Routegebaseerde VPN configureren met statische route op FTD beheerd door FDM

Inhoud

Inleiding

In dit document wordt beschreven hoe u een statische route-gebaseerde site naar site VPN-tunnel configureert op een FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een goed begrip van hoe een VPN tunnel werkt.
- Voorkennis van het navigeren door de Firepower Device Manager (FDM).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

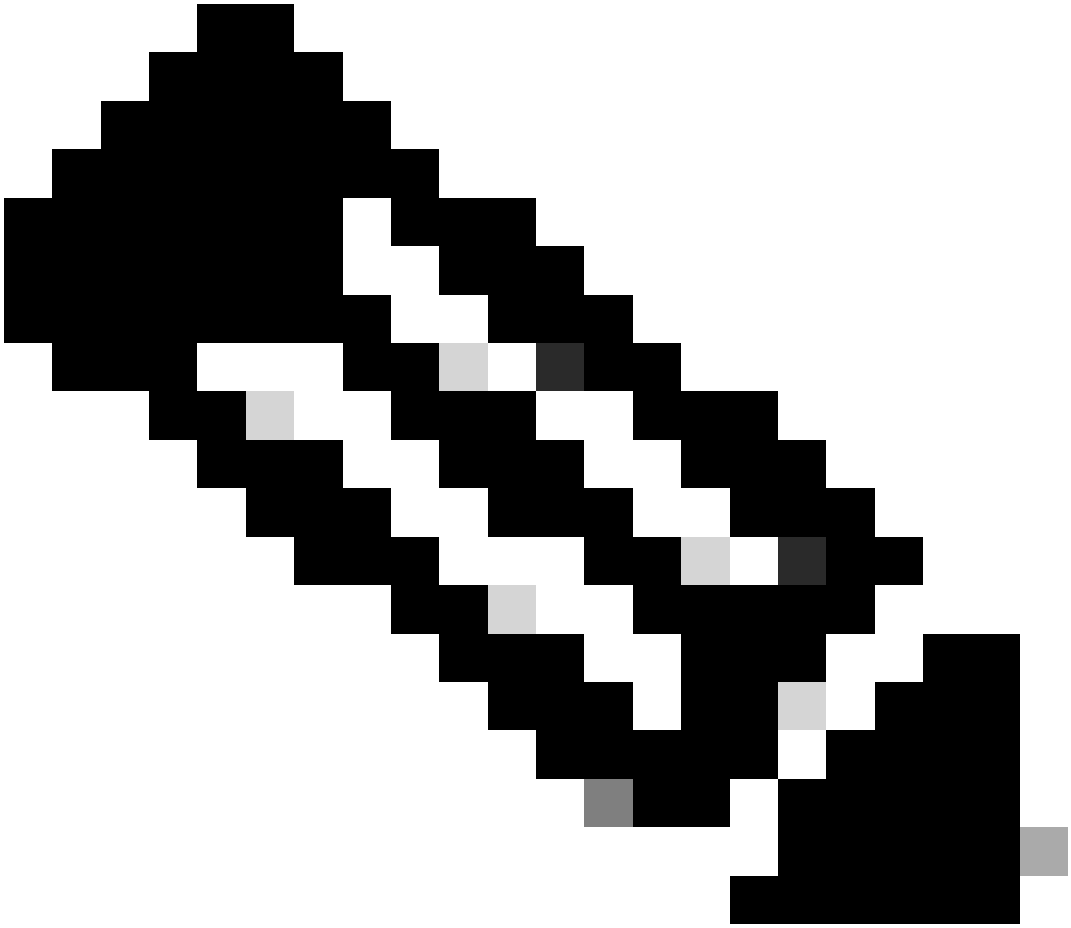
- Cisco Firepower Threat Defense (FTD) versie 7.0 wordt beheerd door Firepower Device Manager (FDM).

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

Met routegebaseerde VPN kan interessant verkeer worden gecodeerd of via een VPN-tunnel worden verzonden en verkeersroutering worden gebruikt in plaats van een beleid / toegangslijst zoals in een op beleid gebaseerde of op Crypto-map gebaseerde VPN. Het encryptiedomein is ingesteld om elk verkeer toe te staan dat de IPsec-tunnel binnenkomt. IPsec De lokale en externe verkeersselectors zijn ingesteld op 0.0.0.0/0.0.0.0. Dit betekent dat elk verkeer dat naar de IPsec-tunnel wordt geleid, wordt gecodeerd, ongeacht het bron- / bestemmingssubnet.

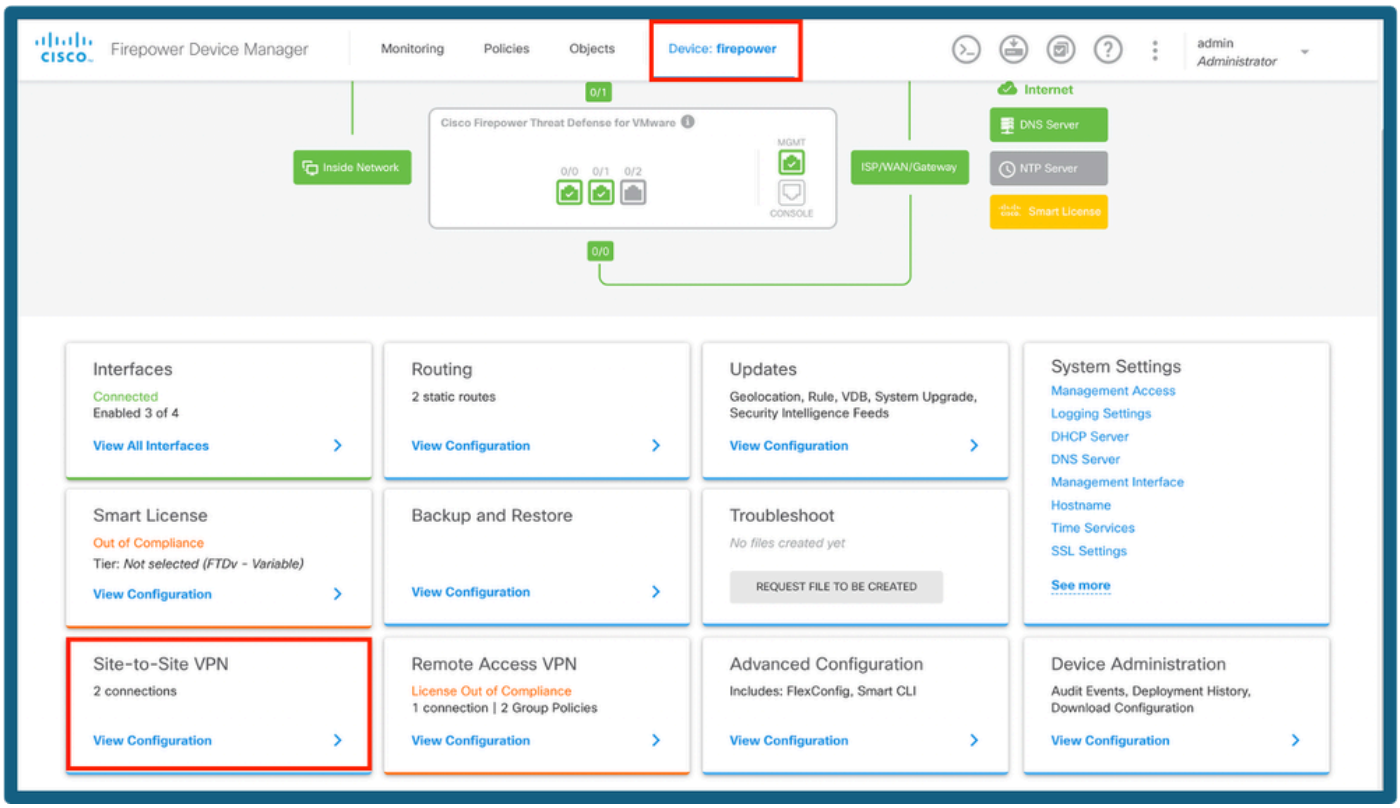
Dit document richt zich op de configuratie van de statische Virtual Tunnel Interface (SVTI).



> Opmerking: er is geen extra licentie nodig, Route Based VPN kan worden geconfigureerd in zowel Licensed als Evaluation Modes. Zonder crypto-compliance (Export Controlled Features Enabled) kan alleen DES worden gebruikt als een coderingsalgoritme.

Configuratiestappen op FDM

Stap 1. Navigeer naar Apparaat > Site-to-site.



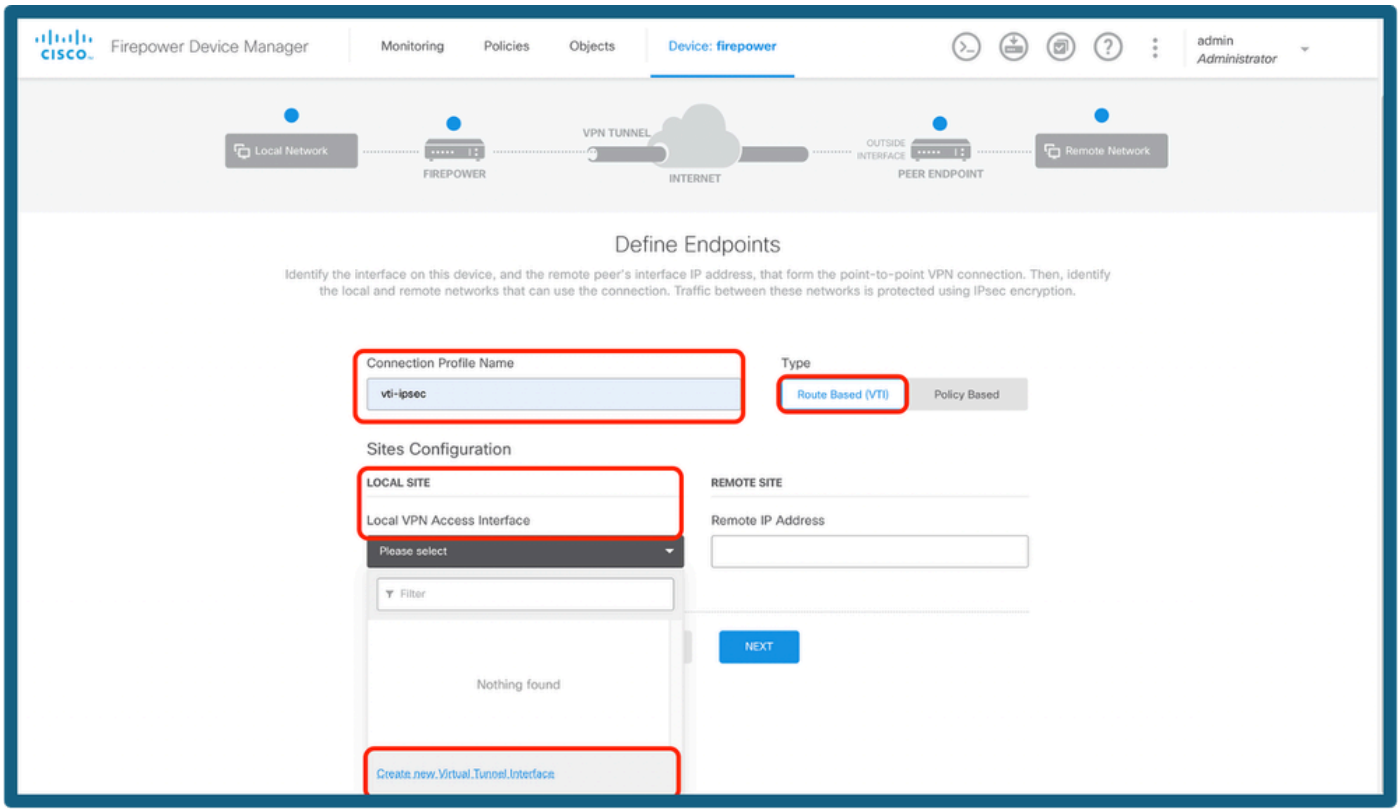
FDM-dashboard

Stap 2. Klik op het + pictogram om een nieuwe site aan de siteverbinding toe te voegen.

