

# Configurez AnyConnect pour accéder au serveur via le tunnel IPSec.

## Table des matières

---

[Introduction:](#)

[Conditions préalables:](#)

[Exigences de base](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Configurations sur FMC](#)

[Configuration RAVPN sur le FTD géré par FMC.](#)

[VPN IKEv2 sur FTD géré par FMC.:](#)

[Vérifier](#)

[Dépannage](#)

---

## Introduction:

Ce document décrit les procédures pour déployer une configuration RAVPN sur le FTD géré par FMC et un tunnel de site à site entre les FTD.

## Conditions préalables:

### Exigences de base

- Une compréhension fondamentale des VPN de site à site et du RAVPN est bénéfique.
- Il est essentiel de comprendre les principes fondamentaux de la configuration d'un tunnel basé sur des politiques IKEv2 sur la plate-forme Cisco Firepower.

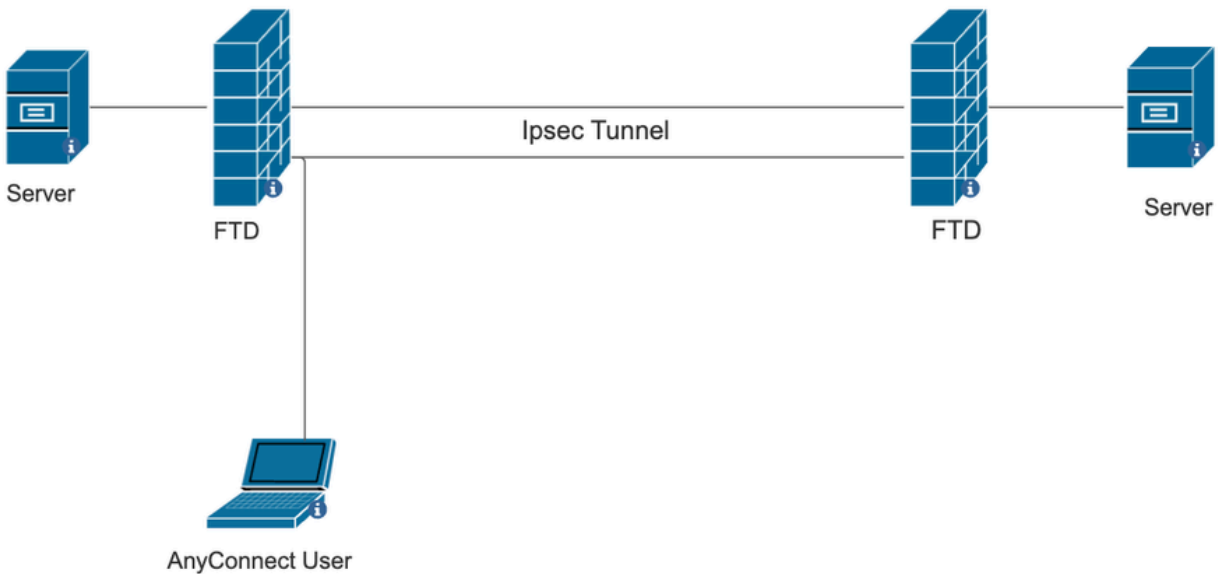
Cette procédure est destinée au déploiement d'une configuration RAVPN sur le FTD géré par FMC et d'un tunnel de site à site entre les FTD où l'utilisateur AnyConnect peut accéder au serveur derrière l'autre homologue FTD.

### Composants utilisés

- Cisco Firepower Threat Defense pour VMware : version 7.0.0
- Firepower Management Center : version 7.2.4 (build 169)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande..

