

# Configuración de VPN de sitio a sitio en FTD gestionada por FMC

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Paso 1. Defina la topología VPN.](#)

[Paso 2. Configure los Parámetros IKE.](#)

[Paso 3. Configure los Parámetros de IPsec.](#)

[Paso 4. Omitir control de acceso.](#)

[Paso 5. Cree una política de control de acceso.](#)

[Paso 6. Configure la exención de NAT.](#)

[Paso 7. Configure el ASA.](#)

[Verificación](#)

[Solución de problemas y depuración](#)

[Problemas de conectividad iniciales](#)

[Problemas específicos del tráfico](#)

## Introducción

Este documento proporciona un ejemplo de configuración para VPN de sitio a sitio en Firepower Threat Defense (FTD) administrado por FMC.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de VPN
- Experiencia con Firepower Management Center
- Experiencia con la línea de comandos ASA

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTD 6.5
- ASA 9.10(1)32

- IKEv2

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configuración

Comience con la configuración en FTD con FirePower Management Center.

### Paso 1. Defina la topología VPN.

1. Navegue hasta **Dispositivos > VPN > Sitio a Sitio**. En **Add VPN**, haga clic en **Firepower Threat Defense Device**, como se muestra en esta imagen.



2. Aparece el cuadro **Create New VPN Topology** . Dé a VPN un nombre que se pueda identificar fácilmente.

Topología de red: Punto a punto

Versión IKE: IKEv2

En este ejemplo, cuando se seleccionan extremos, el Nodo A es el FTD y el Nodo B es el ASA. Haga clic en el botón verde más para agregar dispositivos a la topología, como se muestra en esta imagen.

### Create New VPN Topology

Topology Name:\*

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

**i** Ensure the protected networks are allowed by access control policy of each device.

3. Agregue el FTD como el primer terminal.

Elija la interfaz en la que se coloca un mapa criptográfico. La dirección IP se debe rellenar automáticamente a partir de la configuración del dispositivo.

Haga clic en el signo verde más en Redes protegidas, como se muestra en esta imagen, para seleccionar las subredes que se deben cifrar en esta VPN.

## Add Endpoint




Device:\*

Interface:\*

IP Address:\*


This IP is Private

Connection Type:

Certificate Map:  

