

# Configuración del túnel de sitio a sitio IPv2 IPv6 entre ASA y FTD

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración ASA](#)

[Configuración de FTD](#)

[Omitir control de acceso](#)

[Configuración de la exención de NAT](#)

[Verificación](#)

[Troubleshoot](#)

[Referencias](#)

## Introducción

Este documento proporciona un ejemplo de configuración para configurar un túnel de sitio a sitio IPv6 entre un ASA (Adaptive Security Appliance) y FTD (Firepower Threat Defense) mediante el protocolo Internet Key Exchange versión 2 (IKEv2). La configuración incluye conectividad de red IPv6 de extremo a extremo con ASA y FTD como dispositivos de terminación VPN.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento fundamental de la configuración CLI de ASA
- Conocimiento fundamental de los protocolos IKEv2 e IPSEC
- Introducción al direccionamiento y el ruteo IPv6
- Comprensión básica de la configuración de FTD a través de FMC

## Componentes Utilizados

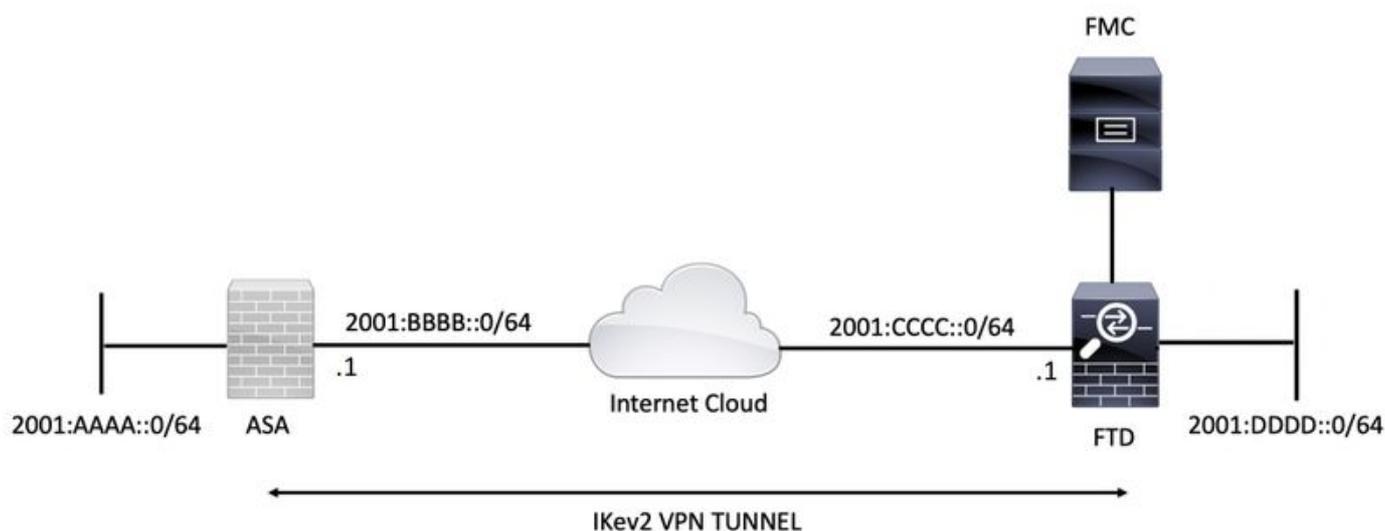
La información de este documento se basa en un entorno virtual, creado a partir de dispositivos en una configuración de laboratorio específica. All of the devices used in this document started with a cleared (default) configuration. Si su red está en producción, asegúrese de comprender el impacto potencial de cualquier comando.

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

- Cisco ASA con 9.6.(4)12
- Cisco FTD con 6.5.0
- Cisco FMC con 6.6.0

## Configurar

### Diagrama de la red



### Configuración ASA

Esta sección describe la configuración requerida en el ASA.

