配置AnyConnect以通过IPSec隧道访问服务器。

目录

简介：

本文档介绍在由FMC管理的FTD上部署RAVPN设置以及在FTD之间部署站点到站点隧道的过程。

先决条件:

基本要求

- 对站点到站点VPN和RAVPN的基本了解是有益的。
- 了解在Cisco Firepower平台上配置基于IKEv2策略的隧道的基础知识至关重要。

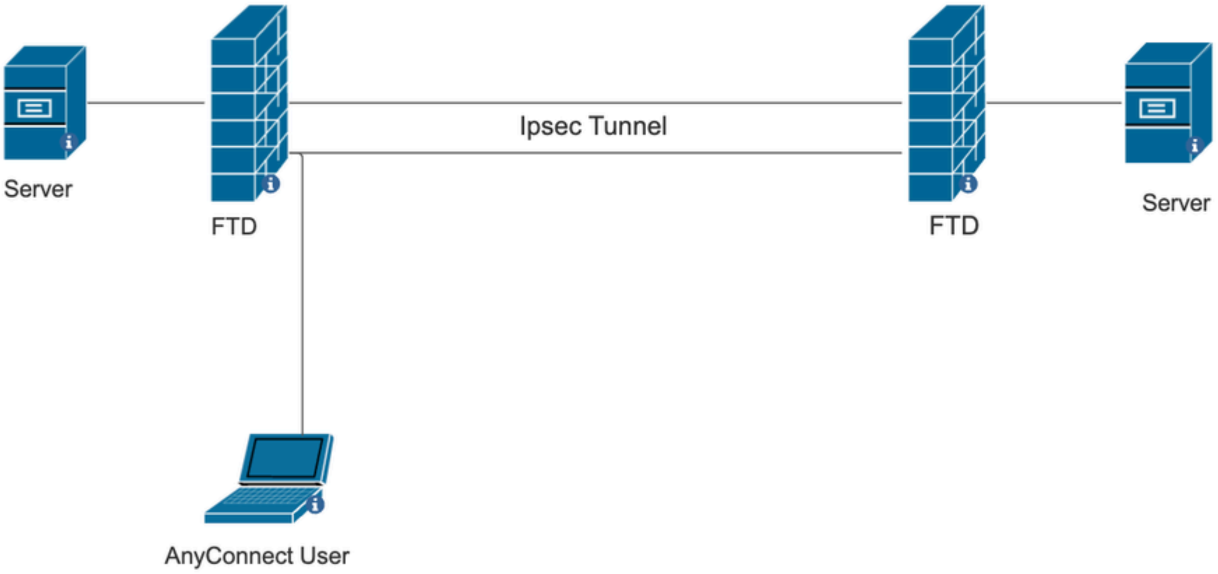
此过程适用于在由FMC管理的FTD上部署RAVPN设置，并在FTD之间部署站点到站点隧道，其中AnyConnect用户可以访问其他FTD对等体后面的服务器。

使用的组件

- 适用于VMware的Cisco Firepower威胁防御：版本7.0.0
- Firepower管理中心：版本7.2.4（内部版本169）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。.