Protected Networks:\*

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

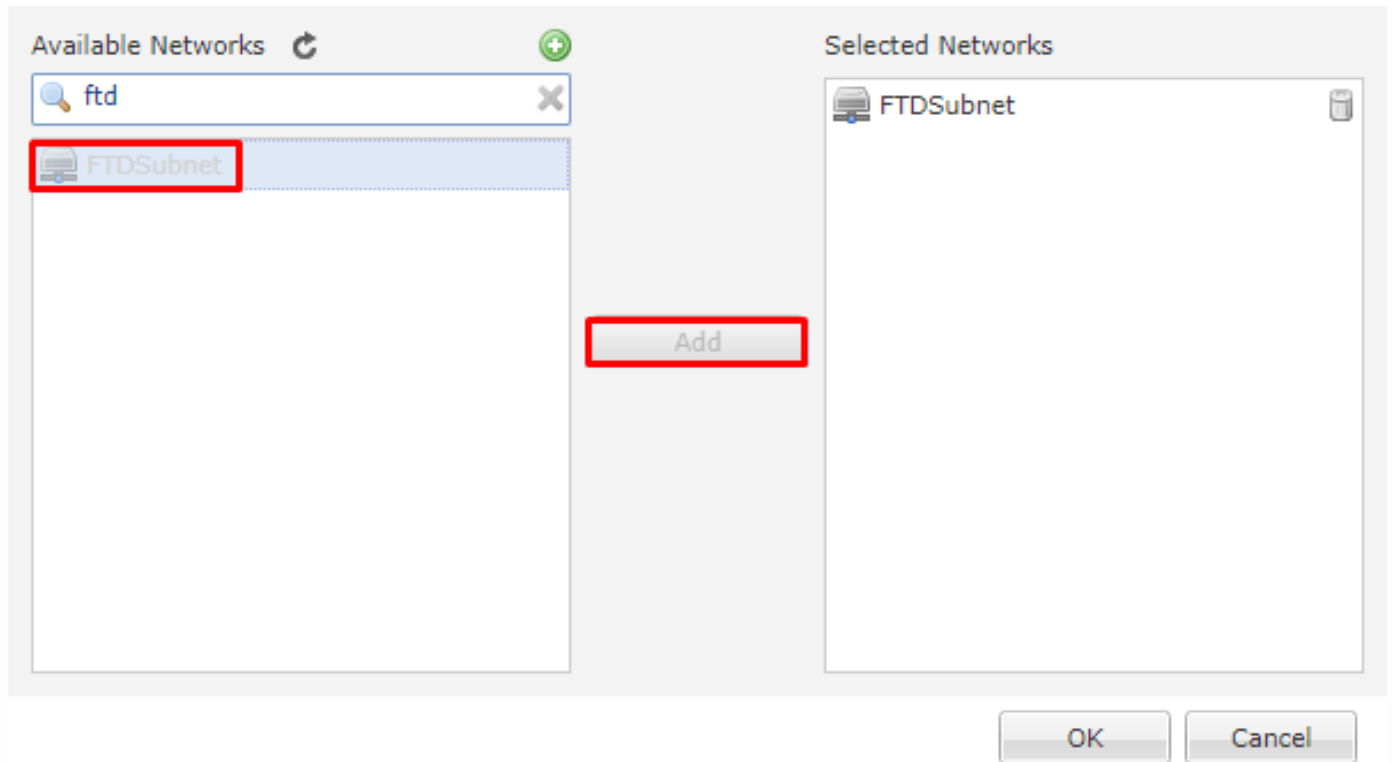


4. Haga clic en verde más y aquí se creará un objeto de red.

5. Agregue todas las subredes locales al FTD que deben cifrarse. Haga clic en **Agregar** para moverlos a las redes seleccionadas. Ahora haga clic en **Aceptar**, como se muestra en esta imagen.

FTDSubnet = 10.10.113.0/24

## Network Objects



Nodo A: (FTD) se ha completado. Haga clic en el verde más para el nodo B, como se muestra en la imagen.

### Create New VPN Topology

Topology Name: RTPVPN-ASA

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
FTD	outside/172.16.100.20	FTDSubnet

Node B:

Device Name	VPN Interface	Protected Networks
-------------	---------------	--------------------

ⓘ Ensure the protected networks are allowed by access control policy of each device.

Save Cancel

El nodo B es un ASA. Los dispositivos que no son administrados por FMC se consideran Extranet.

6. Agregue un nombre de dispositivo y una dirección IP. Haga clic en el símbolo verde más para agregar redes protegidas, como se muestra en la imagen.

