Konfigurieren von AnyConnect für den Zugriffsserver über den IPSec-Tunnel

Inhalt

Einführung:

In diesem Dokument werden die Verfahren für die Bereitstellung einer RAVPN-Konfiguration auf dem vom FMC verwalteten FTD sowie ein Site-to-Site-Tunnel zwischen FTDs beschrieben.

Voraussetzungen:

Grundlegende Anforderungen

- Ein grundlegendes Verständnis von Site-to-Site-VPNs und RAVPNs ist von Vorteil.
- Grundlegende Informationen zur Konfiguration eines richtlinienbasierten IKEv2-Tunnels auf der Cisco FirePOWER-Plattform sind wichtig.

Dieses Verfahren dient zur Bereitstellung einer RAVPN-Konfiguration auf dem vom FMC verwalteten FTD sowie eines Site-to-Site-Tunnels zwischen FTDs, über den AnyConnect-Benutzer auf den Server hinter dem anderen FTD-Peer zugreifen können.

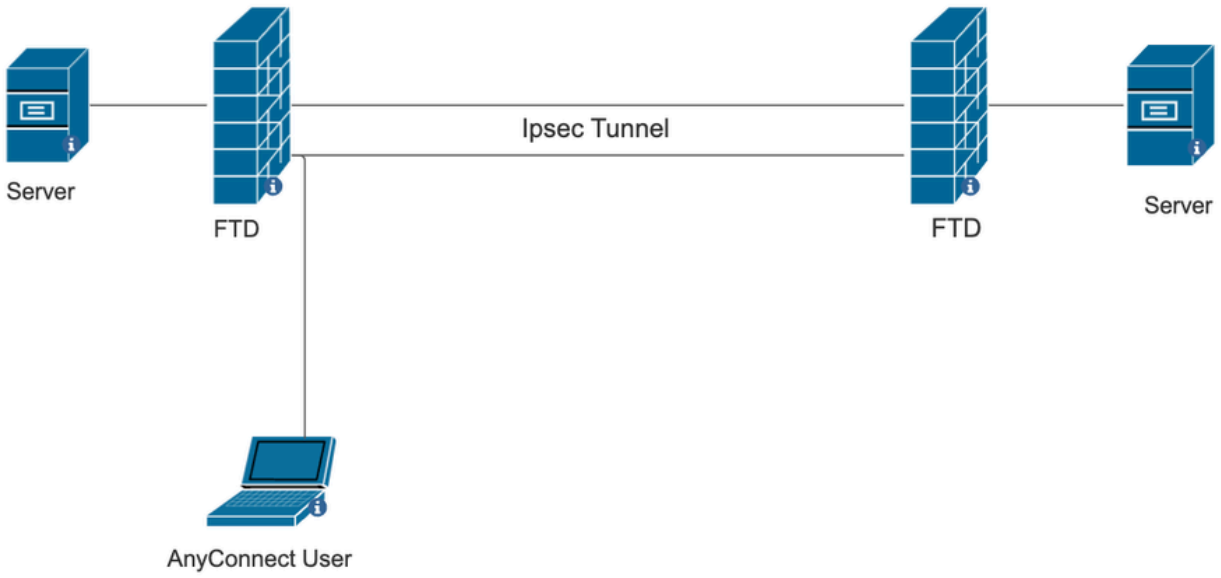
Verwendete Komponenten

- Cisco Firepower Threat Defense für VMware: Version 7.0.0
- FirePOWER Management Center: Version 7.2.4 (Build 169)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die potenziellen Auswirkungen aller Befehle verstehen..

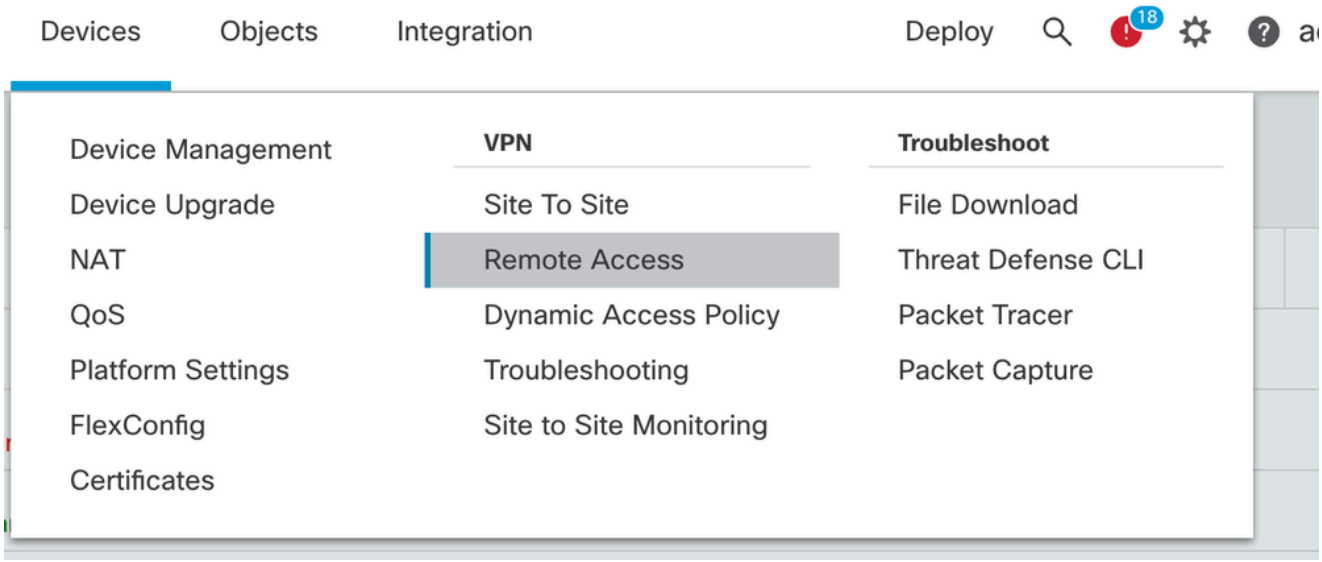
Netzwerkdiagramm



Konfigurationen auf FMC

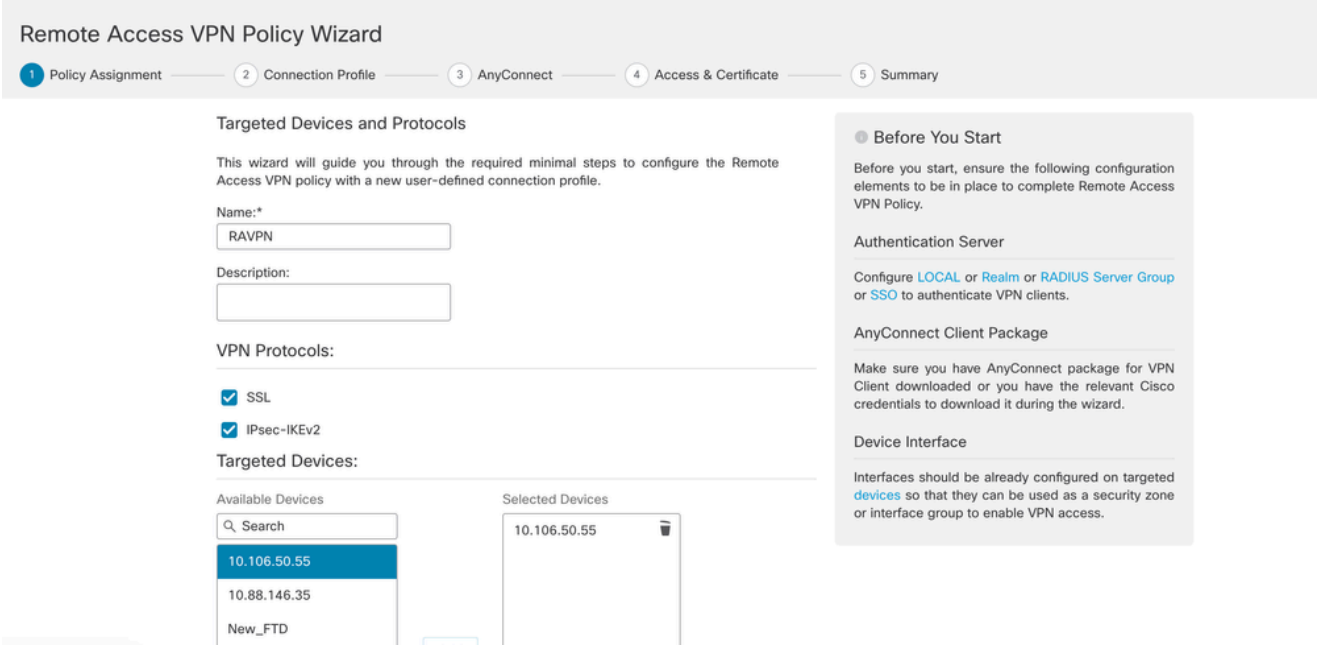
RAVPN-Konfiguration auf dem von FMC verwalteten FTD.

