Beveiligde toegang configureren met Secure FTD en ASA voor privétoegang met NAT

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Secure Access Network Tunnel Group kunt configureren met Network Address Translation.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Firewall Management Center
- Cisco Secure Firewall Threat Defense
- Cisco Secure Access

- Cisco Adaptive Security Appliance
- netwerkadresvertaling
- op beleid gebaseerde routering
- Pakketvastlegging op firewall

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defense 7.10
- Cisco Secure Access
- Cisco Adaptive Security Appliance 9.22
- Cisco-routers

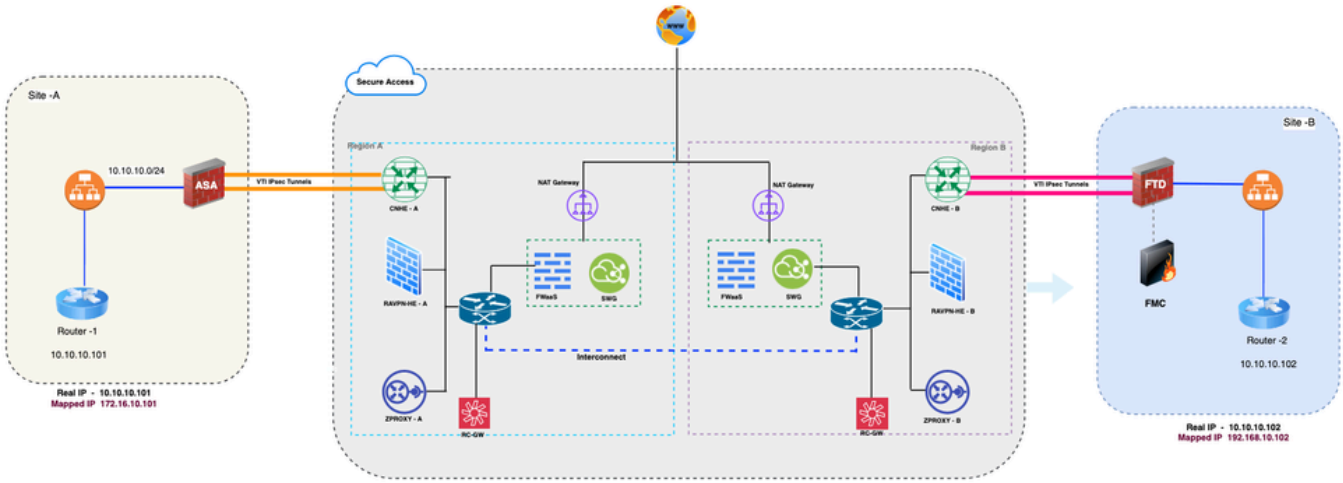
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Secure Access biedt cloud-native Secure Service Edge-mogelijkheden, waaronder Secure Internet Access (SIA) en Secure Private Access (SPA). Voor organisaties die de toegang tot privétoepassingen uitbreiden tot externe gebruikers zonder al het verkeer via een datacenter te backhalen, maakt Secure Access gebruik van IPsec Network Tunnel Groups (NTG's) om gecodeerde tunnels te maken tussen on-premises netwerkapparaten - zoals Cisco Firewall Threat Defense (FTD), Adaptive Security Appliance (ASA) en Cisco Secure Access cloud Points-of-Presence (PoP's).

In dit document wordt beschreven hoe een routegebaseerde IPsec-tunnel tot stand kan worden gebracht met behulp van IKEv2 tussen Cisco FTD, ASA en Cisco Secure Access, waardoor Network Address Translation (NAT) op Secure Access en Policy-Based Routing (PBR) op de FTD en ASA alleen privéverkeer naar de tunnel kan sturen.

Netwerkdiagram



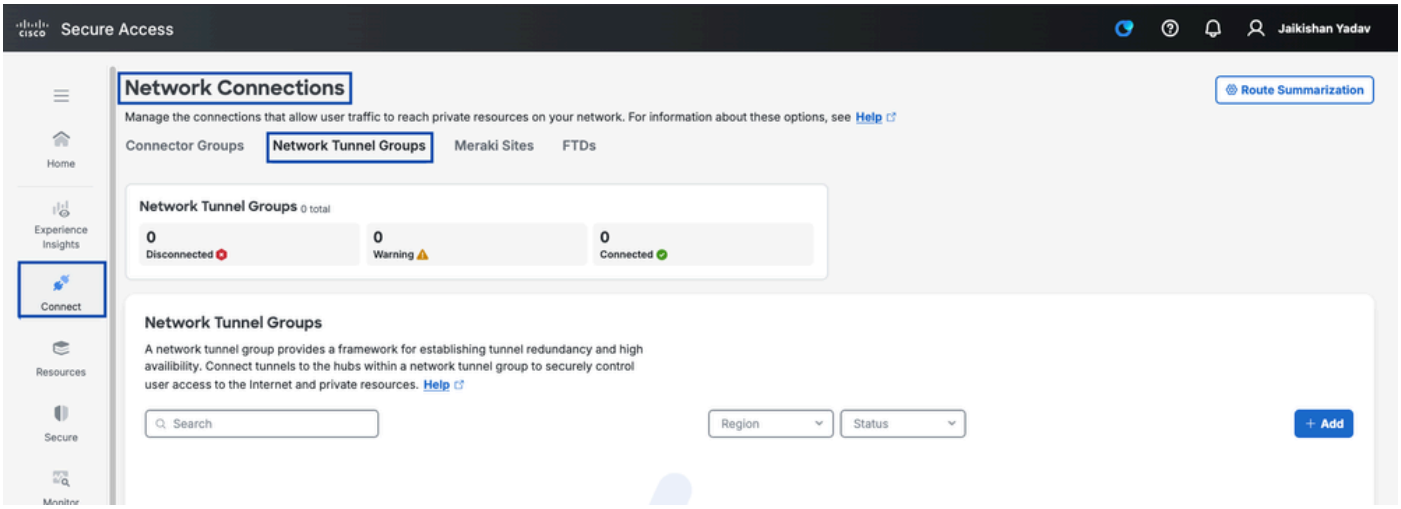
Netwerktopologie

Configureren

Veilige toegang en veilige firewall Thread Defense - Dynamic (BGP) routegebaseerde VPN met PBR

Netwerktunnelgroep configureren voor beveiligde toegang

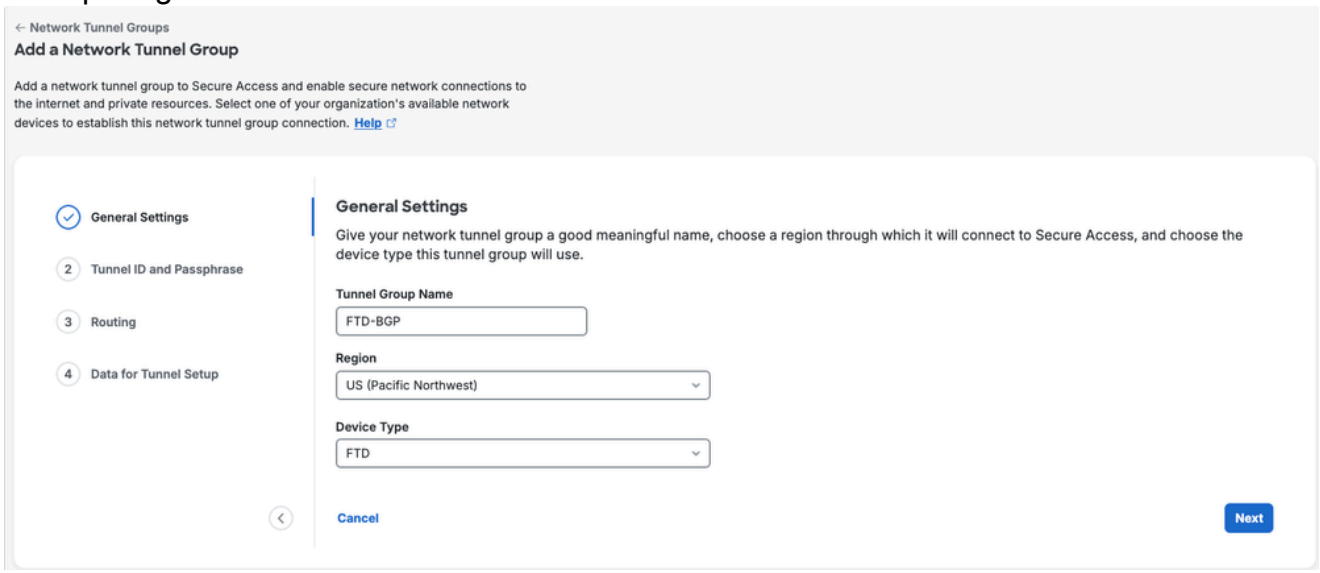
1. Meld u aan bij het dashboard voor beveiligde toegang Veilige toegang
2. Navigeer naar Verbinden > Netwerkverbindingen > Netwerktunnelgroepen en klik op +Toevoegen om de Netwerktunnelgroep te configureren



Veilige toegang - Netwerktunnelgroepen

3. Network Tunnel Group configureren - Algemene instellingen

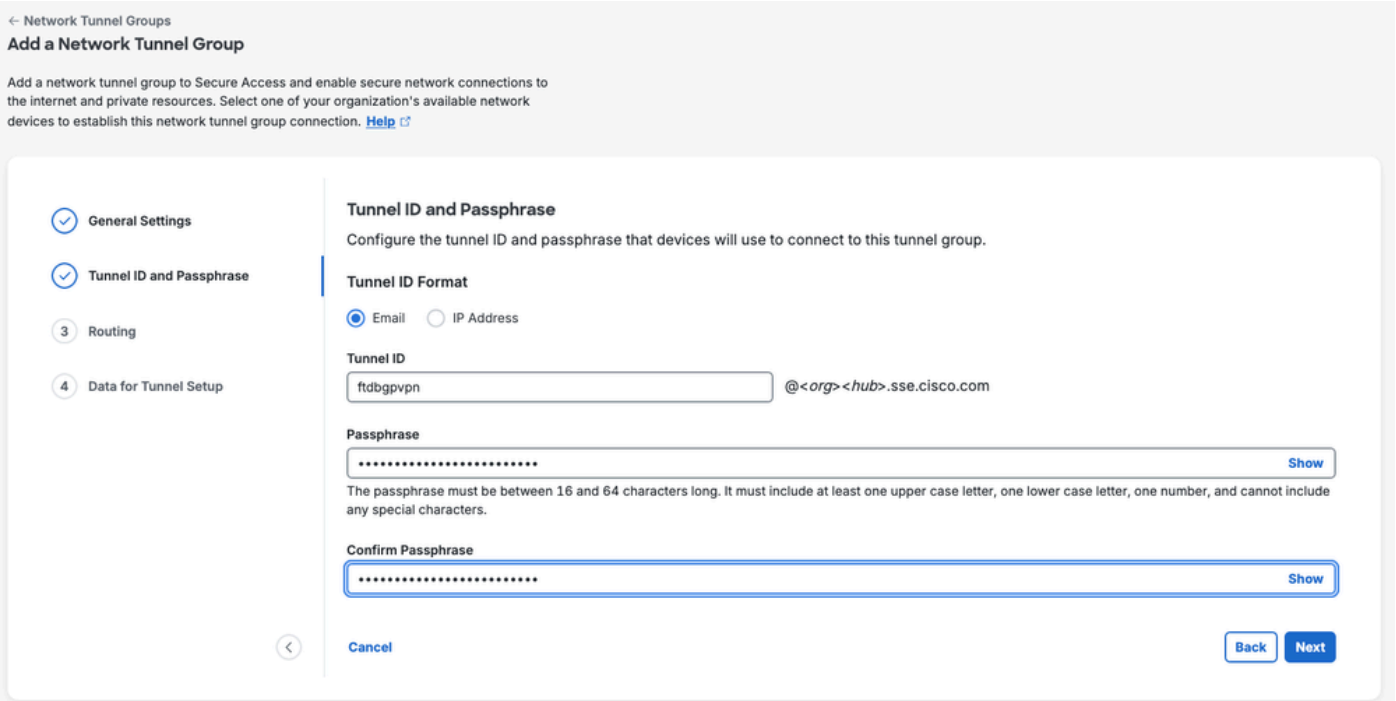
- Naam, regio en apparaattype van tunnelgroep configureren
- Klik op Volgende



Veilige toegang - Algemene instellingen voor netwerktunnelgroepen

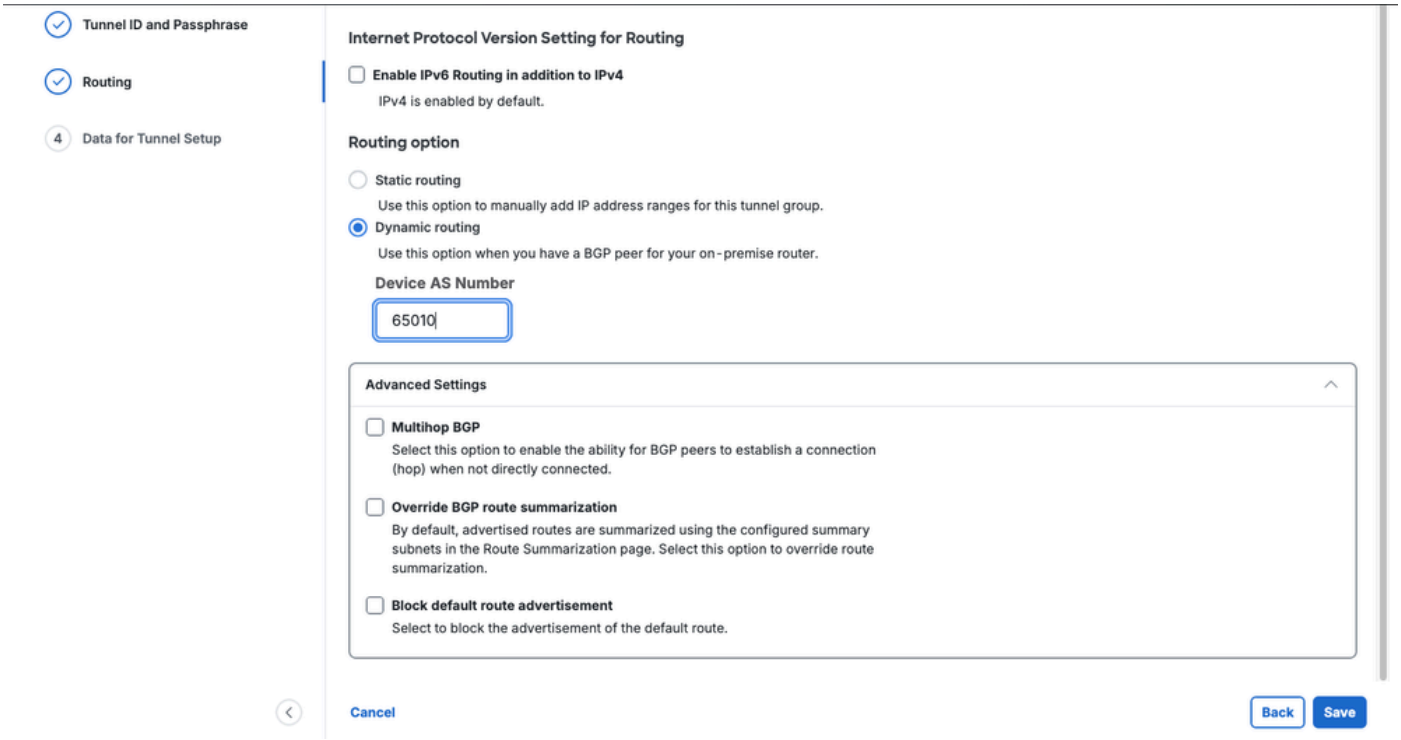
4. Configureer Tunnel ID en wachtwoordgroep.