S2S-verbinding toevoegen

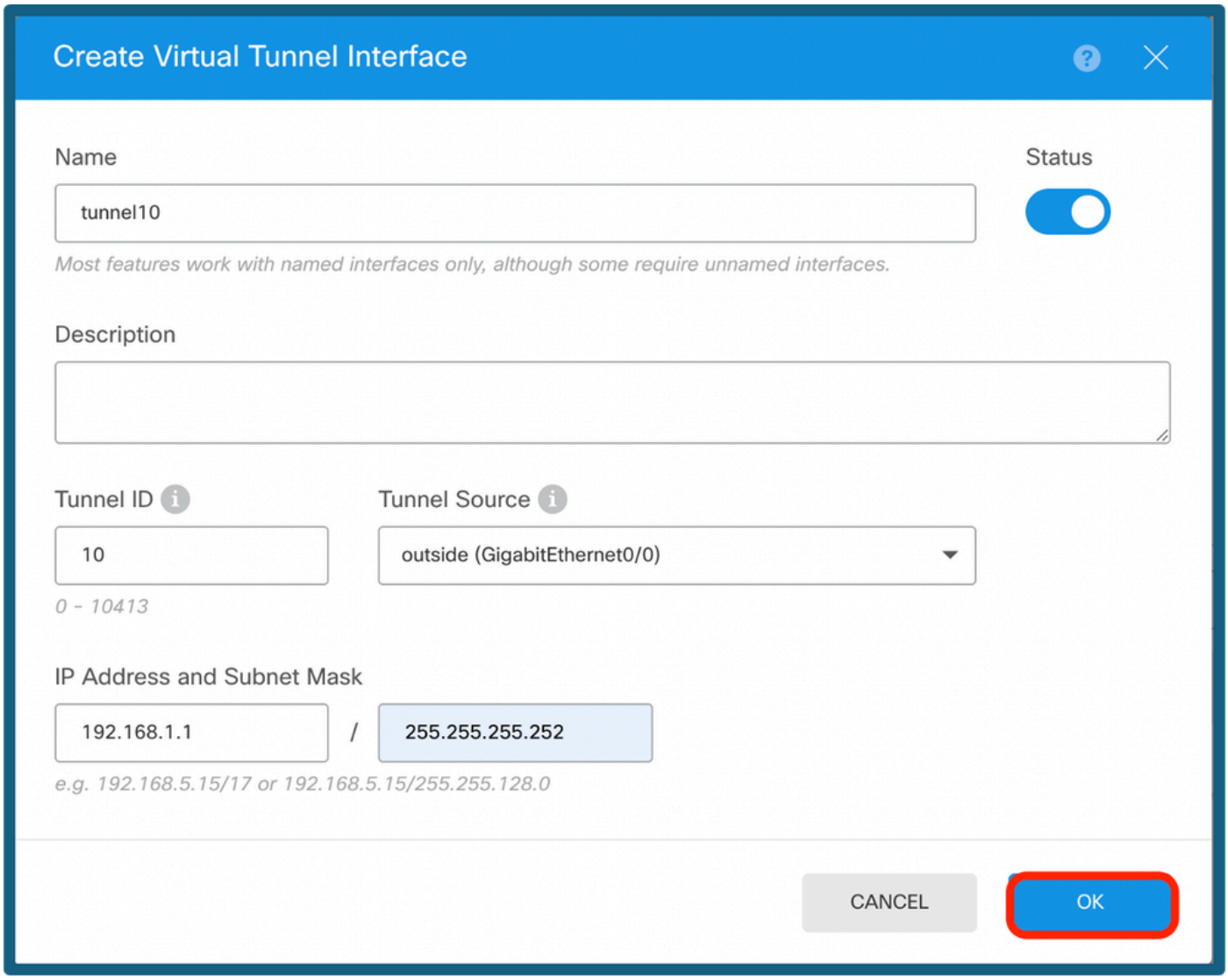
Stap 3: Geef een topologienaam op en selecteer het type VPN als Route Based (VTI).

Klik op Local VPN Access Interface en klik vervolgens op Create new Virtual Tunnel Interface of selecteer een van de bestaande lijsten.



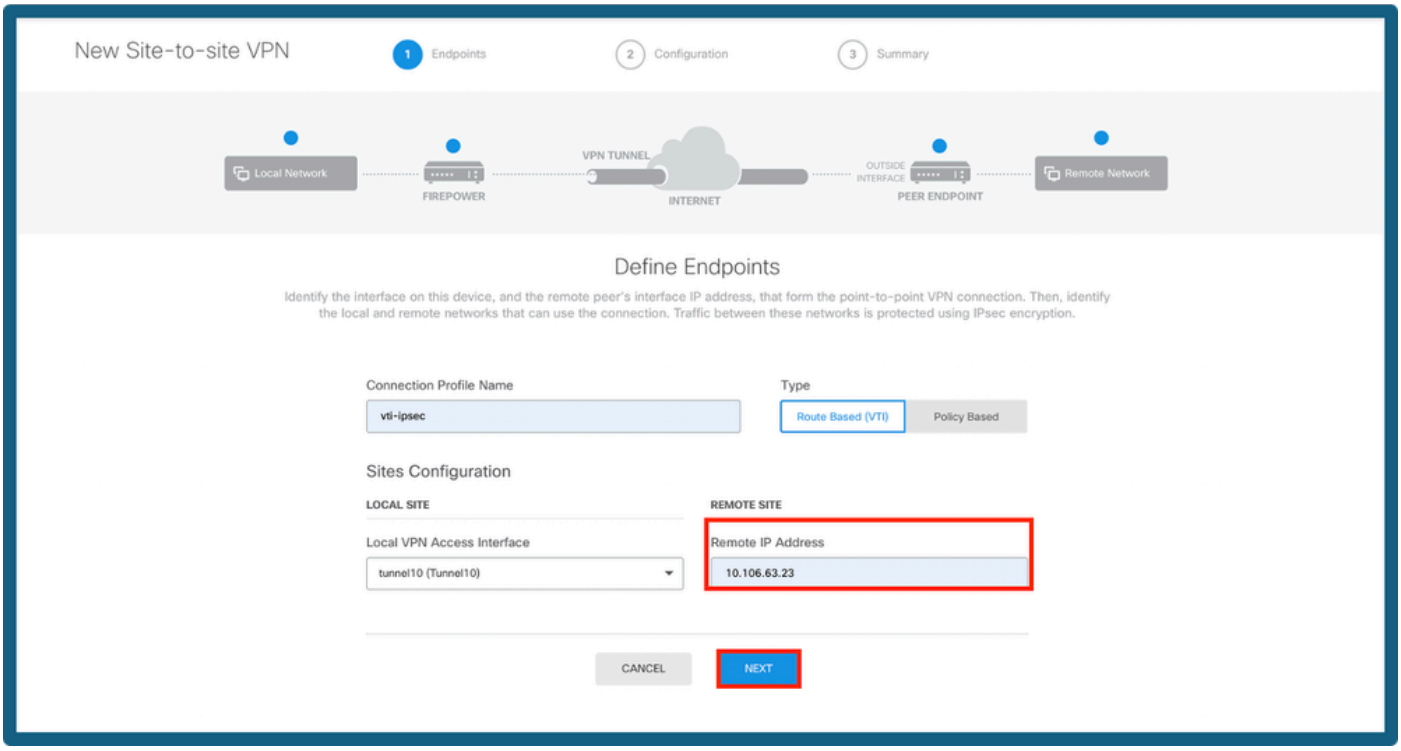
Tunnel-interface toevoegen

Stap 4. Definieer de parameters van de nieuwe virtuele tunnelinterface. Klik op OK.



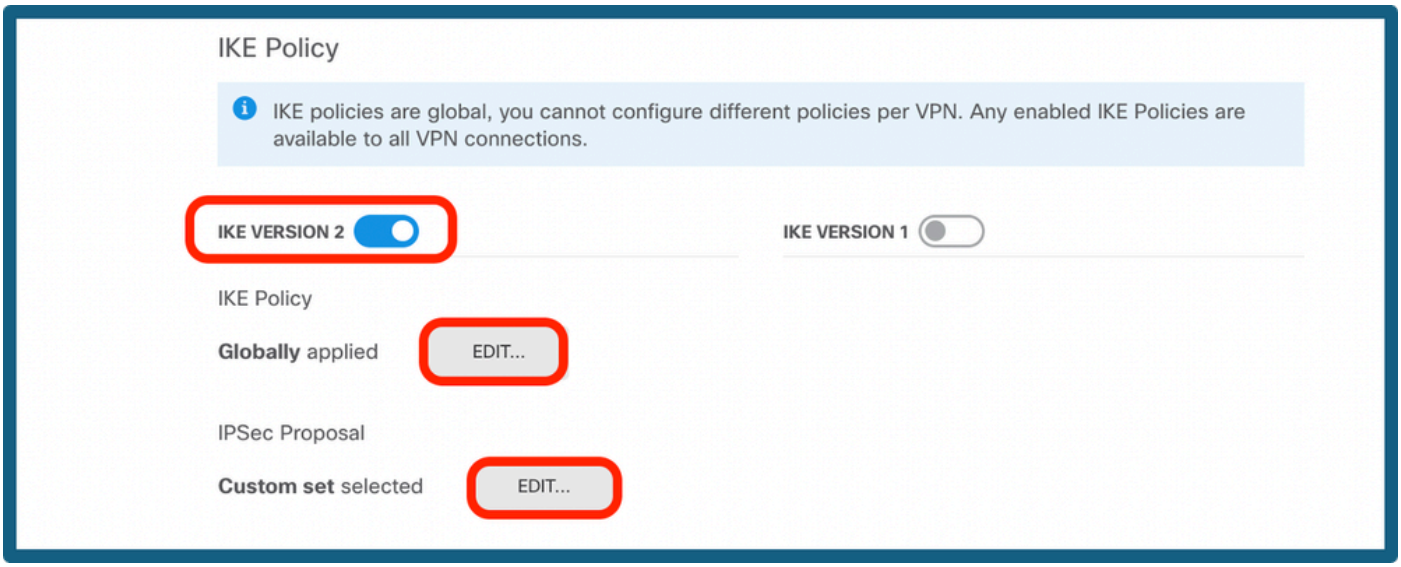
VTI-configuratie

Stap 5. Kies de nieuw gemaakte VTI of een VTI die bestaat onder Virtual Tunnel Interface.Geef het externe IP-adres op.



