

# Configure AnyConnect para acceder al servidor a través del túnel IPsec.

## Contenido

---

[Introducción:](#)

[Requisitos previos:](#)

[Requisitos básicos](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuraciones en FMC](#)

[Configuración de RAVPN en el FTD gestionado por FMC.](#)

[VPN IKEv2 en FTD gestionada por FMC:](#)

[Verificación](#)

[Troubleshoot](#)

---

## Introducción:

Este documento describe los procedimientos para implementar una configuración RAVPN en el FTD administrado por FMC y un túnel de sitio a sitio entre FTD.

## Requisitos previos:

### Requisitos básicos

- Un entendimiento básico de VPN de sitio a sitio y RAVPN es beneficioso.
- Es fundamental comprender los aspectos básicos de la configuración de un túnel basado en políticas IKEv2 en la plataforma Cisco Firepower.

Este procedimiento es para implementar una configuración RAVPN en el FTD administrado por FMC y un túnel de sitio a sitio entre FTD donde el usuario de AnyConnect puede acceder al servidor detrás del otro peer FTD.

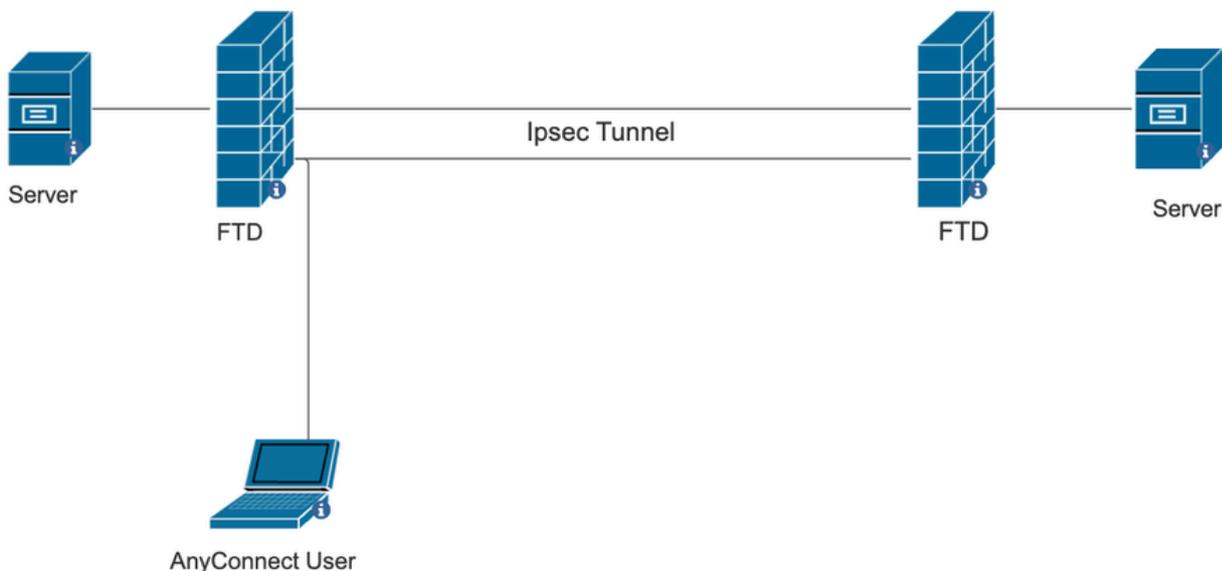
### Componentes Utilizados

- Cisco Firepower Threat Defense para VMware: versión 7.0.0
- Firepower Management Center: versión 7.2.4 (compilación 169)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está activa,

asegúrese de comprender el impacto potencial de cualquier comando..