- Configureer de tunnel-ID en wachtwoordgroep.
- Klik op Volgende

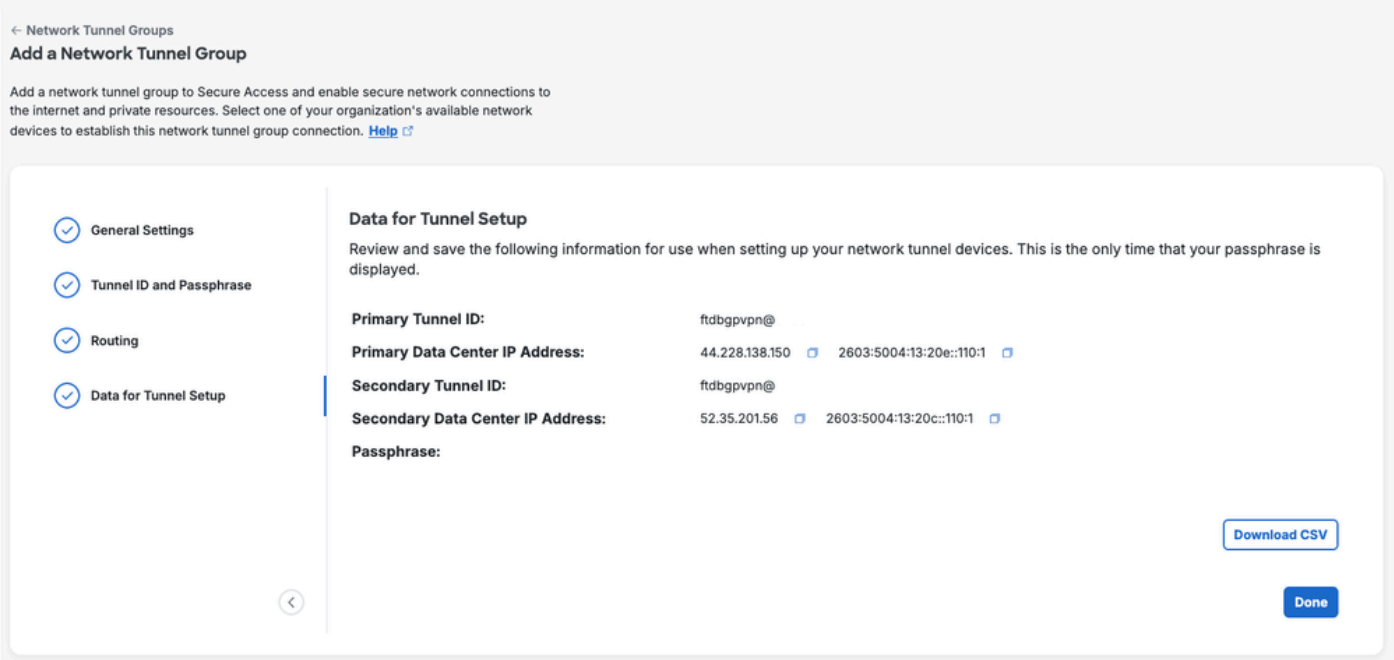


5. Routering configureren

- AS-nummer van apparaat configureren
- Klik op Opslaan



6. Configuratie van netwerktunnelgroep opslaan



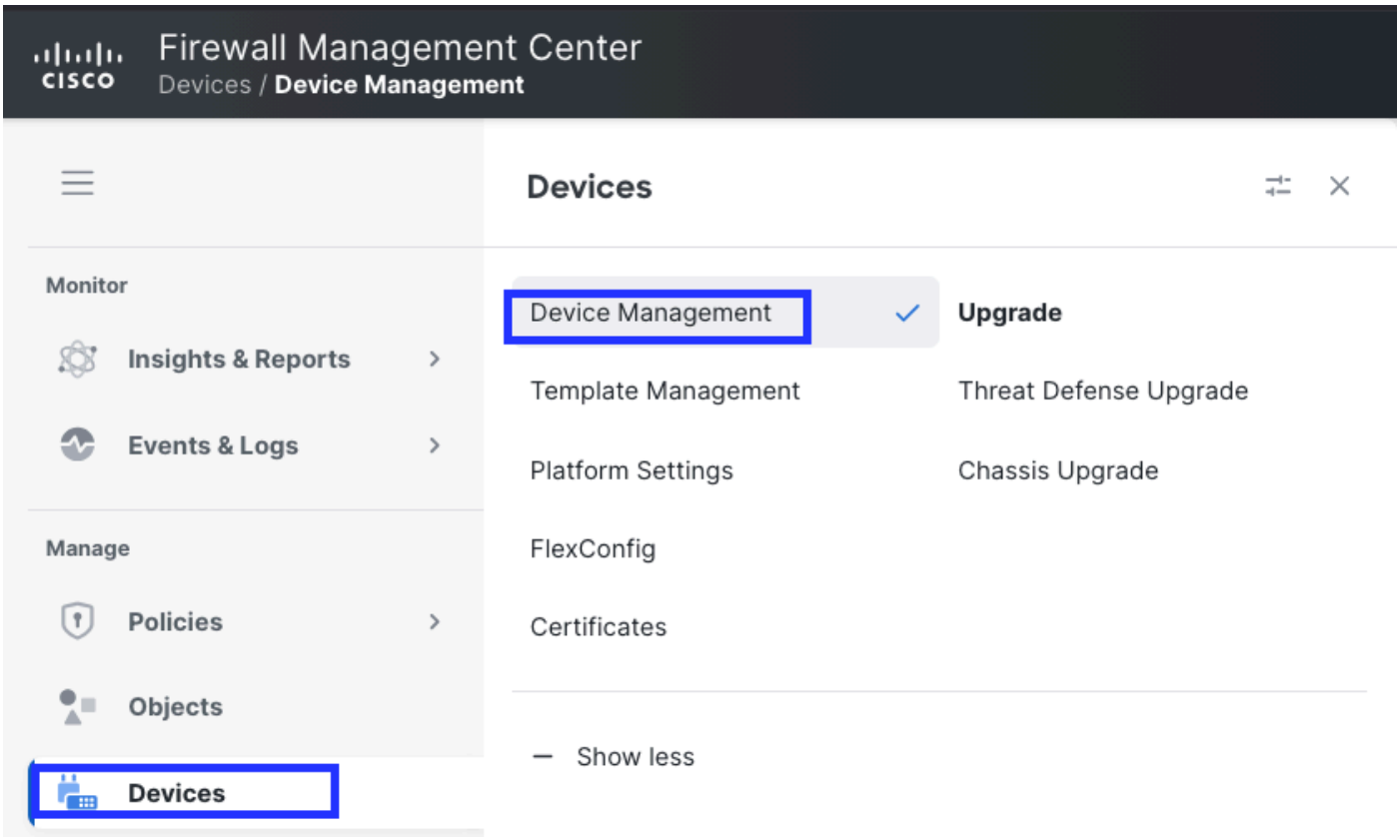
Veilige toegang - Netwerktunnelgroepen

Dynamic Route-based IPsec VPN configureren op Secure Firewall Threat Defense (FTD) met PBR

1. Aanmelden bij Firewall Management Center (FMC)

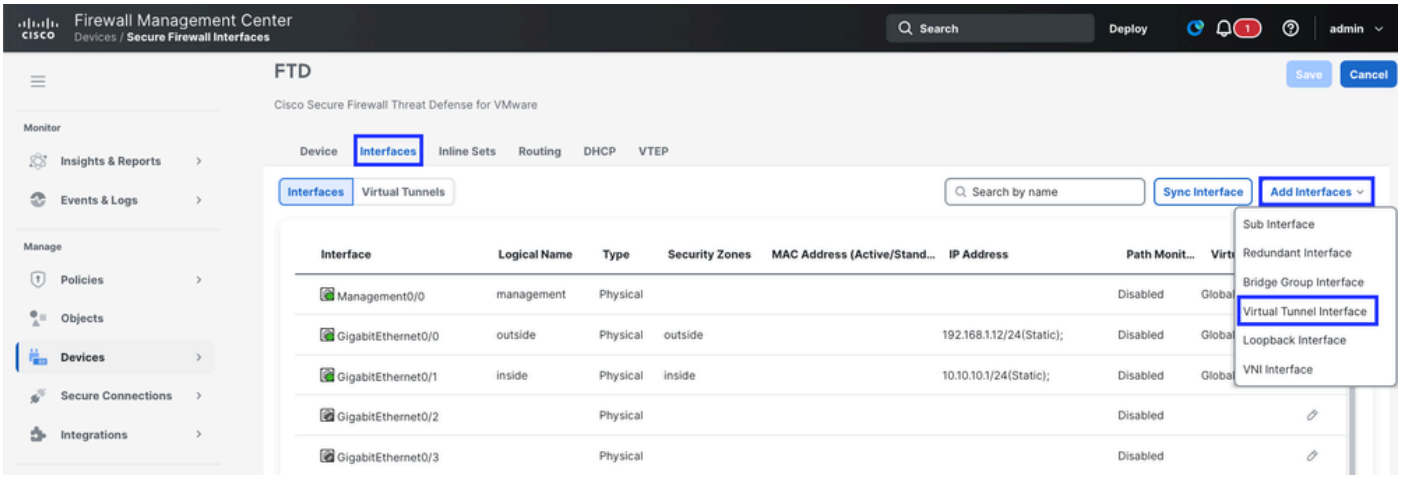
2. Virtual Tunnel Interface VTI configureren

- Navigeer naar Apparaten > Apparaatbeheer



Veilig firewallbeheer - Dashboard

- Klik op het potloodpictogram naast het apparaat en navigeer naar de sectie Interface
- Klik op Interfaces toevoegen en selecteer Virtual Tunnel Interface



Veilig firewallbeheer - FTD VTI-configuratie

- VTI configureren

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

VTI-1

[x] Enabled

Description:

Virtual Tunnel interface for Primary VTI VPN

Security Zone:

vti

Priority:

0 *(0 - 65535)*

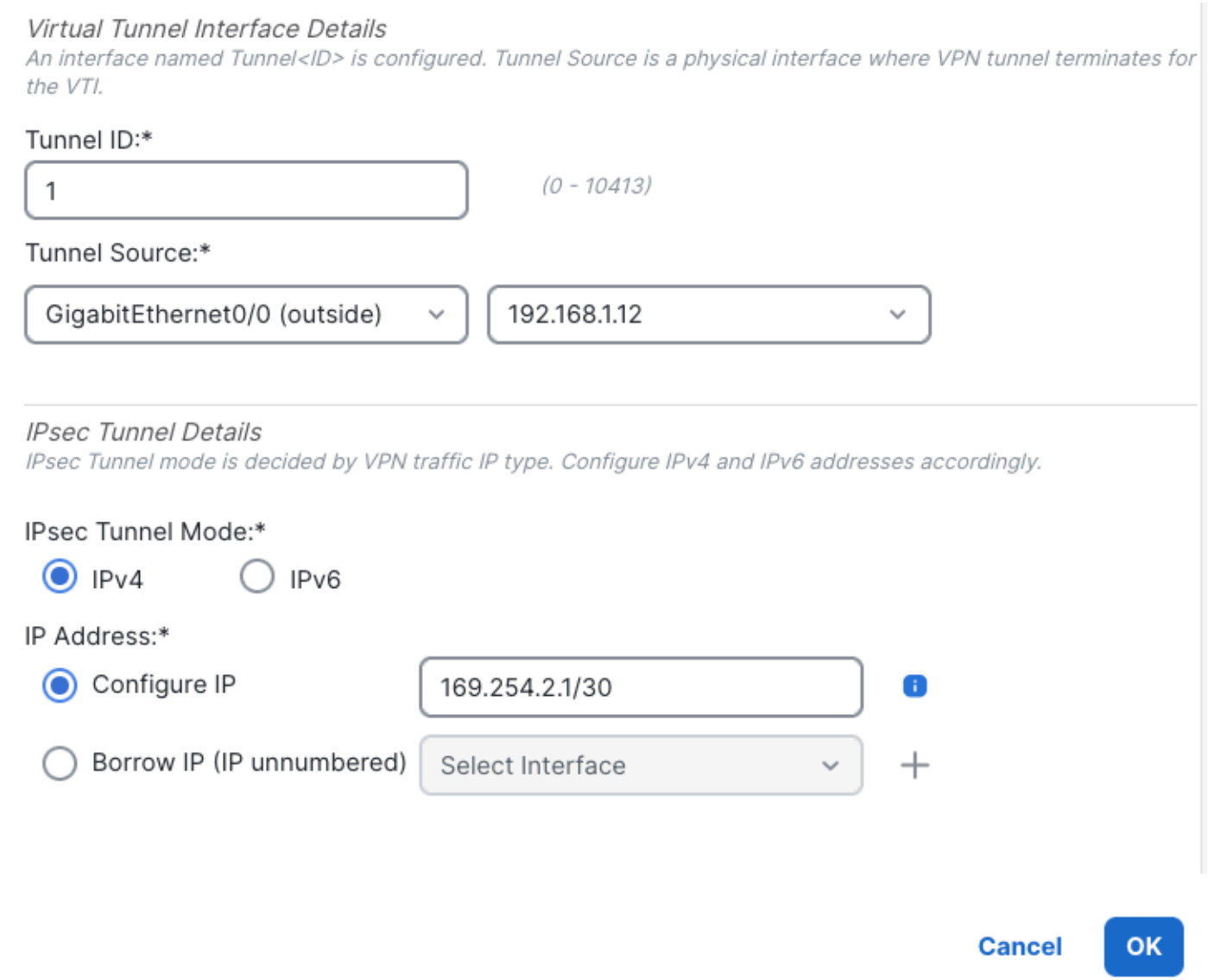
Propagate Security Group Tag: [x]