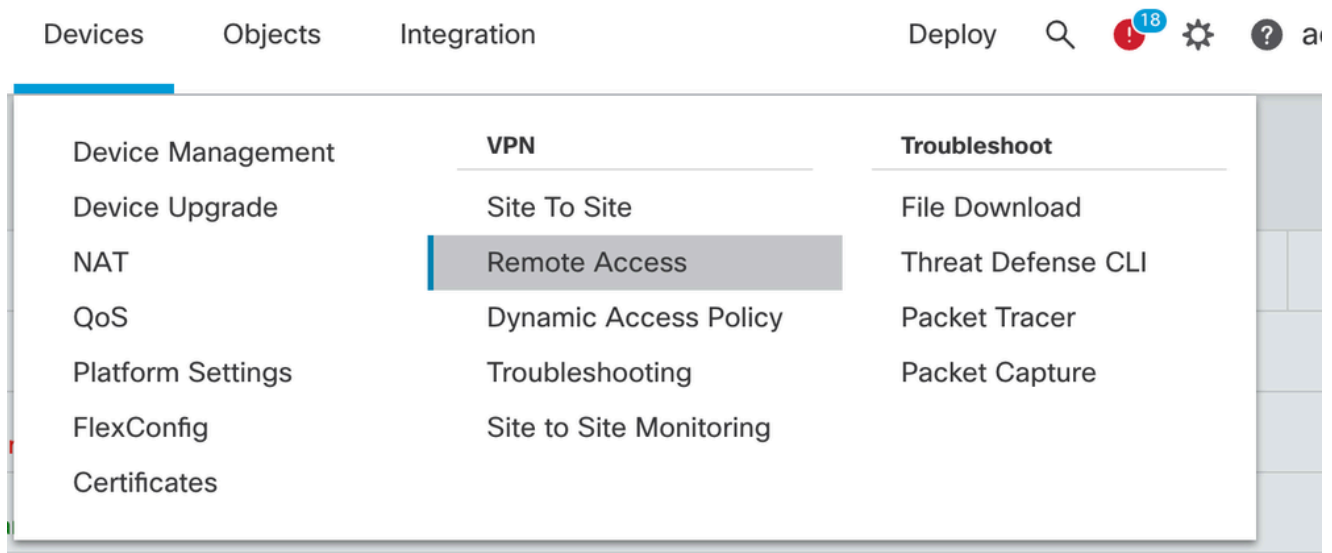
# Diagramme du réseau



## Configurations sur FMC

Configuration RAVPN sur le FTD géré par FMC.

1. Accédez à Périphériques > Accès à distance.



2. Cliquez sur Add.
3. Configurez un nom et sélectionnez le FTD parmi les périphériques disponibles, puis cliquez sur Next.

## 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

- 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. Configurez un nom de profil de connexion et choisissez la méthode d'authentification.

REMARQUE : pour cet exemple de configuration, nous utilisons uniquement AAA et l'authentification locale. Toutefois, configurez en fonction de vos besoins.

## 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:\*

**!** 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. Configurez le pool VPN utilisé pour l'attribution d'adresses IP pour 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:  

IPv6 Address Pools:  

6. Créez une stratégie de groupe. Cliquez sur + pour créer une stratégie de groupe. Ajoutez le nom de la stratégie de groupe.

### Edit Group Policy

Name:\*

Description:

General AnyConnect Advanced

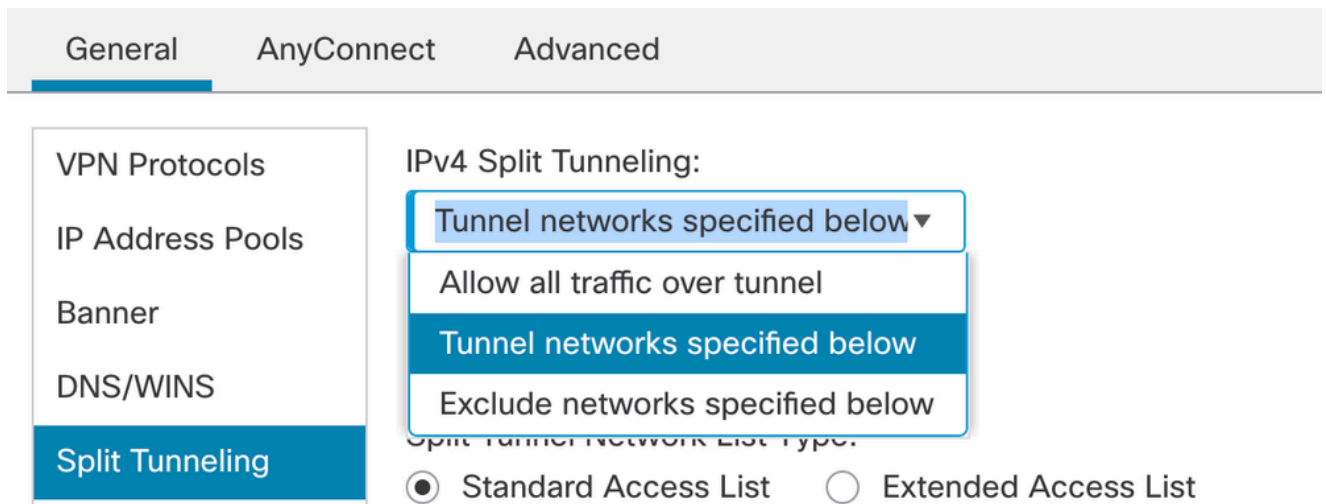
**VPN Protocols**

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

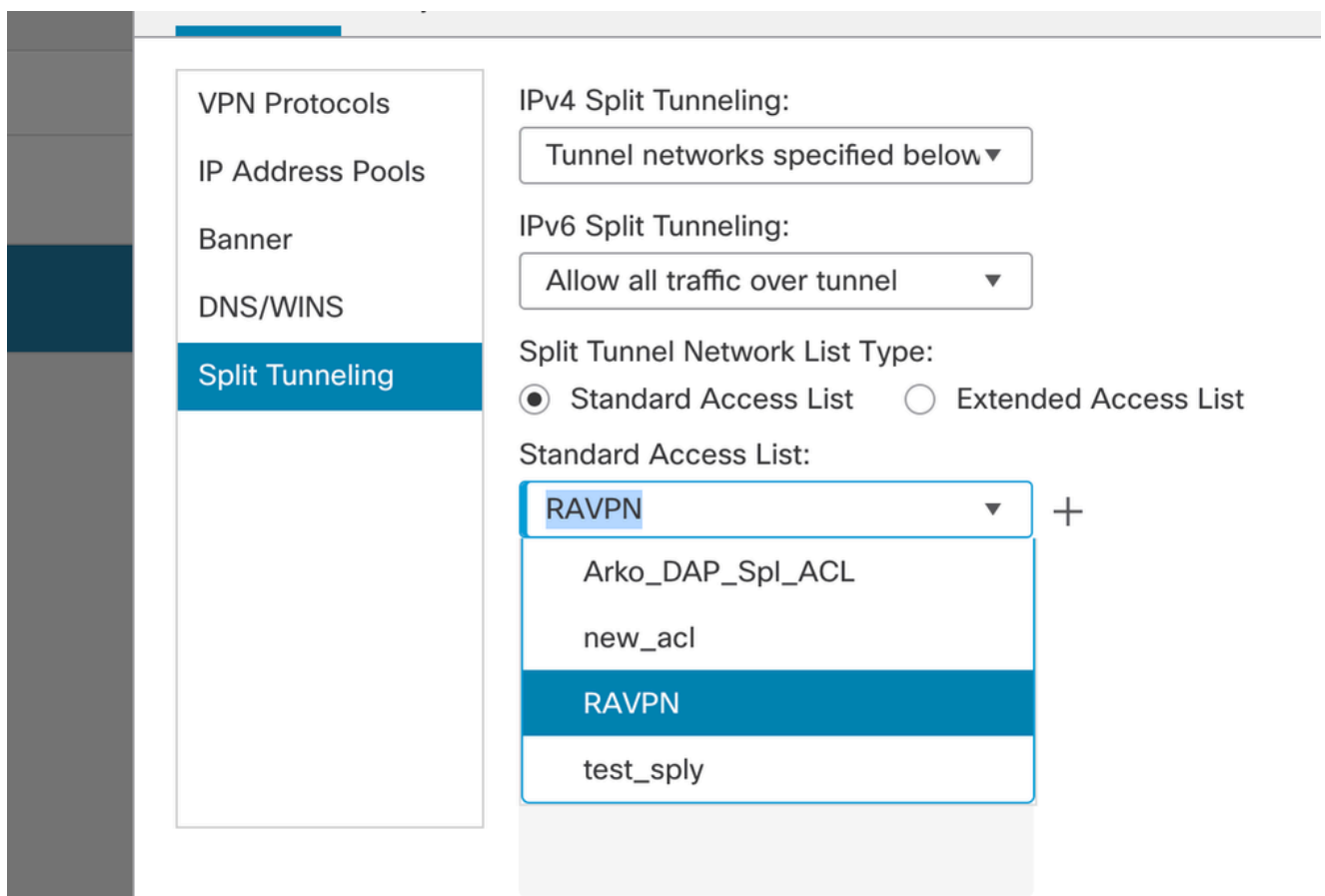
VPN Tunnel Protocol:  
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

- SSL
- IPsec-IKEv2

7. Accédez à Split tunneling. Sélectionnez les réseaux de tunnel spécifiés ici :



8. Sélectionnez la liste de contrôle d'accès appropriée dans la liste déroulante. Si une liste de contrôle d'accès n'est pas déjà configurée : Cliquez sur l'icône + pour ajouter la liste de contrôle d'accès standard et en créer une nouvelle.  
Cliquez sur Save.