## Edit Endpoint



Device:\*

Device Name:\*

IP Address:\*  Static  Dynamic

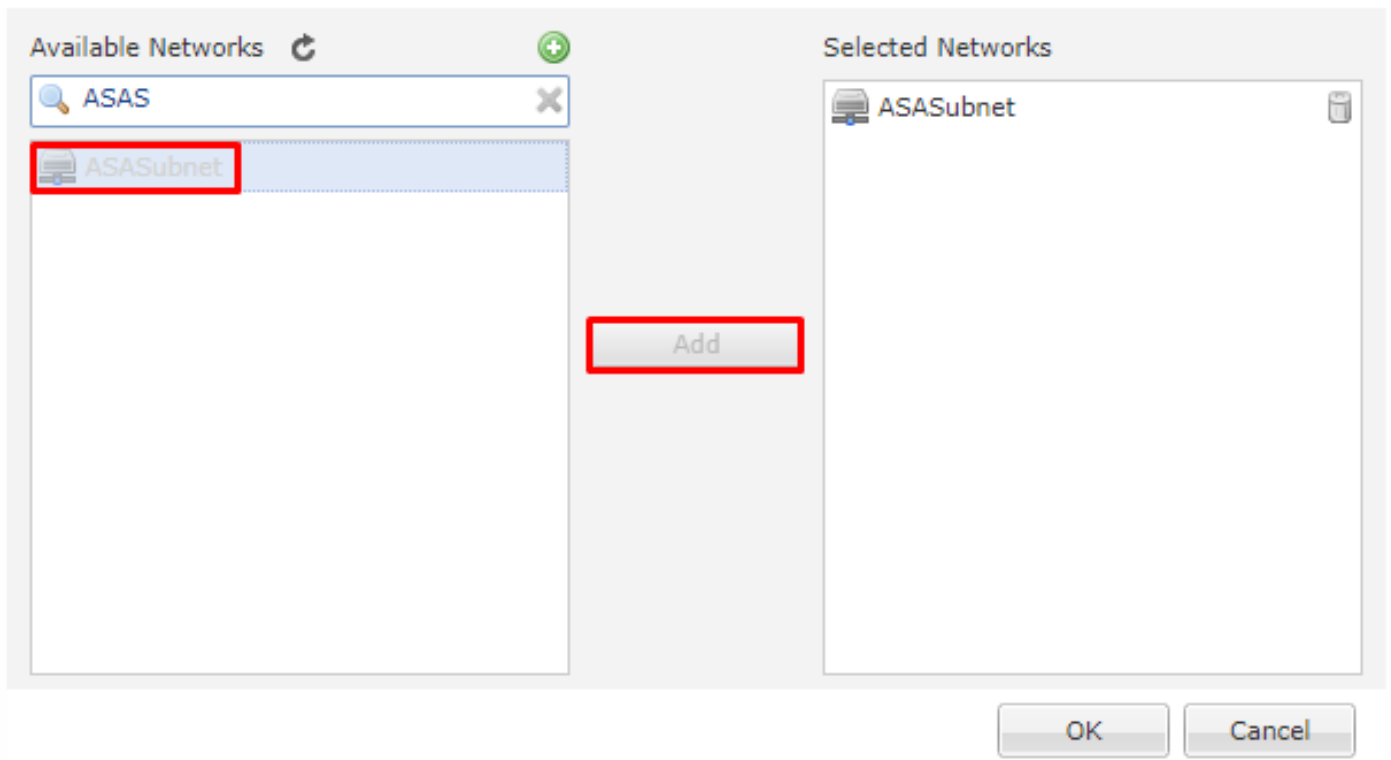
Certificate Map:

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

7. Como se muestra en esta imagen, seleccione las **subredes ASA** que deben cifrarse y agréguelas a las redes seleccionadas.

ASASubnet = 10.10.110.0/24

## Network Objects



### Paso 2. Configure los Parámetros IKE.

Ahora ambos terminales están instalados, pase por la configuración IKE/IPSEC.

1. En la pestaña **IKE**, especifique los parámetros que se utilizan para el intercambio inicial IKEv2. Haga clic en el símbolo verde más para crear una nueva política IKE, como se muestra en la imagen.



### Create New VPN Topology ? X

Topology Name:\*

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\*  +

Authentication Type:

Pre-shared Key Length:\*  Characters (Range 1-127)

**IKEv2 Settings**

Policy:\*  +

Authentication Type:

Pre-shared Key Length:\*  Characters (Range 1-127)

2. En la nueva política IKE, especifique un número de prioridad así como la duración de la fase 1 de la conexión. Este documento utiliza estos parámetros para el intercambio inicial: Integrity (SHA256), Encryption (AES-256), PRF (SHA256) y Diffie-Hellman Group (Grupo 14)

**Nota:** Todas las políticas IKE del dispositivo se envían al par remoto independientemente de lo que esté en la sección de políticas seleccionada. Se seleccionará la primera política IKE coincidente con el par remoto para la conexión VPN. Elija la política que se envía primero utilizando el campo de prioridad. La prioridad 1 se enviará primero.