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

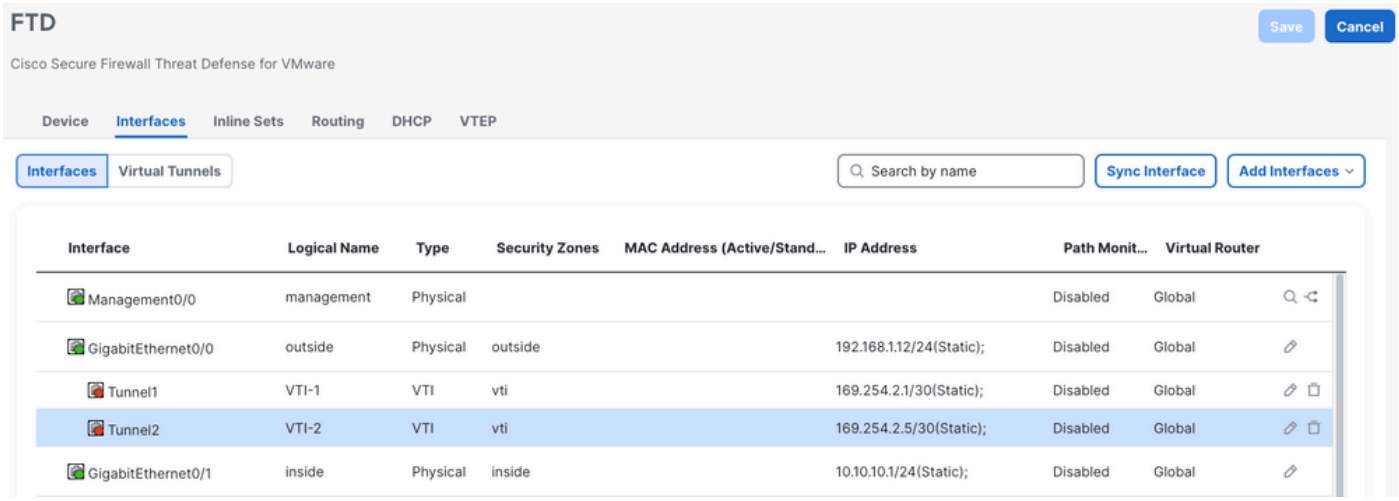
Tunnel ID:*

1 *(0 - 10413)*

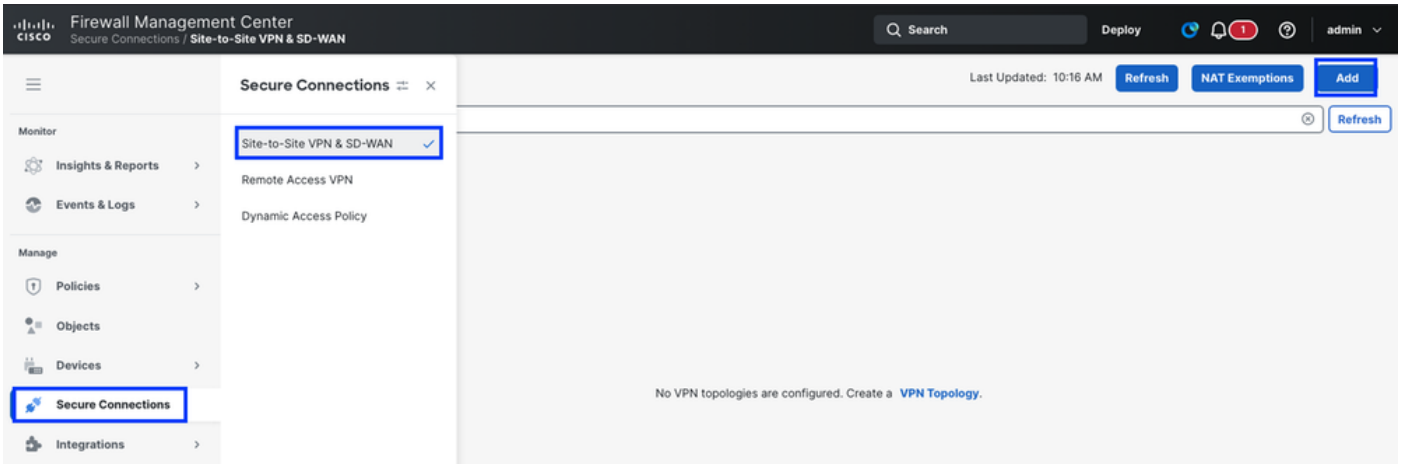


Veilig firewallbeheer - FTD VTI-configuratie

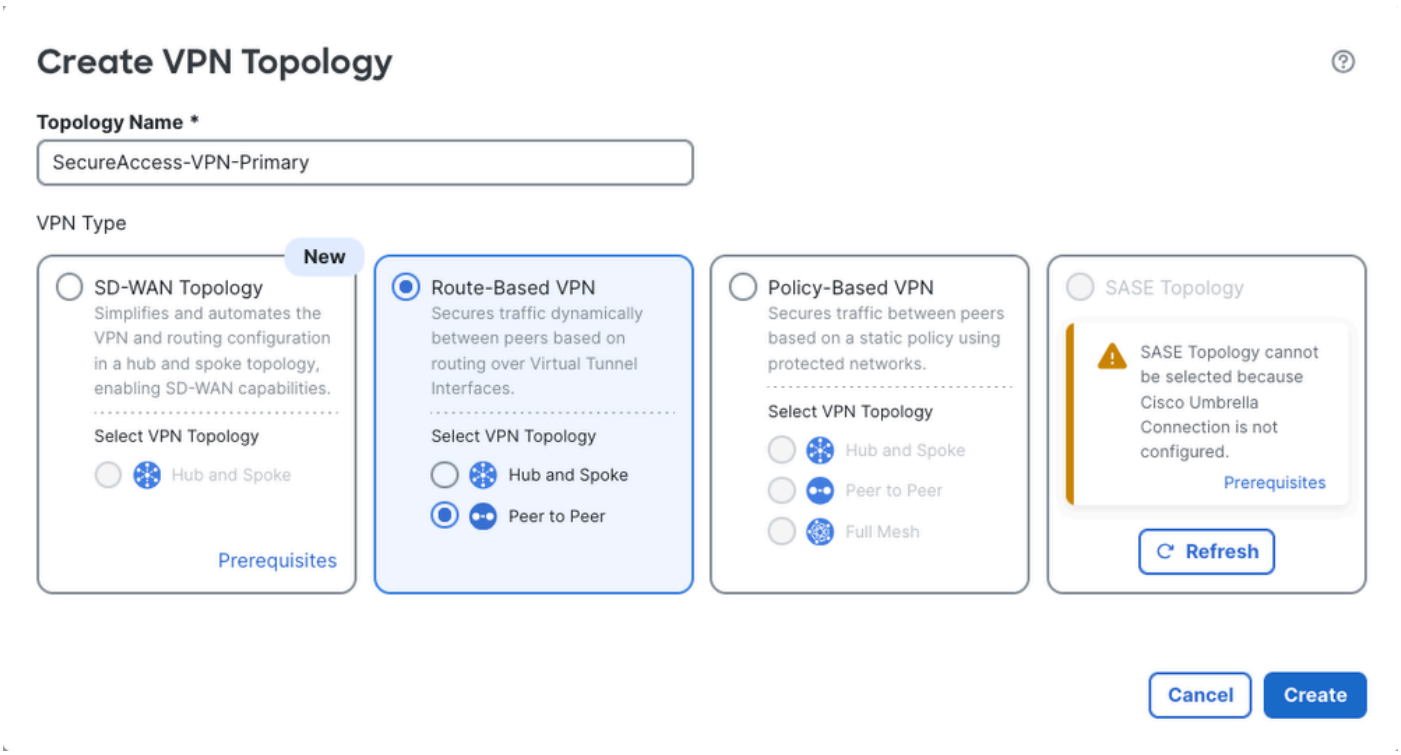
- Configureer ook VTI-2 voor secundaire IPsec VPN met beveiligde toegang



3. Navigeer naar Beveiligde verbindingen > Site-to-Site VPN & SD-WAN en klik op Toevoegen om de VPN te configureren



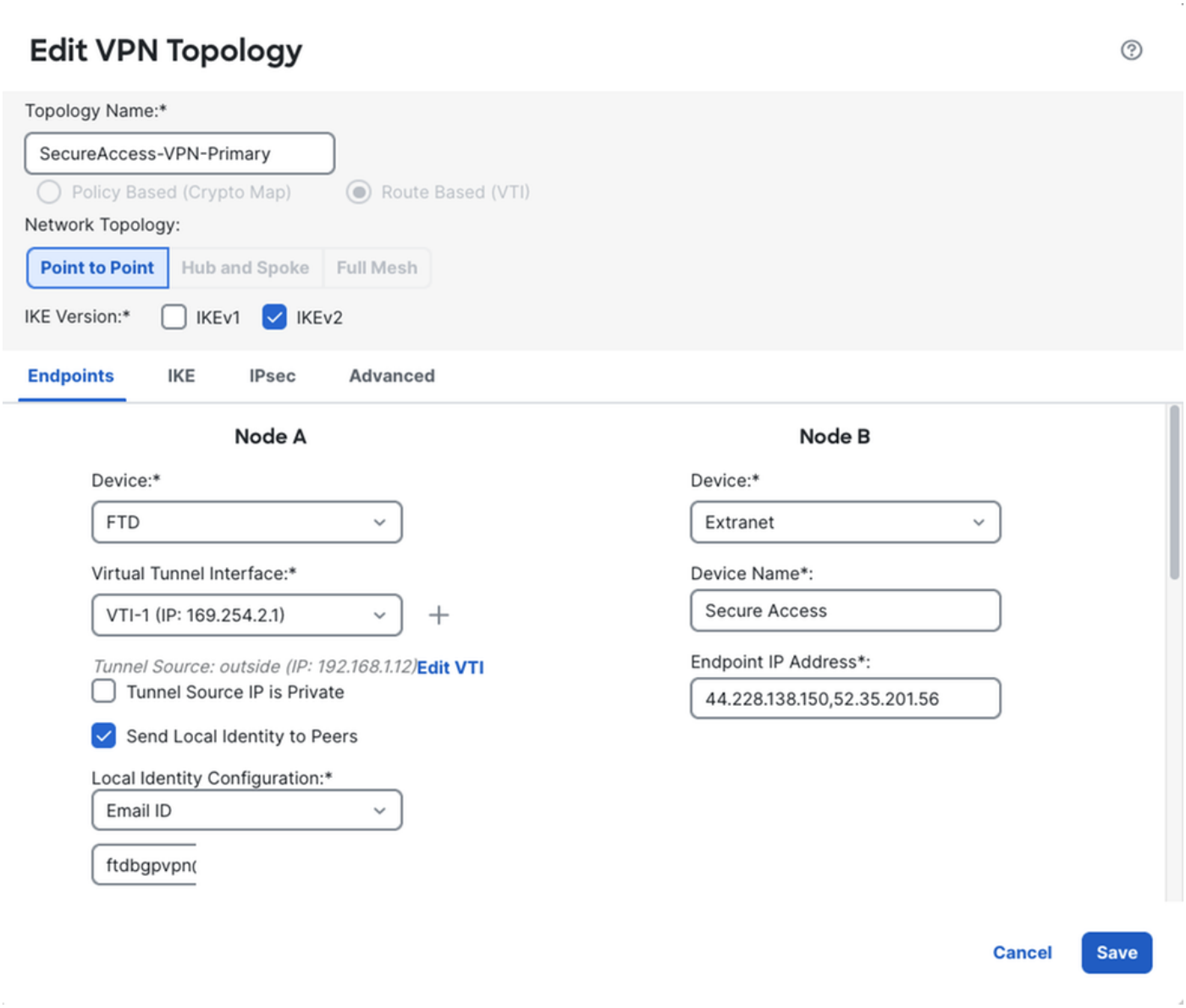
- VPN-topologie maken



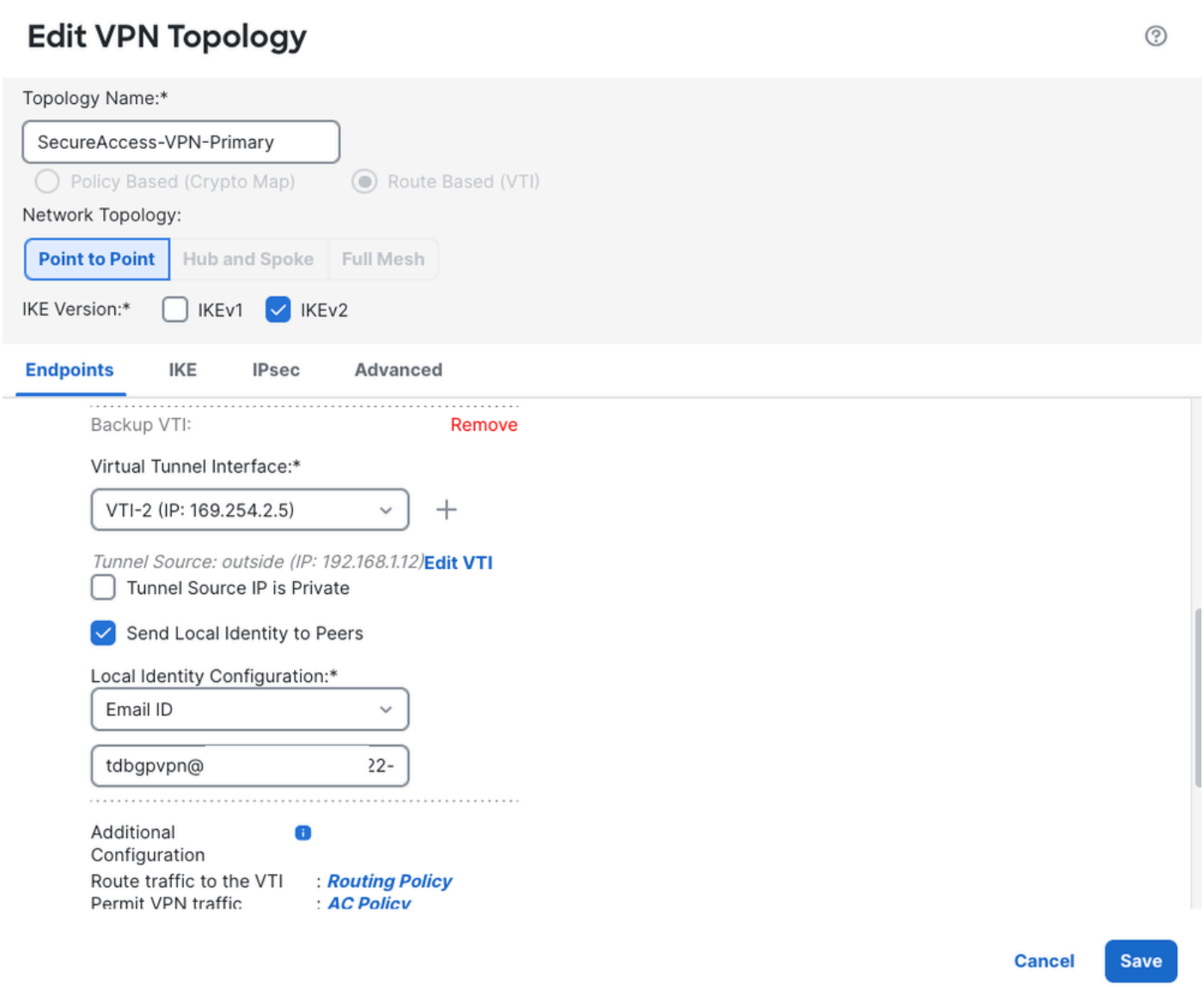
- Verkrijg vanaf stap 6 van de Configure Network Tunnel Group on Secure Access de tunnel-

ID's en IP-adressen voor de primaire en secundaire datacenters.

