IPSecトンネルを介してアクセスサーバにAnyConnectを設定します。

内容

概要：

このドキュメントでは、FMCによって管理されるFTDと、FTD間のサイト間トンネルにRAVPN設定を展開する手順について説明します。

前提条件

基本的な要件

- サイト間VPNとRAVPNの基本的な知識があれば役に立ちます。
- Cisco FirepowerプラットフォームでIKEv2ポリシーベースのトンネルを設定するための基礎を理解することが不可欠です。

この手順では、FMCによって管理されるFTD上にRAVPN設定を展開し、FTD間にサイト間トンネルを展開します。このトンネルでは、AnyConnectユーザが他のFTDピアの背後にあるサーバにアクセスできます。

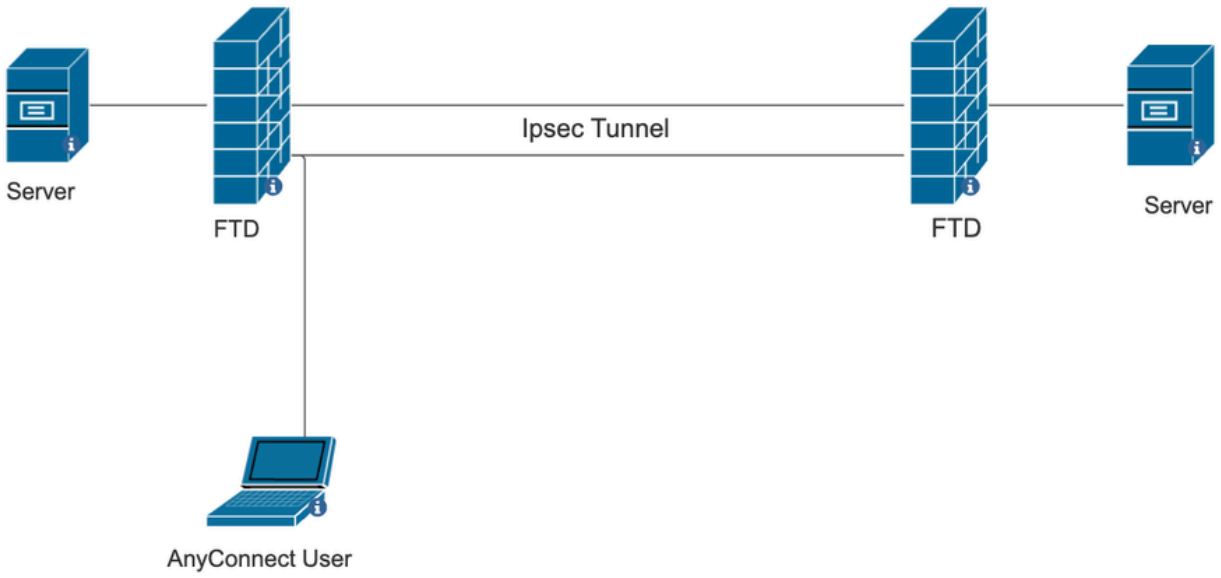
使用するコンポーネント

- VMware向けCisco Firepower Threat Defense：バージョン7.0.0
- Firepower Management Center：バージョン7.2.4（ビルド169）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作