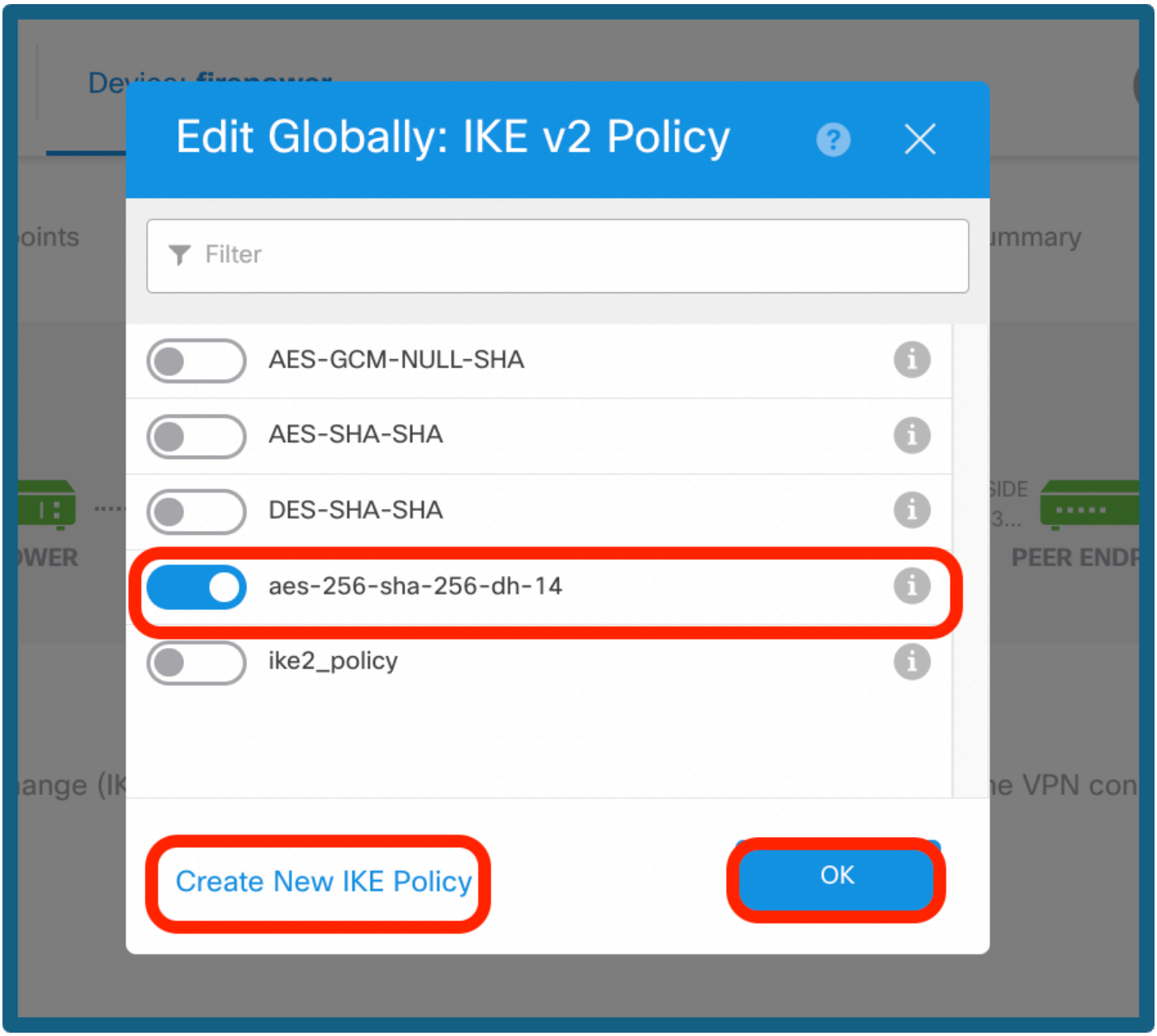
Peer IP toevoegen

Stap 6. Kies de IKE-versie en kies de knop Bewerken om de IKE- en IPsec-parameters in te stellen zoals weergegeven in de afbeelding.

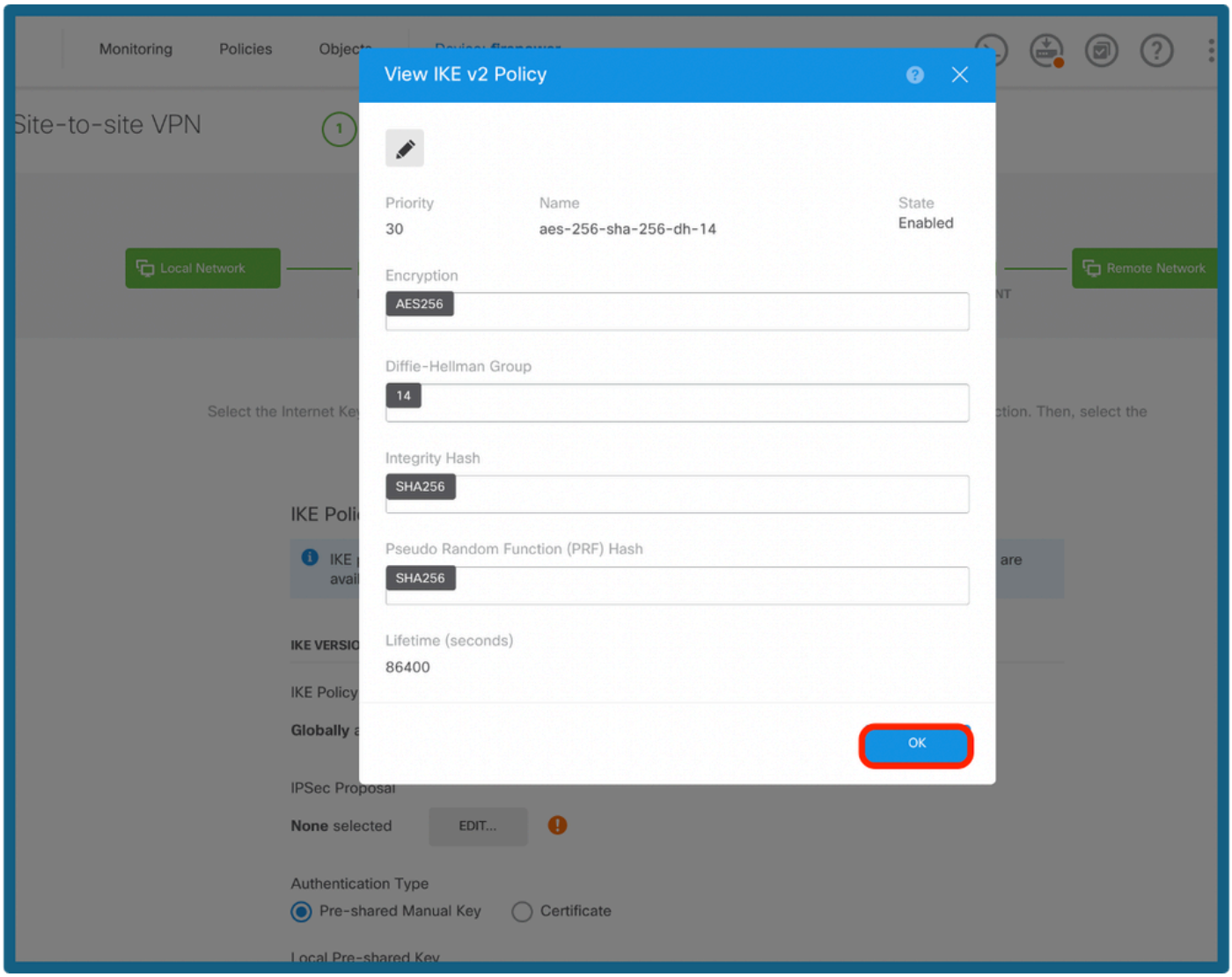


IKE-versie configureren

Stap 7a. Kies de knop IKE-beleid zoals weergegeven in de afbeelding en klik op ok of Nieuwe IKE-beleid maken, als u een nieuw beleid wilt maken.

