

# 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](#) :

[前提条件](#)

[基本的な要件](#)

[使用するコンポーネント](#)

[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。](#)

[FMCによるFTD上のIKEv2 VPNの管理](#)

[確認](#)

[トラブルシューティング](#)

---

## 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。

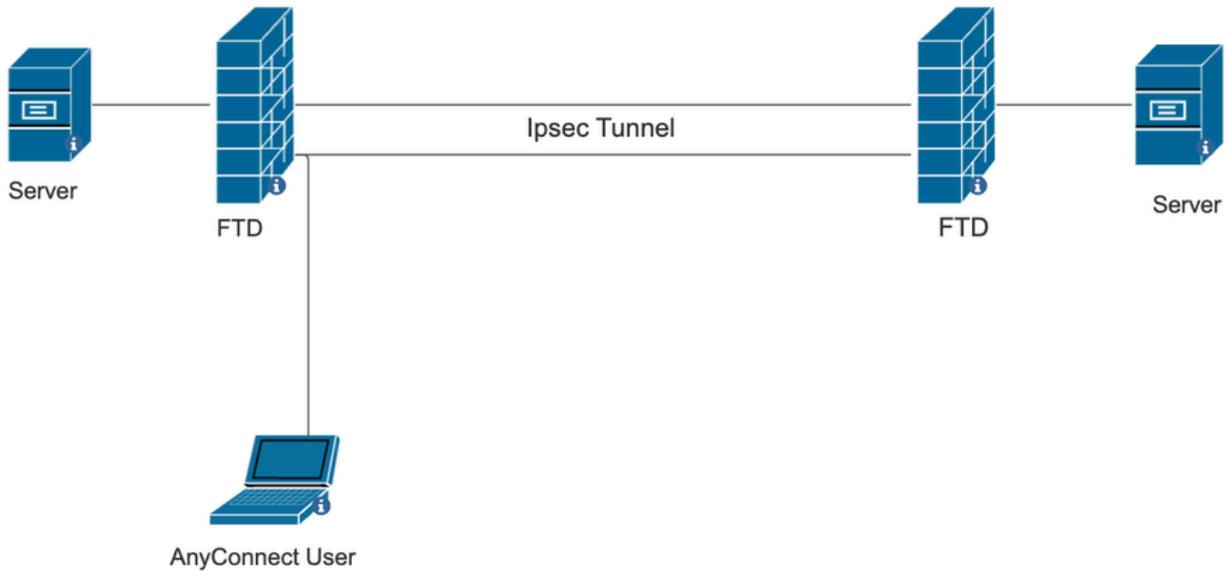
### 使用するコンポーネント

- 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。

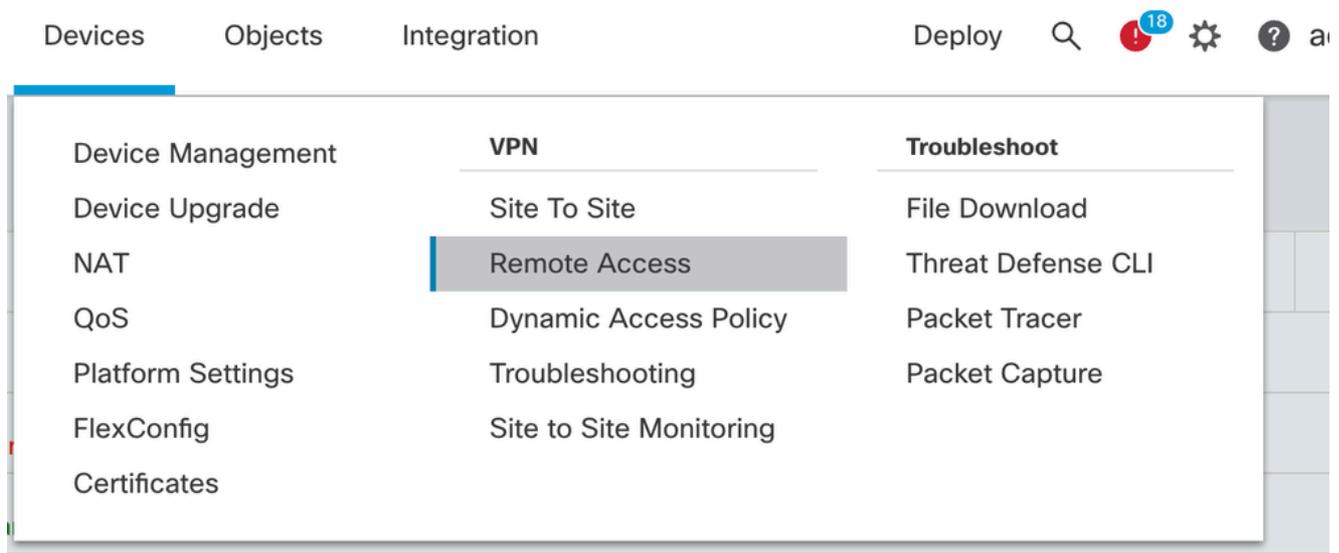
## ネットワーク図



## 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。

### Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

#### 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:\*

Description:

VPN Protocols:

SSL  