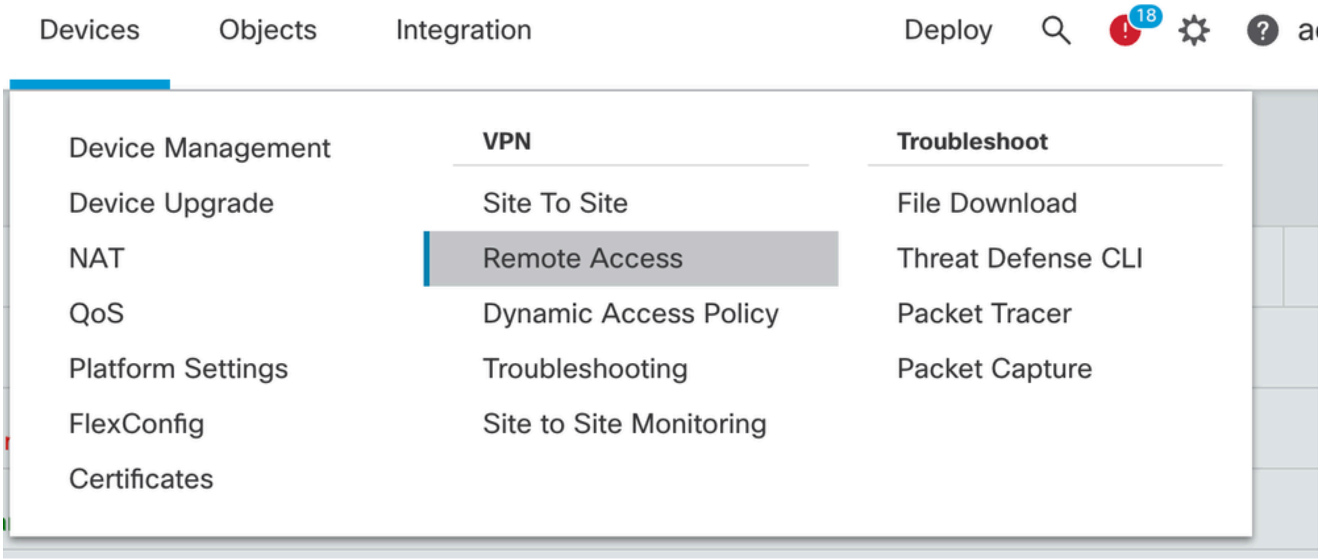
网络图



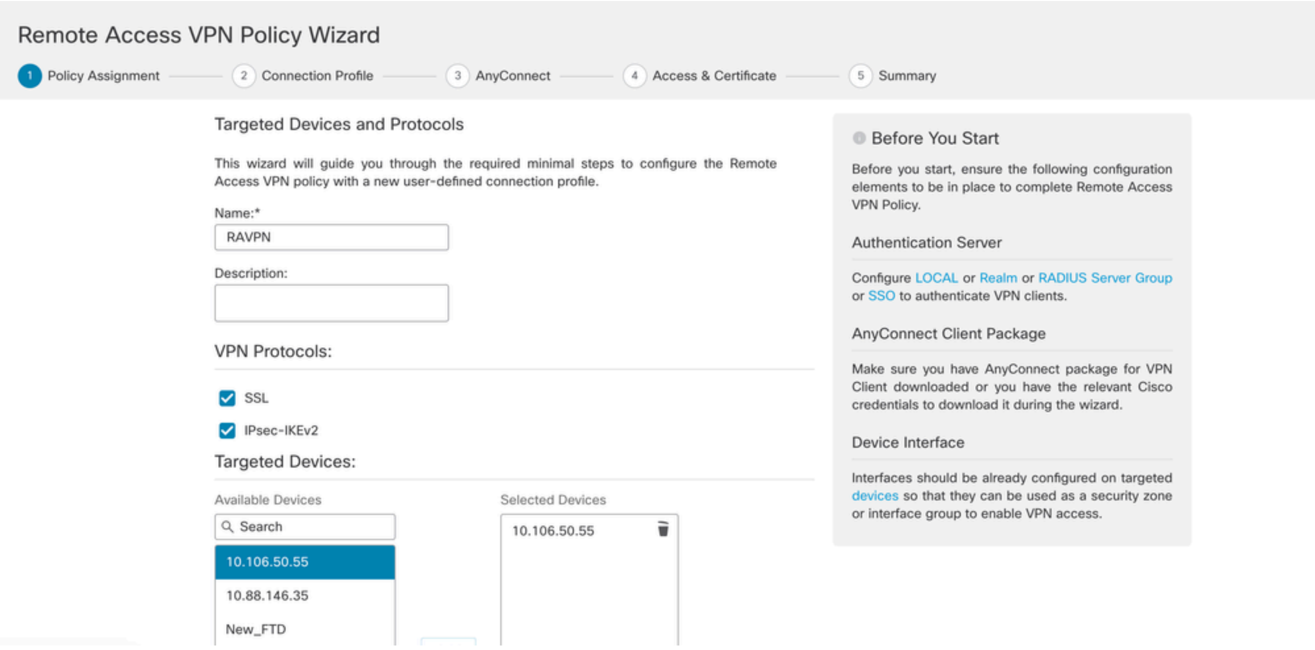
FMC上的配置

FMC管理的FTD上的RAVPN配置。

1. 导航到设备>远程访问。



2. 单击 Add。
3. 配置名称并从可用设备中选择FTD，然后单击Next。



Remote Access VPN Policy Wizard

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

Search

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

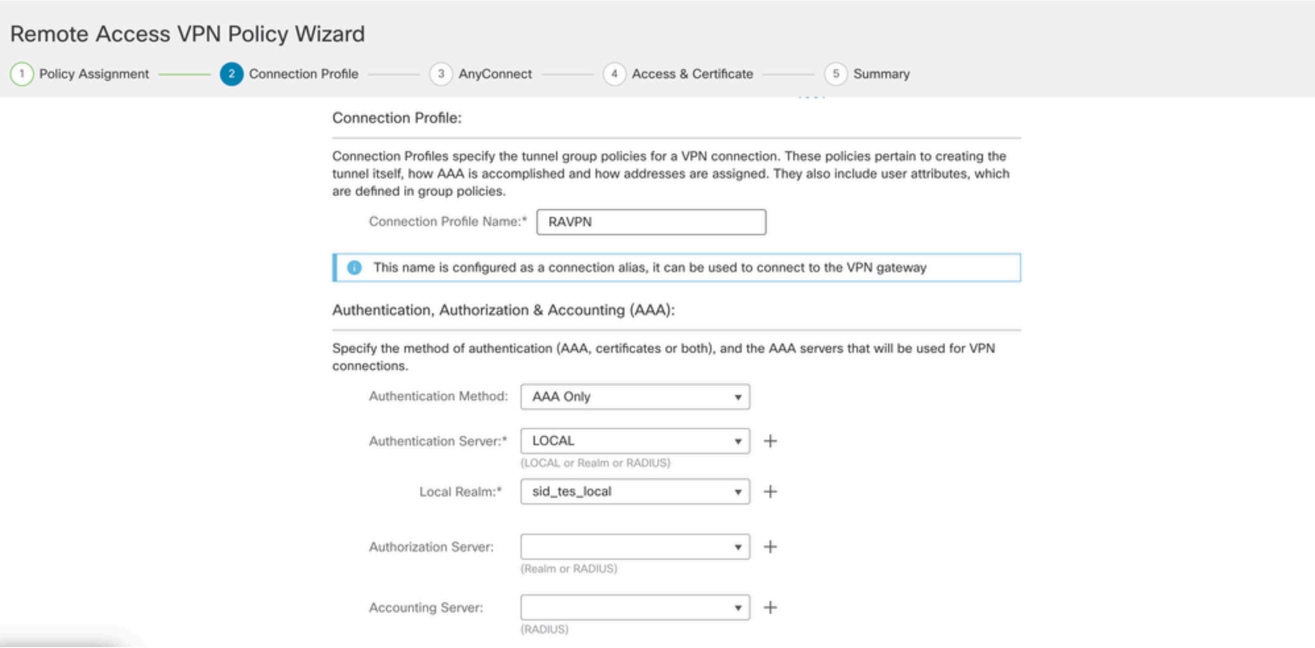
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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. 配置连接配置文件名称并选择身份验证方法。

   注意：对于此配置示例，我们使用仅AAA和本地身份验证。但是，请根据您的要求进行配置。



Remote Access VPN Policy Wizard

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

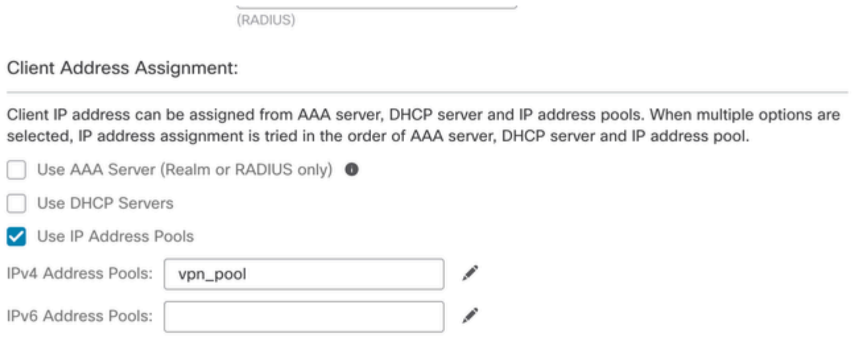
Authentication Server:* LOCAL (LOCAL or Realm or RADIUS)

Local Realm:* sid_tes_local

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

5. 配置用于AnyConnect的IP地址分配的VPN池。



(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)