1. Navigieren Sie zu Geräte > Remotezugriff.



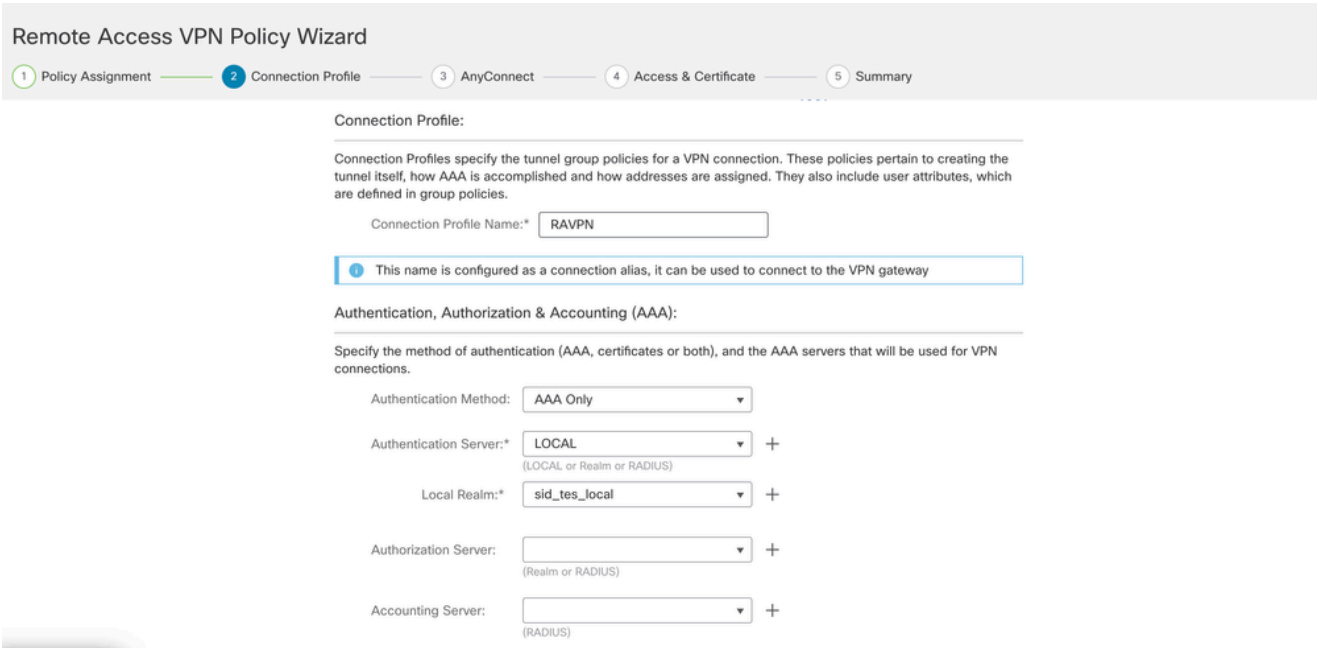
2. Klicken Sie auf Hinzufügen.
3. Konfigurieren Sie einen Namen, und wählen Sie die FTD aus den verfügbaren Geräten aus,

und klicken Sie auf Weiter.

