Configureer de dubbele ISP VTI op FTD die door FMC wordt beheerd

Inhoud

Inleiding

Voorwaarden

- Basisvereisten
- Gebruikte componenten

Configuraties op VCC

- Configuratie van topologie

Endpoint configuratie

IKE-configuratie

IPsec-configuratie

Routingconfiguratie

Inleiding

Dit document beschrijft de implementatie van dubbele ISP-instellingen met behulp van virtuele tunnelinterfaces op een FTD-apparaat dat door FMC wordt beheerd.

Voorwaarden

Basisvereisten

- Een fundamenteel begrip van site-to-site VPN's zou nuttig zijn. Deze achtergrond helpt bij het begrijpen van het VTI setup proces, inclusief de belangrijkste concepten en configuraties die erbij betrokken zijn.
- De basiskennis over het configureren en beheren van VTI's op het Cisco Firepower platform is essentieel. Dit omvat kennis over de werking van VTI's in het FTD en over de wijze waarop zij via de FMC-interface worden bestuurd.

Gebruikte componenten

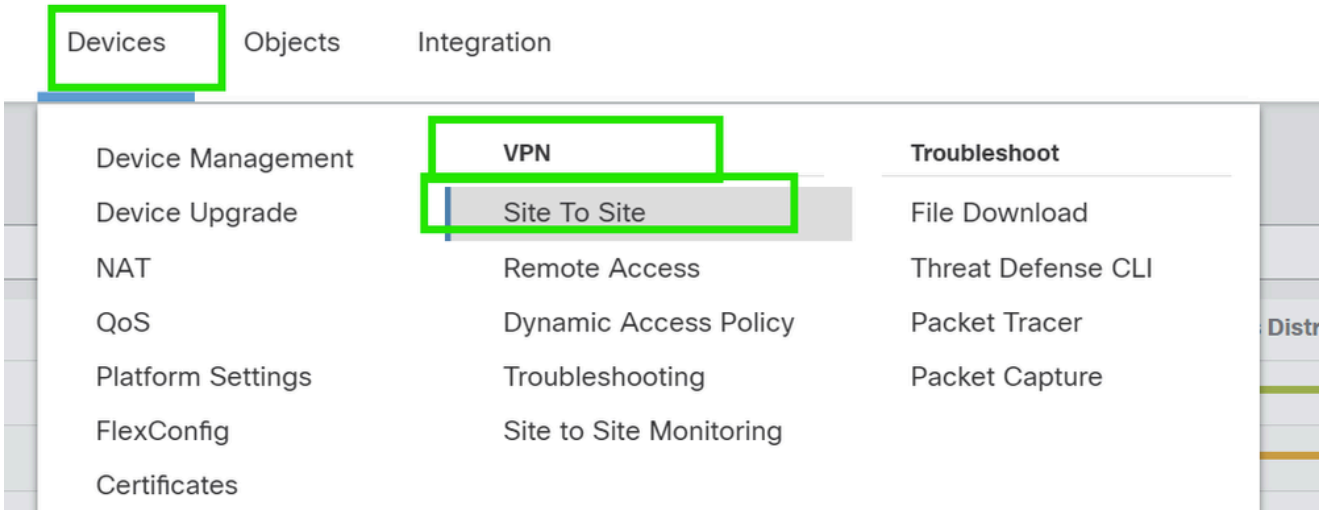
- Cisco Firepower Threat Defence (FTD) voor VMware: versie 7.0.0
- Firepower Management Center (FMC): versie 7.2.4 (build 169)

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.

