Configurare AnyConnect per l'accesso al server sul tunnel IPSec.

Sommario

Introduzione:

Questo documento descrive le procedure per la distribuzione di una configurazione RAVPN sull'FTD gestito da FMC e di un tunnel da sito a sito tra FTD.

Prerequisiti:

Requisiti di base

- Una conoscenza di base delle VPN da sito a sito e di RAVPN è vantaggiosa.
- È essenziale comprendere i concetti fondamentali della configurazione del tunnel basato su criteri IKEv2 sulla piattaforma Cisco Firepower.

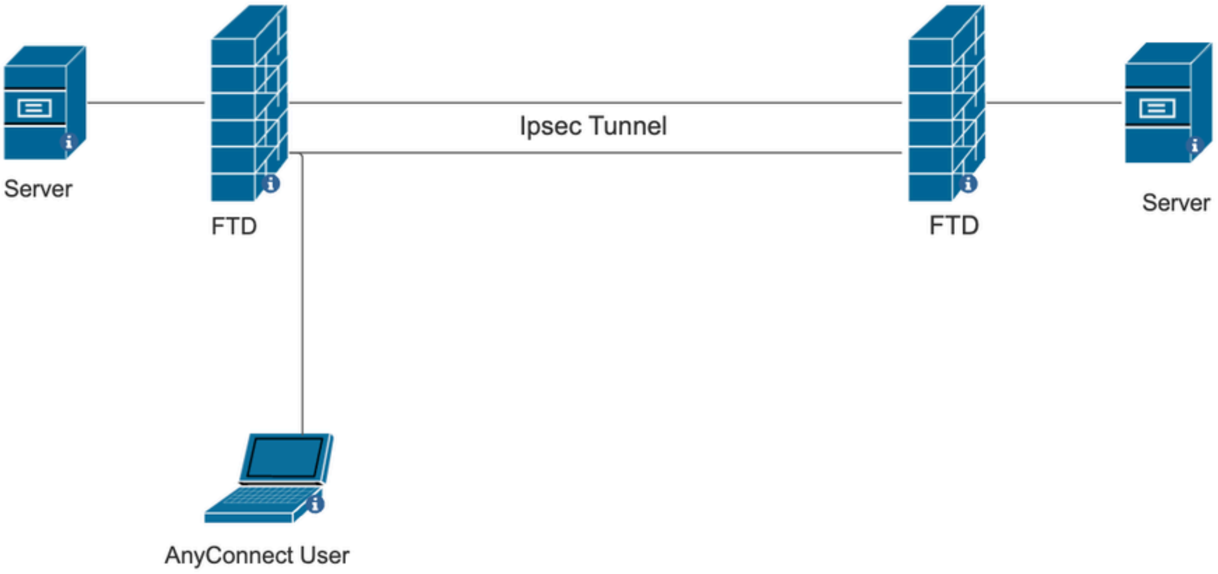
Questa procedura è per la distribuzione di una configurazione RAVPN sull'FTD gestito da FMC e di un tunnel da sito a sito tra FTD in cui gli utenti AnyConnect possono accedere al server dietro l'altro peer FTD.

Componenti usati

- Cisco Firepower Threat Defense per VMware: versione 7.0.0
- Firepower Management Center: versione 7.2.4 (build 169)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi..

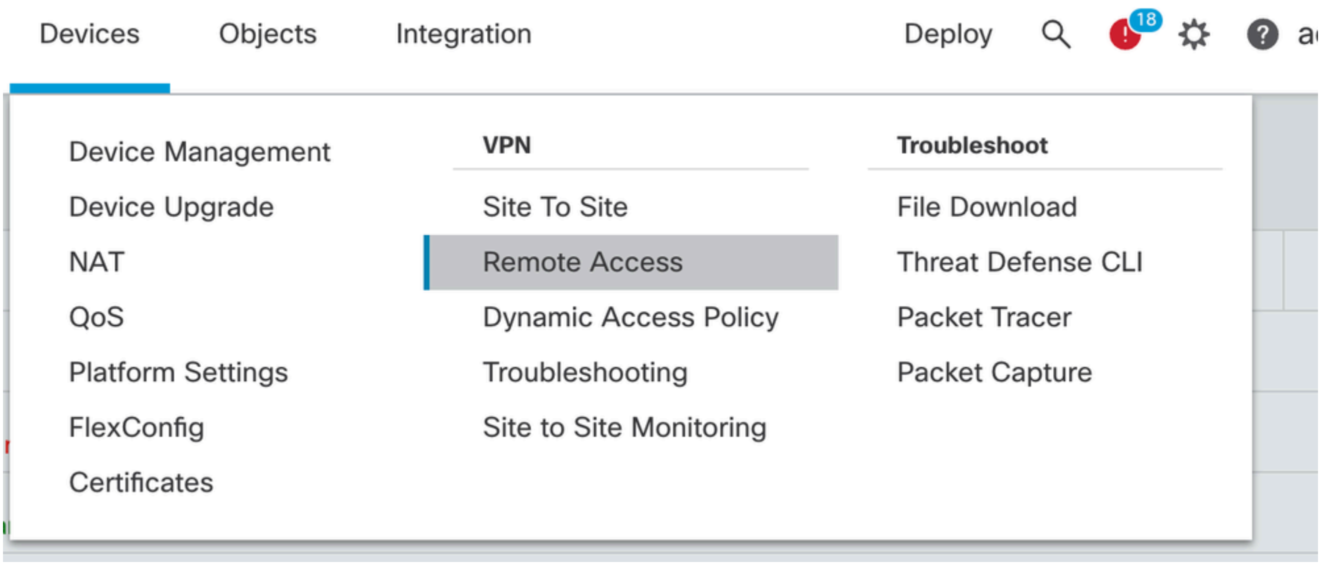
Esempio di rete



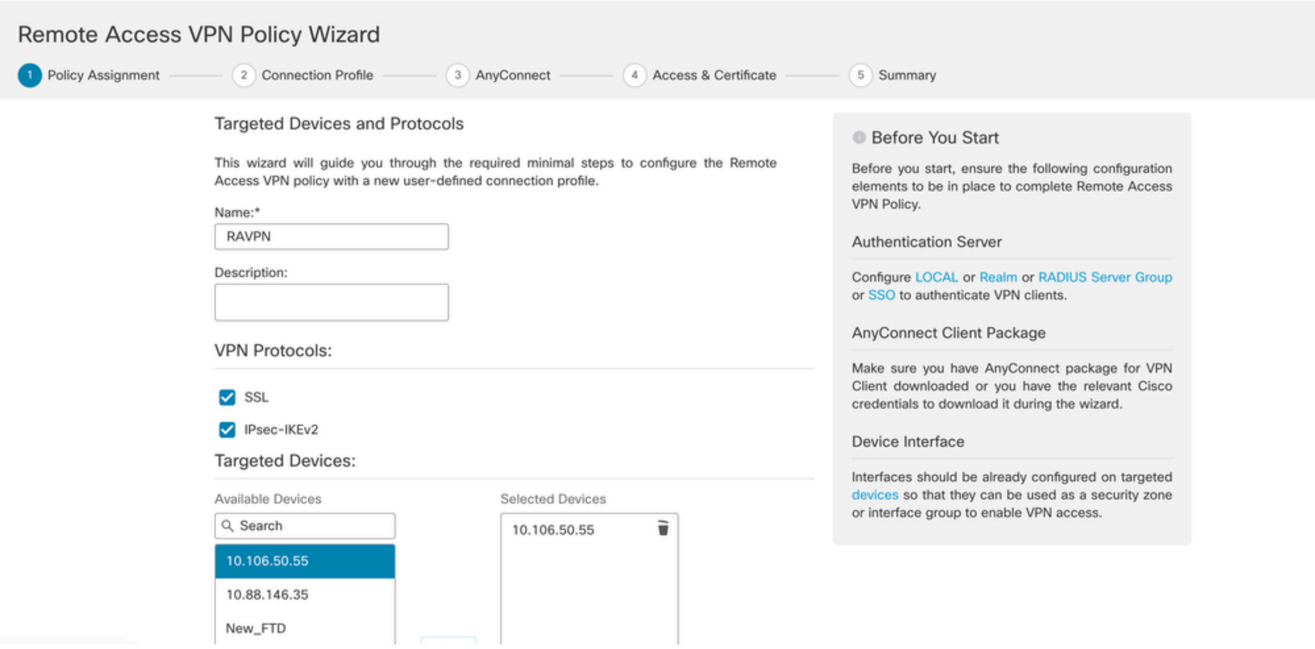
Configurazioni su FMC

Configurazione RAVPN sull'FTD gestito da FMC.