# New IKEv2 Policy

Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

- Integrity Algorithms**
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

- Available Algorithms
- MD5
  - SHA
  - SHA512
  - SHA256**
  - SHA384
  - NULL

Add

- Selected Algorithms
- SHA256

Save Cancel

# New IKEv2 Policy

Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

Integrity Algorithms

**Encryption Algorithms**

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

## New IKEv2 Policy



Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

### Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384

Add

### Selected Algorithms

- SHA256

Save Cancel

## New IKEv2 Policy



Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

**Diffie-Hellman Group**

Available Groups

- 1
- 2
- 5
- 14**
- 15
- 16
- 19
- 20
- 21

Add

Selected Groups

- 14

Save Cancel

- Una vez agregados los parámetros, seleccione esta política y elija el **Tipo de autenticación**.
- Elija el manual **de clave previamente compartida**. Para este documento, se utiliza PSK cisco123.

**Create New VPN Topology** ? X

Topology Name:\* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

**Endpoints** **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\* preshared\_sha\_aes256\_dh5\_5

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

**IKEv2 Settings**

Policy:\* **ASA**

Authentication Type: **Pre-shared Manual Key**

Key:\* .....

Confirm Key:\* .....

Enforce hex-based pre-shared key only

Save Cancel

### Paso 3. Configure los Parámetros de IPsec.

1. En **IPsec**, haga clic en el lápiz para editar el conjunto de transformación y crear una nueva propuesta de IPsec, como se muestra en esta imagen.

## Create New VPN Topology

? x

Topology Name:\* RTPVPN-ASA



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  IKEv2 IPsec Proposals\*   
tunnel\_aes256\_sha AES-GCM

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Save Cancel

2. Para crear una nueva propuesta IPsec de IKEv2, haga clic en el verde más e introduzca los parámetros de la fase 2.

Seleccione **Cifrado ESP > AES-GCM-256**. Cuando se utiliza el algoritmo GCM para el cifrado, no se necesita un algoritmo Hash. Con GCM, la función hash está integrada.

## Edit IKEv2 IPsec Proposal



Name:\* ASA

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-25

Add

Selected Algorithms

- AES-GCM-256

Save Cancel

3. Una vez creada la nueva propuesta de IPsec, agréguela a los conjuntos de transformación seleccionados.

## IKEv2 IPsec Proposal



Available Transform Sets

Search

- AES-GCM
- AES-SHA
- ASA
- DES\_SHA-1

Add

Selected Transform Sets

- ASA

OK Cancel

La propuesta IPsec recién seleccionada aparece en las propuestas IPsec de IKEv2.



Si es necesario, la vida útil de la fase 2 y PFS se pueden editar aquí. Para este ejemplo, la duración se establecerá como predeterminada y PFS se desactivará.

**Create New VPN Topology**

Topology Name: RTPVPN-ASA

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\*: ASA

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

Opcional: debe completar la opción para omitir el control de acceso o Crear una directiva de control de acceso.

#### Paso 4. Omitir control de acceso.

Opcionalmente, `sysopt permit-vpn` se puede habilitar bajo el **Avanzado > Túnel**.

Esto elimina la posibilidad de utilizar la política de control de acceso para inspeccionar el tráfico proveniente de los usuarios. Los filtros VPN o las ACL descargables todavía se pueden utilizar para filtrar el tráfico de los usuarios. Este es un comando global y se aplicará a todas las VPN si esta casilla de verificación está activada.

**Create New VPN Topology** ? x

Topology Name:\* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints IKE IPsec **Advanced**

IKE  
IPsec  
**Tunnel**

NAT Settings

Keepalive Messages Traversal  
Interval: 20 Seconds (Range 10 - 3600)

**Access Control for VPN Traffic**

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

Certificate Map Settings

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

Save Cancel

Si **sysopt permit-vpn** no está habilitado, se debe crear una política de control de acceso para permitir el tráfico VPN a través del dispositivo FTD. Si **sysopt permit-vpn** está habilitado, omite la creación de una política de control de acceso.

