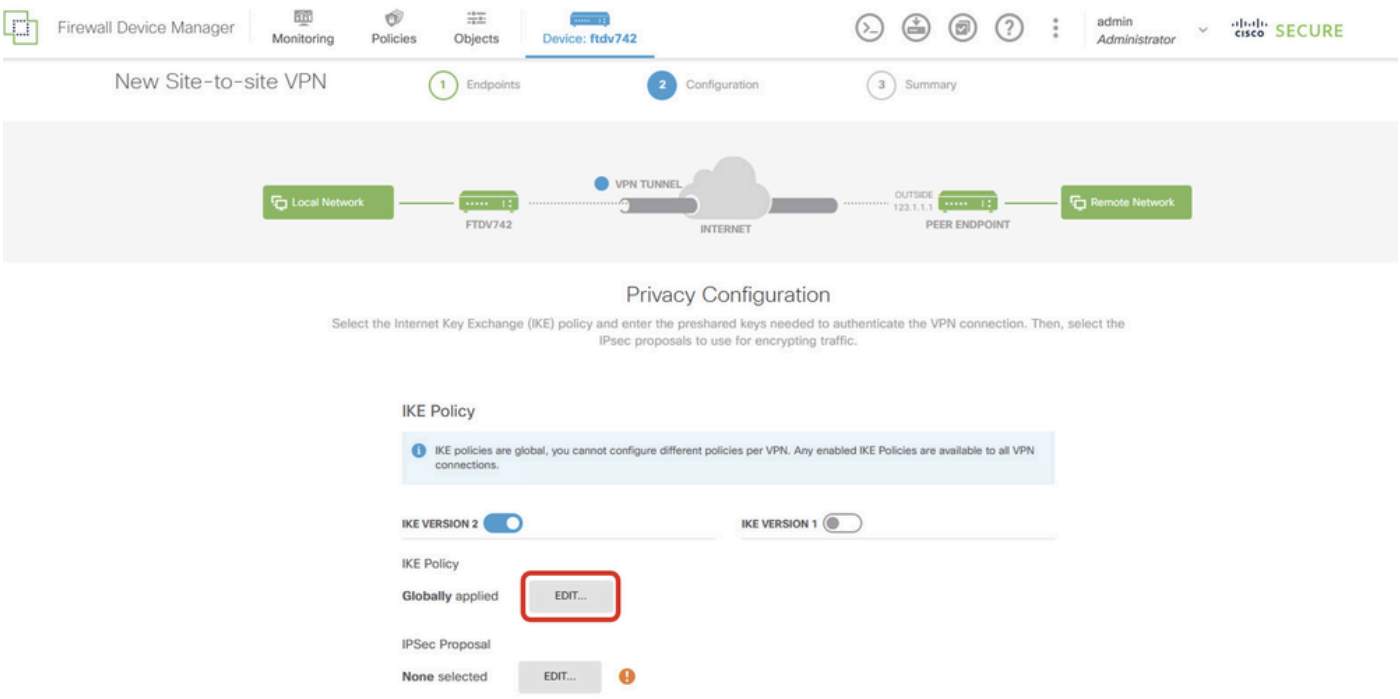
Stap 5.1. Verstrek de nodige informatie over endpoints. Klik op VOLGENDE knop.

- Naam verbindingsprofiel: Demo_S2S
- Type: Routegebaseerde (VTI)
- Lokale VPN-toegangsinterface: demovti (gemaakt in stap 3.)
- Remote IP-adres: 192.168.10.1 (dit is Site2 FTD/ISP1 IP-adres)



Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

Stap 5.2. Navigeren naar IKE-beleid. Klik op DE knop BEWERKEN.

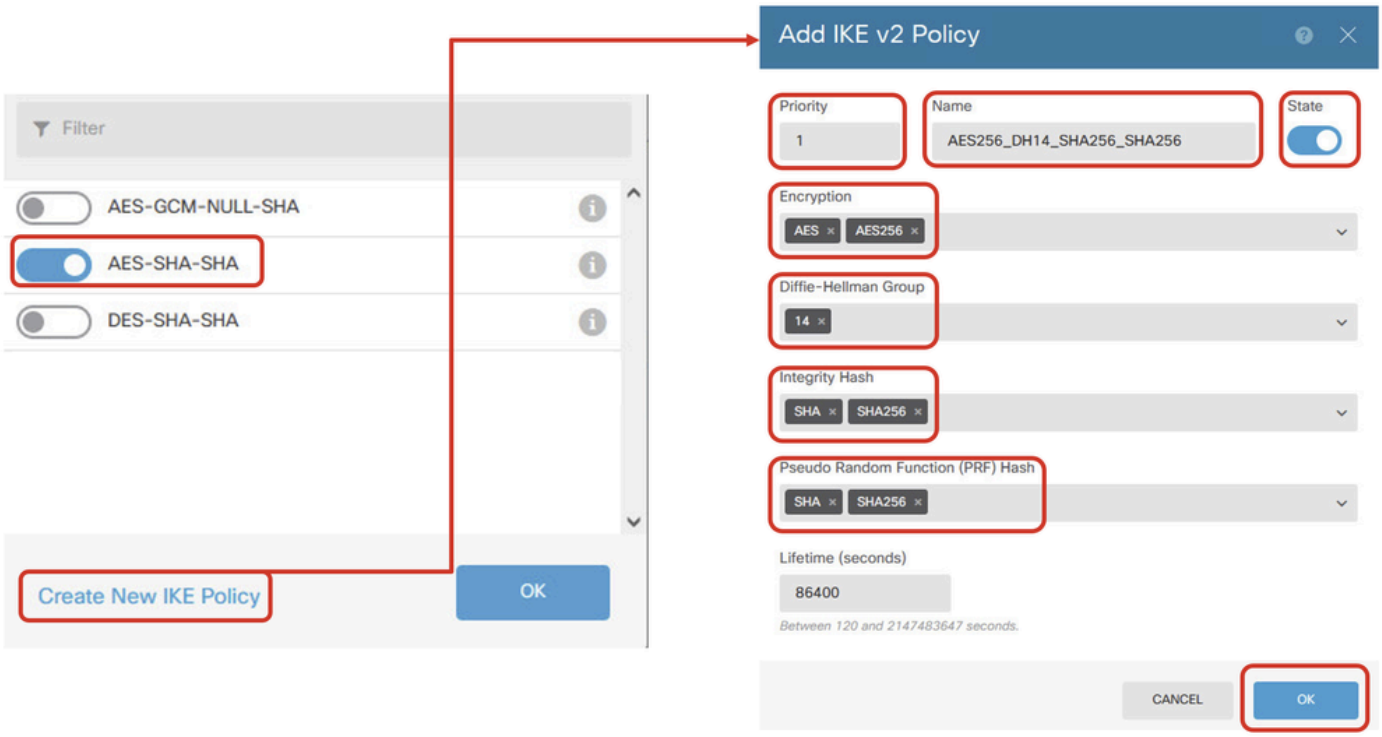


Site1FTD_Edit_IKE_Policy

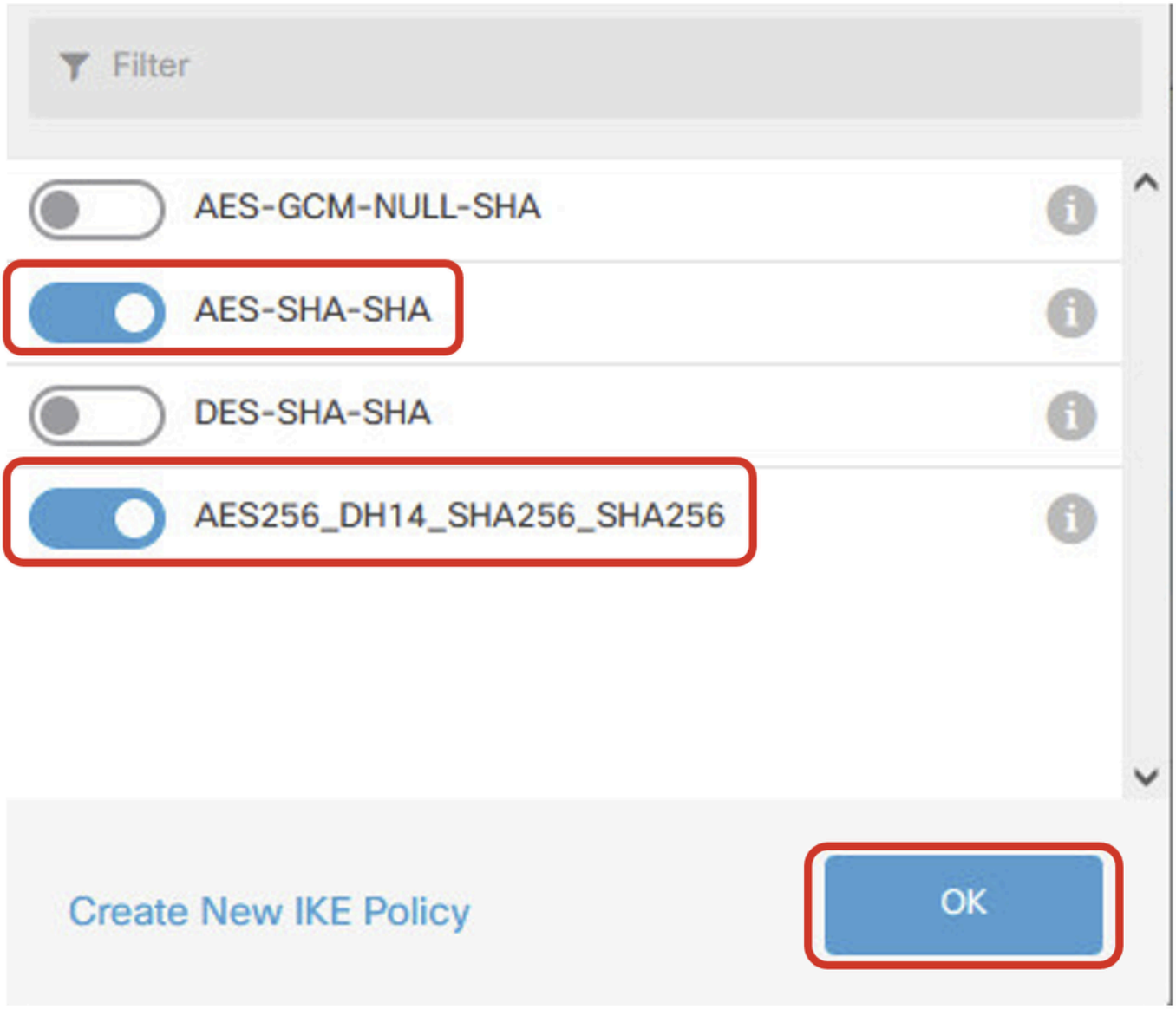
Stap 5.3. Voor IKE-beleid kunt u vooraf gedefinieerde gebruiken of u kunt een nieuwe maken door op Nieuw IKE-beleid maken te klikken.

In dit voorbeeld, schakel een bestaand IKE-beleid AES-SHA-SHA en creëer ook een nieuwe voor demo doeleinden. Klik op OK om op te slaan.

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

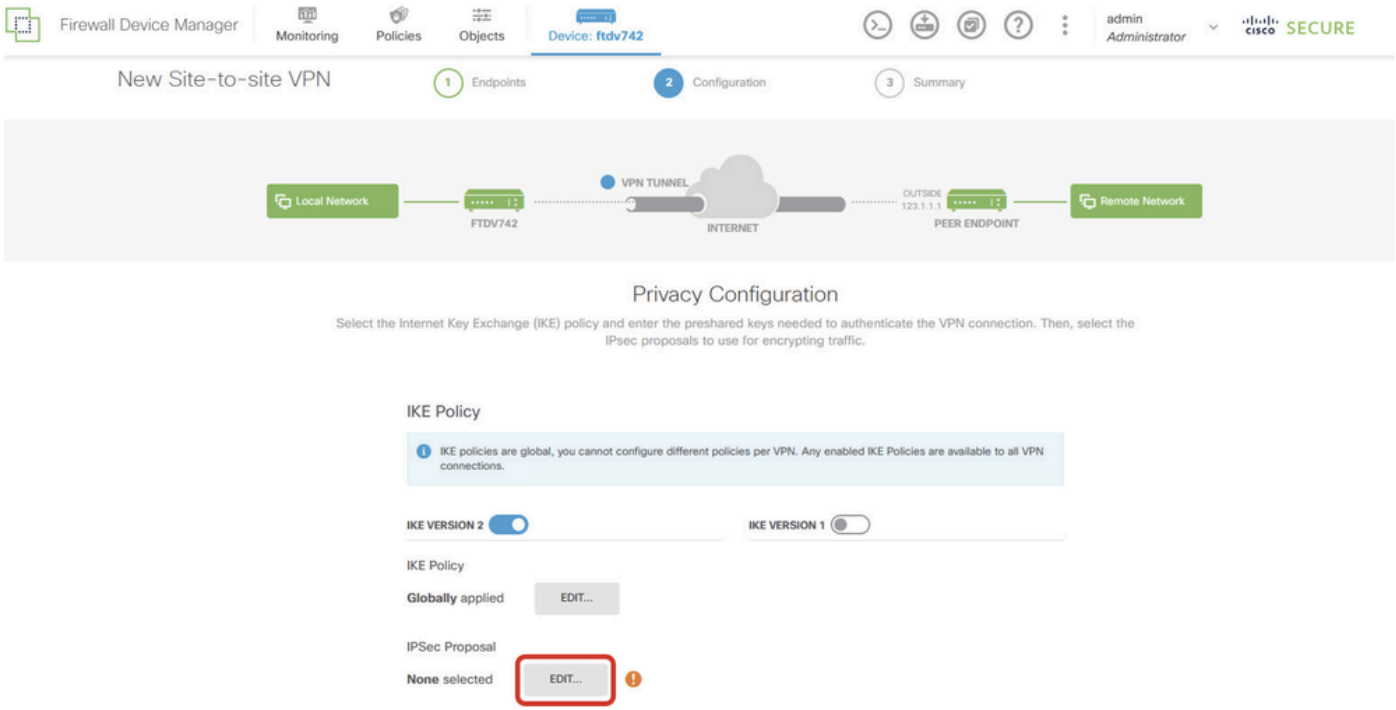


Site1FTD_Add_New_IKE_Policy



Site1FTD_Enable_New_IKE_Policy

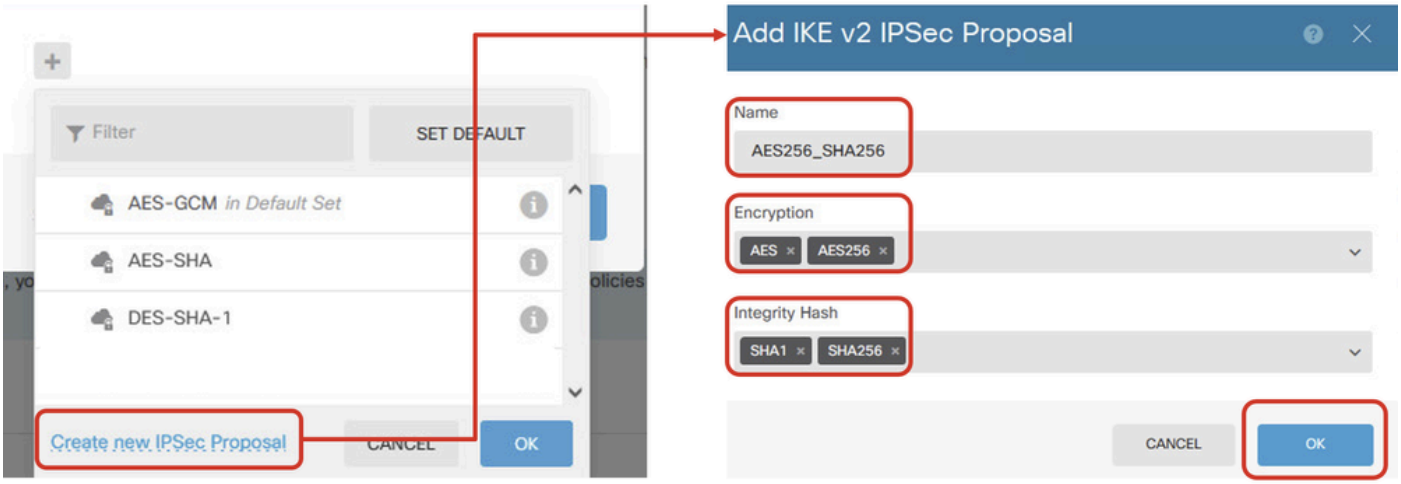
Stap 5.4. Navigeren naar het IPSec-voorstel. Klik op DE knop BEWERKEN.



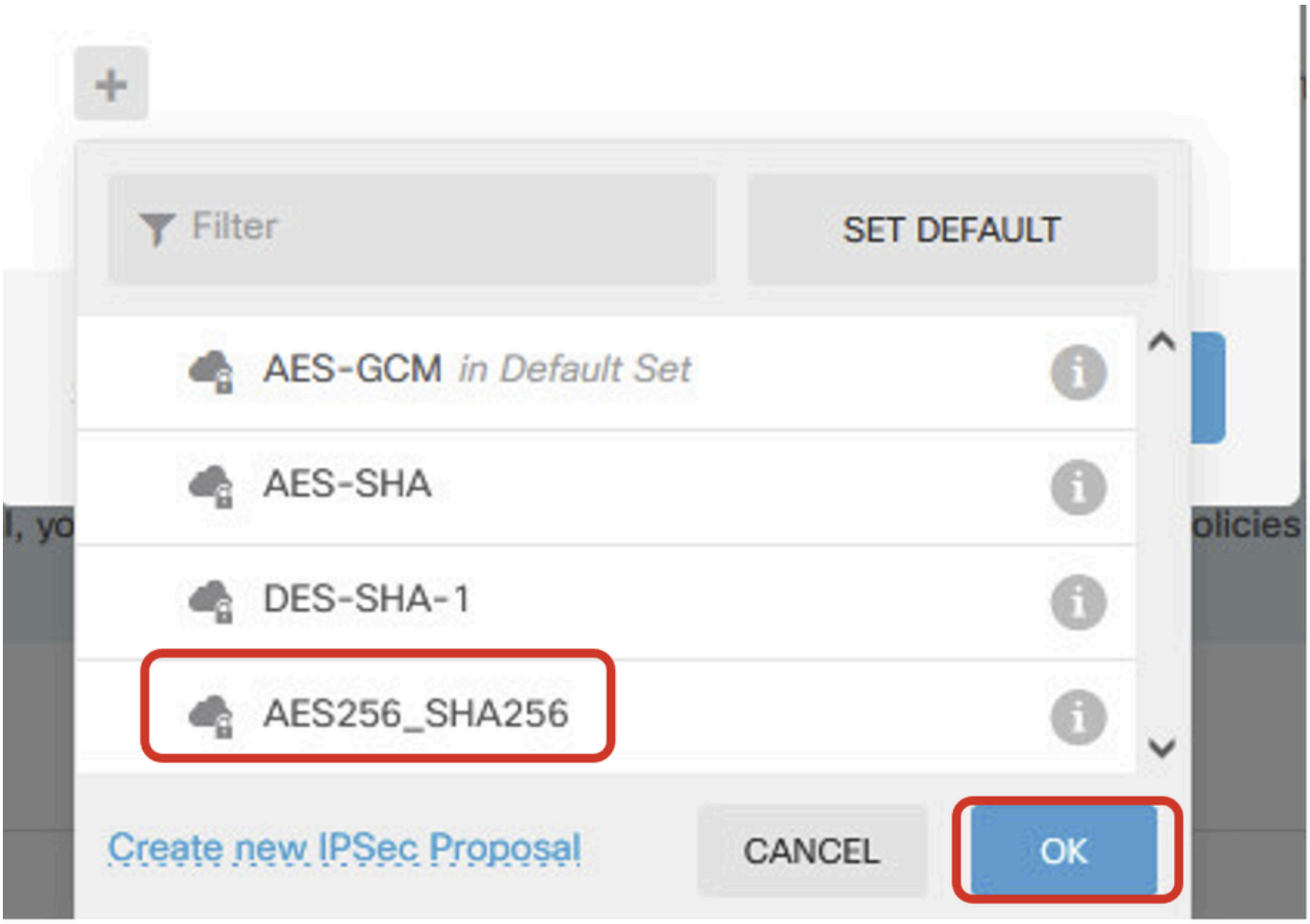
Site1FTD_Edit_IKE_Proposal

Stap 5.5. Voor een IPSec-voorstel kunt u vooraf gedefinieerde bestanden gebruiken of een nieuwe maken door op Nieuw IPSec-voorstel maken te klikken. In dit voorbeeld, maak een nieuwe voor demo doel. Klik op OK om op te slaan.

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



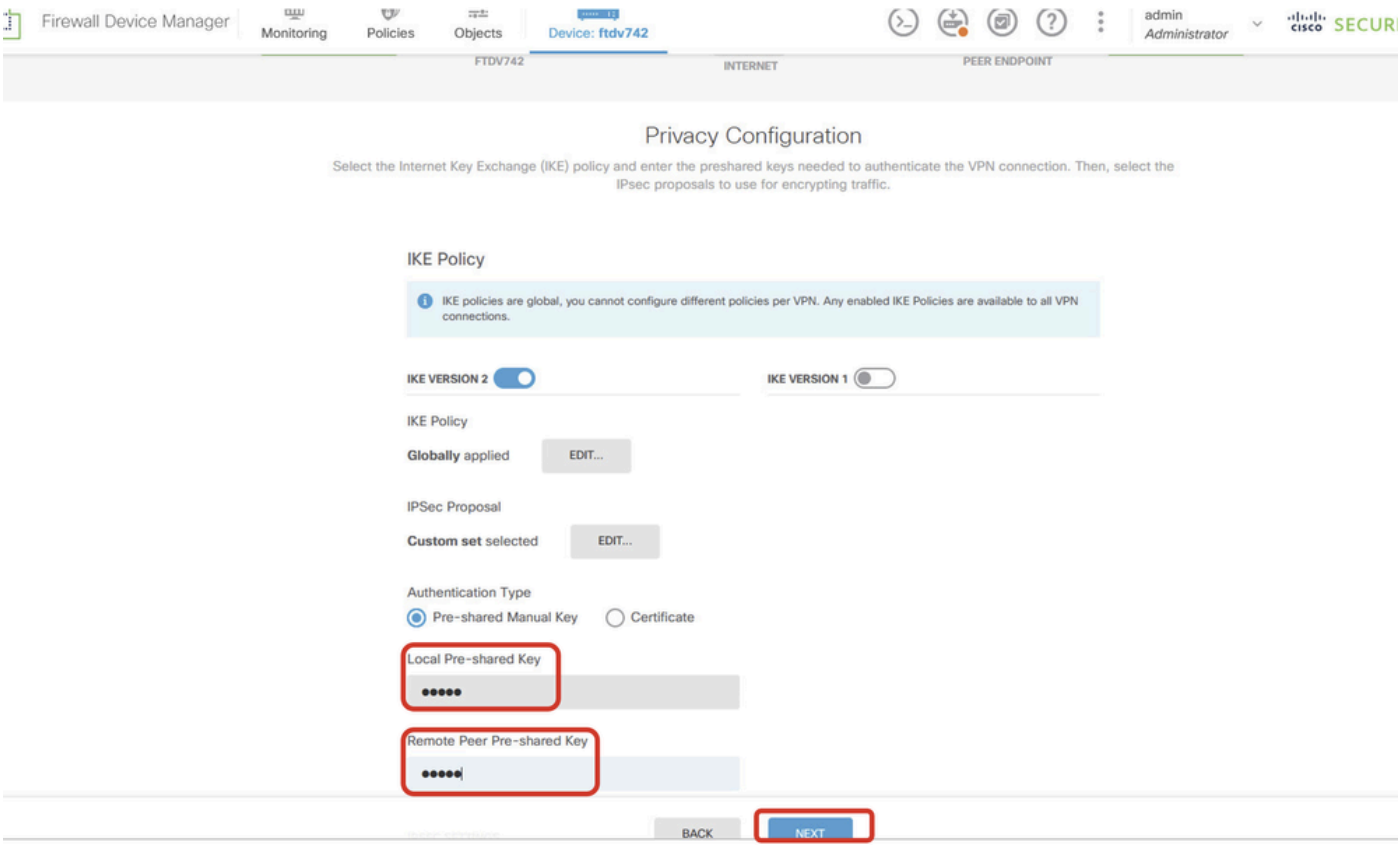
Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

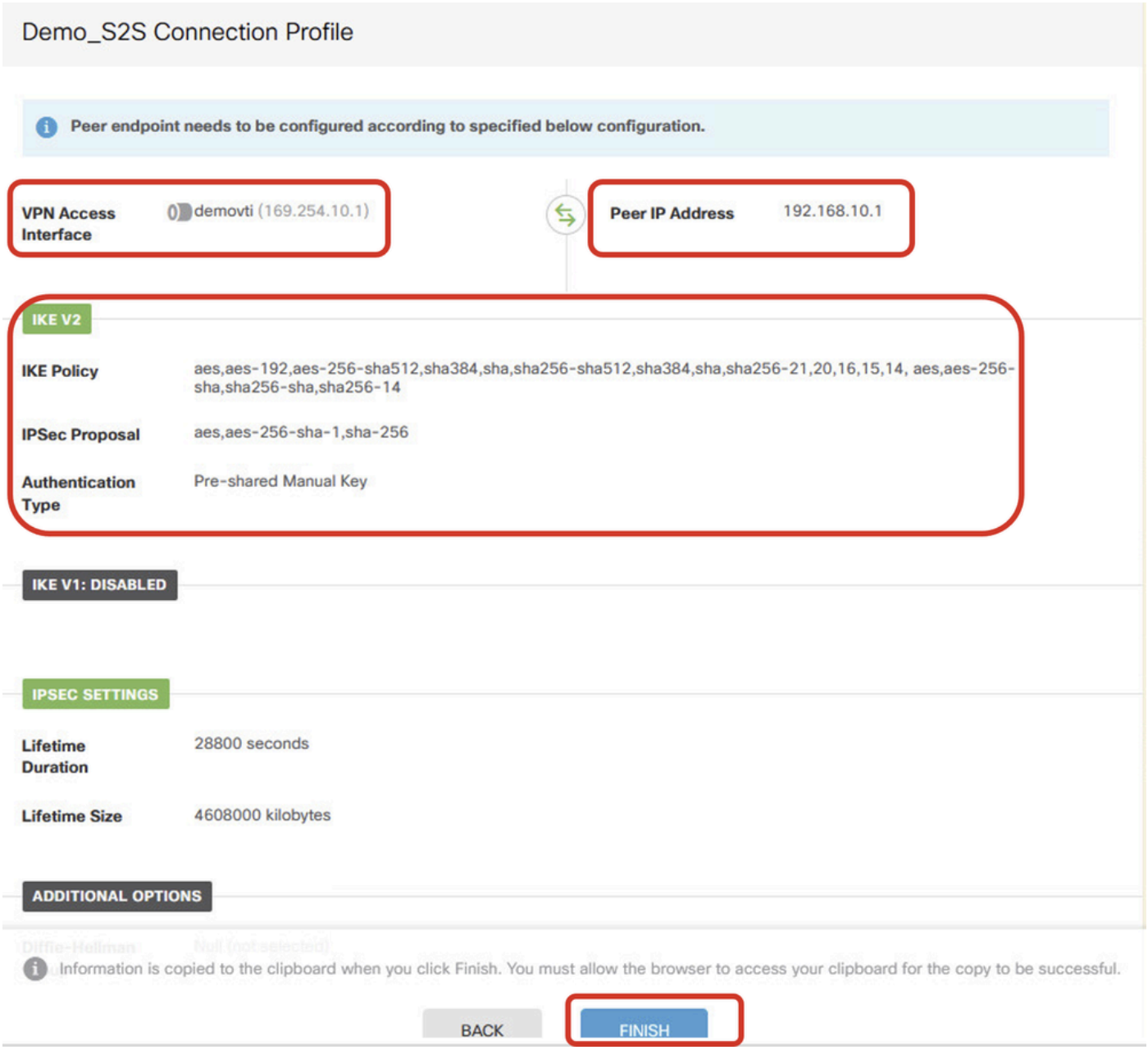
Stap 5.6. Scroll naar beneden op de pagina en configureer de voorgedeelde sleutel. Klik op de knop VOLGENDE.