1. Selezionare Dispositivi > Accesso remoto.



2. Fare clic su Add.
3. Configurare un nome e selezionare l'FTD dai dispositivi disponibili e fare clic su Avanti.



Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:* RAVPN

Description:

VPN Protocols:

☑ SSL

☑ IPsec-IKEv2

Targeted Devices:

Available Devices: 10.106.50.55, 10.88.146.35, New_FTD

Selected Devices: 10.106.50.55

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

AnyConnect Client Package

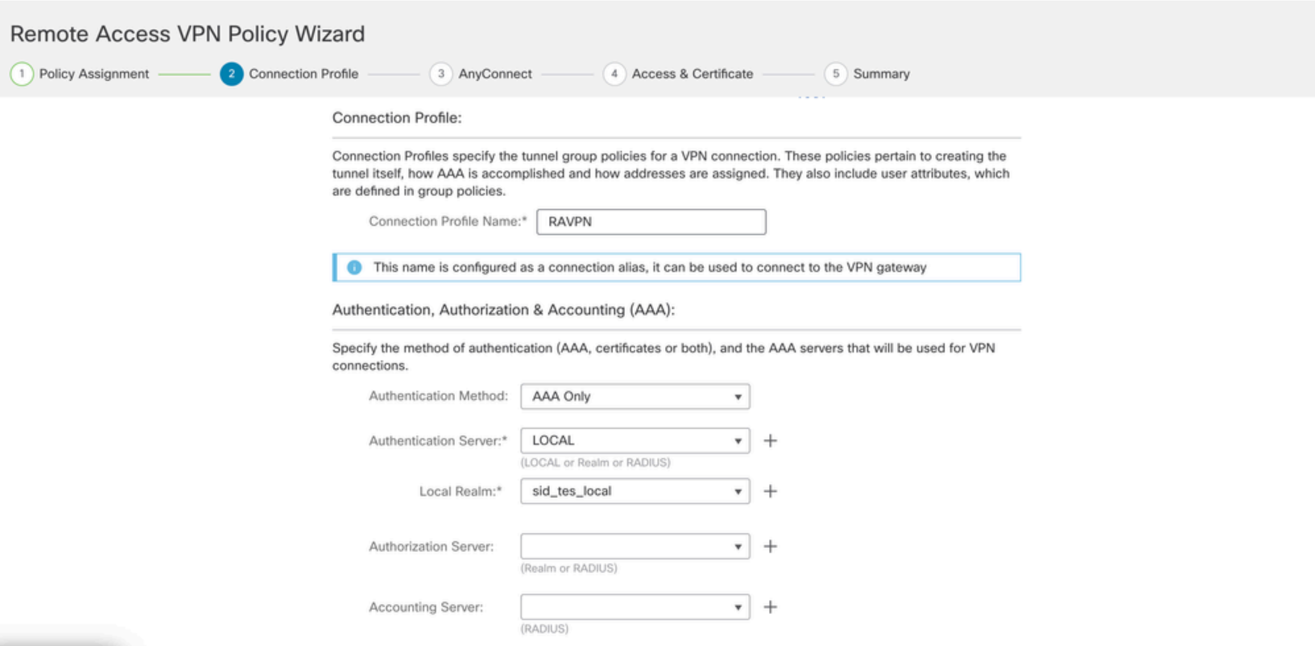
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

4. Configurare il nome di un profilo di connessione e scegliere il metodo di autenticazione.

   NOTA: per questo esempio di configurazione viene utilizzata solo l'autenticazione AAA e l'autenticazione locale. Tuttavia, è possibile eseguire la configurazione in base ai requisiti.



Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RAVPN

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

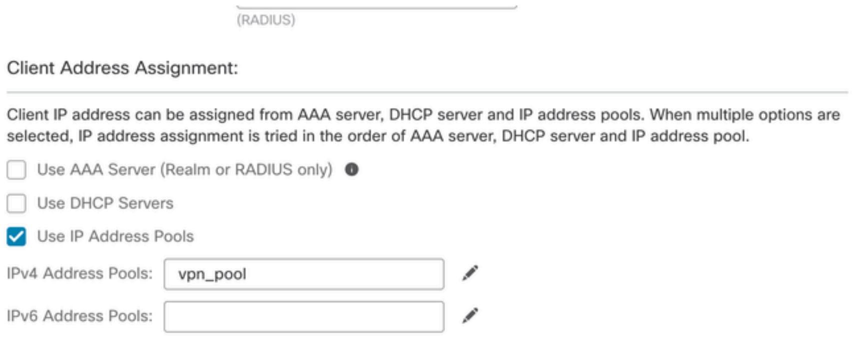
Authentication Server:* LOCAL (LOCAL or Realm or RADIUS)

Local Realm:* sid_tes_local

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

5. Configurare il pool VPN utilizzato per l'assegnazione dell'indirizzo IP ad AnyConnect.



(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

☐ Use AAA Server (Realm or RADIUS only)