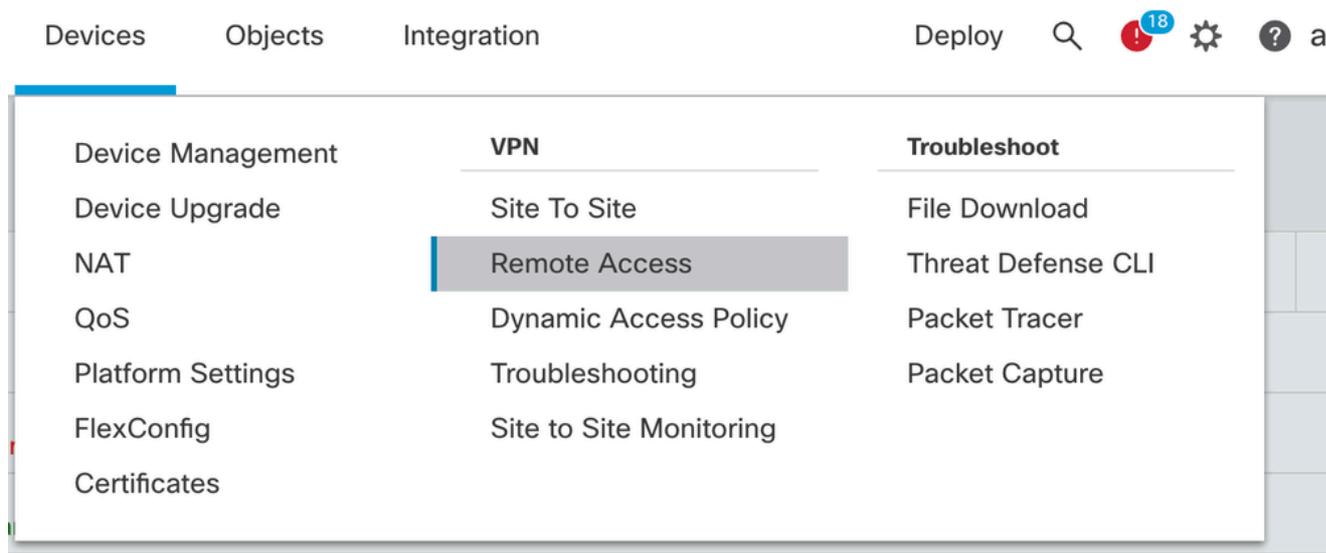
## Diagrama de la red



## Configuraciones en FMC

Configuración de RAVPN en el FTD gestionado por FMC.

1. Vaya a Devices > Remote Access.



2. Haga clic en Add (Agregar).
3. Configure un nombre y seleccione el FTD de los dispositivos disponibles y haga clic en

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:\*  
RAVPN

Description:

VPN Protocols:

- SSL
- IPsec-IKEv2

Targeted Devices:

Available Devices

Selected Devices

10.106.50.55

10.88.146.35

New\_FTD

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. Configure un nombre de perfil de conexión y elija el método de autenticación.

NOTA: Para este ejemplo de configuración, solo utilizamos AAA y autenticación local. Sin embargo, la configuración se basa en sus requisitos.

**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:\* RAVPN

**i** 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. Configure el grupo VPN que se utiliza para la asignación de direcciones IP para 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. Cree una política de grupo. Haga clic en + para crear una política de grupo. Agregue el nombre de la directiva de grupo.

### Edit Group Policy ?

Name:\*

Description:

