Configureer AnyConnect met Access Server via IPSec-tunnel.

Inhoud

Inleiding:

In dit document worden de procedures beschreven voor het opzetten van een RAVPN-installatie op de FTD die wordt beheerd door het FMC en een site-to-site-tunnel tussen FTD's.

Voorwaarden:

Basisvereisten

- Een fundamenteel begrip van plaats-aan-plaats VPNs en RAVPN is voordelig.
- Het is van essentieel belang dat u inzicht hebt in de grondbeginselen van het configureren van een IKEv2-beleidstunnel op basis van Cisco Firepower-platform.

Deze procedure betreft de implementatie van een RAVPN-installatie op de FTD die wordt beheerd door het FMC en een site-to-site tunnel tussen FTD's waar AnyConnect-gebruikers toegang kunnen krijgen tot de server achter de andere FTD-peer.

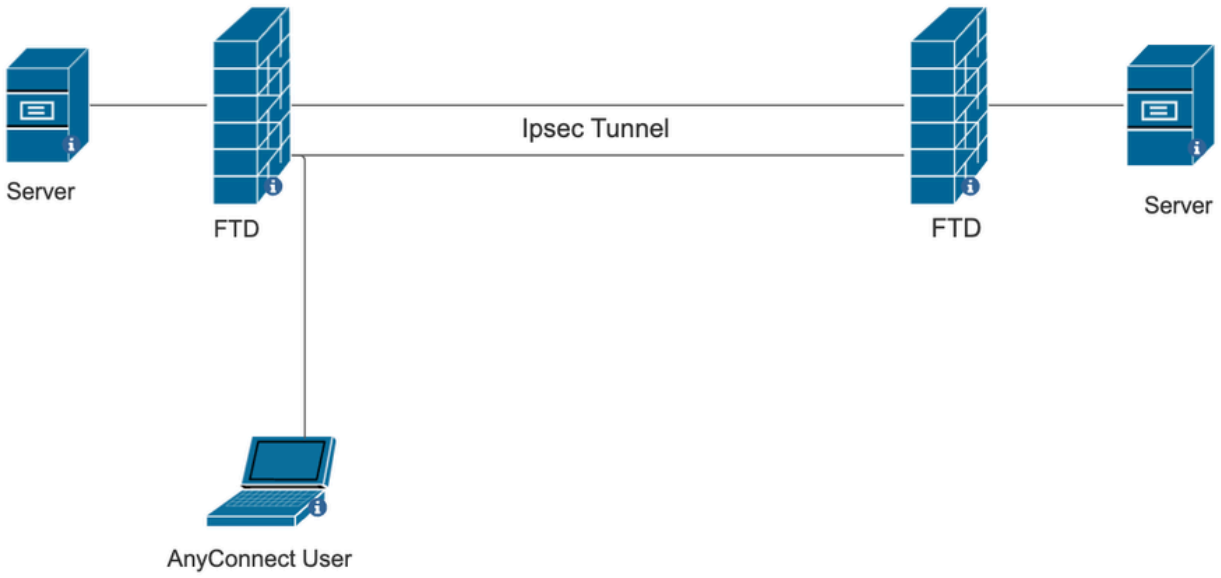
Gebruikte componenten

- Cisco Firepower Threat Defence voor VMware: versie 7.0.0
- Firepower Management Center: 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, zorg er dan voor dat u de potentiële

impact van elke opdracht begrijpt..

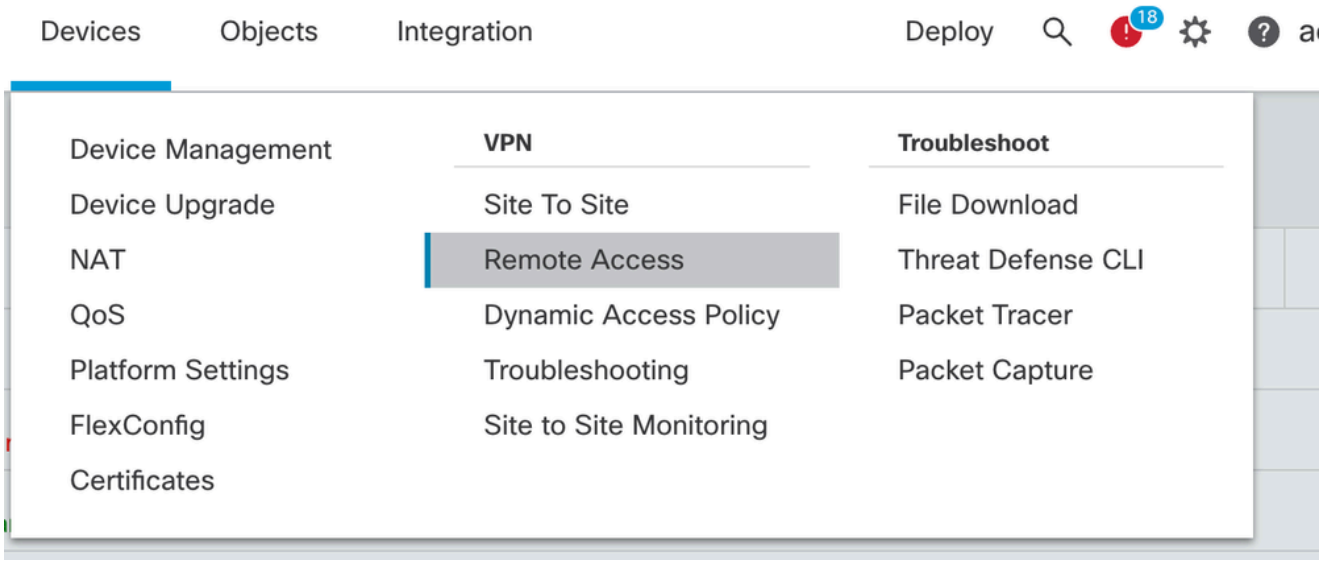
Netwerkdiagram



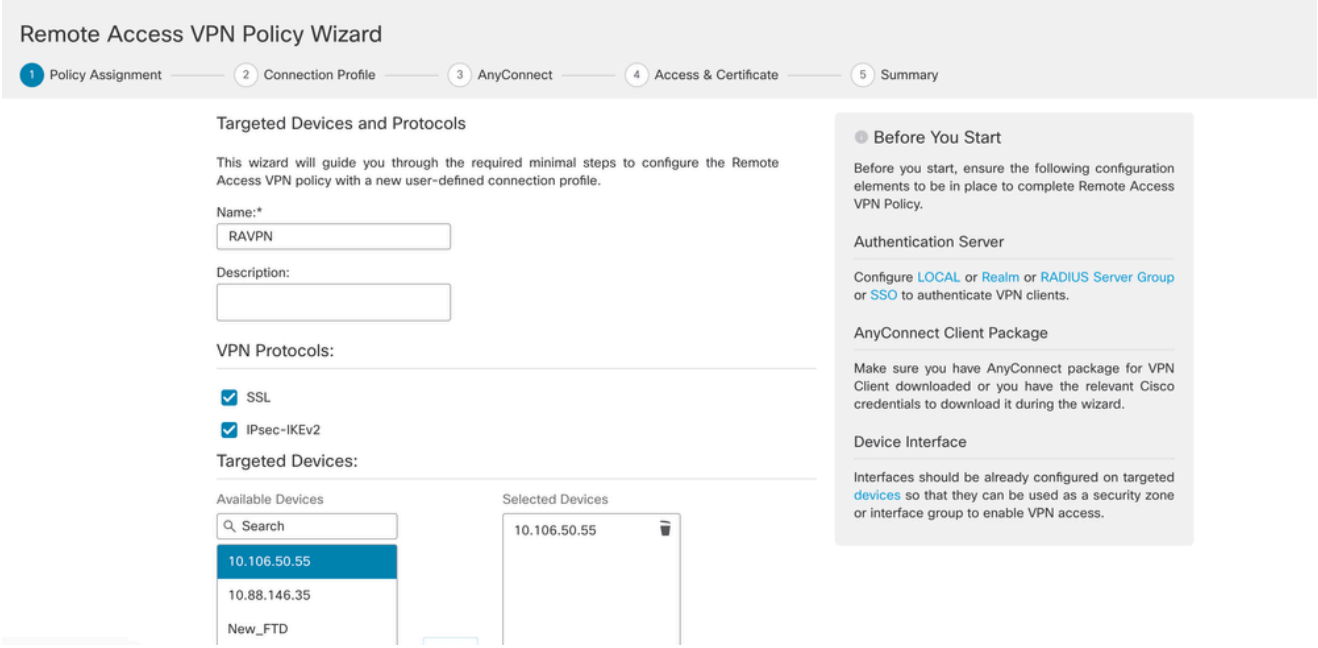
Configuraties op VCC

RAVPN-configuratie op de FTD die wordt beheerd door het VCC.