## Paso 5. Cree una política de control de acceso.

En Políticas de control de acceso, navegue hasta **Políticas > Control de acceso > Control de acceso** y seleccione la política que se dirige al dispositivo FTD. Para agregar una regla, haga clic en **Agregar regla**, como se muestra en la imagen aquí.

Se debe permitir el tráfico de la red interna a la red externa y de la red externa a la red interna. Cree una regla para ambas o cree dos reglas para mantenerlas separadas. En este ejemplo, se crea una regla para ambas.

## Editing Rule - VPN\_Traffic

Name: VPN\_Traffic  Enabled Move

Action: Allow

Zones: Networks | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks:  +

Source Networks (2):

Source	Original Client
ASASubnet	
FTDSubnet	

Destination Networks (2):

ASASubnet
FTDSubnet

Buttons: Add To Source Networks, Add to Destination, Save, Cancel

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Filter by Device | Show Rule Conflicts | Add Category | Add Rule | Search Rules

Name	Source Zone	Dest Zones	Source Networks	Dest Networks	VL...	Us...	Ap...	So...	De...	URLs	So...	De...	A...
1 VPN_Traffic	Inside Outside	Inside Outside	ASASubnet FTDSubnet	ASASubnet FTDSubnet	Any	Any	Any	Any	Any	Any	Any	Any	Any

Default Action: Access Control: Block All Traffic

## Paso 6. Configure la exención de NAT.

Configure una declaración de exención de NAT para el tráfico VPN. La exención de NAT debe estar implementada para evitar que el tráfico VPN llegue a otra sentencia NAT y traduzca incorrectamente el tráfico VPN.

1. Navegue hasta **Dispositivos > NAT**, seleccione la política NAT dirigida al FTD. Cree una nueva regla al hacer clic en el botón **Agregar regla**.

Overview | Analysis | Policies | **Devices** | Objects | AMP | Intelligence

Device Management | **NAT** | VPN | QoS | Platform Settings | FlexConfig | Certificates