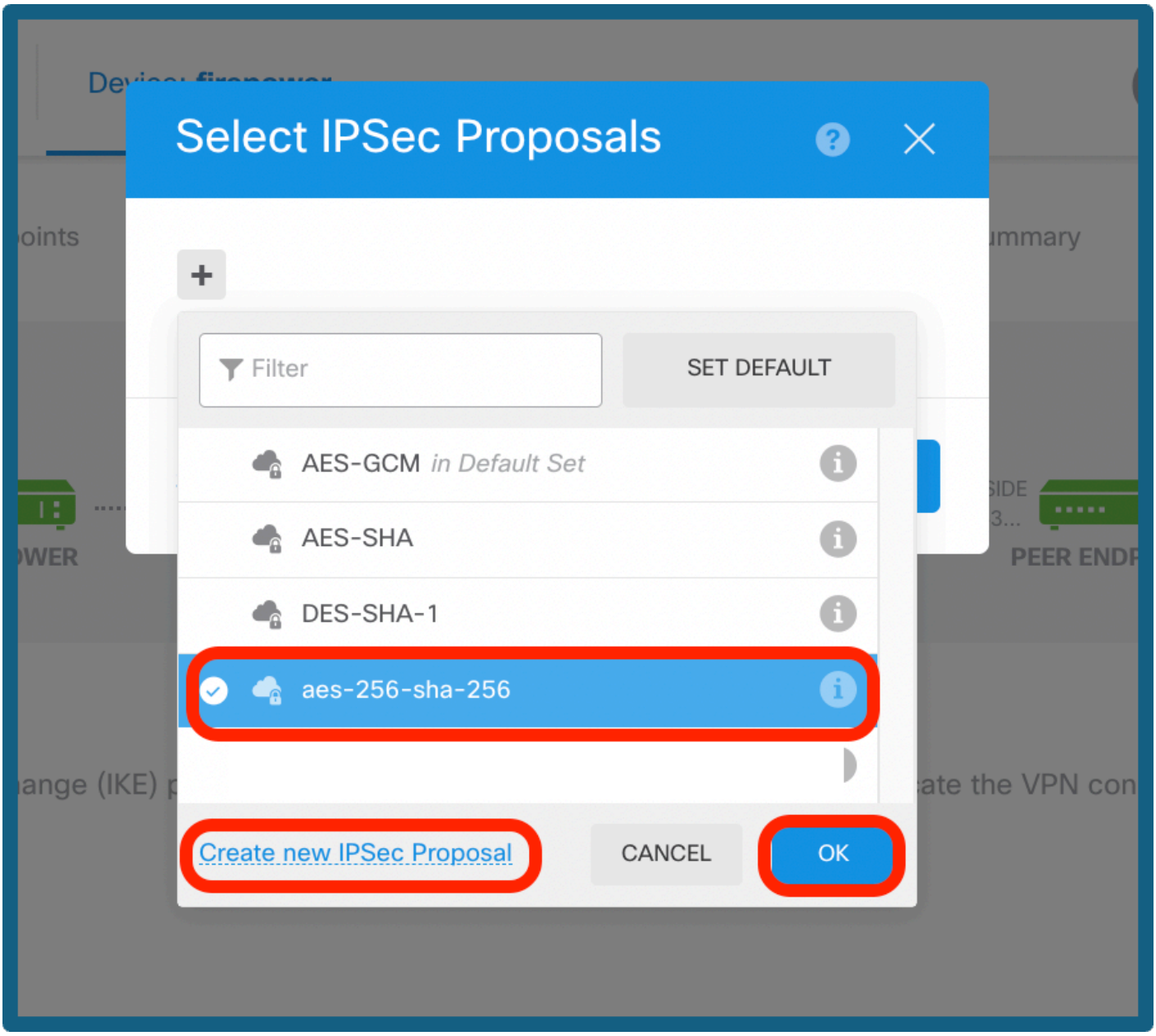


Kies IKE-beleid

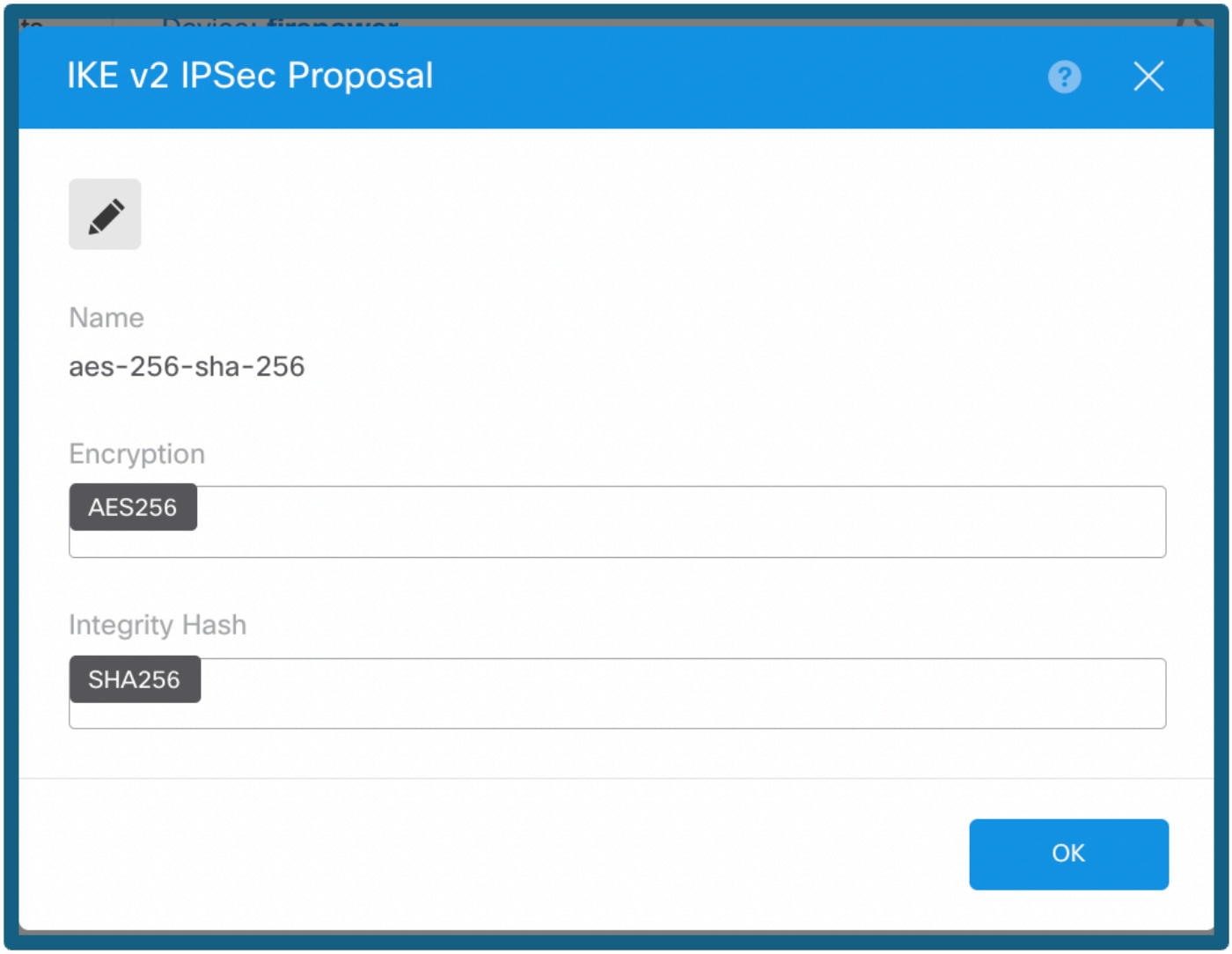


Config van het IKE-beleid

Stap 7b. Kies de knop IPSec-beleid zoals weergegeven in de afbeelding en klik op de knop ok of Maak een nieuw IPsec-voorstel, als u een nieuw voorstel wilt maken.