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



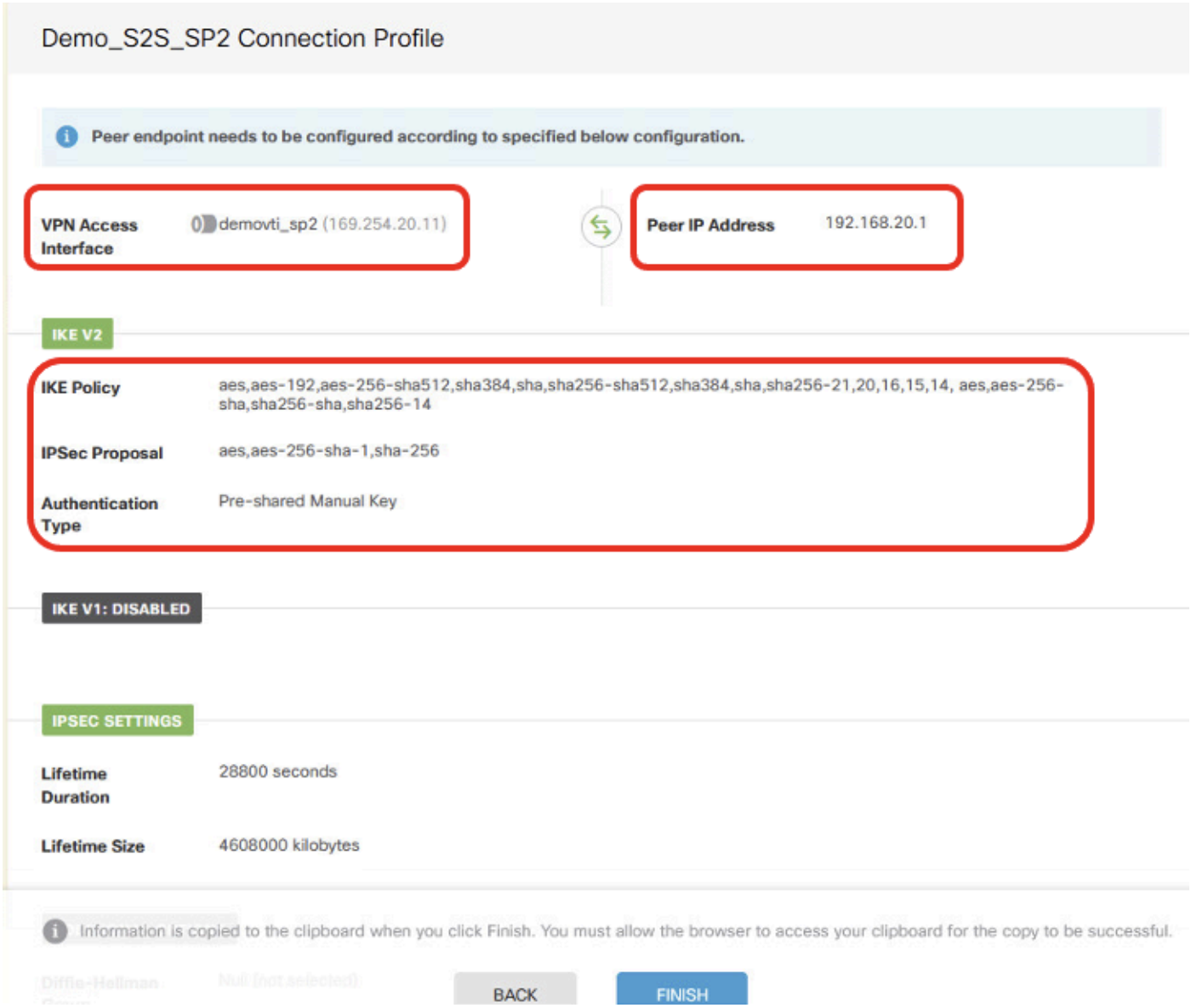
Site1FTD_Configure_Pre_Shared_Key

Stap 5.7. Controleer 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.



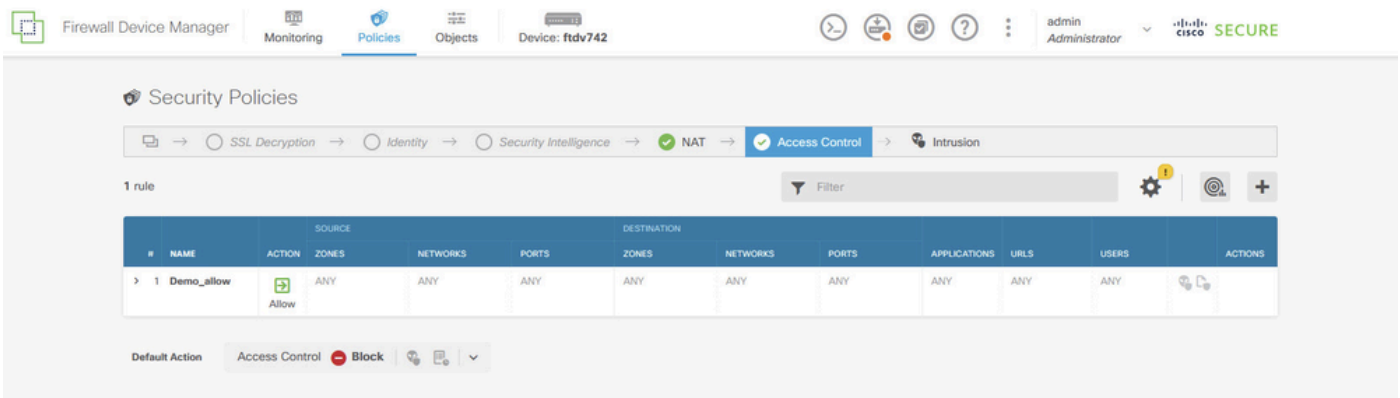
Site1FTD_ISP1_Review_VPN_Config_Samenvatting

Stap 6. Herhaal stap 5. om nieuwe site-to-site VPN te maken via ISP2.



Site1FTD_ISP2_Review_VPN_Config_Samenvatting

Stap 7. Maak een toegangscontroleregel aan om verkeer door de FTD te laten lopen. In dit voorbeeld, sta allen voor demoverkeer toe. Wijzig uw beleid op basis van uw werkelijke behoeften.



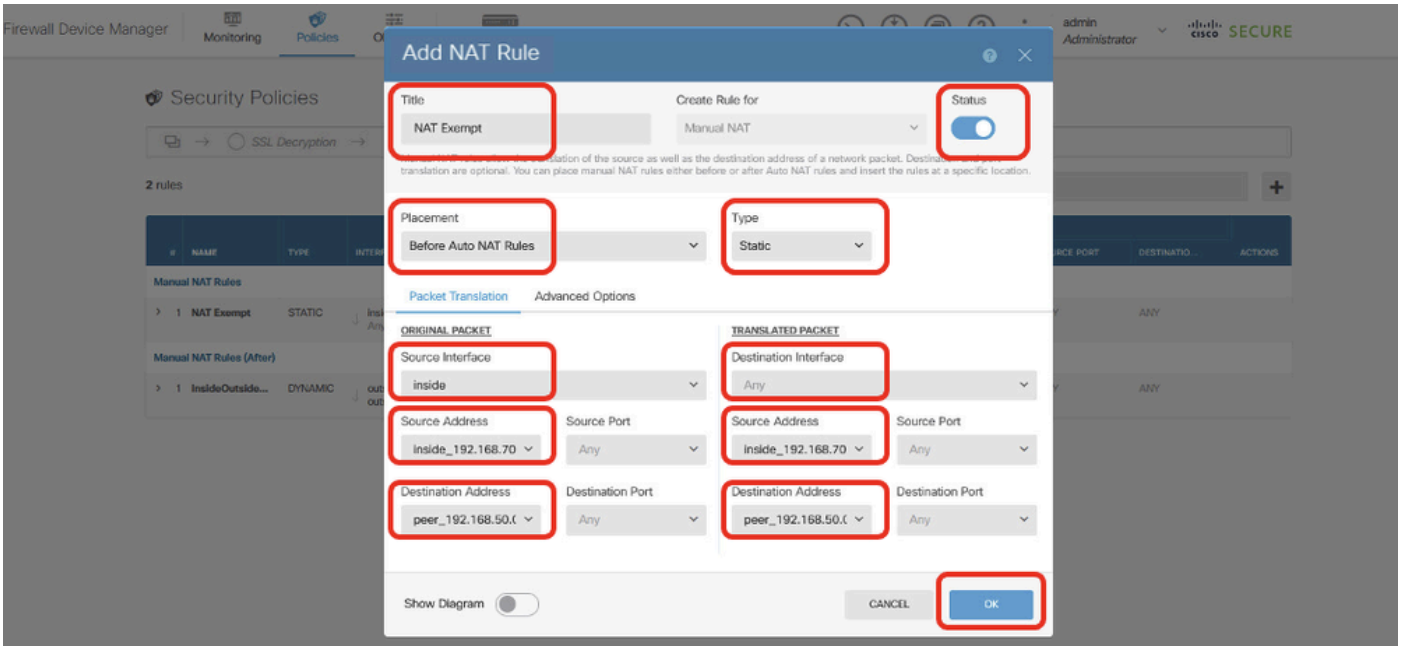
Site1FTD_Allow_Access_Control_Rule_Voorbeeld

Stap 8. (Optioneel) Configureer NAT-vrijstellingsregel voor het clientverkeer op FTD als er voor de client dynamische NAT is geconfigureerd voor toegang tot internet.

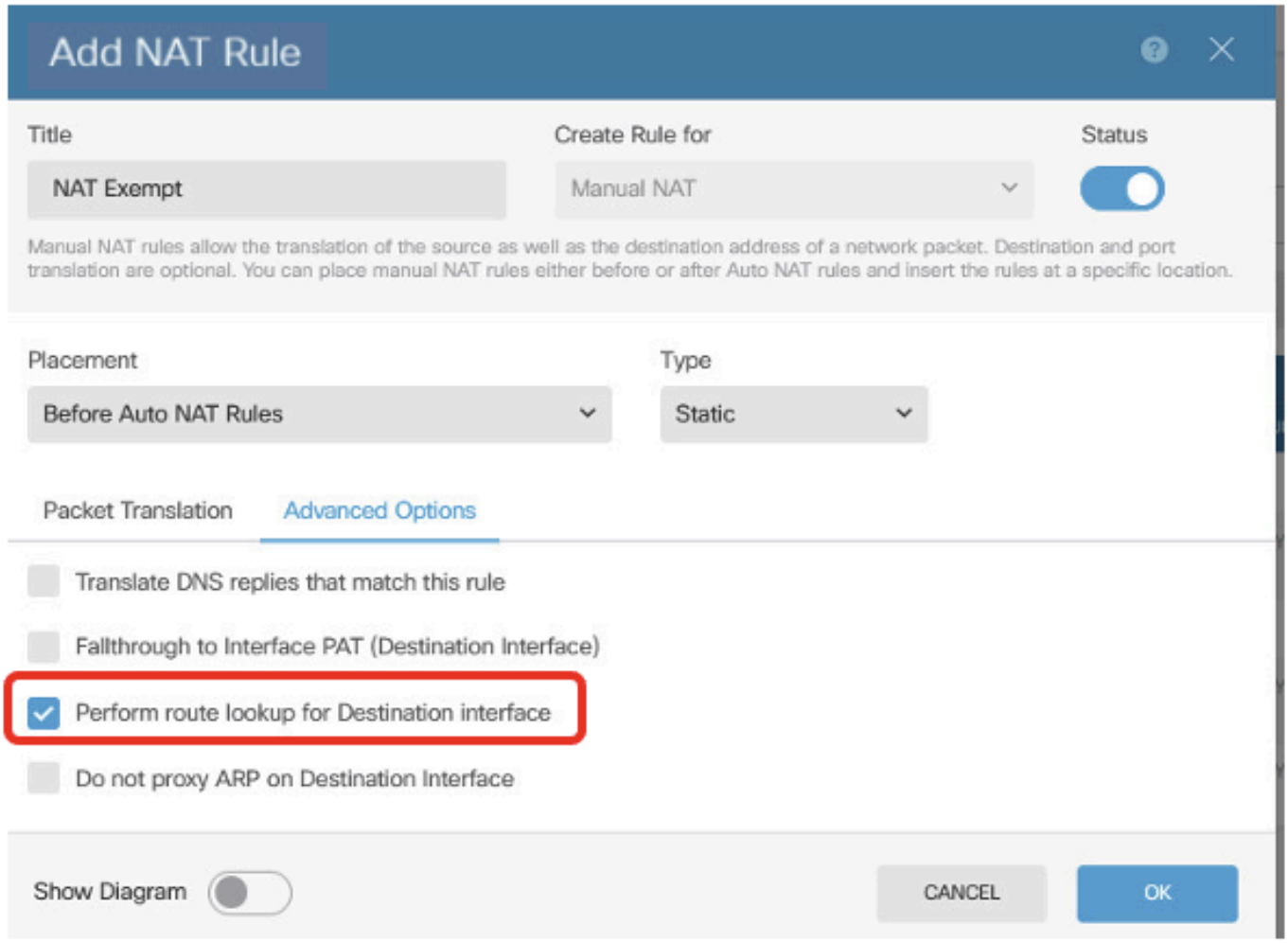
Voor demo-doeleinden, dynamische NAT wordt geconfigureerd voor clients om toegang tot internet in dit voorbeeld. Daarom is NAT-vrijstellingsregel nodig.

Navigeer naar Beleid > NAT. Klik op + knop. Verstrek de details en klik op OK.

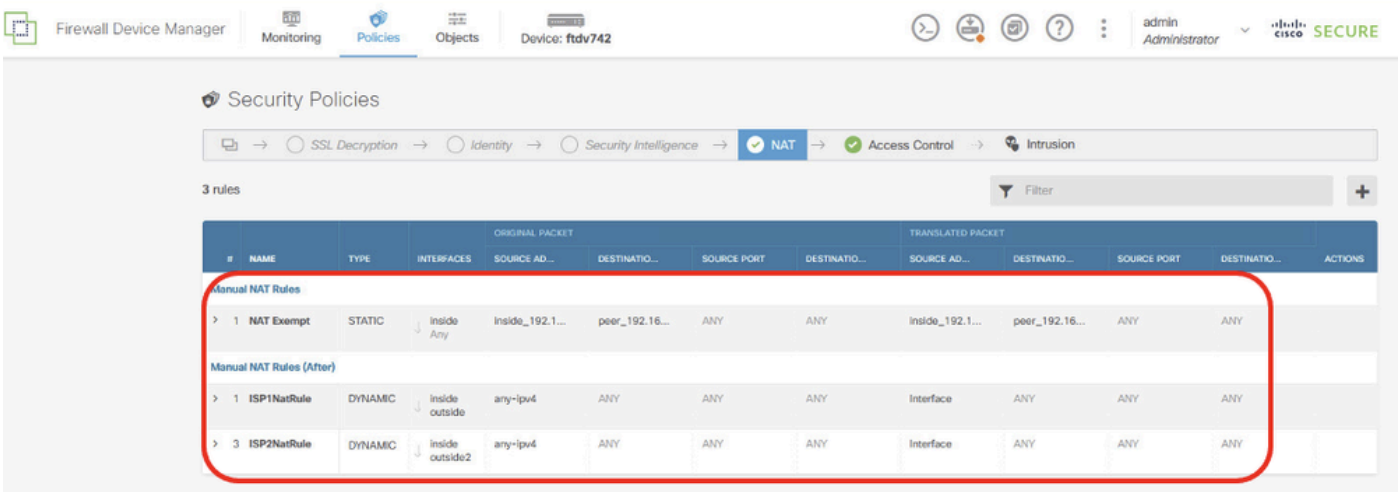
- Titel: NAT-vrijstelling
- Plaatsing: Vóór Auto NAT-regels
- Type: Statisch
- Broninterface: Binnenzijde
- Bestemming: Alle
- Oorspronkelijk bronadres: 192.168.70.0/24
- Vertaald bronadres: 192.168.70.0/24
- Oorspronkelijk doeladres: 192.168.50.0/24
- Vertaald doeladres: 192.168.50.0/24
- Met Route-Lookup ingeschakeld



Site1FTD_Nat_Exempt_Rule



Site1FTD_Nat_Exempt_Rule_2



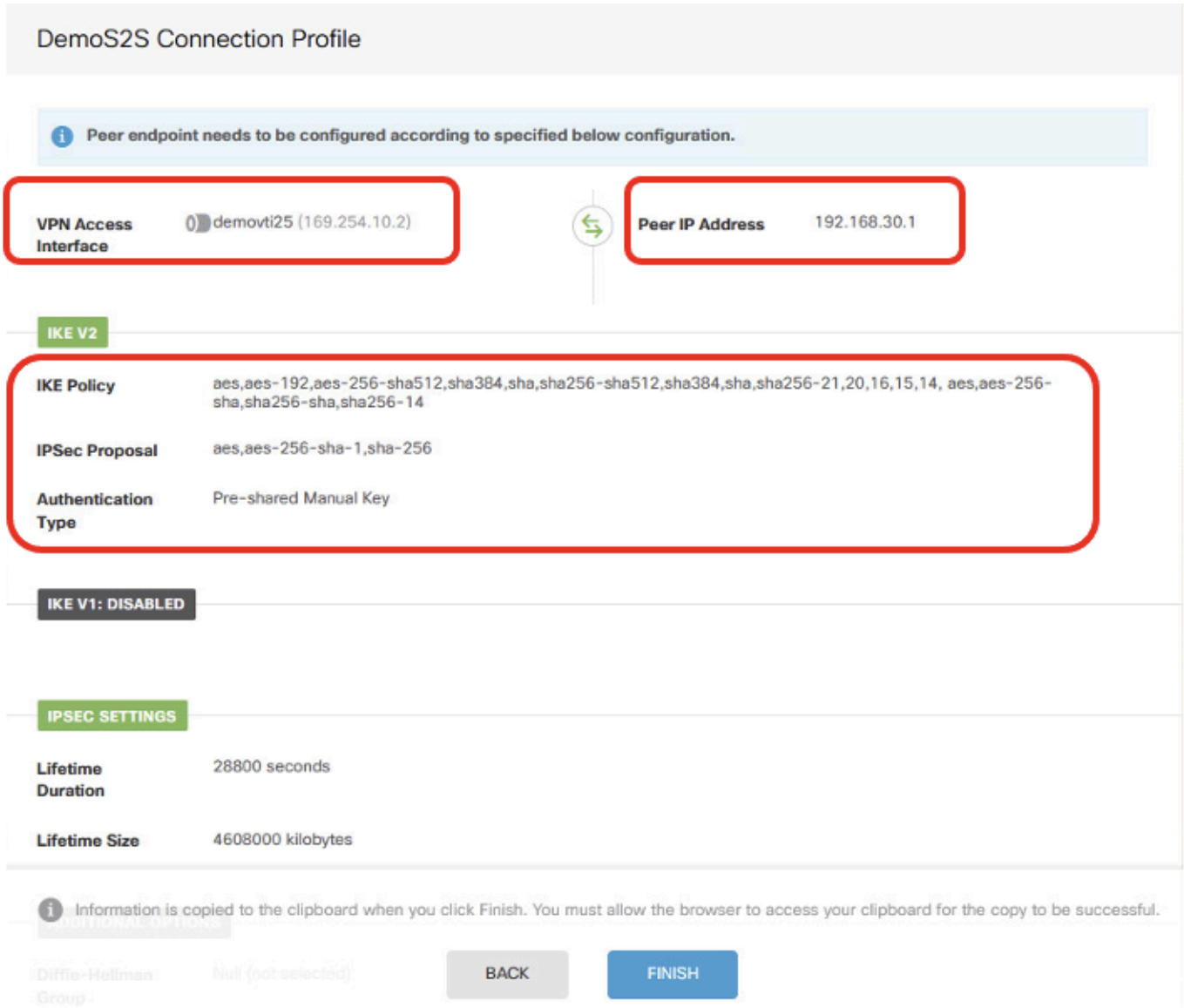
Site1FTD_Nat_Rule_Overzicht

Stap 9. Stel de configuratieveranderingen op.