業してください。

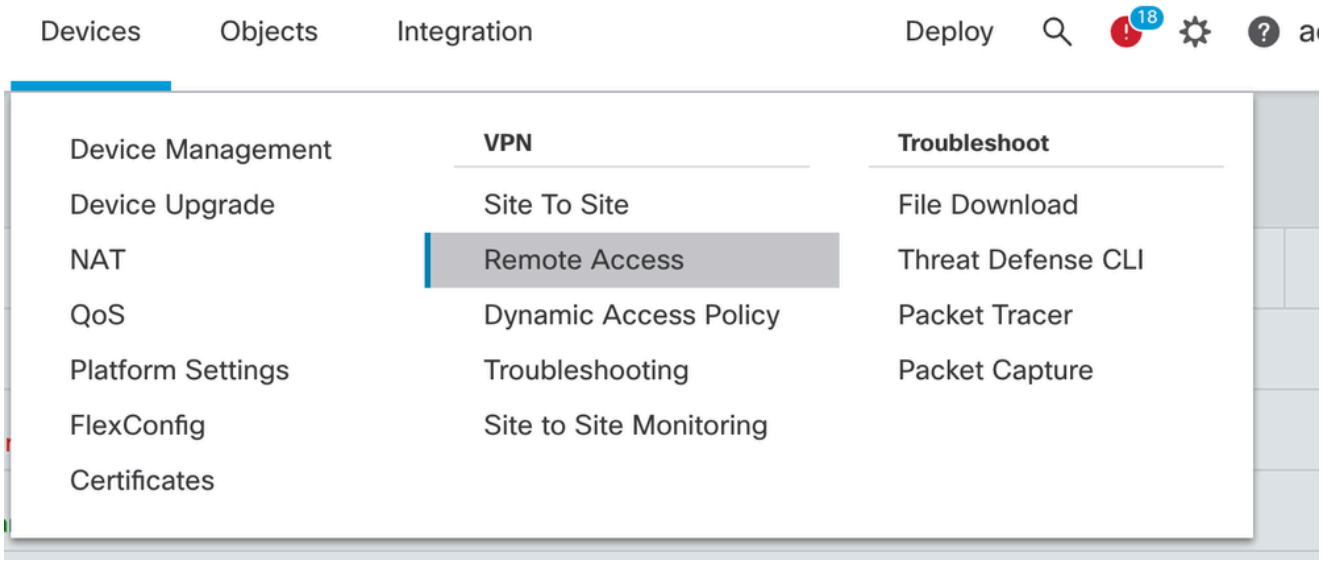
ネットワーク図



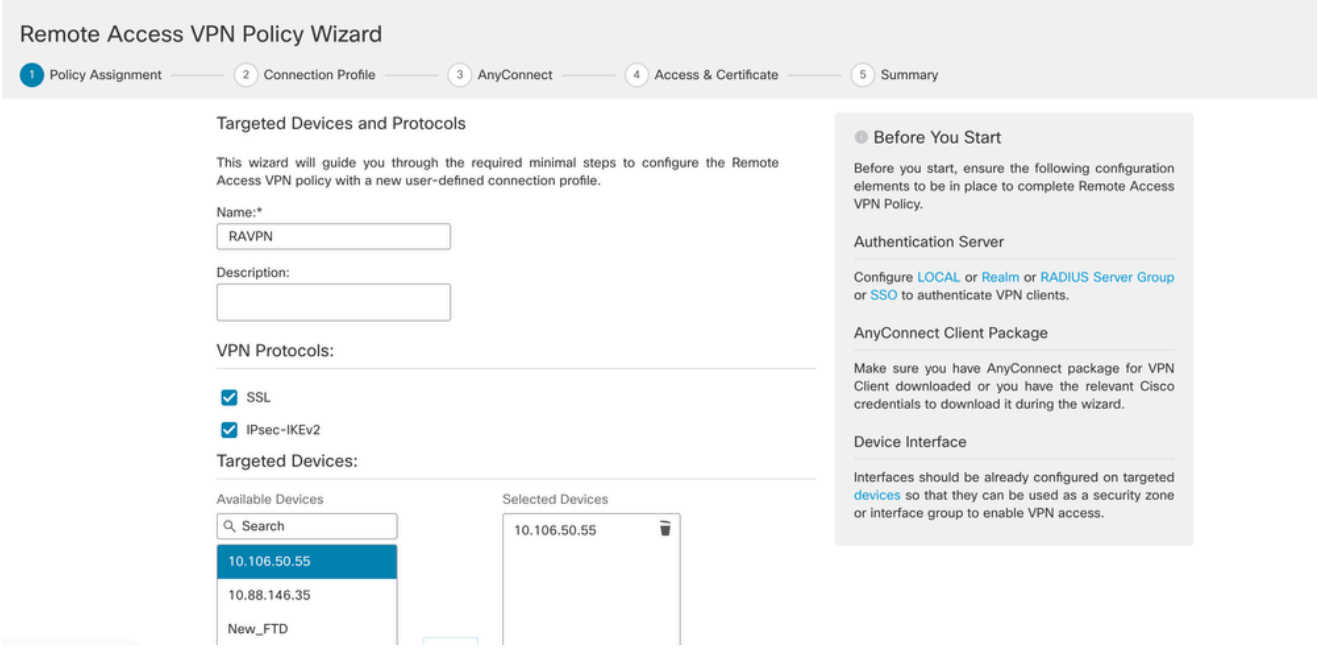
FMCでの設定

FMCによって管理されるFTDのRAVPN設定。

1. Devices > Remote Accessの順に移動します。

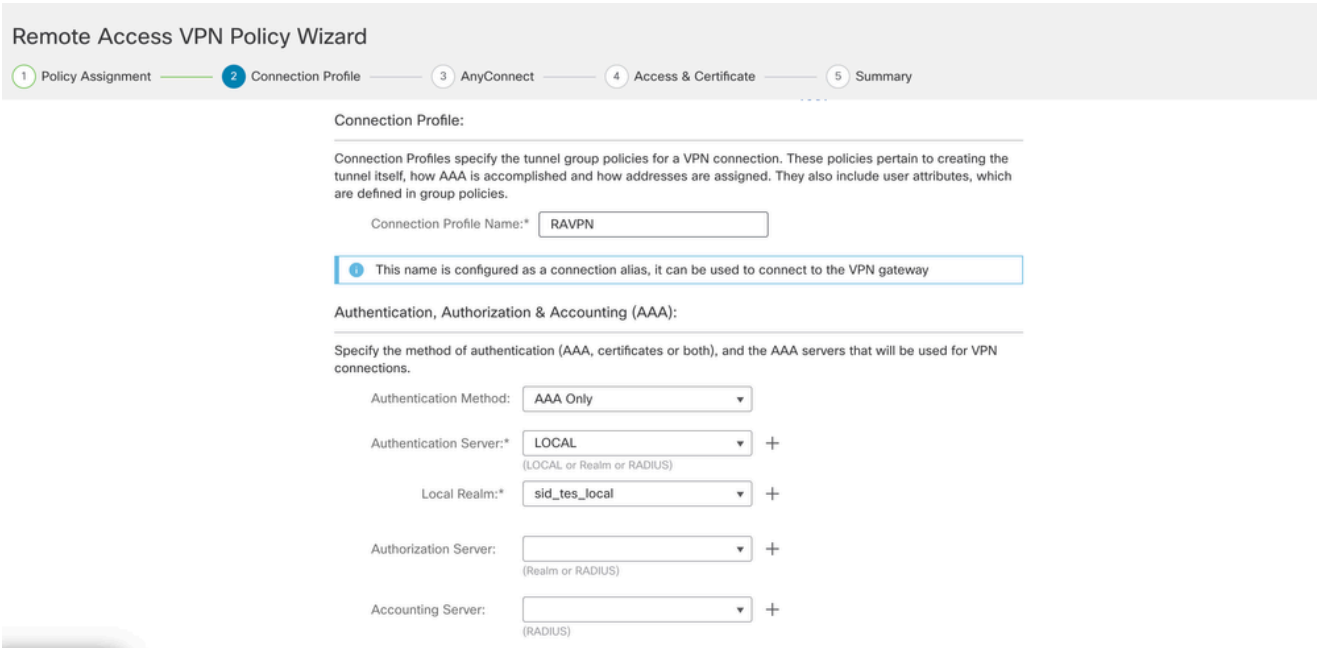