9. Sélectionnez la stratégie de groupe qui est ajoutée et cliquez sur 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:\*  +

[Edit Group Policy](#)

## 10. Sélectionnez l'image 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](#).

[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. Sélectionnez l'interface qui doit être activée pour la connexion AnyConnect, ajoutez le certificat, sélectionnez la stratégie Contourner le contrôle d'accès pour le trafic décrypté, et

### 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.*

cliquez sur Suivant.

## 12. Vérifiez la configuration et cliquez sur 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.

Cancel Back Finish

## 13. Cliquez sur Enregistrer et déployer.

RAVPN

Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

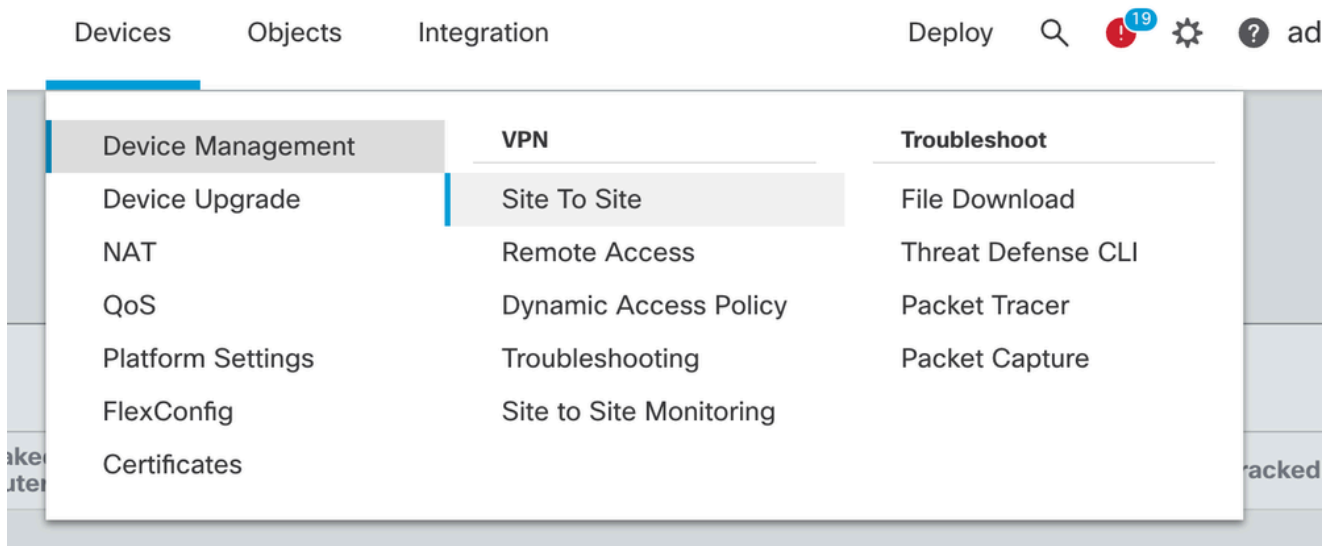
Local Realm: New\_Realm Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