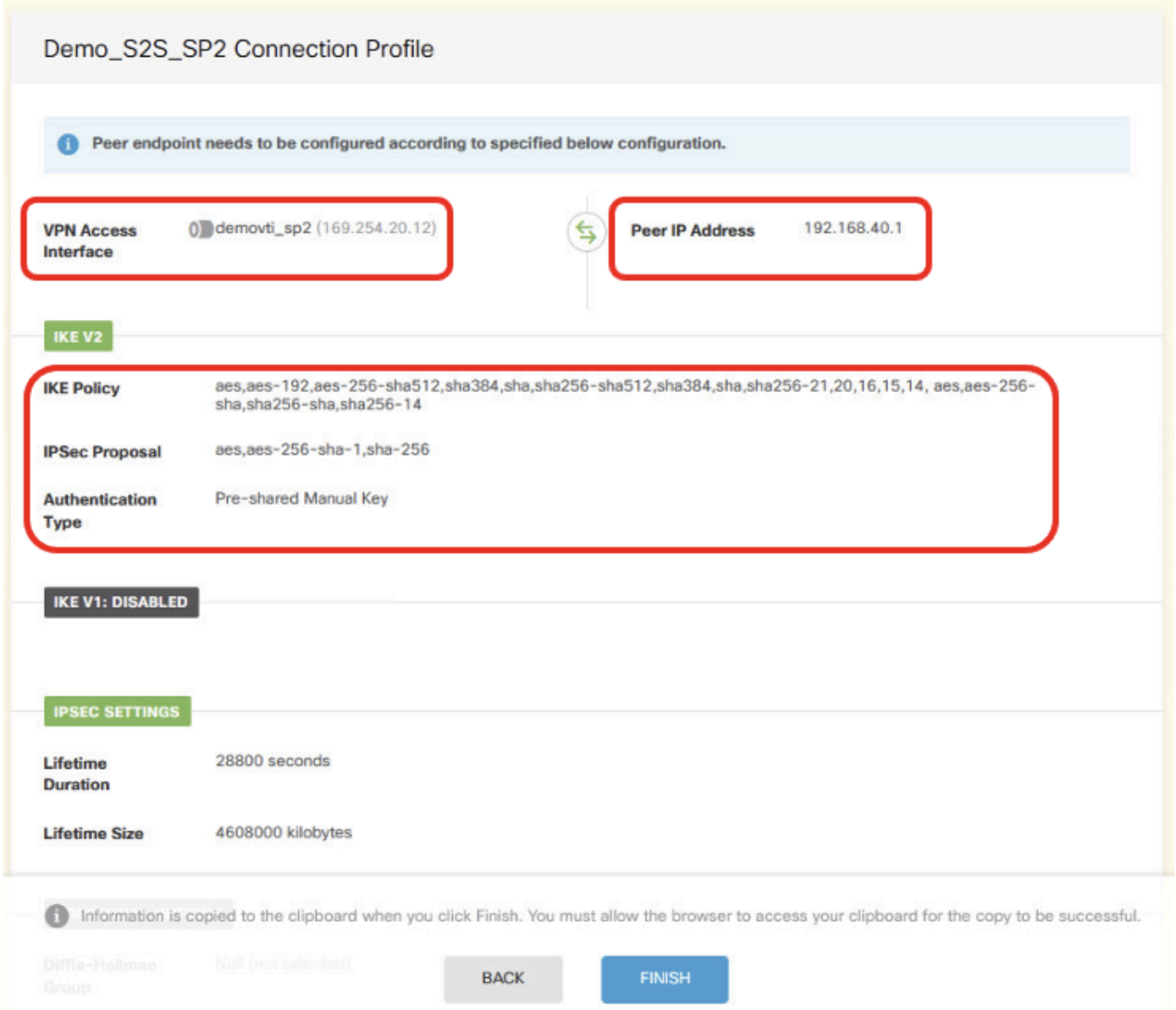
Site1FTD_Implementatie_Wijzigingen

Configuratie van Site2 FTD VPN

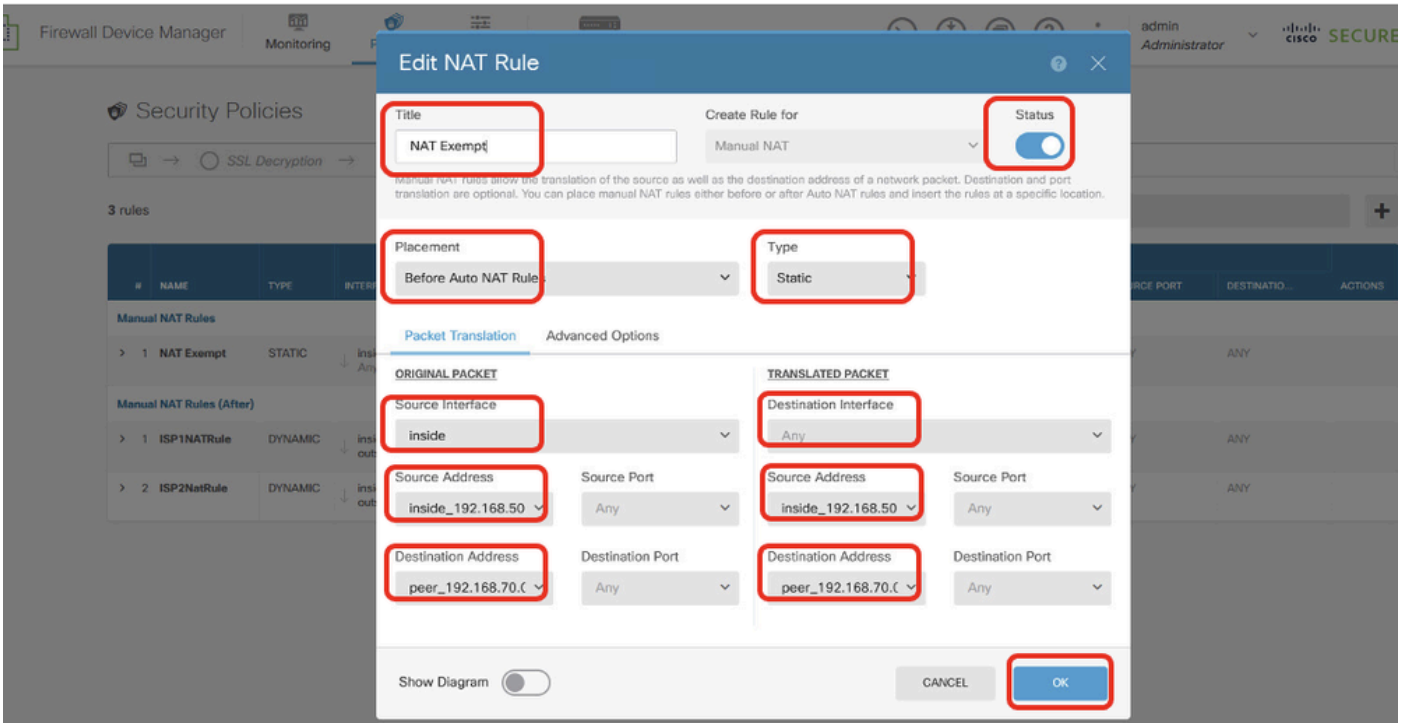
Stap 10. Herhaal stap 1 tot en met stap 9 met de corresponderende parameters voor Site2 FTD.



Site2FTD_ISP1_Review_VPN_Config_Samenvatting



Site2FTD_ISP2_Review_VPN_Config_Samenvatting

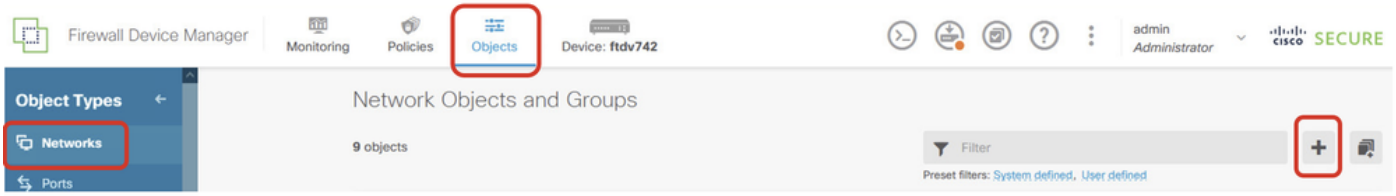


Site2FTD_Nat_Exempt_Rule

Configuraties op PBR

Configuratie Site1 FTD/PBR

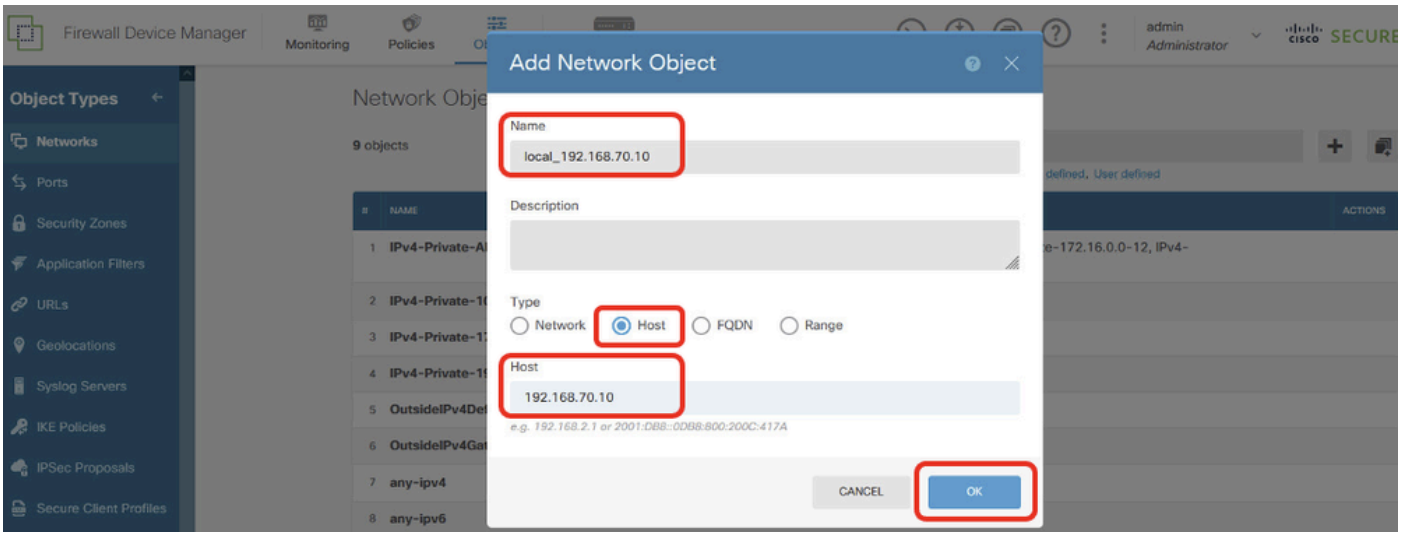
Stap 1. Maak nieuwe netwerkobjecten die door PBR access-list voor Site1 FTD moeten worden gebruikt. Navigeer naar Objecten > Netwerken en klik op +.



Site1FTD_Create_Network_Object

Stap 11.1. Maak een object van Site1 Client2 IP-adres. Geef de benodigde informatie. Klik op de knop OK.

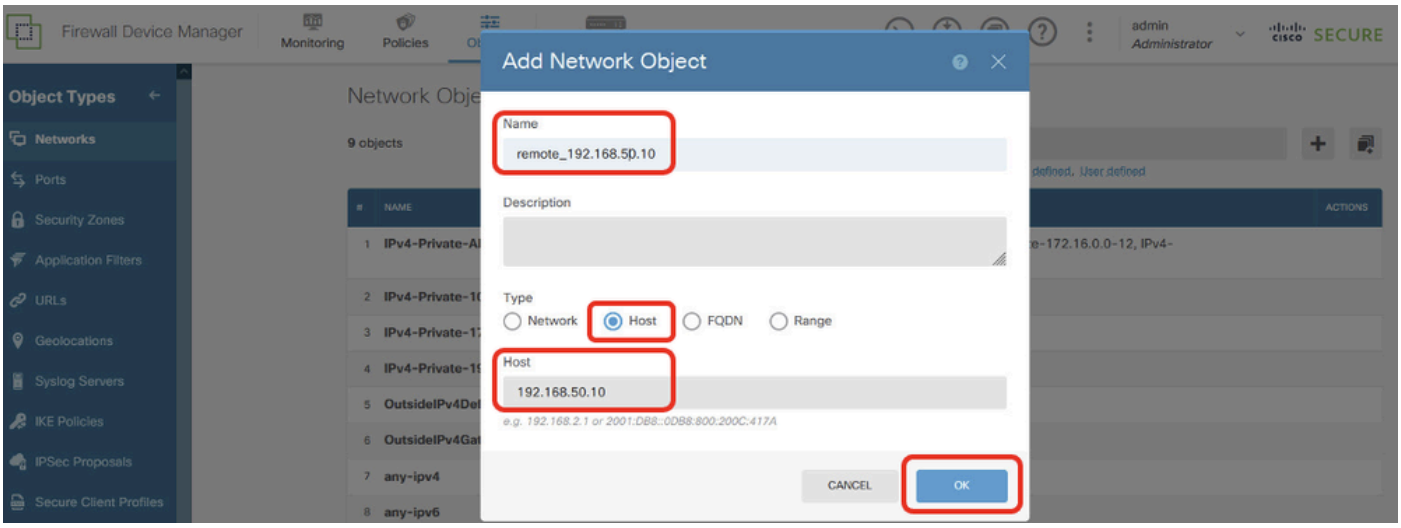
- Naam: lokaal_192.168.70.10
- Type: Host
- Host: 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

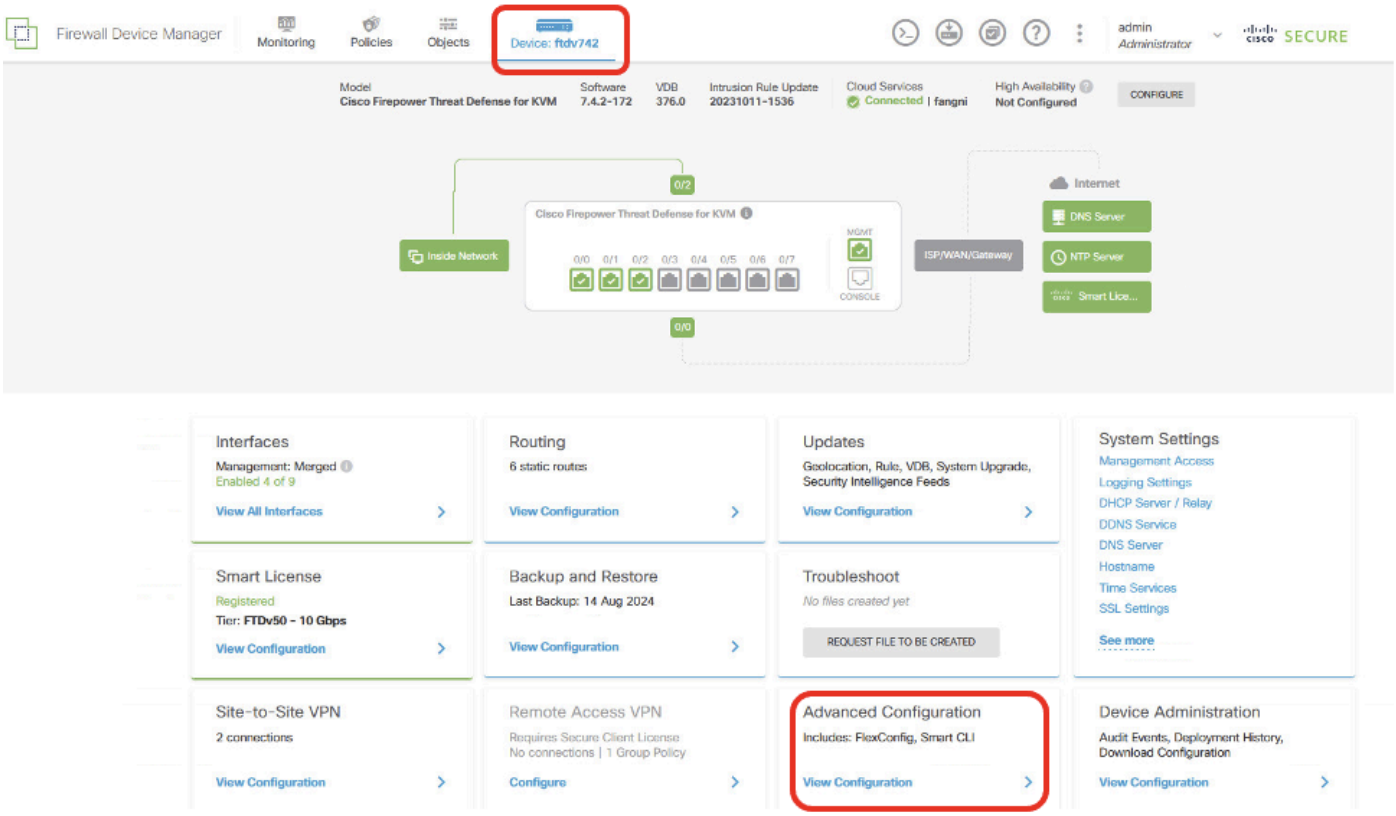
Stap 11.2. Maak een object van Site2 Client2 IP-adres. Geef de benodigde informatie. Klik op de knop OK.

- Naam: afstandsbediening_192.168.50.10
- Type: Host
- Host: 192.168.50.10



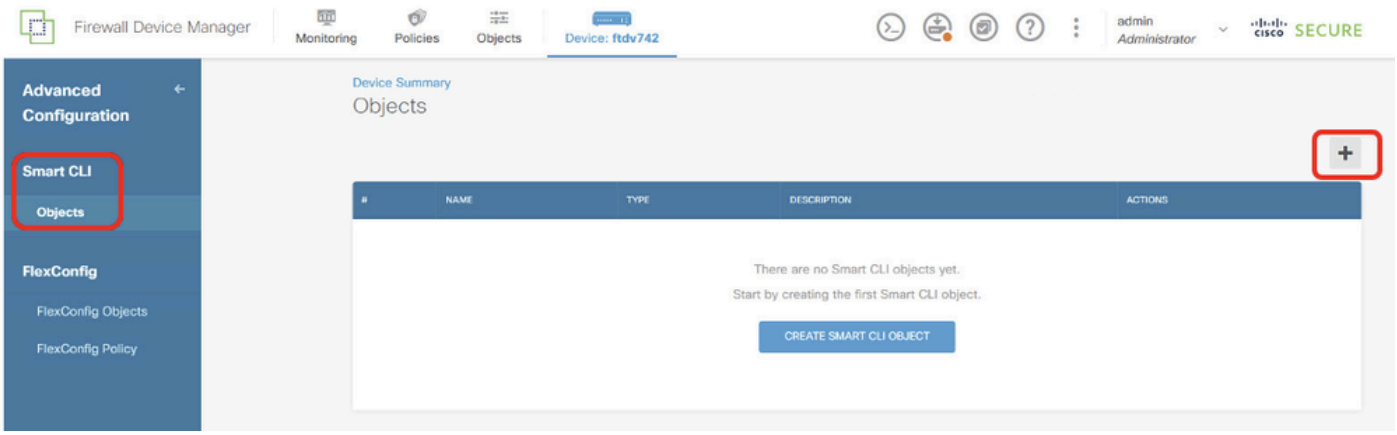
Site1FTD_PBR_RemoteObject

Stap 12. Maak een uitgebreide toegangslijst voor PBR. Ga naar Apparaat > Geavanceerde configuratie. Klik op Configuratie weergeven.



Site1FTD_View_Advanced_Configuration

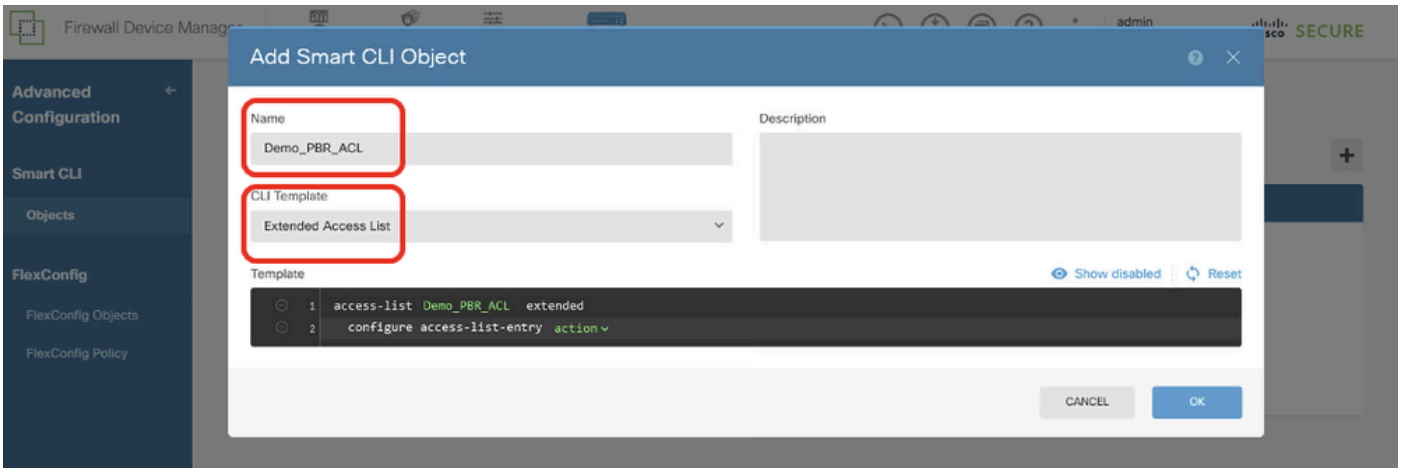
Stap 12.1. Navigeer naar slimme CLI > Objecten. Klik op + knop.



Site1FTD_Add_SmartCLI_Object

Stap 12.2. Voer een naam voor het object in en kies de CLI-sjabloon.

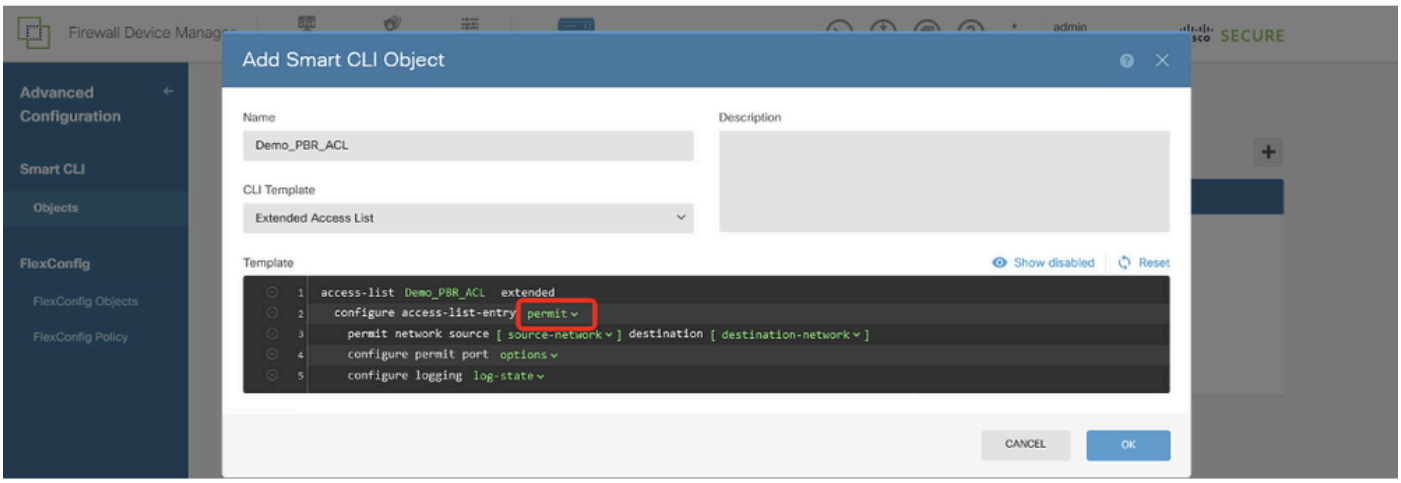
- Naam: Demo_PBR_ACL
- CLI-sjabloon: Uitgebreide toegangslijst



Site1FTD_Create_PBR_ACL_1

Stap 12.3. Navigeer naar Sjabloon en configureer. Klik op de knop OK om op te slaan.

Lijn 2, klik op actie. Selecteer Permit (Toestaan).

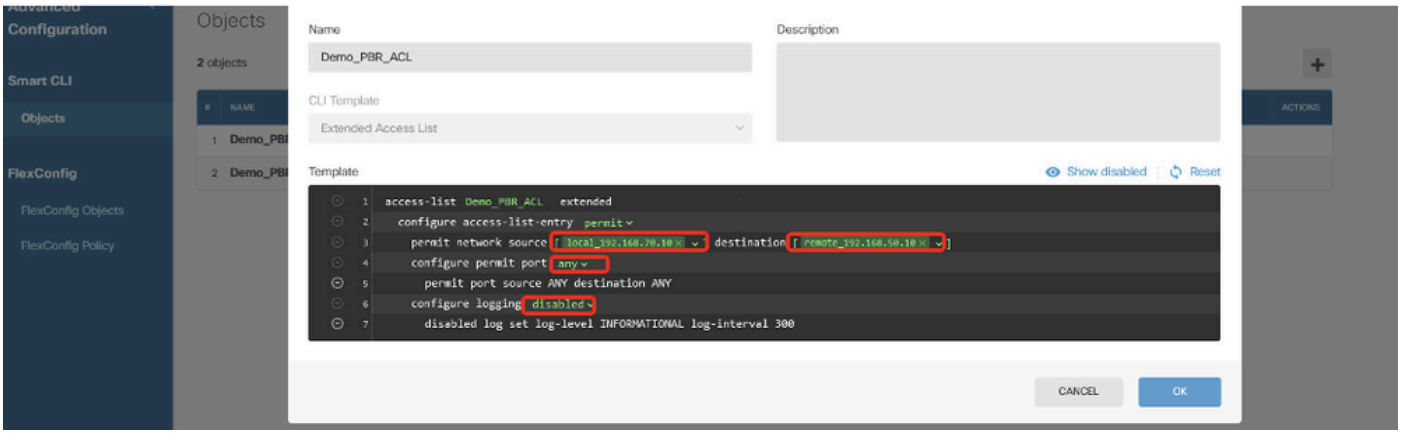


Site1FTD_Create_PBR_ACL_2

Lijn 3, klik op het bronnetwerk. Kies local_192.168.70.10. Klik op doelnetwerk. Kies remote_192.168.50.10.

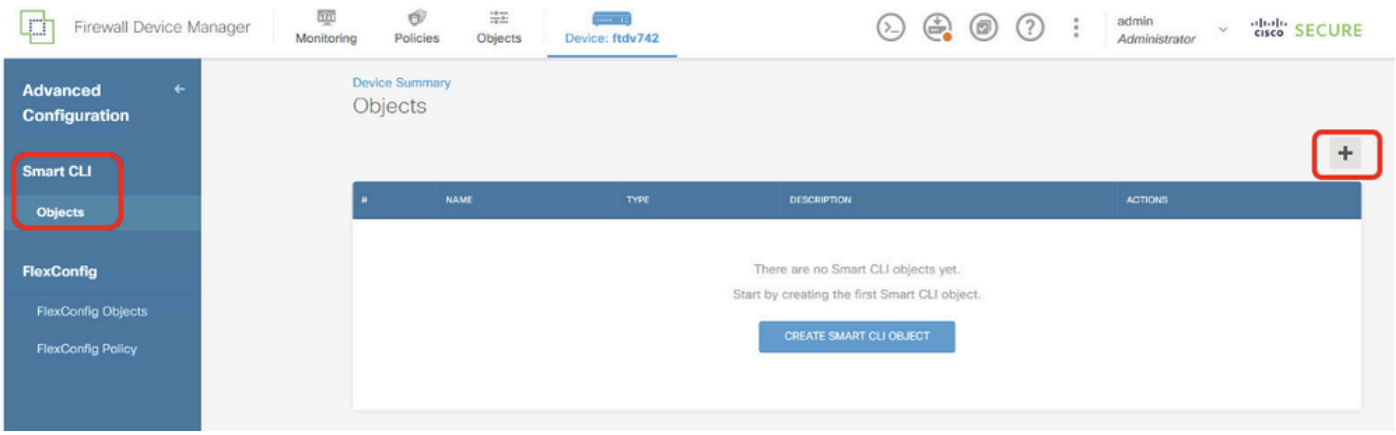
Lijn 4, klik op opties en kies een willekeurige optie.