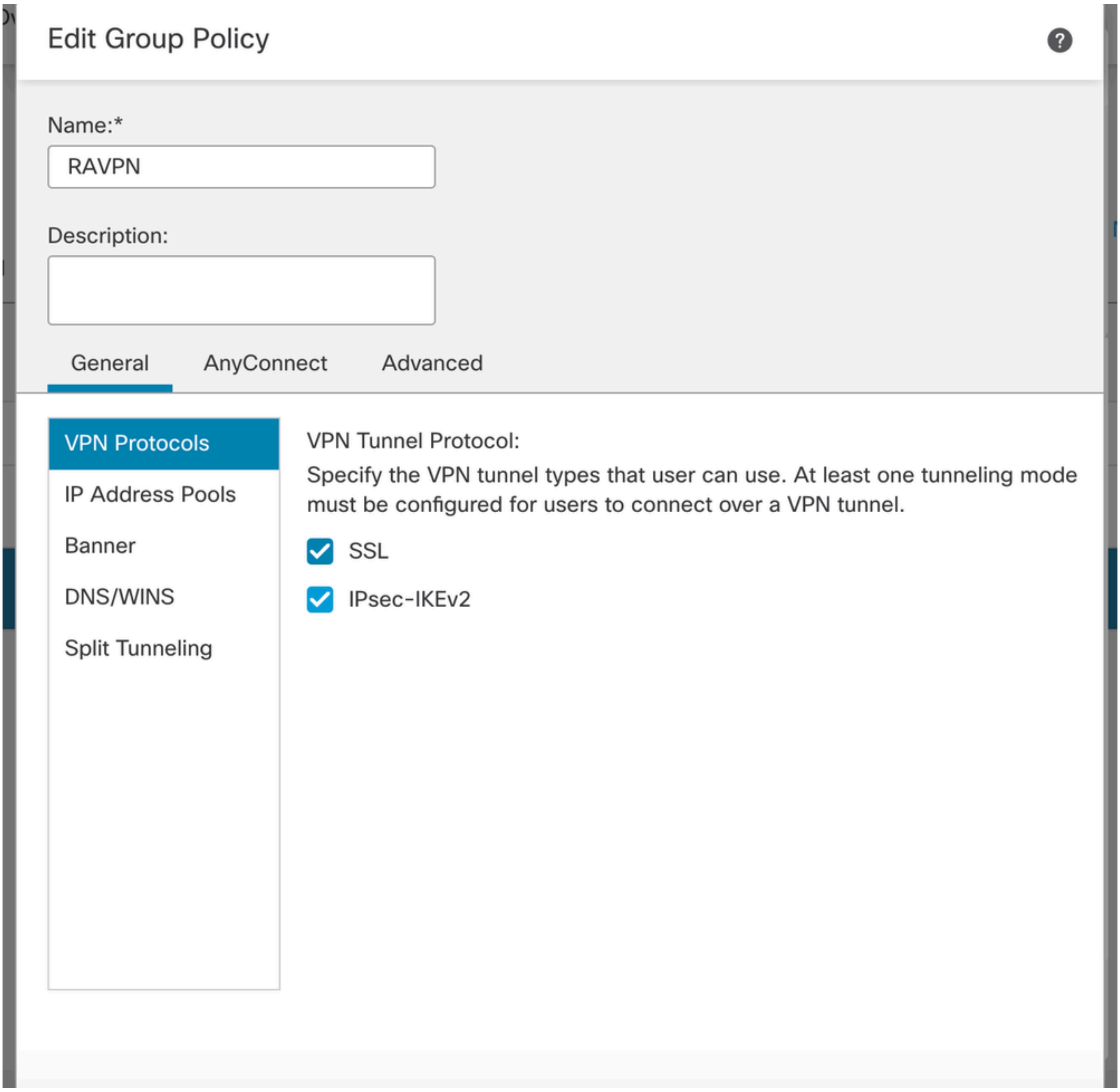
□ Use DHCP Servers

☑ Use IP Address Pools

IPv4 Address Pools: vpn_pool

IPv6 Address Pools:

6. 创建组策略。单击+以创建组策略。添加组策略的名称。



Edit Group Policy

Name:* RAVPN

Description:

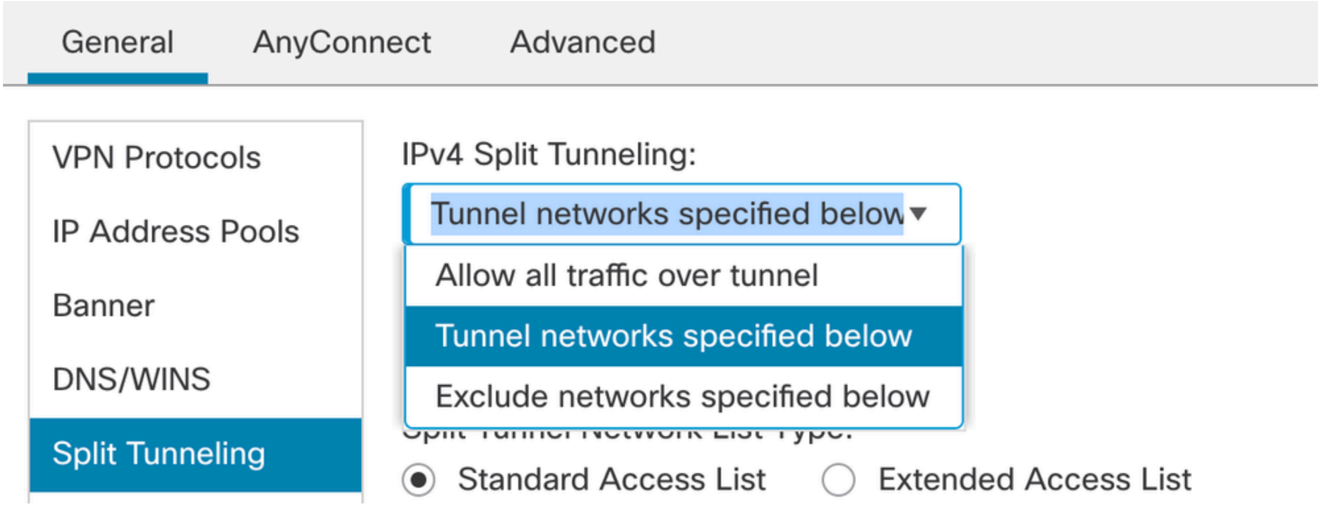
VPN Tunnel Protocol:

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. 转到Split tunneling。选择此处指定的Tunnel networks：

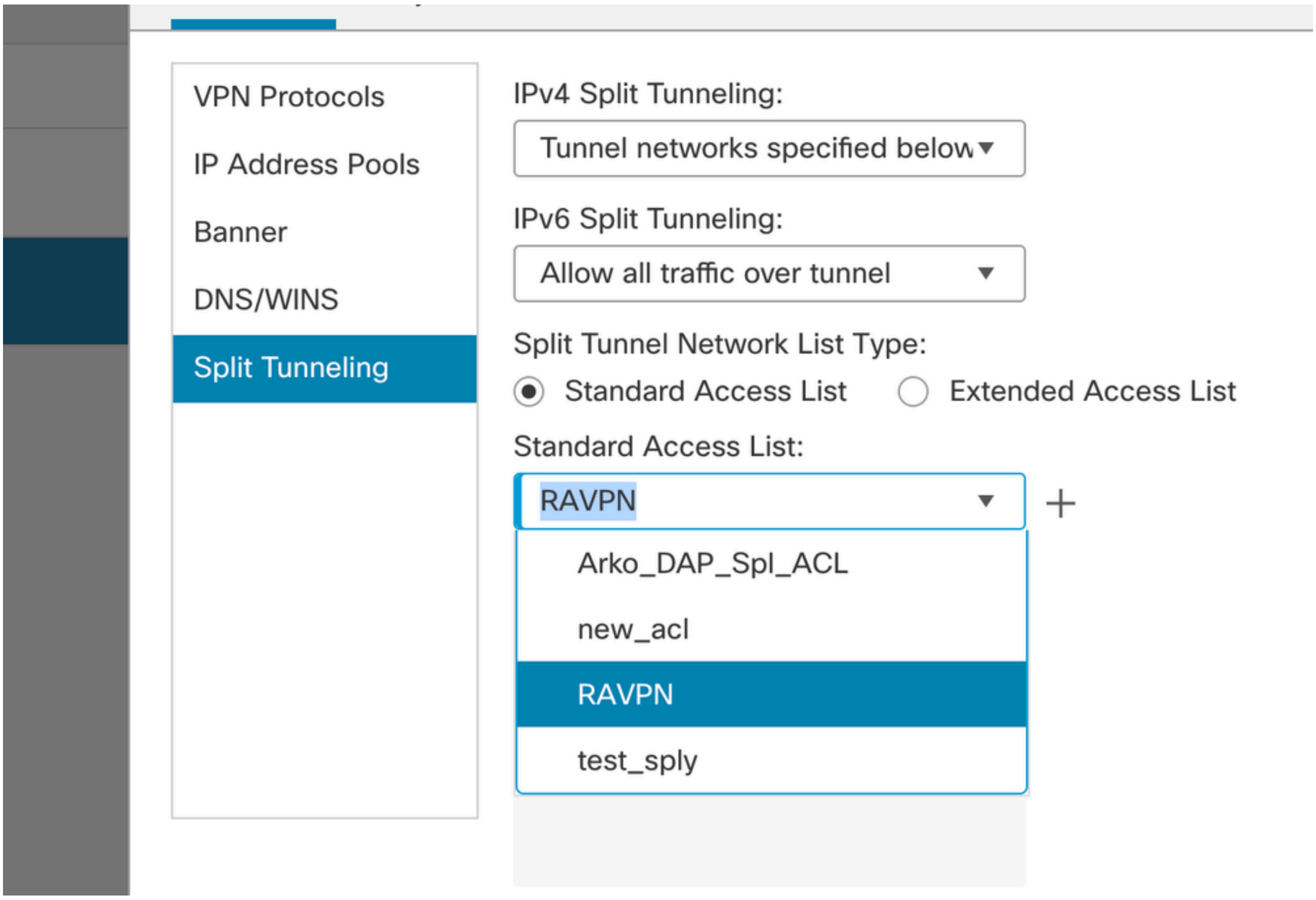

General
AnyConnect
Advanced
VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling
Allow all traffic over tunnel
Tunnel networks specified below
Exclude networks specified below

IPv4 Split Tunneling: Tunnel networks specified below

Split Tunnel Network List Type:

● Standard Access List ○ Extended Access List

8. 从下拉列表中选择正确的访问列表。如果尚未配置ACL：点击+图标添加标准访问列表并创建一个新访问列表。
   Click Save.