- Klik op Eindpunten
- Klik onder knooppunt A op Apparaat en selecteer uw FTD-apparaat
- Klik op Virtual Tunnel Interface en selecteer de eerste VTI-interface die in de vorige stap is gemaakt
- Klik op de optie Lokale identiteit naar collega's verzenden en selecteer E-mail-ID, voer de primaire tunnel-ID in (van "Configuratie netwerktunnelgroep opslaan" onder Netwerktunnelgroep configureren voor beveiligde toegang)
- Klik onder knooppunt B op Apparaat en selecteer Extranet
- Klik op Apparaatnaam en geef deze een naam
- Klik op IP-adressen van eindpunten en voer de primaire en secundaire IP-adressen voor beveiligde toegang in, gescheiden door een komma (van "Configuratie netwerktunnelgroep opslaan" onder Netwerktunnelgroep configureren voor beveiligde toegang)
- Klik op VTI voor back-up toevoegen
- Klik op Virtual Tunnel Interface en selecteer de tweede VTI-interface die in de vorige stap is gemaakt
- Klik op de optie Lokale identiteit naar collega's verzenden en selecteer E-mail-ID, voer de secundaire tunnel-ID in (van "Configuratie netwerktunnelgroep opslaan" onder Netwerktunnelgroep configureren voor beveiligde toegang)
- Klik op Opslaan

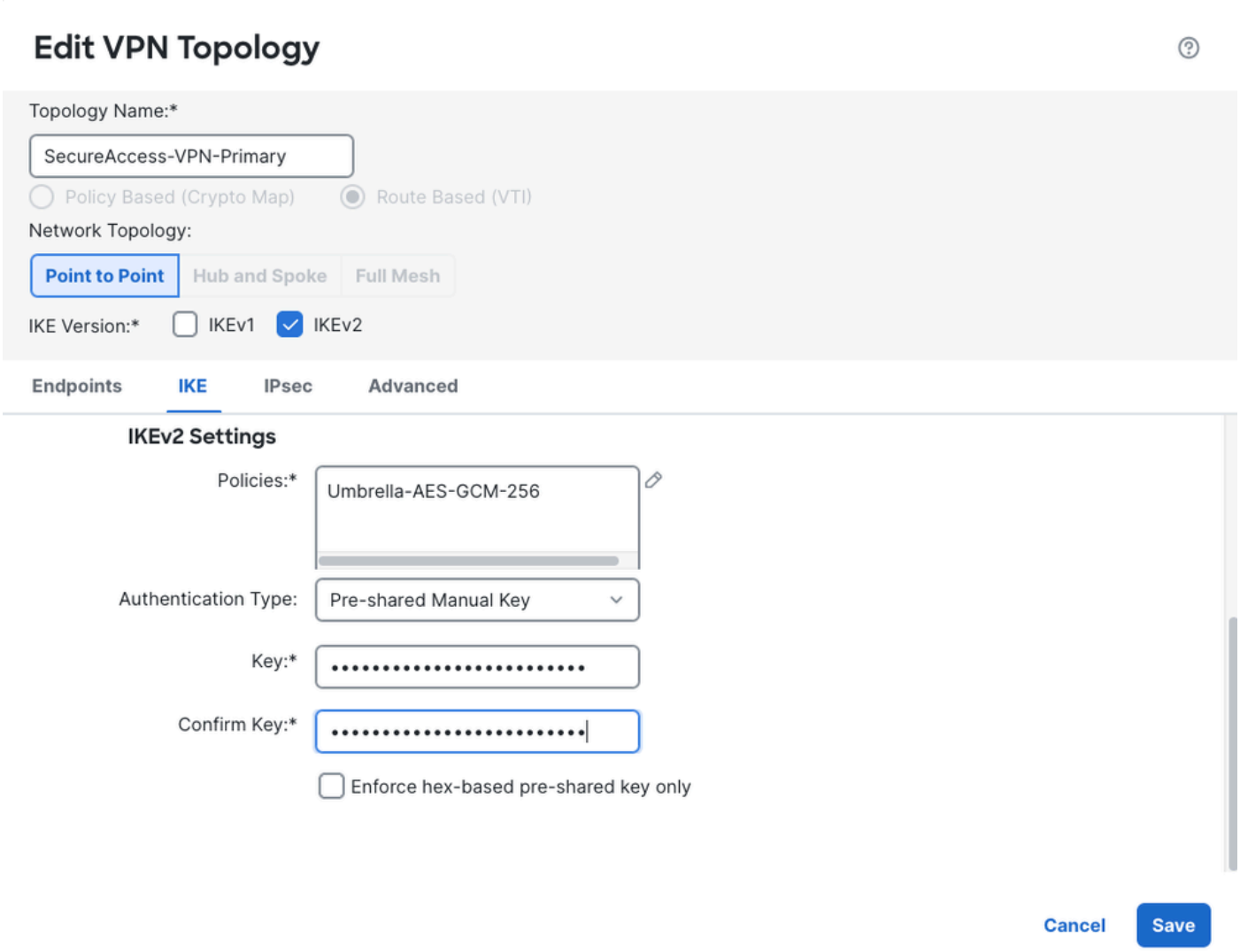


Veilige FTD - VPN-eindpuntconfiguratie



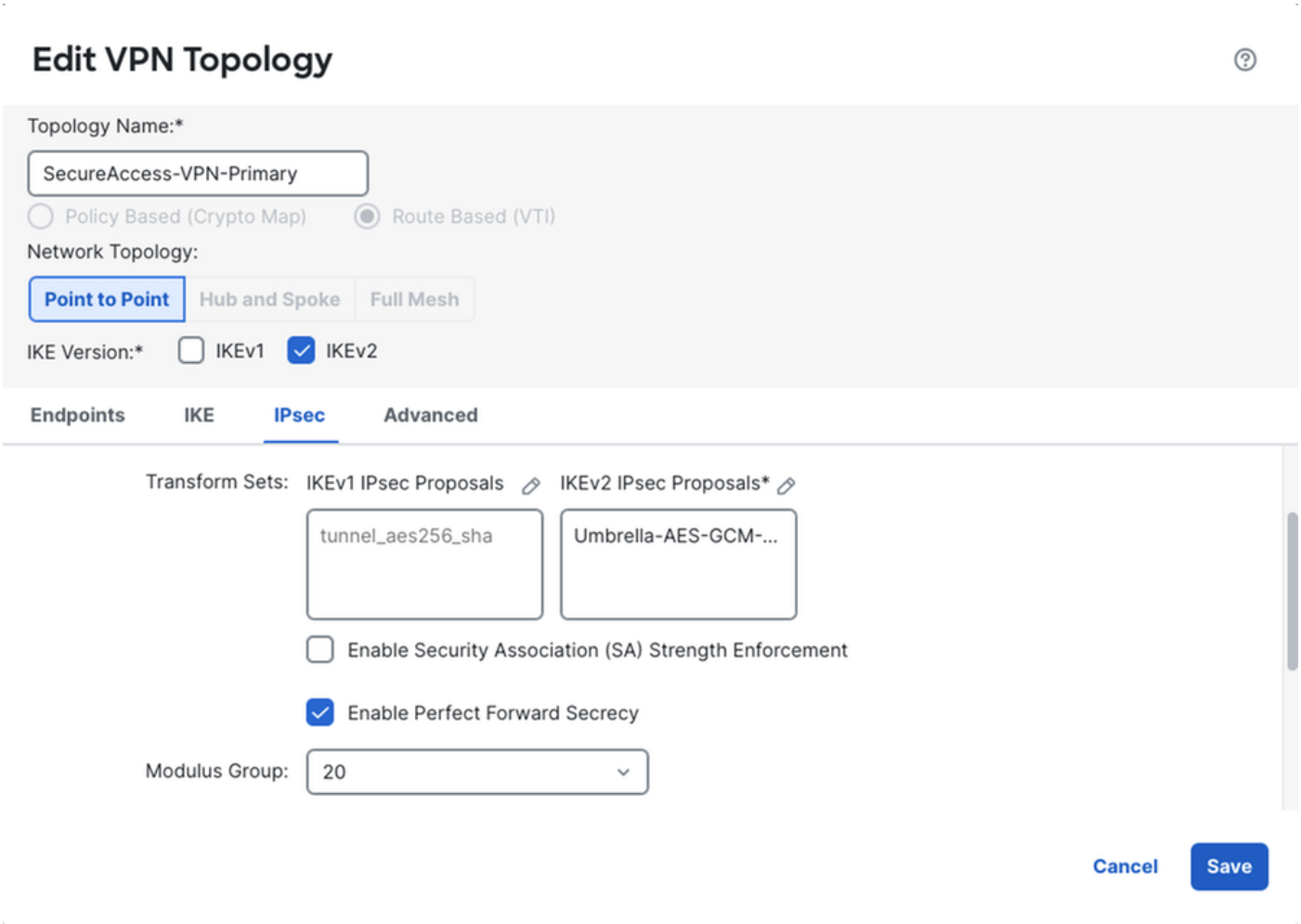
Veilige FTD - VPN-eindpuntconfiguratie

- IKEv2-instellingen configureren volgens ondersteunde IPsec-parameters
  - Selecteer Beleid als Paraplu-AES-GCM-256
  - Selecteer Verificatietype als vooraf gedeelde handmatige sleutel



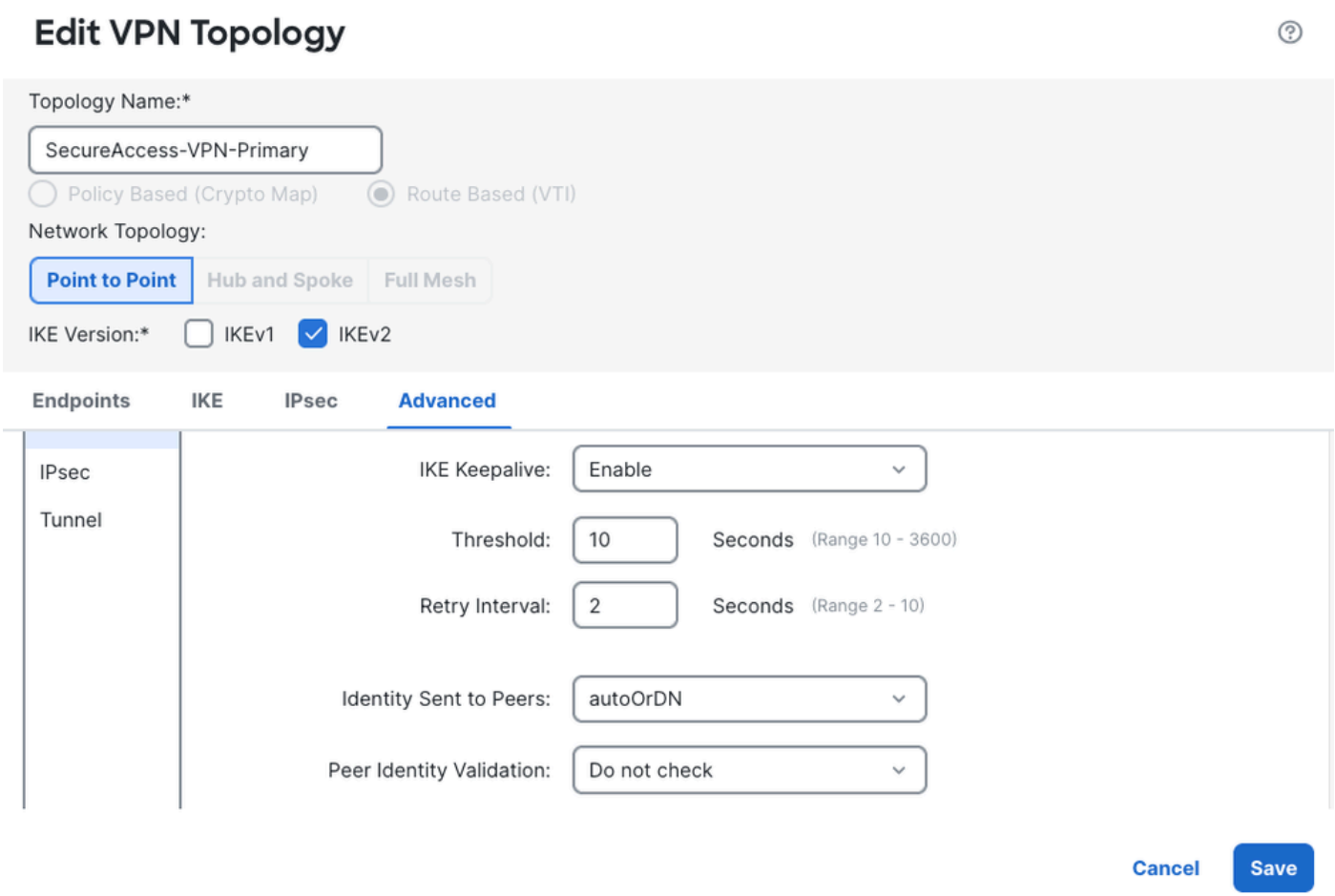
Secure FTD - VPN IKE-instellingen

- IPsec-instellingen configureren
  - Selecteer IKEv2 IPsec-voorstellen als paraplu-AES-GCM-256
  - Inschakelen PFS als geselecteerde Modulus-groep als 20



Secure FTD - VPN IPsec-instellingen

- Geavanceerde instellingen
- Klik op Opslaan



Secure FTD - Geavanceerde VPN-instellingen

FTD-beleidsgebaseerde routering

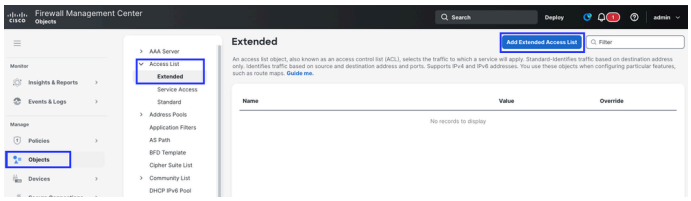
Bij traditionele routering worden pakketten gerouteerd op basis van het IP-adres van de bestemming. Het veranderen van de routering van specifiek verkeer in een op bestemming gebaseerd routeringssysteem is moeilijk. Policy Based Routing (PBR) breidt de mechanismen die worden geboden door routeringsprotocollen uit en vult deze aan, waardoor u meer controle hebt over routering.

Met PBR kunt u de IP-prioriteit instellen. Hiermee kunt u ook een pad opgeven voor bepaald verkeer, zoals prioriteitsverkeer via een dure link. Met PBR kunt u routering definiëren die is gebaseerd op andere criteria dan het bestemmingsnetwerk, zoals de bronpoort, het bestemmingsadres, de bestemmingspoort, het protocol, toepassingen of een combinatie van deze objecten. Raadpleeg Beleidsgebaseerde routering voor meer informatie

1. Toegangslijst configureren

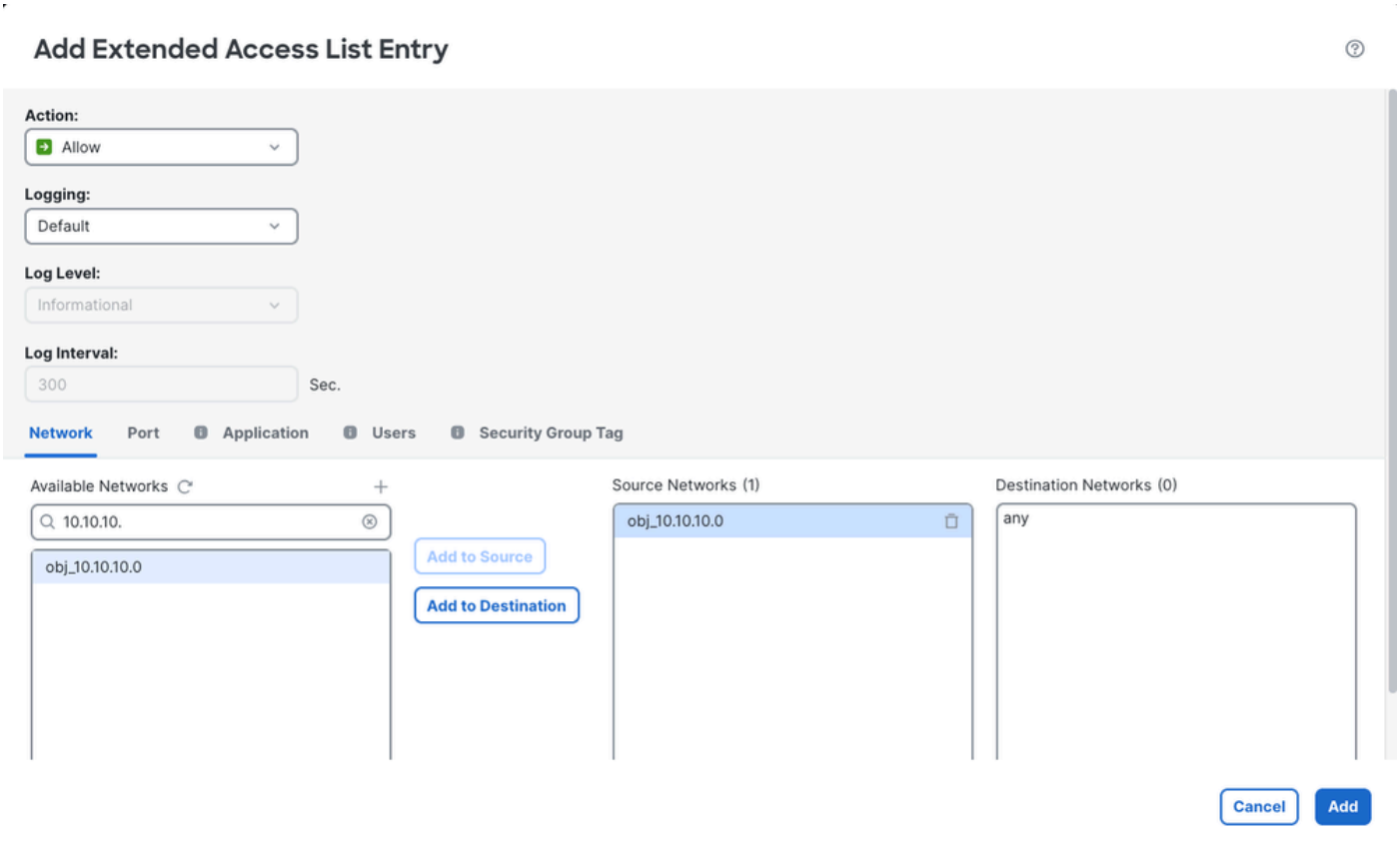
- Navigeer naar Objecten > Toegangslijst > Uitgebreid