1. Navigeer naar Apparaten > Externe toegang.

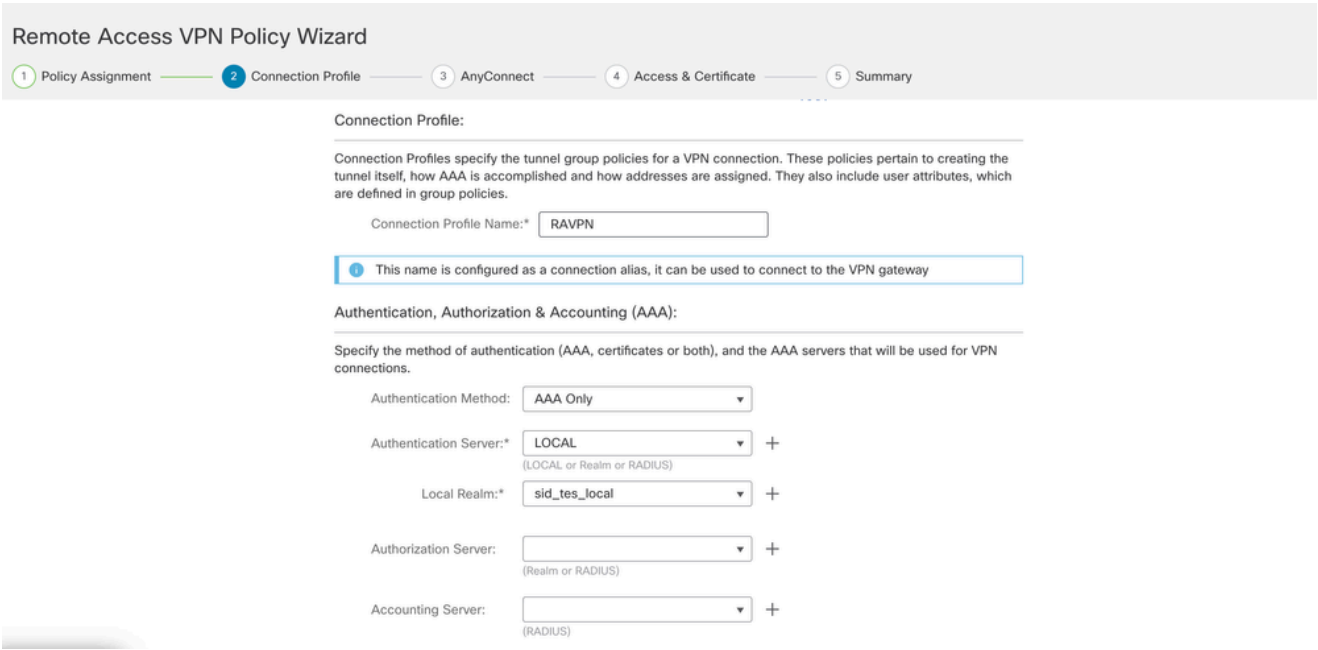


2. Klik op Add (Toevoegen).
3. Configureer een naam, selecteer de FTD uit de beschikbare apparaten en klik op Volgende.

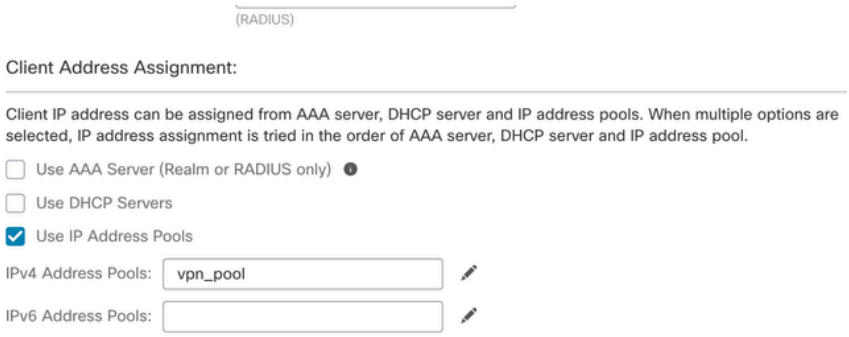


4. Configureer een naam voor het verbindingsprofiel en kies de verificatiemethode.

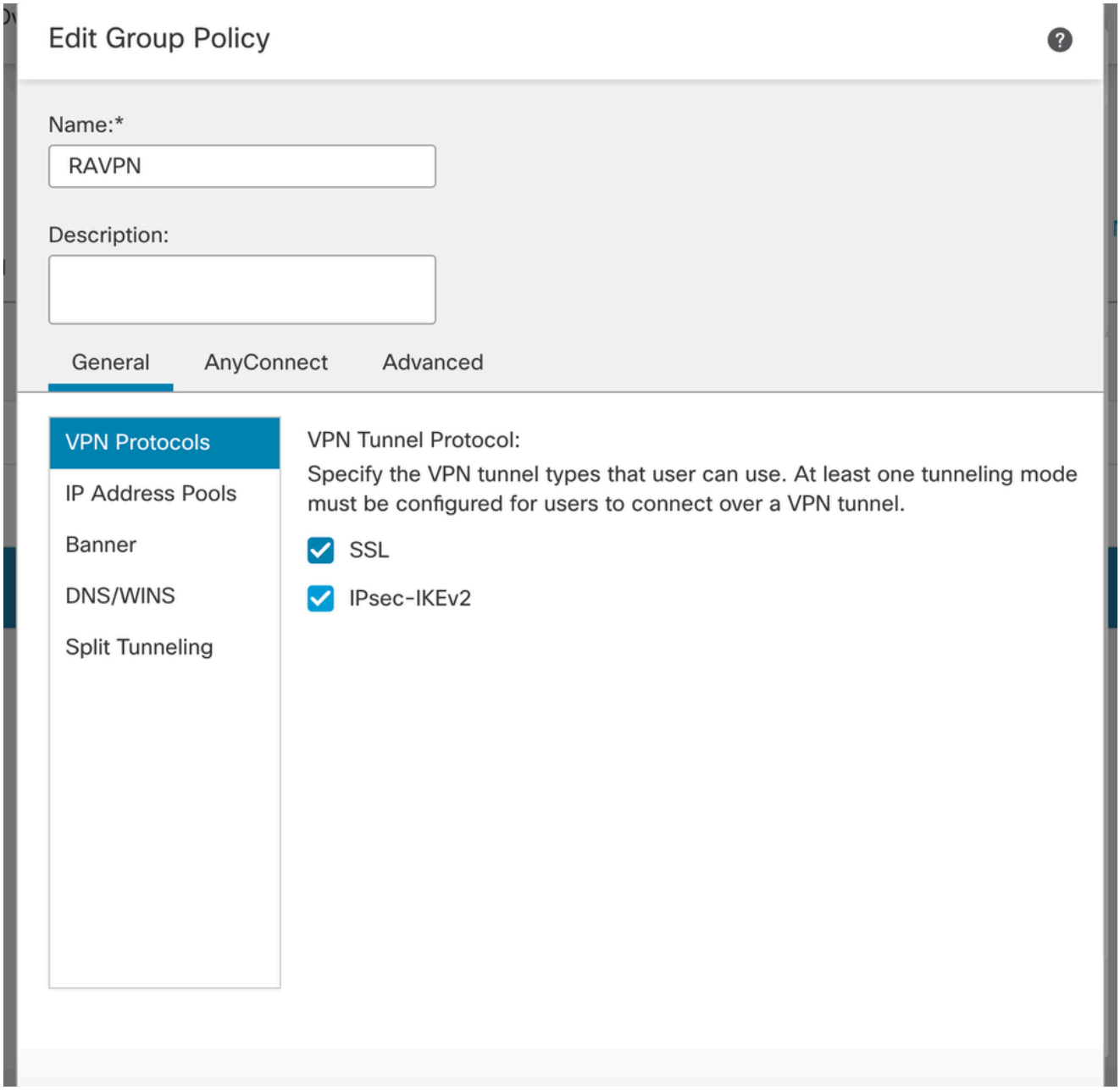
   OPMERKING: voor deze configuratievoorbeeld gebruiken we alleen AAA en lokale verificatie. Configureer echter op basis van uw vereisten.