Paso 1. Configure las interfaces ASA.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable
```

```
interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

Paso 2. Establezca una ruta predeterminada IPv6.

```
ipv6 route outside ::/0 2001:bbbb::2
```

Paso 3. Configure la política IKEv2 y habilite IKEv2 en la interfaz exterior.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

#### Paso 4. Configure el Grupo de Túnel.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

#### Paso 5. Cree los objetos y la Lista de control de acceso (ACL) para que coincidan con el tráfico interesante.

```
object-group network local-network
network-object 2001:aaaa::/64
```

```
object-group network remote-network
network-object 2001:dddd::/64
```

```
access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

#### Paso 6. Configure las reglas de traducción de direcciones de red (NAT) de identidad para el tráfico interesante.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

#### Paso 7. Configure la propuesta IPsec de IKEv2.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

#### Paso 8. Configure el mapa criptográfico y aplíquelo a la interfaz externa.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route
```

```
crypto map VPN interface outside
```

## Configuración de FTD

Esta sección proporciona instrucciones para configurar un FTD mediante FMC.

### Definir la topología VPN

Paso 1. Navegue hasta **Dispositivos > VPN > Sitio a Sitio**.

Seleccionar 'Agregue VPN' y elija 'Firepower Threat Defense Device', como se muestra en esta imagen.