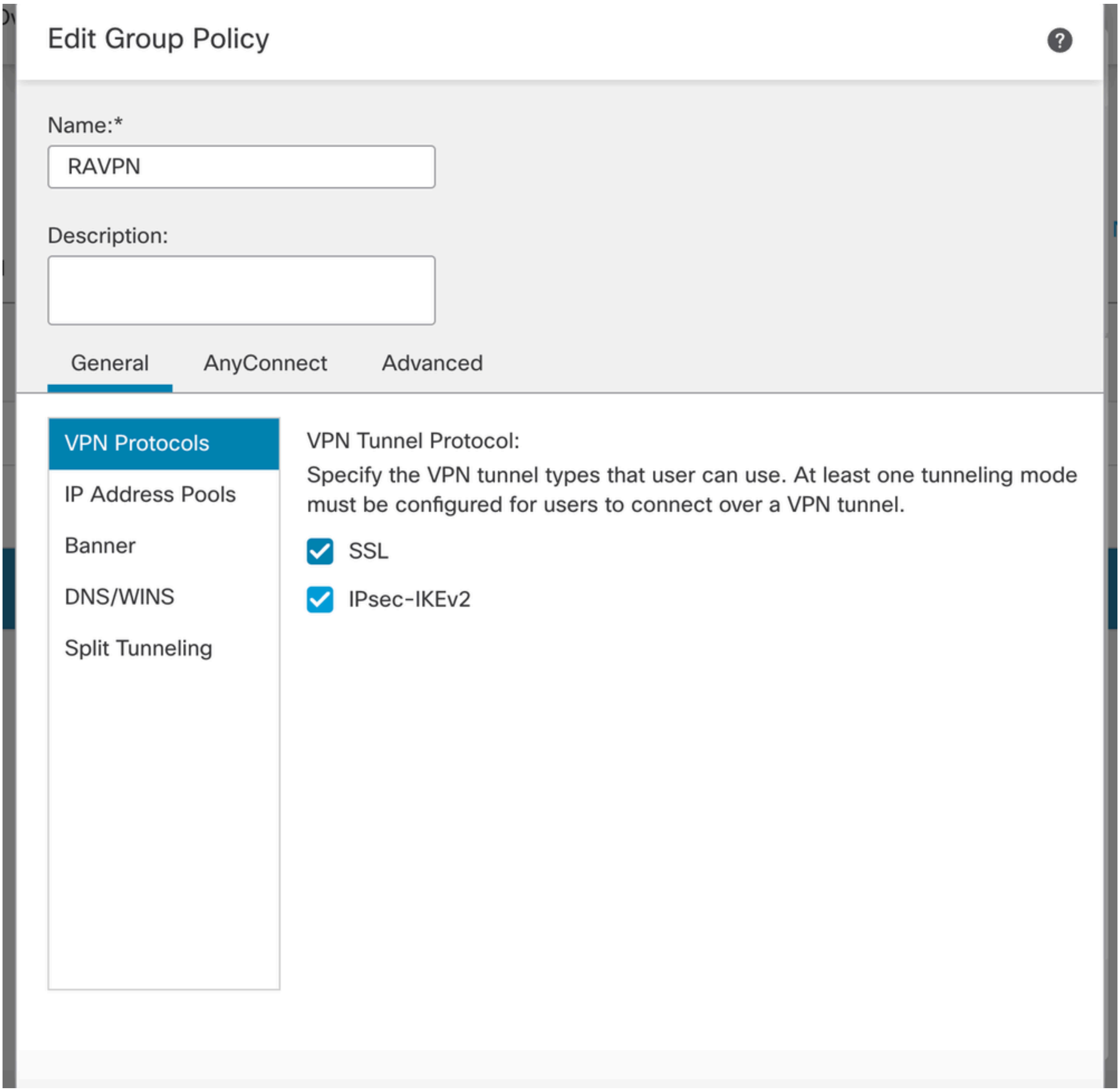
☐ Use DHCP Servers

☑ Use IP Address Pools

IPv4 Address Pools: vpn_pool

IPv6 Address Pools:

6. Creare Criteri di gruppo. Fare clic su + per creare un criterio di gruppo. Aggiungere il nome del criterio di gruppo.



Edit Group Policy

Name:* RAVPN

Description:

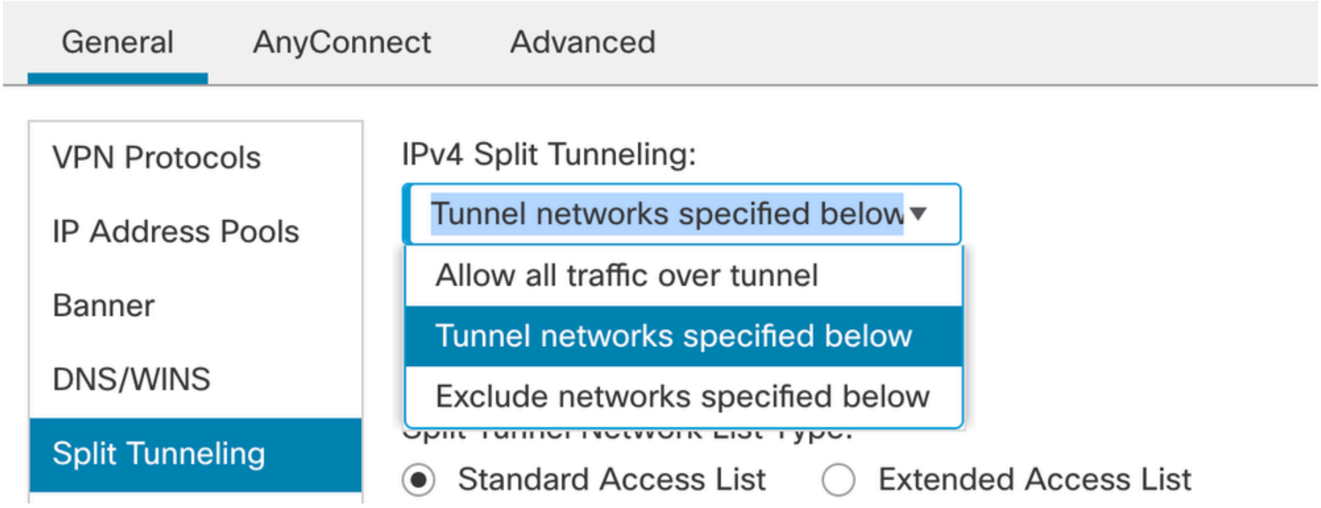
VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☑ SSL

☑ IPsec-IKEv2

7. Andare al tunneling ripartito. Selezionare le reti tunnel specificate qui:

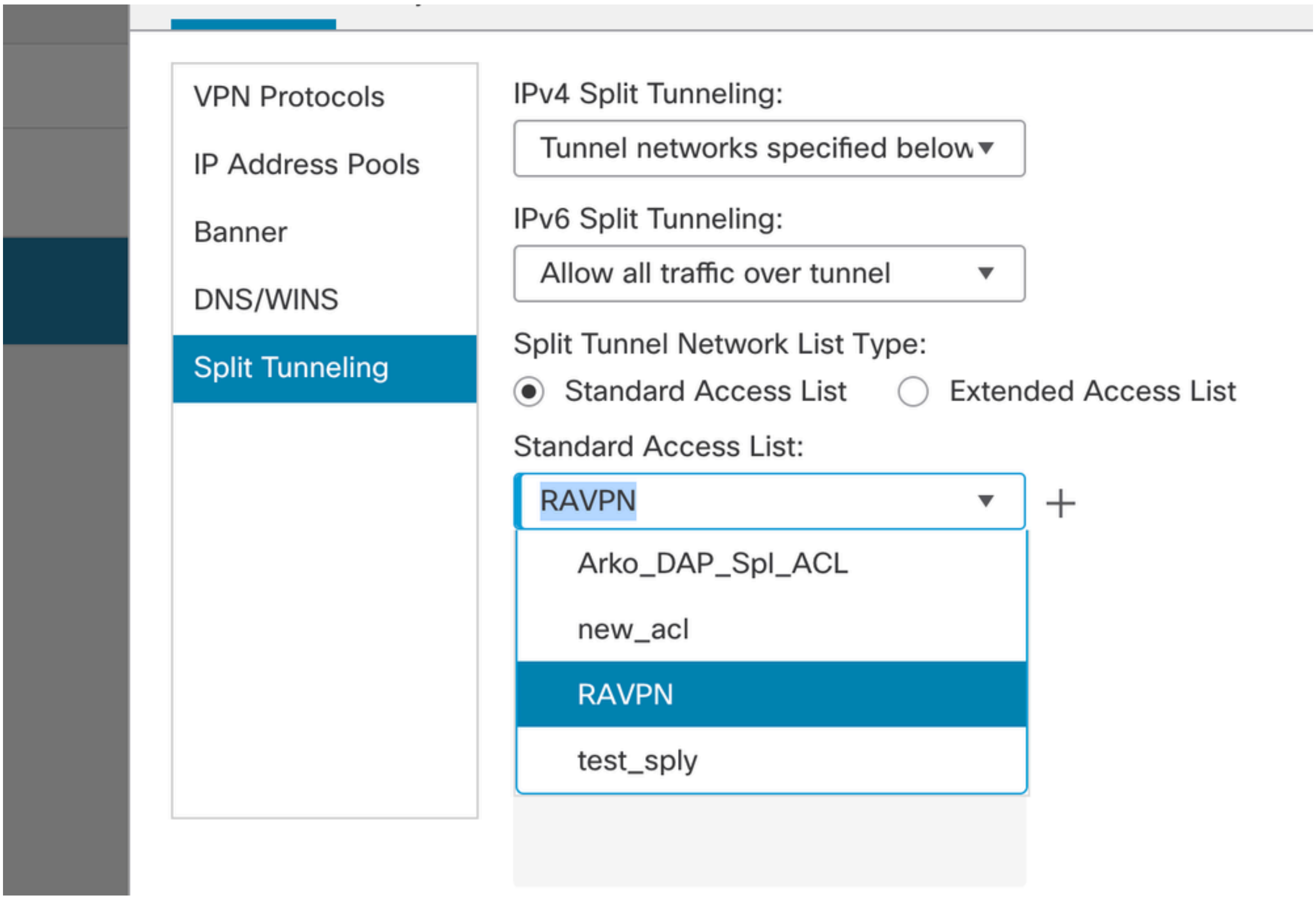


IPv4 Split Tunneling: Tunnel networks specified below

- Allow all traffic over tunnel
- Tunnel networks specified below
- Exclude networks specified below

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

8. Selezionare l'elenco degli accessi corretto dall'elenco a discesa. Se un ACL non è già configurato: fare clic sull'icona + per aggiungere l'elenco degli accessi Standard e crearne uno nuovo.
   Fare clic su Save (Salva).