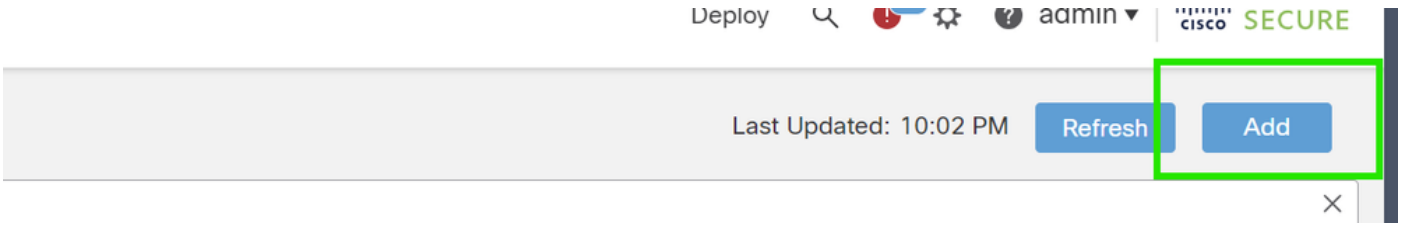
Configuraties op VCC

Configuratie van topologie

1. Ga naar Apparaten > VPN > Site to Site.



2. Klik op Add om VPN-topologie toe te voegen.



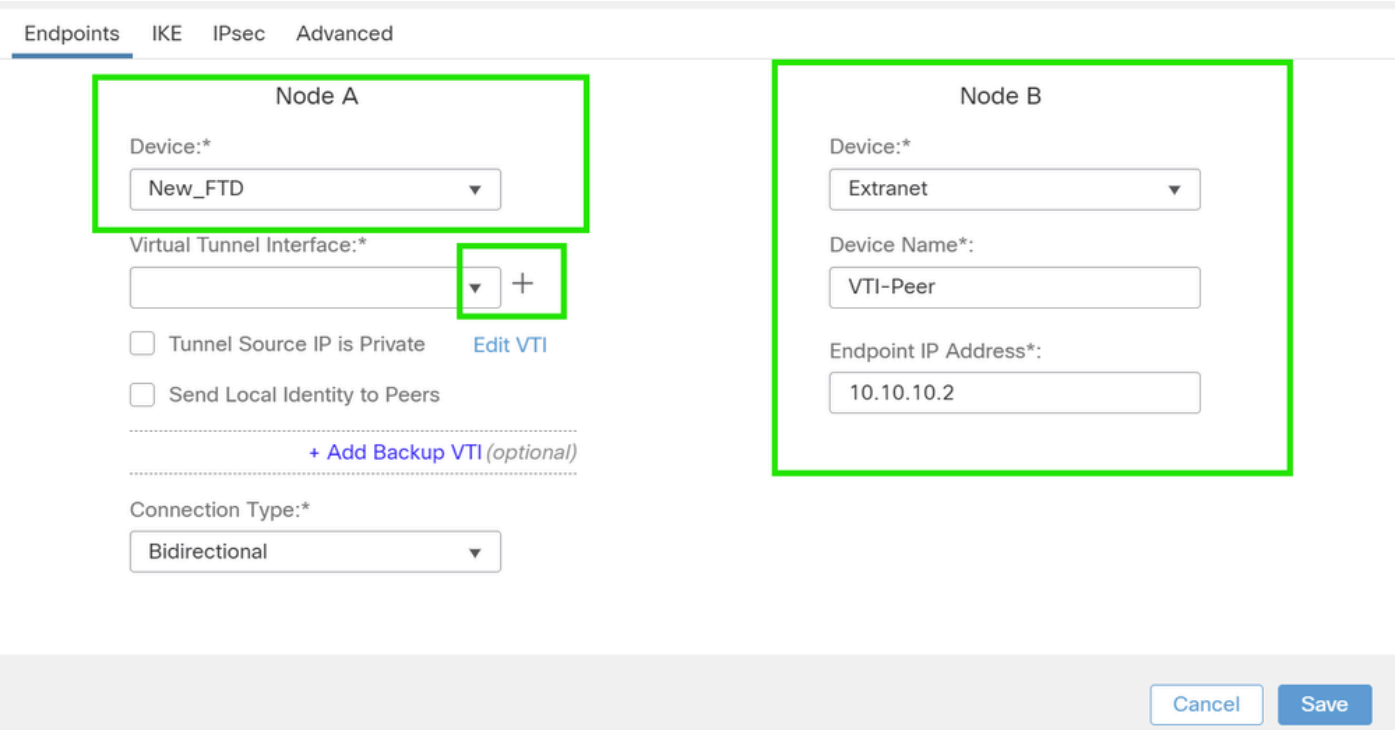
3. Geef een naam voor de topologie, kies VTI en Point-to-Point, en selecteer een IKE-versie (in dit geval IKEv2).

Endpoint configuratie

1. Kies het apparaat waarop de tunnel moet worden geconfigureerd.

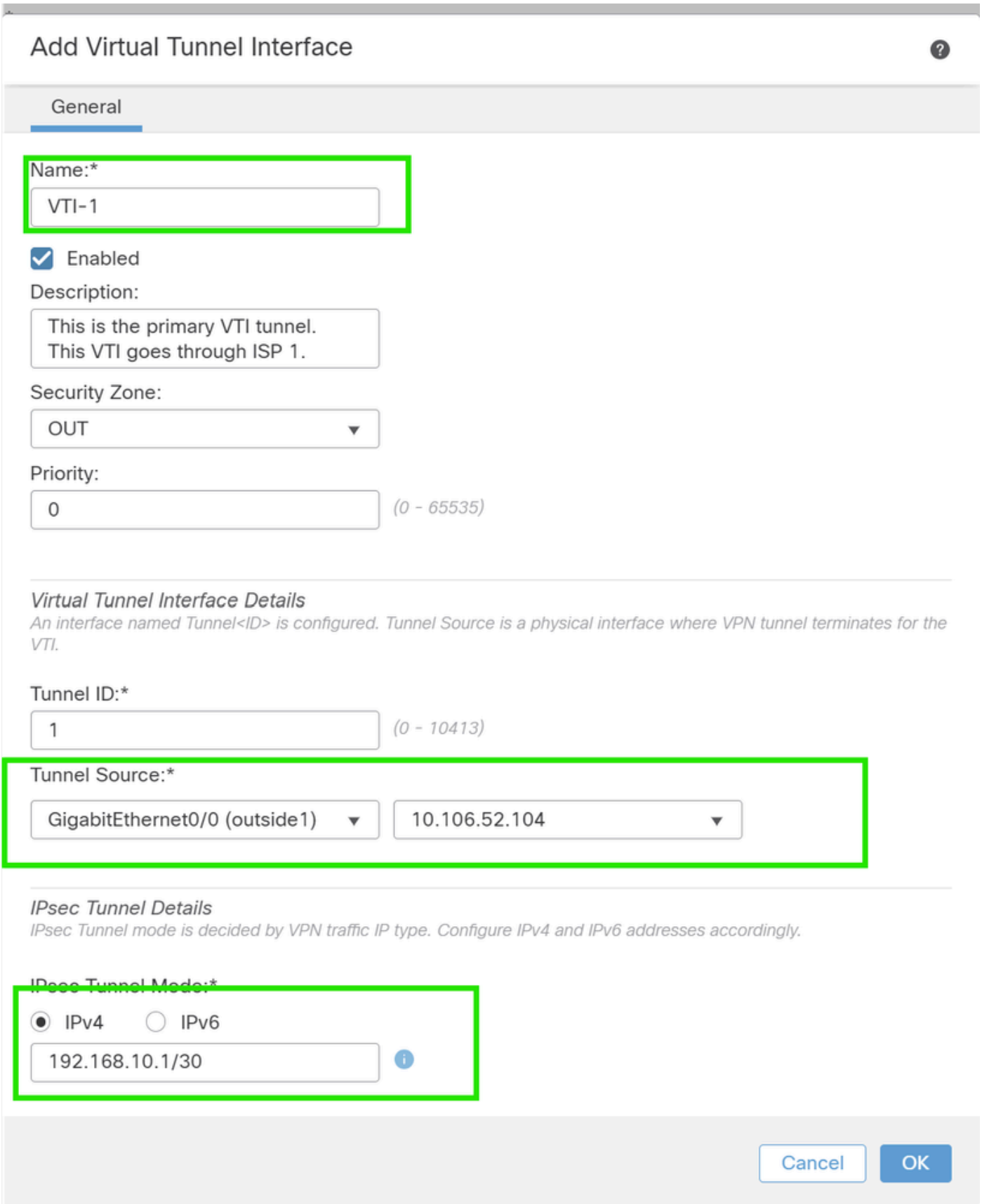
Voeg de externe peer details toe.