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Search"/> <input checked="" type="checkbox"/> 10.106.50.55 <input type="checkbox"/> 10.88.146.35 <input type="checkbox"/> New_FTD	<input type="text" value="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. 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。

### Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

#### 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:\*

**1** 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:

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

Local Realm:\*  +

Authorization Server:  +  
(Realm or RADIUS)

Accounting Server:  +  
(RADIUS)

#### 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。

(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) ●

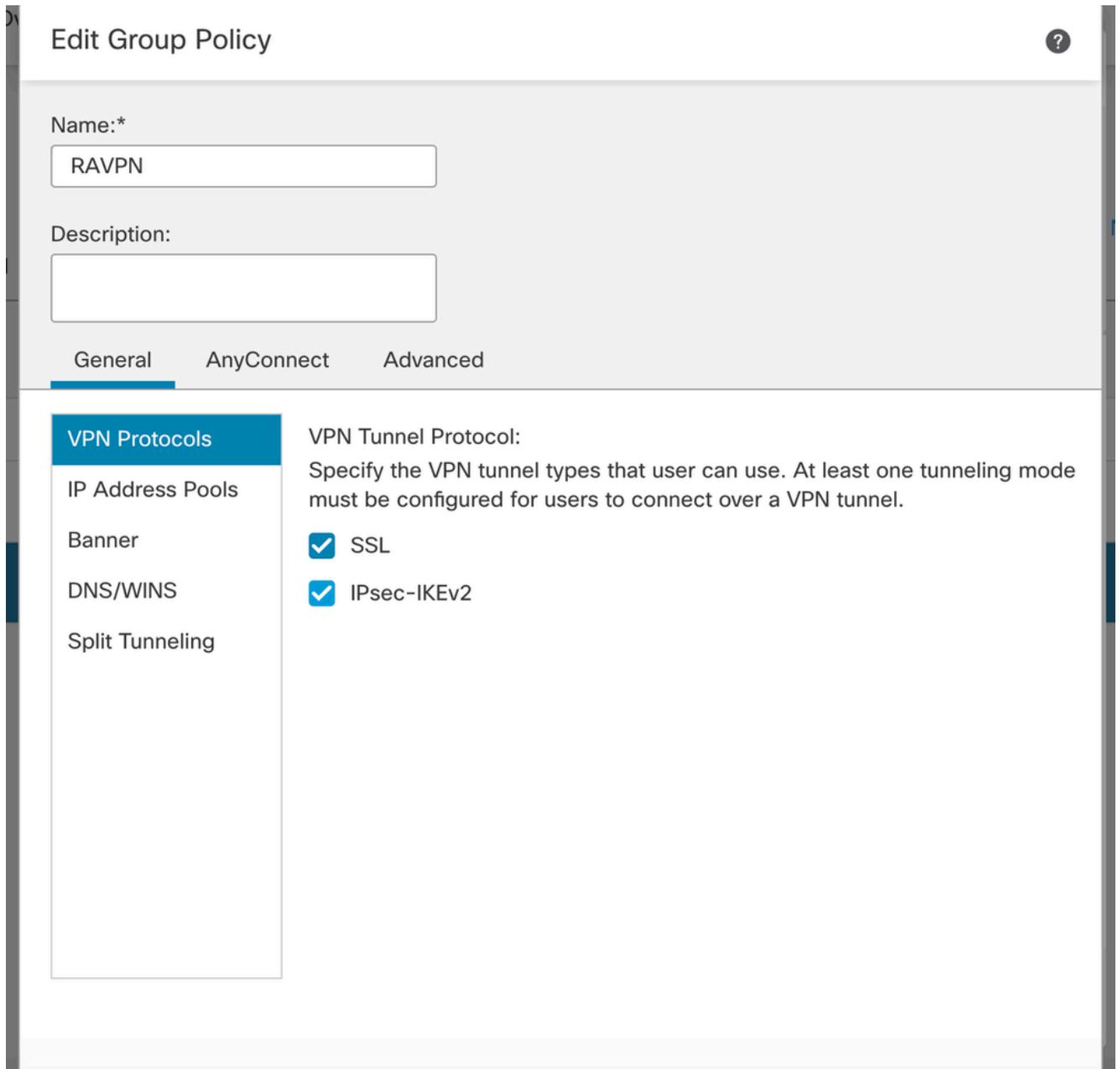
Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:  