IPv4 Split Tunneling: Tunnel networks specified below

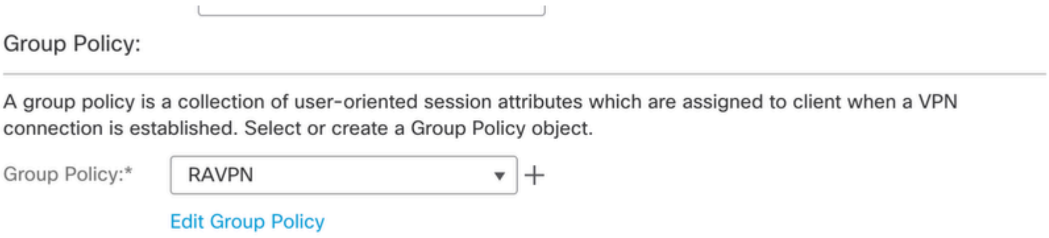
IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type:

● Standard Access List ○ Extended Access List

Standard Access List: RAVPN

9. 选择已添加的组策略，然后单击Next。



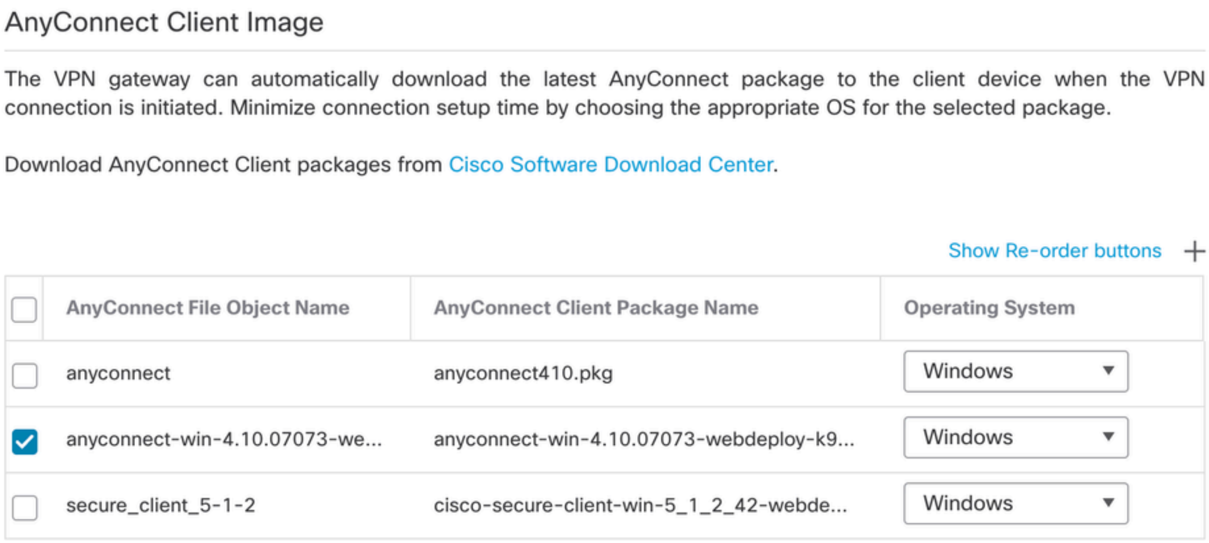
Group Policy:

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 ▾ +

Edit Group Policy

10. 选择AnyConnect映像。



AnyConnect Client Image

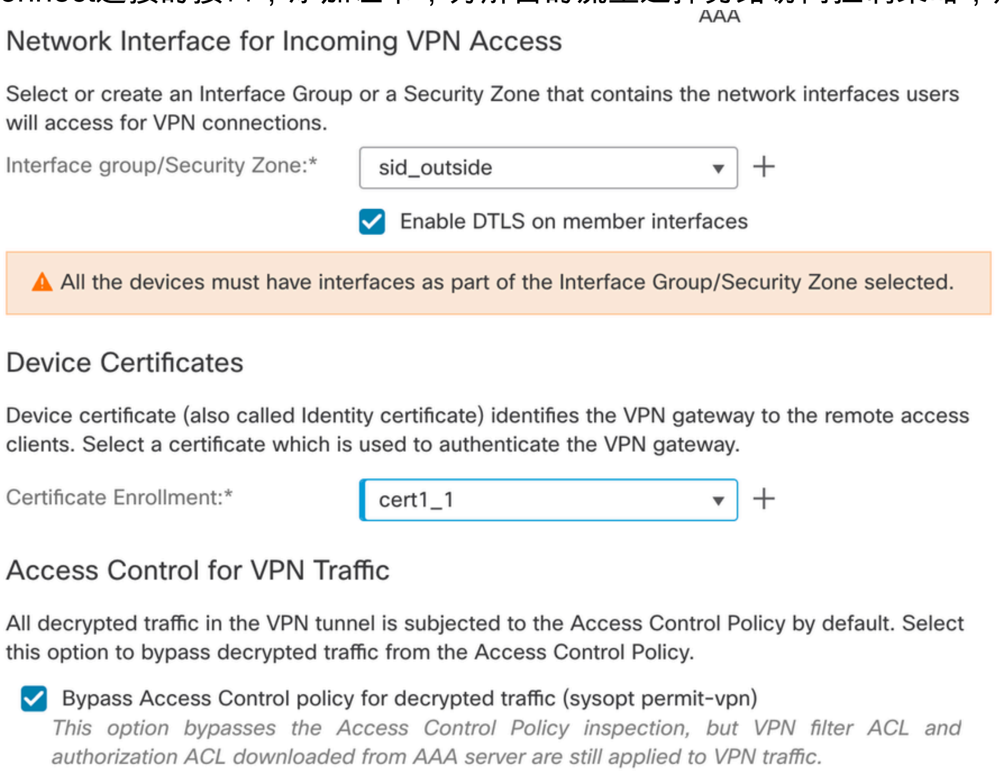
The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from Cisco Software Download Center.

Show Re-order buttons +

□	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. 选择必须启用AnyConnect连接的接口，添加证书，为解密的流量选择旁路访问控制策略，然后单击Next。