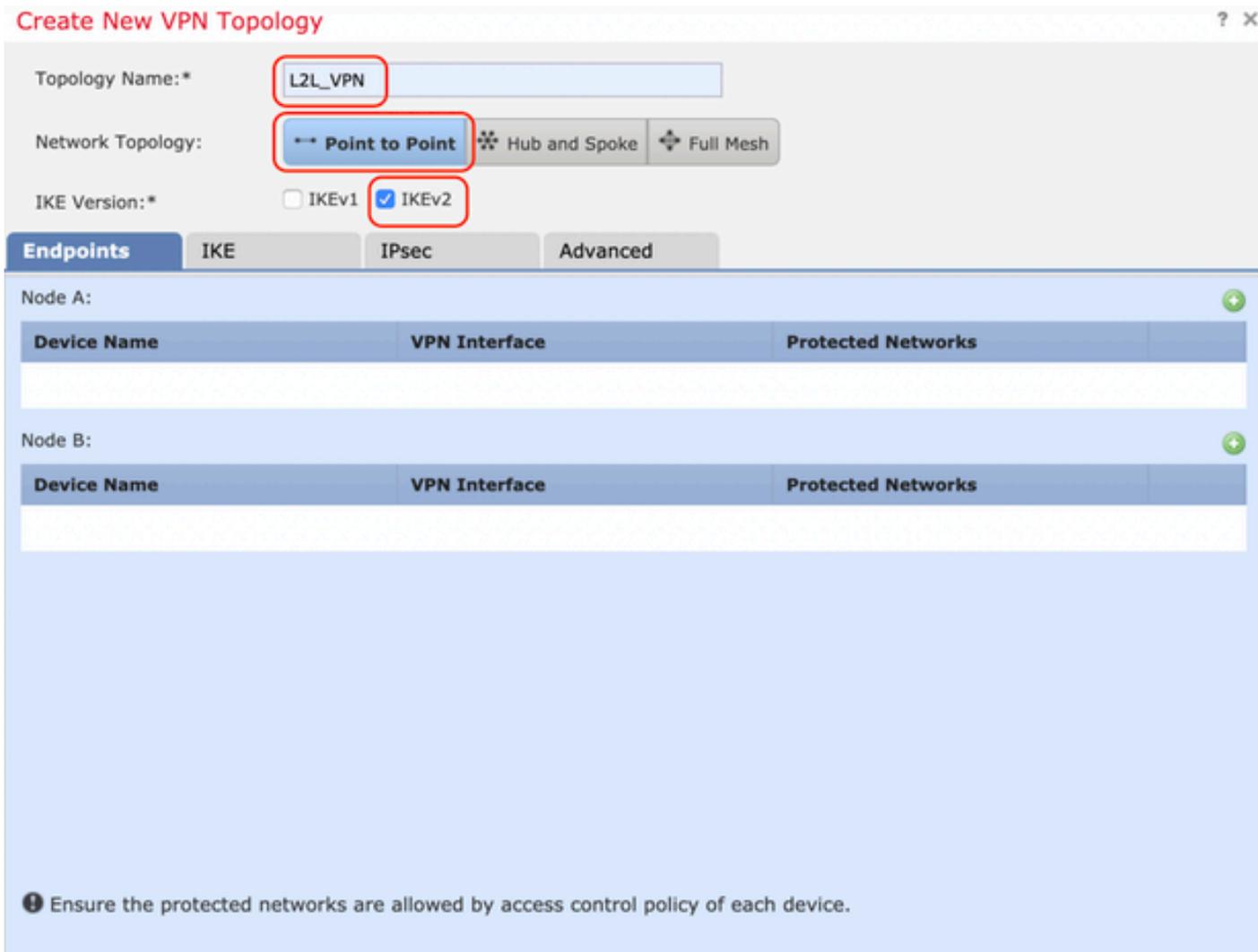


Paso 2. Aparece el cuadro 'Crear nueva topología VPN'. Dé a la VPN un nombre fácilmente identificable.

Topología de red: Punto a punto

Versión IKE: IKEv2

En este ejemplo, al seleccionar los extremos, el Nodo A es el FTD. El nodo B es ASA. Haga clic en el botón verde más para agregar dispositivos a la topología.



Paso 3. Agregue el FTD como el primer terminal.

Elija la interfaz donde se aplica el mapa criptográfico. La dirección IP se debe rellenar automáticamente a partir de la configuración del dispositivo.

Haga clic en el icono verde más bajo Redes protegidas para seleccionar subredes cifradas a través de este túnel VPN. En este ejemplo, el objeto de red 'Proxy local' en FMC consta de la subred IPv6 '2001:DDDD::/64'.