IPv6 Address Pools:  

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。



**Edit Group Policy** ?

Name:\*

Description:

General AnyConnect Advanced

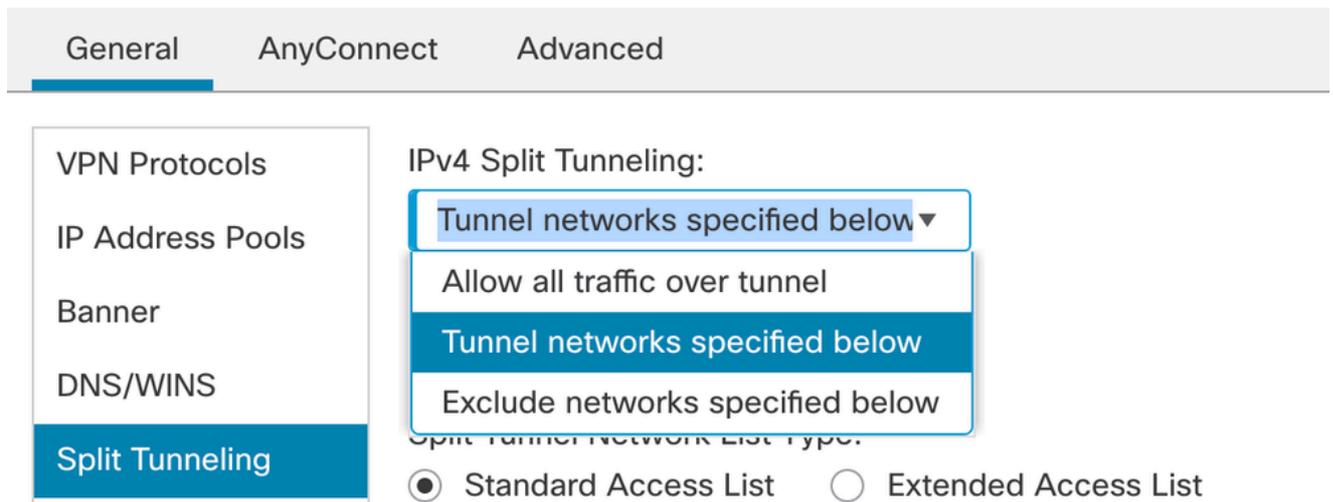
**VPN Protocols**

- IP Address Pools
- Banner
- DNS/WINS
- Split Tunneling

**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.

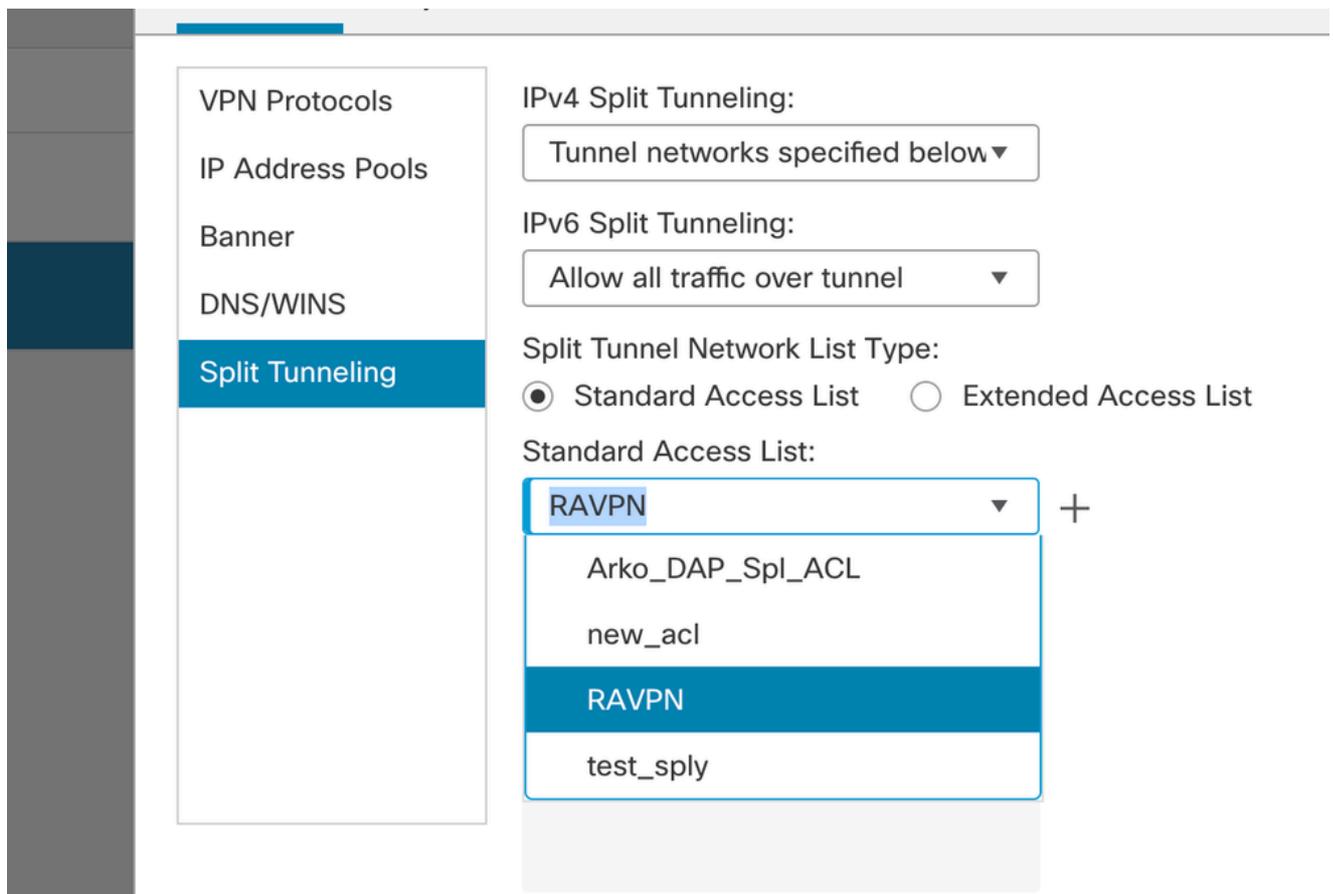
- SSL
- IPsec-IKEv2

7. 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。

## 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:\*  +

[Edit Group Policy](#)

## 10. AnyConnectイメージを選択します。

### 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](#) +

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect	anyconnect410.pkg	<input type="text" value="Windows"/>
<input checked="" type="checkbox"/>	anyconnect-win-4.10.07073-we...	anyconnect-win-4.10.07073-webdeploy-k9...	<input type="text" value="Windows"/>
<input type="checkbox"/>	secure_client_5-1-2	cisco-secure-client-win-5_1_2_42-webde...	<input type="text" value="Windows"/>

## 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、

### 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:\*  +

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:\*  +

### 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.*

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。

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.