AAA

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 ▾ +

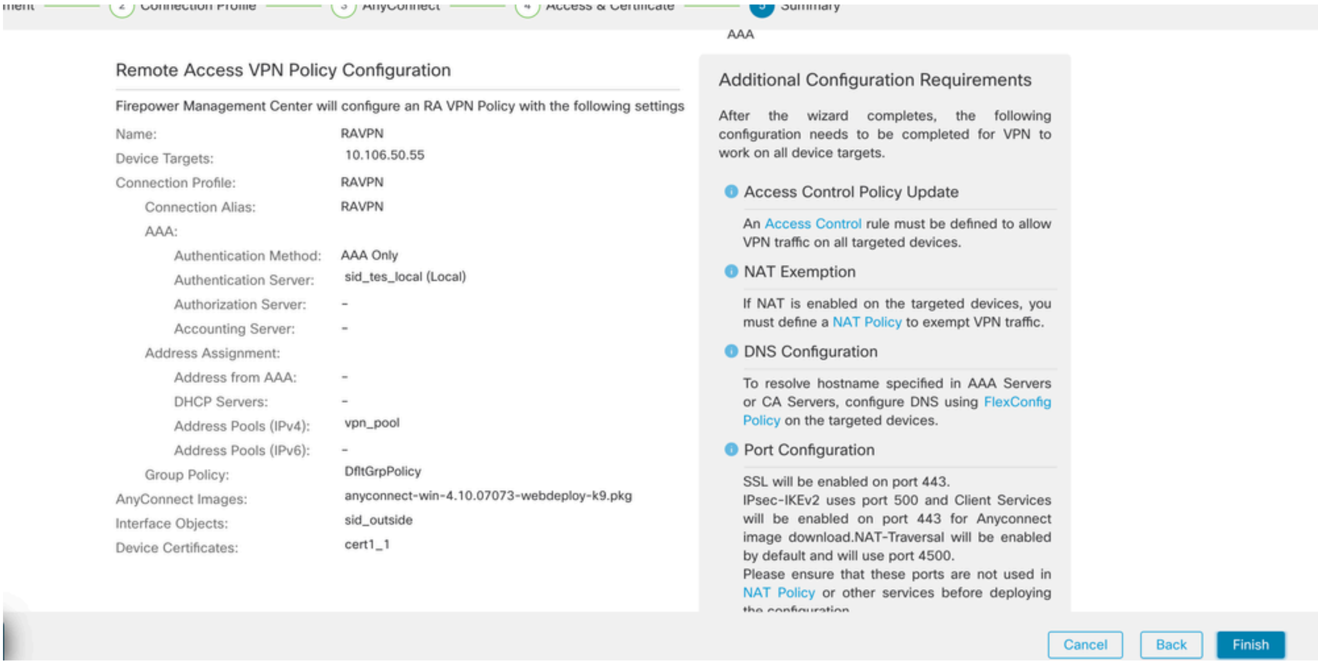
Access Control for VPN Traffic

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. 检查配置并单击Finish。



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.

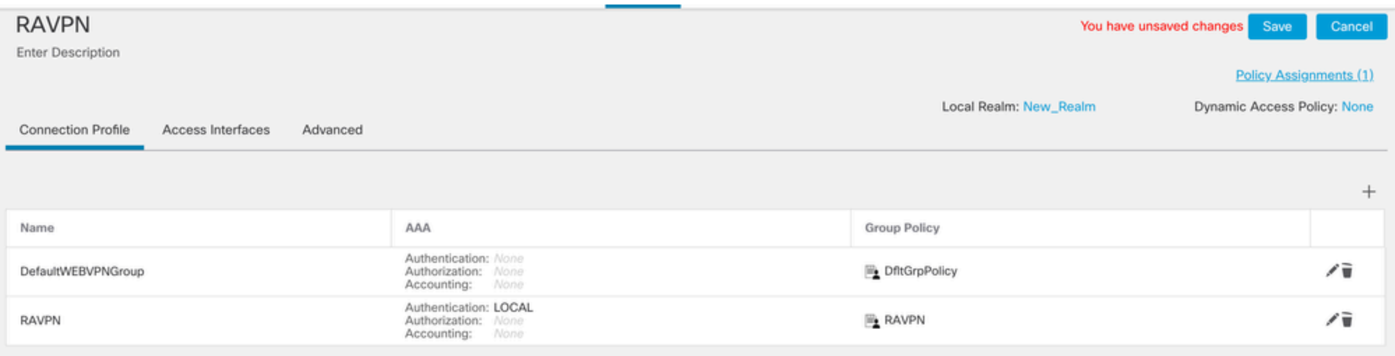
DNS Configuration

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. 单击Save和Deploy。



RAVPN

Enter Description

You have unsaved changes

Policy Assignments (1)