General   AnyConnect   Advanced

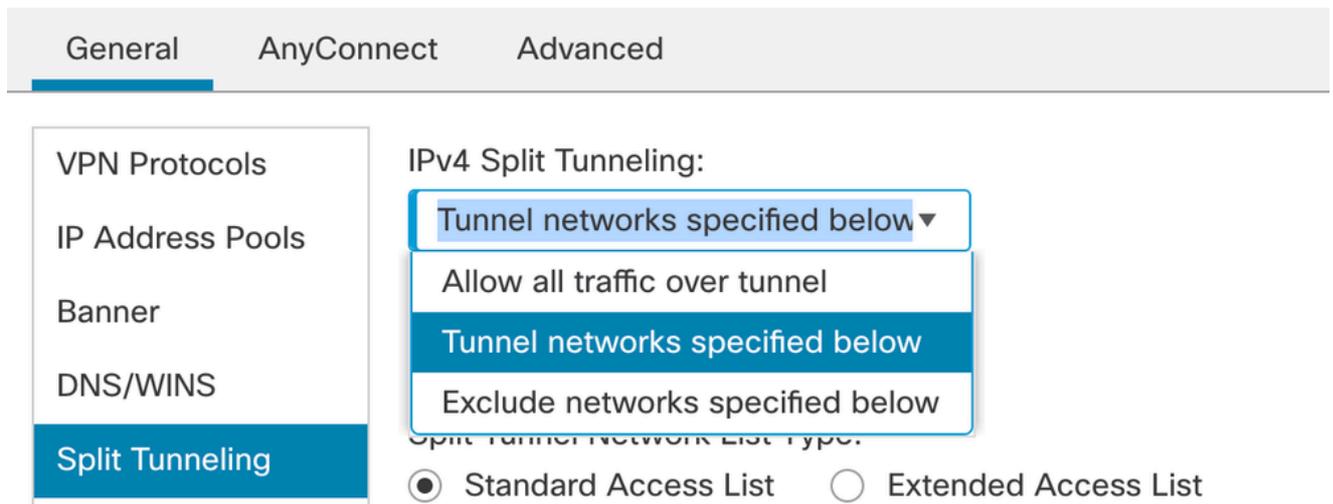
**VPN Protocols**

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

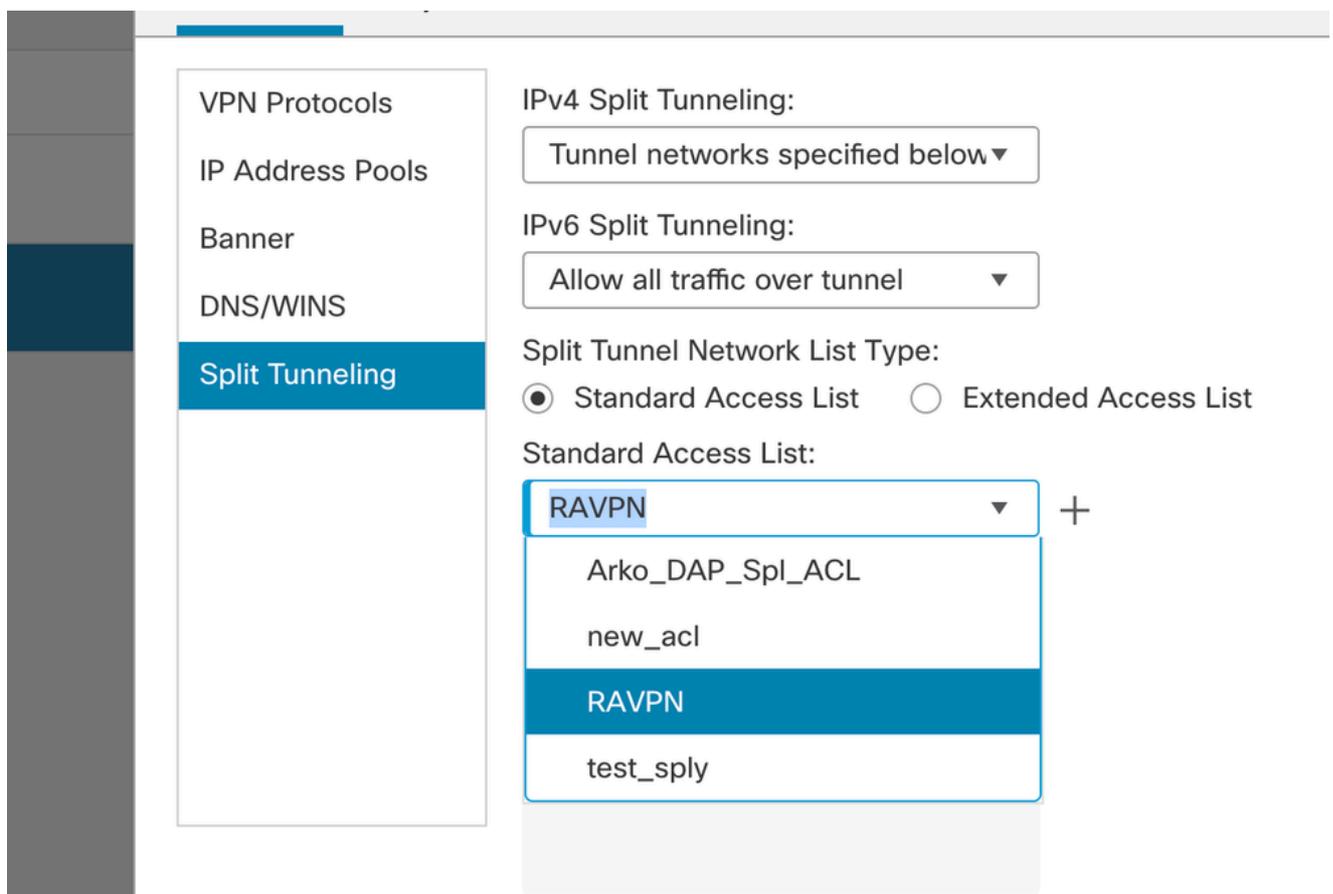
VPN Tunnel Protocol:  
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