IPv4 Split Tunneling: Tunnel networks specified below

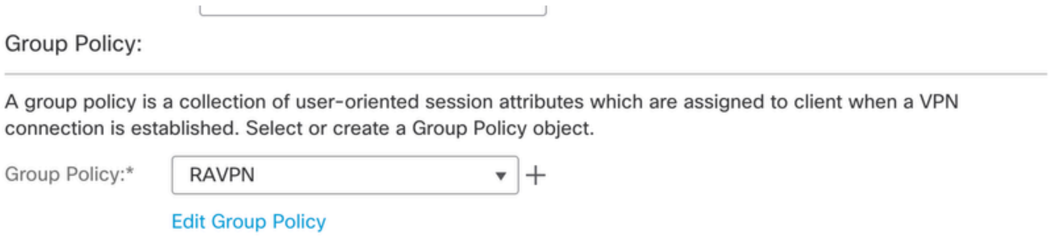
IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

Standard Access List: RAVPN

- Arko_DAP_Spl_ACL
- new_acl
- RAVPN
- test_sply

9. Selezionare il criterio di gruppo aggiunto e fare clic su Avanti.

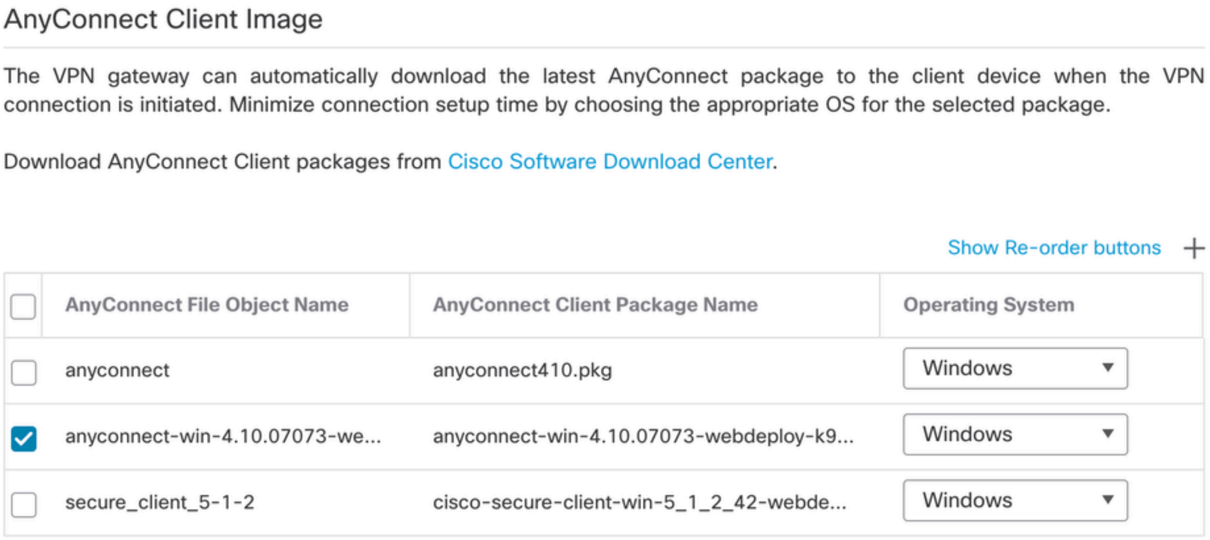


Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* RAVPN ▾ +

10. Selezionare l'immagine AnyConnect.



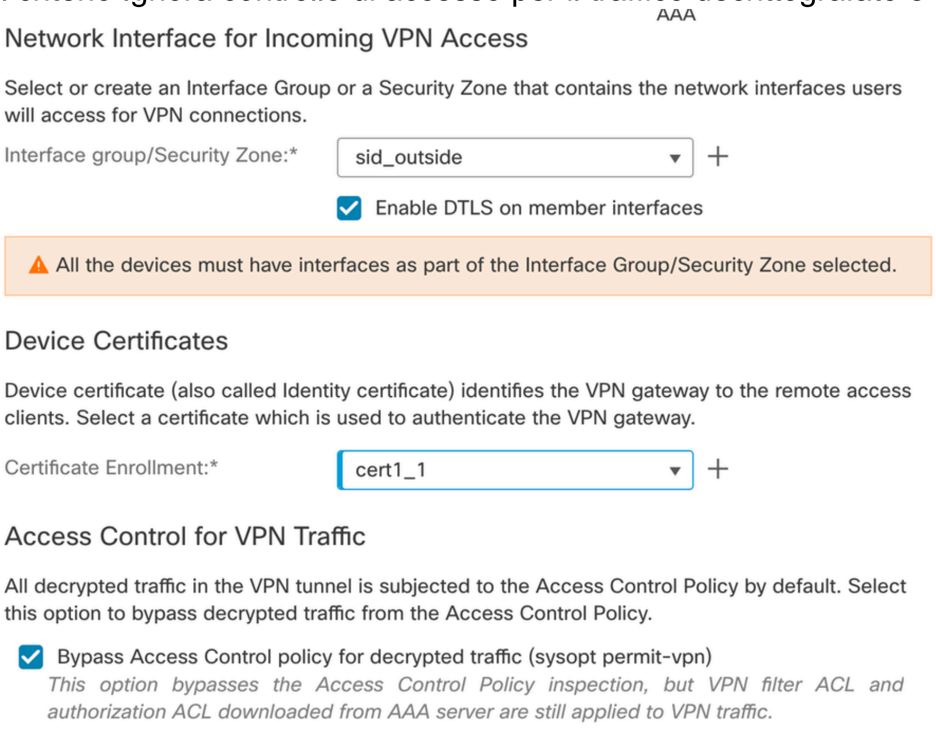
AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from Cisco Software Download Center.

□	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
□	anyconnect	anyconnect410.pkg	Windows ▾
☑	anyconnect-win-4.10.07073-we...	anyconnect-win-4.10.07073-webdeploy-k9...	Windows ▾
□	secure_client_5-1-2	cisco-secure-client-win-5_1_2_42-webde...	Windows ▾

11. Selezionare l'interfaccia da abilitare per la connessione AnyConnect, aggiungere il certificato, selezionare il criterio Ignora controllo di accesso per il traffico decrittografato e fare clic su Avanti.



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* sid_outside ▾ +

☑ Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* cert1_1 ▾ +

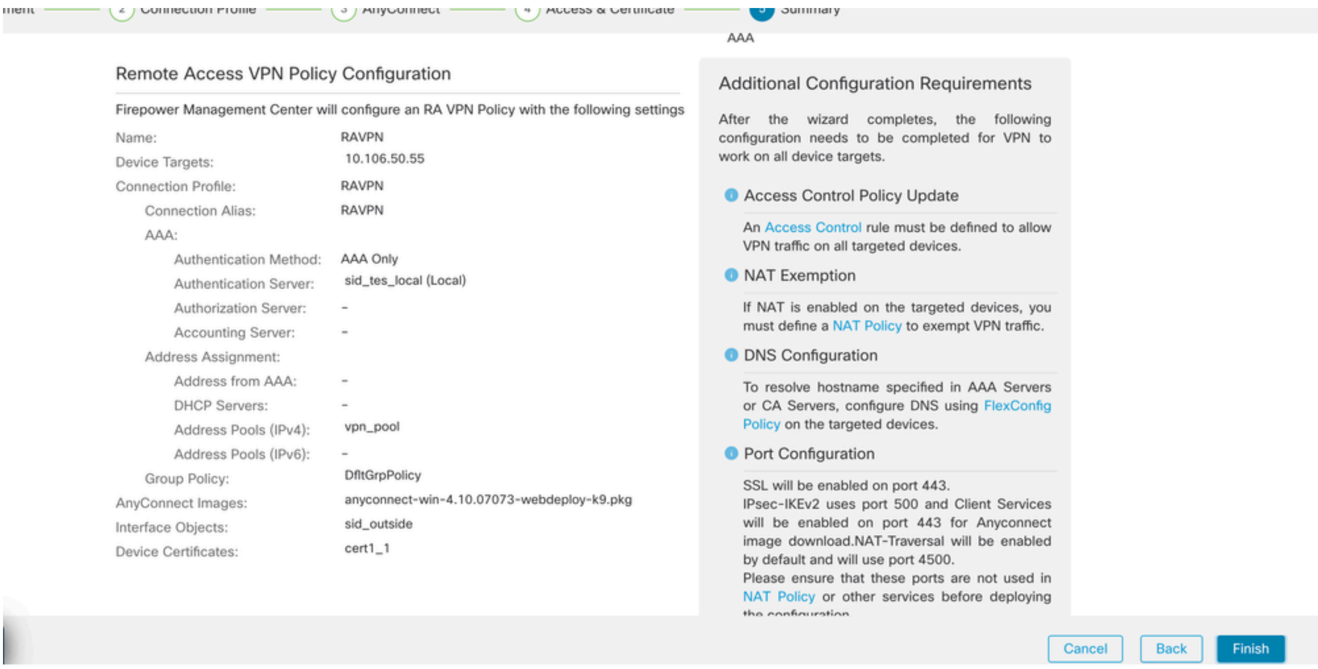
Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