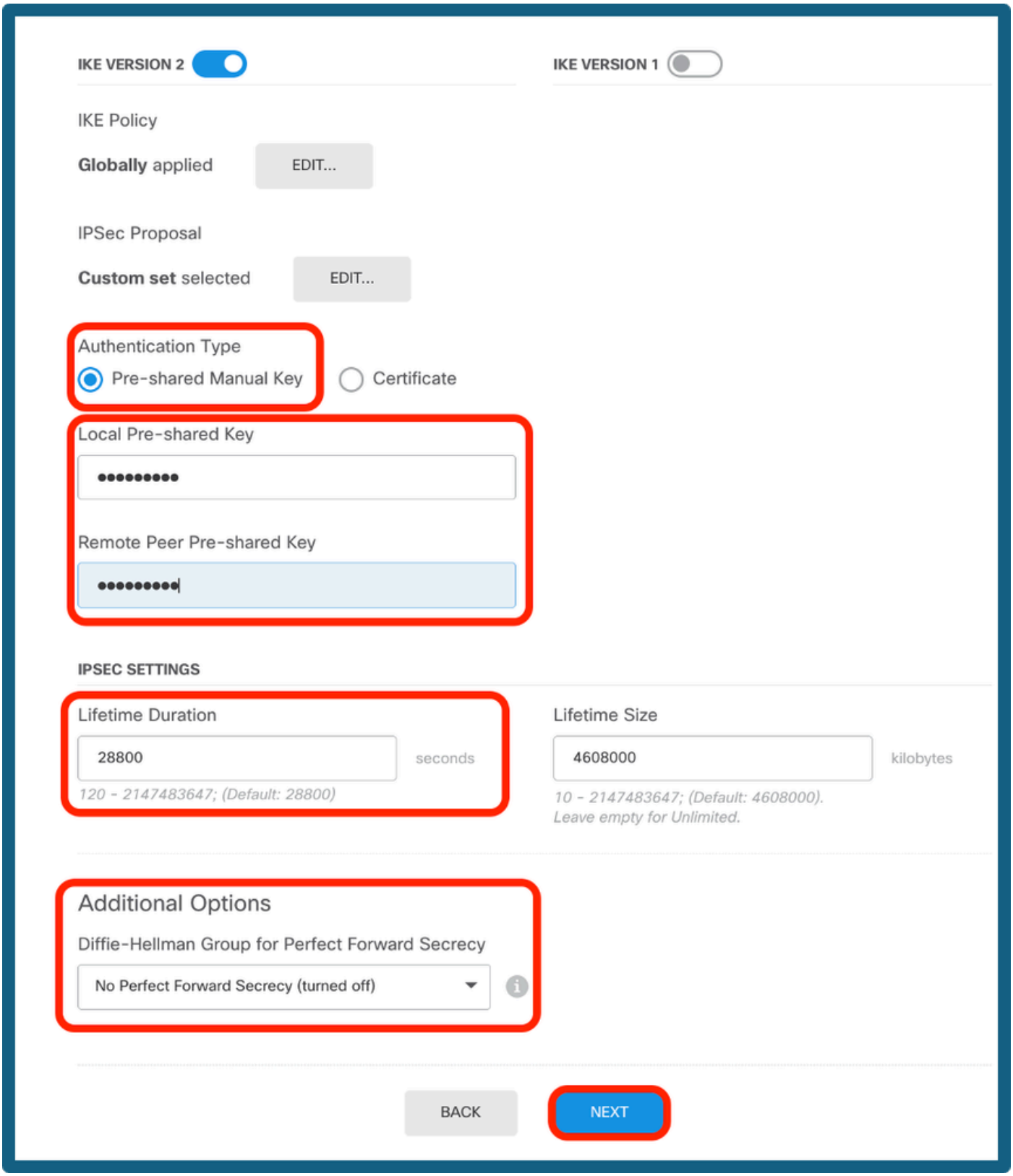
IPsec-voorstel selecteren



Config van het IPsec-voorstel

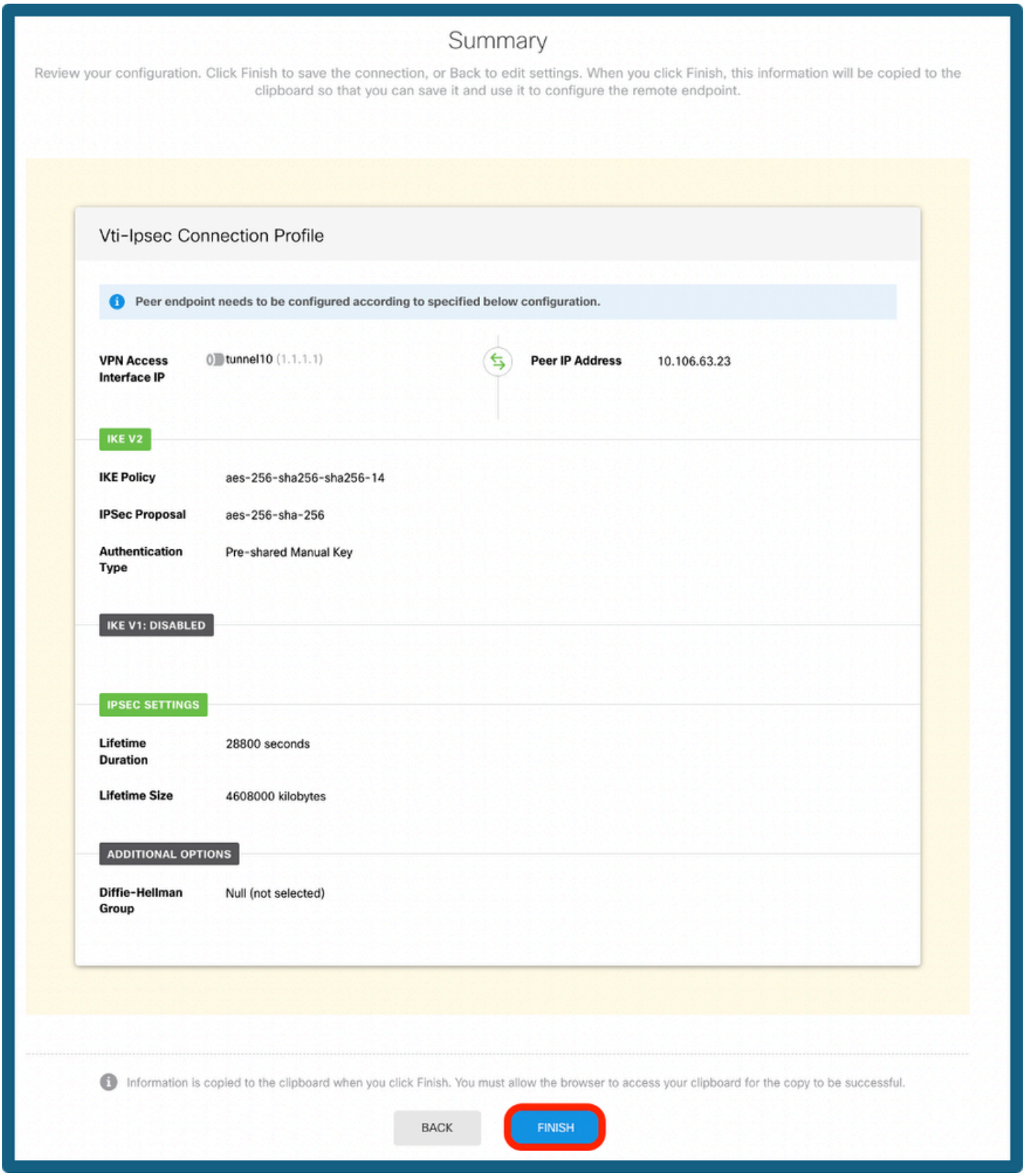
Stap 8a. Selecteer het verificatietype. Als een vooraf gedeelde handmatige sleutel wordt gebruikt, geeft u de lokale en externe vooraf gedeelde sleutel op.

Stap 8b. (Optioneel) Kies de instellingen voor Perfect Forward Secrecy. Configureer de IPsec Lifetime Duration en Lifetime Size en klik vervolgens op Next.



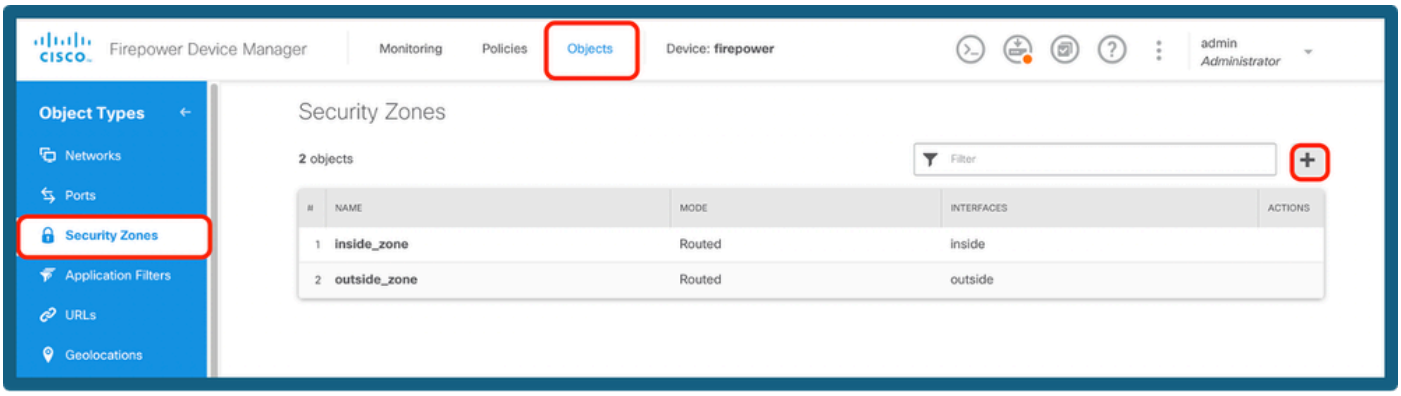
PSK en Lifetime Config

Stap 9. Controleer de configuratie en klik op Voltooien.



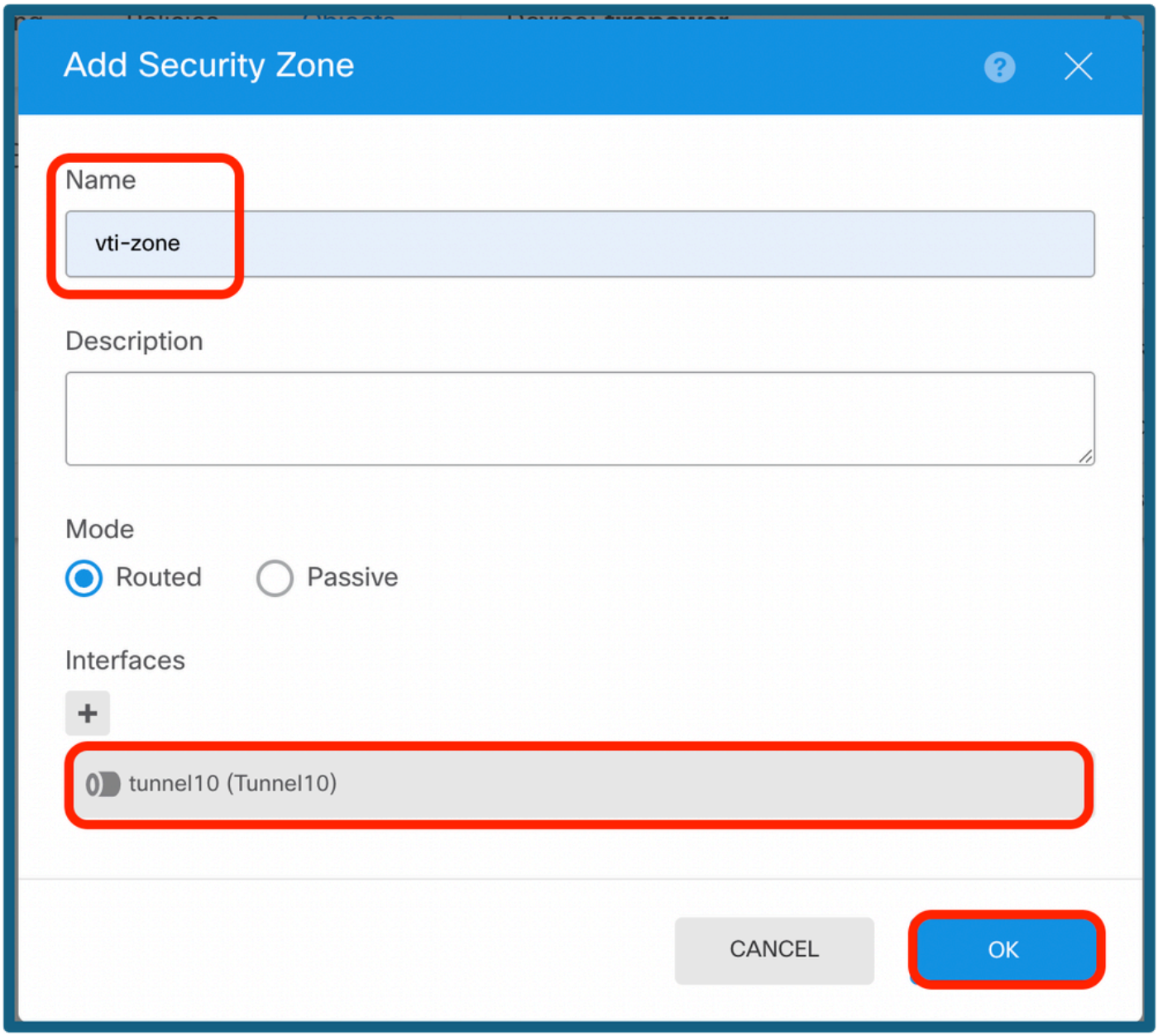
Configuratieoverzicht

Stap 10a. Navigeer naar Objecten > Beveiligingszones en klik op het + pictogram.



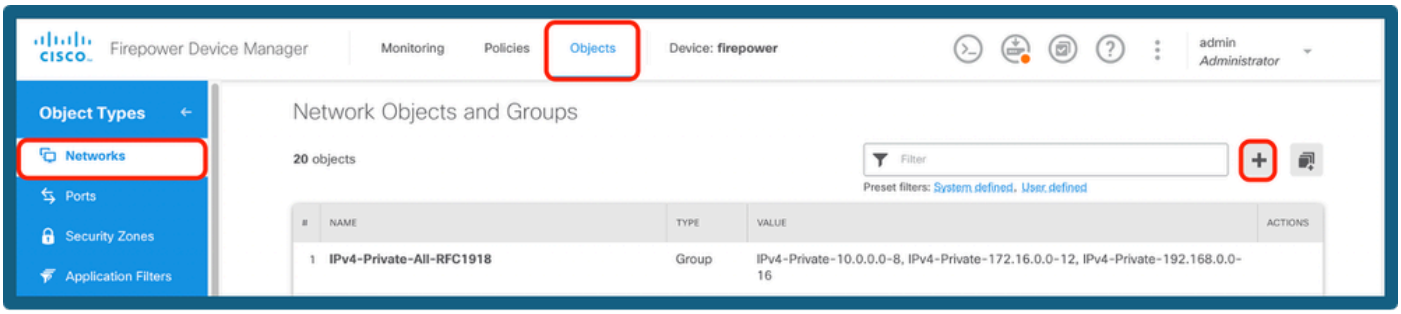
Een beveiligingszone toevoegen

Stap 10b. Maak een zone en selecteer de VTI-interface zoals hieronder wordt weergegeven.