- SSL
- IPsec-IKEv2

7. Vaya a Split tunneling. Seleccione las redes de túnel especificadas aquí:



8. Seleccione la lista de acceso correcta en la lista desplegable. Si todavía no hay una ACL configurada: haga clic en el icono + para agregar la lista de acceso Estándar y crear una nueva.  
Click Save.



9. Seleccione la política de grupo que se agrega y haga clic en 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. Seleccione la imagen de 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. Seleccione la interfaz que debe habilitarse para la conexión de AnyConnect, agregue el certificado, seleccione la directiva Omitir control de acceso para el tráfico descifrado y haga

### 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.*

clic en Siguiente.

## 12. Revise la configuración y haga clic en 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. Haga clic en Guardar e implementar.

**RAVPN** You have unsaved changes Save Cancel

Enter Description Policy Assignments (1)

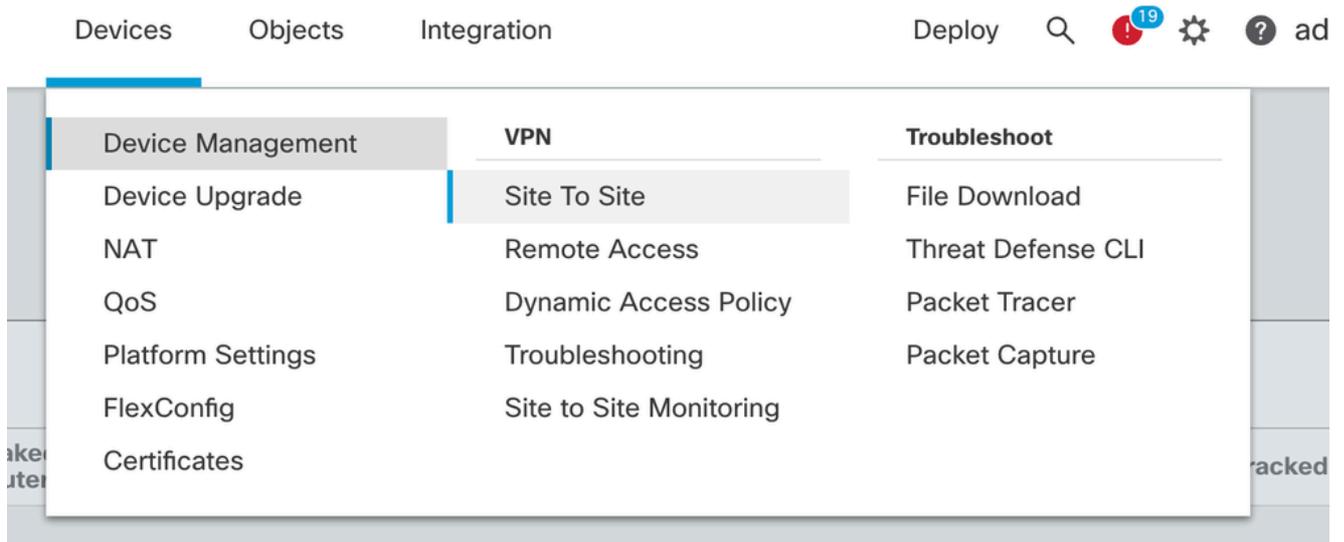
Local Realm: New\_Realm Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