- Klik op Uitgebreide toegangslijst toevoegen

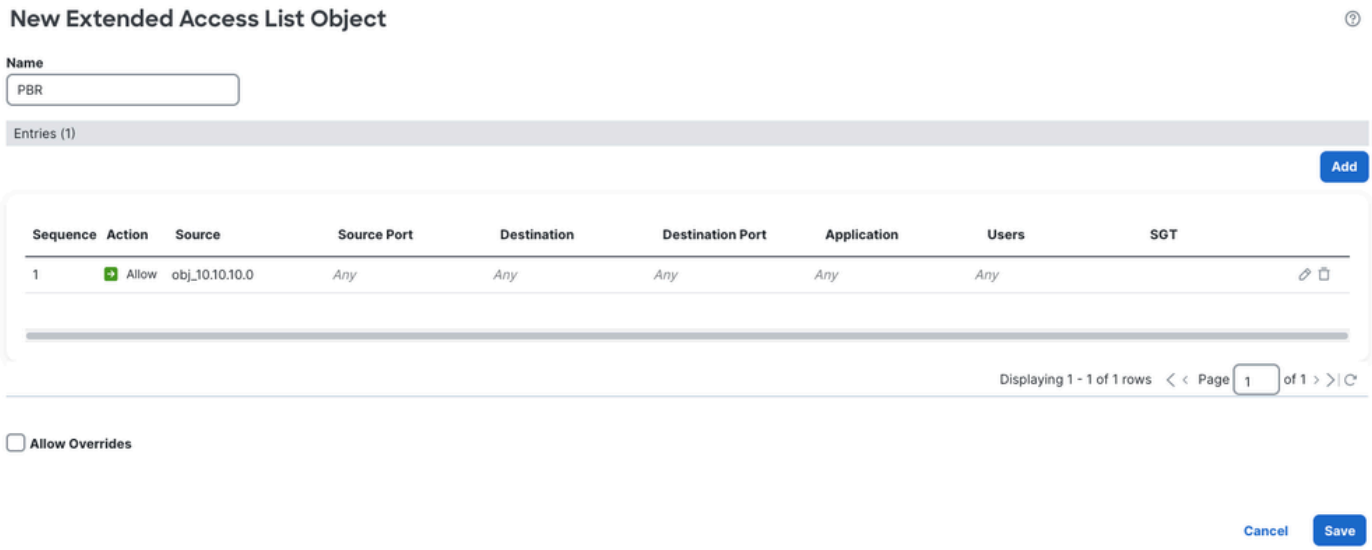


Veilige FTD - Uitgebreide toegangslijst

- Geef de naam van de toegangslijst op
- Definieer de actie
  - Toestaan. - Het gedefinieerde verkeer wordt naar de IPsec-tunnel gestuurd
  - Blokkering - Het verkeer wordt omzeild vanuit de IPsec-tunnel
  - Regel wordt gekoppeld op basis van volgnummer (van lager naar hoger)
  - Klik op Toevoegen
  - Klik op Opslaan



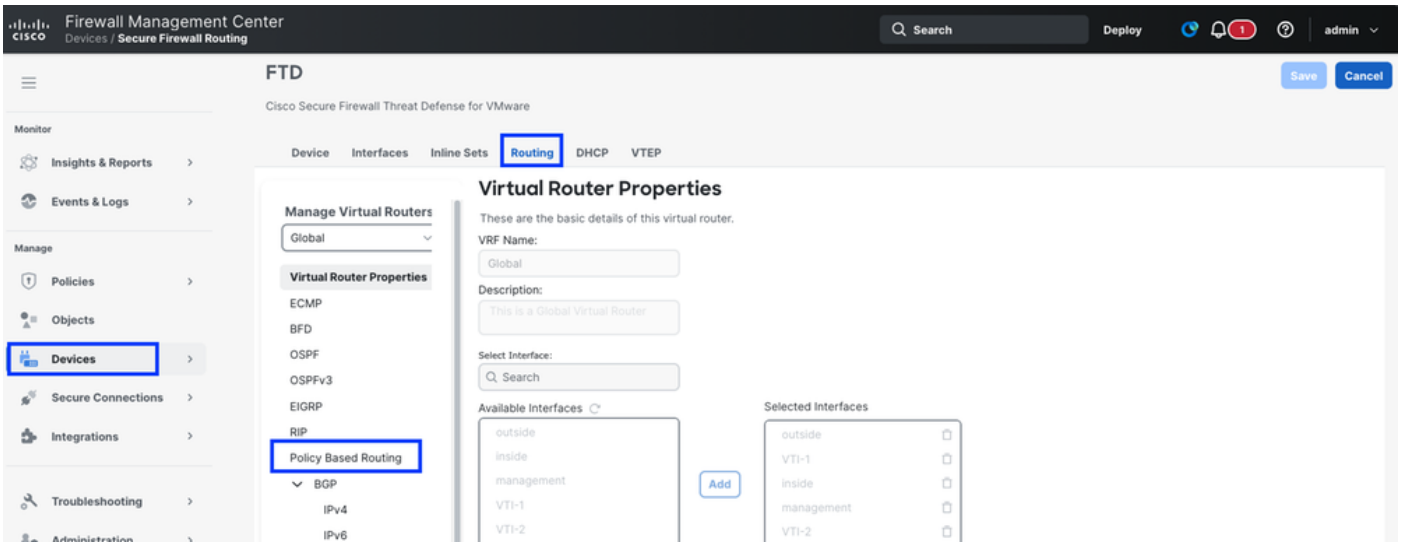
Veilige FTD - Uitgebreide toegangslijst



Veilige FTD - Uitgebreide toegangslijst

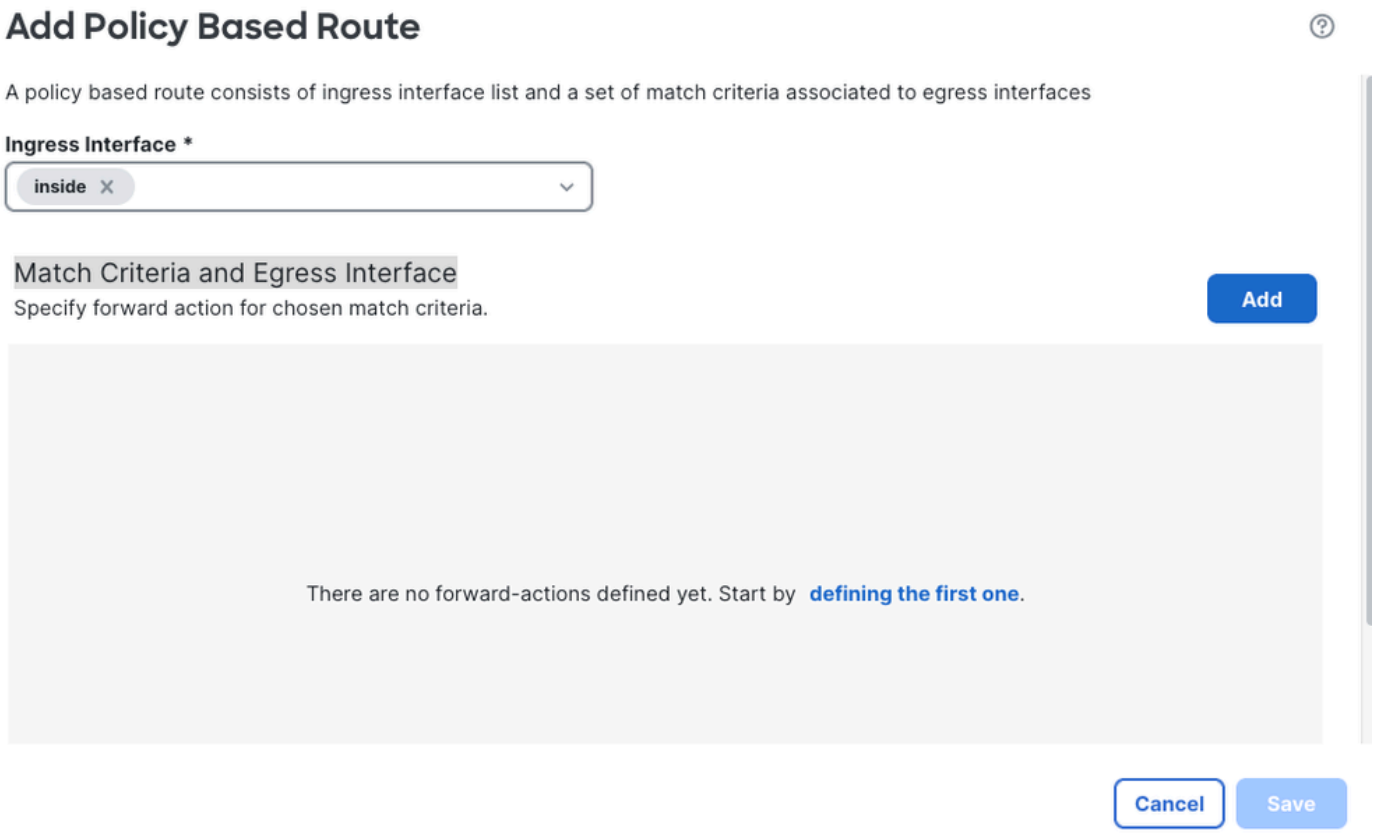
2. Op beleid gebaseerde routering configureren

- Navigeer naar Apparaten > Apparaatbeheer > FTD > Routering



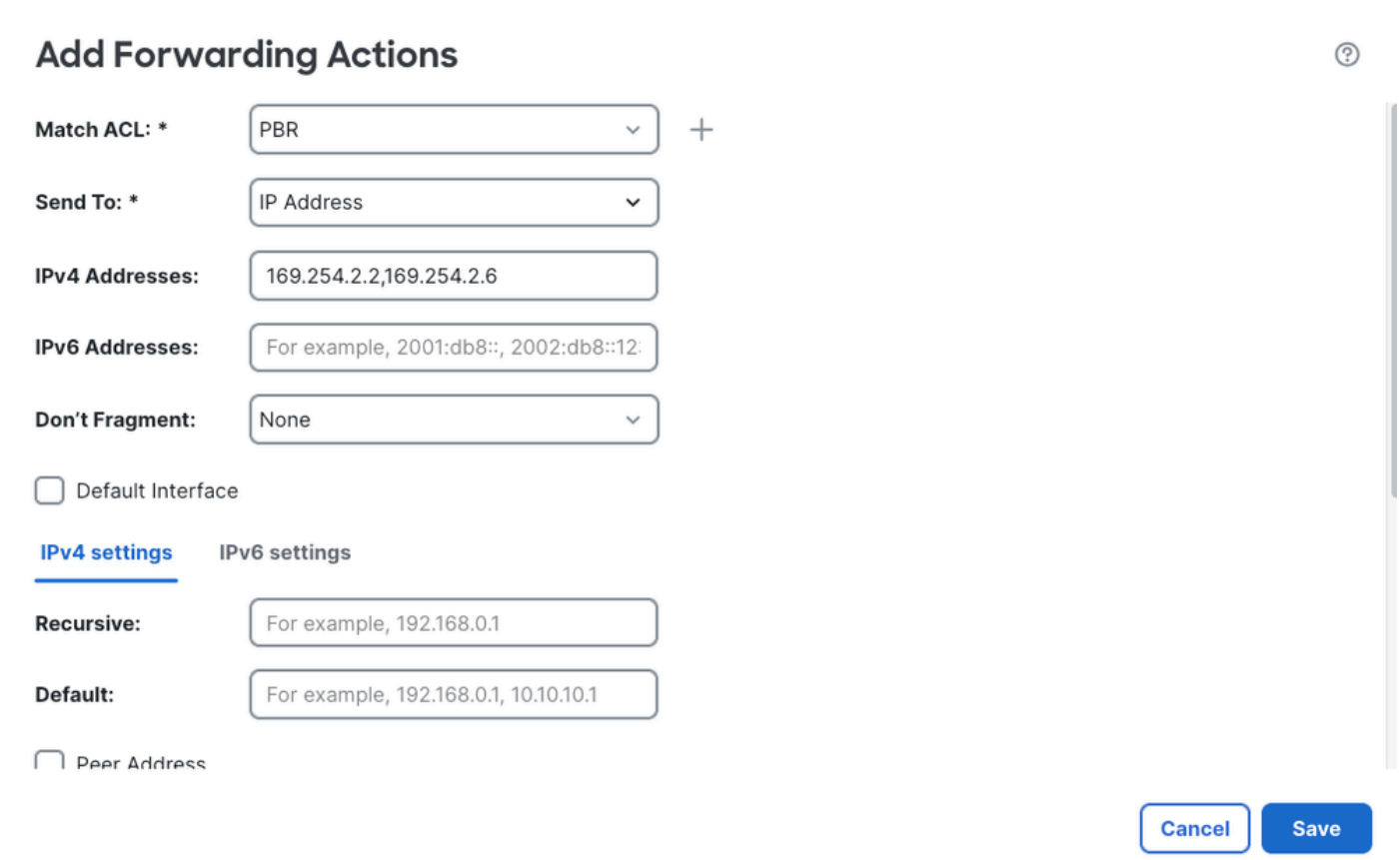
Veilige FTD - op beleid gebaseerde routering

- Klik op Toevoegen
- Selecteer Ingress Interface - Ingress-interface voor het subnet dat we in de toegangslijst hebben gedefinieerd