12. Esaminare la configurazione e fare clic su Fine.



Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	10.106.50.55
Connection Profile:	RAVPN
Connection Alias:	RAVPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	sid_tes_local (Local)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
AnyConnect Images:	anyconnect-win-4.10.07073-webdeploy-k9.pkg
Interface Objects:	sid_outside
Device Certificates:	cert1_1

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update

An Access Control rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption

If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.

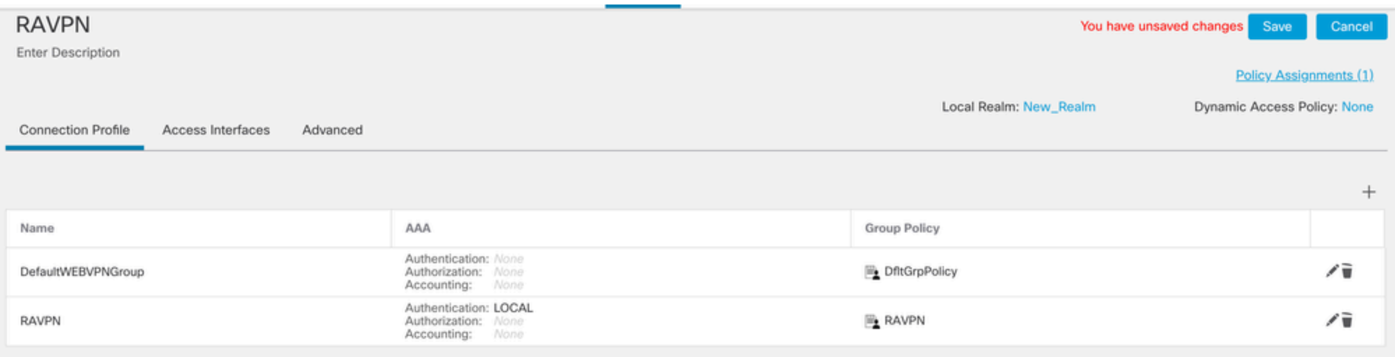
DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.

Port Configuration

SSL will be enabled on port 443.
IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download.NAT-Traversal will be enabled by default and will use port 4500.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

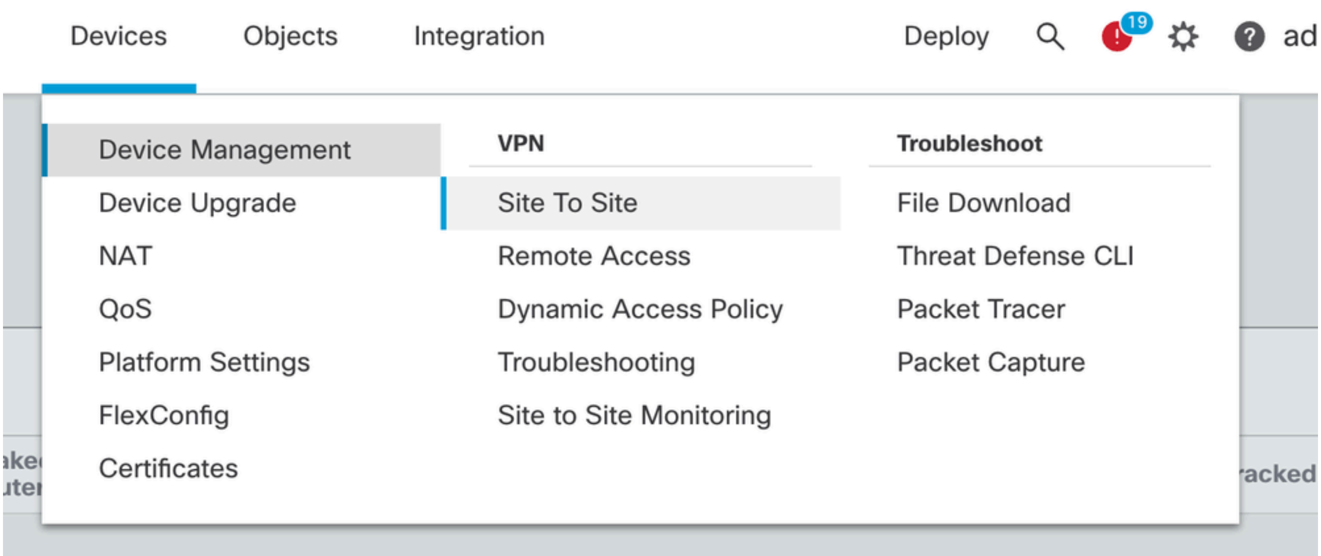
13. Fare clic su Salva e distribuisci.



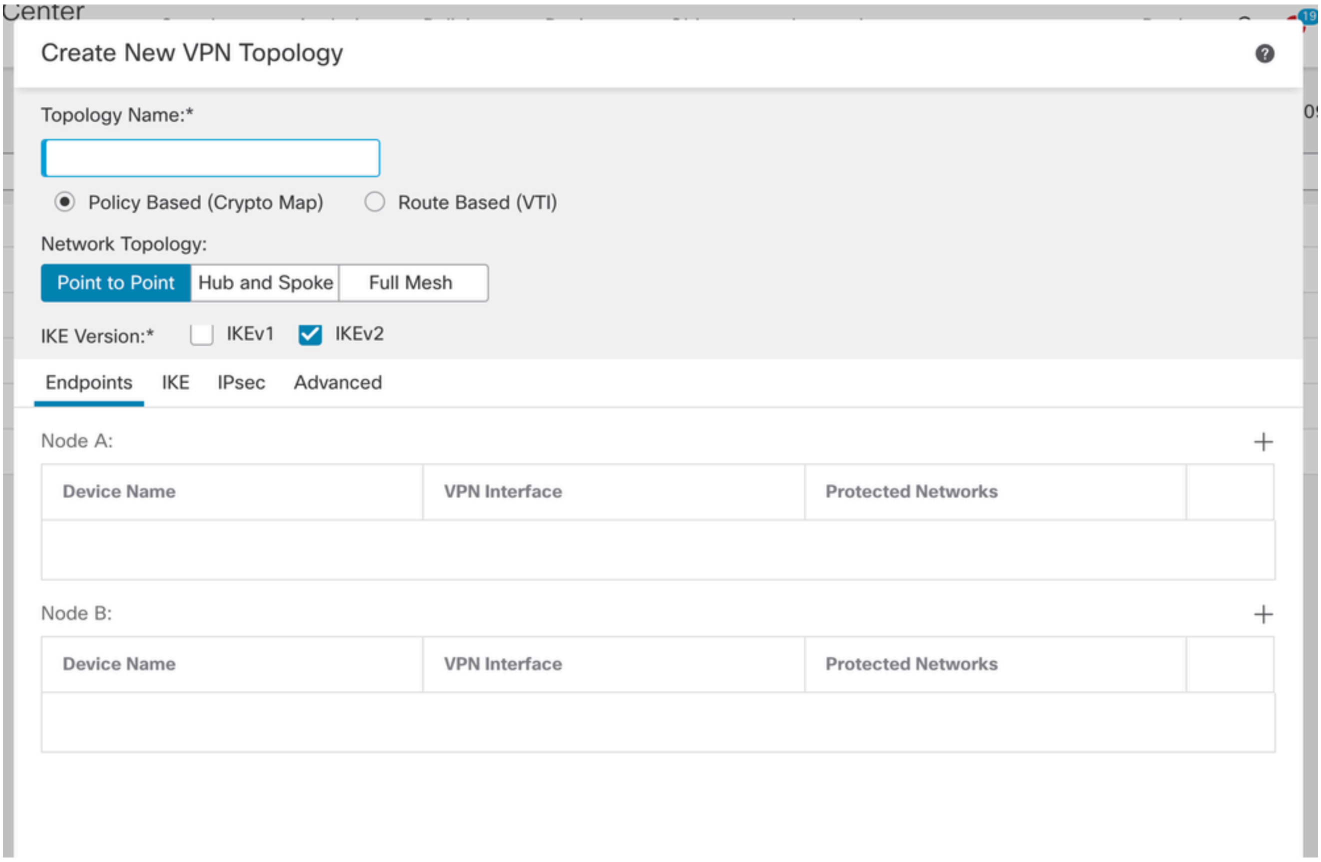
Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN