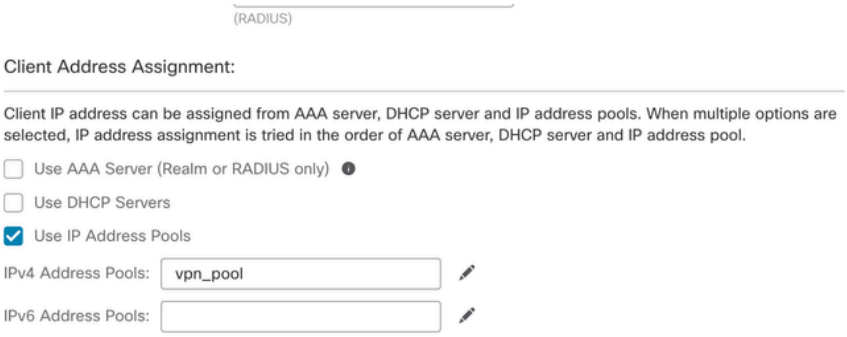


4. Konfigurieren Sie einen Verbindungsprofilnamen, und wählen Sie die Authentifizierungsmethode aus.

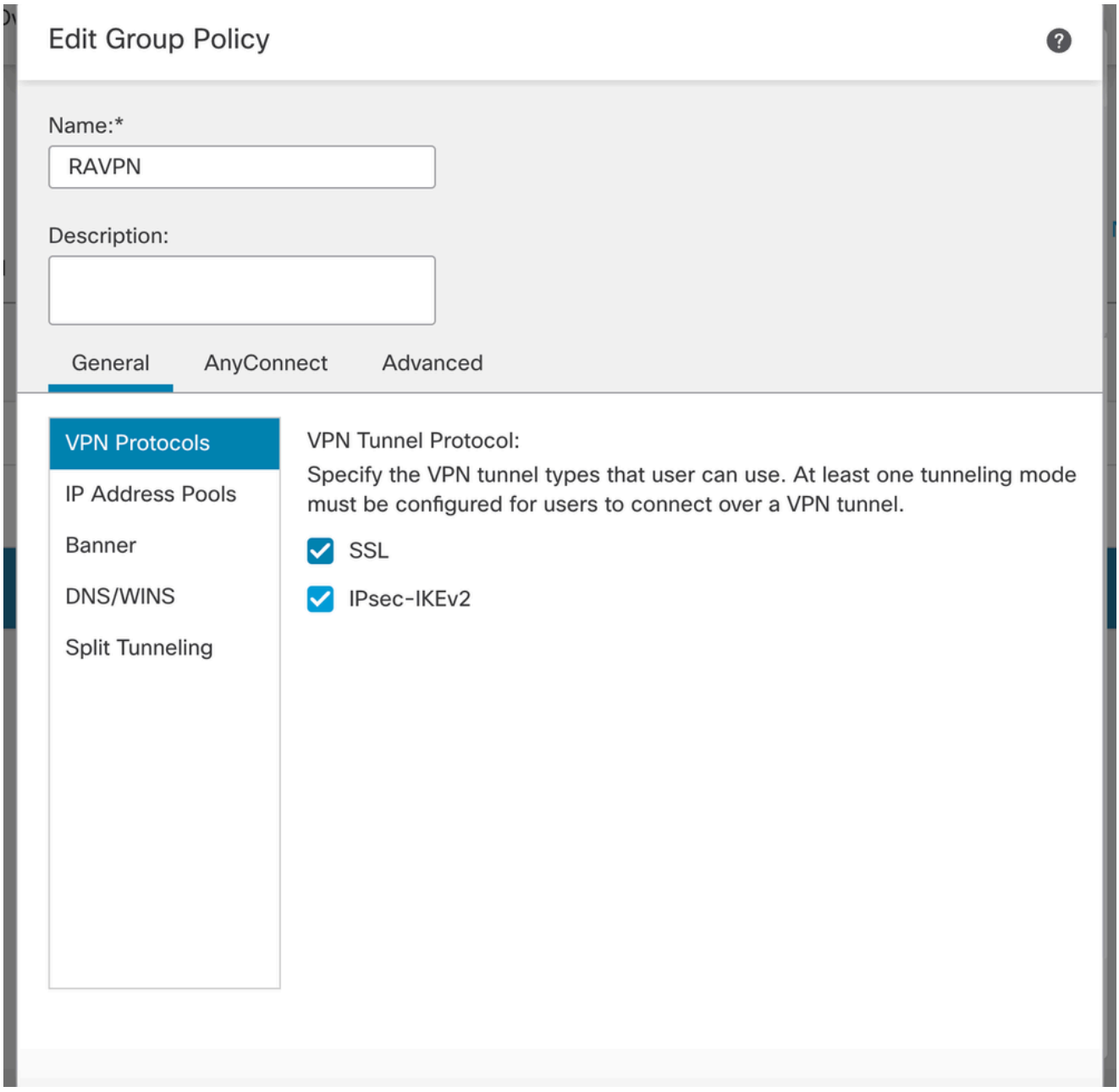
   HINWEIS: Für dieses Konfigurationsbeispiel werden nur AAA und die lokale Authentifizierung verwendet. Konfigurieren Sie sie jedoch entsprechend Ihren Anforderungen.



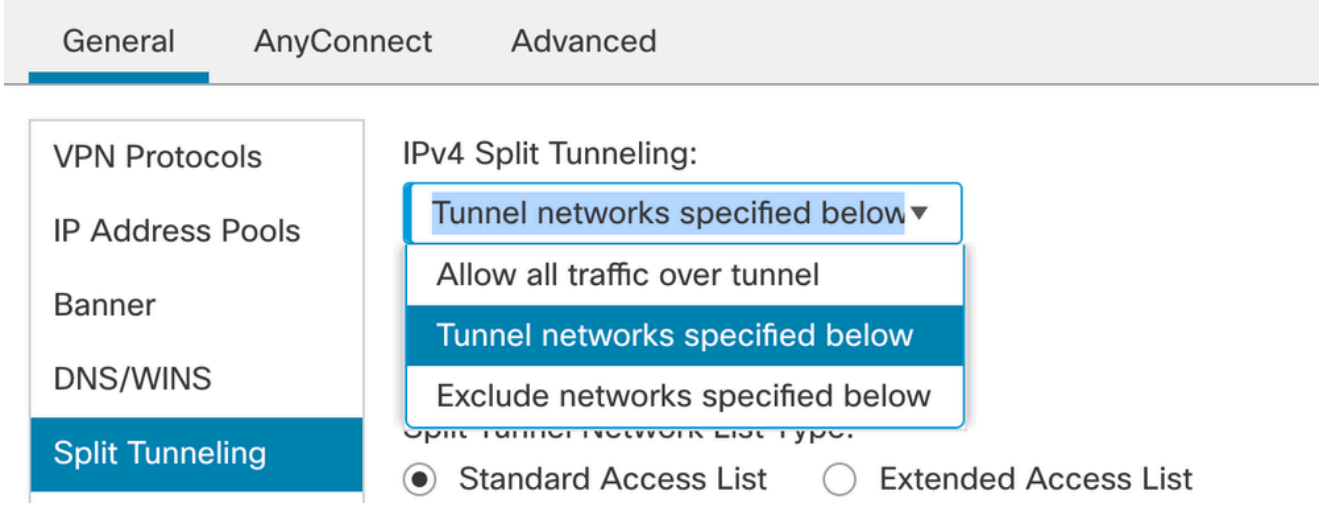
5. Konfigurieren Sie den VPN-Pool, der für die Zuweisung von IP-Adressen für AnyConnect verwendet wird.



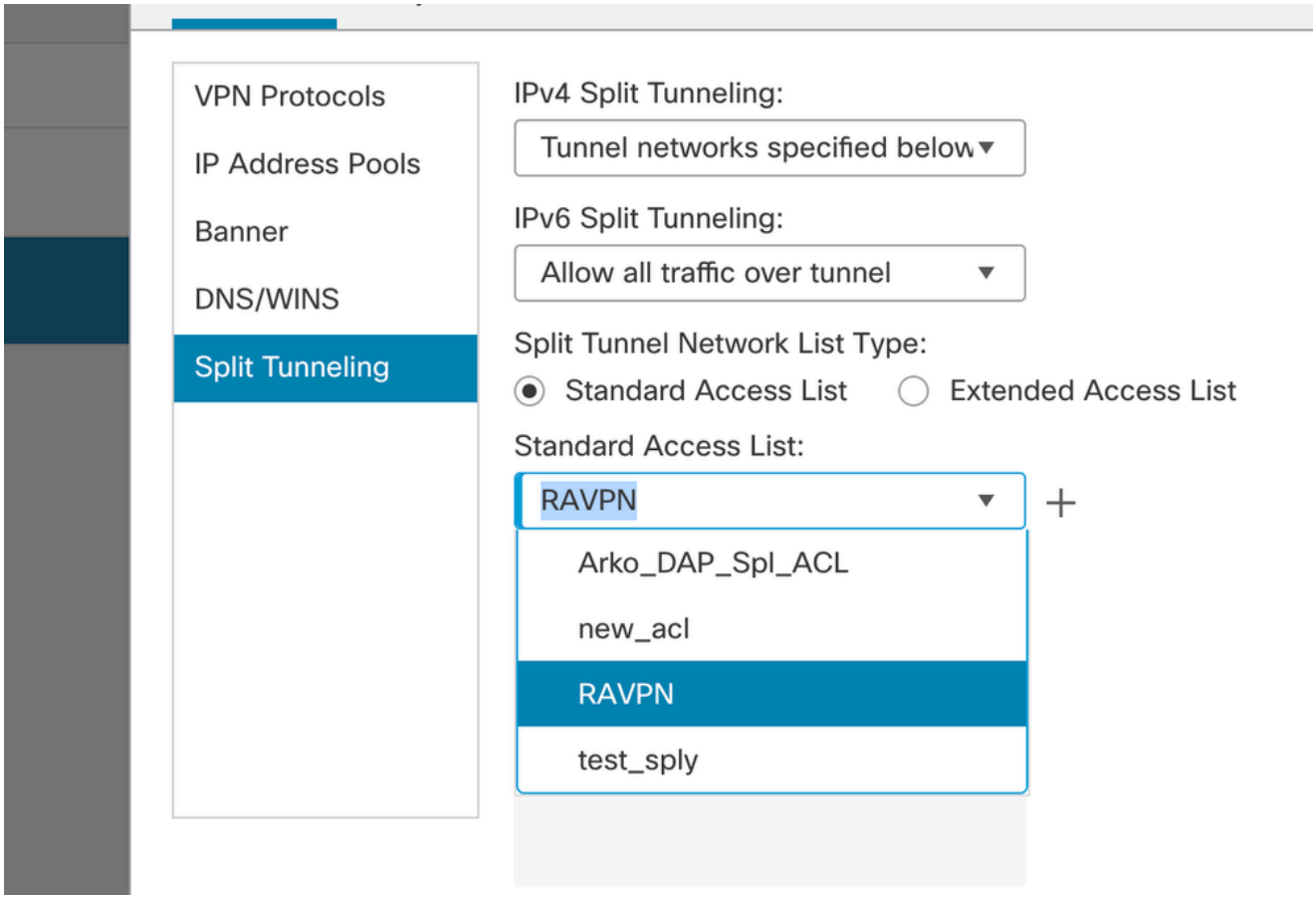
6. Gruppenrichtlinie erstellen. Klicken Sie auf +, um eine Gruppenrichtlinie zu erstellen. Fügen Sie den Namen der Gruppenrichtlinie hinzu.