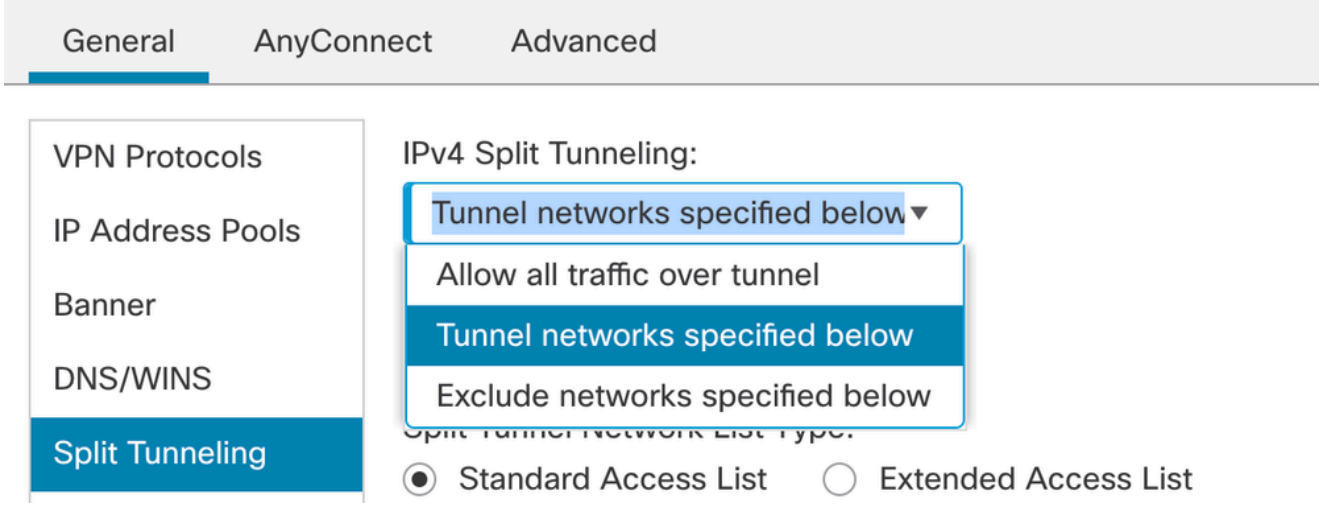
5. Configureer de VPN-pool die wordt gebruikt voor de IP-adrestoewijzing voor AnyConnect.



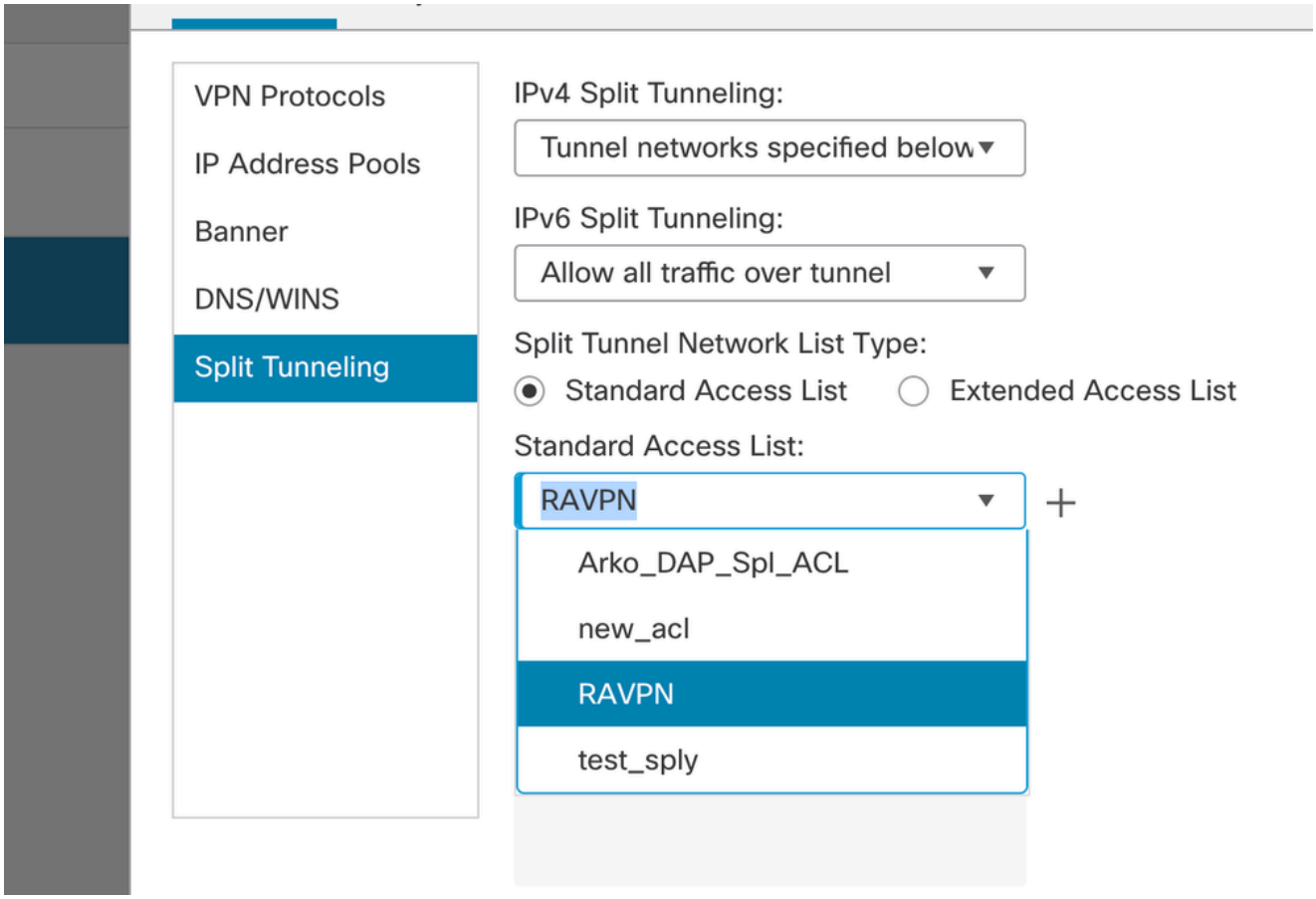
6. Groepsbeleid maken. Klik op + om een groepsbeleid te maken. Voeg de naam van het groepsbeleid toe.