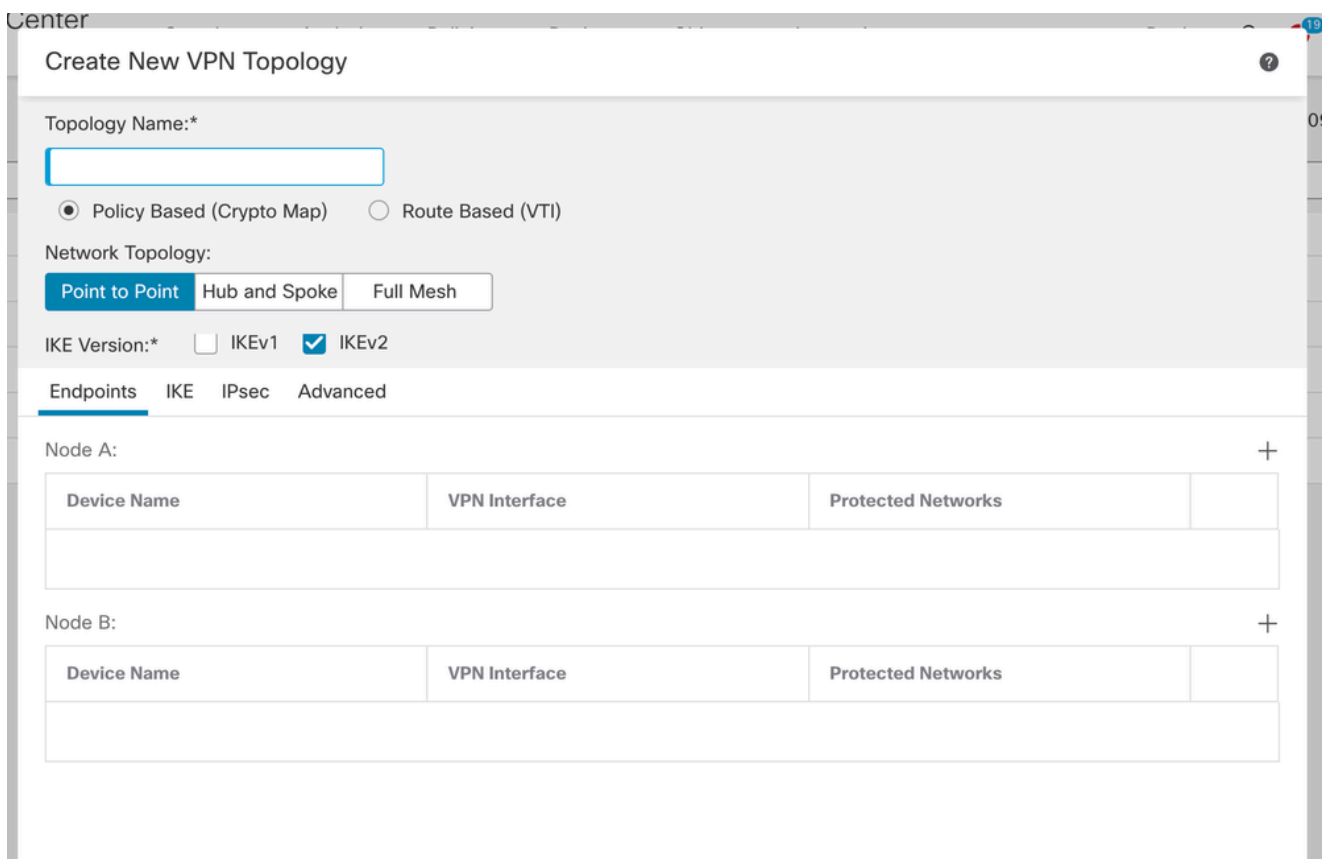
| Name               | AAA  | Group Policy  |  |
|--------------------|--|---------------|--|
| DefaultWEBVPNGroup | Authentication: None<br>Authorization: None<br>Accounting: None  | DfltGrpPolicy |  |
| RAVPN              | Authentication: LOCAL<br>Authorization: None<br>Accounting: None | RAVPN         |  |

## VPN IKEv2 sur FTD géré par FMC :

1. Accédez à Périphériques > Site à site.



2. Cliquez sur Add.
3. Cliquez sur + pour le noeud A :



4. Sélectionnez le FTD à partir du périphérique, sélectionnez l'interface, ajoutez le sous-réseau local qui doit être chiffré via le tunnel IPsec (et dans ce cas, contient également les adresses du pool VPN), puis cliquez sur OK.



## 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. Cliquez sur + pour le noeud B :

> Sélectionnez l'extranet à partir du périphérique et indiquez le nom du périphérique homologue.

> Configurez les détails de l'homologue et ajoutez le sous-réseau distant qui doit être accessible via le tunnel VPN et cliquez sur OK.