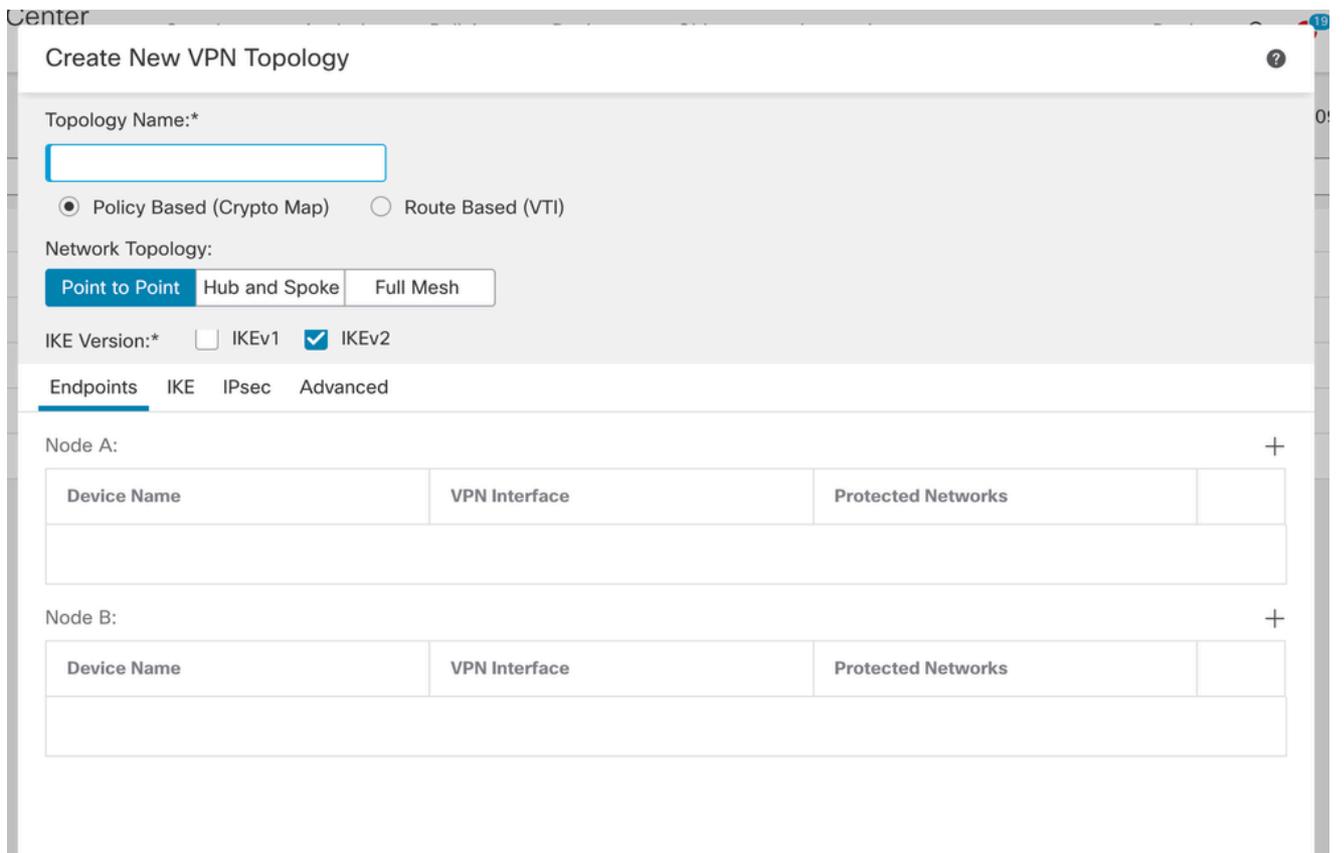
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN	

## VPN IKEv2 en FTD gestionada por FMC:

1. Vaya a Dispositivos > Sitio a sitio.



2. Haga clic en Add (Agregar).
3. Haga clic en + para el nodo A:



4. Seleccione el FTD en Device (Dispositivo), seleccione la interfaz, agregue la subred local que debe cifrarse a través del túnel IPsec (y, en este caso, también contiene las direcciones del grupo VPN) y haga clic en OK (Aceptar).

## 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. Haga clic en + para el nodo B:

> Seleccione Extranet en Device (Dispositivo) y asigne el nombre del dispositivo par.