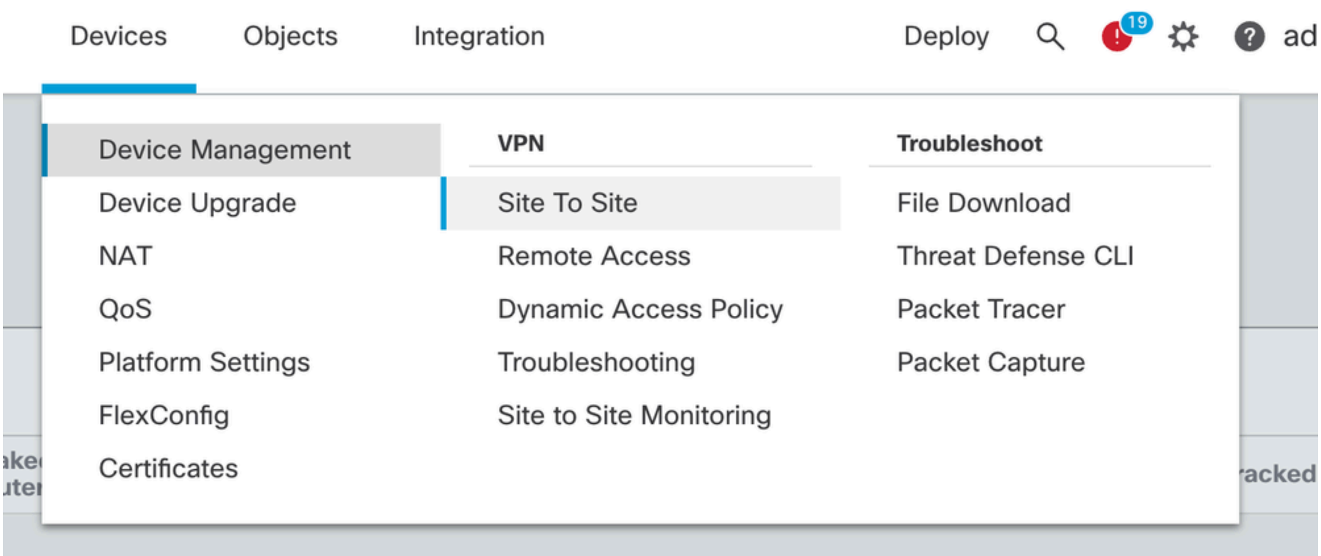
Local Realm: New_Realm

Dynamic Access Policy: None

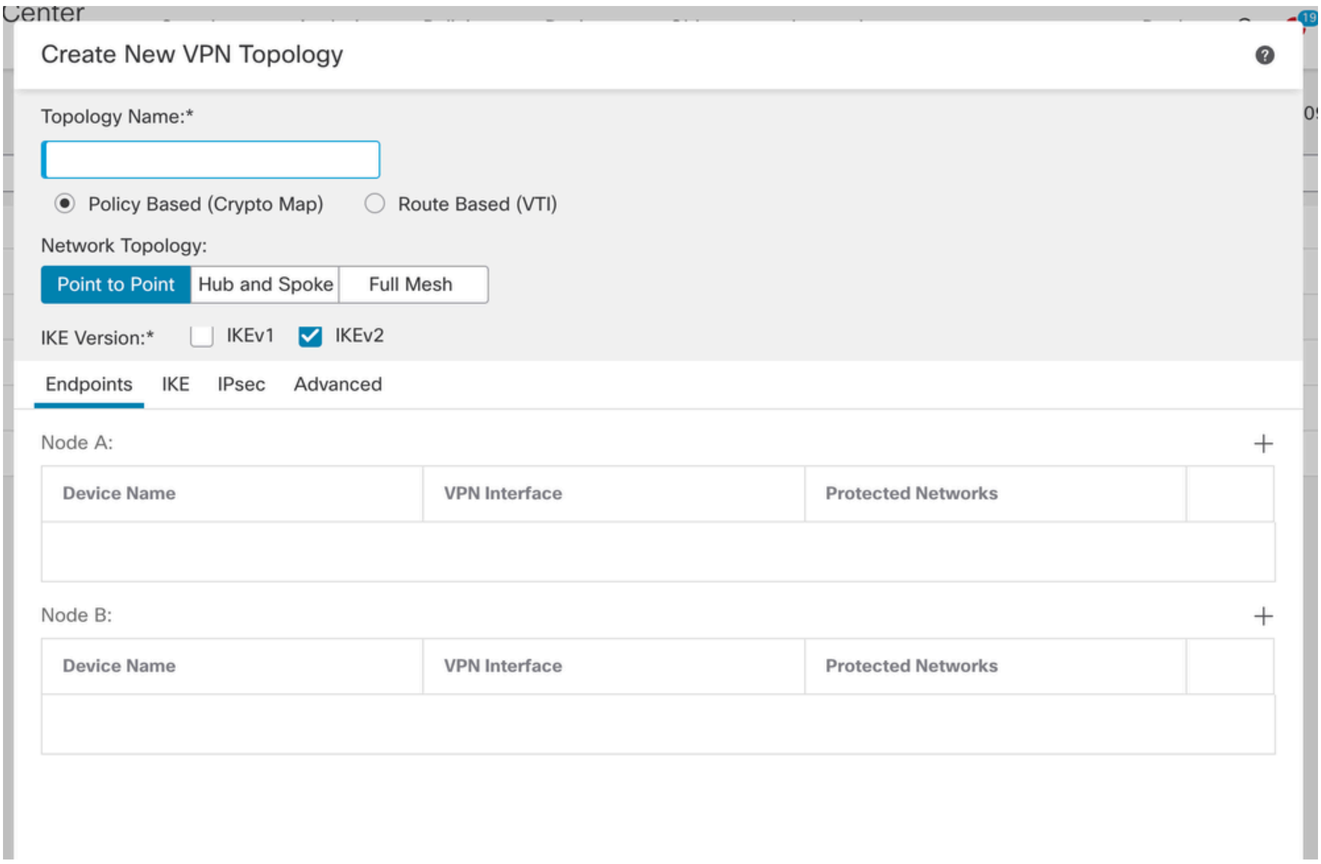
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN	

FTD上的IKEv2 VPN由FMC管理：

1. 导航到设备>站点到站点。



2. 单击 Add。
3. 对于节点A，点击+：


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

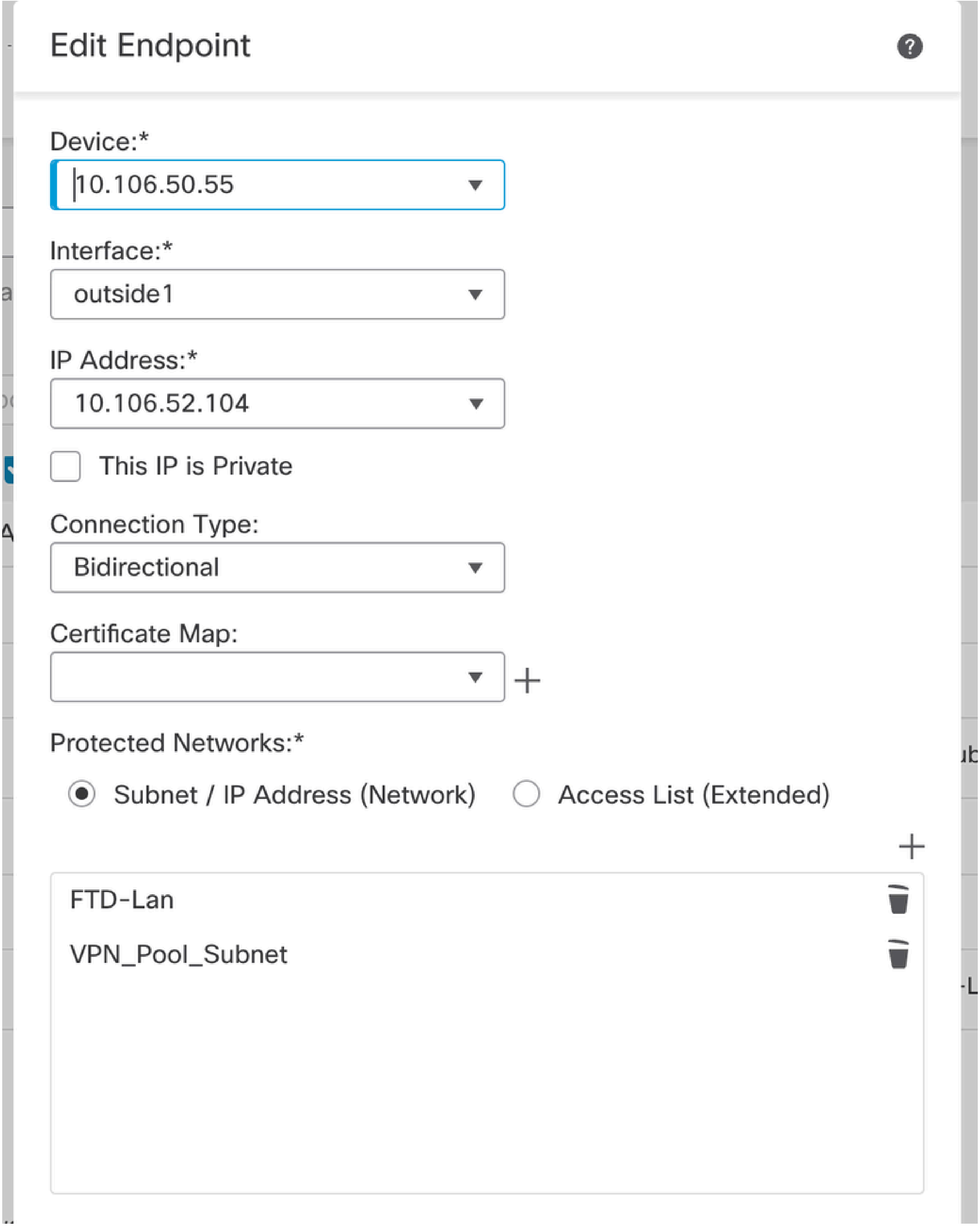
Node A: +

Device Name	VPN Interface	Protected Networks	

Node B: +

Device Name	VPN Interface	Protected Networks	

4. 从Device中选择FTD，选择接口，添加必须通过IPSec隧道加密的本地子网（在本例中还包含VPN池地址），并单击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)