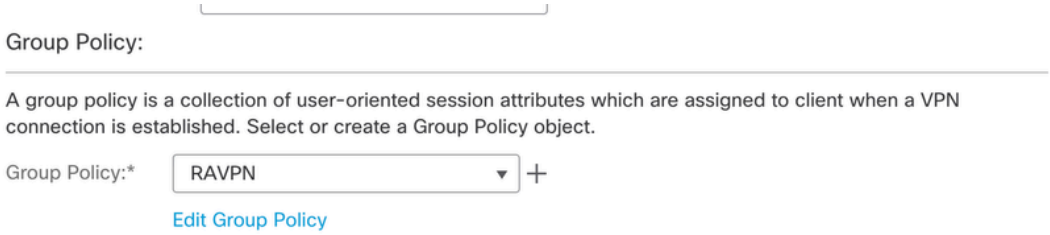
7. Gehen Sie zu Split Tunneling. Wählen Sie die hier angegebenen Tunnelnetzwerke aus:



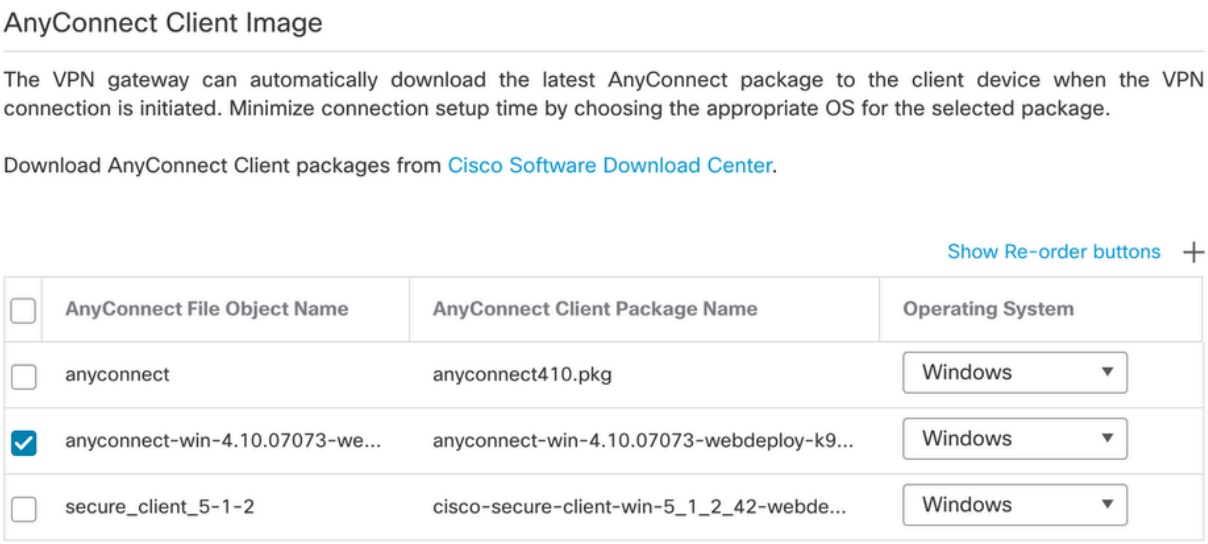
8. Wählen Sie im Dropdown-Menü die gewünschte Zugriffsliste aus. Wenn noch keine ACL konfiguriert ist: Klicken Sie auf das +-Symbol, um die Standard-Zugriffsliste hinzuzufügen und eine neue zu erstellen.
   Klicken Sie auf Speichern.



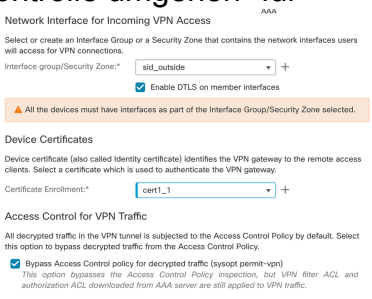
9. Wählen Sie die hinzugefügte Gruppenrichtlinie aus, und klicken Sie auf Weiter.



10. Wählen Sie das AnyConnect-Image aus.

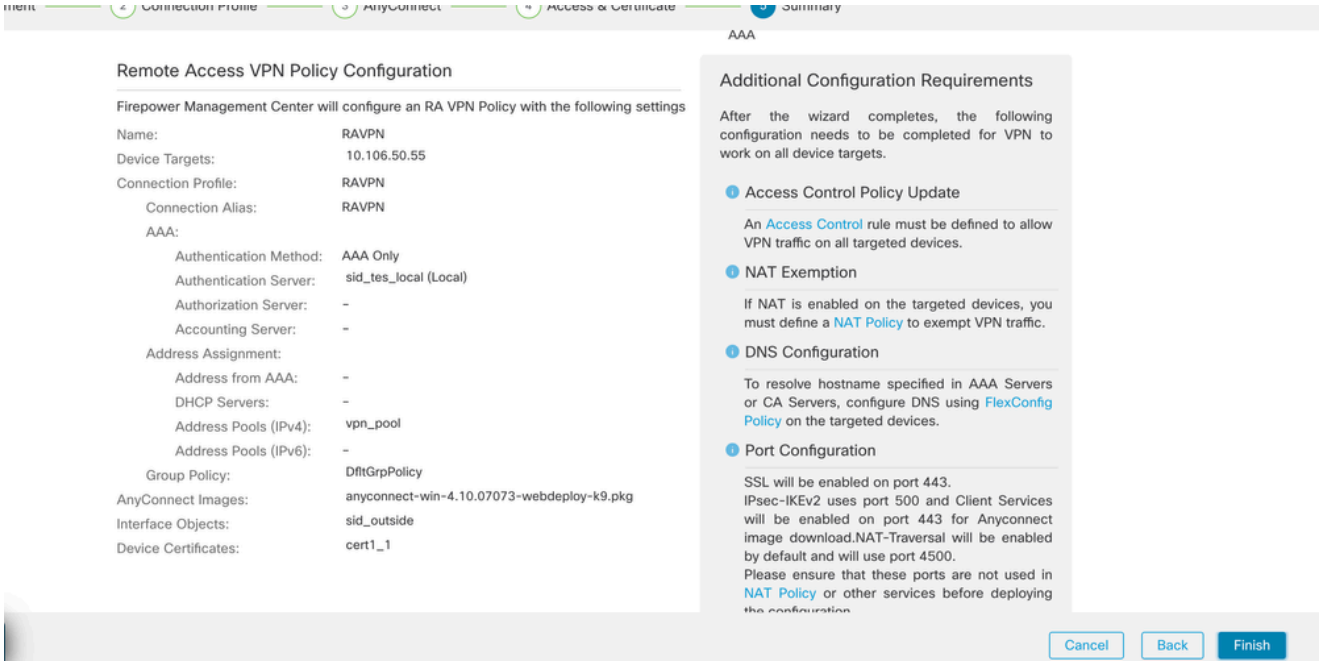


11. Wählen Sie die Schnittstelle aus, die für die AnyConnect-Verbindung aktiviert werden muss, fügen Sie das Zertifikat hinzu, wählen Sie die Richtlinie "Zugriffskontrolle umgehen" für