VPN IKEv2 su FTD gestito da FMC:

1. Passare a Dispositivi > Da sito a sito.



2. Fare clic su Add.
3. Fare clic su + per il Nodo A:


Create New VPN Topology

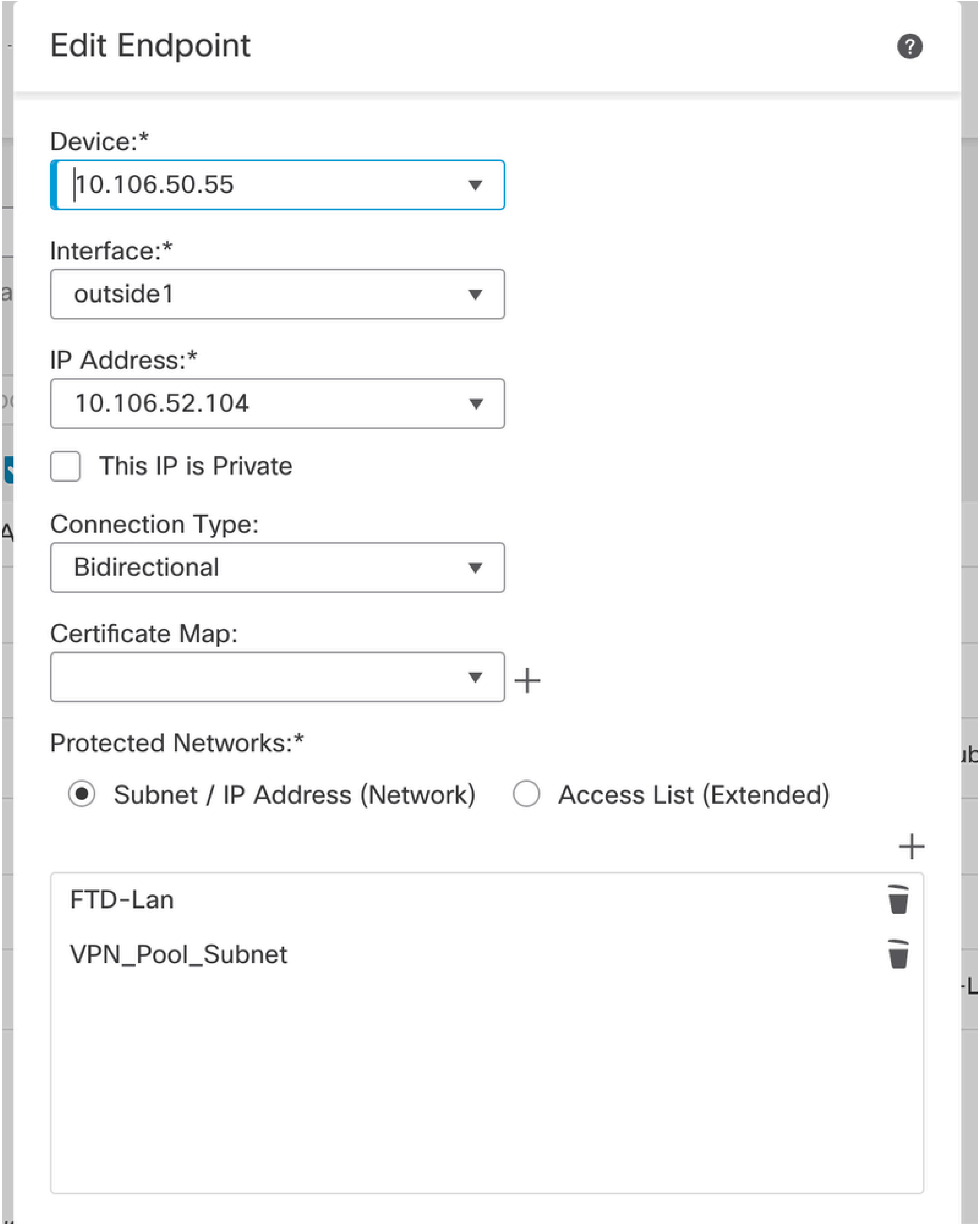
Topology Name:*

● Policy Based (Crypto Map) ○ Route Based (VTI)

Network Topology: Point to Point | Hub and Spoke | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

4. Selezionare l'FTD dal dispositivo, selezionare l'interfaccia, aggiungere la subnet locale da crittografare tramite il tunnel IPSec (in questo caso contiene anche gli indirizzi del pool VPN) e fare clic su OK.



Edit Endpoint

Device:* 10.106.50.55

Interface:* outside1

IP Address:* 10.106.52.104

□ This IP is Private

Connection Type: Bidirectional

Certificate Map:

Protected Networks:*

● Subnet / IP Address (Network) ○ Access List (Extended)