U kunt een nieuwe virtuele sjablooninterface toevoegen door op het pictogram "+" te klikken of een van de bestaande lijst selecteren.

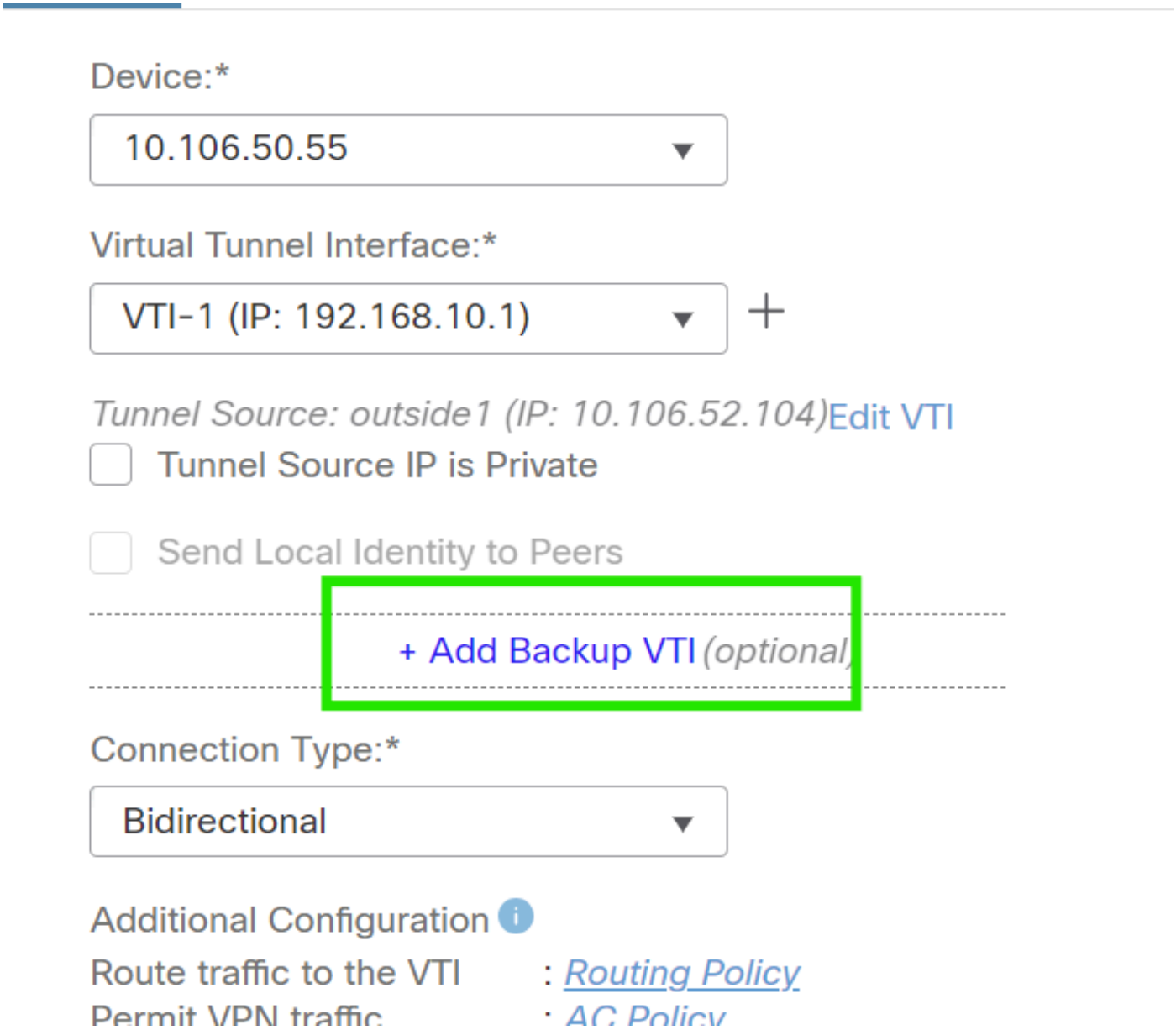


Als u een nieuwe VTI-interface maakt, voegt u de juiste parameters toe, schakelt u deze in en klikt u op "OK".