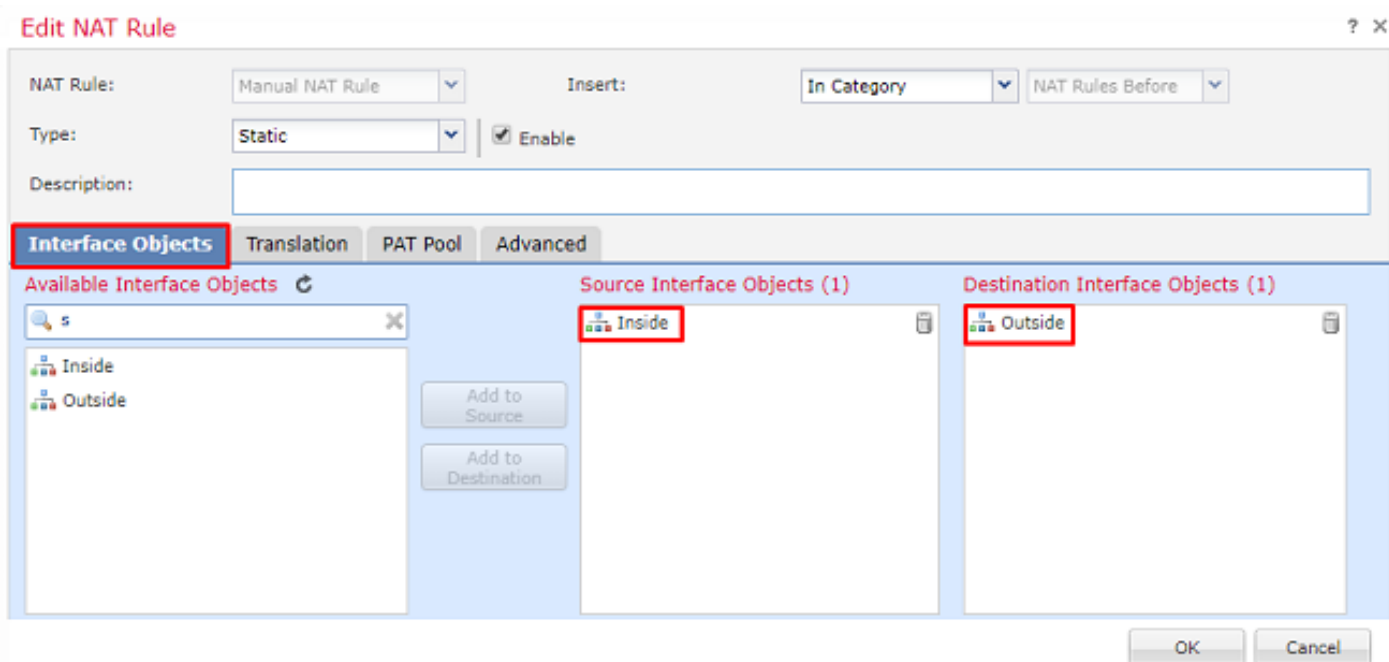
VirtualFTDNAT

Rules

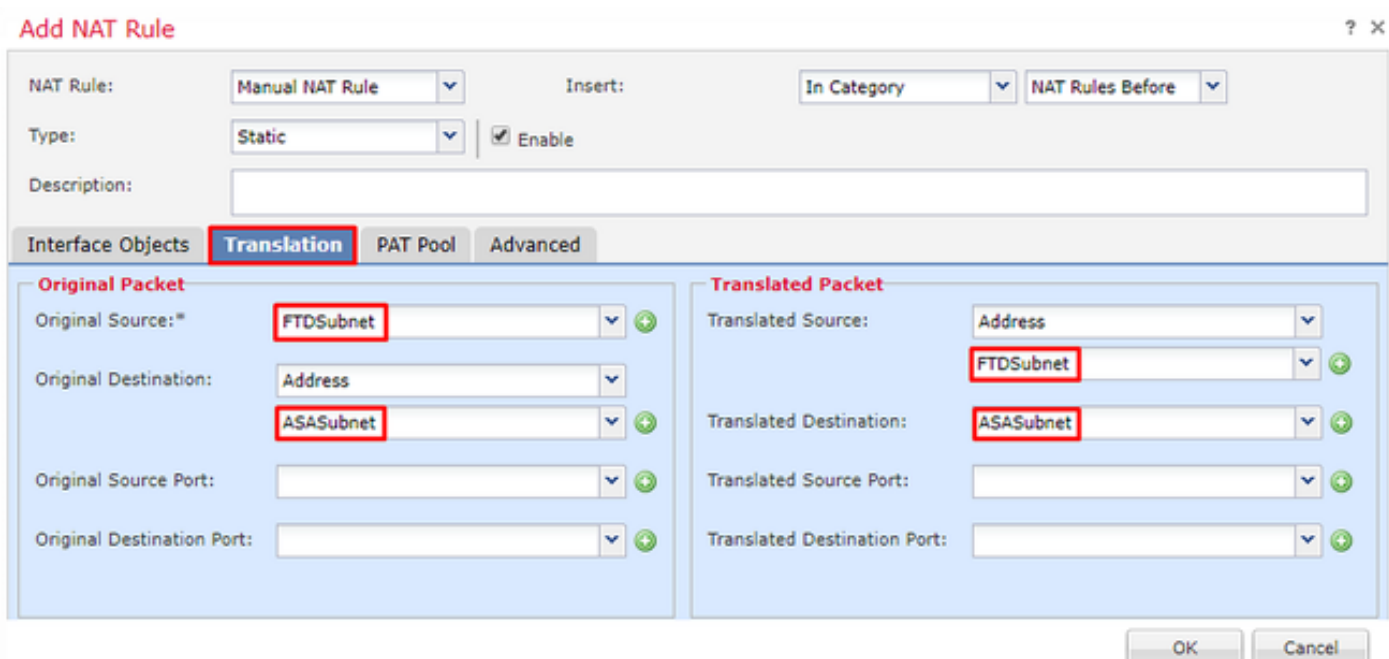
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	