2. [Add] をクリックします。
3. 名前を設定し、使用可能なデバイスからFTDを選択して、Nextをクリックします。

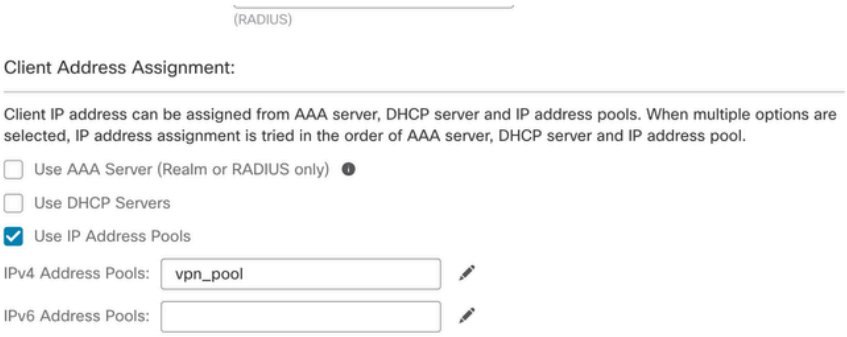


4. 接続プロファイル名を設定し、認証方式を選択します。

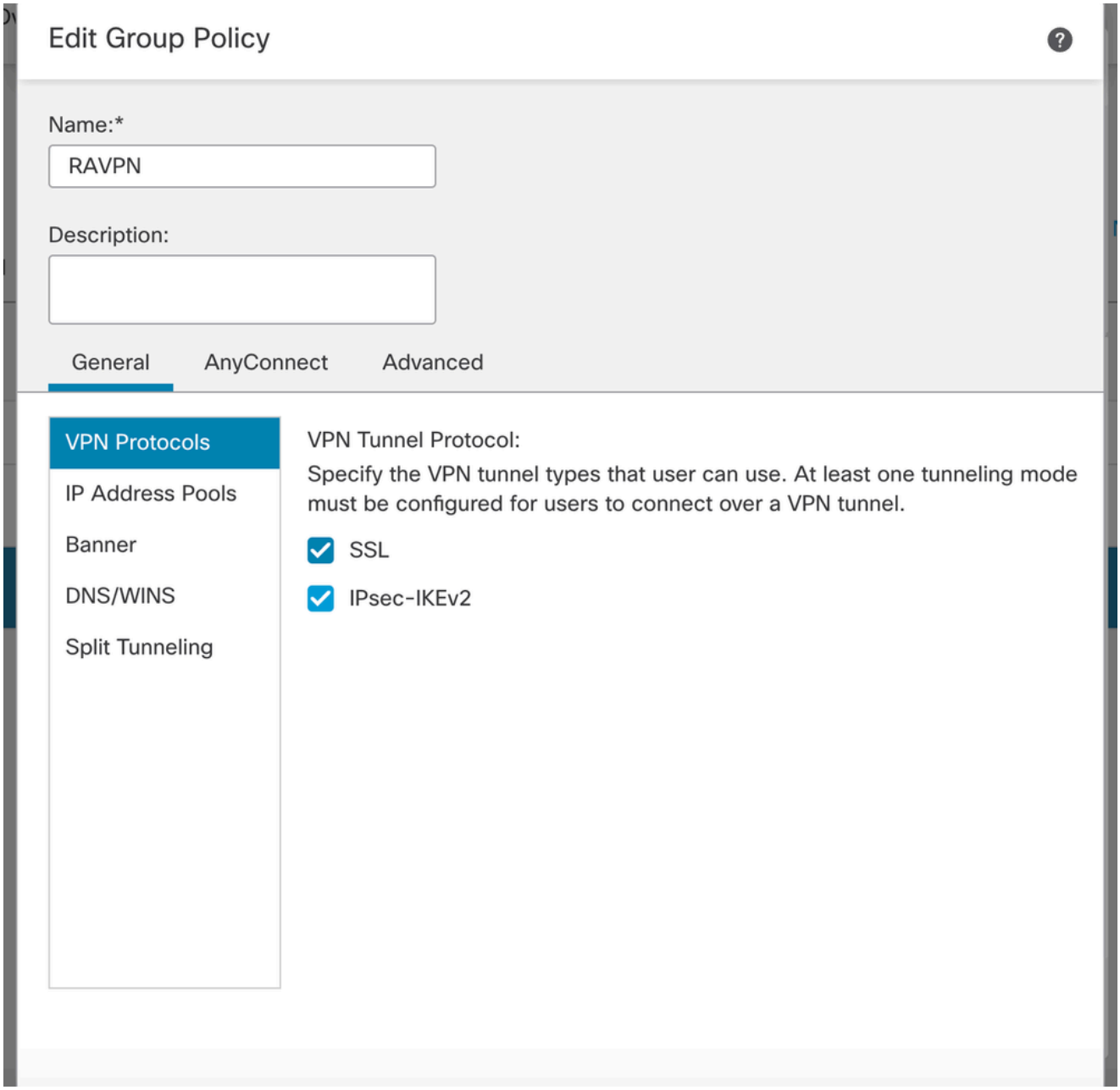
   注：この設定例では、AAAとローカル認証のみを使用しています。ただし、要件に基づいて設定してください。