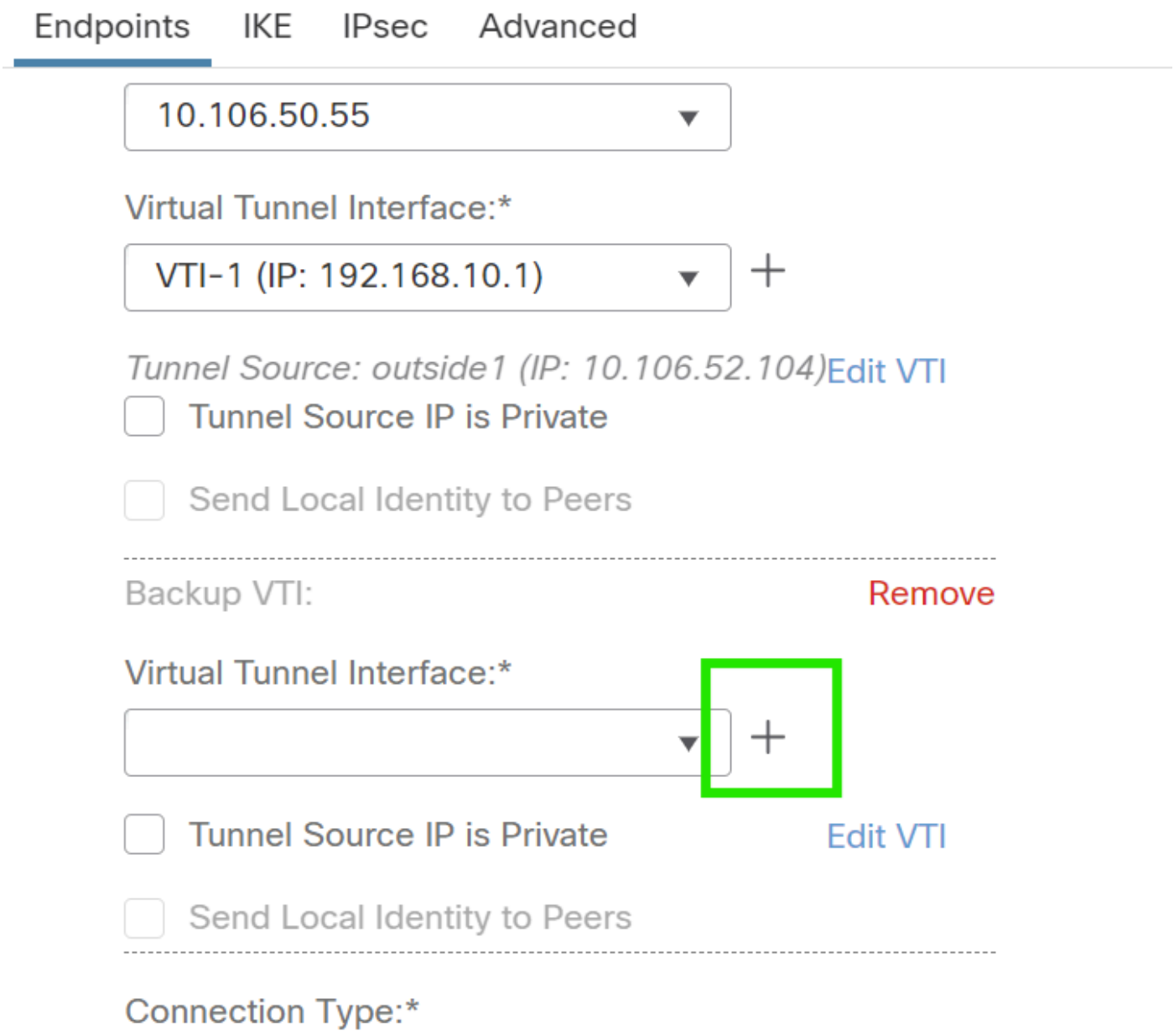
LET OP: dit wordt de primaire VTI.