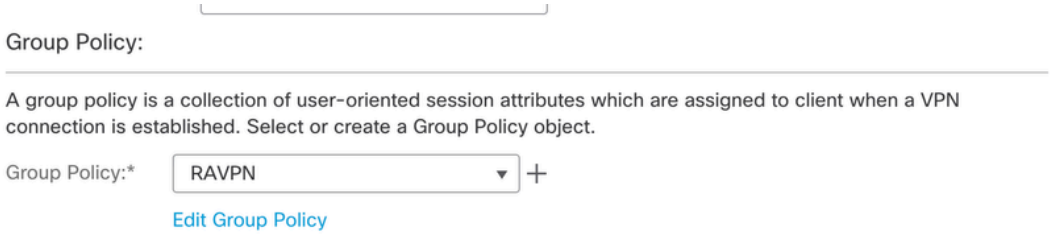
7. Ga naar Split tunneling. Selecteer de hier gespecificeerde tunnelnetwerken:



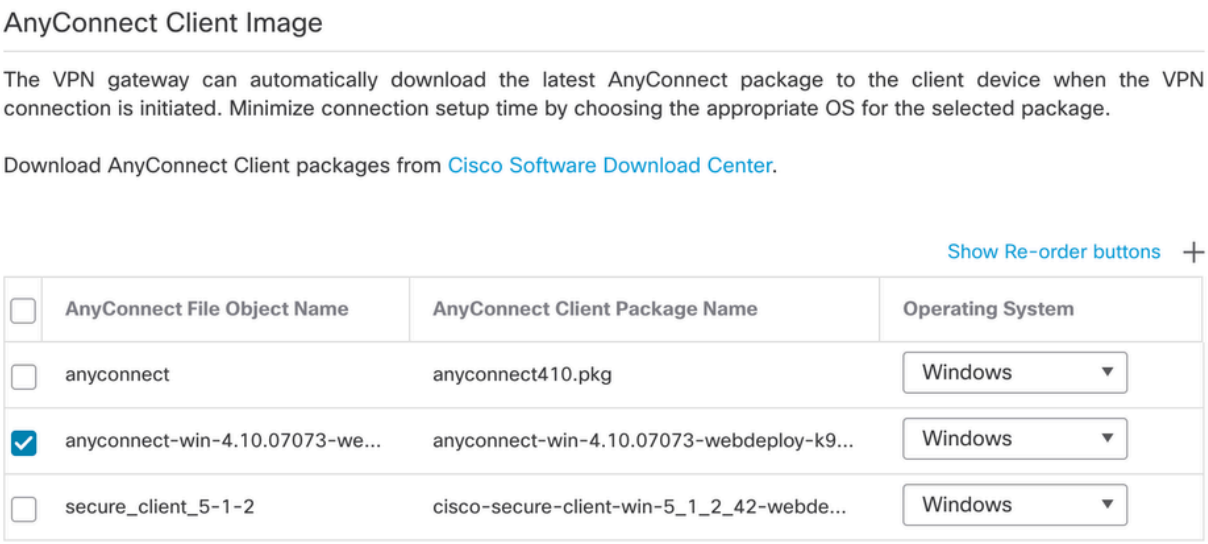
8. Selecteer de juiste toegangslijst in de vervolgkeuzelijst. Als een ACL nog niet is geconfigureerd: klik op het + pictogram om de standaardtoegangslijst toe te voegen en een nieuwe te maken.
   Klik op Save (Opslaan).



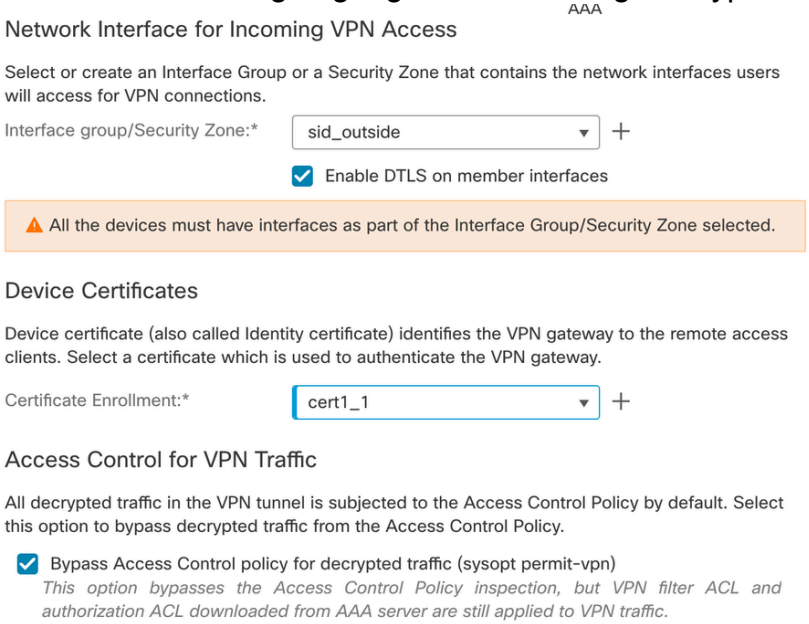
9. Selecteer het groepsbeleid dat wordt toegevoegd en klik op Volgende.



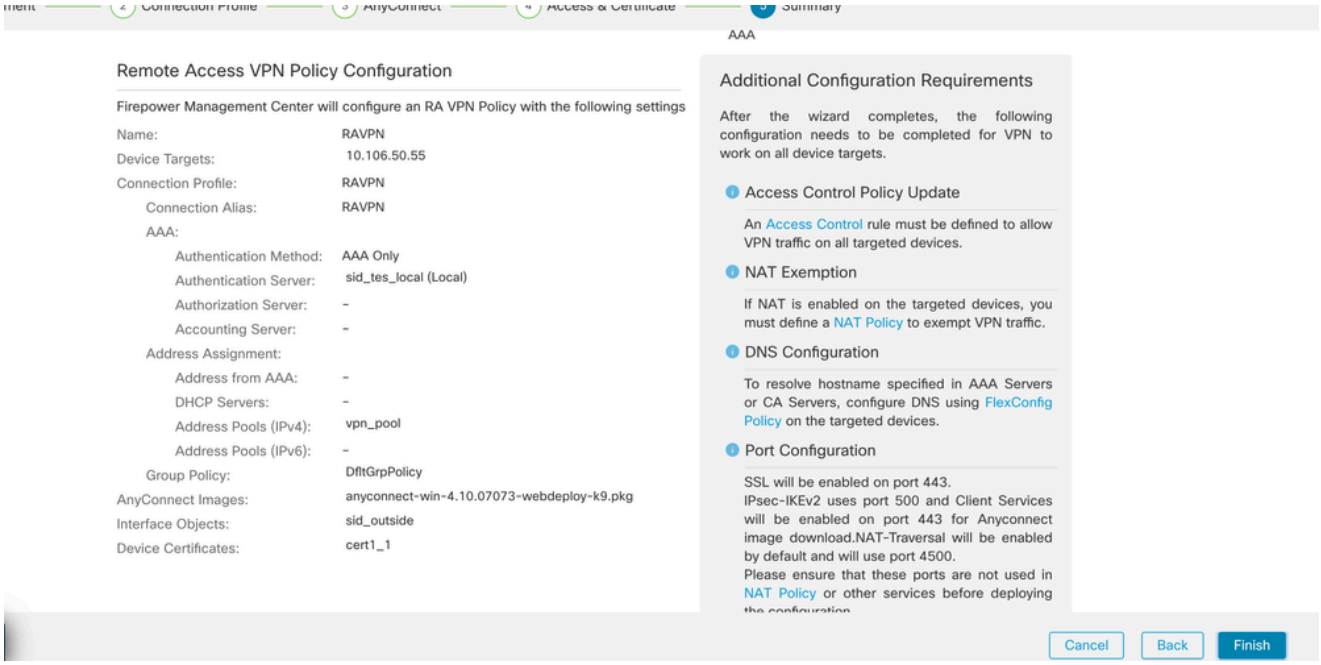
10. Selecteer de AnyConnect-afbeelding.