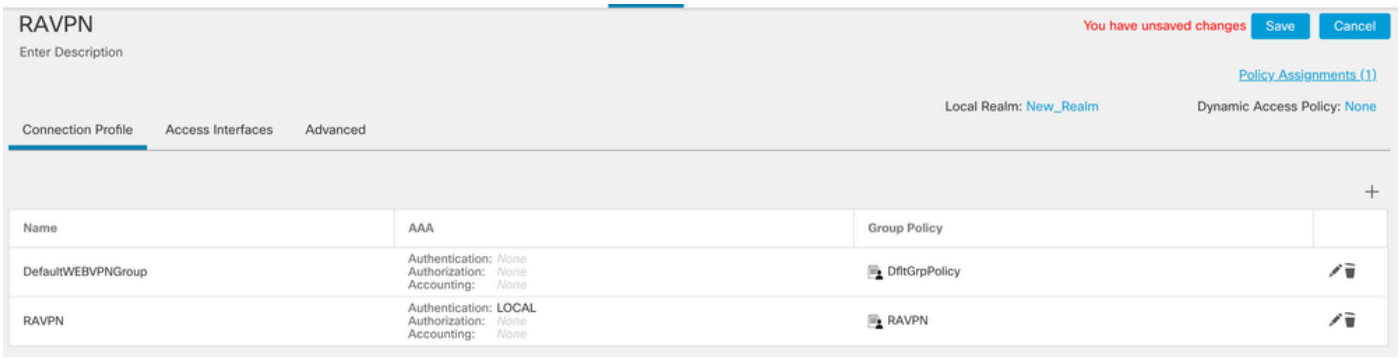


entschlüsselten Datenverkehr aus, und klicken Sie auf "Weiter".

12. Überprüfen Sie die Konfiguration, und klicken Sie auf Fertig stellen.