Buttons: Show Warnings, Add Rule

2. Cree una nueva regla NAT estática manual. Haga referencia a las interfaces interna y externa.



3. En la pestaña **Traducción** y seleccione las subredes de origen y destino. Como esta es una regla de exención de NAT, haga que el origen/destino original y el origen/destino traducido sean iguales, como se muestra en esta imagen:



4. Por último, pase a la pestaña **Avanzadas** y habilite no-proxy-arp y route-lookup.

**Add NAT Rule** ? X

NAT Rule:  Insert:

Type:   Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

5. Guarde esta regla y observe los resultados finales en la lista NAT.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

**VirtualFTDNAT**  
Enter Description Policy Assignments

Rules Add Rule

Filter by Device

#	Direction	Type	Source Interface...	Destination Interface...	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
1	↔	Static	Inside	Outside	FTDSubnet	ASASubnet		FTDSubnet	ASASubnet		Dns:fal route-k no-pro
▼ Auto NAT Rules											
#	↔	Dynamic	Inside	Outside	any-obj			Interface			Dns:fal
▼ NAT Rules After											

6. Una vez completada la configuración, guarde e implemente la configuración en el FTD.

## Paso 7. Configure el ASA.

1. Habilite IKEv2 en la interfaz exterior del ASA:

```
Crypto ikev2 enable outside
```

2. Cree la política IKEv2 que define los mismos parámetros configurados en el FTD:

```
Crypto ikev2 policy 1
Encryption aes-256
Integrity sha256
Group 14
Prf sha256
Lifetime seconds 86400
```

3. Cree una política de grupo que permita el protocolo ikev2:

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
Vpn-tunnel-protocol ikev2
```

4. Cree un grupo de túnel para la dirección IP pública FTD de peer. Haga referencia a la política de grupo y especifique la clave previamente compartida:

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
```

5. Cree una lista de acceso que defina el tráfico que se cifrará: (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSUBNET
Subnet 10.10.113.0 255.255.255.0
Object network ASASUBNET
Subnet 10.10.110.0 255.255.255.0
Access-list ASAToFTD extended permit ip object ASASUBNET object FTDSUBNET
```

6. Cree una propuesta ipsec ikev2 que haga referencia a los algoritmos especificados en FTD:

```
Crypto ipsec ikev2 ipsec-proposal FTD
Protocol esp encryption aes-gcm-256
```

7. Cree una entrada de mapa criptográfico que vincule la configuración:

```
Crypto map outside_map 10 set peer 172.16.100.20
Crypto map outside_map 10 match address ASAToFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. Cree una declaración de exención de NAT que evite que el firewall NATURE el tráfico VPN:

```
Nat (inside,outside) 1 source static ASASUBNET ASASUBNET destination static FTDSUBNET FTDSUBNET
no-proxy-arp route-lookup
```

## Verificación

**Nota:** En este momento no hay forma de revisar el estado del túnel VPN desde el FMC. Hay una solicitud de mejora para esta capacidad [CSCvh77603](#).

Intente iniciar el tráfico a través del túnel VPN. Con el acceso a la línea de comandos del ASA o FTD, esto se puede hacer con el comando packet tracer. Cuando se utiliza el comando packet-tracer para activar el túnel VPN, se debe ejecutar dos veces para verificar que el túnel se activa. La primera vez que se ejecuta el comando, el túnel VPN se encuentra inactivo, por lo que el comando packet-tracer fallará con el DROP de cifrado VPN. No utilice la dirección IP interna del firewall como la dirección IP de origen en el packet-tracer ya que esto siempre fallará.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

Phase: 10  
Type: VPN  
Subtype: encrypt  
Result: DROP  
Config:  
Additional Information:

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

Phase: 1  
Type: ROUTE-LOOKUP  
Subtype: Resolve Egress Interface  
Result: ALLOW  
Config:  
Additional Information:  
found next-hop 172.16.100.1 using egress ifc outside