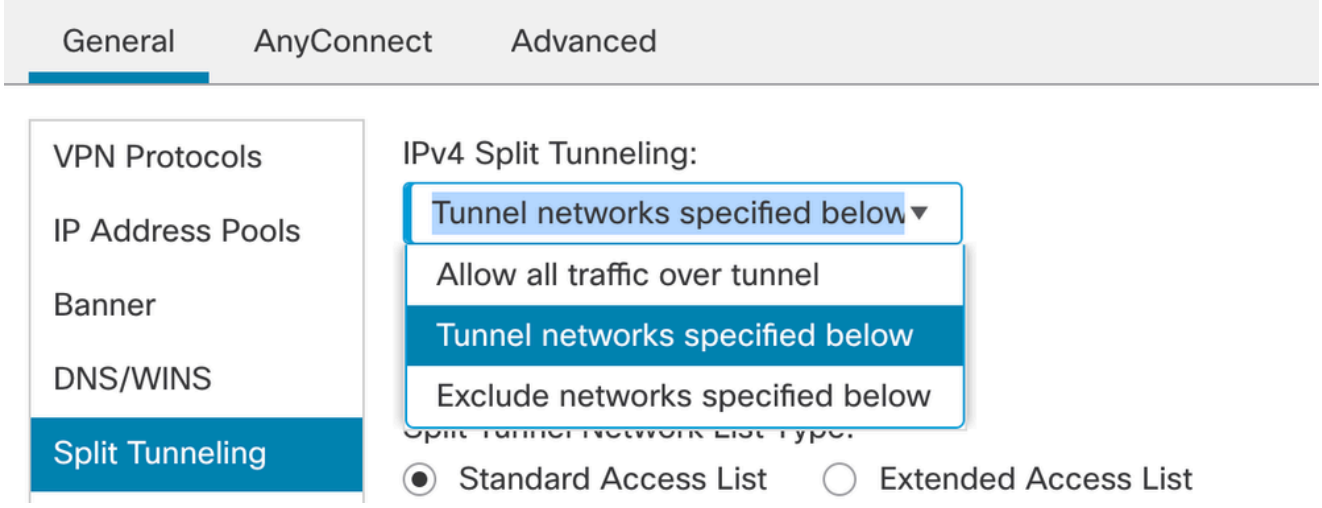
5. AnyConnectのIPアドレス割り当てに使用されるVPNプールを設定します。



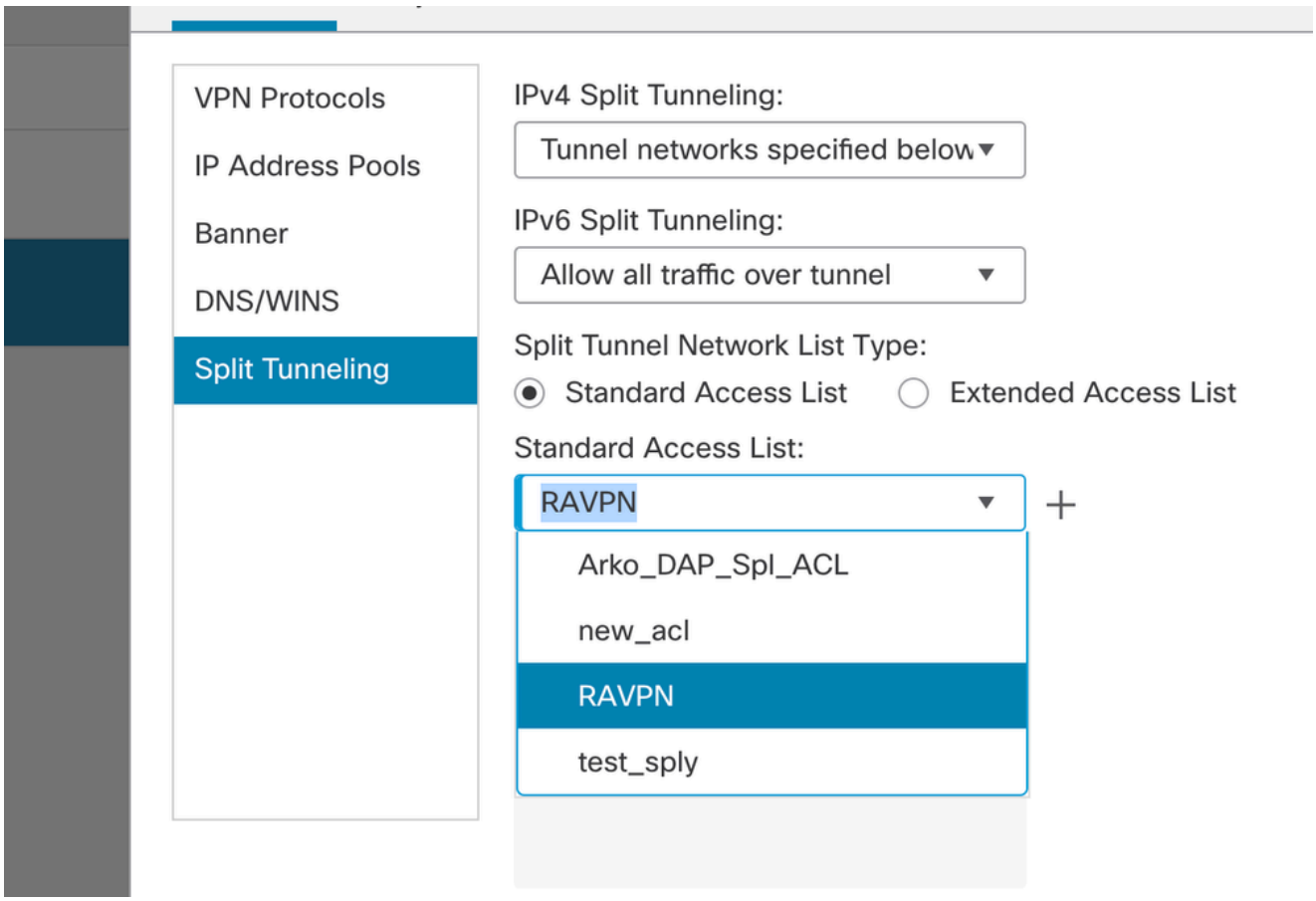
6. グループポリシーを作成します。グループポリシーを作成するには、+をクリックします。グループポリシーの名前を追加します。