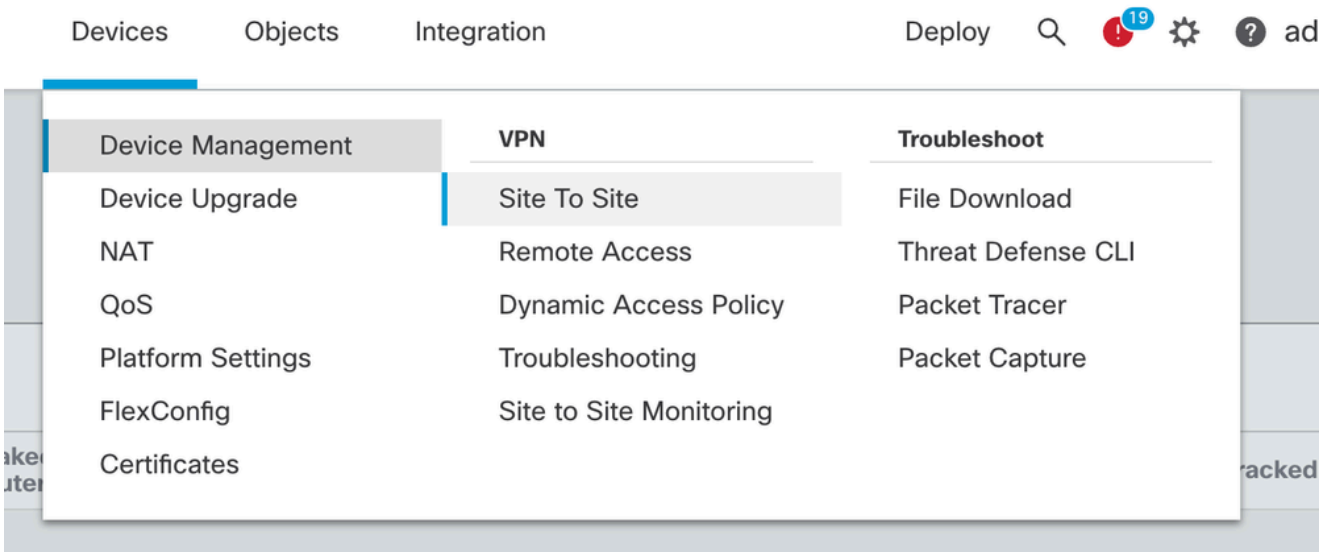


13. Klicken Sie auf Speichern und Bereitstellen.

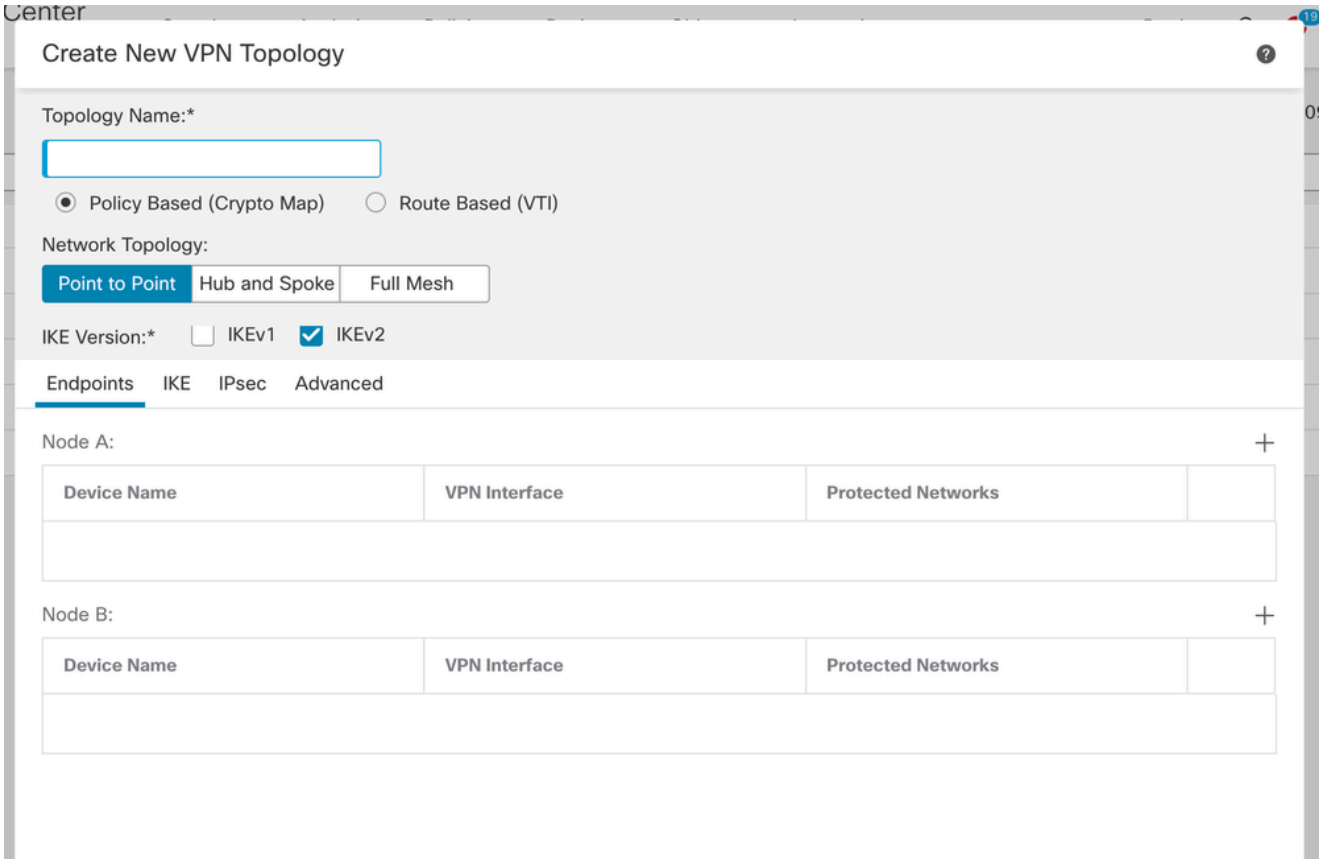


IKEv2 VPN auf FTD, von FMC verwaltet:

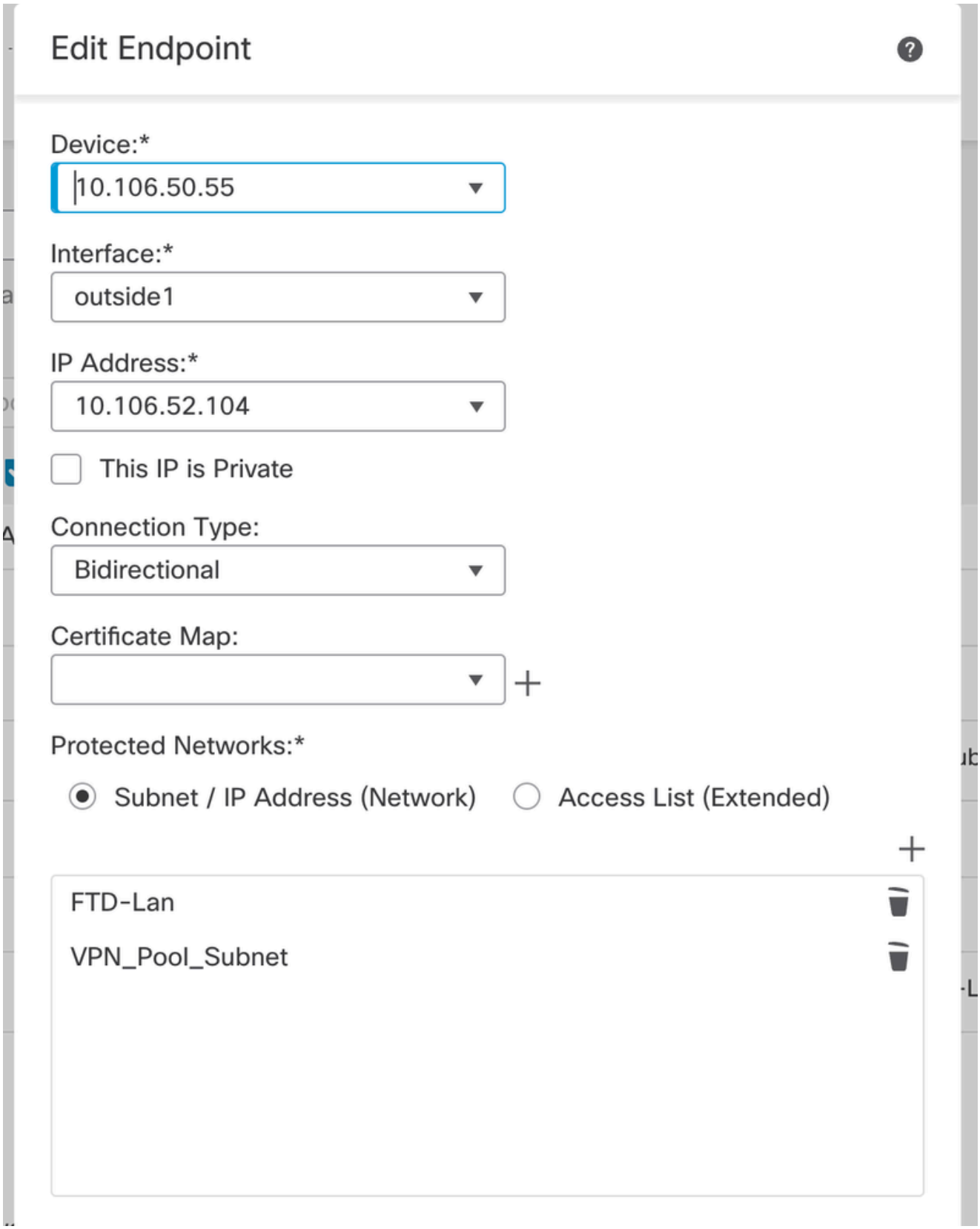
1. Navigieren Sie zu Geräte > Site-to-Site.



2. Klicken Sie auf Hinzufügen.
3. Klicken Sie für Knoten A auf +:



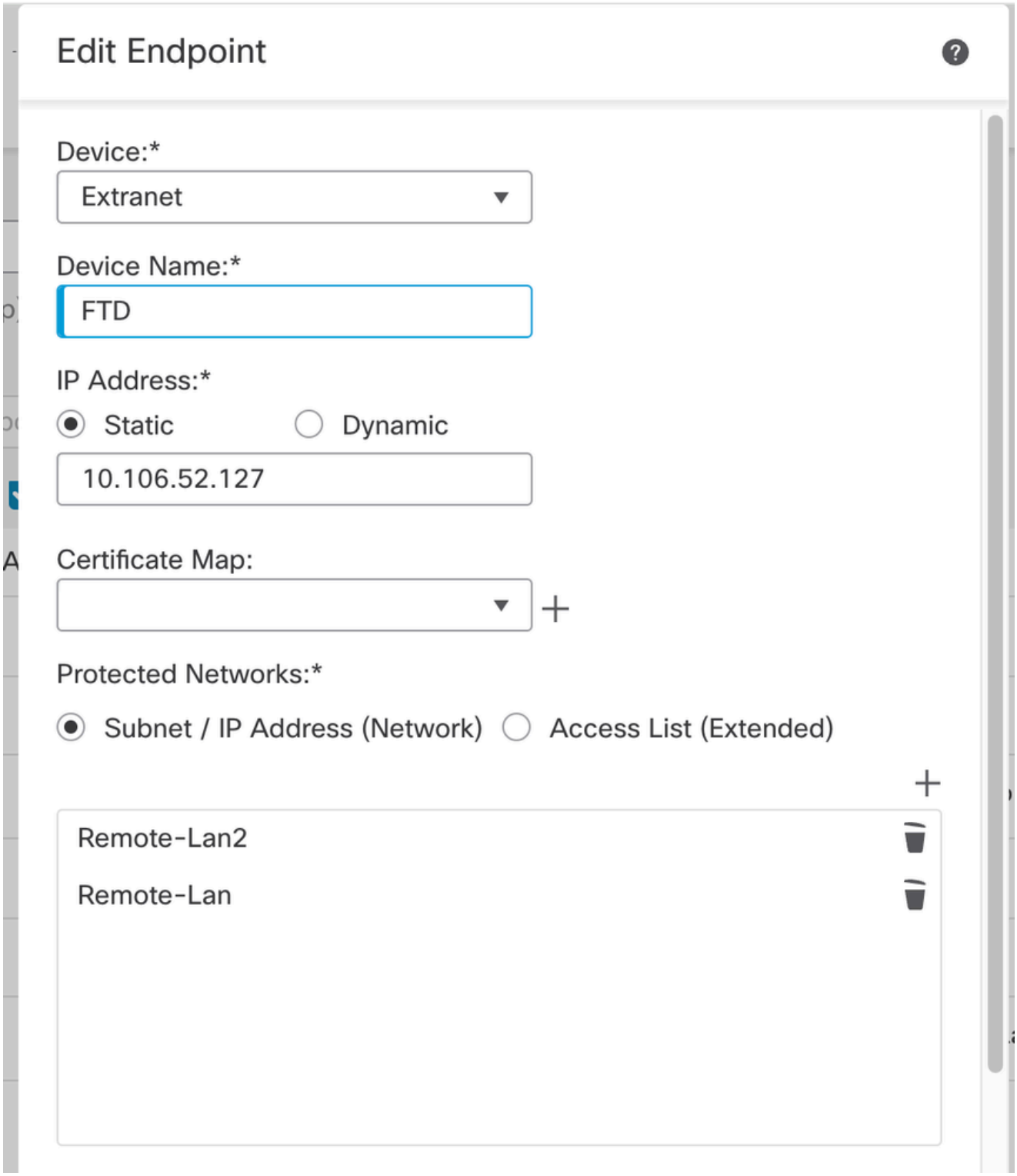
4. Wählen Sie die FTD vom Gerät aus, wählen Sie die Schnittstelle aus, fügen Sie das lokale Subnetz hinzu, das über den IPSec-Tunnel verschlüsselt werden muss (und in diesem Fall auch die VPN-Pooladressen enthält), und klicken Sie auf OK.