Cancel Back Finish

13. Save and deployをクリックします。

RAVPN

Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

Local Realm: New\_Realm Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

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

## 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。

Devices Objects Integration Deploy 🔍 19 ⚙️ ? ad

Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
FlexConfig	Site to Site Monitoring	
Certificates		

2. [Add] をクリックします。
3. ノードAの+をクリックします。

Center

### 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

Endpoints IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	

Node B: +

Device Name	VPN Interface	Protected Networks	

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。

## Edit Endpoint



Device:\*

Interface:\*

IP Address:\*

This IP is Private

Connection Type:

Certificate Map:

 +

Protected Networks:\*

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

FTD-Lan	
VPN_Pool_Subnet	

+

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。

## Edit Endpoint ?

Device:\*

Device Name:\*

IP Address:\*  
 Static  Dynamic

Certificate Map:  
 +

Protected Networks:\*  
 Subnet / IP Address (Network)  Access List (Extended)

Remote-Lan2 +

Remote-Lan +

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。

Topology Name:\*  
FTD-S2S-FTD

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

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

Cancel Save

7. IPsecタブをクリックし、要件に応じてIPSec設定を行います。

Topology Name:\*  
FTD-S2S-FTD

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode: Tunnel

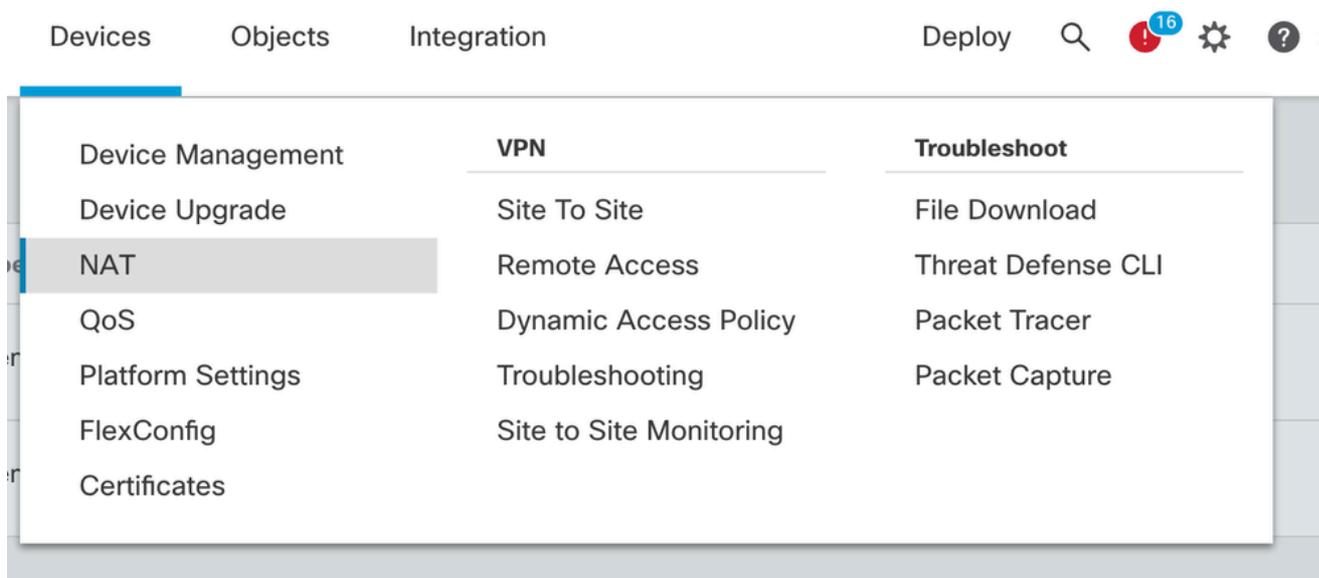
Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals\*

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. 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			Translated Packet			Options	
						Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
<input type="checkbox"/>	3	↔	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	4	↔	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan2		FTD-Lan	Remote-Lan2		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	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_outsidel_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。