## Edit Endpoint



Device:\*

FTDv

Interface:\*

OUTSIDE

IP Address:\*

2001:CCCC::1

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

Protected Networks:\*

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

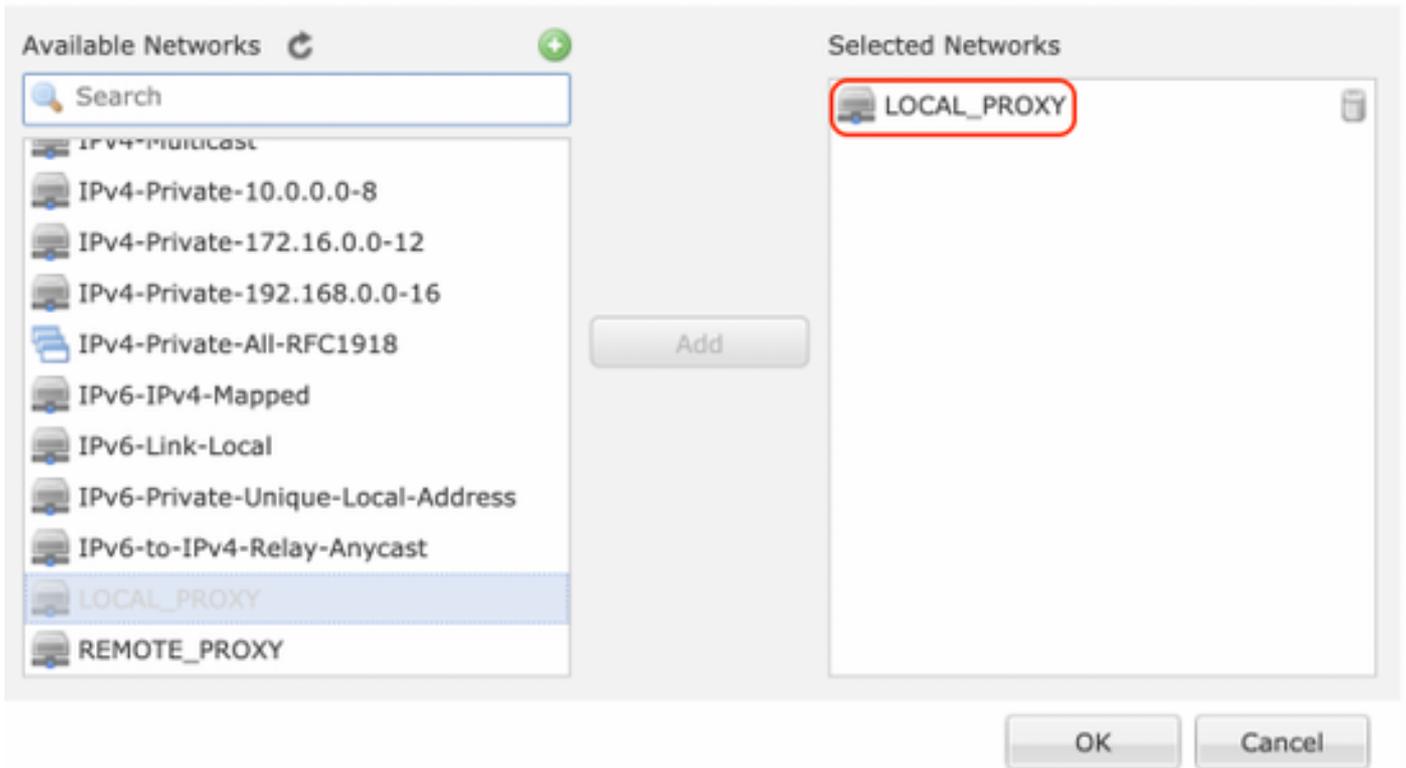


LOCAL\_PROXY

OK

Cancel

## Network Objects



Con el paso anterior, la configuración del terminal FTD está completa.

Paso 4. Haga clic en el icono verde más para el Nodo B que es un ASA en el ejemplo de configuración. Los dispositivos que no son administrados por FMC se consideran Extranet. Agregue un nombre de dispositivo y una dirección IP.

Paso 5. Seleccione el icono verde más para agregar redes protegidas.