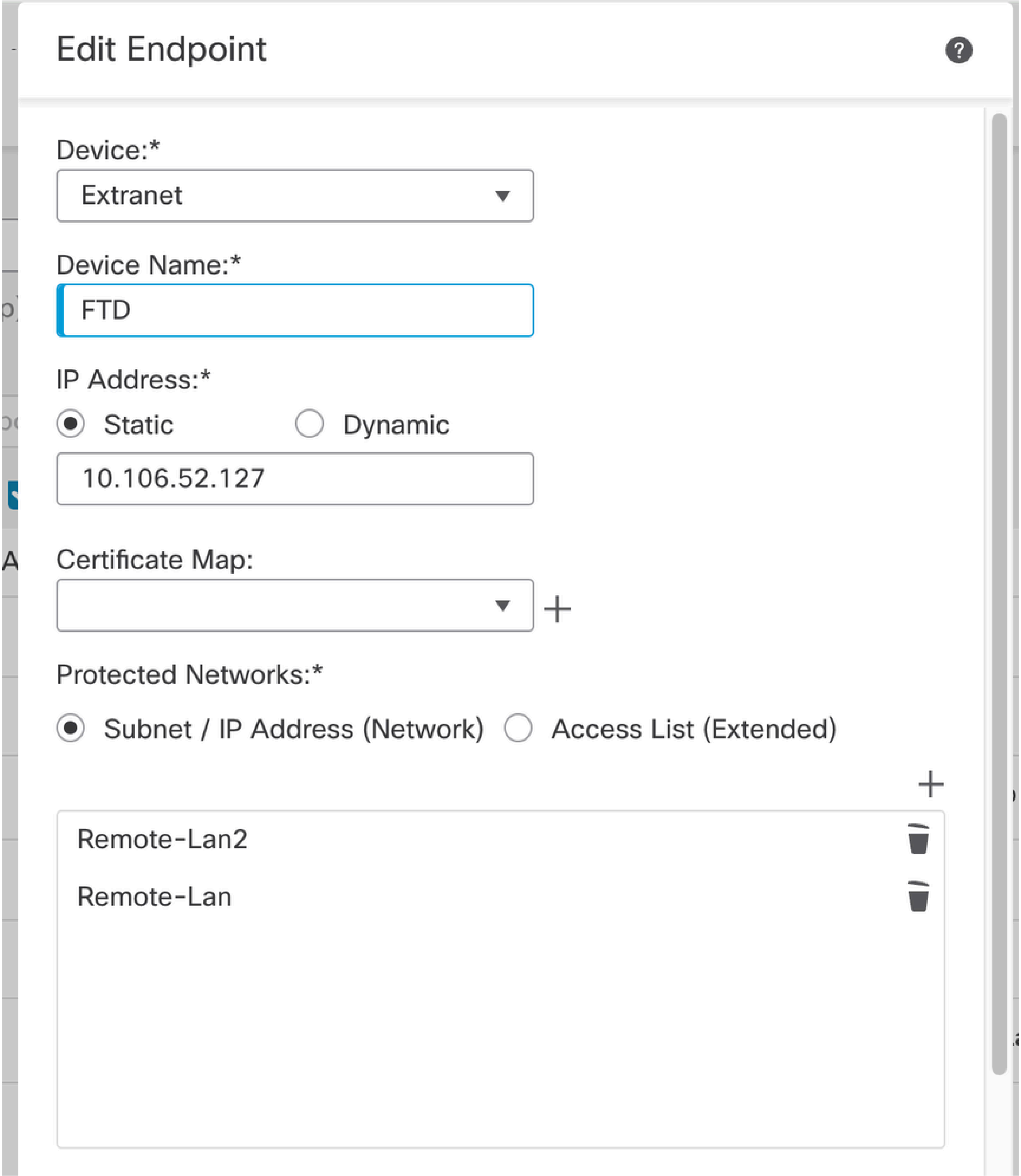
FTD-Lan

VPN_Pool_Subnet

5. 对于节点B，点击+：

> Select the Extranet from the Device， and give the Name of the peer Device。

>配置对等体详细信息并添加需要通过VPN隧道访问的远程子网，然后单击OK。



Edit Endpoint

Device:*

Extranet

Device Name:*

FTD

IP Address:*

● Static ○ Dynamic

10.106.52.127

Certificate Map:

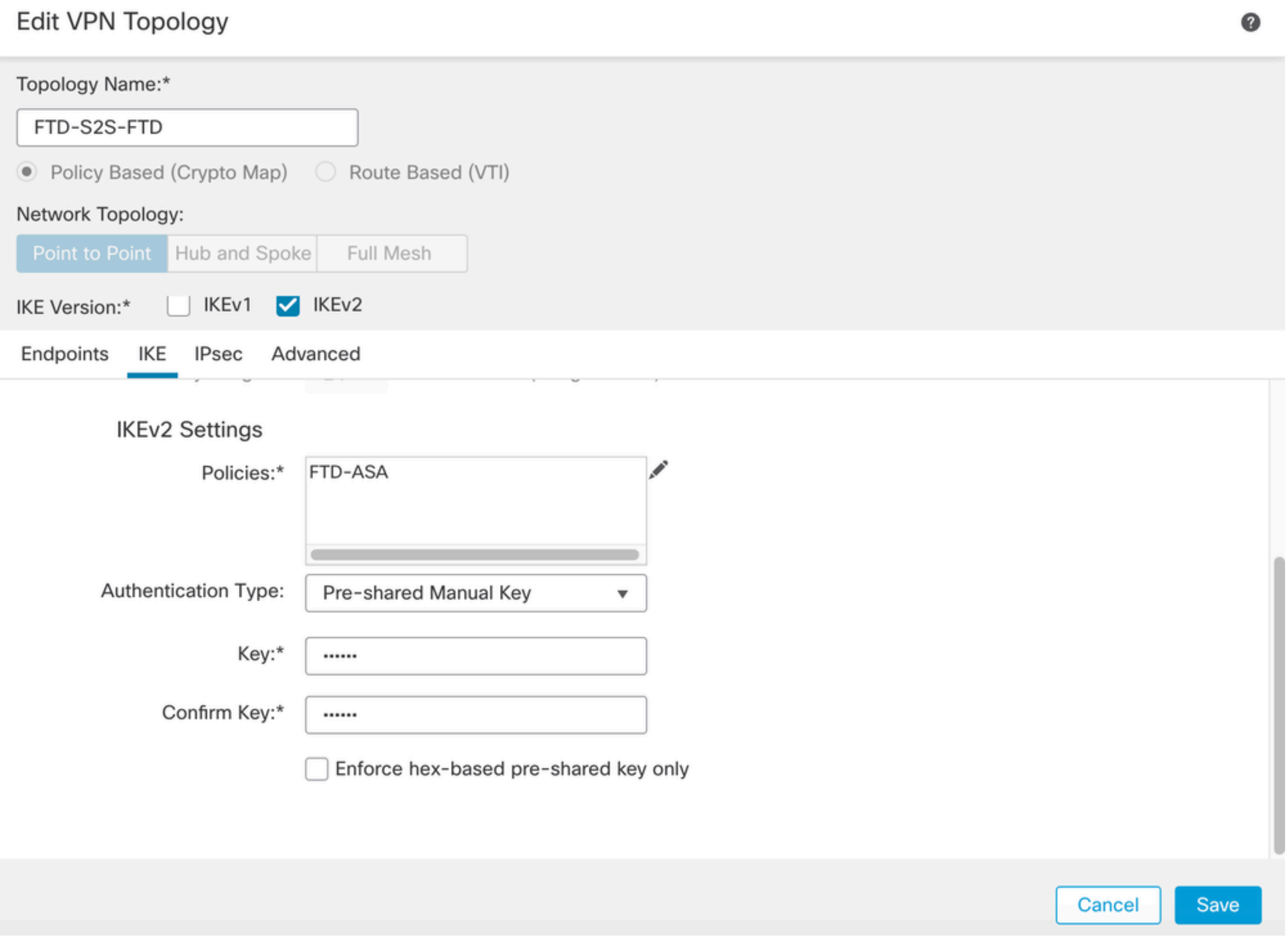
Protected Networks:*

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

Remote-Lan2

Remote-Lan

6. 点击IKE选项卡：根据要求配置IKEv2设置


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

IKEv2 Settings

Policies:* FTD-ASA

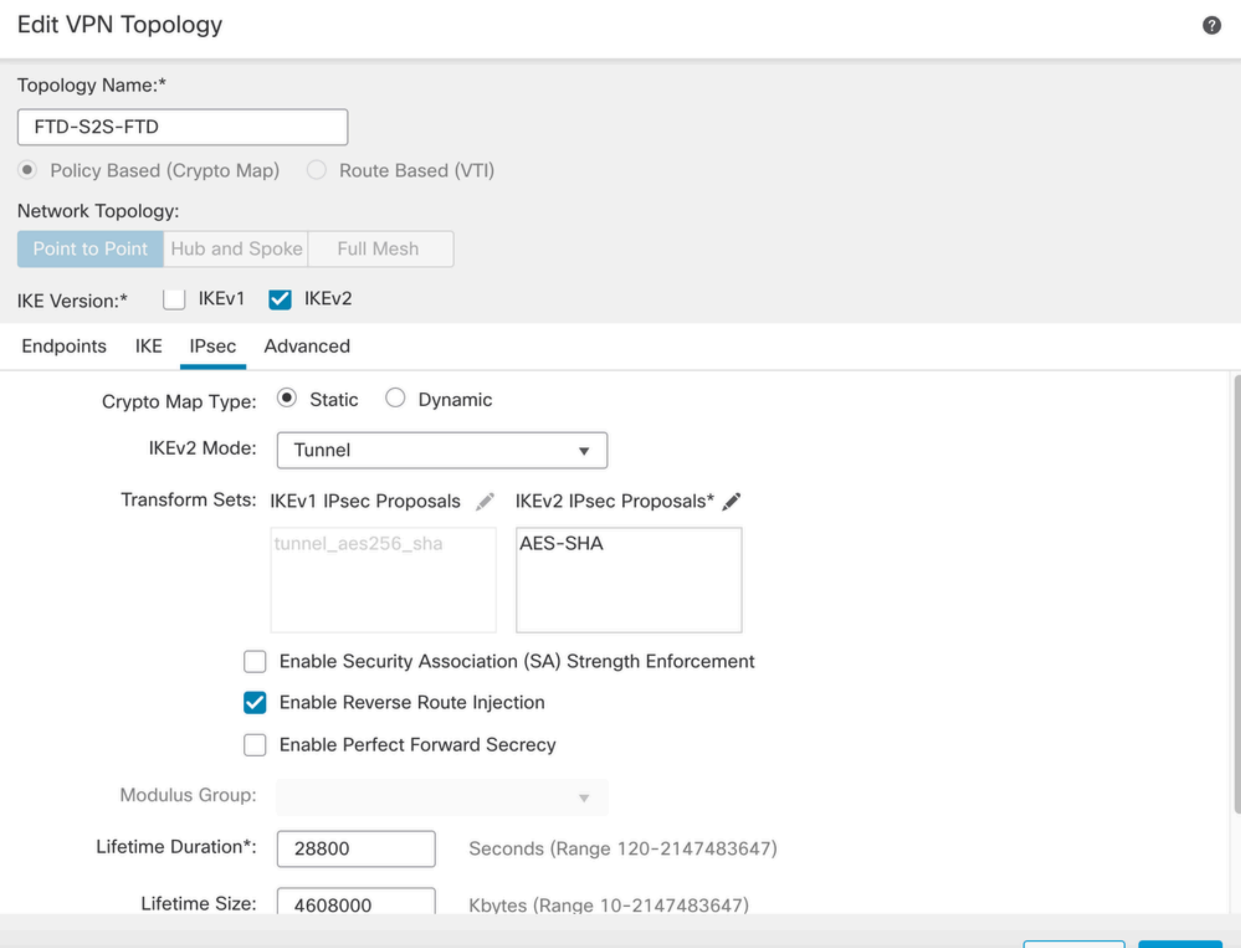
Authentication Type: Pre-shared Manual Key

Key:* ••••••

Confirm Key:* ••••••

□ Enforce hex-based pre-shared key only

7. 单击IPsec选项卡：根据需要配置IPSec设置。



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

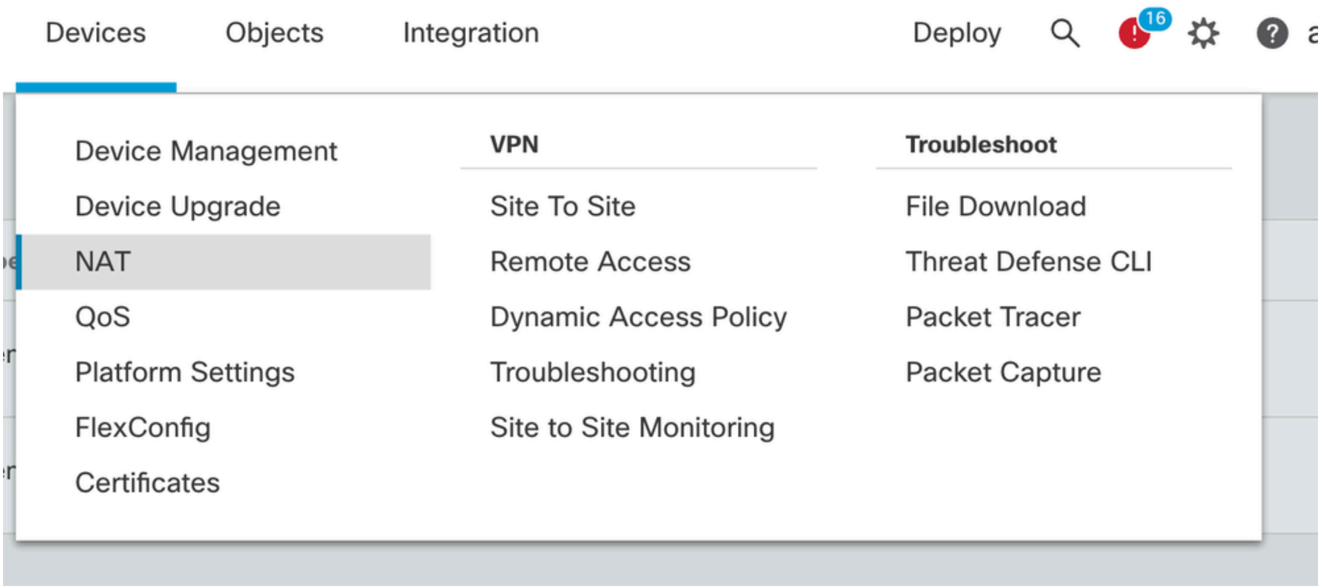
□ Enable Perfect Forward Secrecy

Modulus Group:

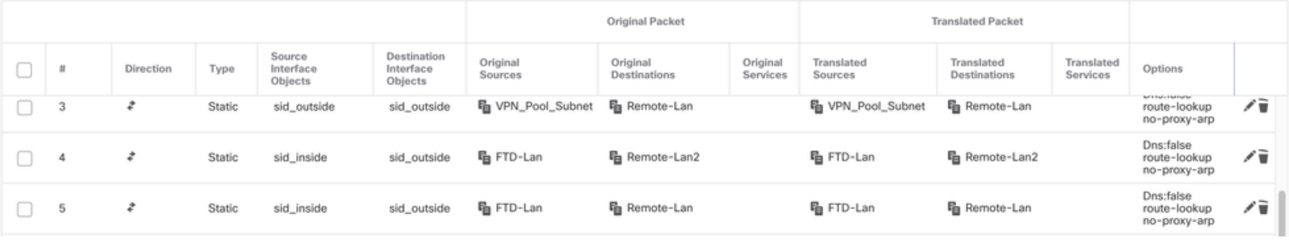
Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

8. 为相关流量配置Nat-Exempt（可选）
单击Devices > NAT



9. 此处配置的NAT允许RAVPN和内部用户通过S2S IPSec隧道访问服务器。



						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		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. 同样地，在另一个对等端上进行配置以启用S2S隧道。

    注意：加密ACL或相关流量子网必须是对等体上彼此的镜像副本。

验证

1. 要验证RAVPN连接，请执行以下操作：

<#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. 要验证IKEv2连接，请执行以下操作：

<#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. 要验证IPSec连接，请执行以下操作：

<#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
```

故障排除

1. 要排除AnyConnect连接故障，请收集DART捆绑包或启用AnyConnect调试。
2. 要排除IKEv2隧道故障，请使用以下调试：

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

3. 要排除FTD上的流量问题，请捕获数据包并检查配置。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。