Lijn 6, klik op log-state en kies uitgeschakeld.



Site1FTD_Create_PBR_ACL_3

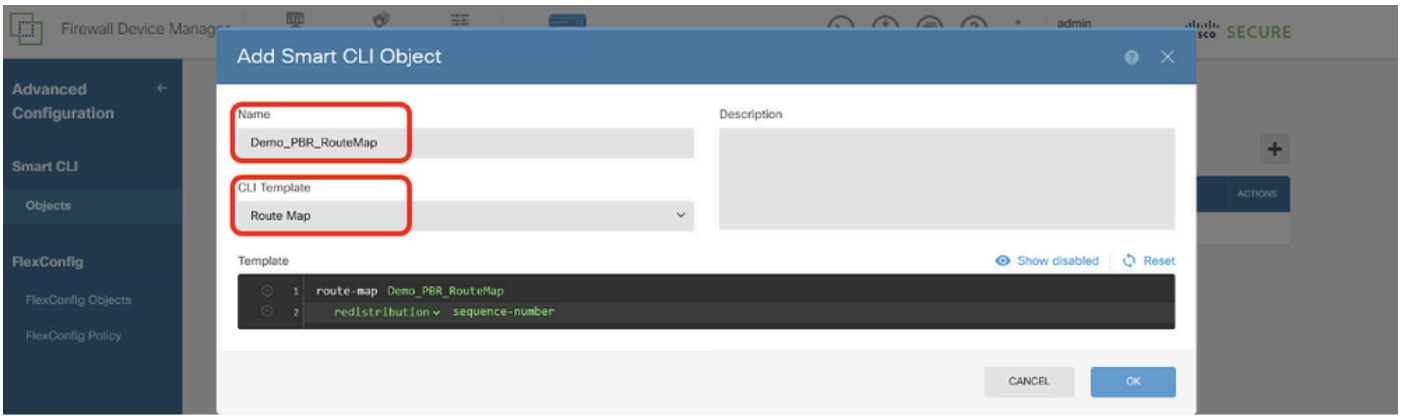
Stap 13. Maak een routekaart voor PBR. Navigeer naar apparaat > Geavanceerde configuratie > Slimme CLI > Objecten. Klik op + knop.



Site1FTD_Add_SmartCLI_Object

Stap 13.1. Voer een naam voor het object in en kies de CLI-sjabloon.

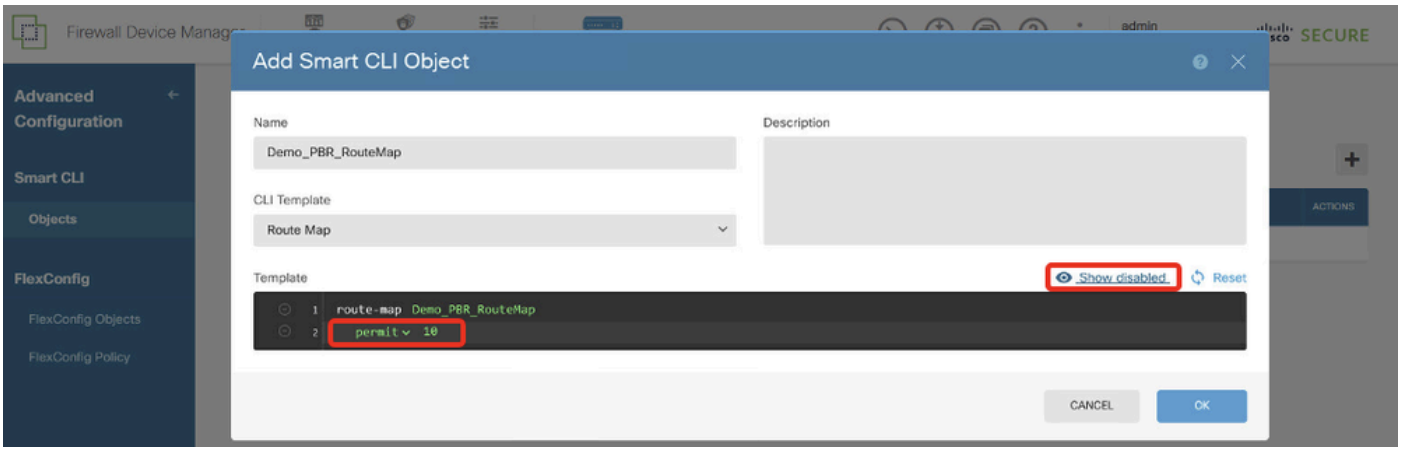
- Naam: Demo_PBR_routekaart
- CLI-sjabloon: Routekaart



Site1FTD_Create_PBR_RouteMap_1

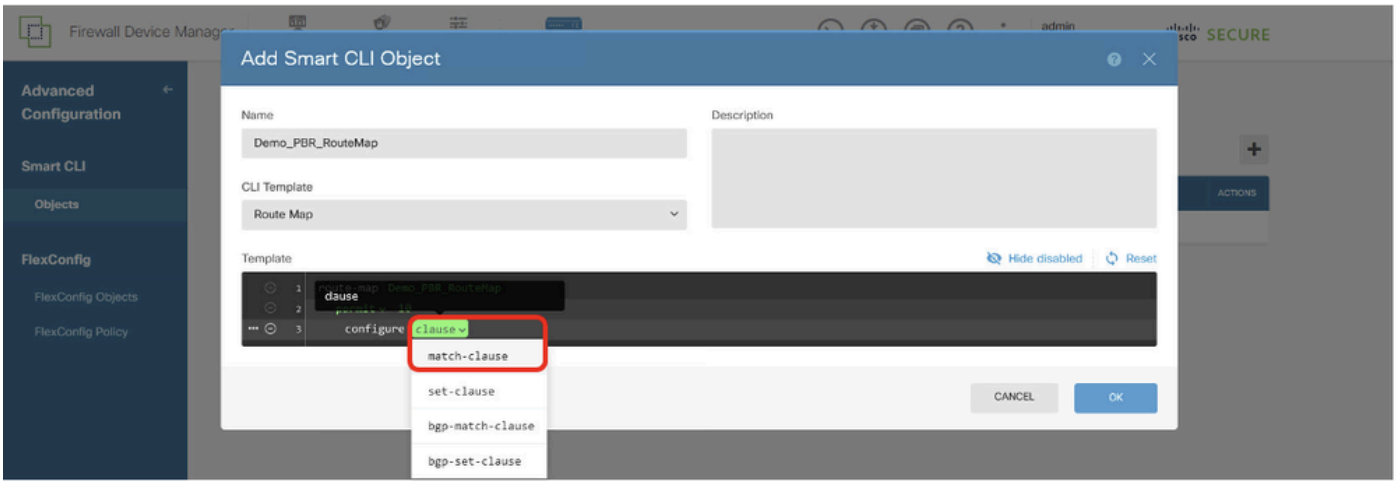
Stap 13.2. Navigeer naar Sjabloon en configureer. Klik op OK om op te slaan.

Lijn 2, klik op Herdistributie. Selecteer Permit (Toestaan). Klik op volgnummer, handmatige invoer 10. Klik op Uitgeschakeld tonen.



Site1FTD_Create_PBR_RouteMap_2

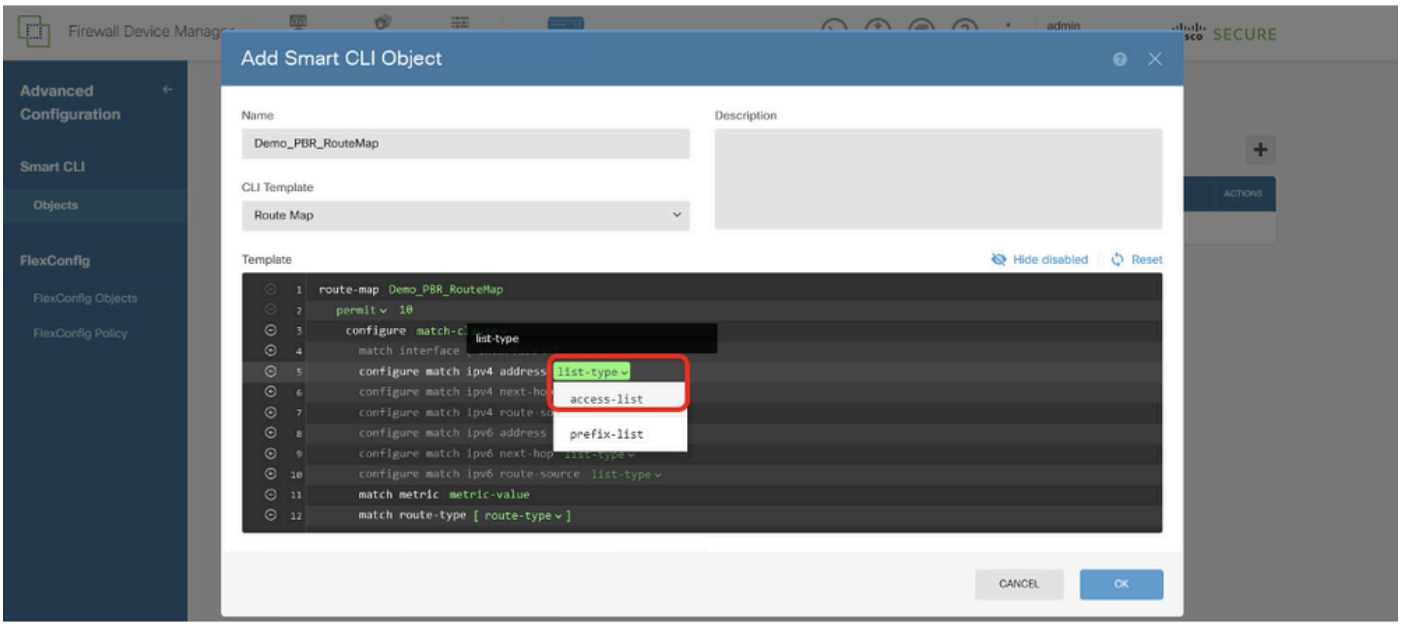
Lijn 3, klik op + om de lijn in te schakelen. Klik op clause. Kies de match-clause.



Site1FTD_Create_PBR_RouteMap_3

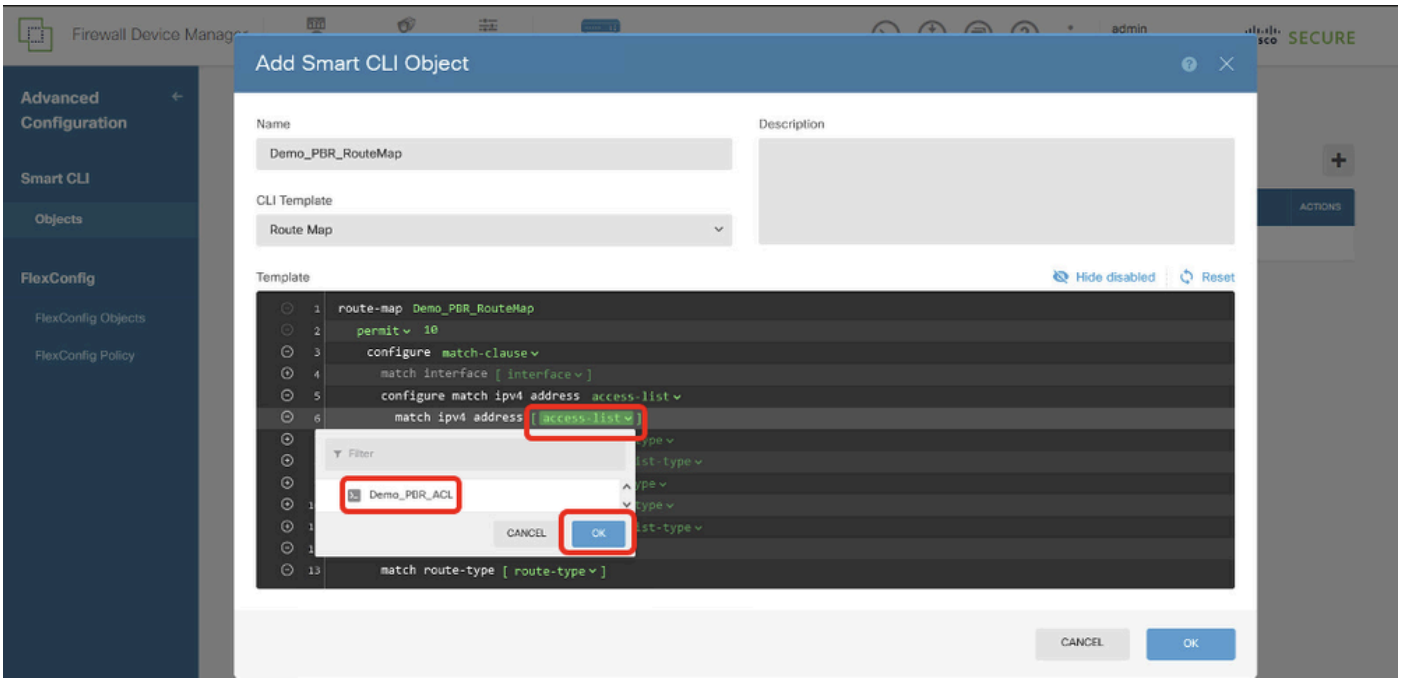
Lijn 4, klik op - om de lijn uit te schakelen.

Lijn 5, klik op + om de lijn in te schakelen. Klik op lijsttype. Kies de toegangslijst.



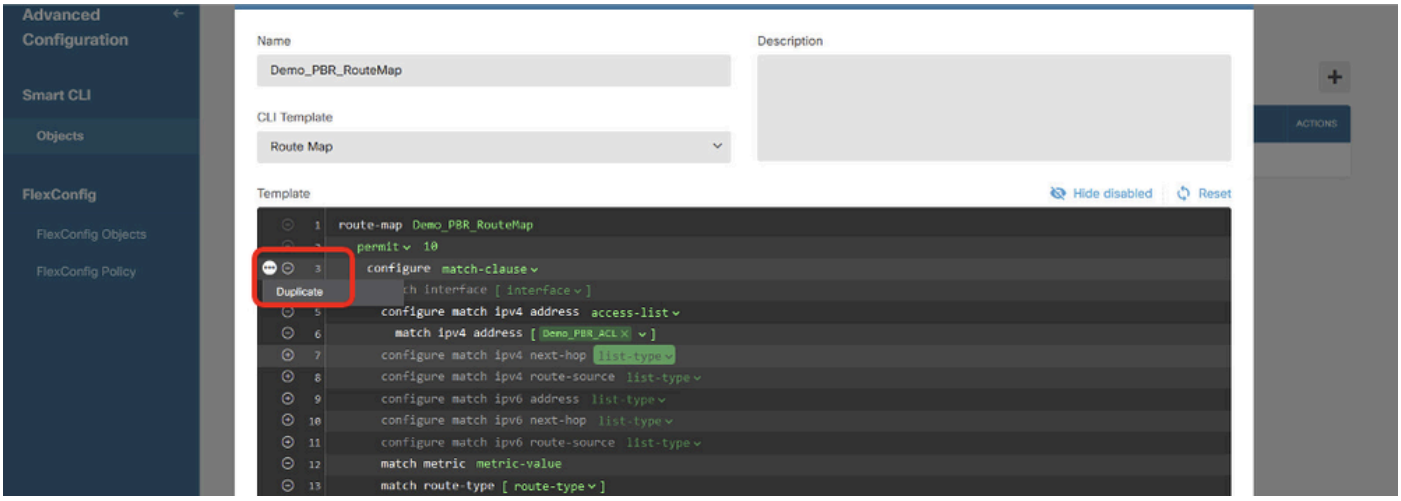
Site1FTD_Create_PBR_RouteMap_4

Lijn 6, klik op de toegangslijst. Kies de ACL-naam die in Stap 12 is gemaakt. In dit voorbeeld is het Demo_PBR_ACL.



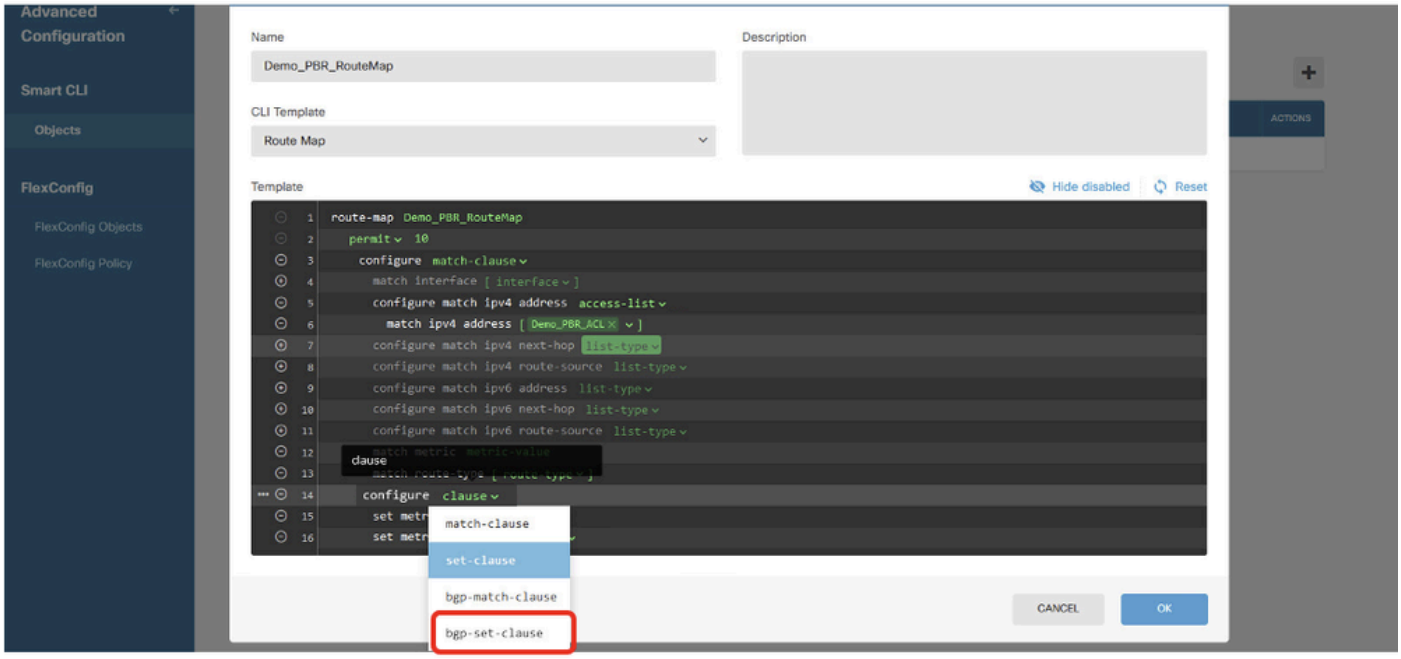
Site1FTD_Create_PBR_RouteMap_5

Terug naar regel 3. Klik op de opties ... en kies Duplicaat.



Site1FTD_Create_PBR_RouteMap_6

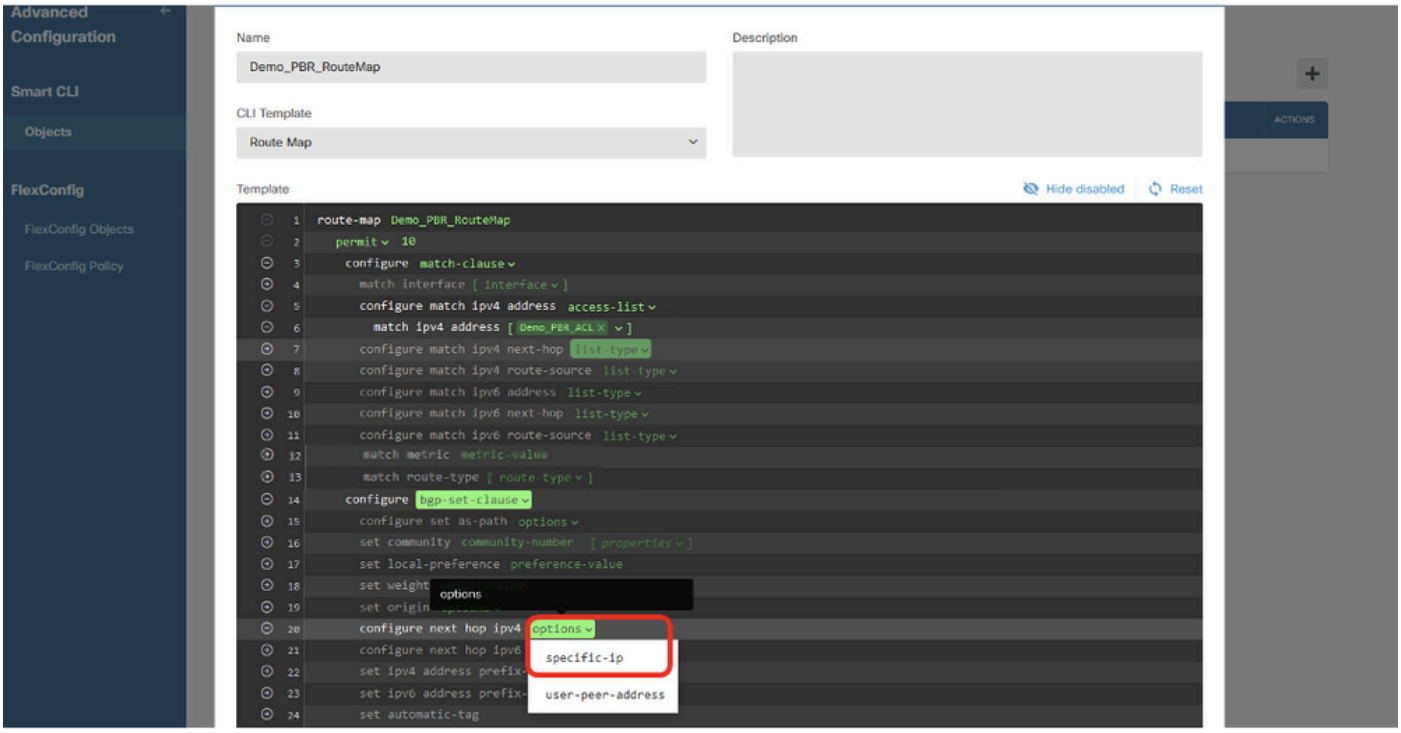
Lijn 14, klik op clause en kies bgp-set-clause.



Site1FTD_Create_PBR_RouteMap_7

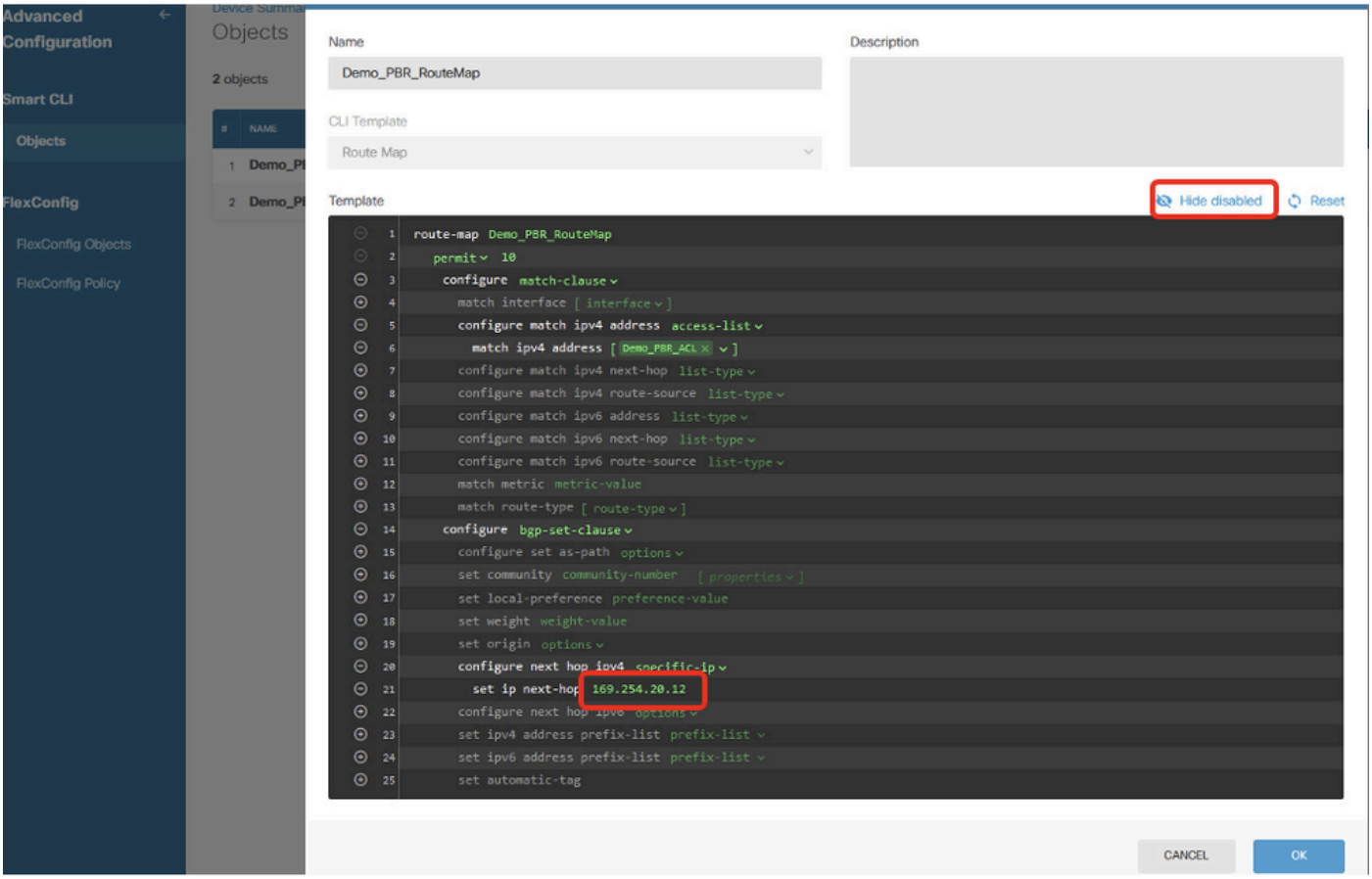
In de lijnen 12, 13, 15, 16, 17, 18, 19, 21, 22, 23, 24 klikt u op -toets om deze uit te schakelen.