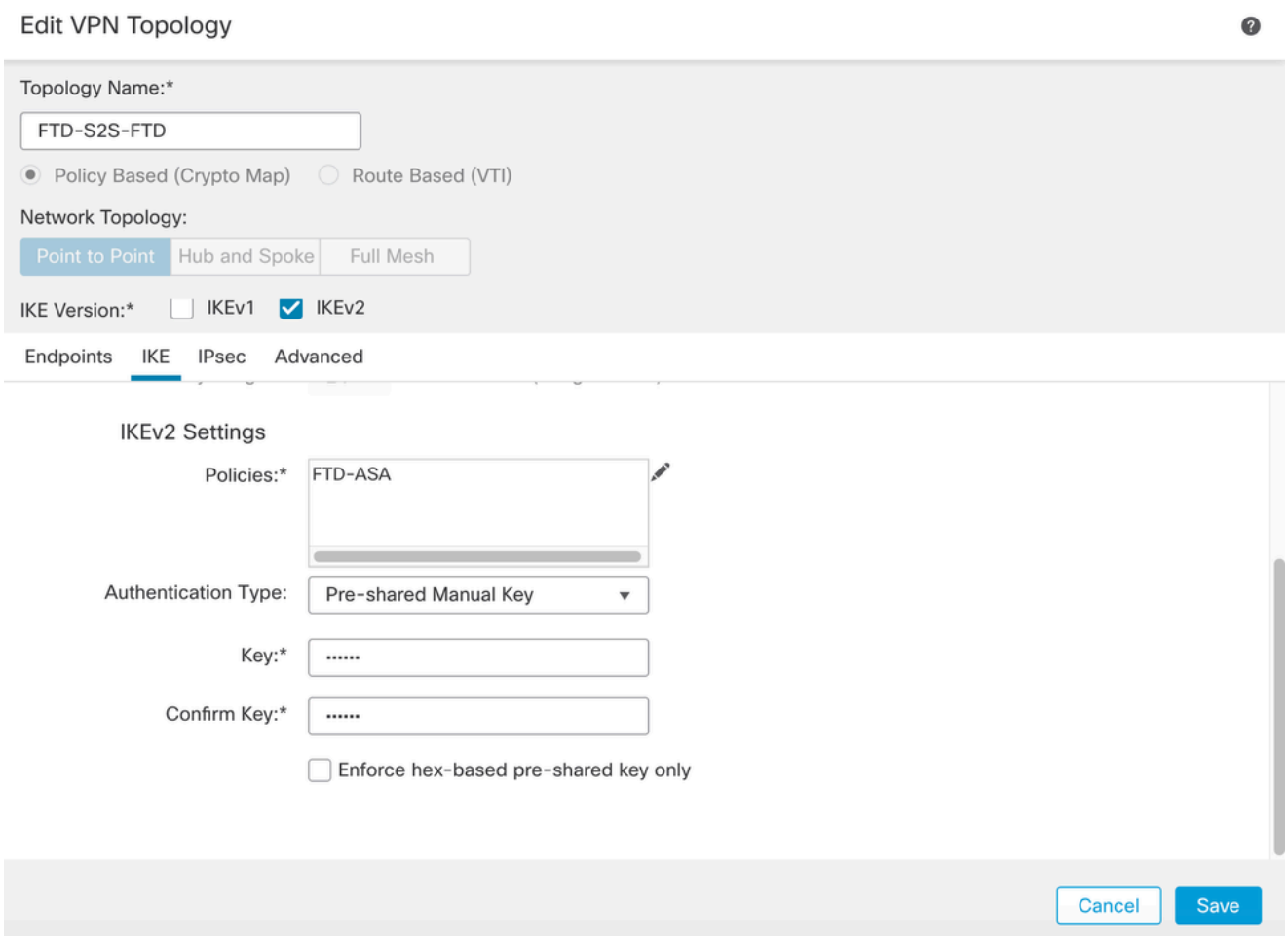
5. Klicken Sie auf + für Knoten B:

> Wählen Sie das Extranet vom Gerät aus, und geben Sie den Namen des Peer-Geräts an.