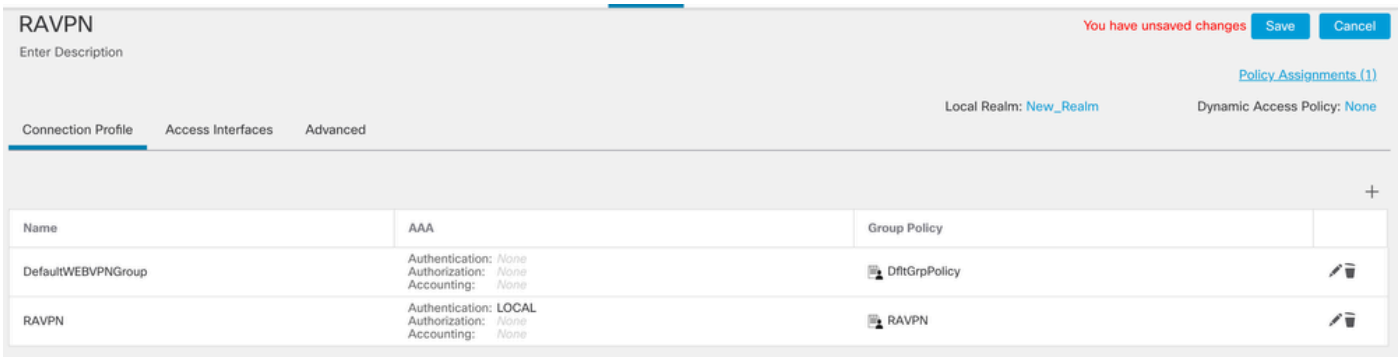
11. Selecteer de interface die moet worden ingeschakeld voor de AnyConnect-verbinding, voeg het certificaat toe, selecteer het beleid voor omzeilingtoegangscontrole voor gedecrypteerd AAA verkeer en klik op Volgende.



12. Controleer de configuratie en klik op Voltooien.

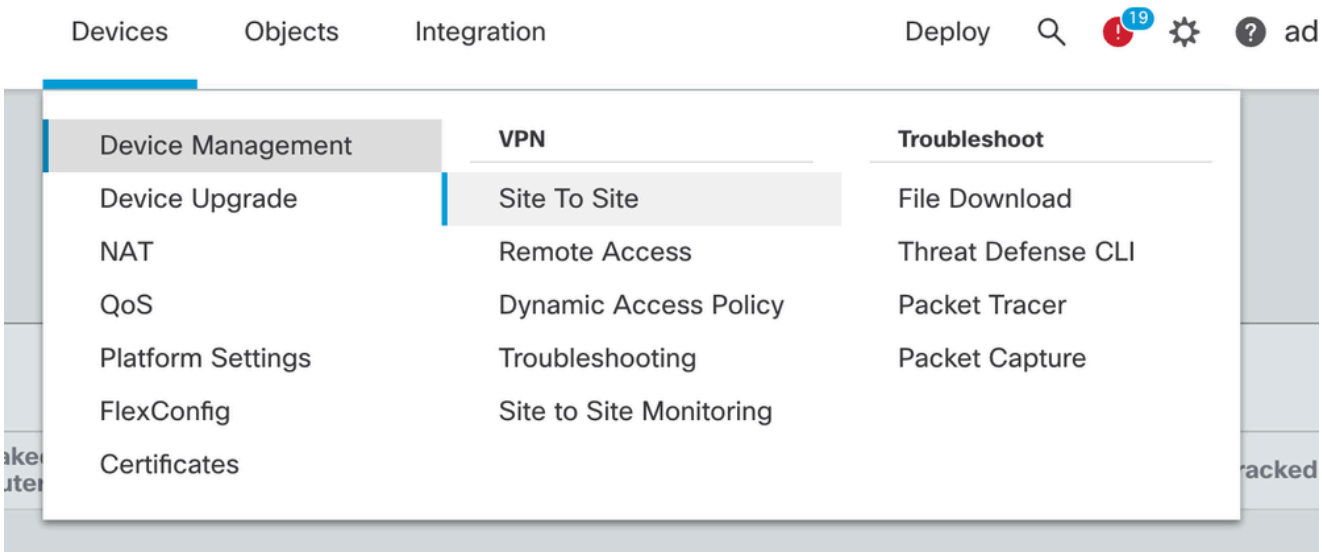


13. Klik op Opslaan en implementeren.

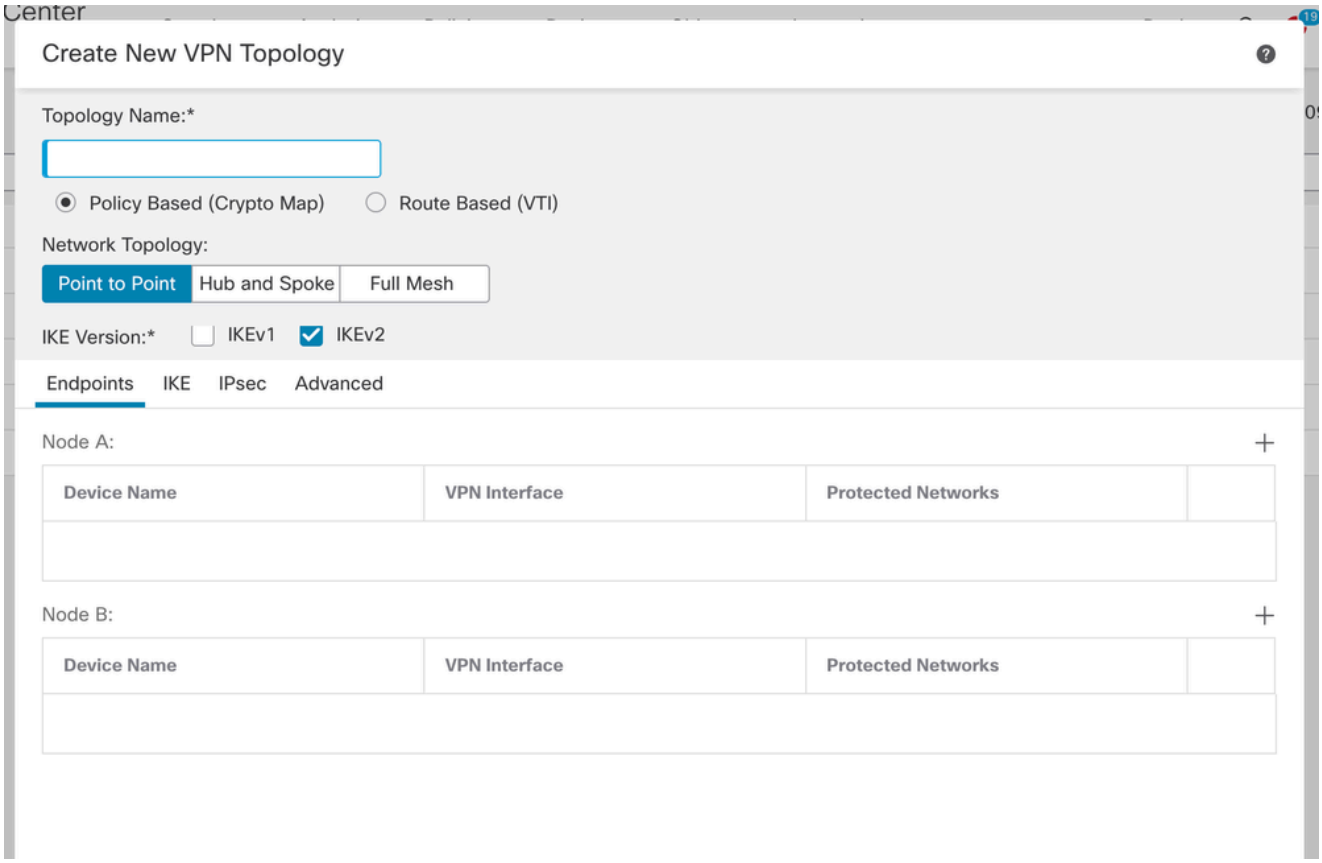


IKEv2 VPN op FTD beheerd door FMC:

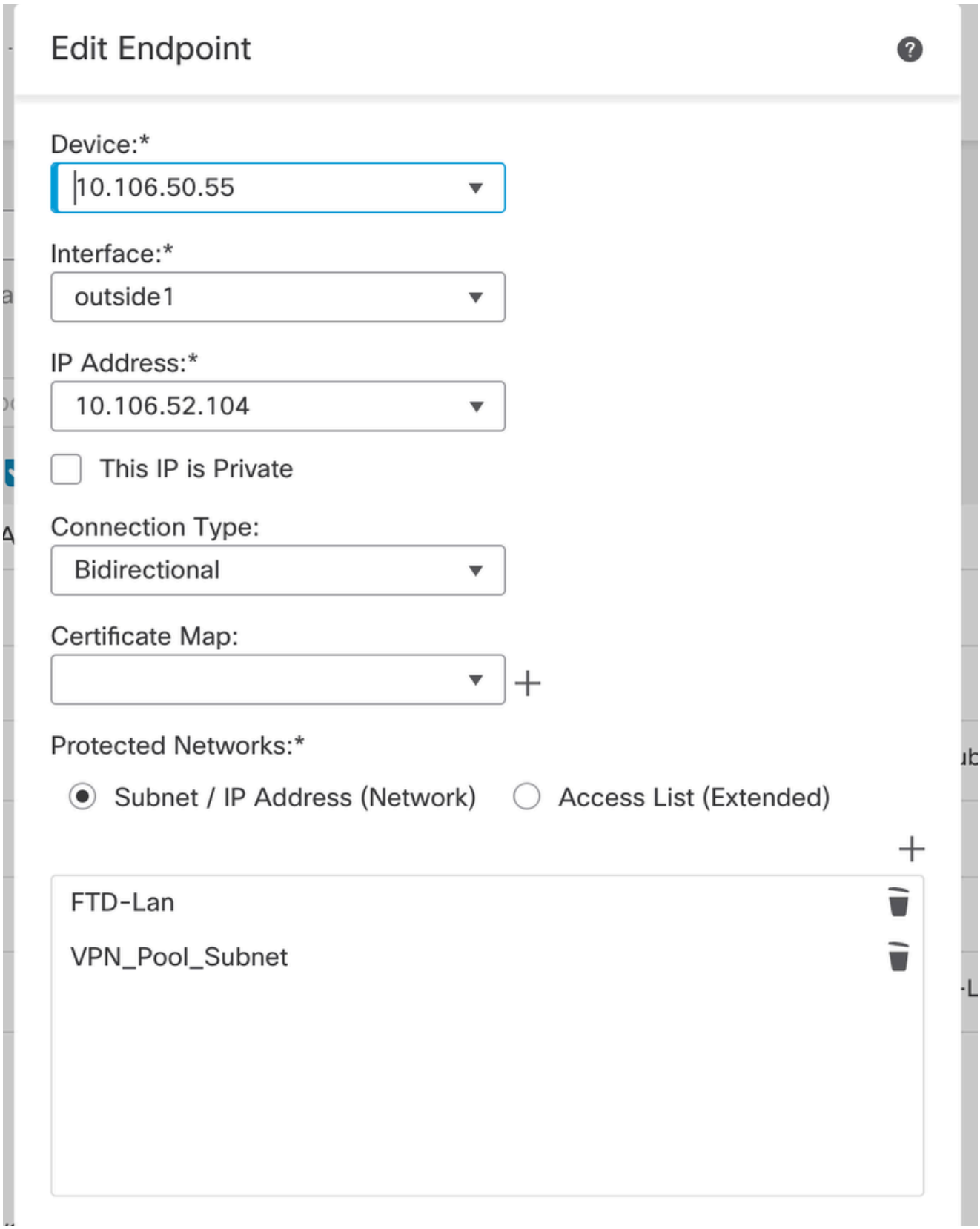
1. Ga naar Apparaten > Site to Site.



2. Klik op Add (Toevoegen).
3. Klik op + voor knooppunt A:



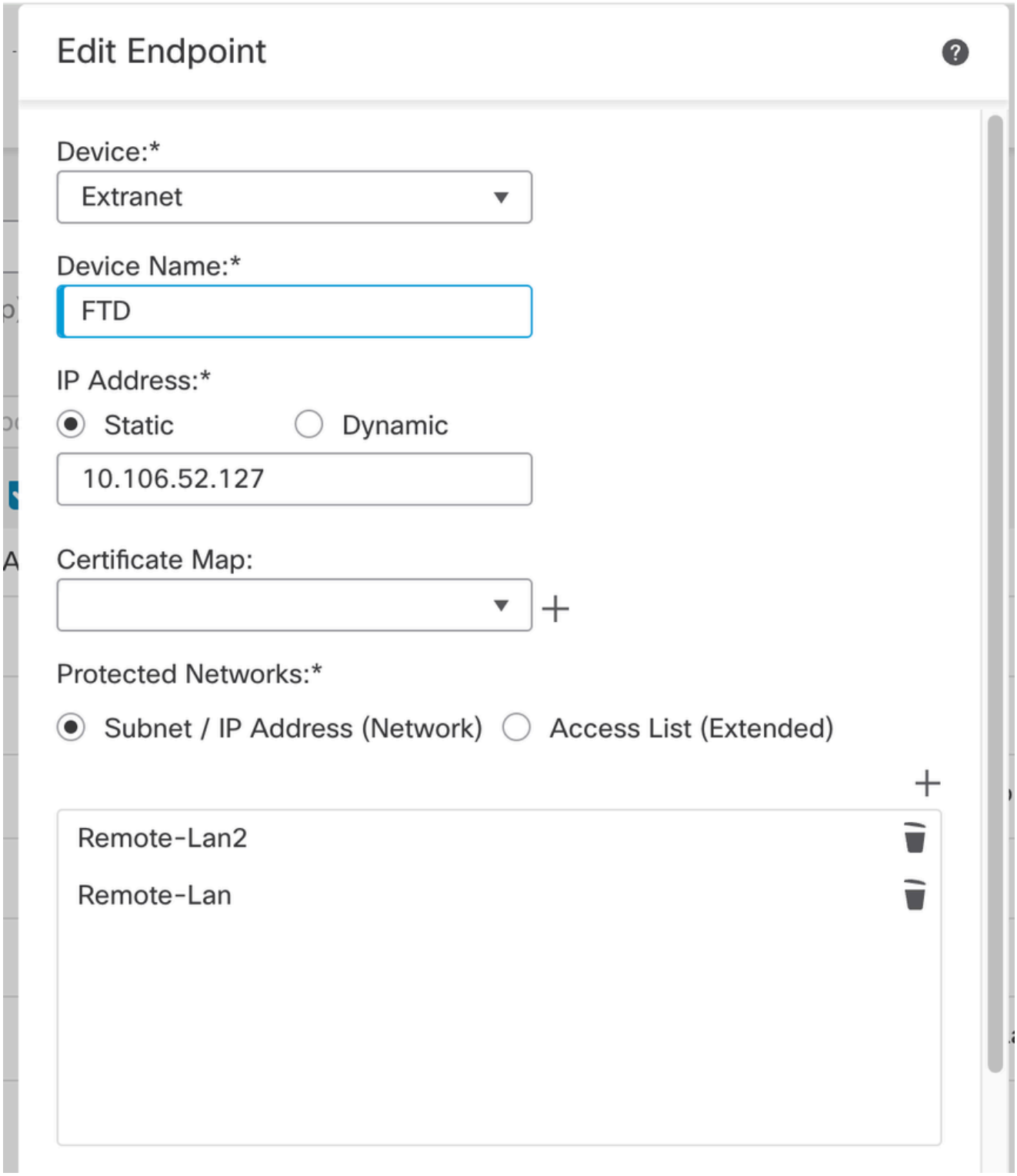
4. Selecteer de FTD in het apparaat, selecteer de interface, voeg het lokale subnetbestand toe dat versleuteld moet worden door de IPSec-tunnel (en bevat in dit geval ook de VPN-pooladressen) en klik op OK.