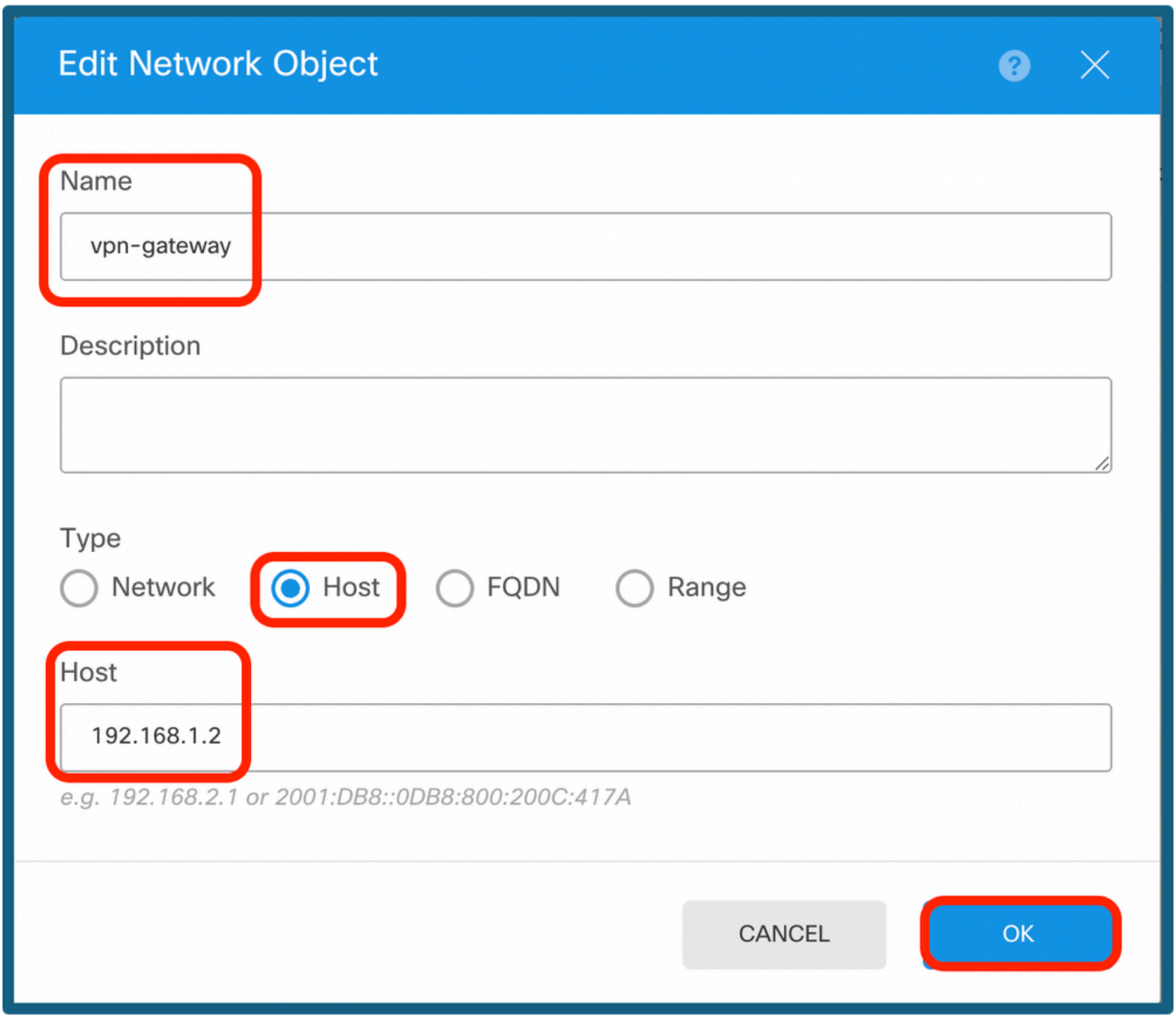
Beveiligingszone configureren

Stap 11a. Navigeer naar Objecten > Netwerken, klik op + pictogram.



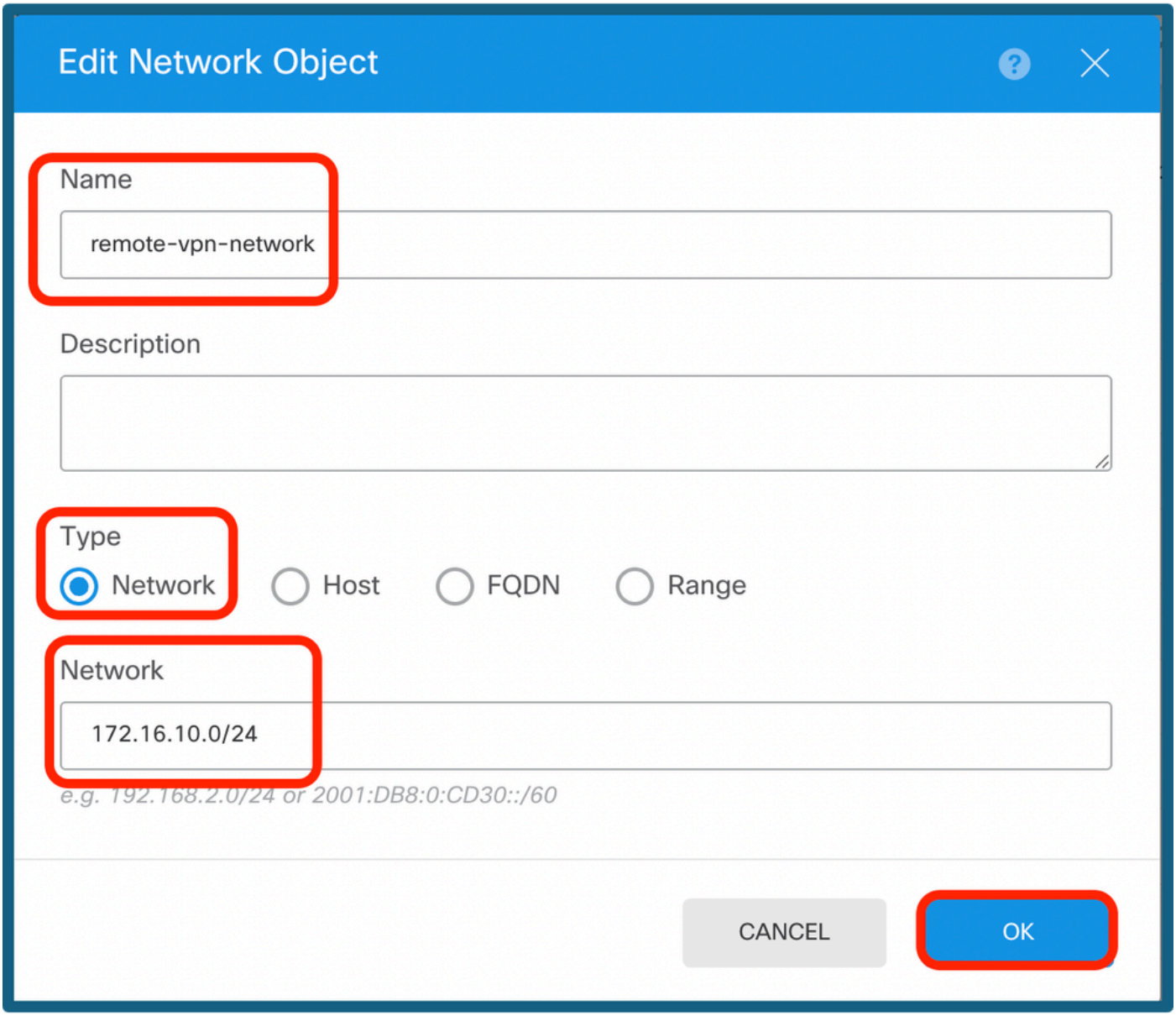
Netwerkobjecten toevoegen

Stap 11b. Voeg een host-object toe en maak een gateway met een IP-tunnel van peer-end.

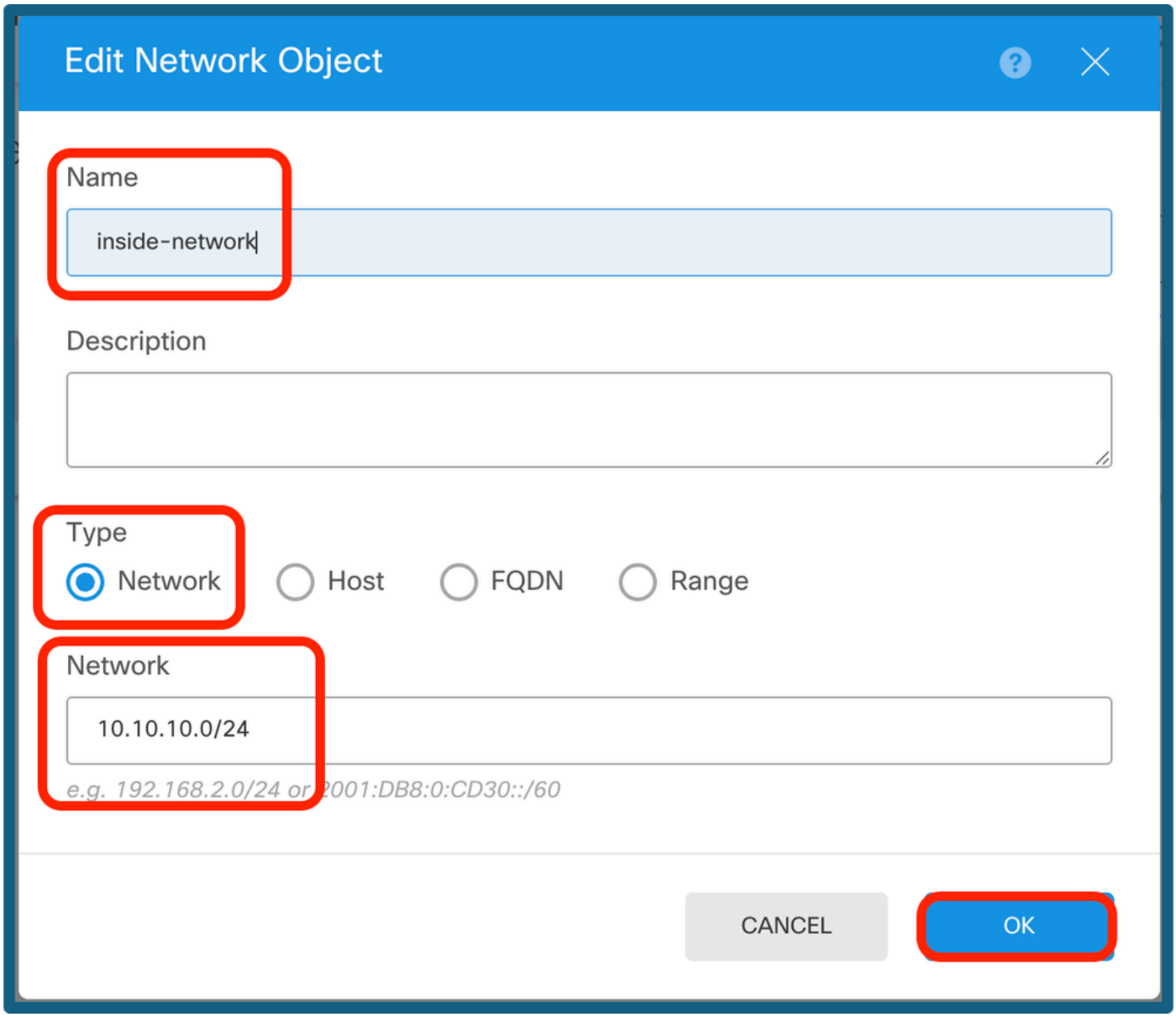


VPN-gateway configureren

Stap 11c. Voeg het externe subnet en het lokale subnet toe.