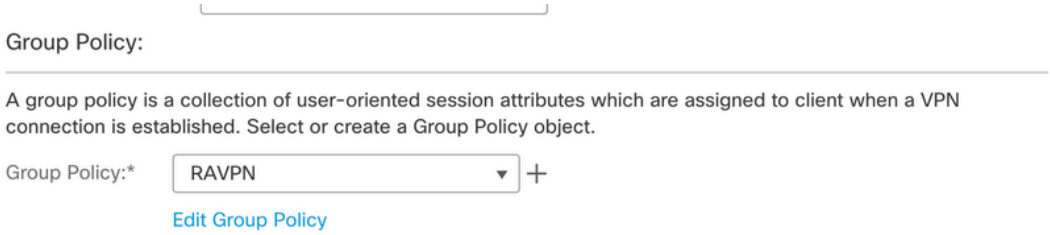
7. スプリットトンネリングに移動します。ここで指定したトンネルネットワークを選択します。



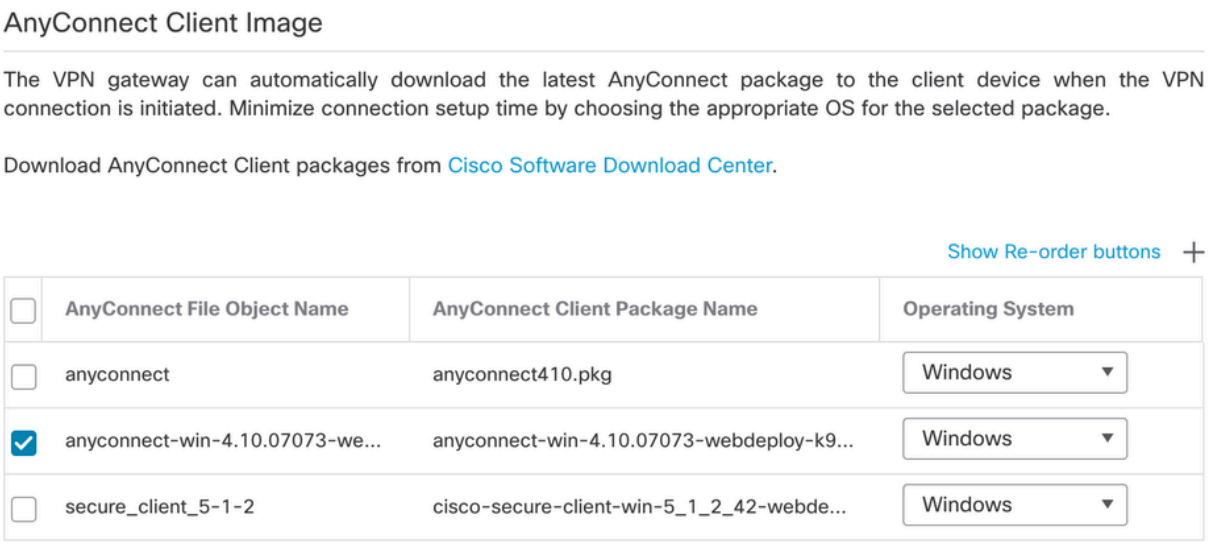
8. ドロップダウンから正しいアクセスリストを選択します。ACLがまだ設定されていない場合：+アイコンをクリックして標準アクセスリストを追加し、新しいアクセスリストを作成します。
[Save] をクリックします。