> Configure los detalles del par y agregue la subred remota a la que se debe acceder a través del túnel VPN y haga clic en Aceptar.

## 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. Haga clic en la ficha IKE: Configure los parámetros de IKEv2 según sus necesidades

## 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. Haga clic en la ficha IPsec: Configure los parámetros de IPsec según sus requisitos.

## 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\*

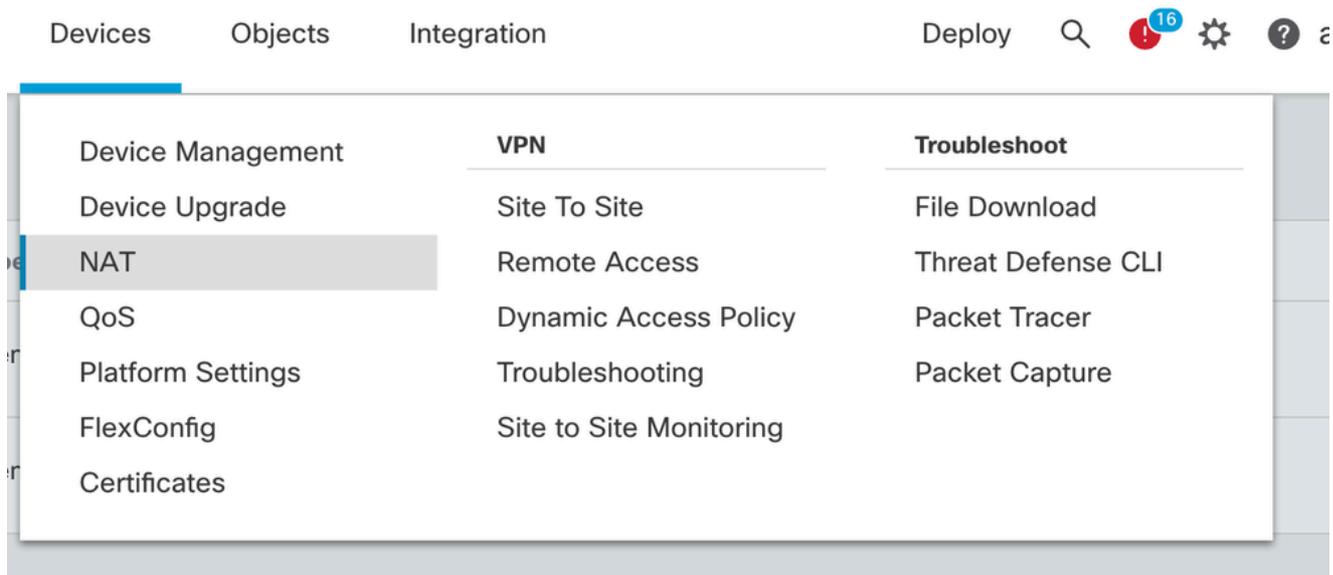
Enable Security Association (SA) Strength Enforcement  
 Enable Reverse Route Injection  
 Enable Perfect Forward Secrecy

Modulus Group:

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

Lifetime Size:  Kbytes (Range 10-2147483647)

### 8. Configure Nat-Exempt para su tráfico interesante (Opcional) Haga clic en Devices > NAT



### 9. La NAT configurada aquí permite a la RAVPN y a los usuarios internos acceder a los servidores a través del túnel IPsec S2S.

						Original Packet			Translated Packet				
<input type="checkbox"/>	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
<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. De manera similar, la configuración en el otro extremo del par para que aparezca el túnel S2S.

NOTA: La ACL crypto o las subredes de tráfico interesantes tienen que ser copias simétricas entre sí en ambos peers.

## Verificación

1. Para verificar la conexión 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. Para verificar la conexión 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. Para verificar la conexión 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
```

## Troubleshoot

1. Para solucionar el problema de conexión de AnyConnect, recopile el paquete dart o habilite las depuraciones de AnyConnect.
2. Para resolver problemas del túnel IKEv2, utilice estos debugs:

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

3. Para resolver el problema de tráfico en el FTD, tome la captura de paquetes y verifique la configuración.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).