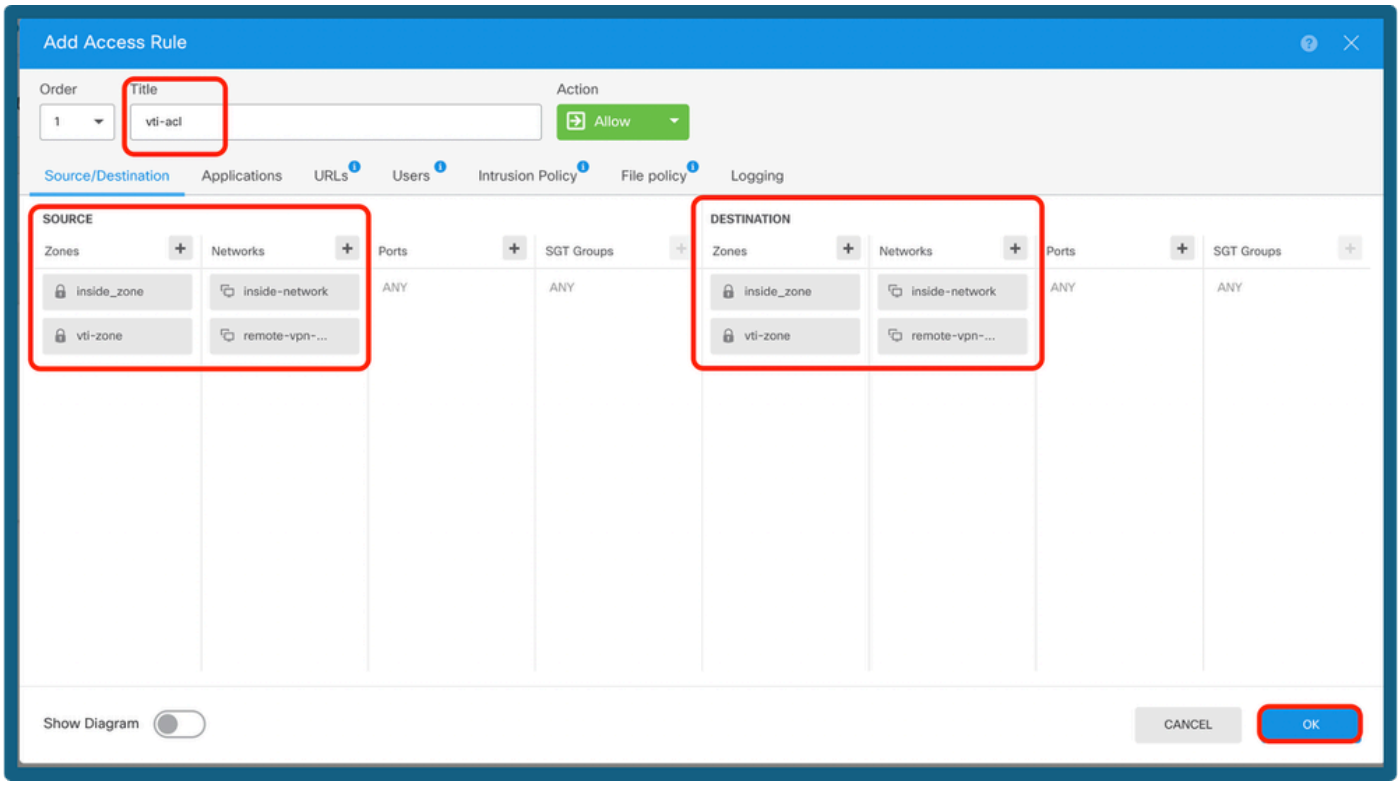


Externe IP-configuratie



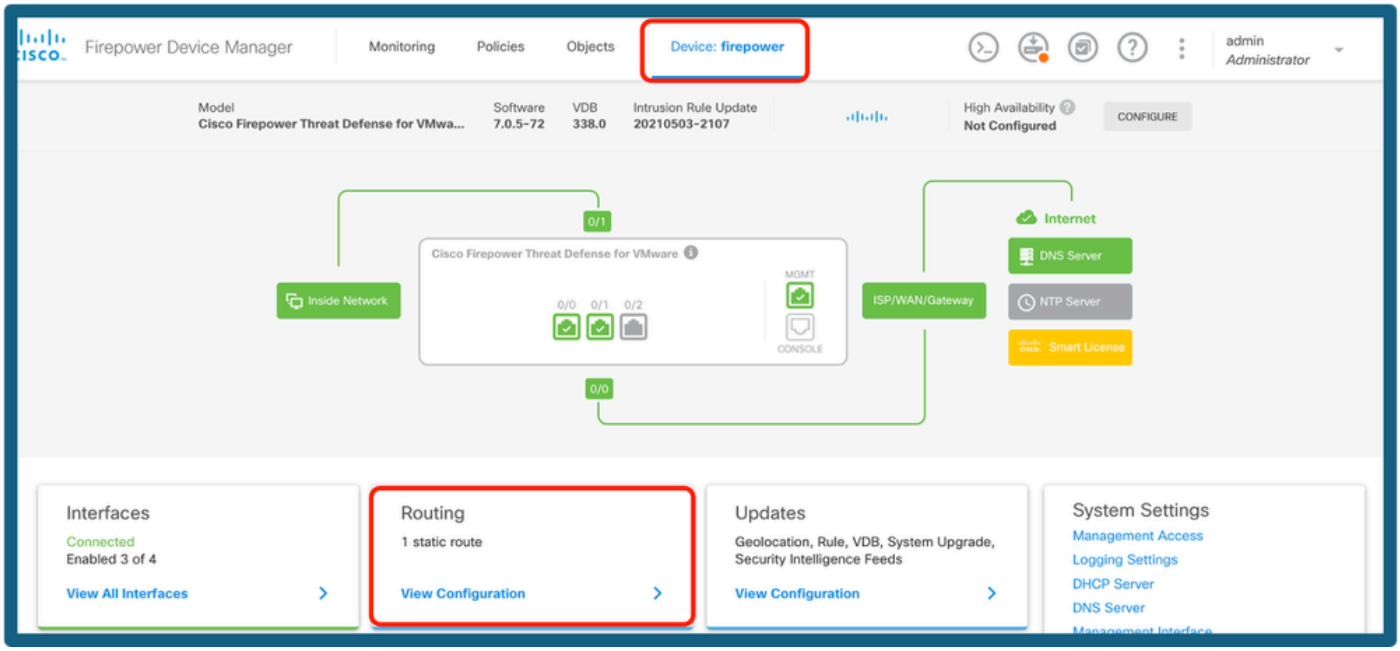
Lokale IP-configuratie

Stap 12. Navigeer naar Apparaat > Beleid en configureer het beleid voor toegangscontrole.



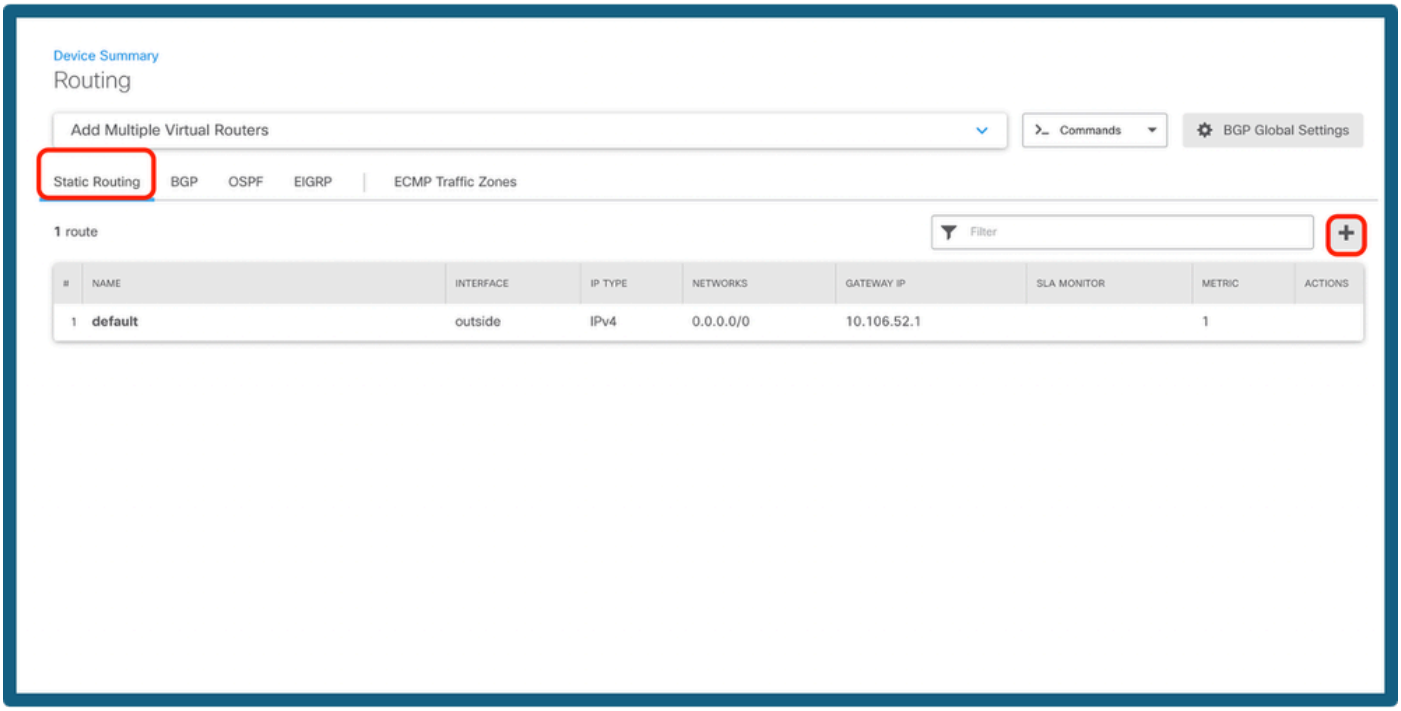
Toegangscontrolebeleid toevoegen

Stap 13a. Voeg de routering over de VTI-tunnel toe. Navigeer naar Apparaat > Routering.