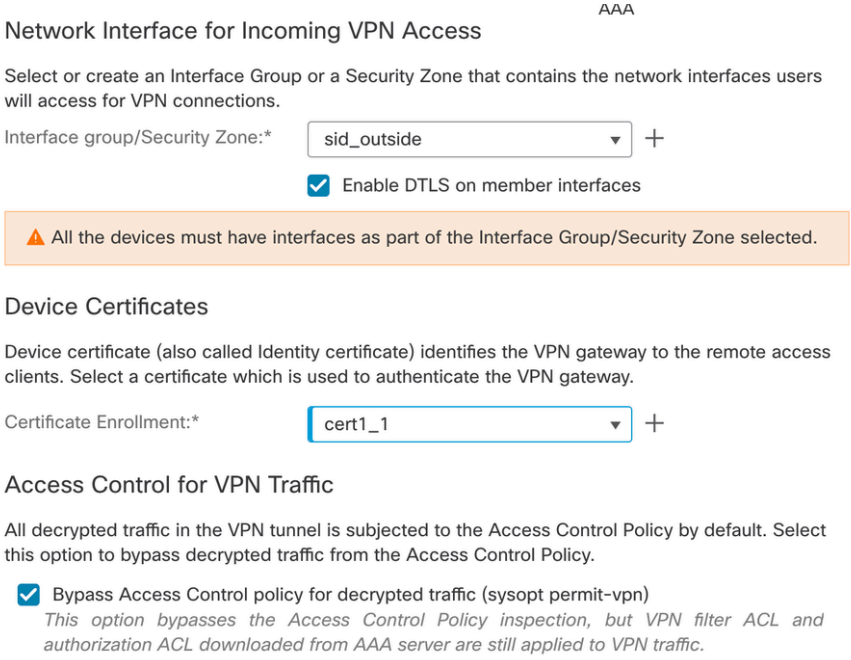
9. 追加するグループポリシーを選択し、Nextをクリックします。



10. AnyConnectイメージを選択します。

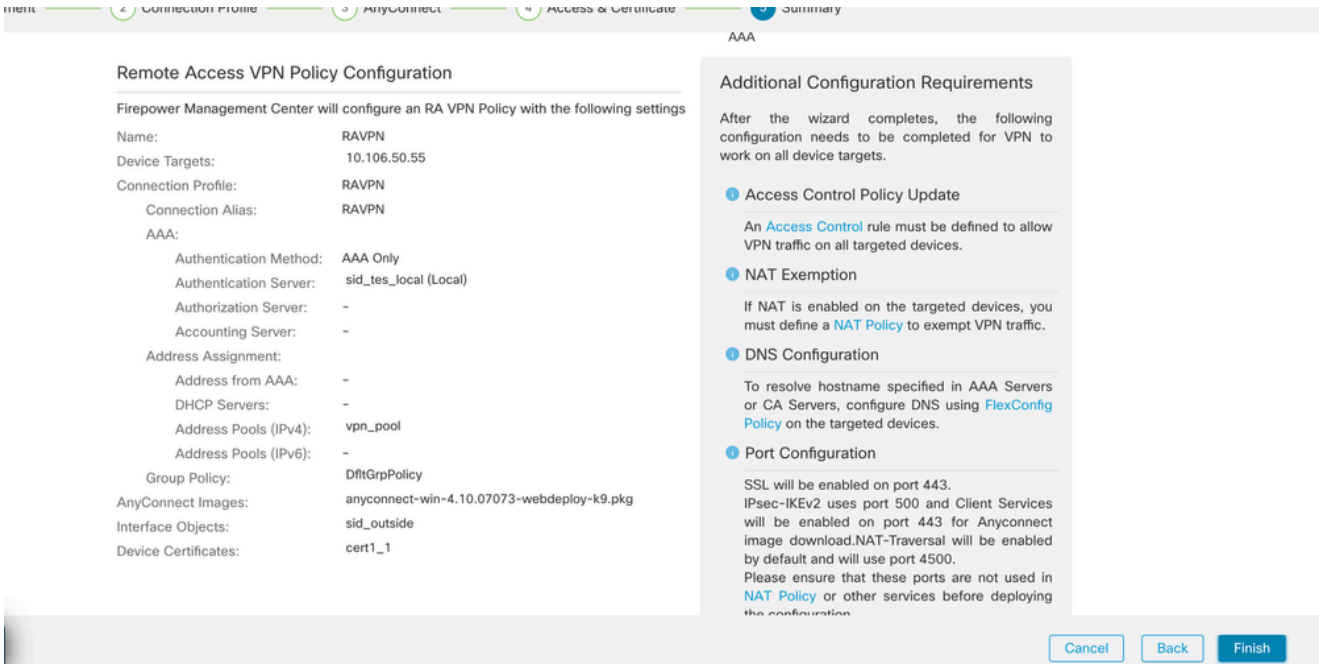


11. AnyConnect接続を有効にする必要があるインターフェイスを選択し、証明書を追加し、復号化されたトラフィックに対するバイパスアクセスコントロールポリシーを選択して、AAA

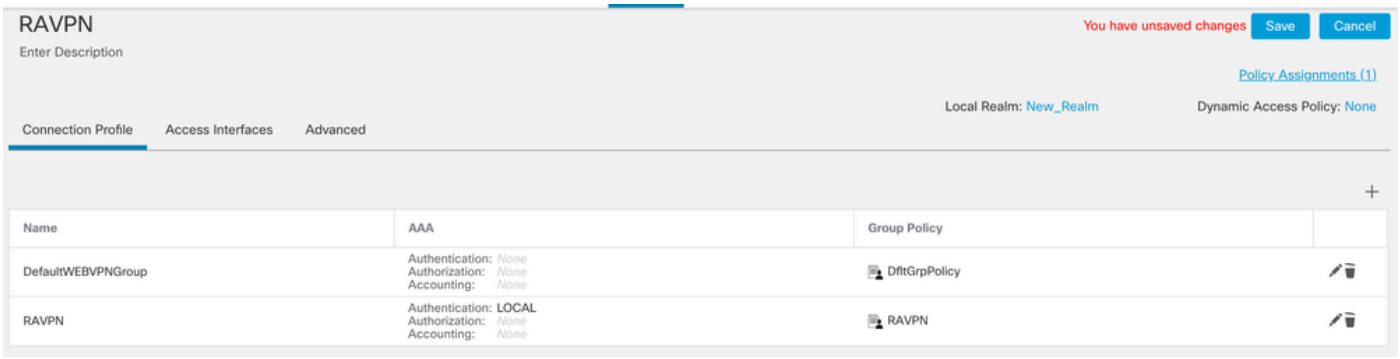


Nextをクリックします。

12. 設定を確認し、Finishをクリックします。

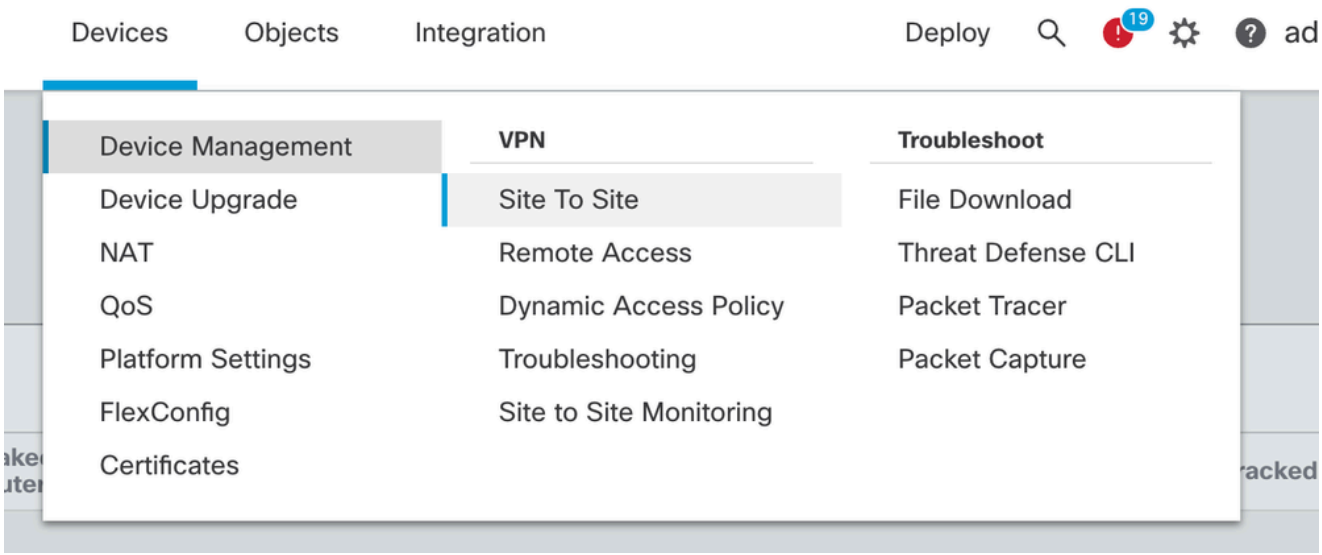