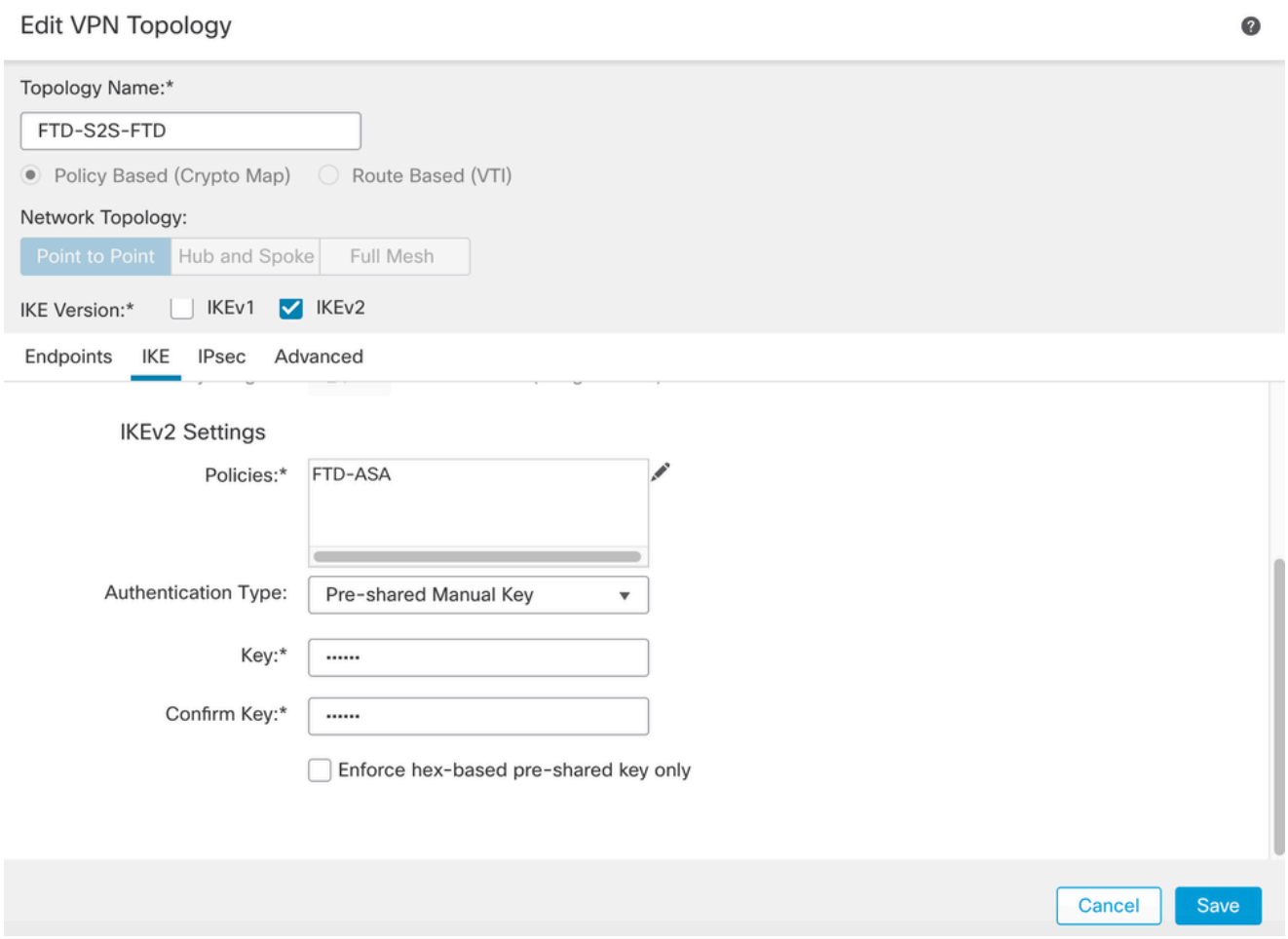
5. Klik op + voor knooppunt B:

> Selecteer het Extranet vanuit het apparaat en geef de naam van het peer-apparaat.

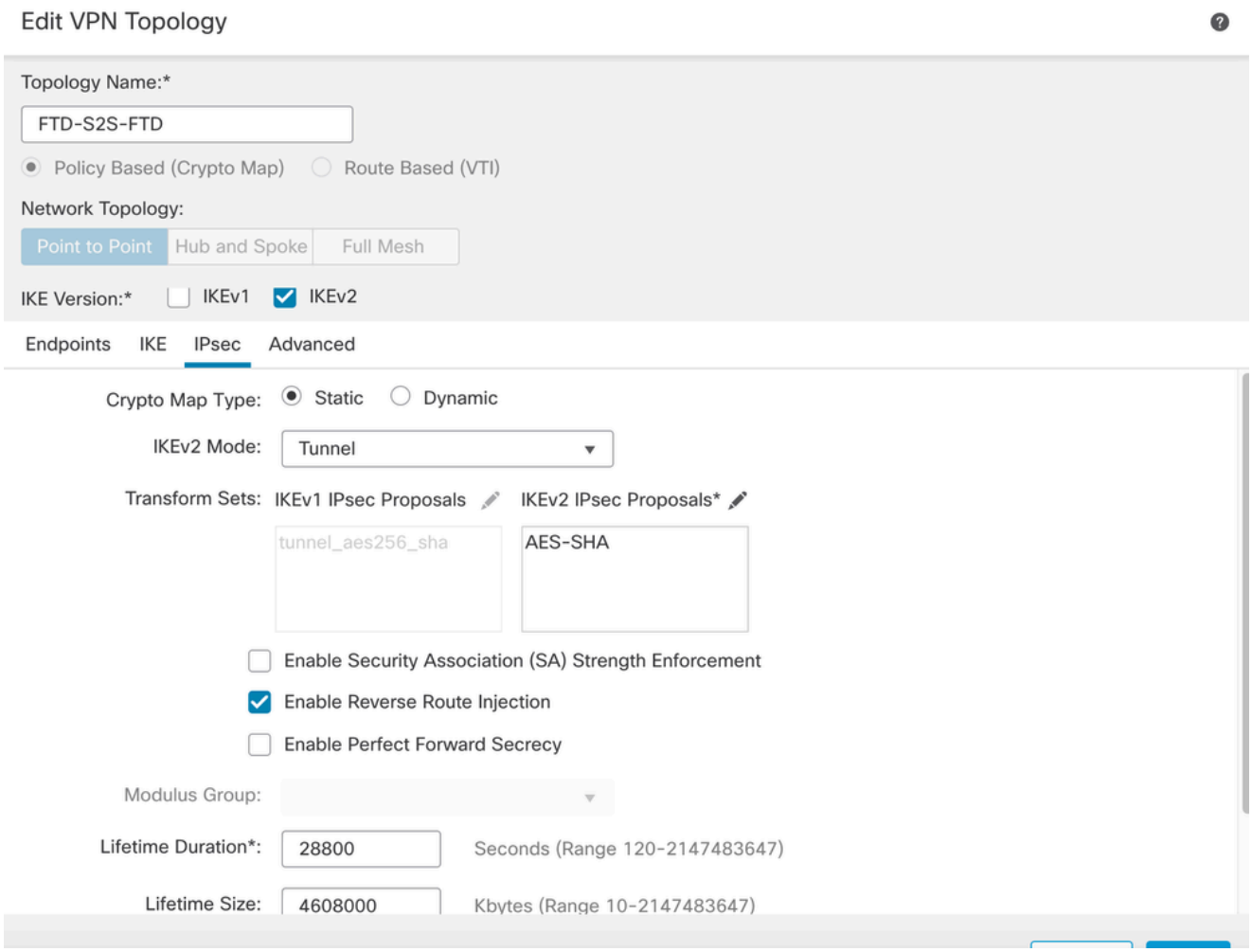
> Configureer de peer details en voeg de externe subnetverbinding toe die via de VPN-tunnel benaderd moet worden en klik op OK.