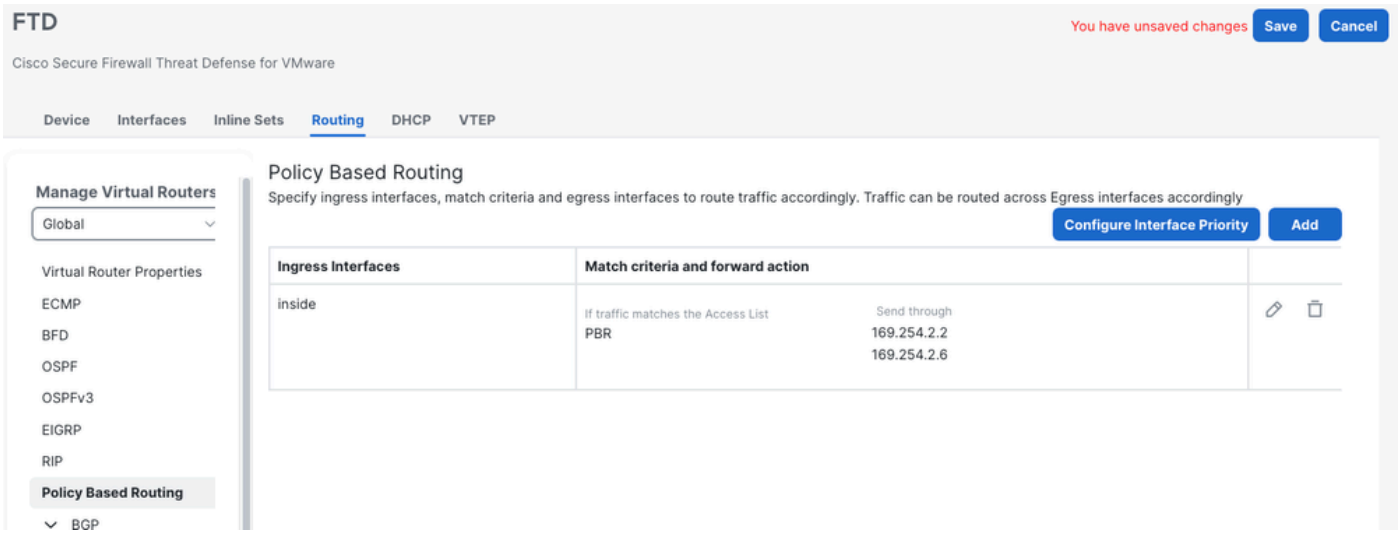


Veilige FTD - op beleid gebaseerde routering

- Overeenstemmingscriteria en uitgang-interface definiëren
  - Klik op Toevoegen
  - Selecteer de ACL-overeenkomst
  - Selecteer Verzenden naar als IP-adres
  - IP-adres voor volgende hop toevoegen. - IP-adressen van de VTI-interface worden verwijderd. 169.254.2.130 en. 169.254.2.5/30 . De volgende IP-adressen voor VTI-1 en VTI-2 zouden dus 169.254.2.2 en hoger zijn. 169 254 2,6
  - Klik op Opslaan



Veilige FTD - op beleid gebaseerde routering

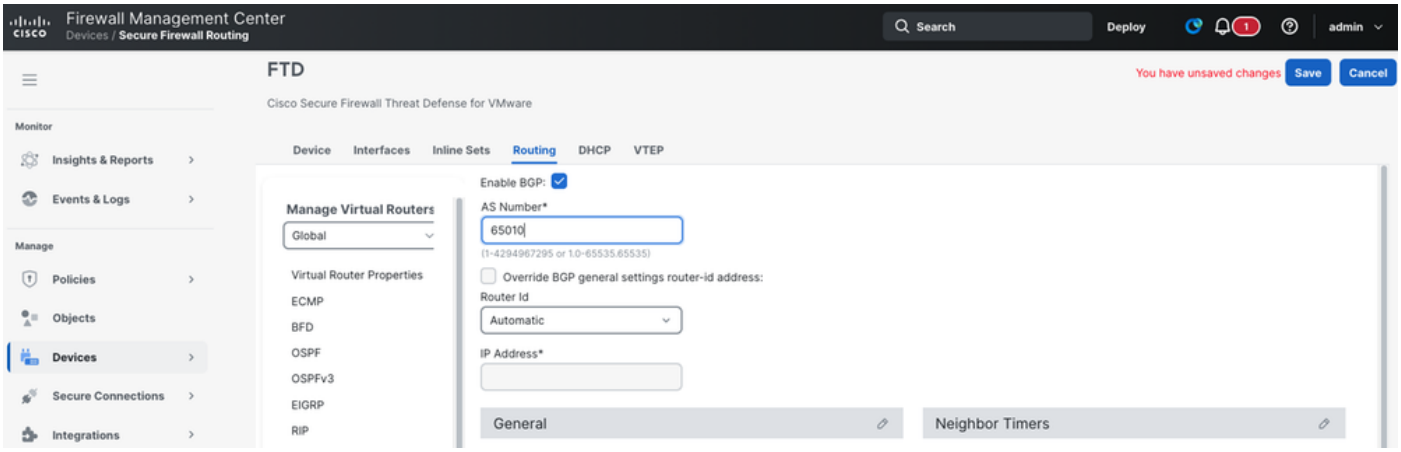


Veilige FTD - op beleid gebaseerde routering

BGP configureren op FTD

1. BGP inschakelen

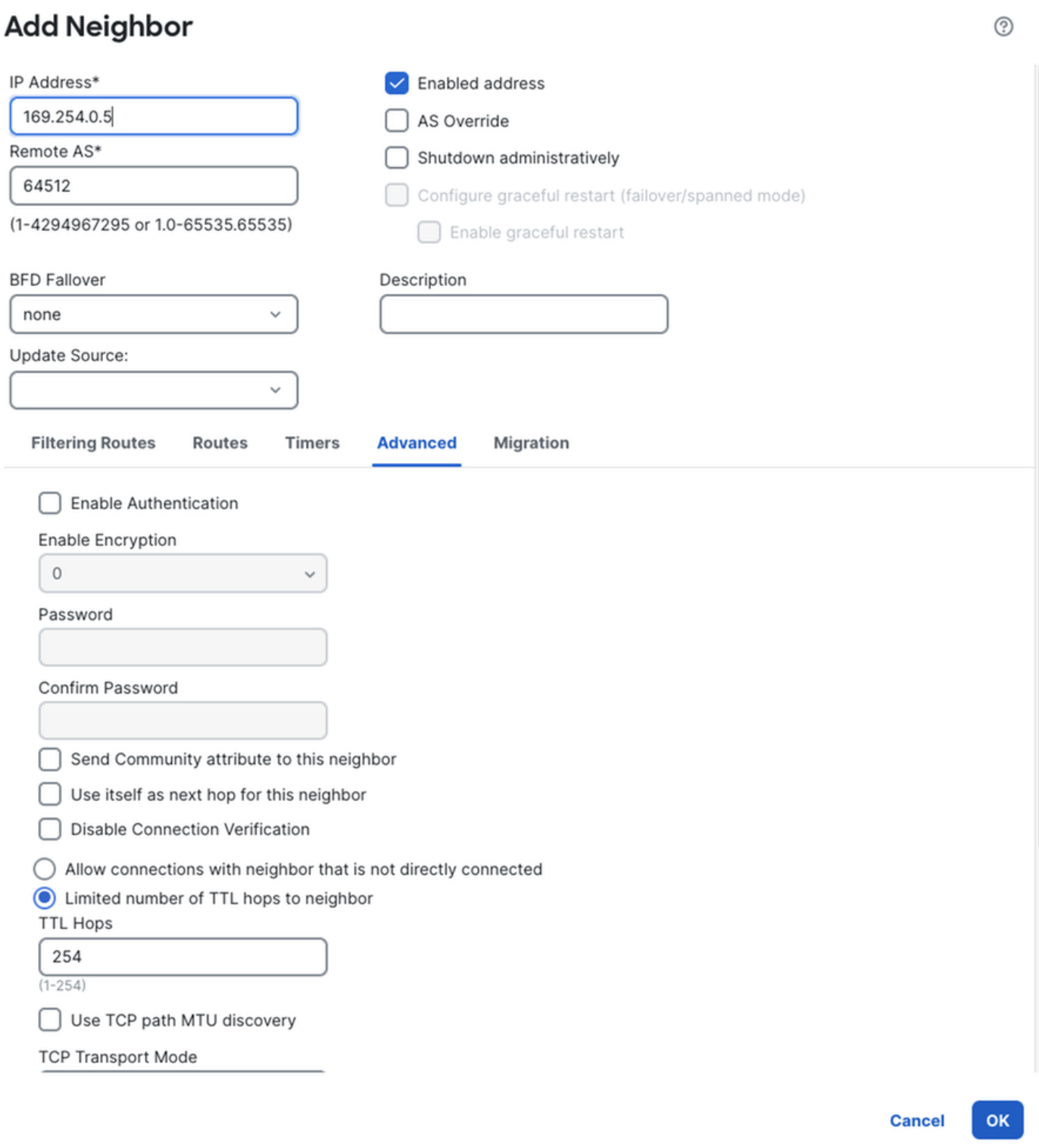
- Navigeer naar Apparaten > Apparaatbeheer > FTD > Routering > Algemene instellingen > BGP
- BGP inschakelen en het AS-nummer toevoegen (FTD lokaal AS-nummer)
- Klik op Opslaan

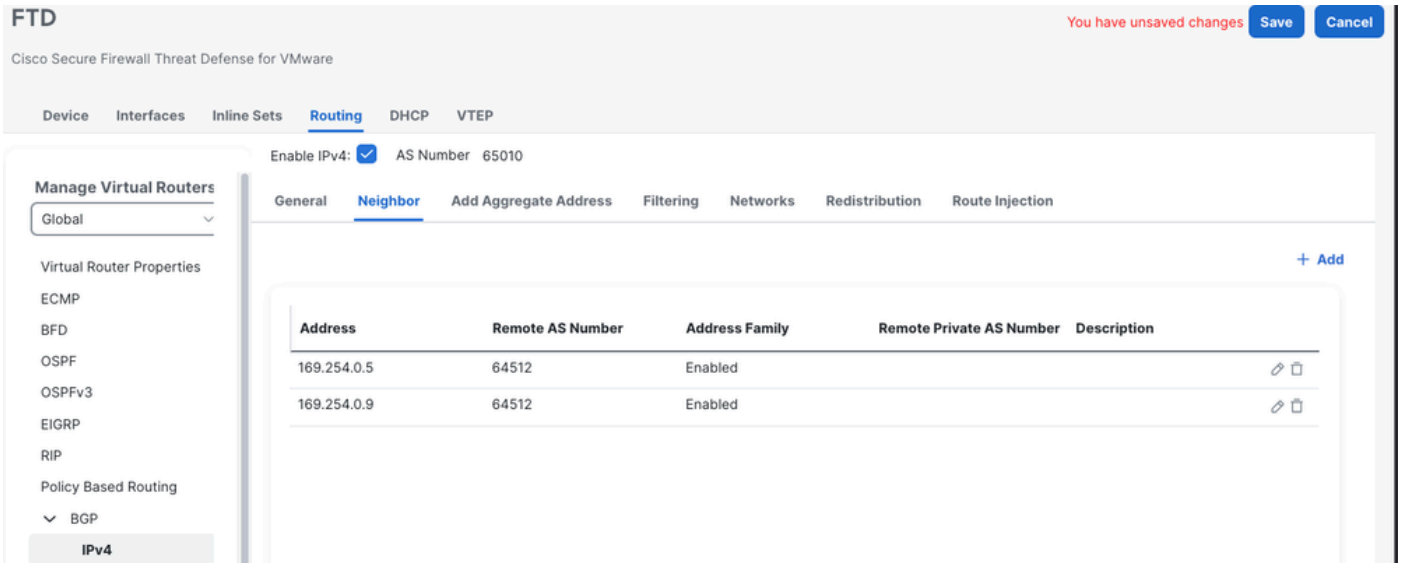


Veilige FTD - BGP-routering

- Navigeer naar BGP > IPv4

2. Voeg BGP Neighbor - Secure Access BGP-peers toe: 169.254.0.5 en. 169.254.0.9

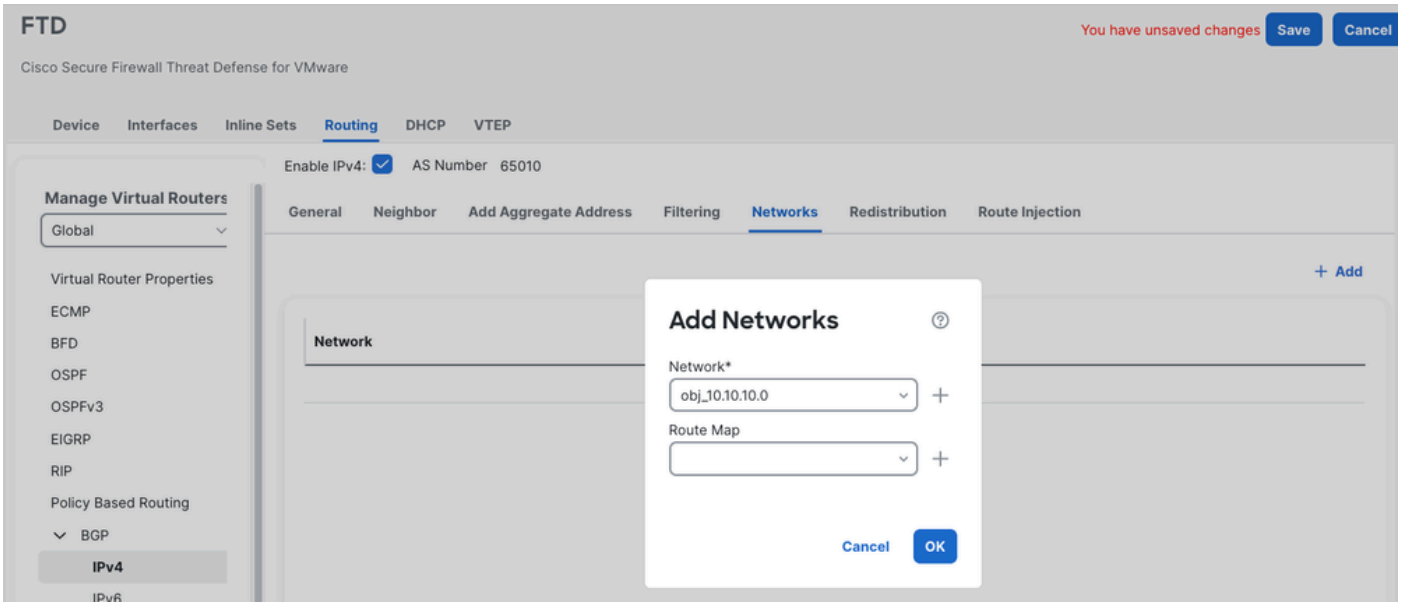

Add Neighbor
IP Address*
169.254.0.5
Remote AS*
64512
(1-4294967295 or 1.0-65535.65535)
Enabled address
AS Override
Shutdown administratively
Configure graceful restart (failover/spanned mode)
Enable graceful restart
BFD Fallover
none
Description
Update Source:
Filtering Routes
Routes
Timers
Advanced
Migration
Enable Authentication
Enable Encryption
0
Password
Confirm Password
Send Community attribute to this neighbor
Use itself as next hop for this neighbor
Disable Connection Verification
Allow connections with neighbor that is not directly connected
Limited number of TTL hops to neighbor
TTL Hops
254
(1-254)
Use TCP path MTU discovery
TCP Transport Mode
Cancel
OK