13. Save and deployをクリックします。

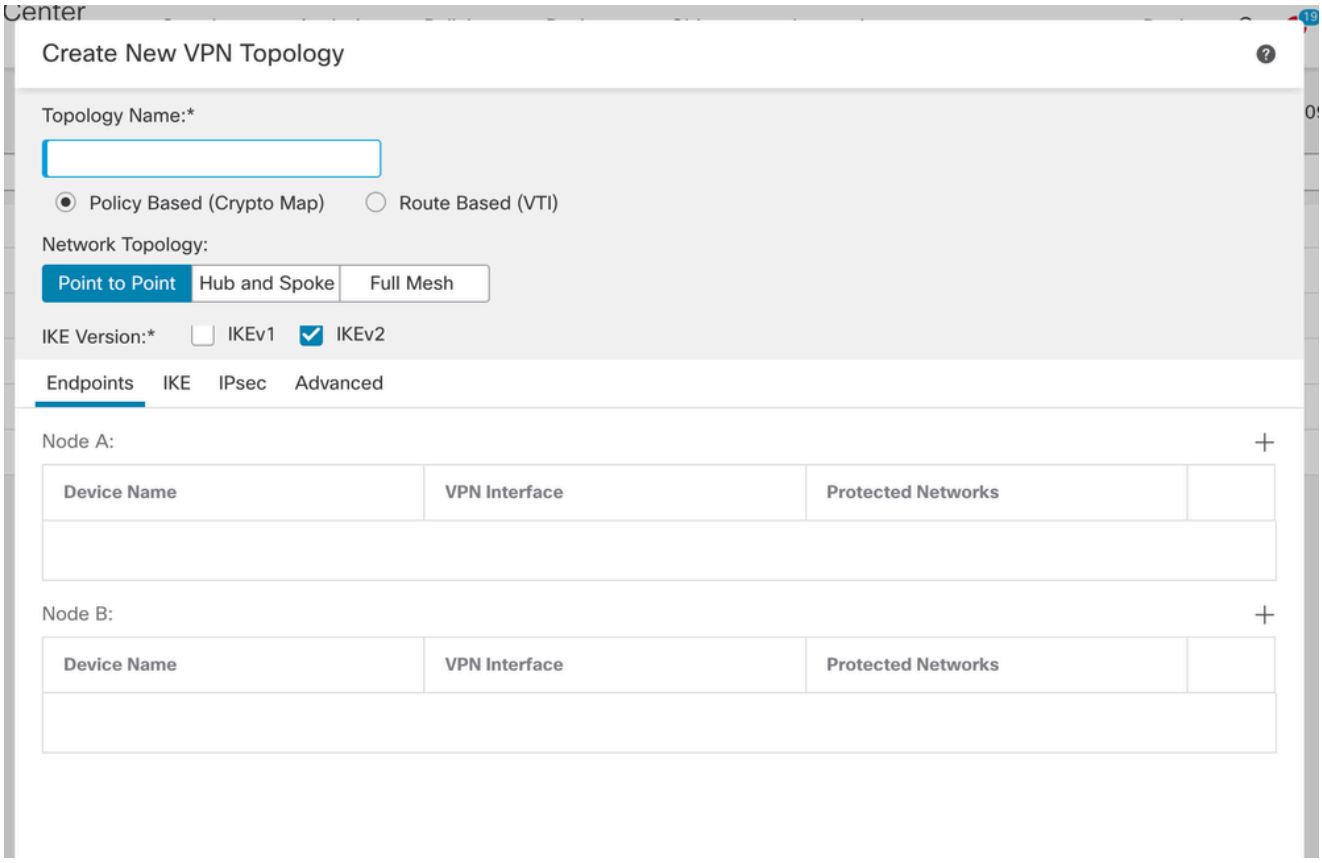


FMCによるFTD上のIKEv2 VPNの管理

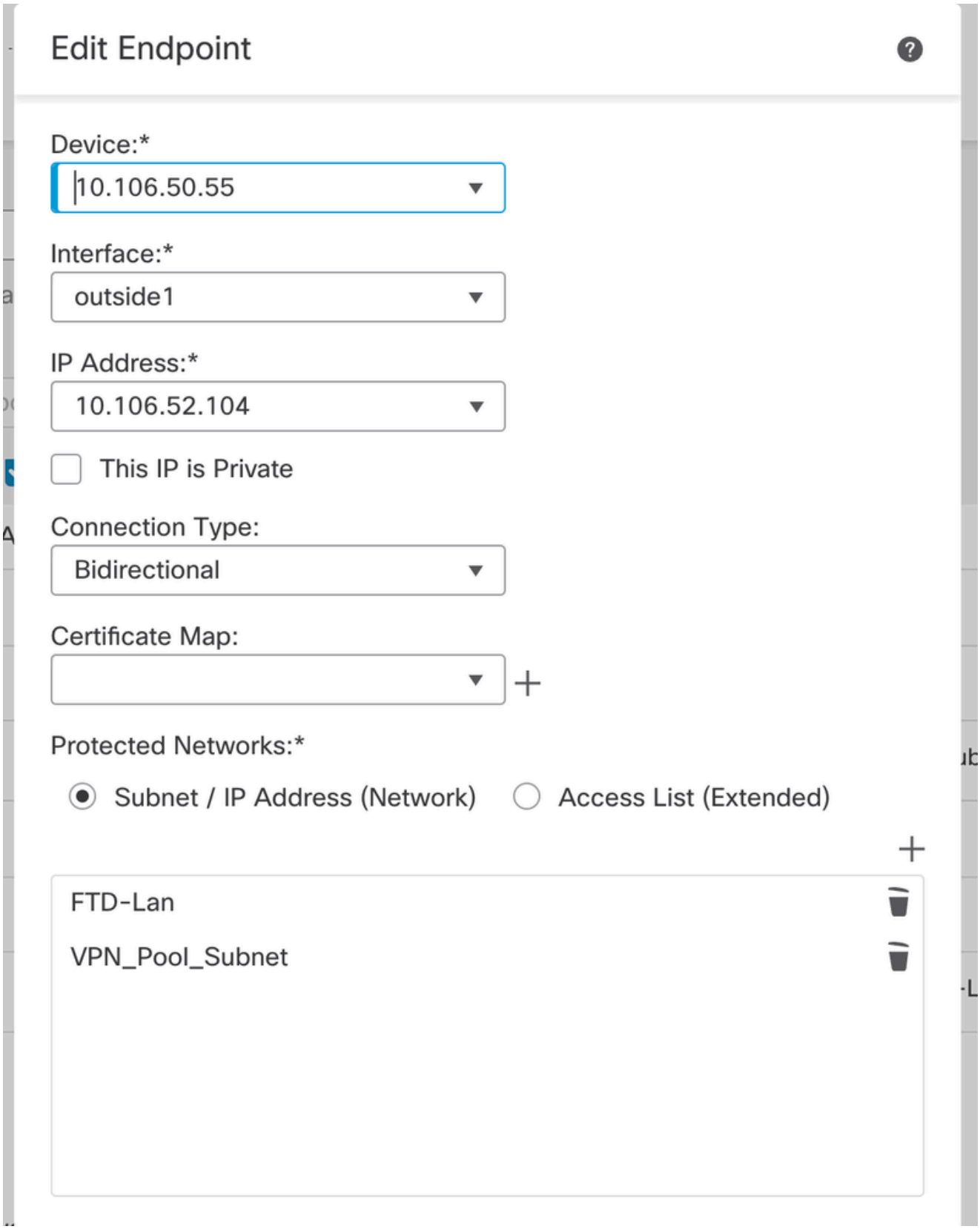
1. Devices > Site To Siteの順に移動します。



2. [Add] をクリックします。
3. ノードAの+をクリックします。



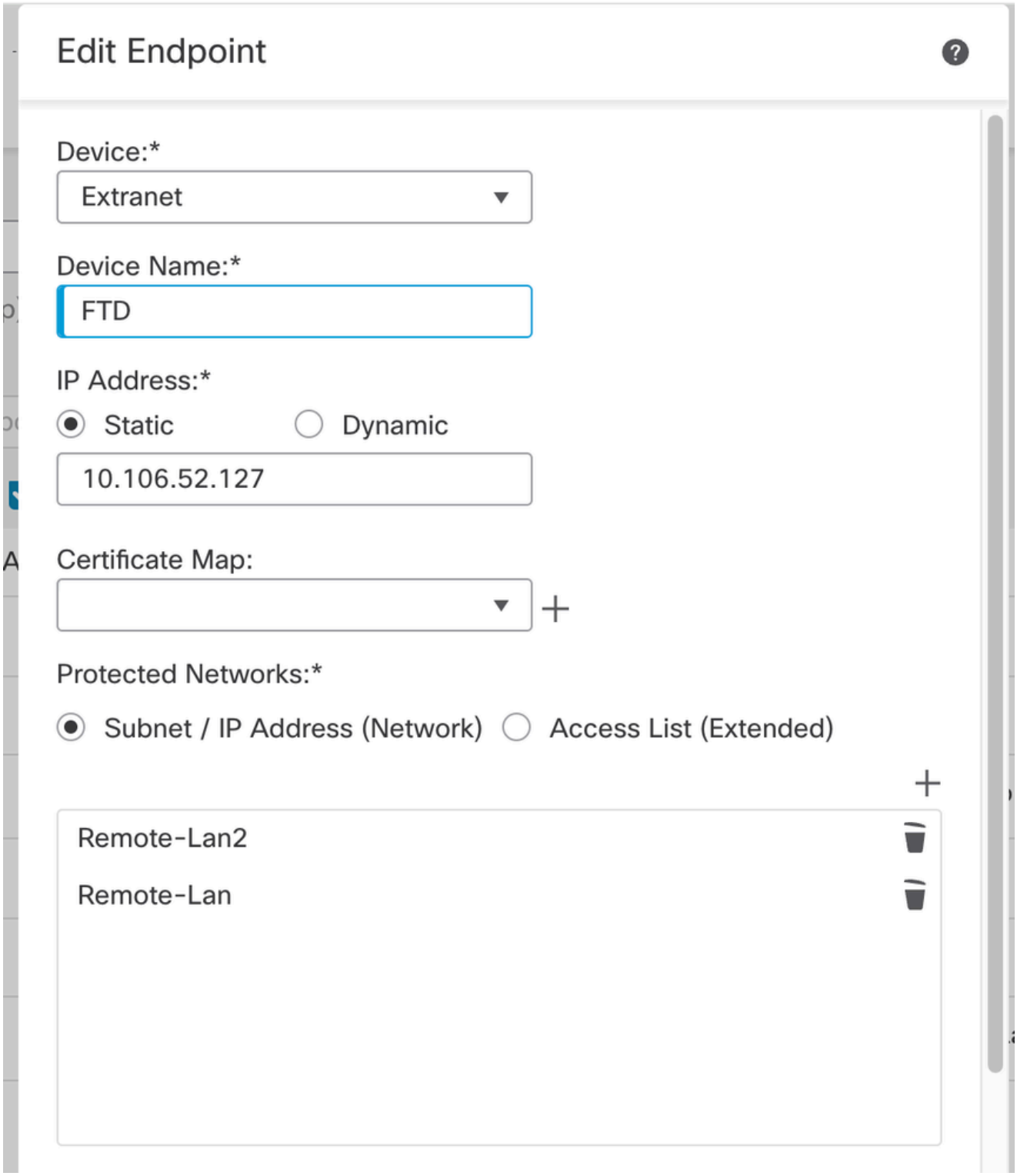
4. デバイスからFTDを選択して、インターフェイスを選択し、IPSecトンネルを介して暗号化される必要があるローカルサブネット（この場合はVPNプールアドレスも含まれます）を追加し、OKをクリックします。