## 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. Cliquez sur l'onglet IKE : Configurez les paramètres IKEv2 selon vos besoins

## 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

Cancel

Save

7. Cliquez sur l'onglet IPsec : Configurez les paramètres IPsec selon vos besoins.

## Edit VPN Topology

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

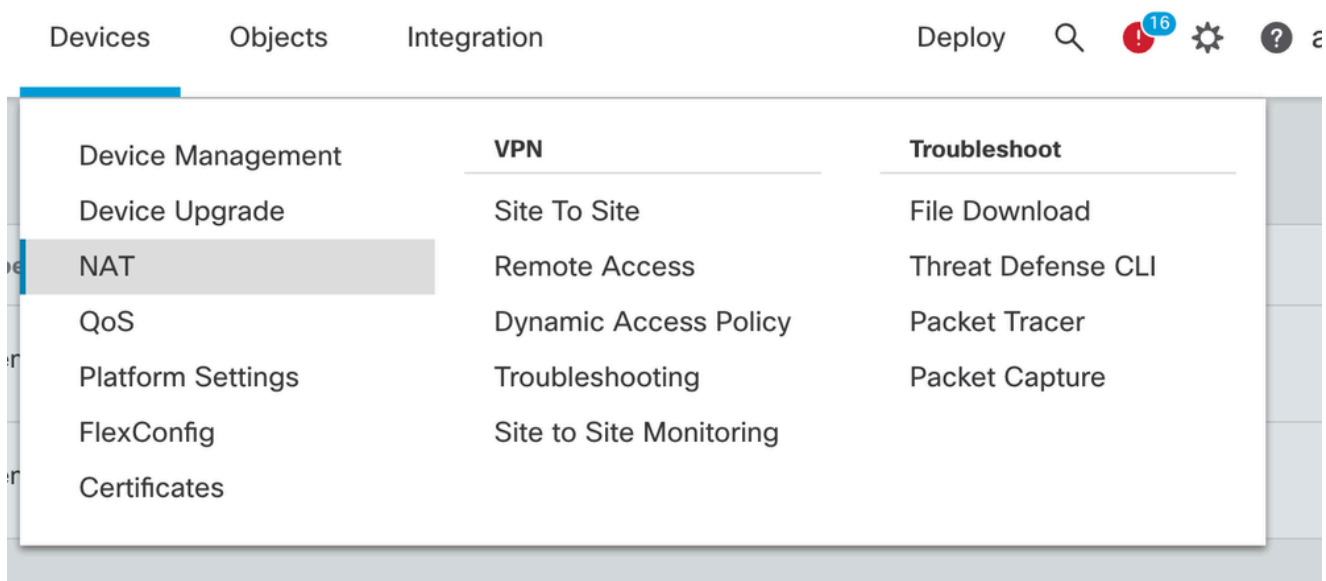
Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals\*

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. Configurer Nat-Exempt pour votre trafic intéressant (facultatif) Cliquez sur Devices > NAT



### 9. La NAT configurée ici permet aux utilisateurs RAVPN et internes d'accéder aux serveurs via le tunnel IPsec S2S.

|                          | # | 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<br>route-lookup<br>no-proxy-arp |  |
| <input type="checkbox"/> | 4 | ↔         | Static | sid_inside               | sid_outside                   | FTD-Lan          | Remote-Lan2           |                   | FTD-Lan            | Remote-Lan2             |                     | Dns:false<br>route-lookup<br>no-proxy-arp |  |
| <input type="checkbox"/> | 5 | ↔         | Static | sid_inside               | sid_outside                   | FTD-Lan          | Remote-Lan            |                   | FTD-Lan            | Remote-Lan              |                     | Dns:false<br>route-lookup<br>no-proxy-arp |  |

10. Effectuez de même la configuration sur l'autre extrémité homologue pour que le tunnel S2S s'active.

REMARQUE : la liste de contrôle d'accès de chiffrement ou les sous-réseaux de trafic intéressants doivent être des copies miroir l'un de l'autre sur les deux homologues.

## Vérifier

1. Pour vérifier la connexion 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. Pour vérifier la connexion 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. Pour vérifier la connexion IPsec :

<#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
```

## Dépannage

1. Pour résoudre le problème de connexion AnyConnect, collectez le bundle dart ou activez les débogages AnyConnect.
2. Pour dépanner le tunnel IKEv2, utilisez ces débogages :

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

3. Pour dépanner le problème de trafic sur le FTD, prenez la capture de paquets et vérifiez la configuration.



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.