3. Klik op "+ ". Back-up VIT toevoegen" om een tweede VIT toe te voegen.

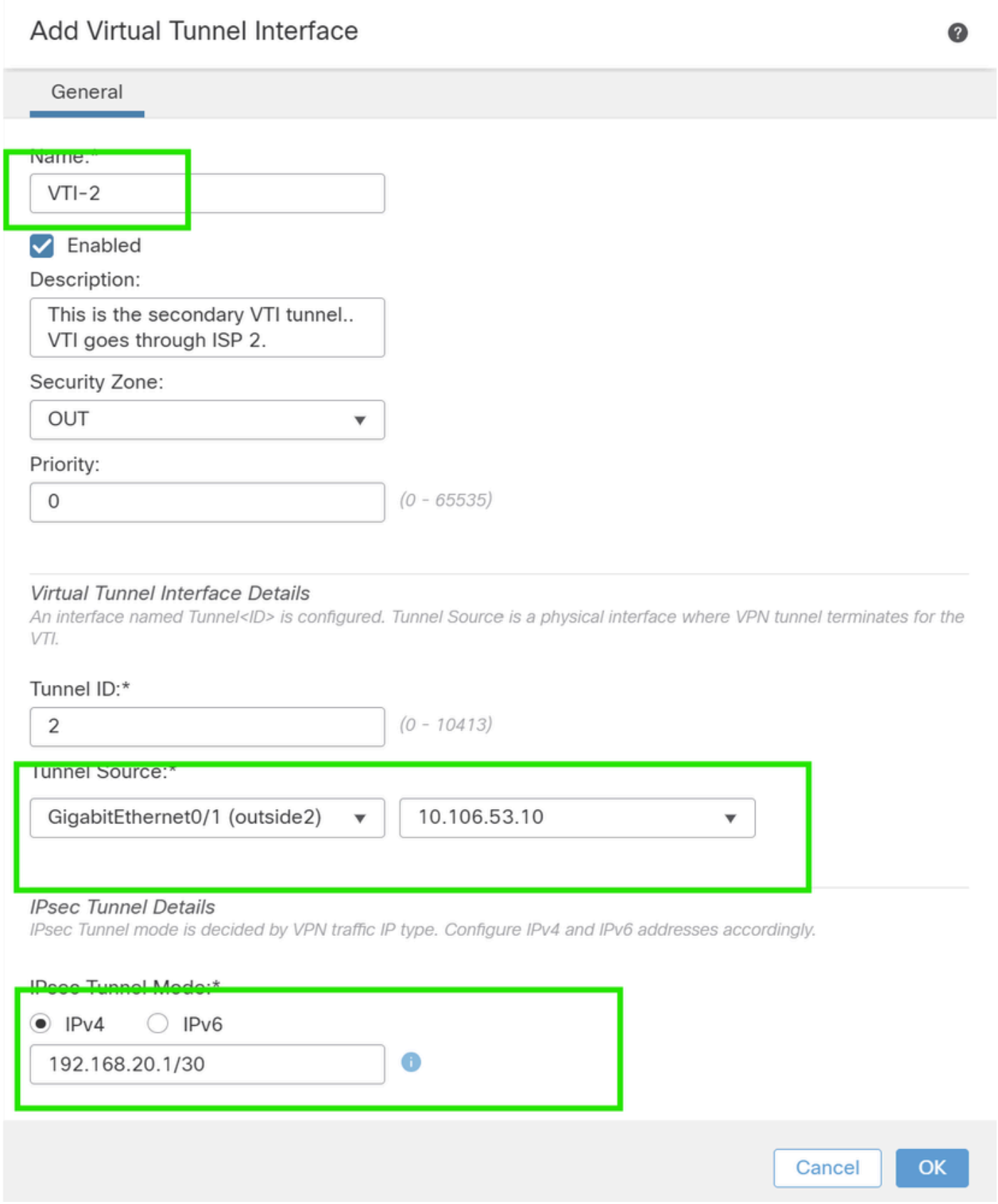


4. Klik op '+' om een parameter toe te voegen voor secundaire VTI (indien niet reeds geconfigureerd).



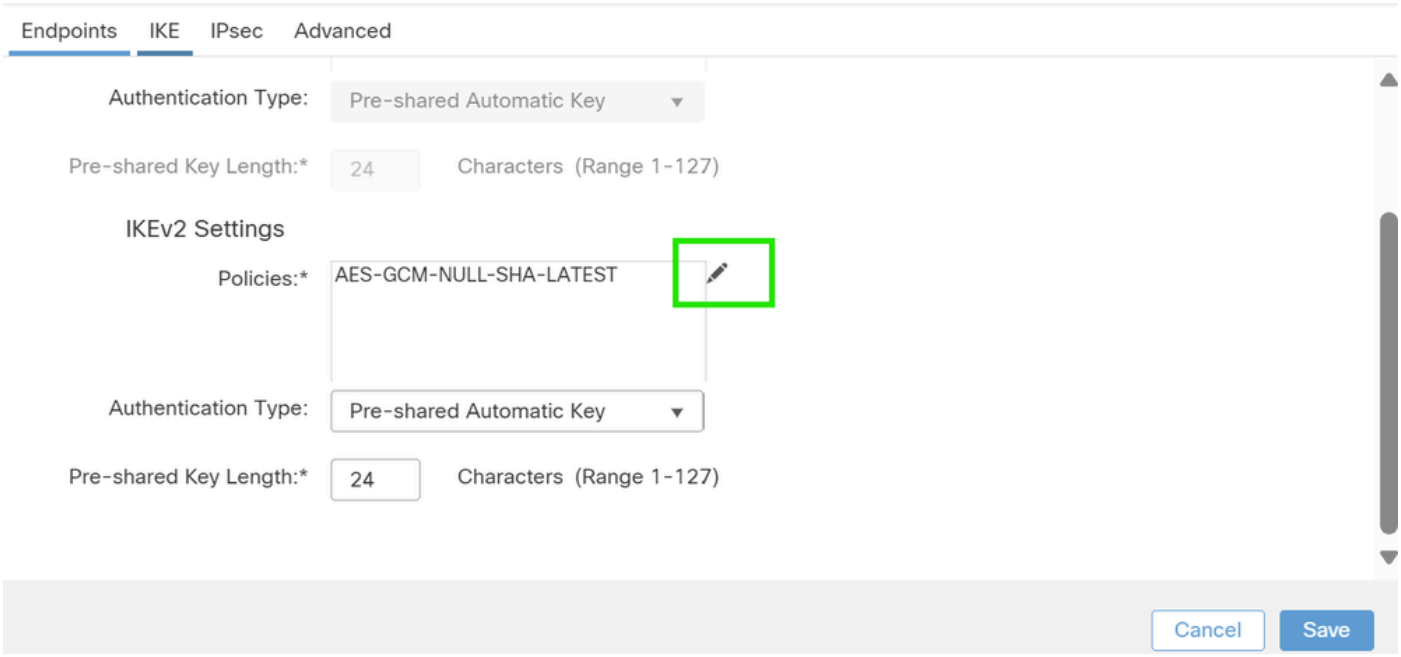
5. Als u een nieuwe VTI-interface maakt, voegt u de juiste parameters toe, schakelt u deze in en klikt u op "OK".

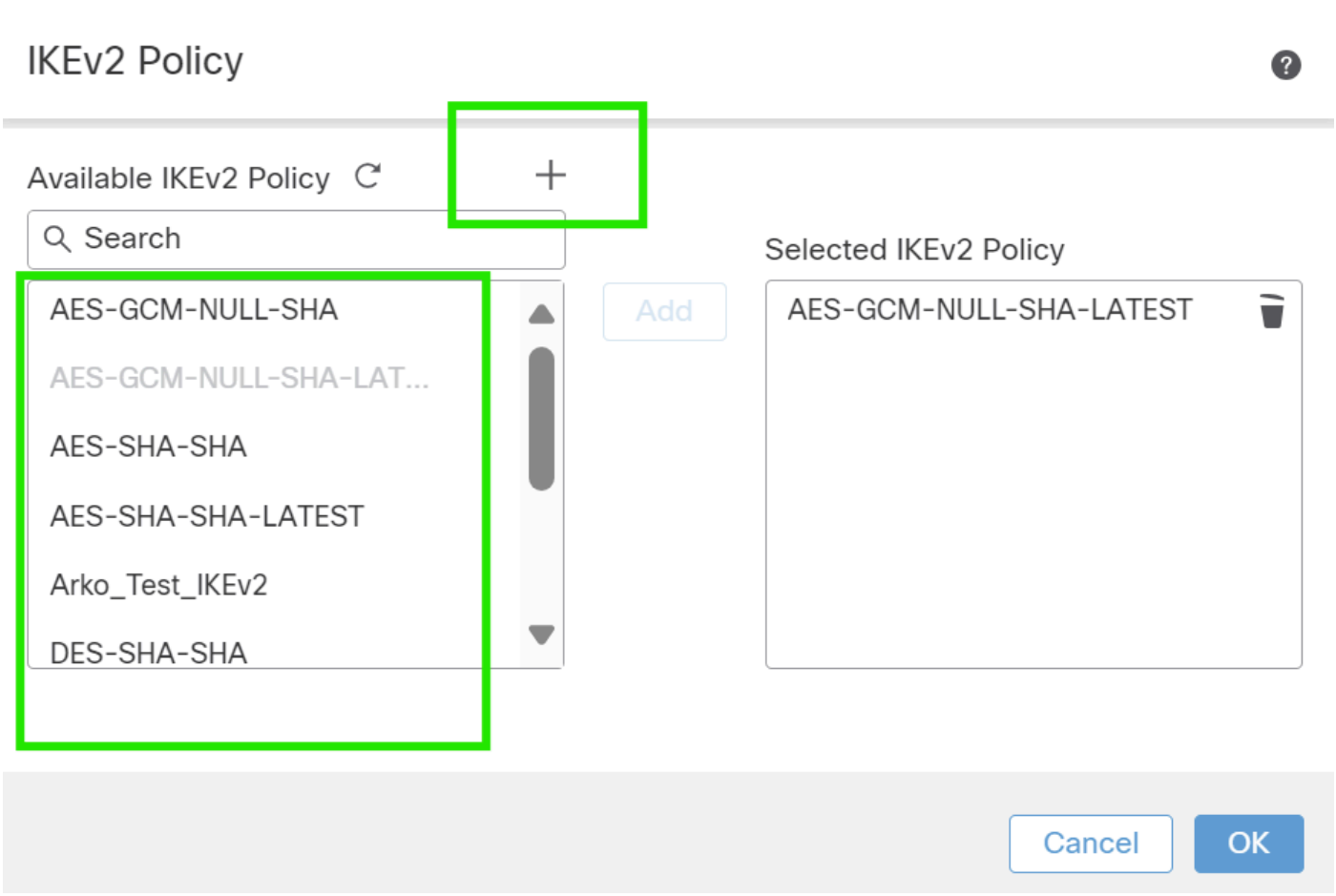
LET OP: dit wordt de secundaire VTI.