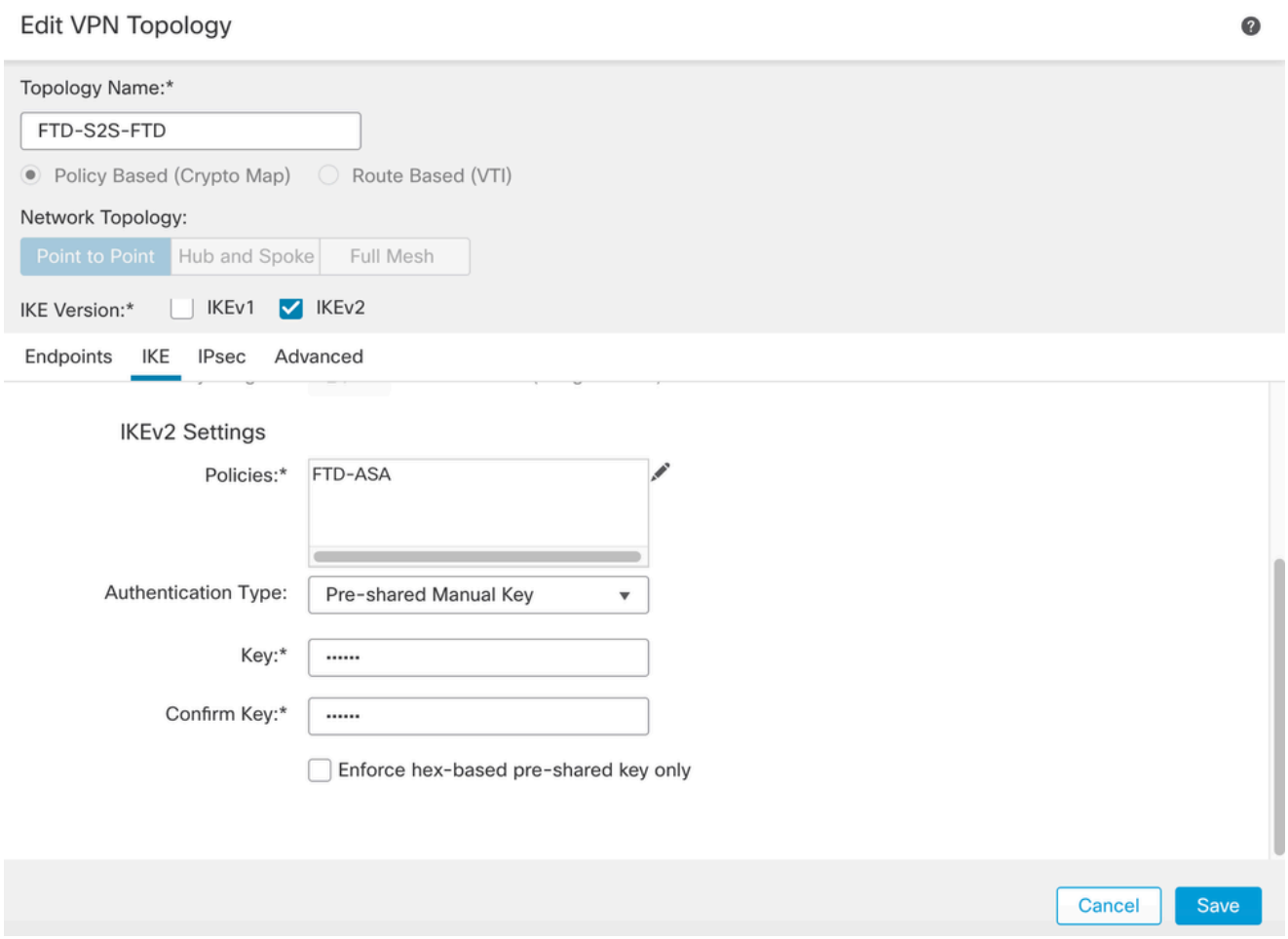
5. ノードBで+をクリックします。

>デバイスからエクストラネットを選択し、ピアデバイスの名前を指定します。

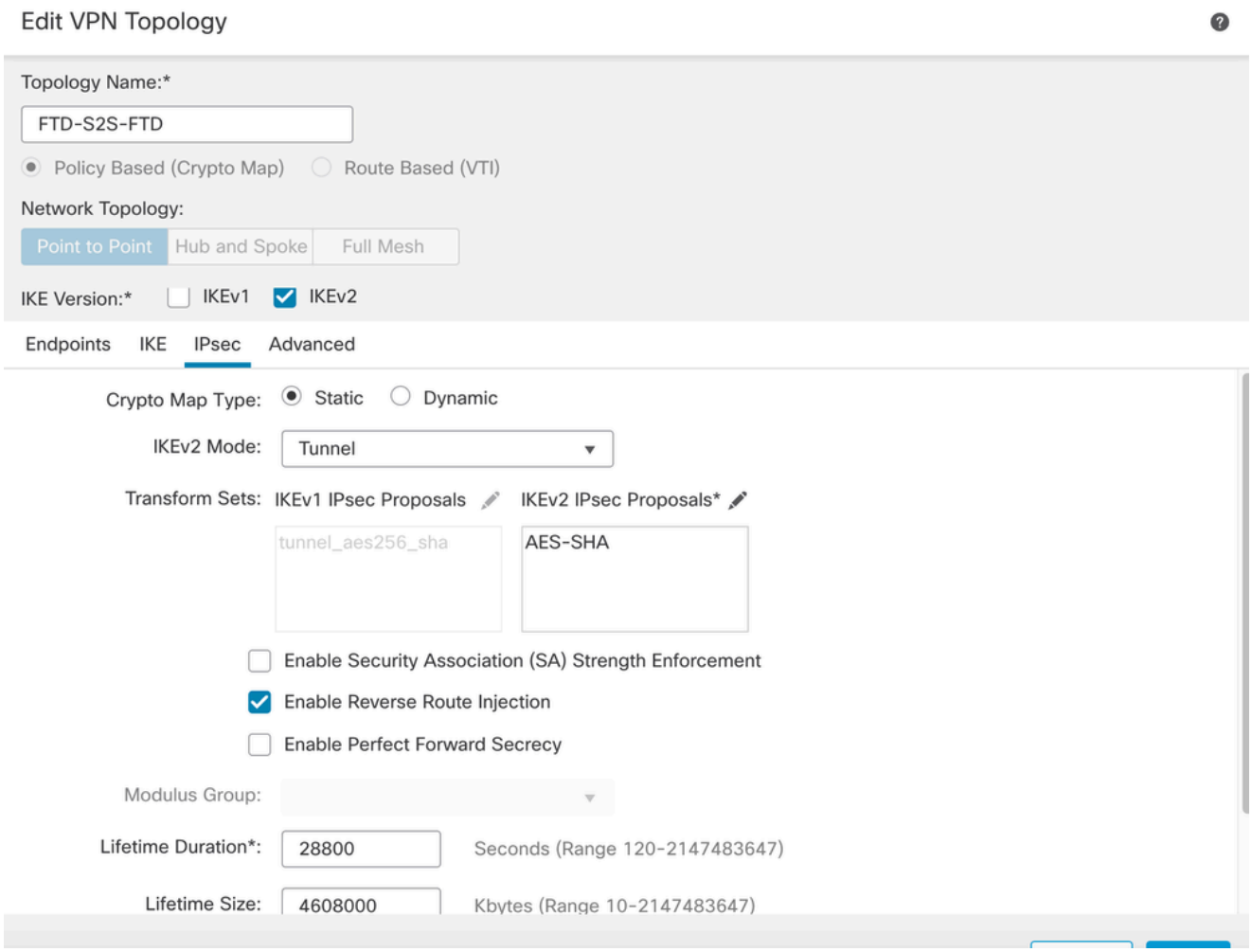
>ピアの詳細を設定し、VPNトンネル経由でのアクセスが必要なリモートサブネットを追加して、OKをクリックします。



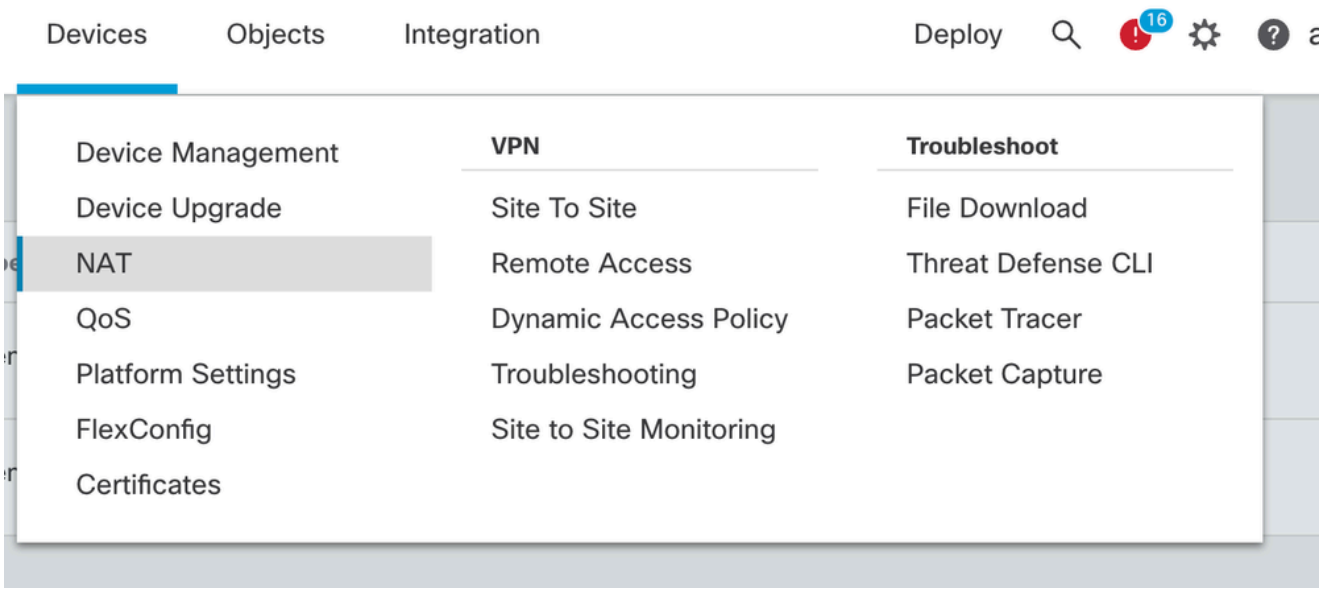
6. IKEタブをクリックし、必要に応じてIKEv2設定を設定します。



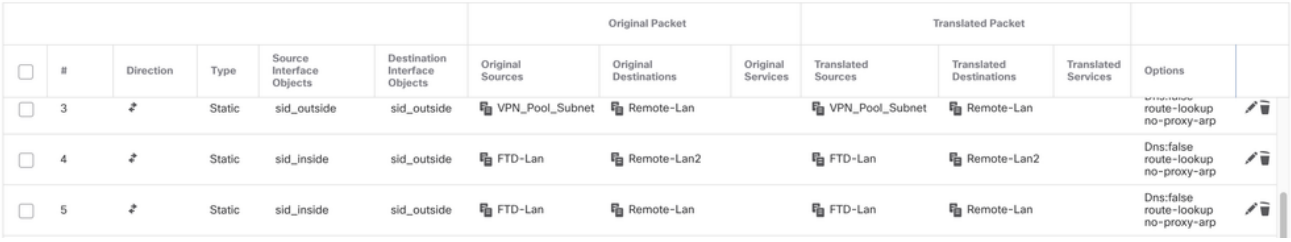
7. IPsecタブをクリックし、要件に応じてIPSec設定を行います。



8. 対象トラフィックのNAT免除を設定します（オプション）。
Devices > NATの順にクリックします。



9. ここで設定するNATにより、RAVPNおよび内部ユーザはS2S IPSecトンネルを介してサーバにアクセスできます。



	#	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. 同様に、S2Sトンネルがアップ状態になるために、もう一方のピアエンドで設定を行います。

    注：暗号化ACLまたは対象トラフィックサブネットは、両方のピアで相互にミラーコピーを作成する必要があります。

確認

1. RAVPN接続を確認するには、次の手順を実行します。

<#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. IKEv2接続を確認するには、次の手順を実行します。

<#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. IPSec接続を確認するには：

<#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
```

トラブルシュート

1. AnyConnect接続の問題をトラブルシューティングするには、dartバンドルを収集するか、AnyConnectのデバッグを有効にします。
2. IKEv2トンネルをトラブルシューティングするには、次のデバッグを使用します。

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

3. FTDでトラフィックの問題をトラブルシューティングするには、パケットキャプチャを実行して設定を確認します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。