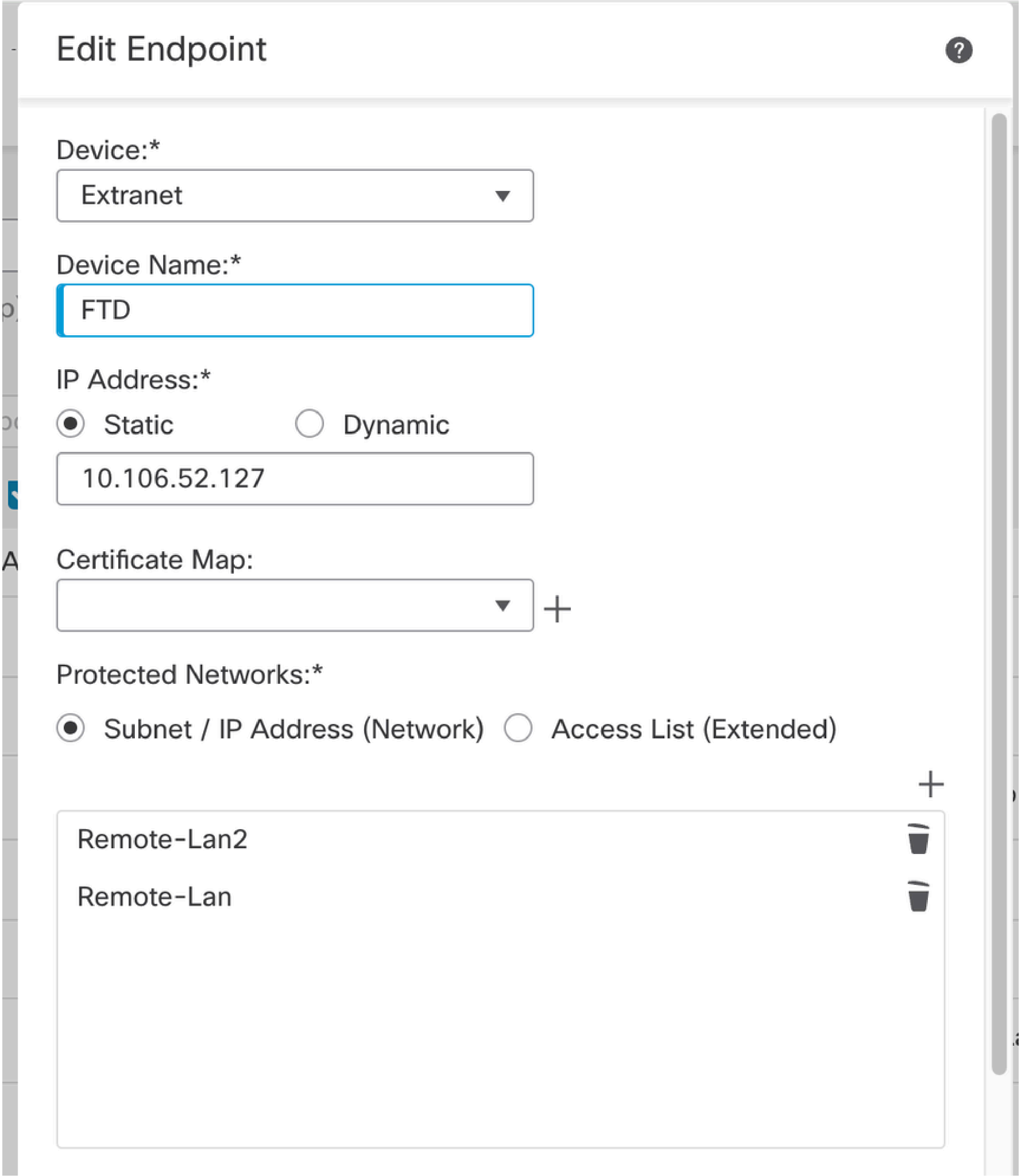
FTD-Lan

VPN_Pool_Subnet

5. Fare clic su + per il Nodo B:

> Selezionare la rete Extranet dal dispositivo e fornire il nome del dispositivo peer.

> Configurare i dettagli del peer e aggiungere la subnet remota a cui è necessario accedere tramite il tunnel VPN e fare clic su OK.



Edit Endpoint

Device:*

Extranet

Device Name:*

FTD

IP Address:*

● Static ○ Dynamic

10.106.52.127

Certificate Map:

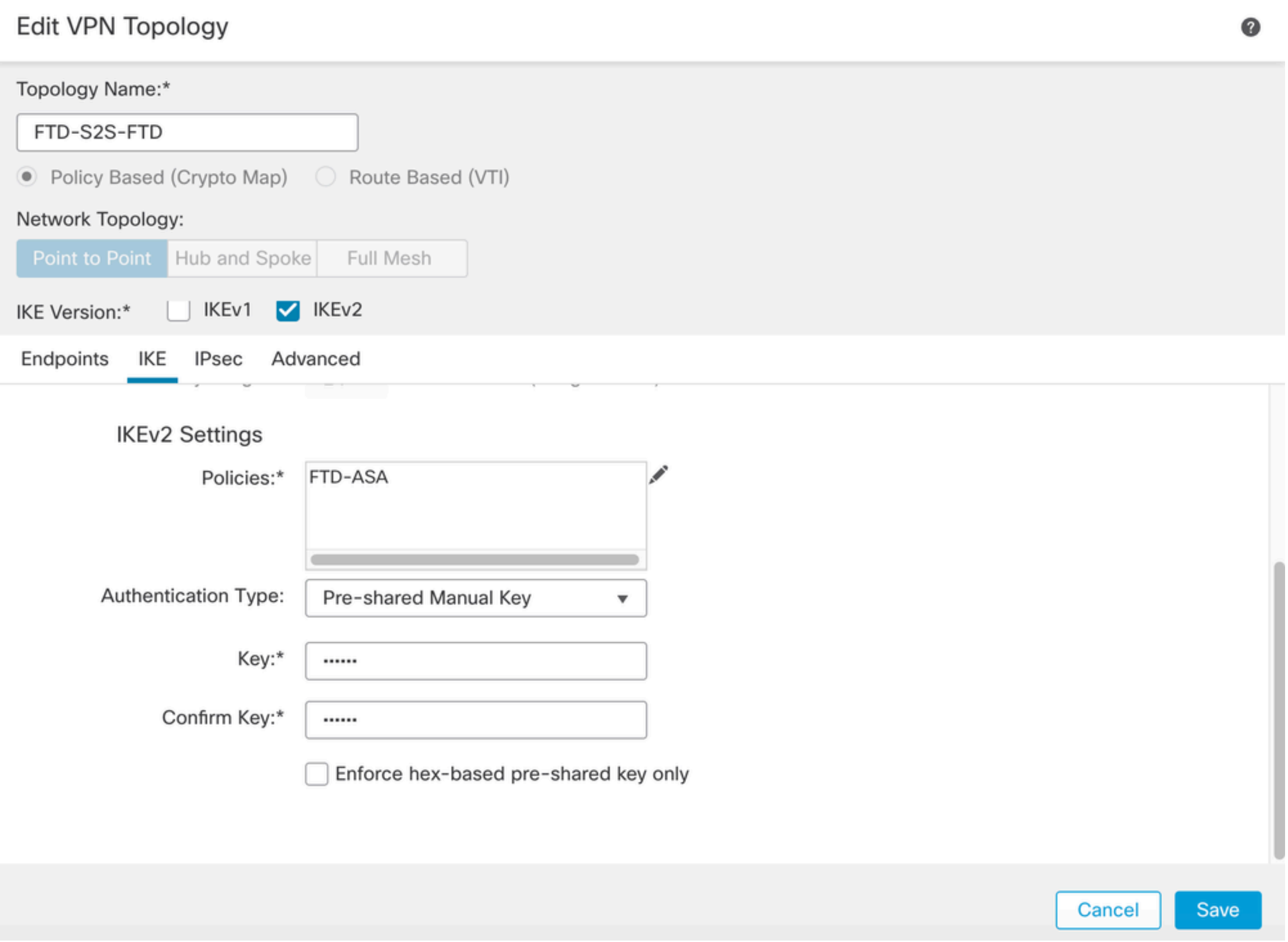
Protected Networks:*

● Subnet / IP Address (Network) ○ Access List (Extended)

Remote-Lan2

Remote-Lan

6. Fare clic sulla scheda IKE: Configurare le impostazioni IKEv2 in base alle proprie esigenze



Edit VPN Topology

Topology Name:* FTD-S2S-FTD

● Policy Based (Crypto Map) ○ Route Based (VTI)

Network Topology: Point to Point | Hub and Spoke | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