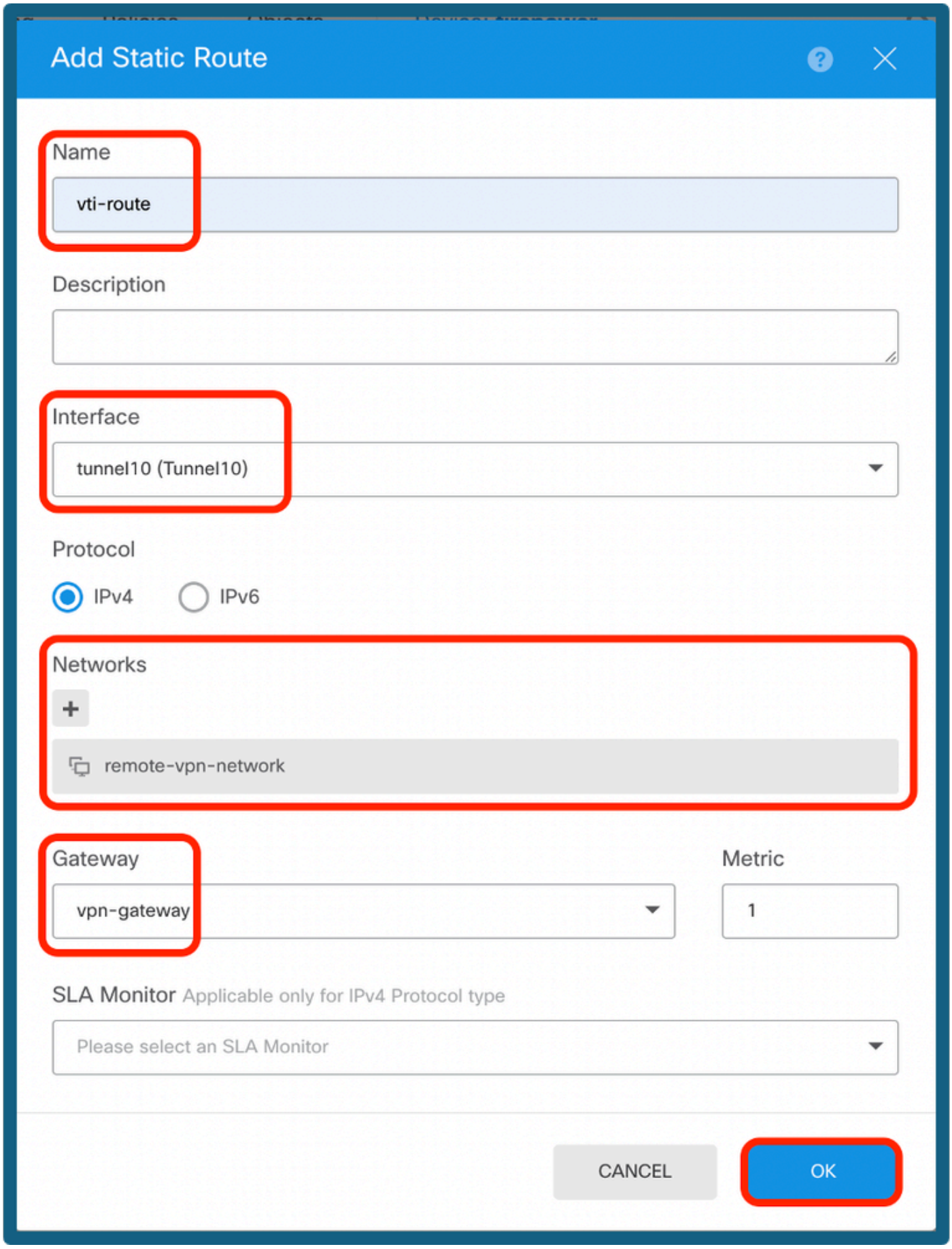
Routering selecteren

Stap 13b. Navigeer naar Statische route onder het tabblad Routering. Klik op + pictogram.



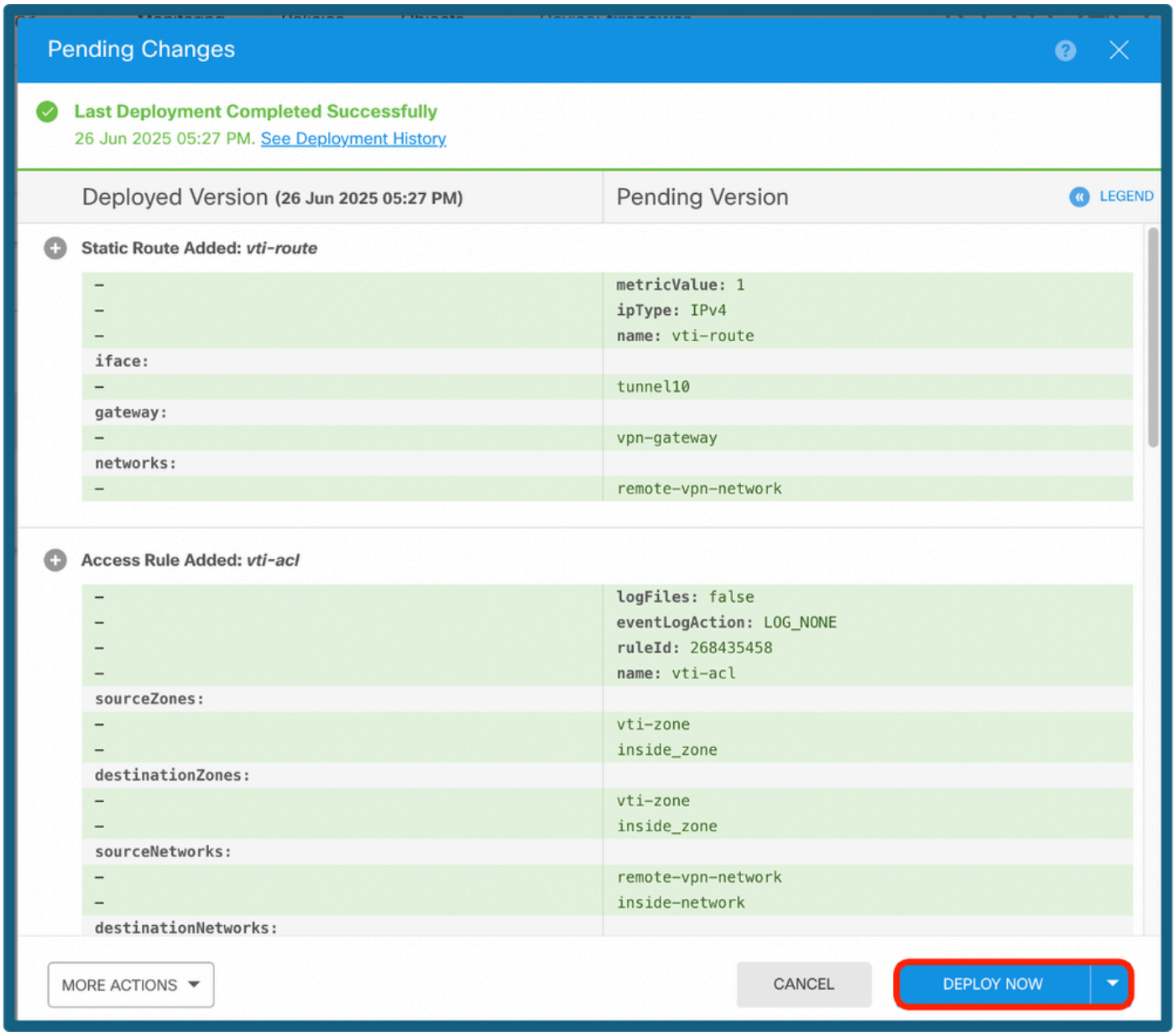
Route toevoegen

Stap 13c. Geef de interface op, kies het netwerk, geef de gateway op. Klik op OK.



Statische route configureren

Stap 14. Navigeer naar Implementeren. Controleer de wijzigingen en klik op Nu implementeren.

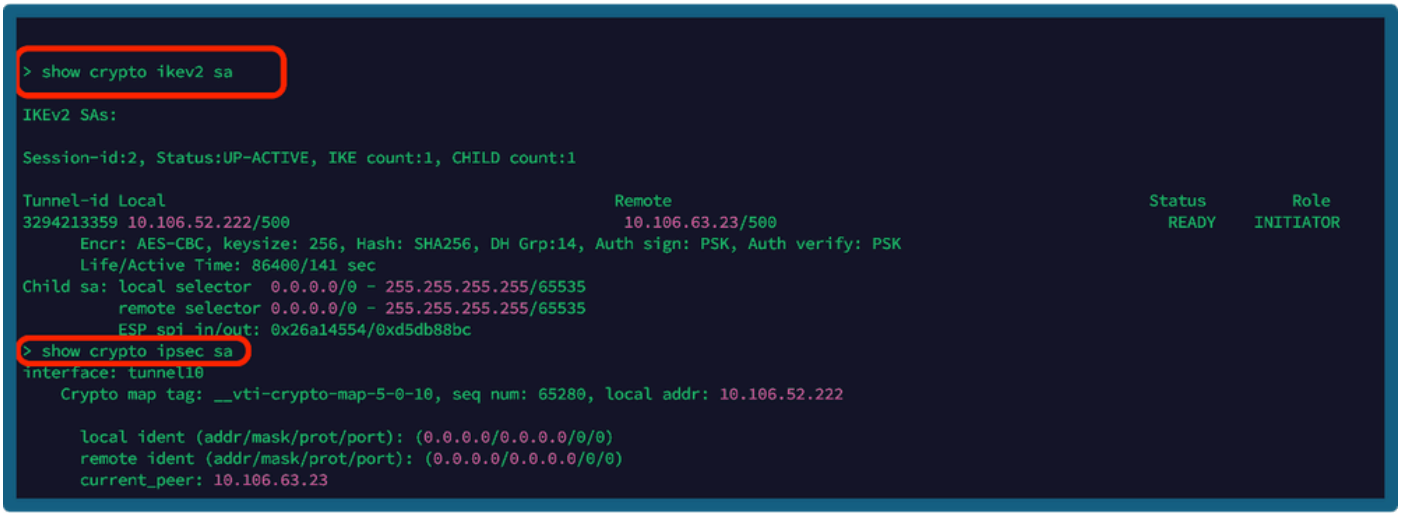


Implementeer de configuratie

Verifiëren

Nadat de implementatie is voltooid, kunt u de tunnelstatus op de CLI controleren met behulp van de volgende opdrachten:

1. Crypto IKEV2 SA weergeven
2. Crypto IPSec SA <peer-IP> weergeven



Opdrachten weergeven

Gerelateerde informatie

Voor meer informatie over Site-to-Site VPN's op de FTD beheerd door FDM, kunt u de volledige configuratiehandleiding hier vinden:

FTD beheerd door FDM Configuration Guide

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.