Veilige FTD - BGP-routering

3. Voeg de netwerken toe - Netwerken waarvoor moet worden geadverteerd voor beveiligde toegang

- Klik op OK

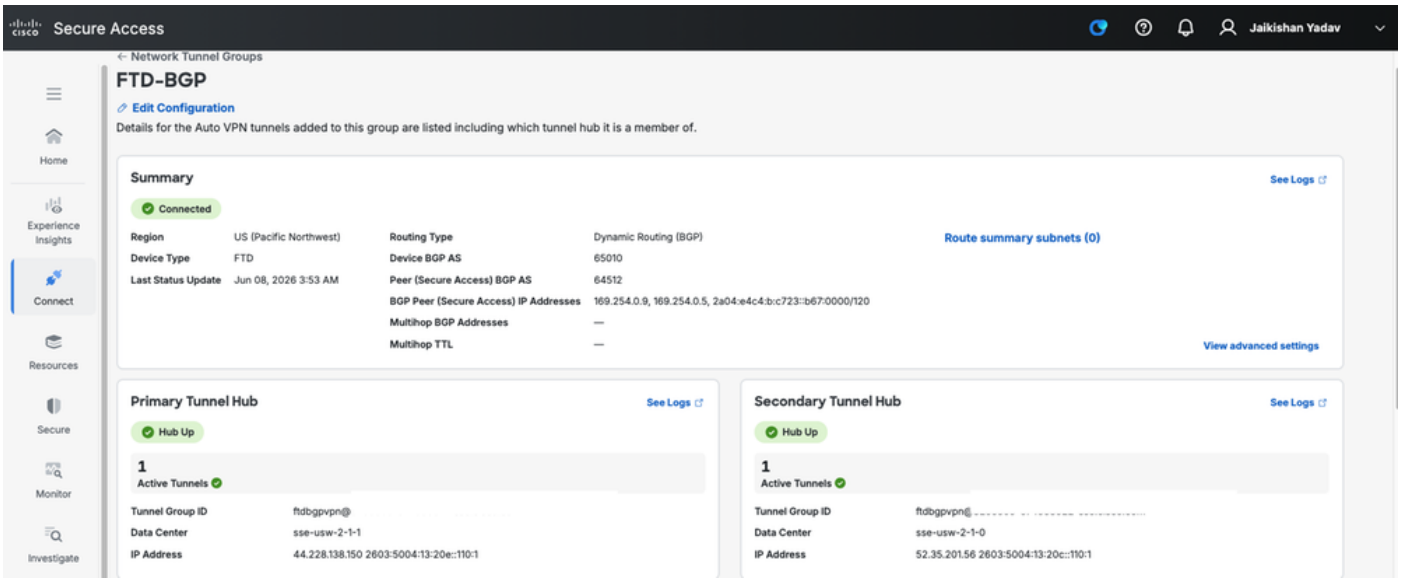


Veilige FTD - BGP-routering

- De wijzigingen opslaan en implementeren

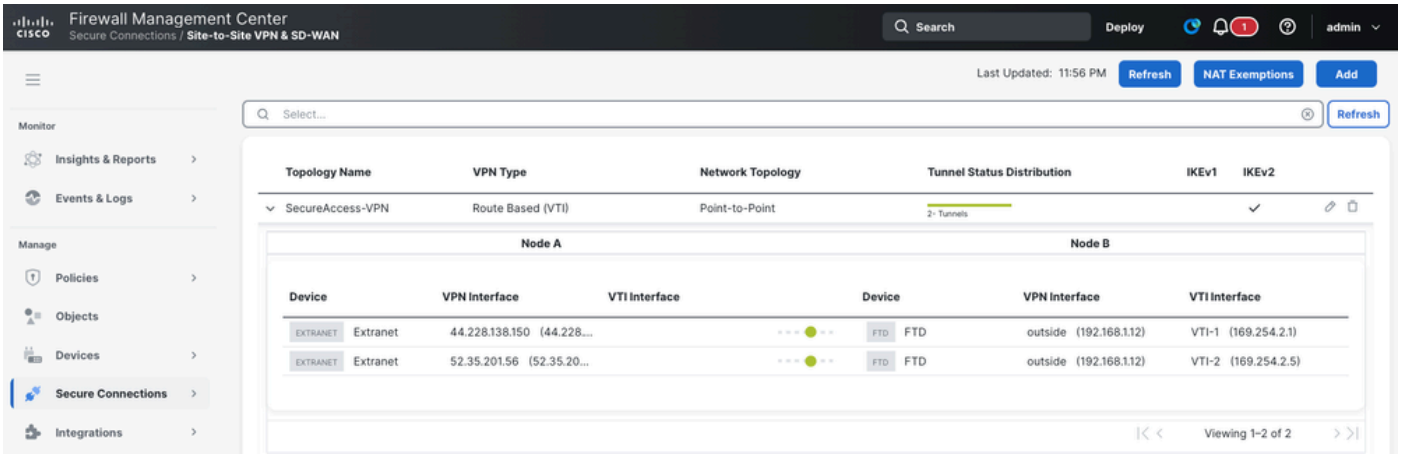
Tunnelstatus controleren

over beveiligde toegang



Veilige FTD - IPsec-tunnelstatus

Over FMC



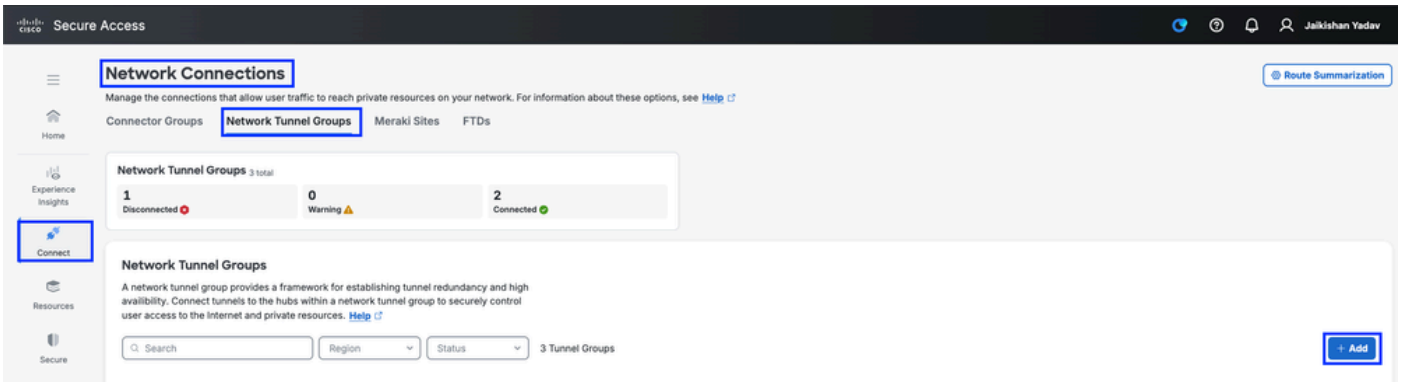
Veilige FMC - IPsec-tunnelstatus

Statische routegebaseerde IPsec VPN configureren op Adaptive Security Appliance (ASA) met PBR

VPN-configuratie voor beveiligde toegang

1. Meld u aan bij het dashboard voor beveiligde toegang Veilige toegang
2. Navigeer naar Verbinden > Netwerkverbindingen > Netwerktunnelgroepen en klik op

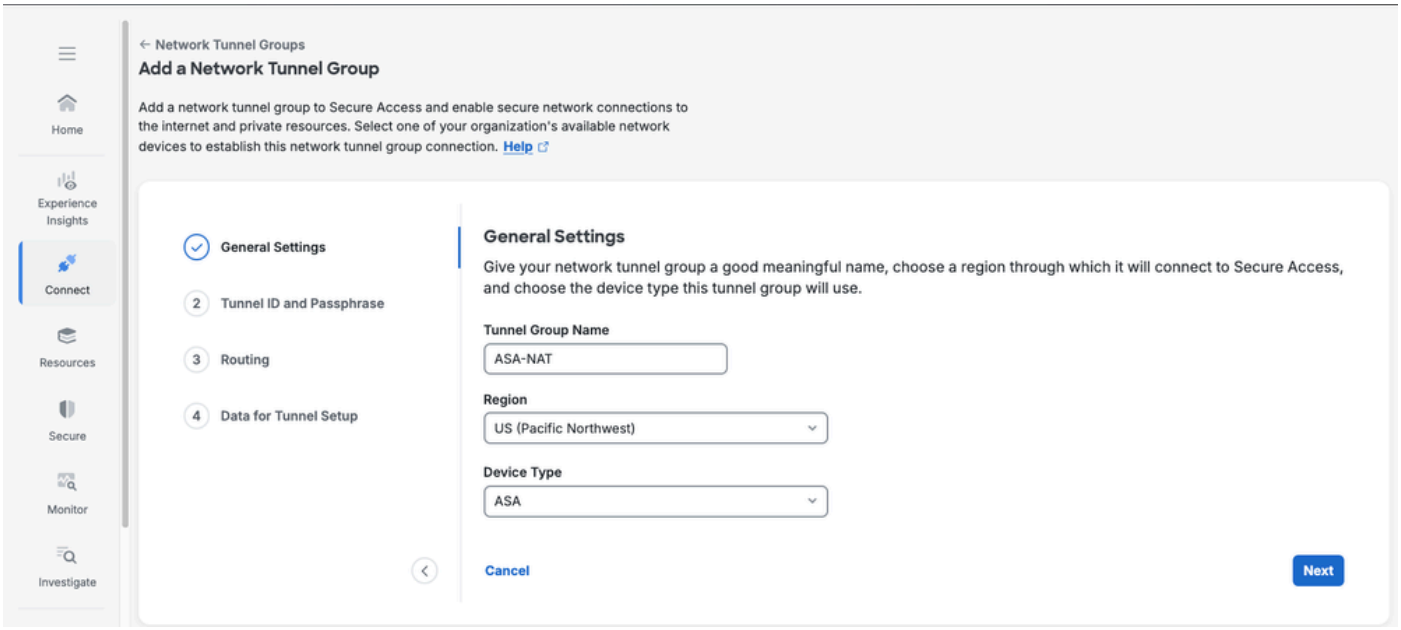
+Toevoegen om de Netwerktunnelgroep te configureren



Veilige toegang - Netwerktunnelgroepen

3. Network Tunnel Group configureren - Algemene instellingen

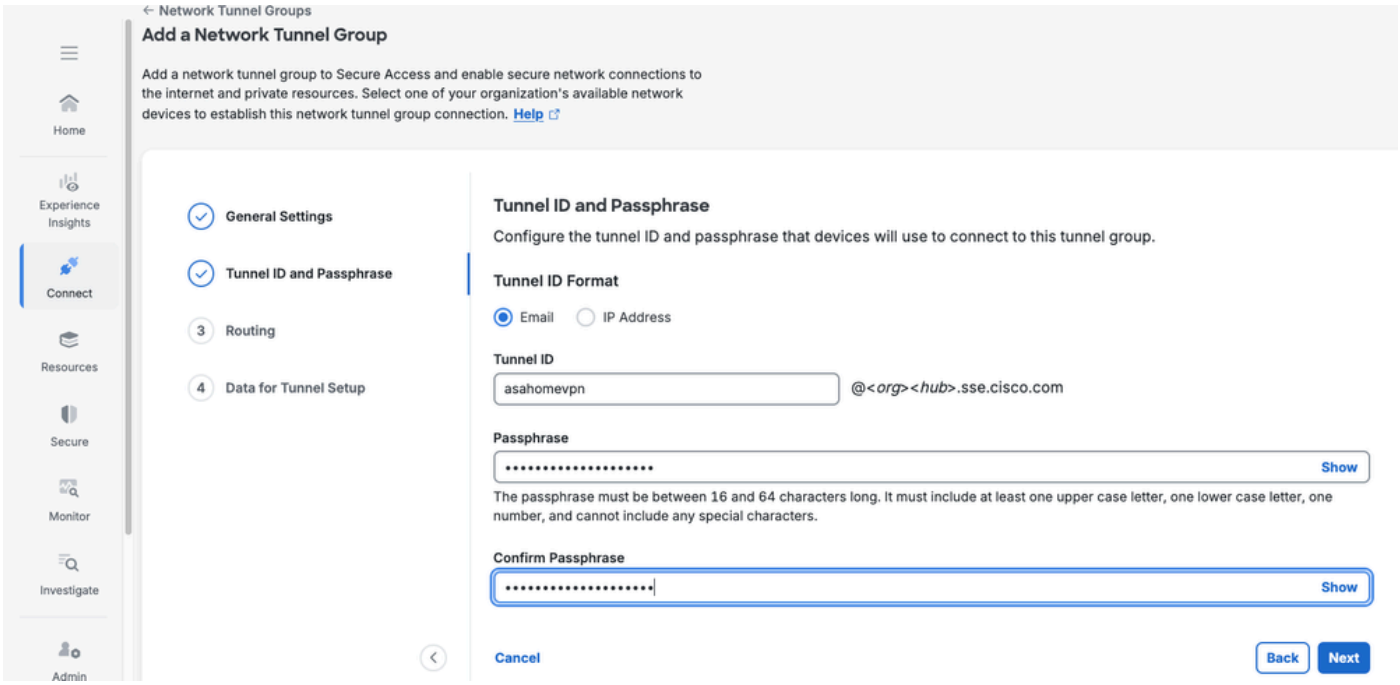
- Naam, regio en apparaattype van tunnelgroep configureren
- Klik op Volgende



Veilige toegang - Algemene instellingen voor netwerktunnelgroepen

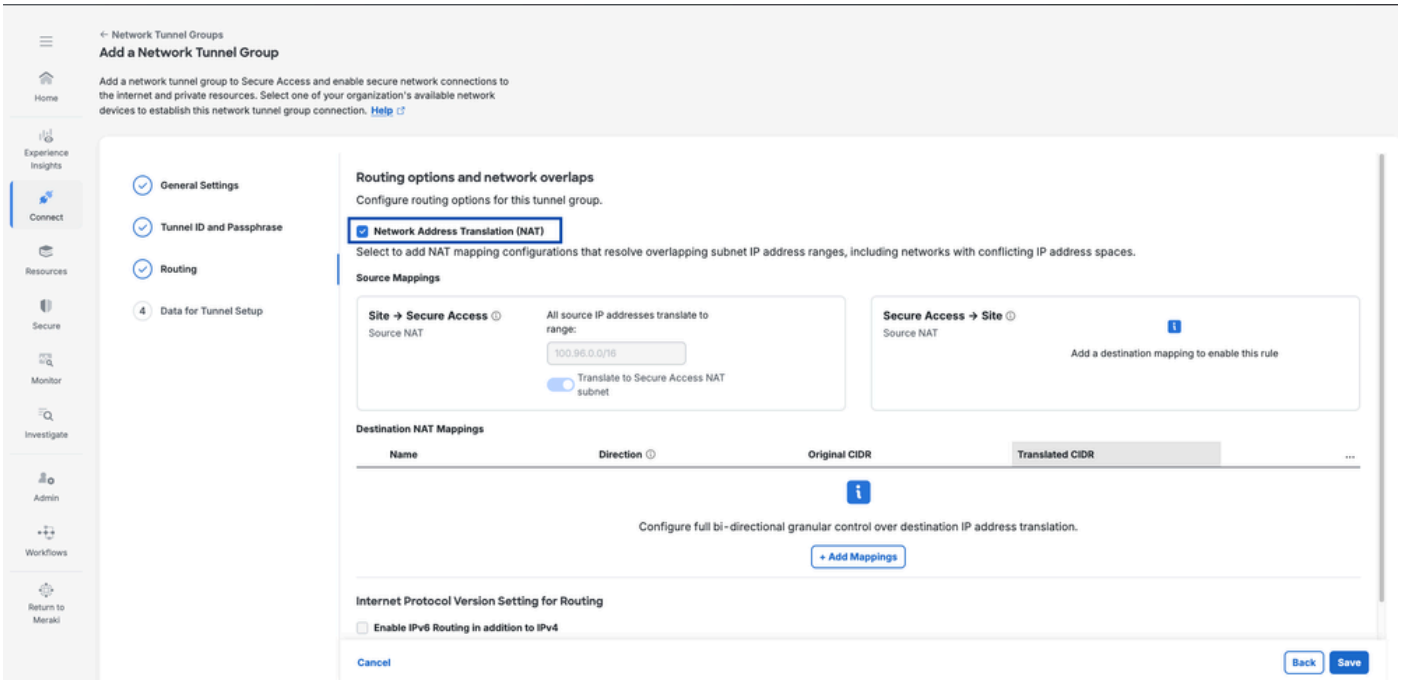
4. Configureer Tunnel ID en wachtwoordgroep.