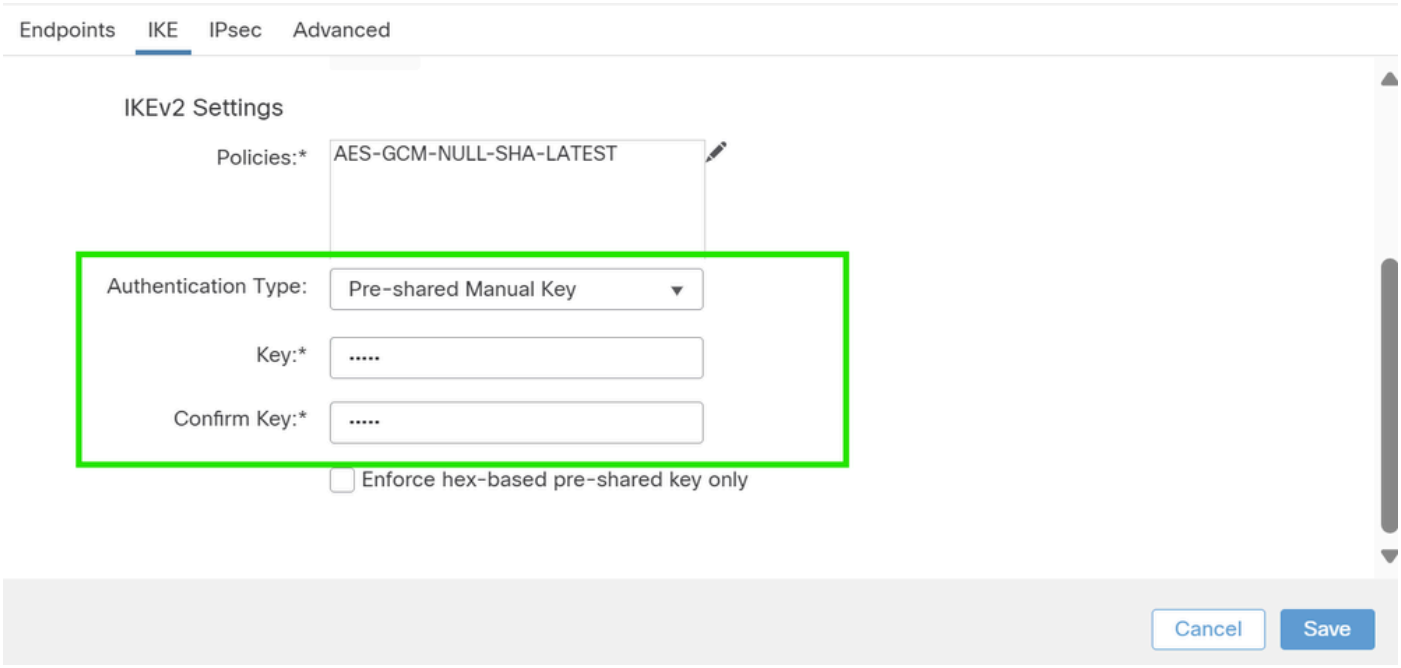
IKE-configuratie

1. Navigeren naar het tabblad IKE. U kunt ervoor kiezen om een vooraf bepaald beleid te gebruiken, klik op de potloodknop naast het tabblad Beleid om een nieuw beleid te maken of selecteer een ander beschikbaar beleid dat is gebaseerd op uw behoefte.