Lijn 20, klik op opties en kies specifiek-ip.



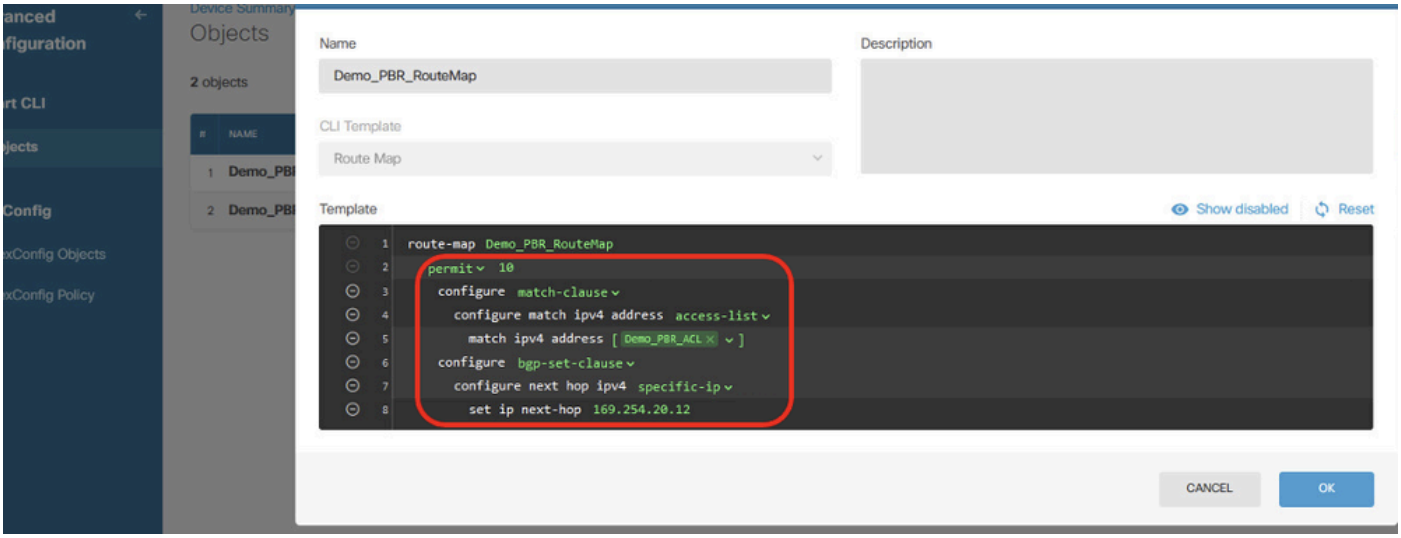
Site1FTD_Create_PBR_RouteMap_8

Lijn 21, klik op IP-adres. Handmatige invoer van next-hop IP-adres. In dit voorbeeld is het IP-adres van peer Site2 FTD VTI tunnel2 (169.254.20.12). Klik op Uitgeschakeld verbergen.



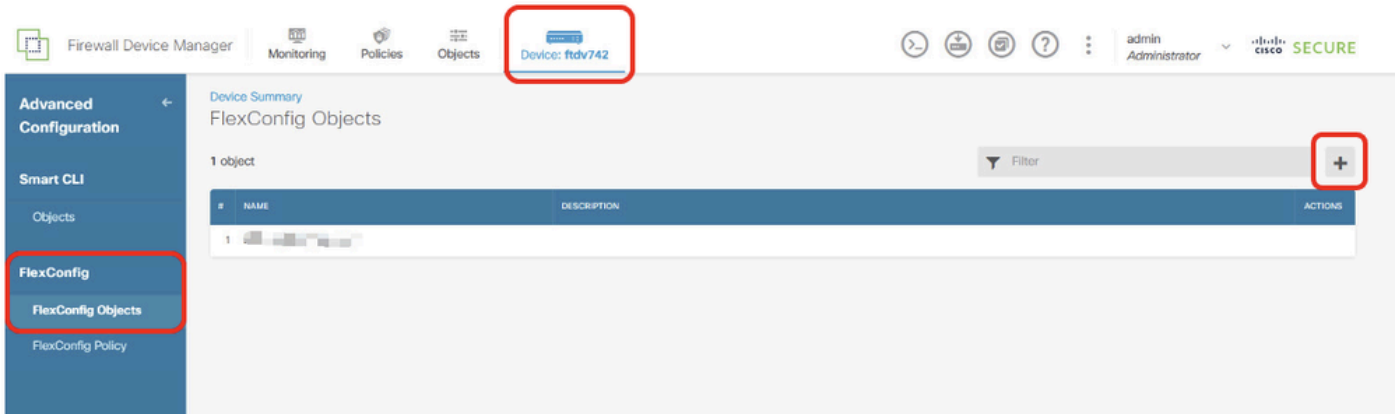
Site1FTD_Create_PBR_RouteMap_9

Herzie de configuratie van routekaart.



Site1FTD_Create_PBR_RouteMap_10

Stap 14. Maak FlexConfig-object voor PBR. Navigeer naar Apparaat > Geavanceerde configuratie > FlexConfig-objecten en klik op de knop +.



Site1FTD_Create_PBR_FlexObj_1

Stap 14.1. Voer een naam in voor het object. In dit voorbeeld, Demo_PBR_FlexObj. In de redacteur van het Malplaatje en van het Negate Malplaatje, ga de bevellijnen in.

- Sjabloon:

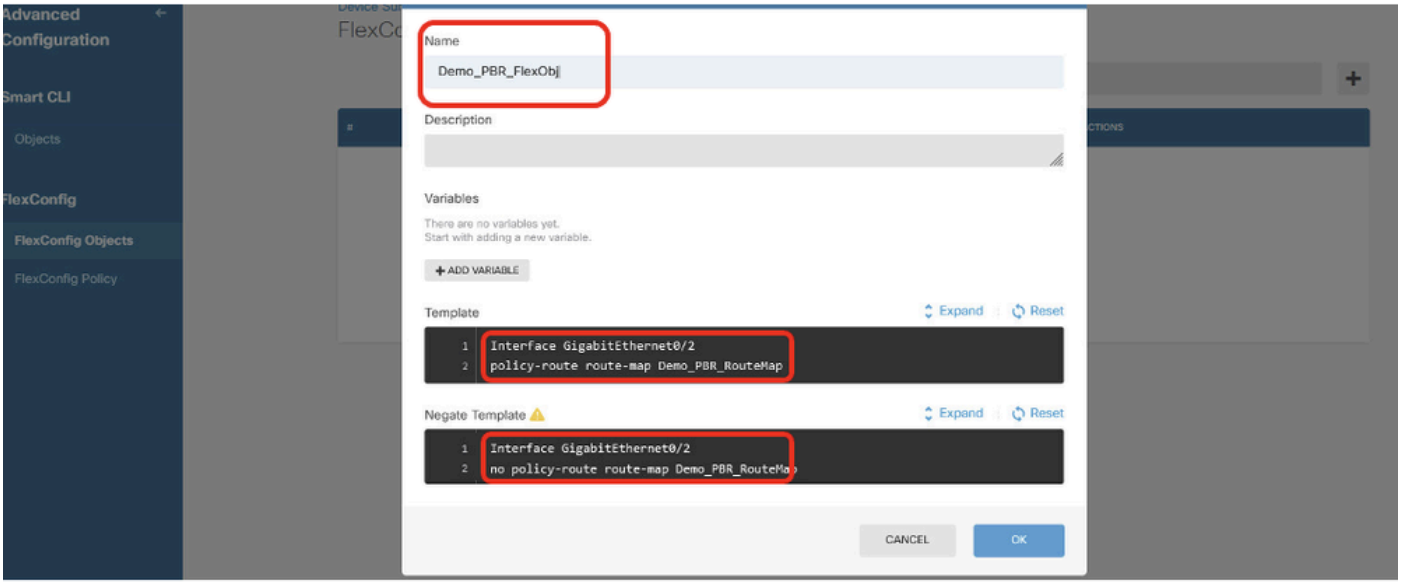
interface Gigabit Ethernet0/2

route-routekaart voor beleid Demo_PBR_RouteMap_Site2

- Template negeren:

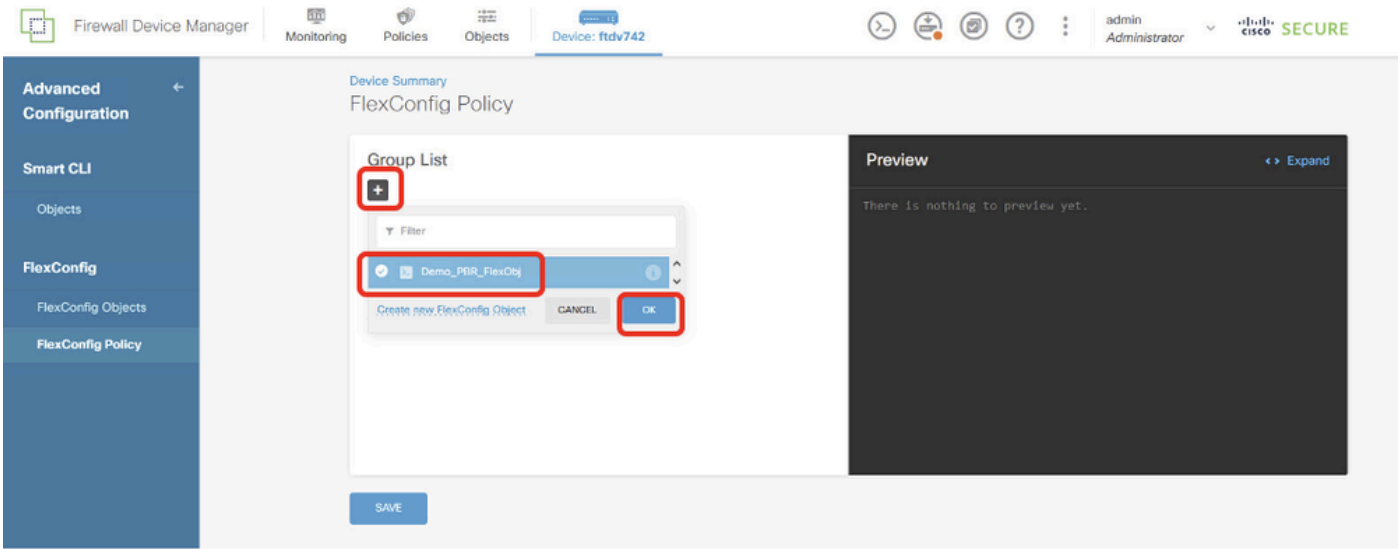
interface Gigabit Ethernet0/2

geen beleid-route routekaart Demo_PBR_RouteMap_Site2



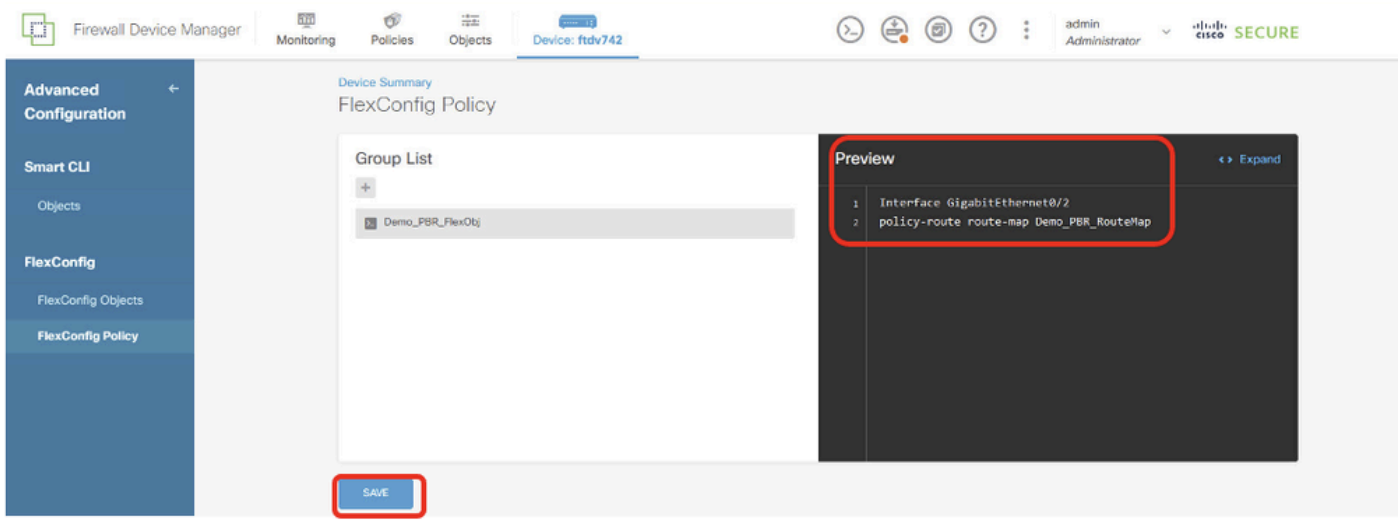
Site1FTD_Create_PBR_FlexObj_2

Stap 15. Maak FlexConfig-beleid voor PBR. Navigeer naar apparaat > Geavanceerde configuratie > FlexConfig-beleid. Klik op + knop. Kies de FlexConfig-objectnaam die in stap 14 is gemaakt. Klik op OK knop.



Site1FTD_Create_PBR_FlexPolicy_1

Stap 15.1. Controleer de opdracht in het Preview-venster. Als het goed is, klikt u op Opslaan.



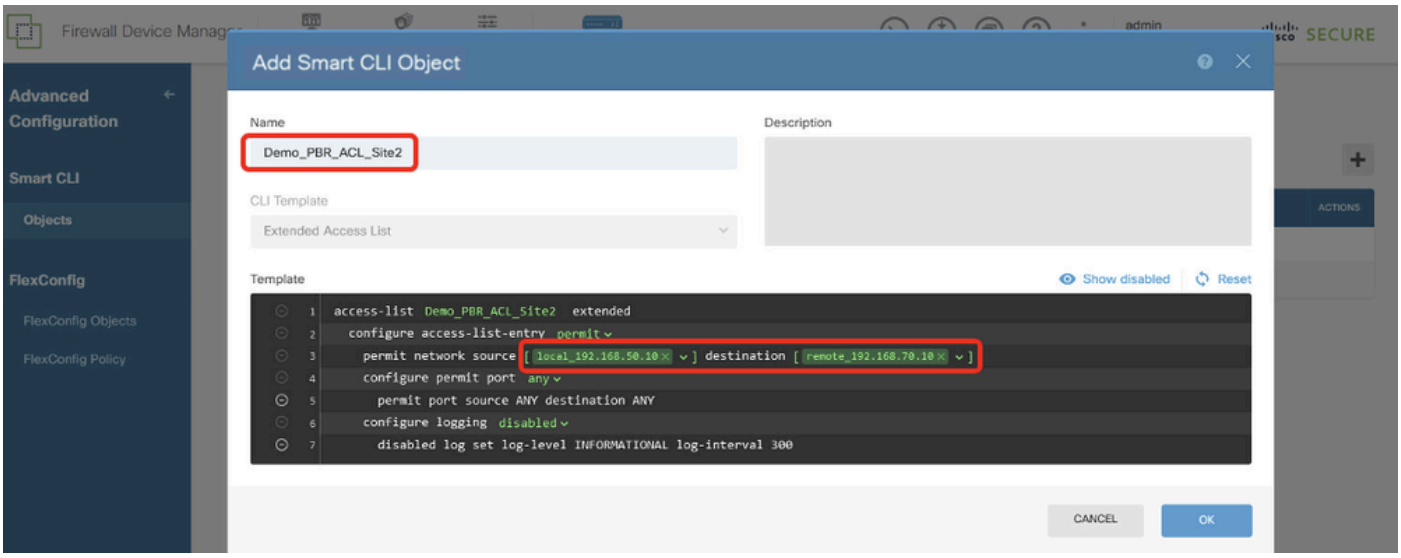
Site1FTD_Create_PBR_FlexPolicy_2

Stap 16. Implementeer de configuratiewijzigingen.

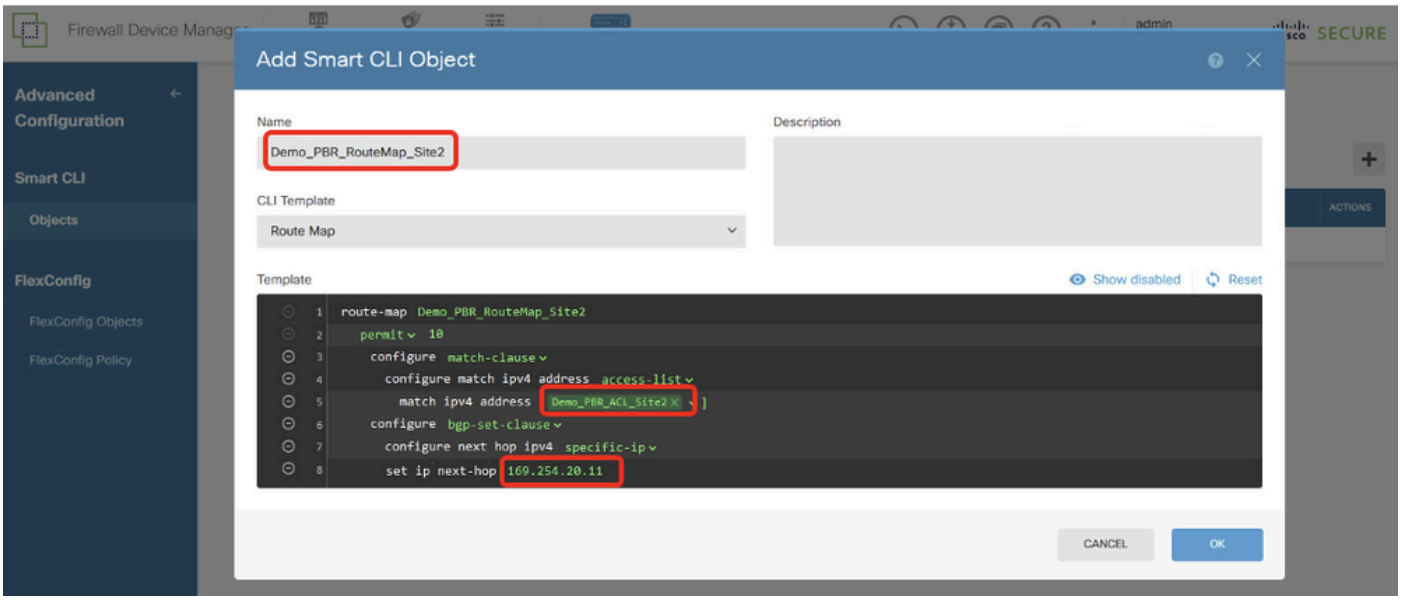
Site1FTD_Implementatie_Wijzigingen

Configuratie Site2 FTD/PBR

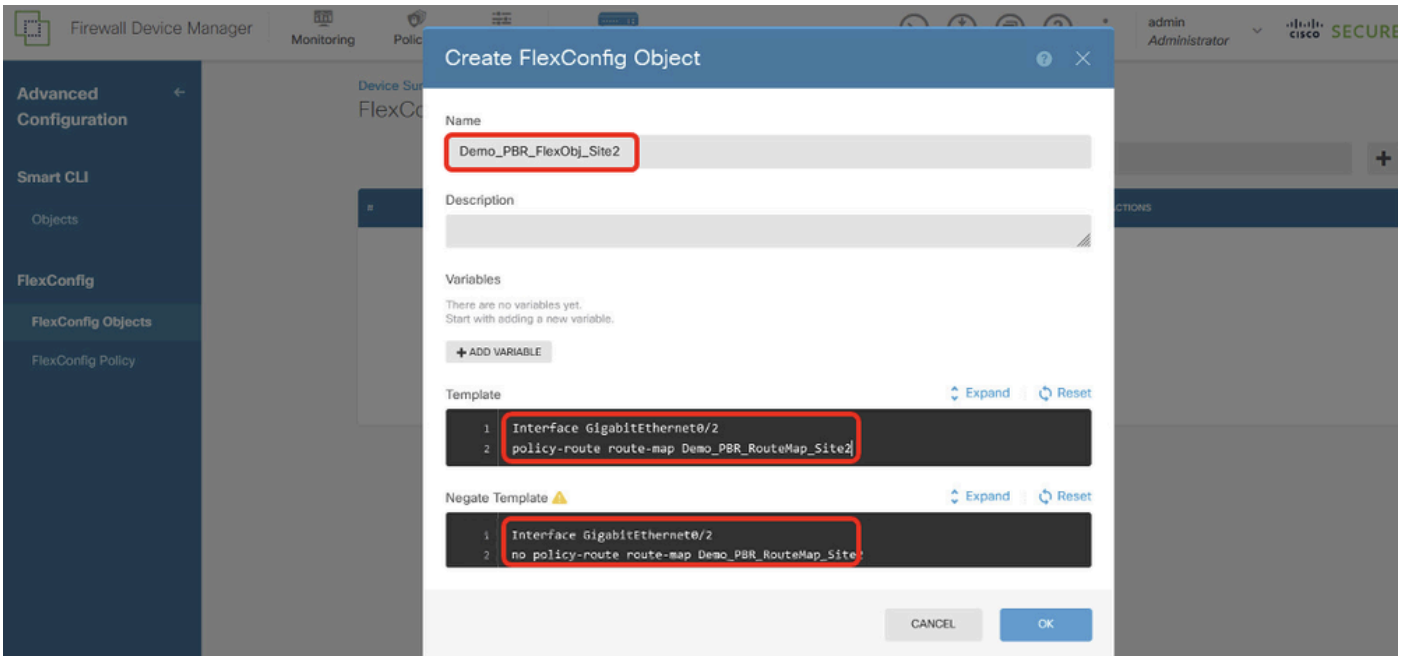
Stap 17. Herhaal stap 11. tot en met stap 16. om PBR te maken met de bijbehorende parameters voor Site2 FTD.