Phase: 2  
Type: UN-NAT  
Subtype: static  
Result: ALLOW  
Config:  
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet  
no-proxy-arp route-lookup  
Additional Information:  
NAT divert to egress interface outside  
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3  
Type: ACCESS-LIST  
Subtype: log  
Result: ALLOW  
Config:  
access-group CSM\_FW\_ACL\_ global  
access-list CSM\_FW\_ACL\_ advanced permit ip ifc Inside object-group FMC\_INLINE\_src\_rule\_268436483  
ifc outside object-group FMC\_INLINE\_dst\_rule\_268436483 rule-id 268436483  
access-list CSM\_FW\_ACL\_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy -  
Mandatory  
access-list CSM\_FW\_ACL\_ remark rule-id 268436483: L7 RULE: VPN\_Traffic  
object-group network FMC\_INLINE\_src\_rule\_268436483  
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-  
Policy/mandatory)  
network-object object ASASubnet  
network-object object FTDSubnet  
object-group network FMC\_INLINE\_dst\_rule\_268436483  
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-  
Policy/mandatory)  
network-object object ASASubnet  
network-object object FTDSubnet  
Additional Information:  
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5  
Type: NAT  
Subtype:  
Result: ALLOW  
Config:  
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet  
no-proxy-arp route-lookup  
Additional Information:  
Static translate 10.10.113.10/0 to 10.10.113.10/0

Phase: 10  
Type: VPN  
Subtype: encrypt  
Result: ALLOW  
Config:  
Additional Information:

Result:  
input-interface: Inside  
input-status: up  
input-line-status: up  
output-interface: outside  
output-status: up  
output-line-status: up  
Action: allow

Para monitorear el estado del túnel, navegue a la CLI del FTD o ASA.

Desde la CLI de FTD, verifique la fase 1 y la fase 2 con este comando:

## Show crypto ikev2 sa

```
> show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local

Remote	Status	Role
9528731 172.16.100.20/500		
192.168.200.10/500	<b>READY</b>	INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/118 sec

Child sa: local selector 10.10.113.0/0 - 10.10.113.255/65535

remote selector 10.10.110.0/0 - 10.10.110.255/65535

ESP spi in/out: 0x66be357d/0xb74c8753

## Solución de problemas y depuración

### Problemas de conectividad iniciales

Al construir una VPN, hay dos lados negociando el túnel. Por lo tanto, es mejor obtener ambos lados de la conversación cuando resuelva cualquier tipo de falla del túnel. Puede encontrar una guía detallada sobre cómo depurar túneles IKEv2 aquí: [Cómo depurar VPN IKEv2](#)

La causa más común de las fallas del túnel es un problema de conectividad. La mejor manera de determinar esto es tomar capturas de paquetes en el dispositivo. Utilice este comando para tomar capturas de paquetes en el dispositivo:

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

Una vez que la captura está en su lugar, intente enviar tráfico a través de la VPN y verificar si hay tráfico bidireccional en la captura de paquetes.

Revise la captura de paquetes con este comando:



## show cap capout

```
firepower# show cap capout
```

```
4 packets captured
```

```
1: 11:51:12.059628      172.16.100.20.500 > 192.168.200.10.500:  udp 690
2: 11:51:12.065243      192.168.200.10.500 > 172.16.100.20.500:  udp 619
3: 11:51:12.066692      172.16.100.20.500 > 192.168.200.10.500:  udp 288
4: 11:51:12.069835      192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

## Problemas específicos del tráfico

Los problemas de tráfico habituales que experimenta son:

- Problemas de ruteo detrás del FTD: la red interna no puede rutear los paquetes a las direcciones IP asignadas y a los clientes VPN.
- Listas de control de acceso que bloquean el tráfico.
- No se omite la traducción de direcciones de red para el tráfico VPN.

Para obtener más información sobre las VPN en el FTD administrado por FMC, puede encontrar la guía de configuración completa aquí: [FTD administrado por la guía de configuración de FMC](#)