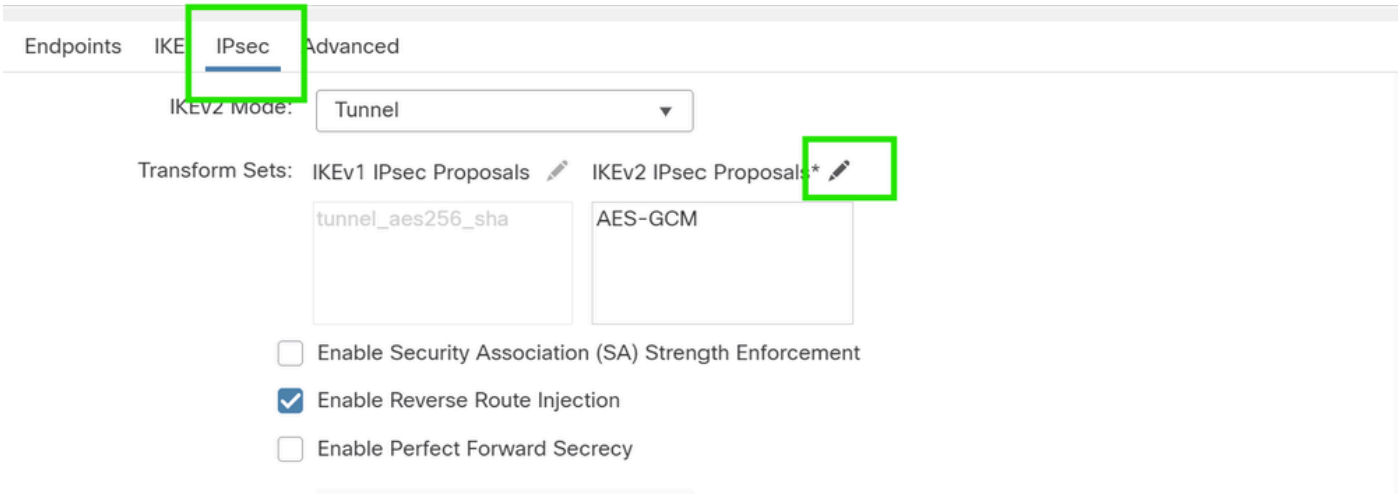


2. Selecteer het verificatietype. Als een vooraf gedeelde handmatige toets wordt gebruikt, specificeert u de toets in de vakjes Sleutel en Bevestig de toets.



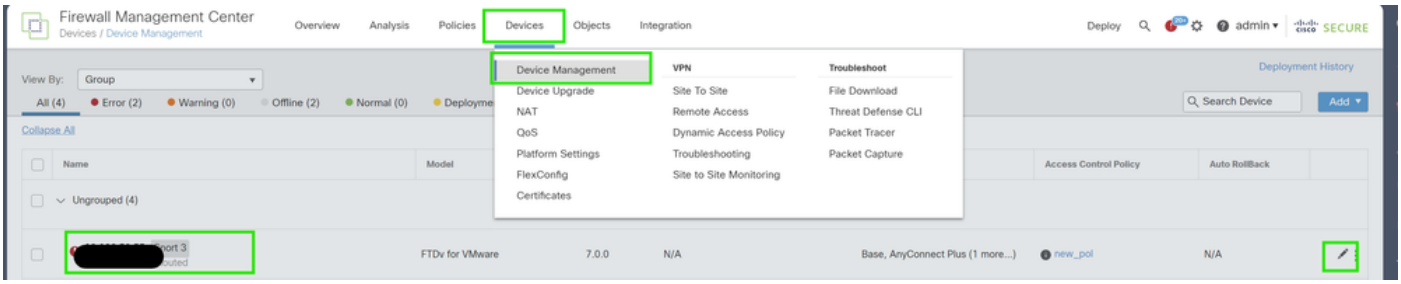
IPsec-configuratie

Ga naar het tabblad IPsec. U kunt ervoor kiezen om een vooraf gedefinieerd voorstel te gebruiken door op de potloodknop naast het tabblad voorstel te klikken om een nieuw voorstel te maken of een ander beschikbaar voorstel te selecteren op basis van uw vereiste.