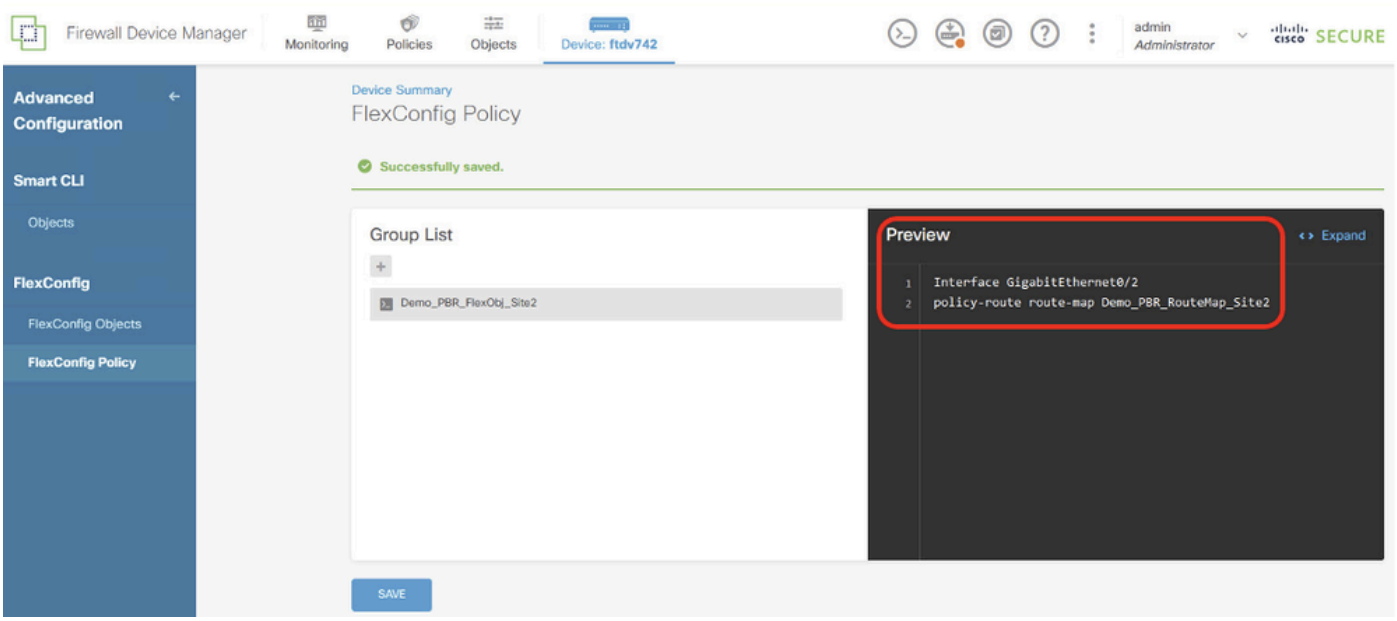
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

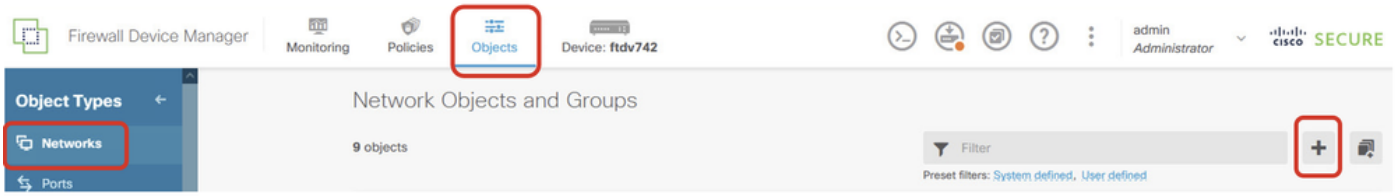


Site2FTD_Create_PBR_FlexPolicy

Configuraties op SLA-monitor

Configuratie van Site1 FTD SLA-monitor

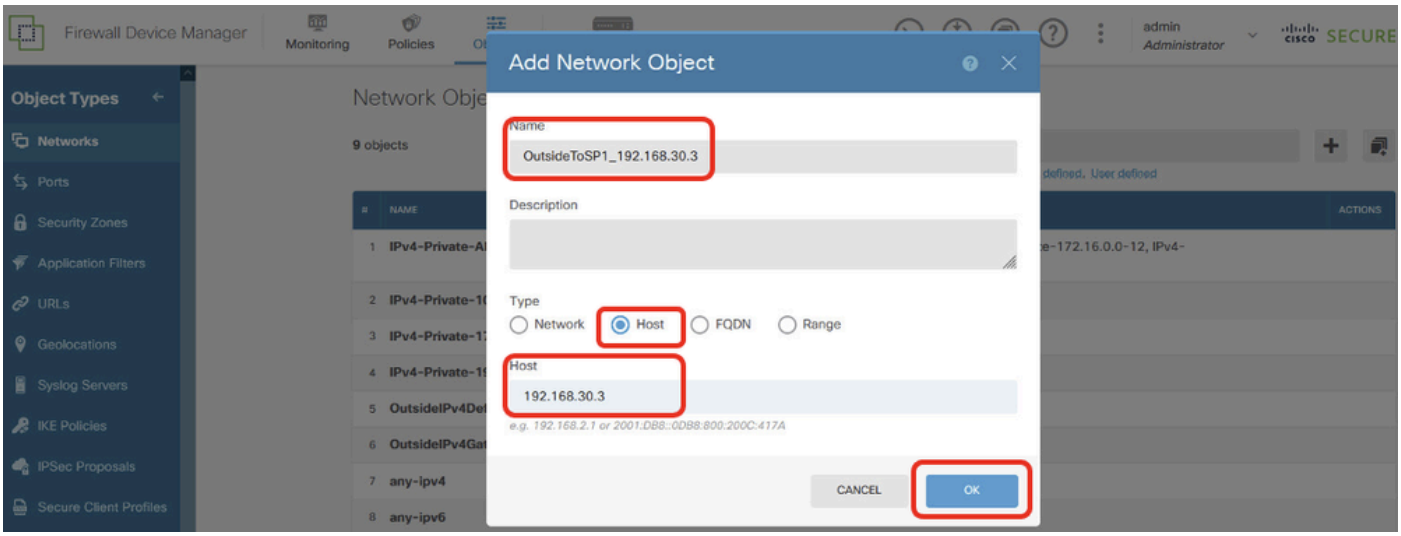
Stap 18. Maak nieuwe netwerkobjecten die door SLA-monitoren voor Site1 FTD moeten worden gebruikt. Navigeer naar objecten > Netwerken en klik op +.



Site1FTD_Create_Network_Object

Stap 18.1. Maak een object voor het IP-adres van de ISP1-gateway. Geef de benodigde informatie. Klik op de knop OK.

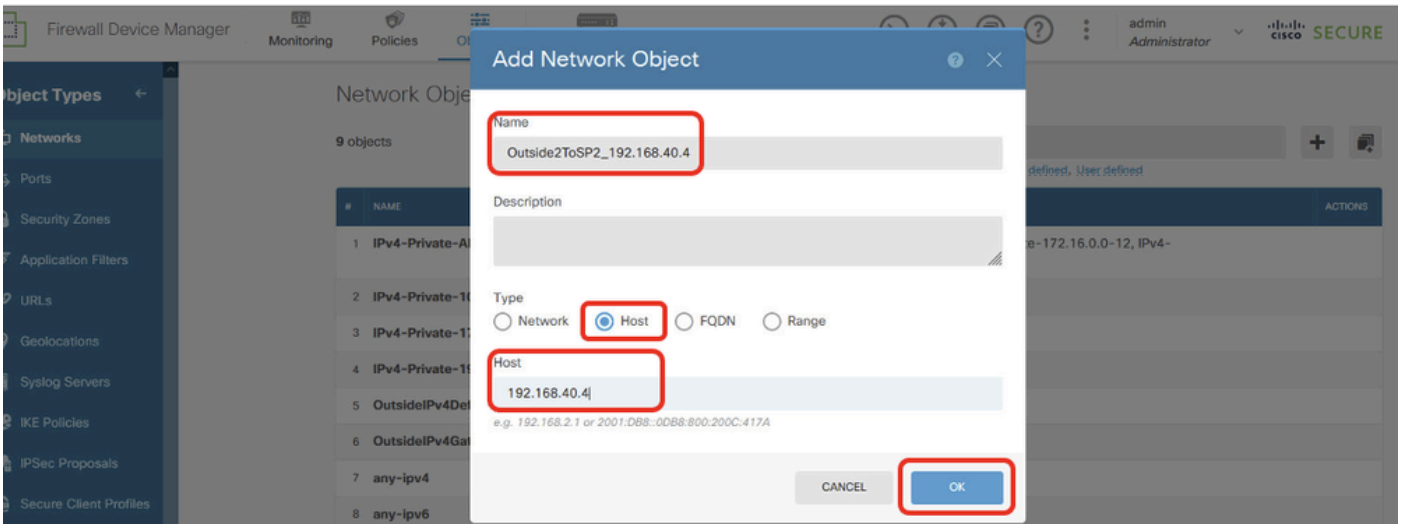
- Naam: BuitenToSP1_192.168.30.3
- Type: Host
- Host: 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

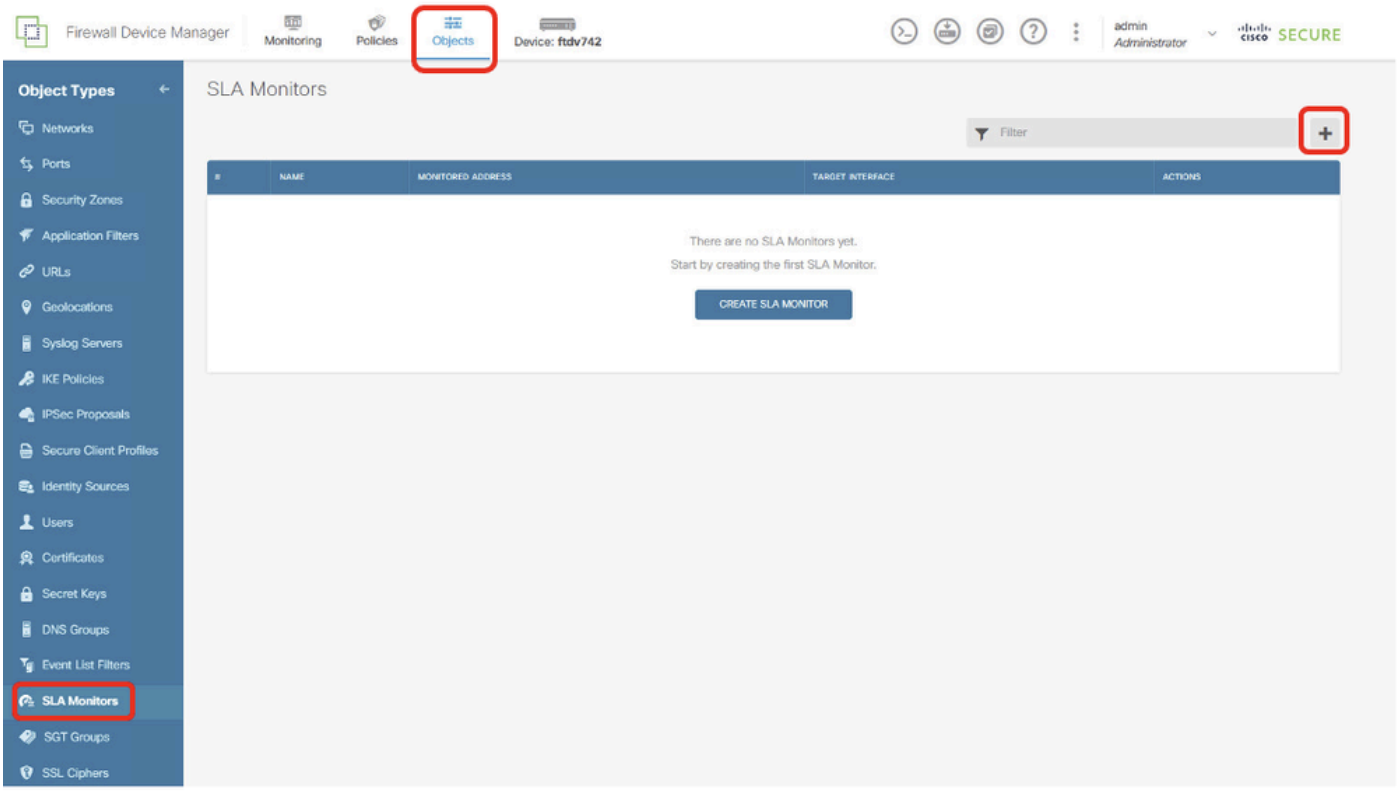
Stap 18.2. Maak een object voor het IP-adres van de ISP2-gateway. Geef de benodigde informatie. Klik op de knop OK.

- Naam: Buiten2ToSP2_192.168.40.4
- Type: Host
- Host: 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

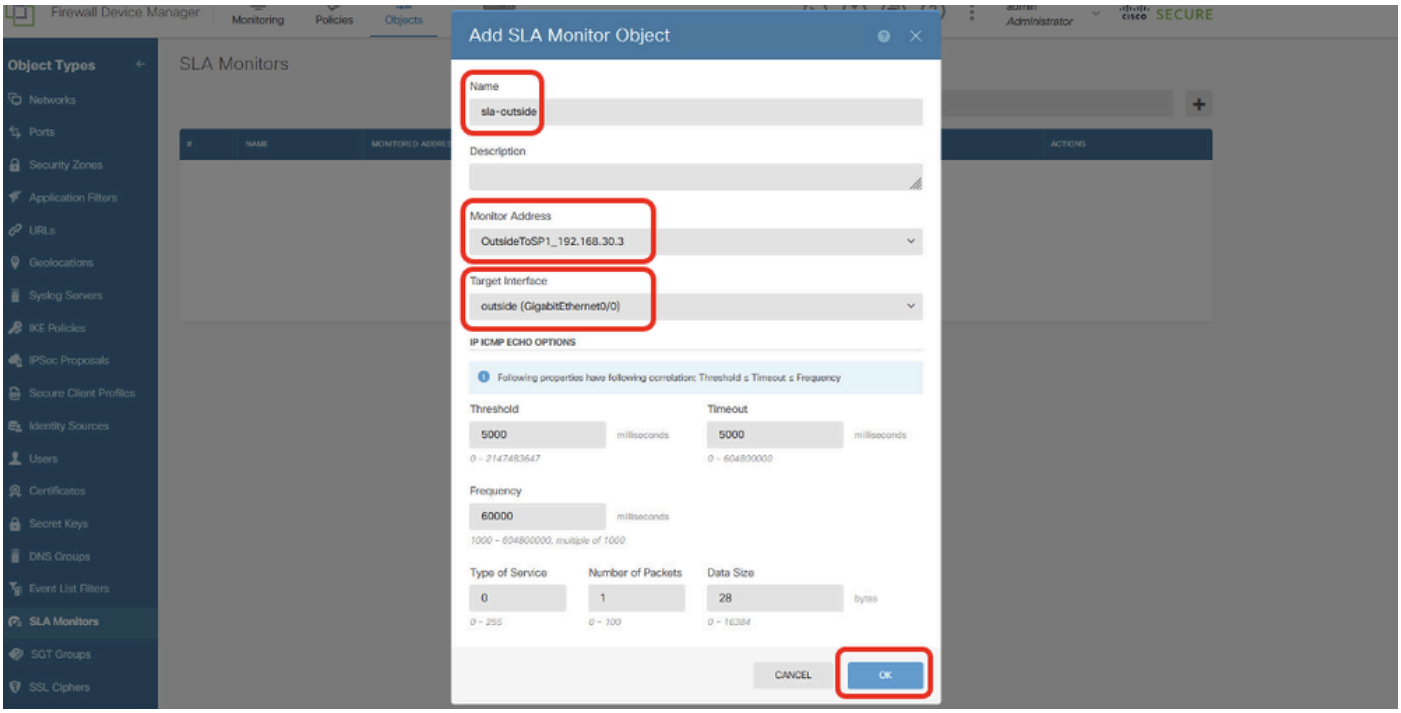
Stap 19. Maak een SLA-monitor. Navigeer naar objecten > Objecttypen > SLA-monitoren. Klik op + om een nieuwe SLA-monitor te maken.



Site1FTD_Create_SLAMonitor

Stap 19.1. Geef in het venster Add SLA Monitor Object de benodigde informatie voor de ISP1-gateway. Klik op OK om op te slaan.

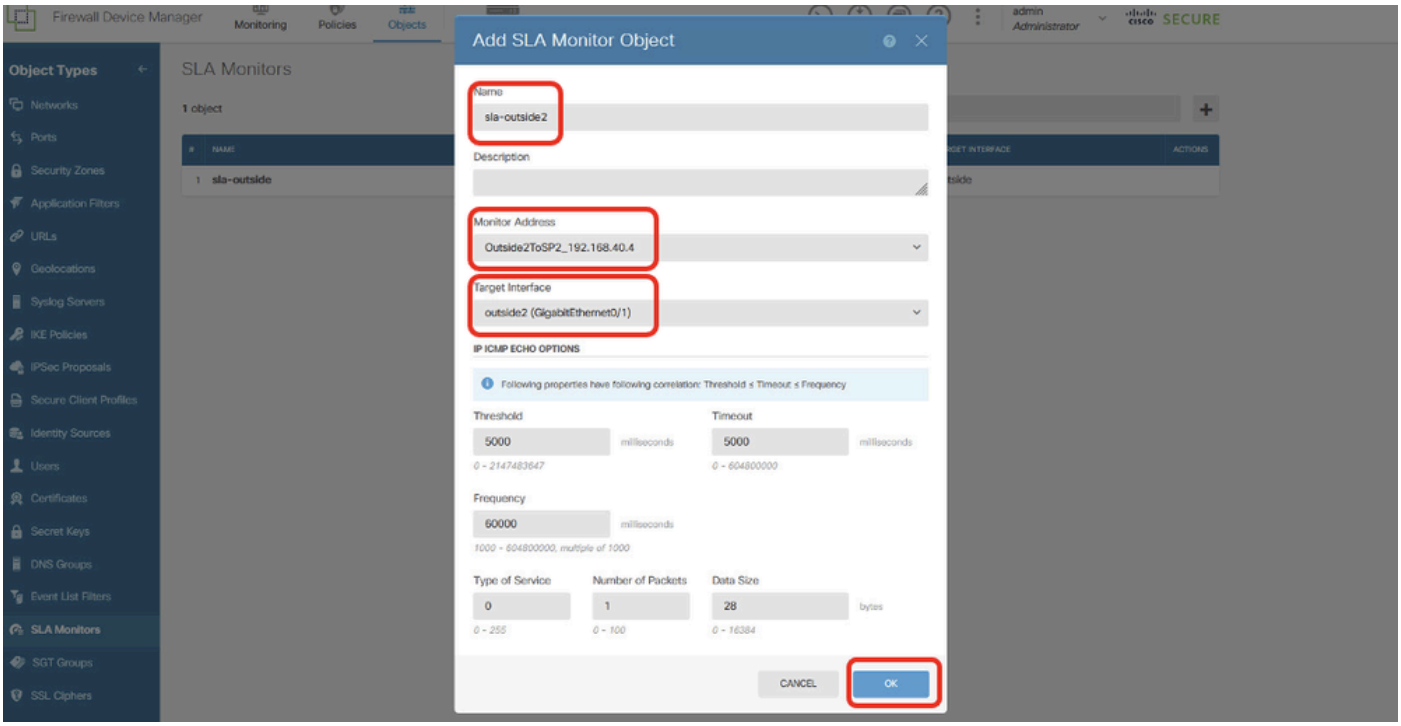
- Naam: buiten
- Monitoradres: BuitenToSP1_192.168.30.3
- Doelinterface: buiten (Gigabit Ethernet0/0)
- OPTIES VOOR IP ICMP-ECHO: standaard



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

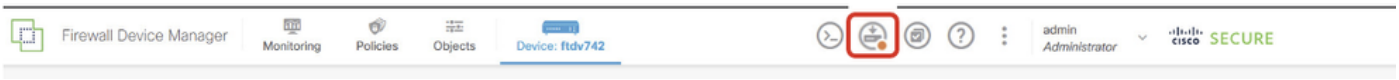
Stap 19.2. Klik op + om een nieuwe SLA-monitor voor ISP2-gateway te maken. Geef in het venster Add SLA Monitor Object de benodigde informatie voor de ISP2-gateway. Klik op OK om op te slaan.

- Naam: Sla-buiten2
- Monitoradres: Buiten2ToSP2_192.168.40.4
- Doelinterface: buiten2 (Gigabit Ethernet0/1)
- OPTIES VOOR IP ICMP-ECHO: standaard



Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

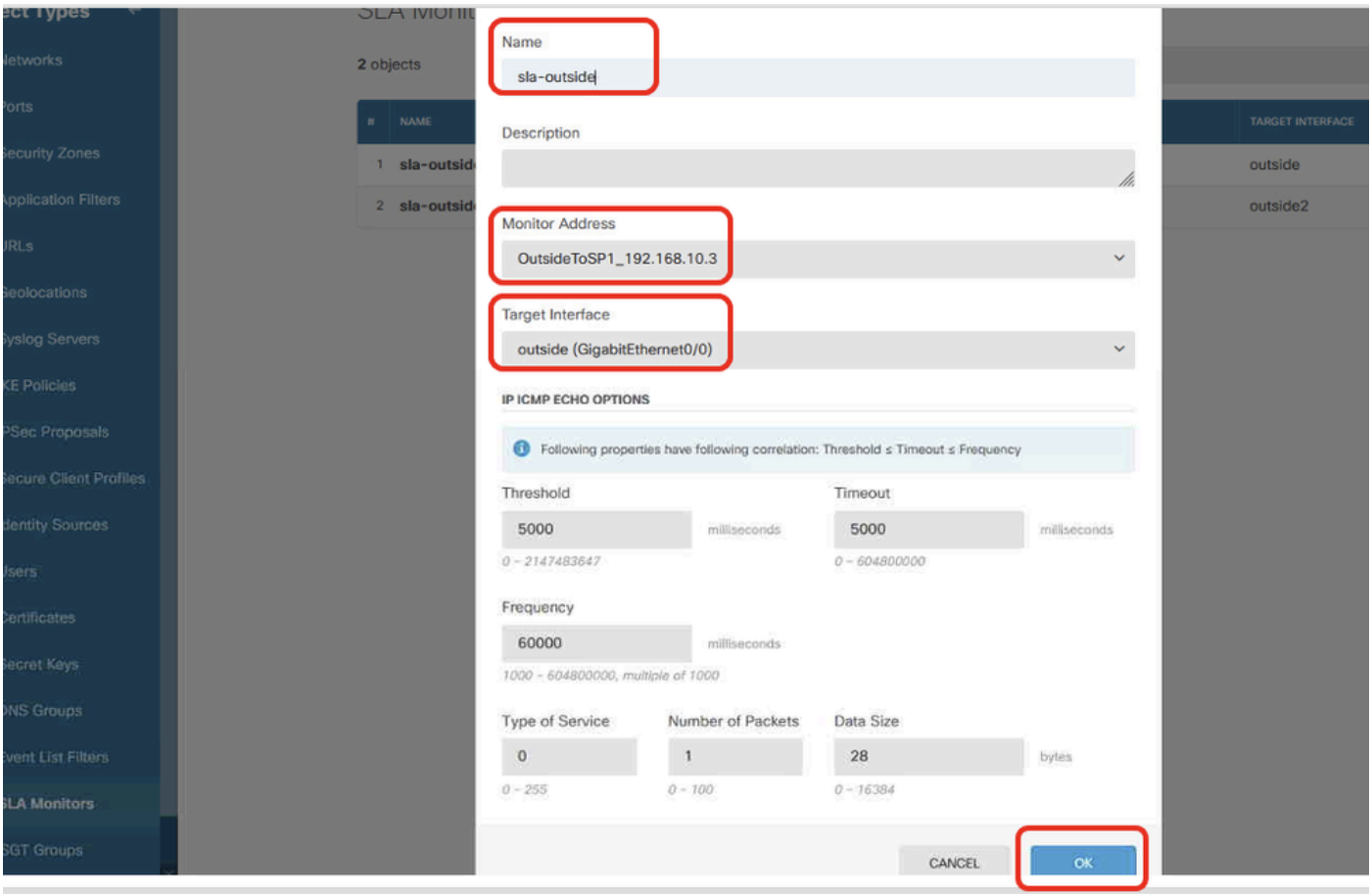
Stap 20. Implementeer de configuratiewijzigingen.



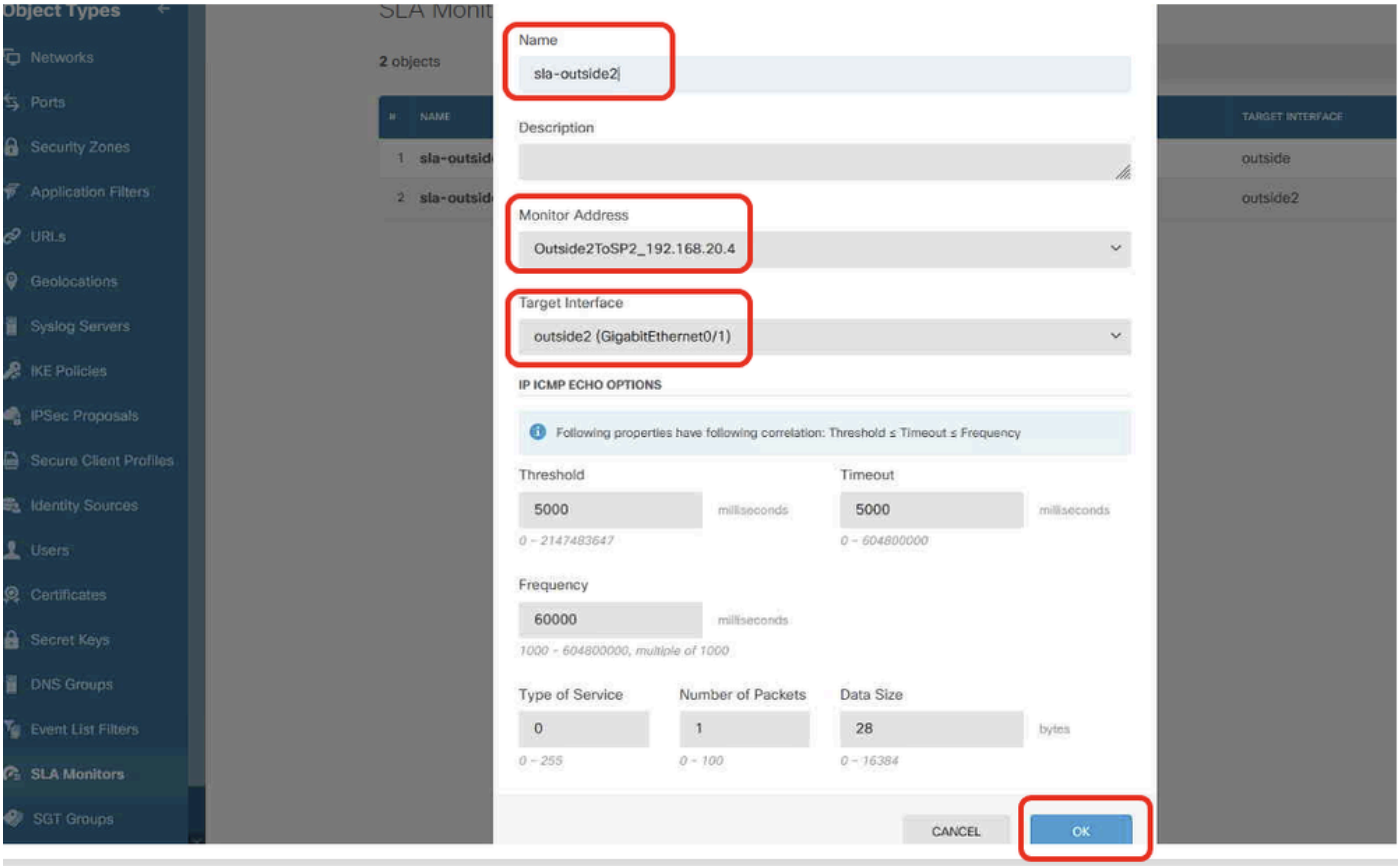
Site1FTD_Implementatie_Wijzigingen

Configuratie van Site2 FTD SLA-monitor

Stap 21. Herhaal stap 18. tot stap 20. maak een SLA-monitor met de bijbehorende parameters op Site2 FTD.