IKEv2 Settings

Policies:* FTD-ASA

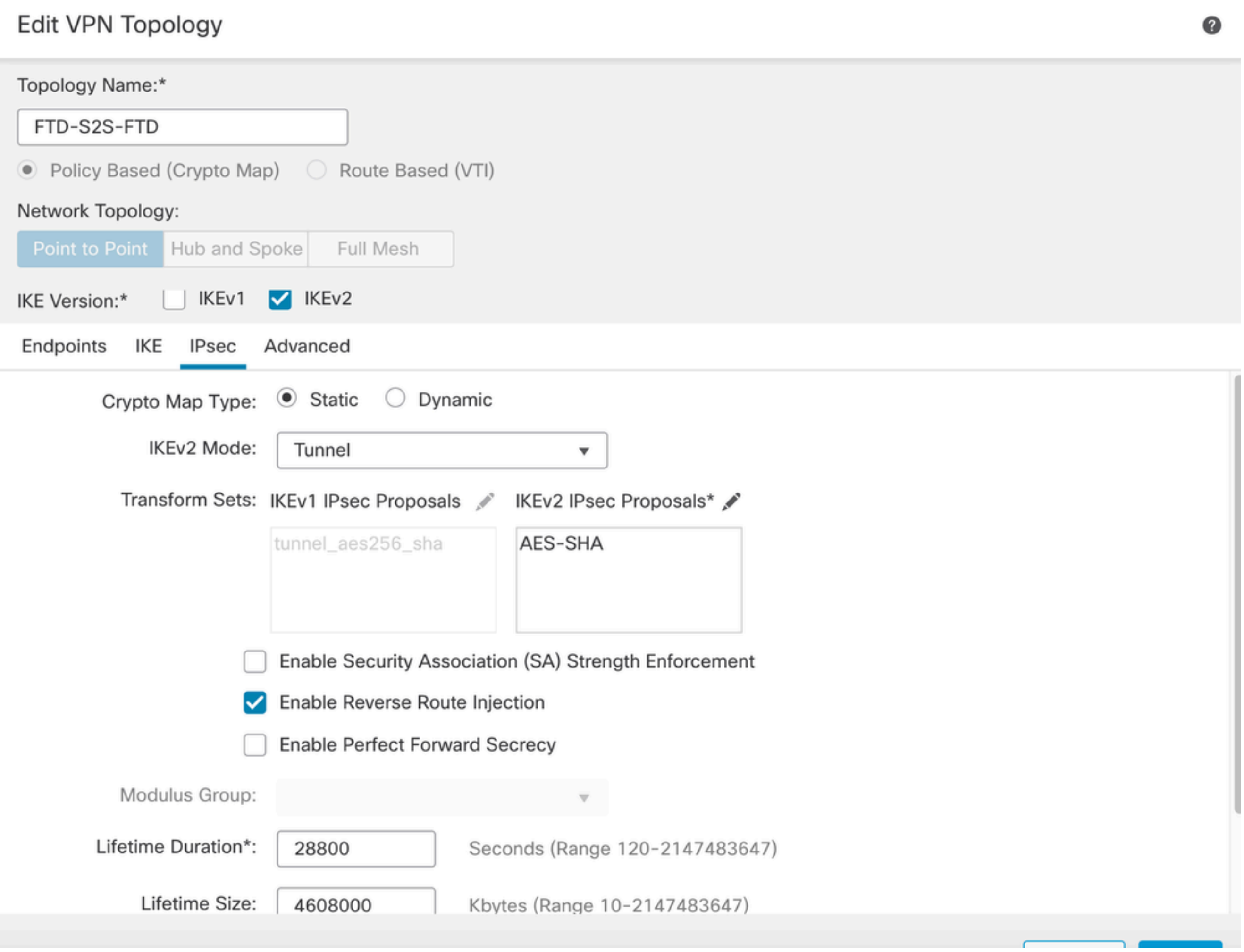
Authentication Type: Pre-shared Manual Key

Key:* ••••••

Confirm Key:* ••••••

□ Enforce hex-based pre-shared key only

7. Fare clic sulla scheda IPSec: Configurare le impostazioni IPSec in base alle proprie esigenze.



Edit VPN Topology

Topology Name:*

FTD-S2S-FTD

● Policy Based (Crypto Map) ○ Route Based (VTI)

Network Topology:

Point to Point | Hub and Spoke | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Endpoints | IKE | IPsec | Advanced

Crypto Map Type: ● Static ○ Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals: tunnel_aes256_sha; IKEv2 IPsec Proposals*: AES-SHA

□ Enable Security Association (SA) Strength Enforcement

☑ Enable Reverse Route Injection

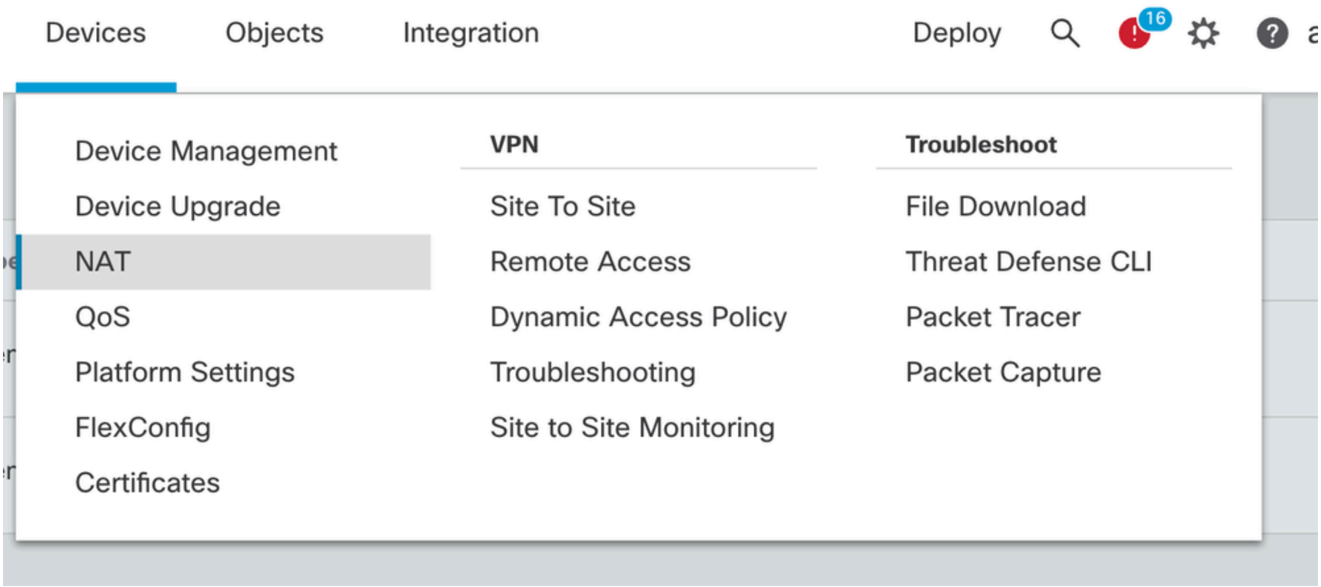
□ Enable Perfect Forward Secrecy

Modulus Group:

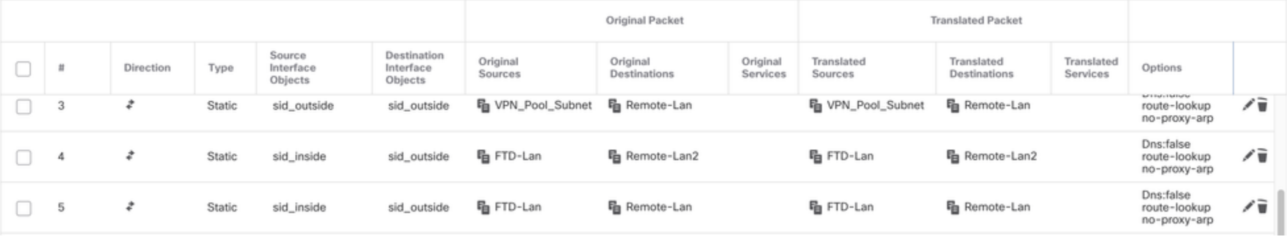
Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

8. Configurare Nat-Exempt per il traffico interessante (facoltativo)
   Fare clic su Devices > NAT



9. Il protocollo NAT qui configurato consente a RAVPN e agli utenti interni di accedere ai server tramite il tunnel IPSec da sito a sito.



						Original Packet			Translated Packet				
□	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
□	3	⇄	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		Dns:false 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. Analogamente, viene visualizzata la configurazione sull'altra estremità peer per il tunnel S2S.

    NOTA: l'ACL crittografico o le subnet del traffico interessanti devono essere copie mirror l'una dell'altra su entrambi i peer.

Verifica

1. Per verificare la connessione RAVPN:

<#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. Per verificare la connessione IKEv2:

<#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. Per verificare la connessione IPSec:

<#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
```

Risoluzione dei problemi

1. Per risolvere i problemi di connessione con AnyConnect, raccogliere il pacchetto dardi o abilitare i debug di AnyConnect.
2. Per risolvere i problemi del tunnel IKEv2, utilizzare i seguenti debug:

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

3. Per risolvere il problema del traffico sull'FTD, acquisire i pacchetti e controllare la configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l&rsquo;accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).