### Edit Endpoint ? X

Device:\* Extranet

Device Name:\* ASA

IP Address:\*  Static  Dynamic  
2001:BBBB::1

Certificate Map:  +

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

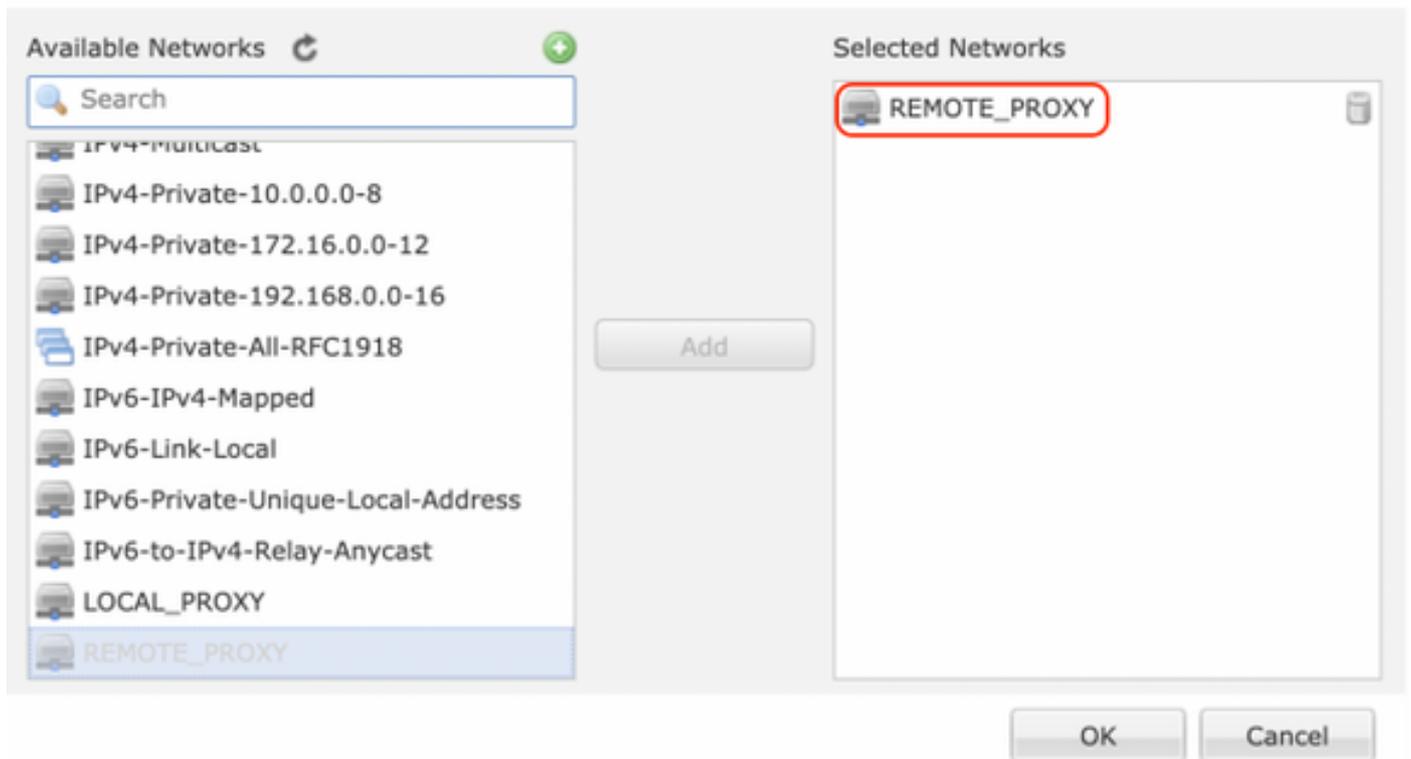
 REMOTE\_PROXY 

OK Cancel

Paso 6. Seleccione las subredes ASA que deben cifrarse y agréguelas a las redes seleccionadas.

'Proxy remoto' es la subred ASA '2001:AAAA::/64' en este ejemplo.

## Network Objects



### Configuración de Parámetros IKE

Paso 1. En la ficha IKE, especifique los parámetros que se utilizarán para el intercambio inicial IKEv2. Haga clic en el icono verde más para crear una nueva política IKE.

## Edit VPN Topology



Topology Name:\* L2L\_VPN

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\* preshared\_sha\_aes256\_dh14\_3

Authentication Type: Pre-shared Automatic Key

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

**IKEv2 Settings**

Policy:\* Ikev2\_Policy

Authentication Type: Pre-shared Manual Key

Key:\* .....

Confirm Key:\* .....

Enforce hex-based pre-shared key only

Save Cancel

Paso 2. En la nueva política IKE, especifique un número de prioridad así como la duración de la fase 1 de la conexión. Esta guía utiliza estos parámetros para el intercambio inicial:

Integridad (SHA256),

Encriptación (AES-256),

PRF (SHA256), y

Grupo Diffie-Hellman (Grupo 14).

Todas las políticas IKE del dispositivo se enviarán al par remoto independientemente de lo que esté en la sección de políticas seleccionada. El primero que coincida el par remoto se seleccionará para la conexión VPN.

[Opcional] Elija la política que se enviará primero mediante el campo de prioridad. La prioridad 1 se envía primero.

# Edit IKEv2 Policy

Name:\*

Ikev2\_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384
- NULL

Selected Algorithms

SHA256

Add

Save

Cancel

## Edit 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

Save

Cancel

# Edit 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

### Selected Algorithms

- SHA256**

## Edit IKEv2 Policy



Name:\* Ikev2\_Policy

Description:

Priority: (1-65535)

Lifetime: 86400 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

Paso 3. Una vez agregados los parámetros, seleccione la política configurada arriba y elija el tipo de autenticación.

Seleccione la opción Pre-shared Manual Key (Clave manual precompartida). Para esta guía, se utiliza la clave previamente compartida 'cisco123'.