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

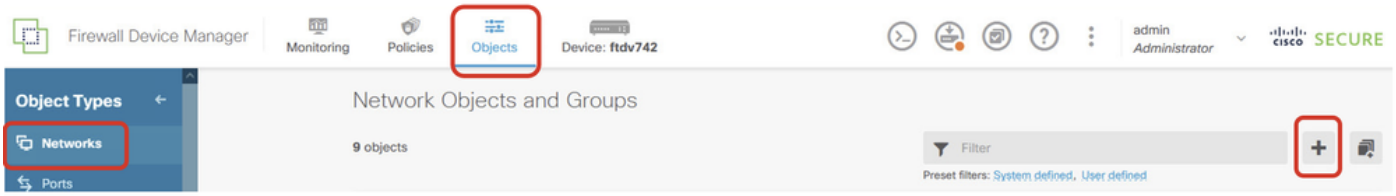


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

Configuraties op statische route

Statische routeconfiguratie van Site1 FTD

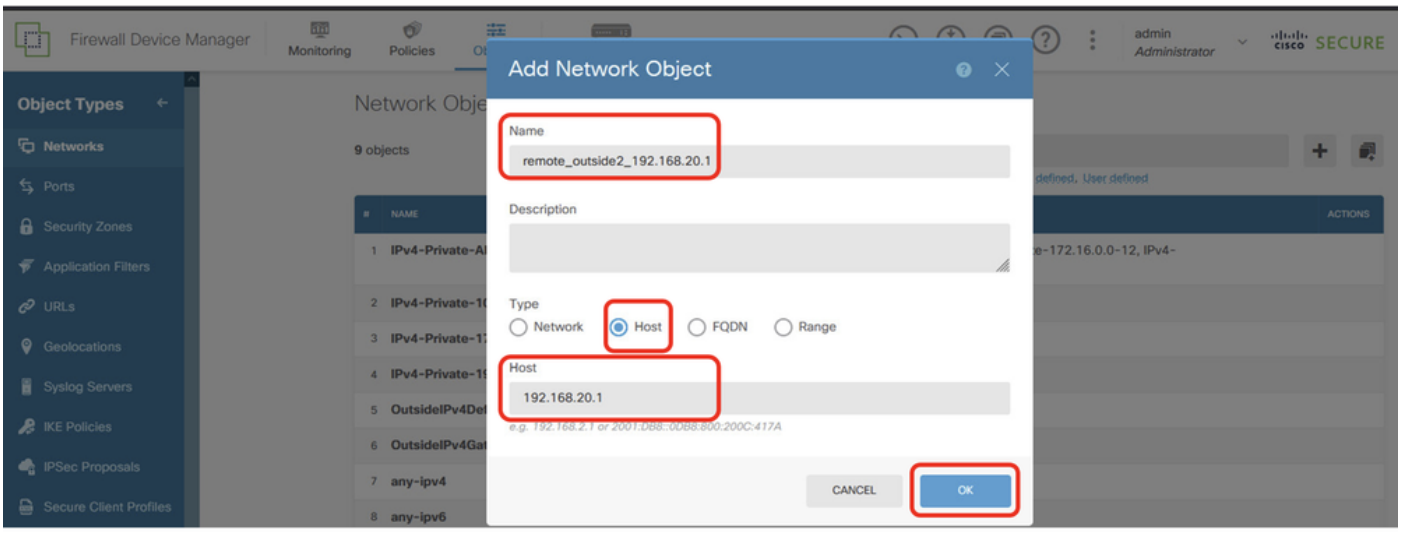
Stap 2. Maak nieuwe netwerkobjecten die door statische route voor Site1 FTD moeten worden gebruikt. Navigeer naar Objecten > Netwerken, klik op + knop.



Site1FTD_Create_Obj

Stap 2.1. Maak een object aan voor het IP-adres buiten 2 van peer Site2 FTD. Geef de benodigde informatie. Klik op de knop OK.

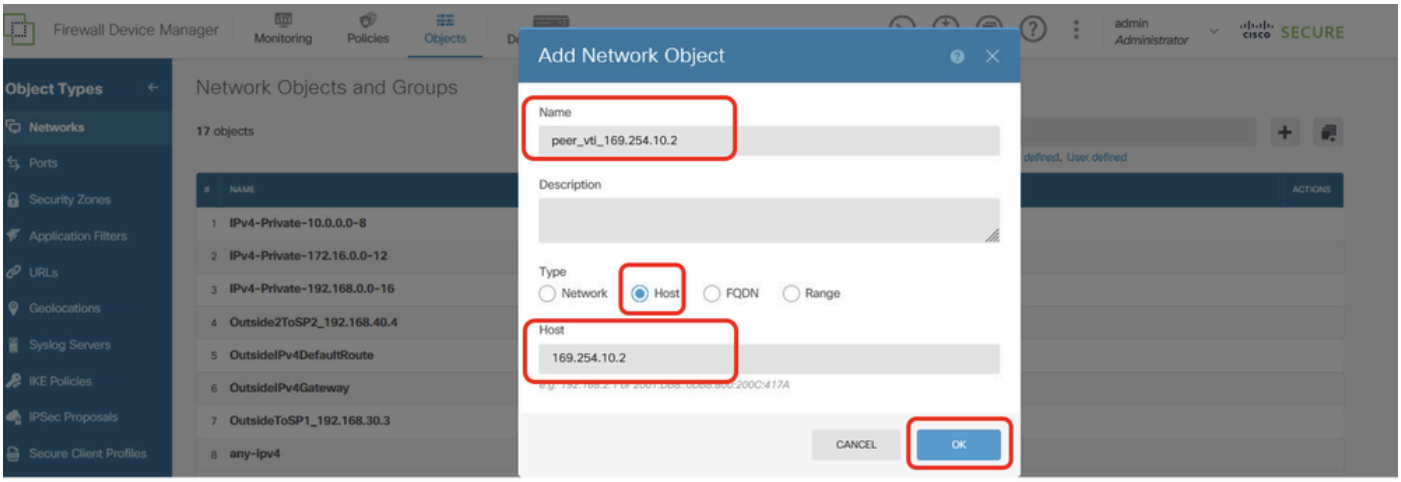
- Naam: remote_external2_192.168.20.1
- Type: GASTHEER
- Netwerk: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

Stap 2.2. Maak een object voor VTI Tunnel1 IP-adres van peer Site2 FTD. Geef de benodigde informatie. Klik op de knop OK.

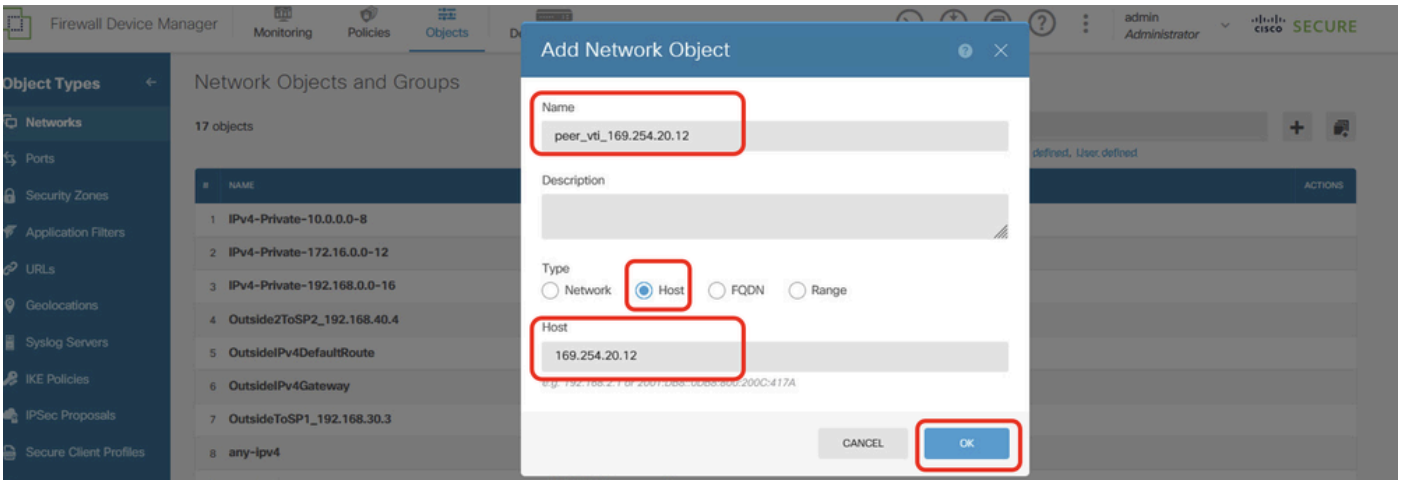
- Naam: peer_vti_169.254.10.2
- Type: GASTHEER
- Netwerk:169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

Stap 2.3. Maak een object voor VTI Tunnel2 IP-adres van peer Site2 FTD. Geef de benodigde informatie. Klik op de knop OK.

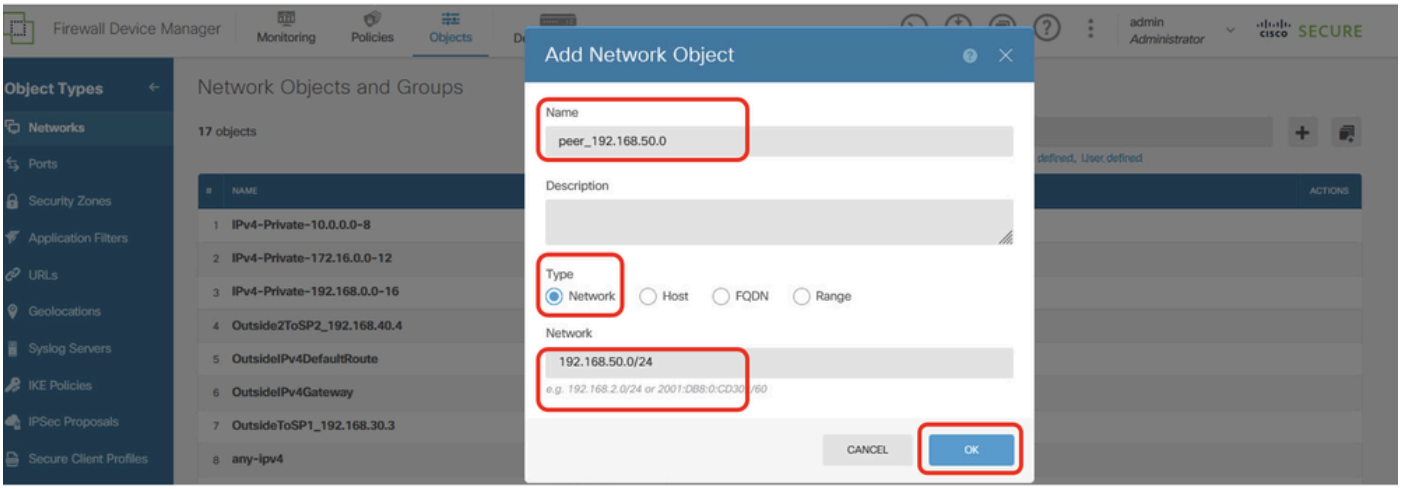
- Naam: peer_vti_169.254.20.12
- Type: GASTHEER
- Netwerk:169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

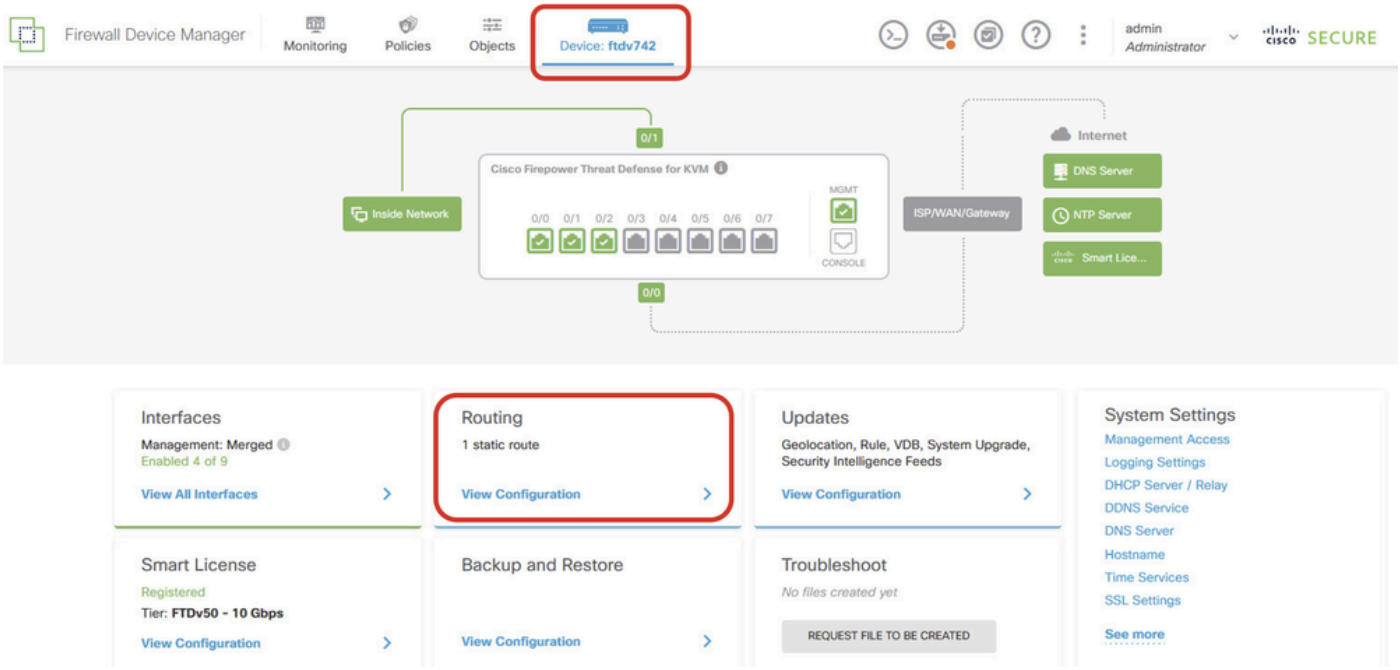
Stap 2.4. Maak een object voor binnen het netwerk van peer Site2 FTD. Geef de benodigde informatie. Klik op de knop OK.

- Naam: peer_192.168.50.0
- Type: NETWERK
- Netwerk:192.168.50.0/24

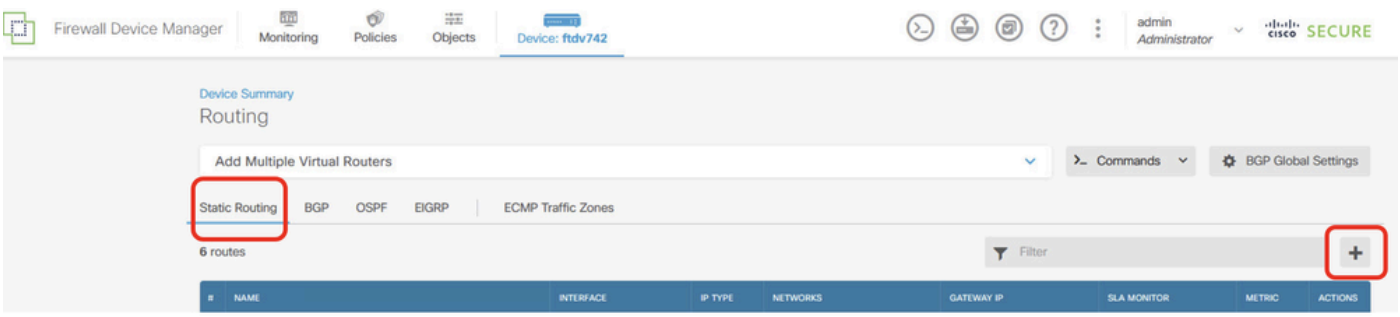


Site1FTD_Create_NetObj_StaticRoute_4

Stap 23. Navigeer naar apparaat > routing. Klik op Configuratie weergeven. Klik op het tabblad Statische routing. Klik op + knop om een nieuwe statische route toe te voegen.



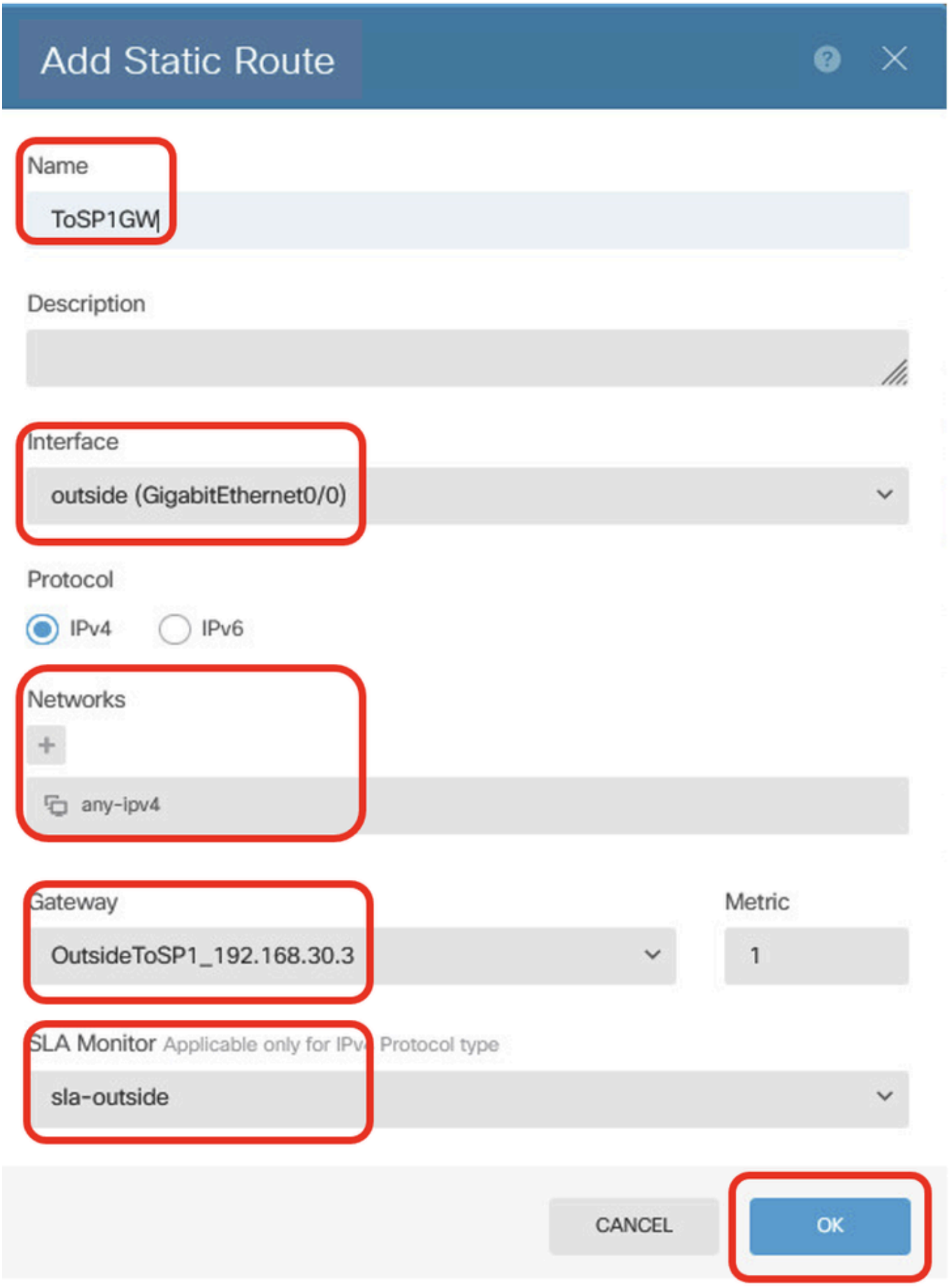
Site1FTD_View_Route_Configuration



Site1FTD_Add_Static_Route

Stap 23.1. Maak een standaardroute met behulp van de ISP1-gateway en SLA-bewaking. Als de ISP1-gateway een onderbreking ondervindt, keren de switches van het verkeer naar de back-up-standaardroute via ISP2. Zodra ISP1 herstelt, keert het verkeer terug naar het gebruik van ISP1. Verstrek de benodigde informatie. Klik op OK om op te slaan.

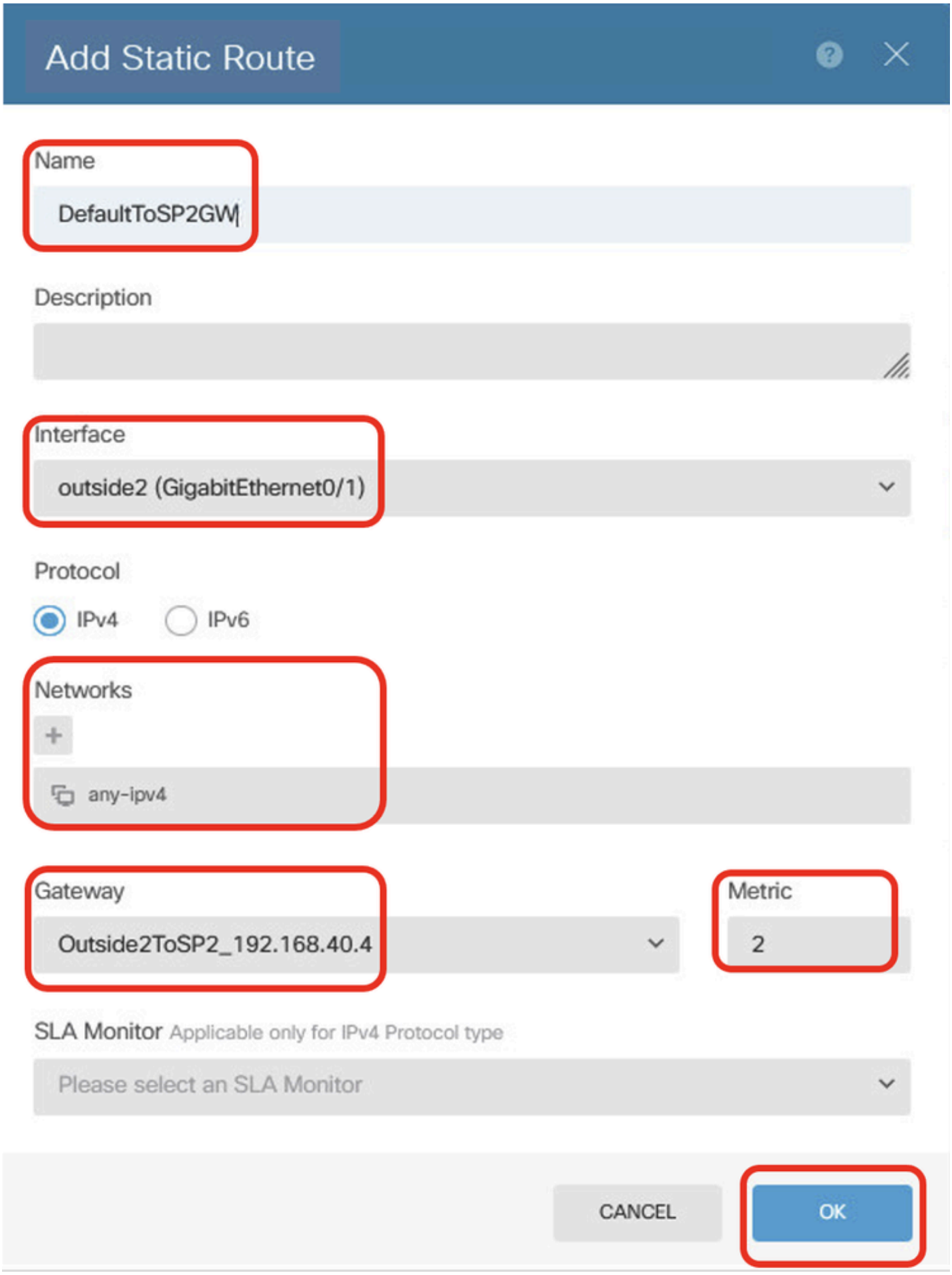
- Naam: ToSP1GW
- Interface: buiten (Gigabit Ethernet0/0)
- Protocol: IPv4
- Netwerken: Any-IP4
- Gateway: BuitenToSP1_192.168.30.3
- Metrisch: 1
- SLA-monitor: buiten



Site1FTD_Create_StaticRoute_1

Stap 23.2. Maak een back-up van de standaardroute via de gateway ISP2. Metriek moet hoger zijn dan 1. In dit voorbeeld is metriek 2. Geef de benodigde informatie op. Klik op OK om op te slaan.