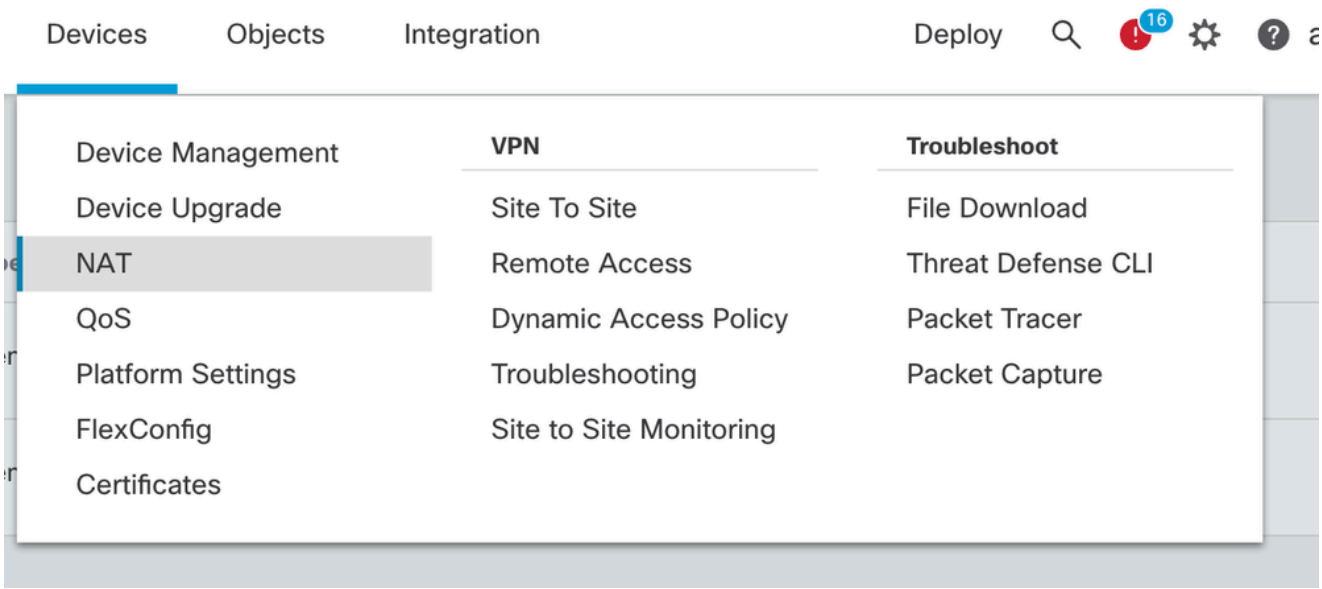
6. Klik op het tabblad IKE: Configureer de IKEv2 instellingen volgens uw vereiste



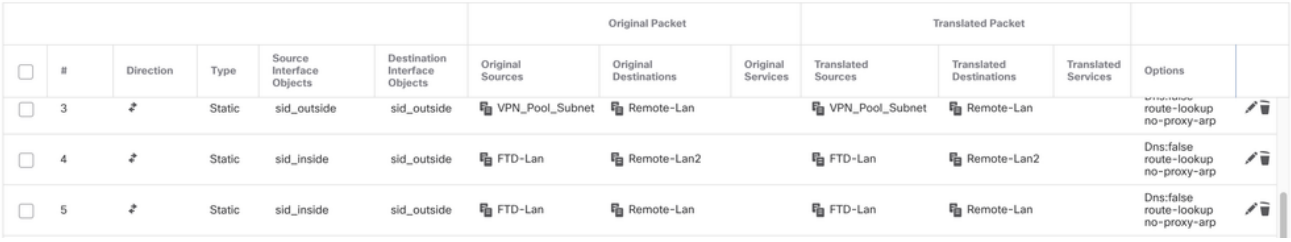
7. Klik op het tabblad IPsec: De IPSec-instellingen configureren volgens uw vereisten.



8. Configureer Nat-Exempt voor uw interessant verkeer (optioneel)
   Klik op Apparaten > NAT



9. De NAT die hier is geconfigureerd, geeft RAVPN en interne gebruikers toegang tot servers via de S2S IPSec-tunnel.



	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet: Original Sources	Original Packet: Original Destinations	Original Packet: Original Services	Translated Packet: Translated Sources	Translated Packet: Translated Destinations	Translated Packet: Translated Services	Options
☐	3	⇄	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		route-lookup no-proxy-arp
☐	4	⇄	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan2		FTD-Lan	Remote-Lan2		Dns:false route-lookup no-proxy-arp
☐	5	⇄	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan		FTD-Lan	Remote-Lan		Dns:false route-lookup no-proxy-arp

10. Op dezelfde manier doet de configuratie op het andere peer-end voor de S2S-tunnel.

    OPMERKING: De crypto ACL of de interessante subnetten moeten spiegelkopieën van elkaar zijn op beide peers.

Verifiëren

1. Controleer de VPN-verbinding als volgt:

<#root>

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : test

 Index : 5869

Assigned IP : 2.2.2.1 Public IP : 10.106.50.179

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

Bytes Tx : 15470 Bytes Rx : 2147

Group Policy : RAVPN Tunnel Group : RAVPN

Login Time : 03:04:27 UTC Fri Jun 28 2024

Duration : 0h:14m:08s

Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a3468016ed000667e283b
Security Grp : none Tunnel Zone : 0
```

2. Controleer de IKEv2-verbinding als volgt:

<#root>

```
firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:2443, Status:UP-ACTIVE

, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555
10.106.52.104/500 10.106.52.127/500 READY INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/259 sec

Child sa: local selector 2.2.2.0/0 - 2.2.2.255/65535

remote selector 10.106.54.0/0 - 10.106.54.255/65535

ESP spi in/out: 0x4588dc5b/0x284a685
```

3. De IPsec-verbinding controleren:

<#root>

```
firepower# show crypto ipsec sa peer 10.106.52.127
peer address: 10.106.52.127
Crypto map tag: CSM_outside1_map

,
seq num: 2, local addr: 10.106.52.104

access-list CSM_IPSEC_ACL_1 extended permit ip 2.2.2.0 255.255.255.0 10.106.54.0 255.255.255.0
local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.106.54.0/255.255.255.0/0/0)
```

current_peer: 10.106.52.127

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 3, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.106.52.104/500, remote crypto endpt.: 10.106.52.127/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 0284A685
current inbound spi : 4588DC5B

i

nbound esp sas:

spi: 0x4588DC5B (1166597211)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map
sa timing: remaining key lifetime (kB/sec): (3962879/28734)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000000F

outbound esp sas:

spi: 0x0284A685 (42247813)

SA State: active

```
transform: esp-aes-256 esp-sha-512-hmac no compression


in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map
sa timing: remaining key lifetime (kB/sec): (4285439/28734)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Problemen oplossen

1. Als u problemen wilt oplossen bij het AnyConnect-verbindingsprobleem, verzamelt u dartbundels of schakelt u de debuggen van AnyConnect in.
2. Om problemen op te lossen in de IKEv2-tunnel, gebruikt u deze debugs:

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. Om het probleem met verkeer op de FTD op te lossen, neemt u pakketopname en controleert u de configuratie.

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.