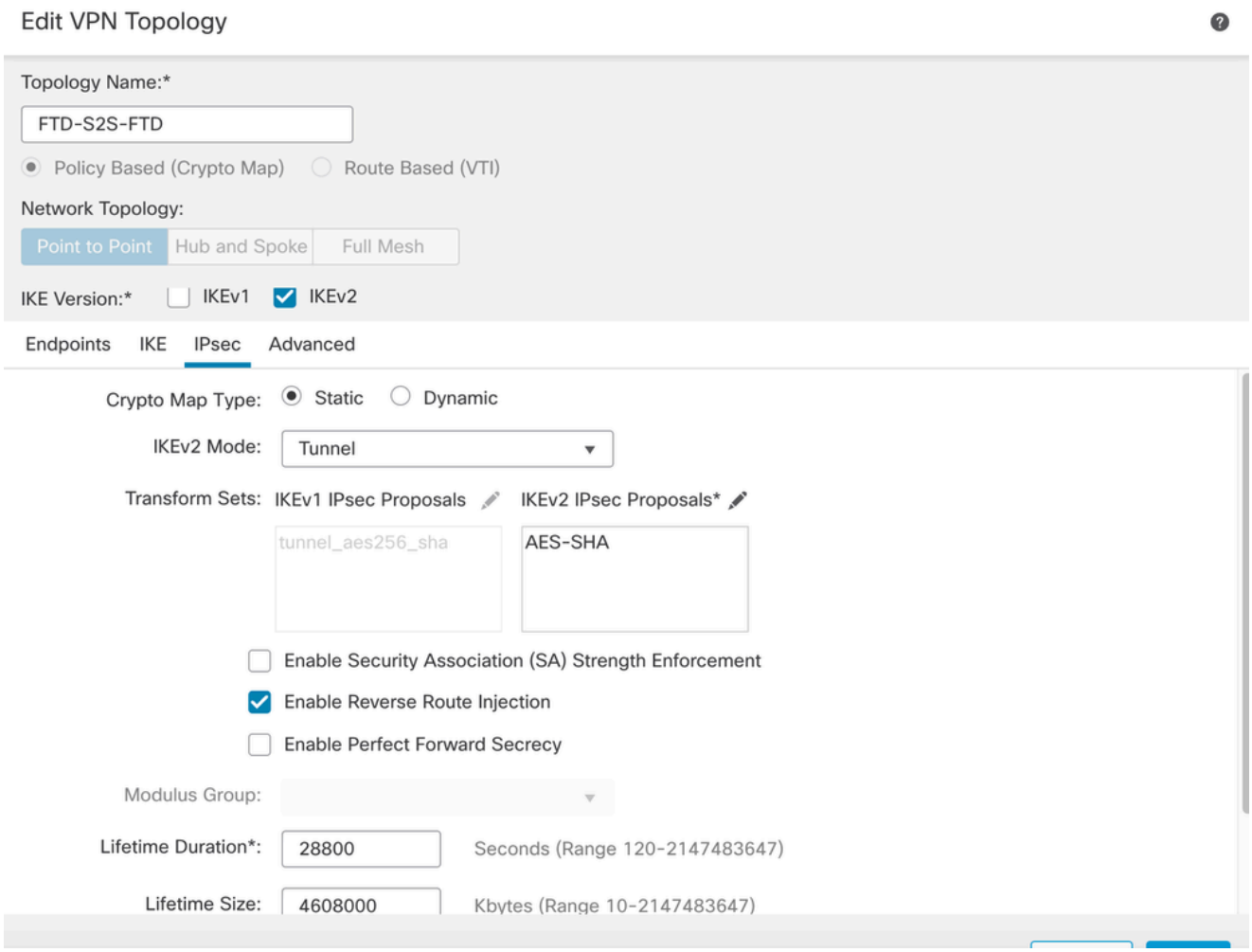
> Konfigurieren Sie die Peer-Details, und fügen Sie das Remote-Subnetz hinzu, auf das über den VPN-Tunnel zugegriffen werden muss, und klicken Sie auf OK.



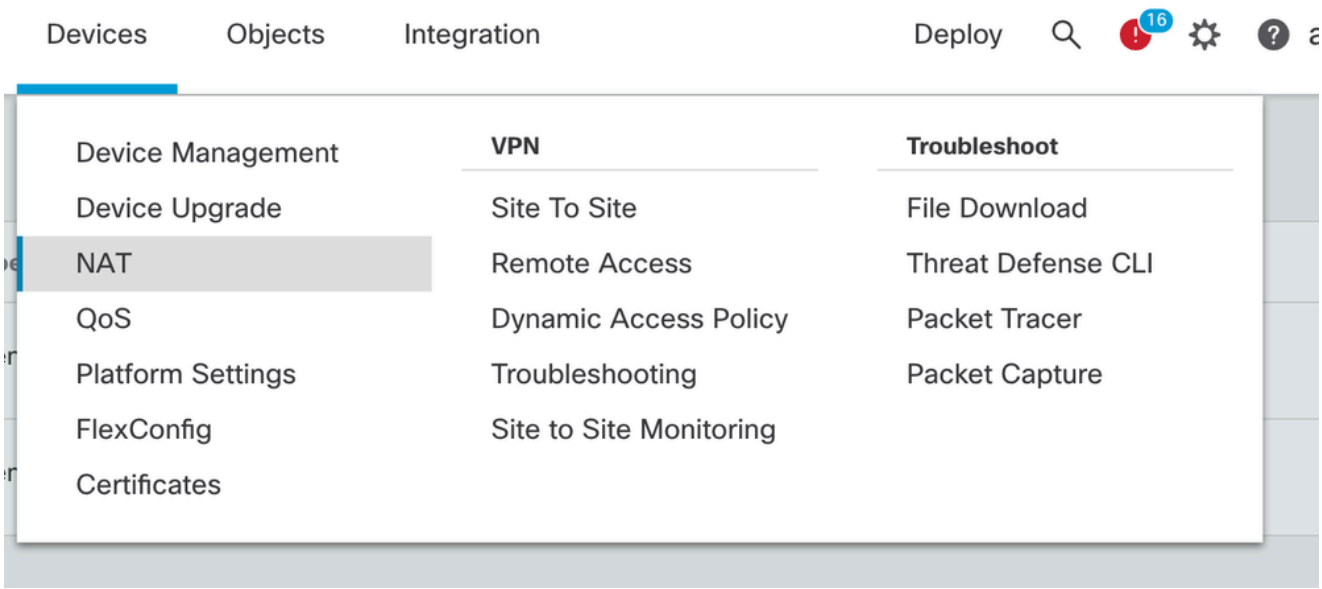
6. Klicken Sie auf die Registerkarte IKE: Konfigurieren Sie die IKEv2-Einstellungen gemäß Ihren Anforderungen.



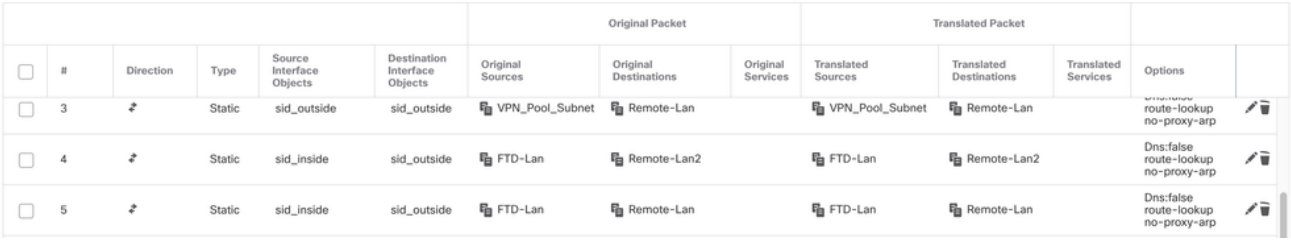
7. Klicken Sie auf die Registerkarte IPsec: Konfigurieren Sie die IPSec-Einstellungen gemäß Ihren Anforderungen.



8. Konfigurieren Sie Nat-Exempt für Ihren interessanten Datenverkehr (optional)
   Klicken Sie auf Geräte > NAT.



9. Die hier konfigurierte NAT ermöglicht es RAVPN und internen Benutzern, über den S2S IPSec-Tunnel auf Server zuzugreifen.



	#	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. Führen Sie auf die gleiche Weise die Konfiguration am anderen Peer-End für den S2S-Tunnel aus.

    HINWEIS: Die Krypto-ACL oder die Subnetze für den interessanten Datenverkehr müssen auf beiden Peers Spiegelkopien der jeweils anderen sein.

Überprüfung

1. RAVPN-Verbindung überprüfen:

<#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. Überprüfen der IKEv2-Verbindung:

<#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. Überprüfen der IPSec-Verbindung:

<#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
```

Fehlerbehebung

1. Sammeln Sie das dart-Paket, oder aktivieren Sie die AnyConnect-Fehlerbehebung, um das AnyConnect-Verbindungsproblem zu beheben.
2. Verwenden Sie zur Fehlerbehebung für den IKEv2-Tunnel die folgenden Debugging-Methoden:

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

3. Um das Datenverkehrsproblem auf dem FTD zu beheben, nehmen Sie die Paketerfassung und überprüfen Sie die Konfiguration.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.