- Configureer de tunnel-ID en wachtwoordgroep.
- Klik op Volgende



Veilige toegang - Netwerktunnelgroepen

5. Network Address Translation (NAT) inschakelen

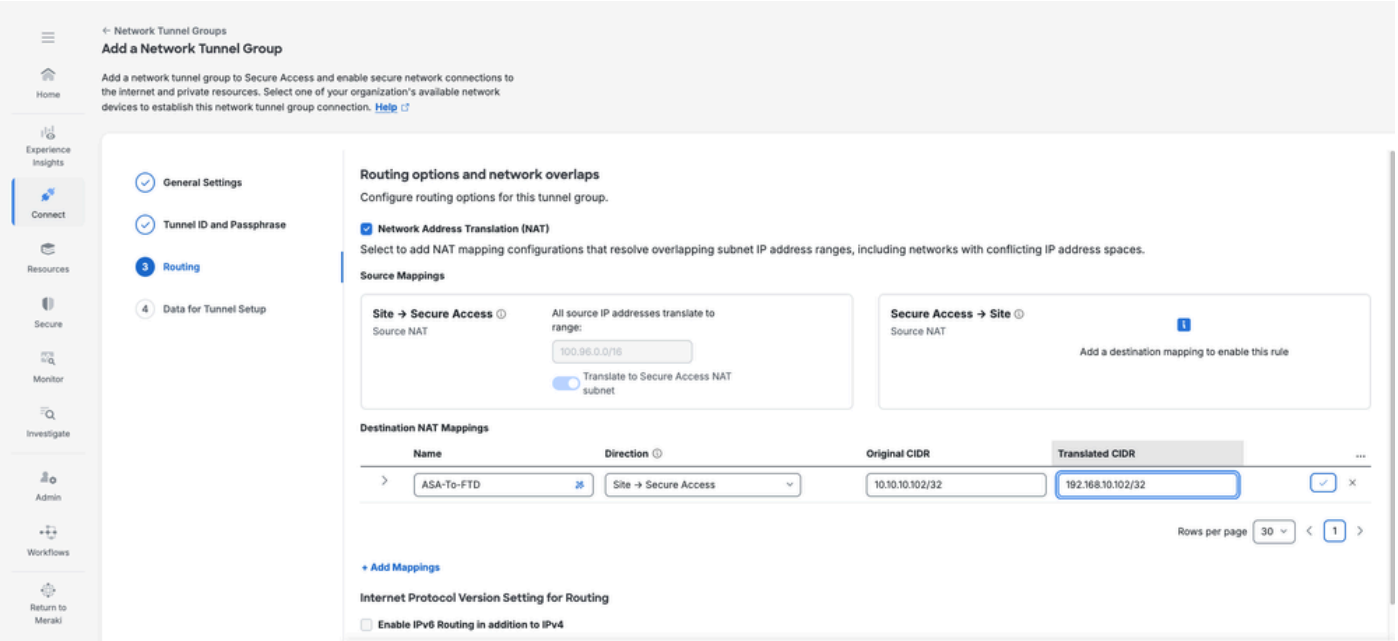


Veilige toegang - NAT-instellingen voor netwerktunnelgroepen

6. Toevoeging van NAT-toewijzing van bestemming toevoegen

Flow 1 - Router 1 naar Router 2 (Site to Secure Access)

Flow 2 - Router 2 naar Router 1 (beveiligde toegang tot de site)

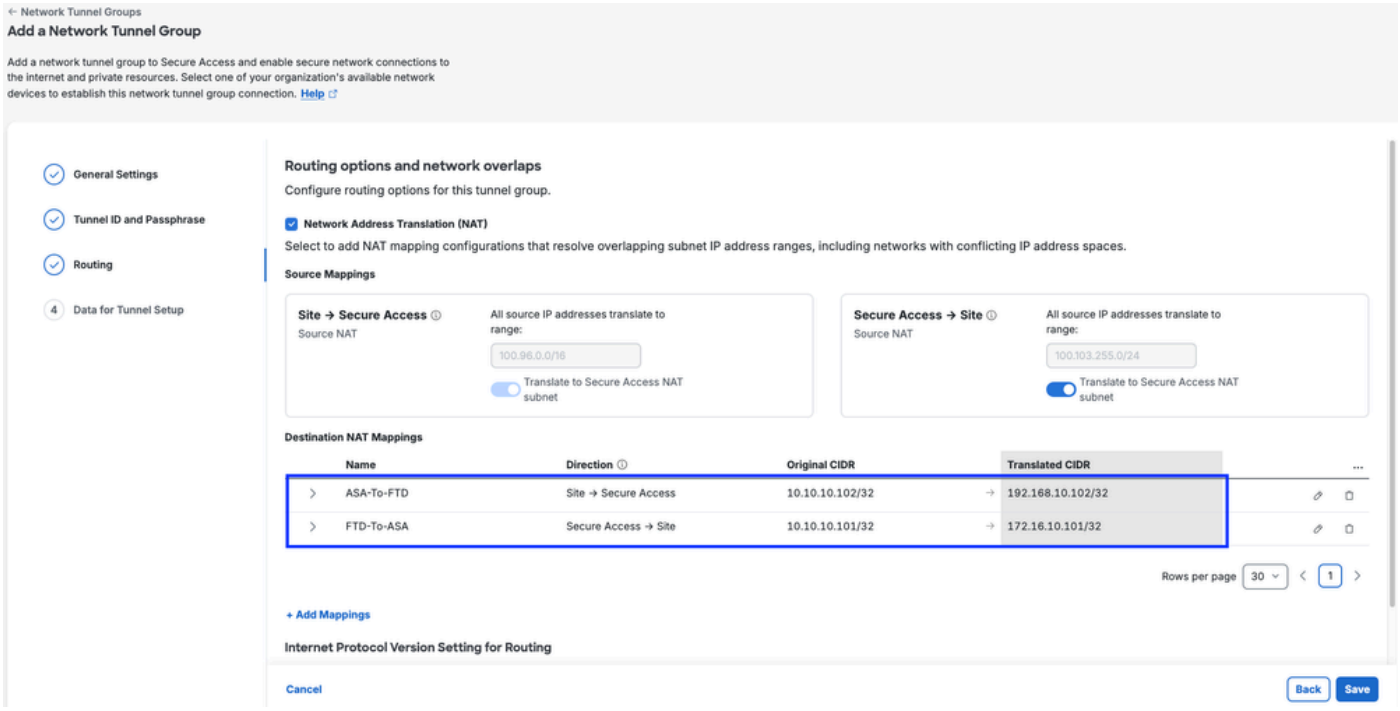


Veilige toegang - NAT-instellingen voor netwerktunnelgroepen

⚠ Let op: Wanneer NAT is ingeschakeld, is BGP niet mogelijk. Configureer ook statische VPN op Customer Edge-apparaten

---

🔍 Tip: vergeet nooit een vertaalde IP te pingen.
Vertaalde IP gaat in Vertaalde CIDR en echte IP gaat in Originele CIDR.



Veilige toegang - NAT-instellingen voor netwerktunnelgroepen

Klik op opslaan

Tip: Voor verkeer dat van 'Site A' naar 'Site B' gaat, is vanuit CNHE-1-oogpunt de richting 'Site-> SecureAccess'

Voor verkeer dat van 'site B' naar 'site A' gaat, is vanuit het oogpunt van CNHE-1 de richting 'SecureAccess -> Site'

VPN-configuratie op ASA

1. Meld u aan bij ASA CLI, voer de activeringsmodus in en controleer de basis-IP-connectiviteit met internet

ASA# schip
Systeem-IP-adressen:
Interface Naam IP adres Subnet masker Methode
Gigabit Ethernet0/0 buiten 192.168.1.40 255.255.255.0 handleiding
Gigabit Ethernet0/1 inside 10.10.10.1 255.255.255.0 handleiding

Huidige IP-adressen:
Interface Naam IP adres Subnet masker Methode
Gigabit Ethernet0/0 buiten 192.168.1.40 255.255.255.0 handleiding

Gigabit Ethernet0/1 inside 10.10.10.1 255.255.255.0 handleiding

ASA# ping 8.8.8.8
Typ escape sequence om af te breken.
De time-out is 2 seconden bij het verzenden van 5, 100-byte ICMP Echo's naar 8.8.8.8:
Ja!!!!
Succespercentage is 100 procent (5/5), retourvlucht min/avg/max = 20/28/30 ms
ASA#

2. IKEv2-beleid configureren en IKEv2 inschakelen op de externe interface

Crypto IKEV2-beleid 10
Codering AES-GCM-256
integriteit null
Groep 19
Levensduur seconden 86400
Crypto IKEV2 inschakelen buiten

3. IPSec-voorstel configureren

crypto ipsec ikev2 ipsec-proposal Ipsec-Proposal-primary
Protocol ESP-codering AES-GCM-256

4. IPsec-profiel configureren

Crypto IPSEC-profiel CSA-profiel-primair
set ikev2 ipsec-proposal Ipsec-Proposal-primary
IKEV2 Local-Identity Email-ID <Primary Tunnel-ID> instellen

5. Configureer groepsbeleid en schakel het IKEv2-protocol in onder attribuut.

Groepsbeleid-CSA-beleid-Primair intern
Groepsbeleid-CSA-beleid-primaire kenmerken
VPN-tunnel-protocol IKEV2

6. Tunnelgroep configureren.

tunnelgroep 44.228.138.150 type IPSec-L2L
tunnelgroep 44.228.138.150 algemene kenmerken
default-group-policy-csa-policy-primary

Tunnel-Group 44.228.138.150 IPSec-attributen
IKEV2-verificatie op afstand, vooraf gedeelde sleutel <pre-shared-key>
IKEV2 Local-Authentication Pre-Shared-Key <Pre-Shared-Key>

7. Virtual Tunnel Interface (VTI) configureren

- Naamgeving kan zijn als uw keuze
- Het IP-adres dat aan VTI is toegewezen, mag niet overlappen met een andere interface op de ASA
- De tunnelbron moet de buiteninterface van de firewall zijn
- De bestemming van de tunnel moet het IP-adres van het datacenter zijn

Tunnel-interface1
naam VTI-1
IP-adres 169.254.2.1 255.255.255.252
tunnelbroninterface buiten
Tunnelbestemming 44.228.138.150
tunnelmodus ipsec ipv4
Tunnel Protection IPSec Profile CSA-Profile-Primary

8. Configureer de routering zodanig dat het verkeer naar het toegewezen IP-adres of subnet binnen de VTI-interface wordt gerouteerd. De volgende hop moet worden uitgevoerd via IP binnen het bereik van VTI.

route VTI-1 0.0.0.0.0.0.0.0 169.254.2.2 5. (voor internetgebaseerd, RAVPN-pool- of CGNAT-verkeer

of

Route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

op beleid gebaseerde routering

1. Toegangslijst

toegangslijst PBR verlengde vergunning ip 10.10.10.0 255.255.255.0 elke

2. Routekaart

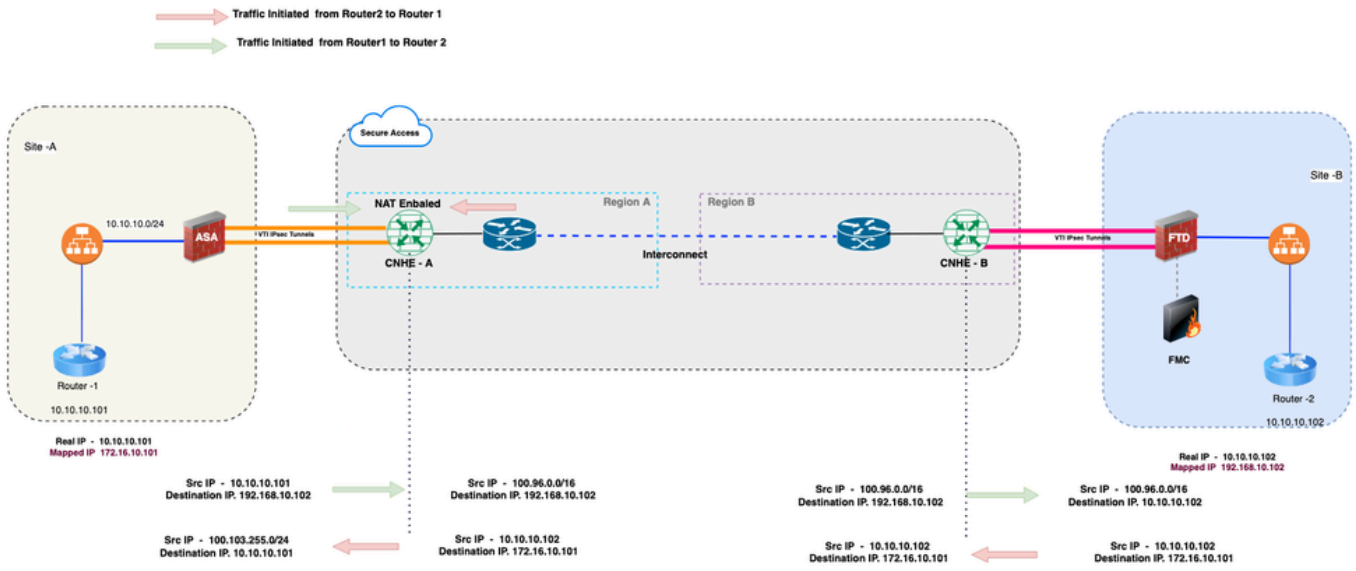
routekaart RM-CSA-vergunning 10

overeenkomend IP-adres PBR
SET IP NEXT-HOP 169.254.2.2 169.254.2.6

3. Routekaart toepassen op de ingangsinterface

Gigabit Ethernet-interface0/1
Naam binnen
veiligheidsniveau 100
IP-adres 10.10.10.1 255.255.255.0
policy-route-map RM-CSA

Verifiëren



Routerinterface en GW-bereikbaarheidsstatus

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.101   YES NVRAM  down                  down
GigabitEthernet2       10.10.10.101    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet9       unassigned      YES unset  administratively down down
Router1#ping  10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Test 1- Router2 --> Router1. - Ping-test

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

Packet capture op ASA (lokaal FW)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

   1: 10:56:45.024244       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.231143       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232470       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441856       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443122       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652477       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653423       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875397       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876450       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082301       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 10:56:45.024458       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.230914       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232516       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441795       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443153       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652432       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653454       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875351       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876480       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082240       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

Packet Capture op FTD (externe FW)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

10 packets captured

   1: 16:06:41.122292       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124856       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.329557       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330442       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546327       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547106       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752036       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752814       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.967891       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968501       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:06:41.123299       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124825       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.330000       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330396       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546800       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547090       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752448       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752783       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.968242       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968486       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
```

Test 2. - Router 2 ---> Router 1 ping test

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.10.10.102    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

FTD Packet Capture (lokaal FW)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

   1: 16:11:45.622450       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823825       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825762       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045667       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046857       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252321       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253572       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453803       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454764       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664119       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:11:45.622083       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823886       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825442       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045697       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046582       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252352       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253313       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453849       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454596       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664150       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
```

ASA packet capture (Remote FW)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

   1: 11:08:30.288391       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289123       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504566       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.504963       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710992       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711404       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917112       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917402       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128243       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128640       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 11:08:30.287964       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289322       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504505       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.505009       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710961       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711434       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917066       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917417       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128197       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128685       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```

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.