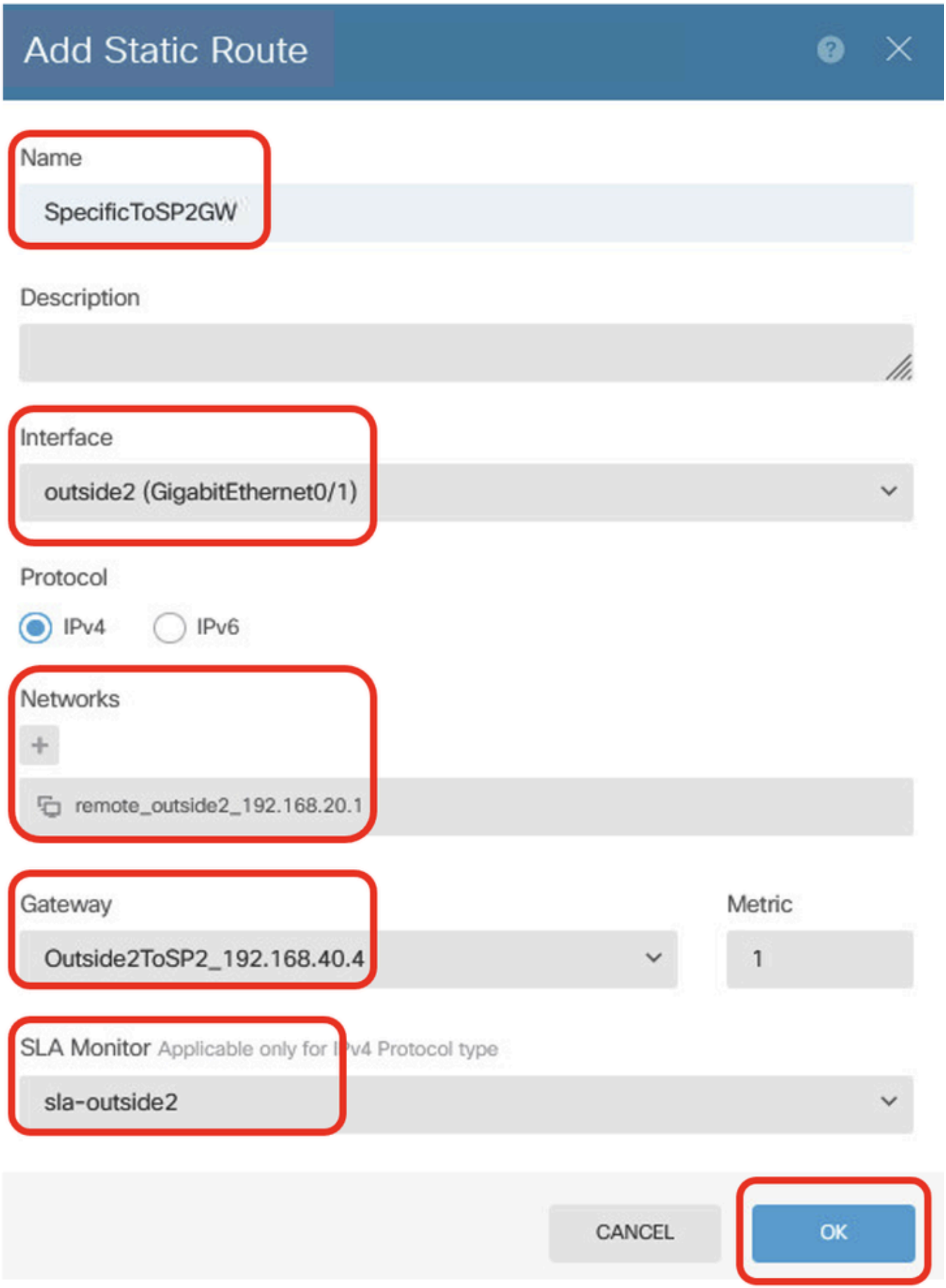
- Naam: StandaardToSP2GW
- Interface: buiten2 (Gigabit Ethernet0/1)
- Protocol: IPv4
- Netwerken: Any-IP4
- Gateway: Buiten2ToSP2_192.168.40.4
- Metrisch: 2



Site1FTD_Create_StaticRoute_2

Stap 23.3. Maak een statische route voor doelverkeer naar een buitenkant2 IP-adres van peer Site2 FTD via ISP2-gateway, met SLA-bewaking, gebruikt voor het opzetten van VPN met buiten2 van Site2 FTD. Geef de benodigde informatie. Klik op OK om op te slaan.

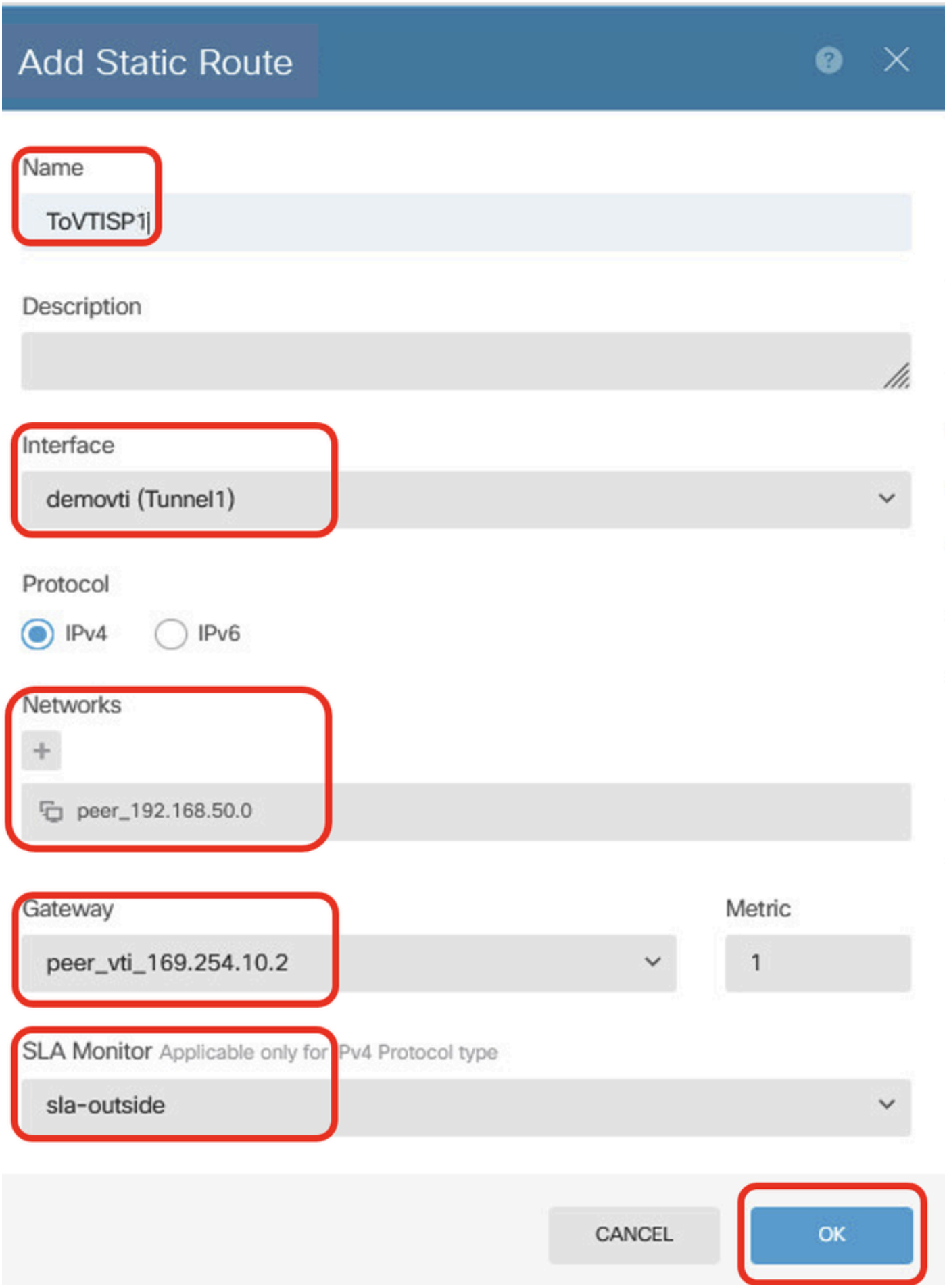
- Naam: Specifiek voorSP2GW
- Interface: buiten2 (Gigabit Ethernet0/1)
- Protocol: IPv4
- Netwerken: remote_external2_192.168.20.1
- Gateway: Buiten2ToSP2_192.168.40.4
- Metrisch: 1
- SLA-monitor: Sla-buiten2



Site1FTD_Create_StaticRoute_3

Stap 23.4. Maak een statische route voor bestemmingsverkeer naar het binnennetwerk van peer Site2 FTD via peer VTI Tunnel 1 van Site2 FTD als de gateway, met SLA-bewaking voor het versleutelen van clientverkeer via Tunnel 1. Als de ISP1-gateway een onderbreking ondervindt, switches van VPN-verkeer naar VTI Tunnel 2 van ISP2. Zodra ISP1 herstelt, keert het verkeer naar VTI Tunnel 1 van ISP1 terug. Geef de benodigde informatie. Klik op OK om op te slaan.

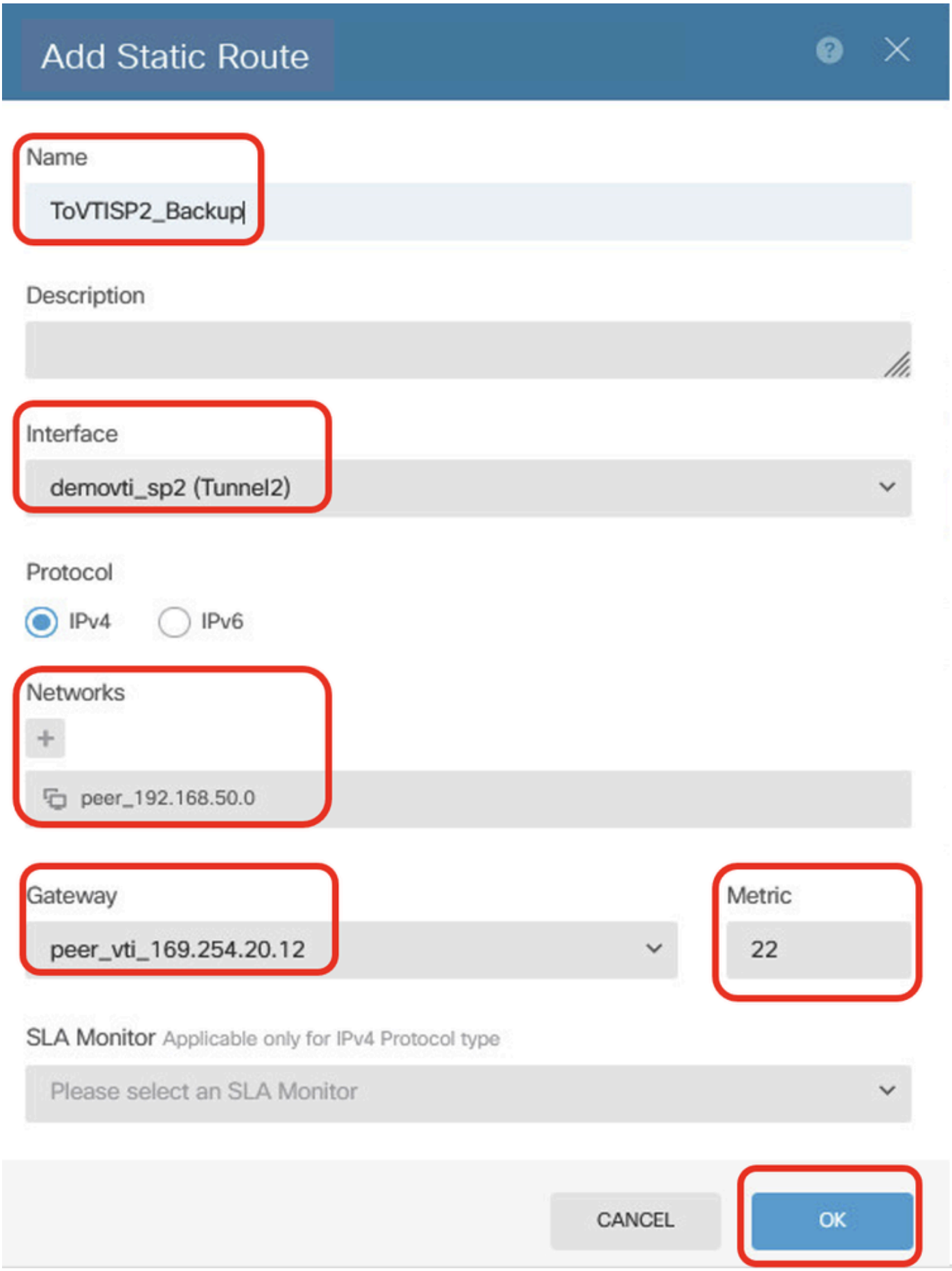
- Naam: Naar VTISP1
- Interface: Demovti(Tunnel1)
- Protocol: IPv4
- Netwerken: peer_192.168.50.0
- Gateway: peer_vti_169.254.10.2
- Metrisch: 1
- SLA-monitor: buiten



Site1FTD_Create_StaticRoute_4

Stap 23.5. Maak een back-up statische route voor bestemmingsverkeer naar het binnennetwerk van peer Site2 FTD via peer VTI Tunnel 2 van Site2 FTD als de gateway, gebruikt voor het versleutelen van clientverkeer via Tunnel 2. Stel de metriek in op een waarde hoger dan 1. In dit voorbeeld is metriek 22. Verstrek de benodigde informatie. Klik op OK om op te slaan.

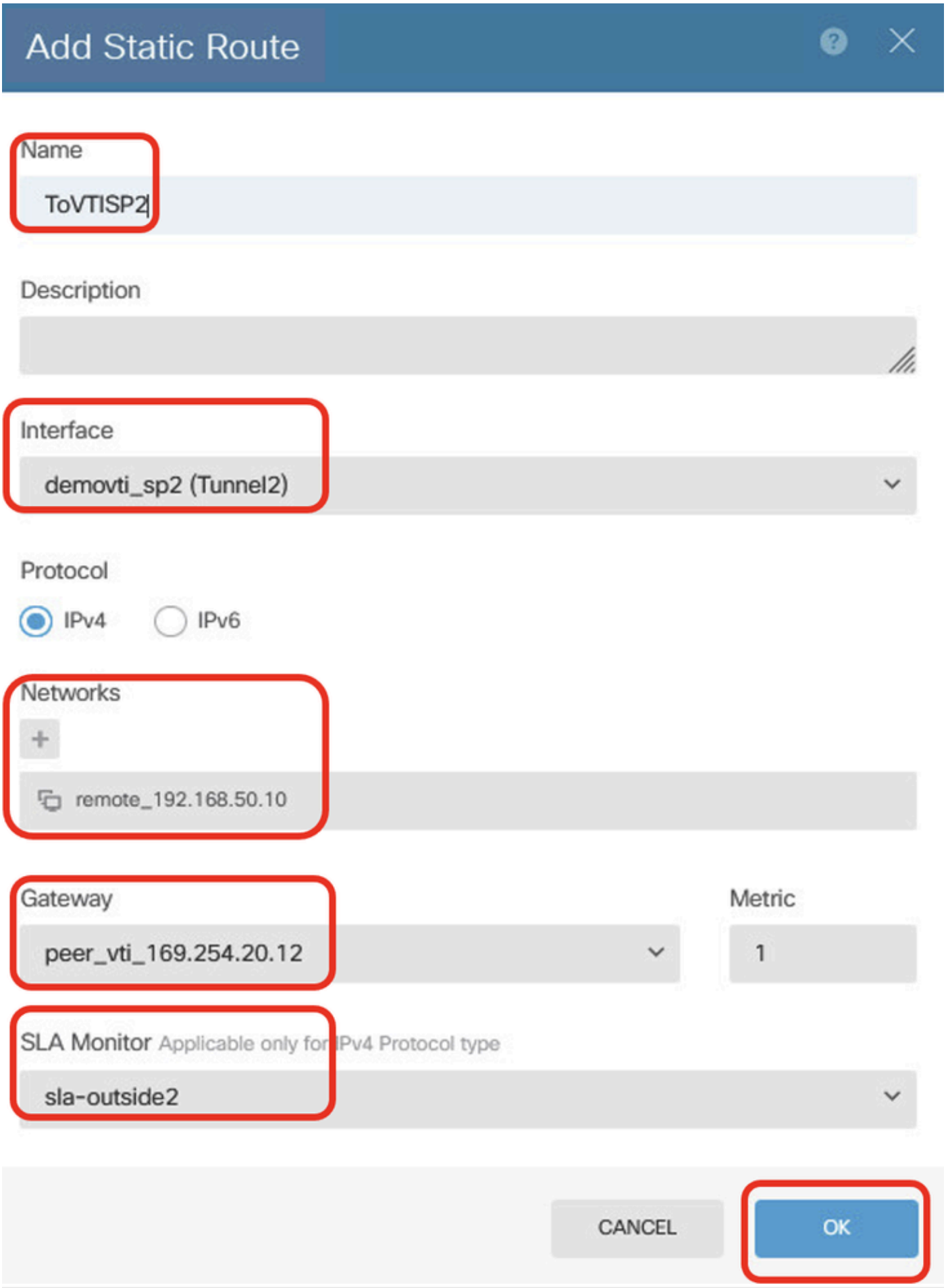
- Naam: Naar VTISP2_Backup
- Interface: demovti_sp2(Tunnel2)
- Protocol: IPv4
- Netwerken: peer_192.168.50.0
- Gateway: peer_vti_169.254.20.12
- Metrisch: 22



Site1FTD_Create_StaticRoute_5

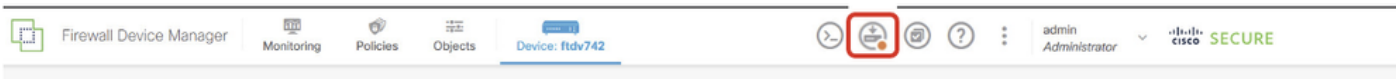
Stap 23.6. Maak een statische route voor PBR-verkeer. Bestemmingsverkeer naar Site2 Client2 via peer-VTI Tunnel 2 van Site2 FTD als gateway, met SLA-bewaking. Verstrek de nodige informatie. Klik op OK om op te slaan.

- Naam: VTISP2
- Interface: demovti_sp2(Tunnel2)
- Protocol: IPv4
- Netwerken: afstandsbediening_192.168.50.10
- Gateway: peer_vti_169.254.20.12
- Metrisch: 1
- SLA-monitor: Sla-buiten2



Site1FTD_Create_StaticRoute_6

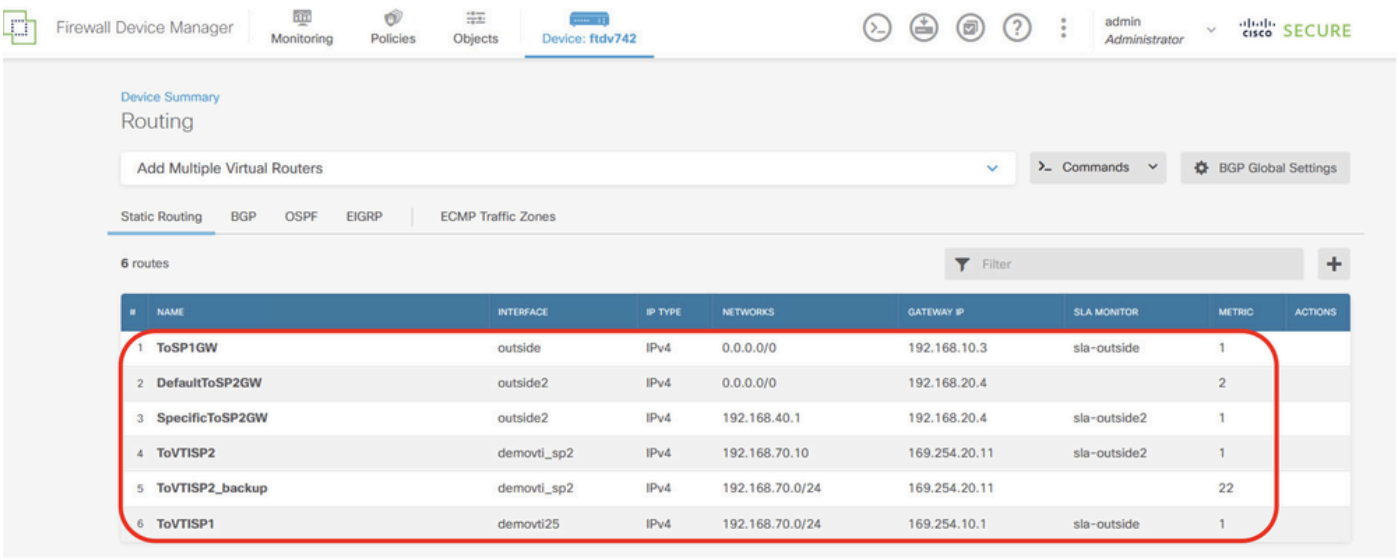
Stap 24. Implementeer de configuratiewijzigingen.



Site1FTD_Implementatie_Wijzigingen

Site2 FTD statische routeconfiguratie

Stap 25. Herhaal stap 22 tot en met 24 om een statische route met de bijbehorende parameters voor Site2 FTD te creëren.



Site2FTD_Create_StaticRoute

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt. Navigeren naar de CLI van Site1 FTD en Site2 FTD via console of SSH.

Zowel ISP1 als ISP2 Work FineReader

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
```

Route

```
// 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-monitor

```
// 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 Test

Scenario 1. Site1 client1 pingt Site2 client1.

Voordat u pingelt, controleer de tellers van show crypto ipsec sa | Inc-interface:|encap|decap op Site1 FTD.

In dit voorbeeld, toont Tunnel1 1497 pakketten voor inkapseling en 1498 pakketten voor decapsulation.

```
// 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 pingt Site2 Client1.

```
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
```

Controleer de tellers van show crypto ipsec sa | inc-interface:|encap|decap op Site1 FTD na ping succesvol.

In dit voorbeeld, toont Tunnel 1 1502 pakketten voor inkapseling en 1503 pakketten voor decapsulation, met beide tellers die met 5 pakketten stijgen, die 5 pingechoverzoeken aanpassen. Dit geeft aan dat pings van Site1 Client1 naar Site2 Client1 worden gerouteerd via ISP1 Tunnel 1. Tunnel 2 toont geen toename in inkapseling- of decapsulatietellers, bevestigend dat het niet wordt gebruikt voor dit verkeer.

```
// 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
```

Scenario 2. Site1 client2 pingt Site2 client2.

Voordat u pingelt, controleer de tellers van show crypto ipsec sa | Inc-interface:|encap|decap op Site1 FTD.

In dit voorbeeld, toont Tunnel2 21 pakketten voor inkapseling en 20 pakketten voor decapsulation.

```
// 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 pingt Site2 Client2 met succes.

```
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
```

Controleer de tellers van show crypto ipsec sa | inc-interface:|encap|decap op Site1 FTD na ping succesvol.

In dit voorbeeld, toont Tunnel 2 26 pakketten voor inkapseling en 25 pakketten voor decapsulation, met beide tellers die met 5 pakketten stijgen, die 5 pingelen echoverzoeken aanpassen. Dit geeft aan dat pings van Site1 Client2 naar Site2 Client2 worden gerouteerd via ISP2 Tunnel 2. Tunnel 1 toont geen toename in inkapseling- of decapsulatietellers, bevestigend dat het niet wordt gebruikt voor dit verkeer.

```
// 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
```

ISP1 ervaart en onderbreking terwijl ISP2 FineReader werkt

In dit voorbeeld, handsluiting de interface E0/1 op ISP1 om ISP1 te simuleren die een onderbreking ervaren.

```
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

De Tunnel 1 ging omlaag. Enkel Tunnel2 is actief met IKEV2 SA.

```
// 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
      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
```

Route

In routetabel worden de back-uproutes van kracht.

```
// 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-monitor

Op Site1 FTD, toont de SLA-monitor entry nummer 855903900 timeout (Doeladres is 192.168.30.3) voor ISP1.

```
// 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 Test

Voordat u pingelt, controleer de tellers van show crypto ipsec sa | Inc-interface:|encap|decap op Site1 FTD.

In dit voorbeeld, toont Tunnel2 36 pakketten voor inkapseling en 35 pakketten voor decapsulation.

```
// 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 pingt Site2 Client1.

```
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 pingt Site2 Client2 met succes.

```
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
```

Controleer de tellers van show crypto ipsec sa | inc-interface:|encap|decap op Site1 FTD na succesvolle ping

In dit voorbeeld, toont Tunnel 2 46 pakketten voor inkapseling en 45 pakketten voor decapsulation, met beide tellers die met 10 pakketten stijgen, die 10 pingelen echoverzoeken aanpassen. Dit geeft aan dat de pingpakketten via ISP2 Tunnel 2 worden gerouteerd.

```
// 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
```

ISP2 ervaart en onderbreking terwijl ISP1 FineReader werkt

In dit voorbeeld, handsluiting de interface E0/1 op ISP2 om ISP2 te simuleren die een onderbreking ervaren.

```
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

De Tunnel2 ging omlaag. Enkel Tunnel1 is actief met IKEV2 SA.

```
// 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
```

Route

In routetabel verdween de aan ISP2 gerelateerde route voor PBR verkeer.

```
// 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-monitor

Op Site1 FTD, toont de SLA-monitor entry nummer 188426425 timeout (Doeladres is 192.168.40.4) voor ISP2.

```
// 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 Test

Voordat u pingelt, controleer de tellers van show crypto ipsec sa | Inc-interface:|encap|decap op Site1 FTD.

In dit voorbeeld, toont Tunnel 1 74 pakketten voor inkapseling en 73 pakketten voor

decapsulation.

```
// 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 pingt Site2 Client1.

```
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 pingt Site2 Client2 met succes.

```
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
```

Controleer de tellers van show crypto ipsec sa | inc-interface:|encap|decap op Site1 FTD na ping succesvol.

In dit voorbeeld, toont Tunnel 1 84 pakketten voor inkapseling en 83 pakketten voor decapsulation, met beide tellers die met 10 pakketten stijgen, die 10 pingelen echoverzoeken aanpassen. Dit wijst erop dat de pingpakketten via ISP1 Tunnel 1 worden gerouteerd.

```
// 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
```

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 PBR sectie op te lossen.

```
debug policy-route
```

U kunt deze debug-opdrachten gebruiken om problemen op te lossen in het gedeelte SLA Monitor.

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

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.