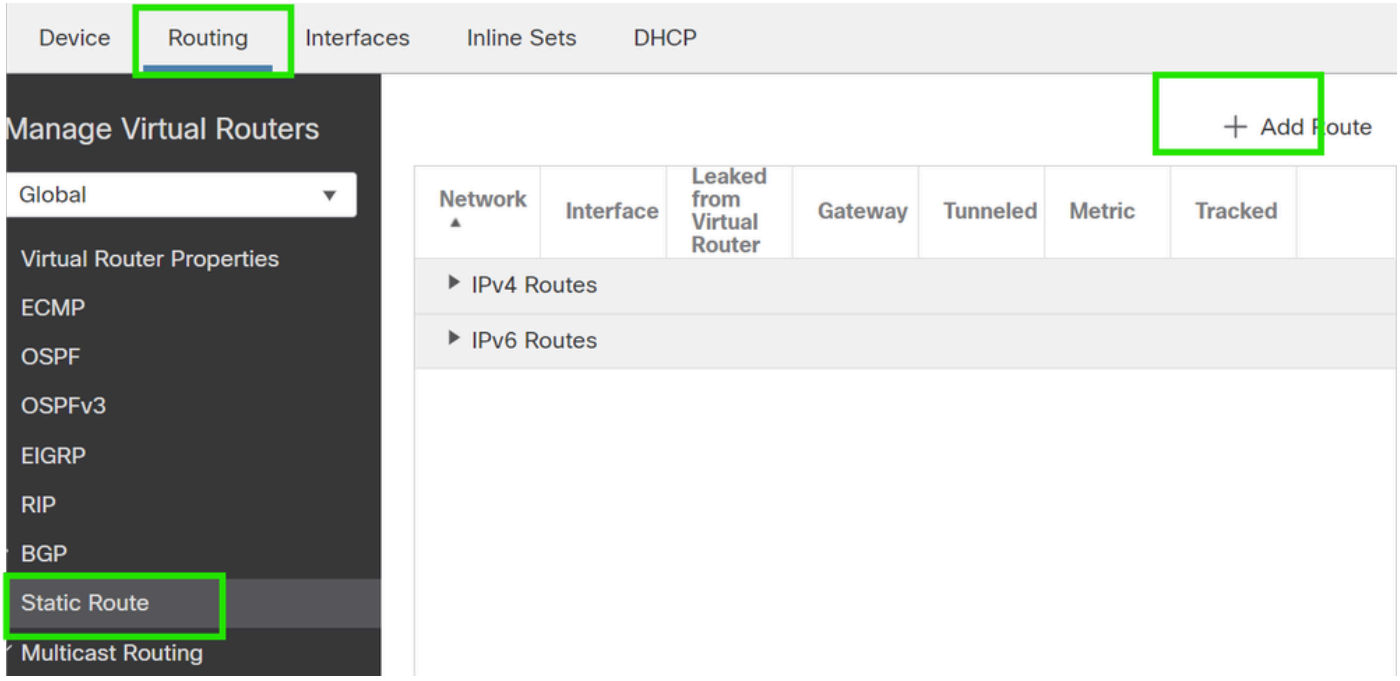
Routingconfiguratie

1. Ga naar Apparaat > Apparaatbeheer en klik op het potloodpictogram om het apparaat (FTD) te bewerken.



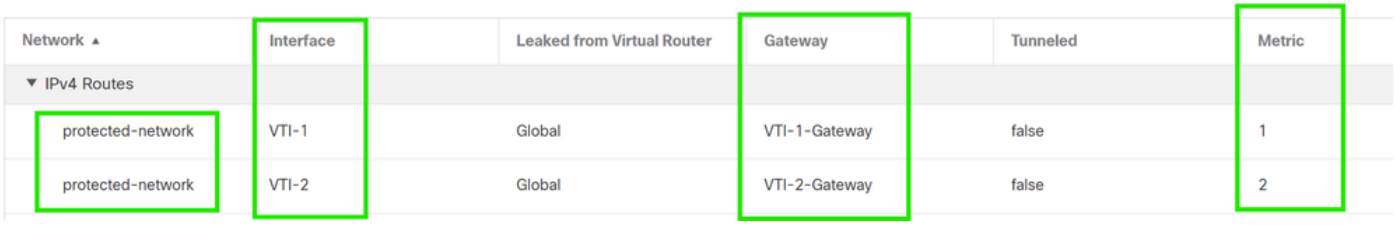
2. Ga naar Routing > Statische Route en klik op de knop "+" om een route toe te voegen aan het primaire en secundaire VTI.

OPMERKING: U kunt de juiste routeringsmethode voor uw verkeer configureren om door de tunnelinterface te gaan. In dit geval zijn statische routes gebruikt.



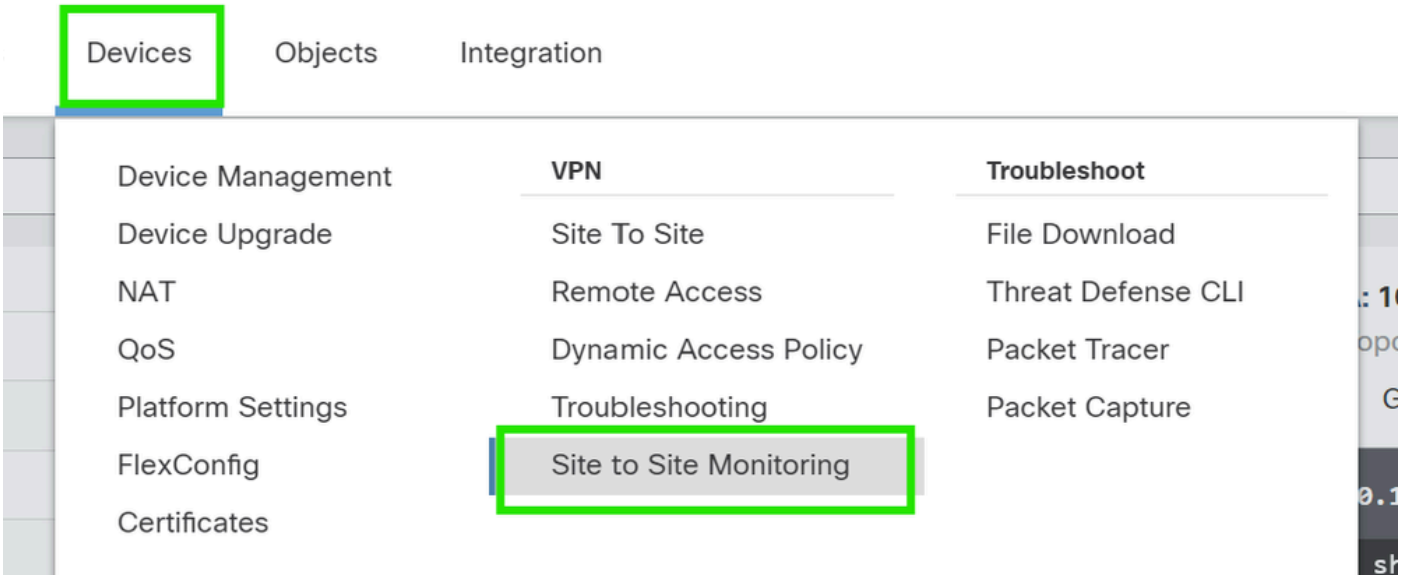
3. Voeg twee routes toe voor uw beveiligd netwerk en stel een hogere AD-waarde (in dit geval 2) in voor de secundaire route.

De eerste route gebruikt de VTI-1 interface, en de tweede gebruikt de VTI-2 interface.

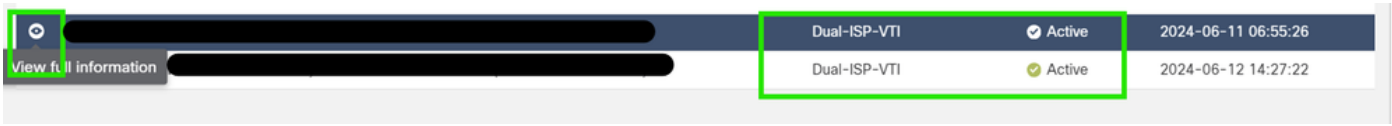


Verifiëren

1. Ga naar Apparaten > VPN > Site to Site Monitoring .



2. Klik op het oog om meer details over de status van de tunnel te controleren.



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.