## Edit VPN Topology



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:

Key:\*

Confirm Key:\*

Enforce hex-based pre-shared key only

## Configurar parámetros IPSEC

Paso 1. Pase a la ficha IPsec y cree una nueva propuesta de IPsec haciendo clic en el icono del lápiz para editar el conjunto de transformación.

## Edit VPN Topology



Topology Name:\*

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:

Transform Sets:

IKEv1 IPsec Proposals	IKEv2 IPsec Proposals*
tunnel_aes256_sha	Ikev2__IPSec_Proposal

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)

— **ESPv3 Settings**

Paso 2. Cree una nueva propuesta IPsec de IKEv2 seleccionando el icono verde más e introduzca los parámetros de la fase 2 como se muestra a continuación:

Hash ESP: SHA-1

Encriptación ESP: AES-256

# Edit IKEv2 IPsec Proposal



Name:\*

Ikev2\_\_IPSec\_Proposal

Description:

ESP Hash

ESP Encryption

Available Algorithms

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5
- NULL

Selected Algorithms

SHA-1

Add

Save

Cancel

## Edit IKEv2 IPsec Proposal



Name:\*

Description:

ESP Hash

**ESP Encryption**

Available Algorithms

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

**Add**

Selected Algorithms

- AES-256**

**Save** **Cancel**

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

## IKEv2 IPsec Proposal



Available Transform Sets

- AES-GCM
- AES-SHA
- DES\_SHA-1
- Ikev2\_\_IPSec\_Proposal**

**Add**

Selected Transform Sets

- Ikev2\_\_IPSec\_Proposal**

**OK** **Cancel**

Paso 4. 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 establece como predeterminada y PFS se inhabilita.

Topology Name:\* L2L\_VPN

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\* Ikev2\_IPSec\_Proposal

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)

ESPv3 Settings

Save Cancel

Debe configurar los pasos siguientes para omitir el control de acceso o crear reglas de política de control de acceso para permitir subredes VPN a través de FTD.

## Omitir control de acceso

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. Este ejemplo de configuración utiliza la opción "Omitir control de acceso".

El parámetro `sysopt permit-vpn` se puede habilitar en Advanced > Tunnel.

**Precaución:** Esta opción 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 aplica a todas las VPN si esta casilla de verificación está activada.

## Edit VPN Topology



Topology Name:\*

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:  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

## Configuración de 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 coincida con otra instrucción NAT y traduzca incorrectamente el tráfico VPN.

Paso 1. Vaya a **Devices > NAT** y cree una nueva política haciendo clic en **New Policy > Threat Defense NAT**.



## New Policy



Name:

Description:

**Targeted Devices**

Select devices to which you want to apply this policy.

**Available Devices**

FTDv

**Selected Devices**

FTDv

Paso 2. Haga clic en **Agregar regla**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPK QoS Platform Settings FlexConfig Certificates

**NAT\_Exempt**

Enter Description

Show Warnings Show Add Cancel

Policy Assignments (1)

Filter by Device

#	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	
▼ NAT Rules Before											
▼ Auto NAT Rules											
▼ NAT Rules After											

Paso 3. Cree una nueva regla NAT estática manual.

Haga referencia a las interfaces interna y externa para la regla NAT. La especificación de las interfaces en la ficha Objetos de Interfaz evita que estas reglas afecten al tráfico de otras interfaces.

Vaya a la ficha Traducción y seleccione las subredes de origen y destino. Como esta es una regla de exención de NAT, asegúrese de que el origen/destino original y el origen/destino traducido sean los mismos.

## Add NAT Rule

? X

NAT Rule:  Insert:

Type:   Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

**Original Packet**

Original Source:\*  +

Original Destination:   +

Original Source Port:  +

Original Destination Port:  +

**Translated Packet**

Translated Source:   +

Translated Destination:  +

Translated Source Port:  +

Translated Destination Port:  +

Haga clic en la pestaña Advanced 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

Guarde esta regla y confirme la sentencia NAT final en la lista NAT.

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

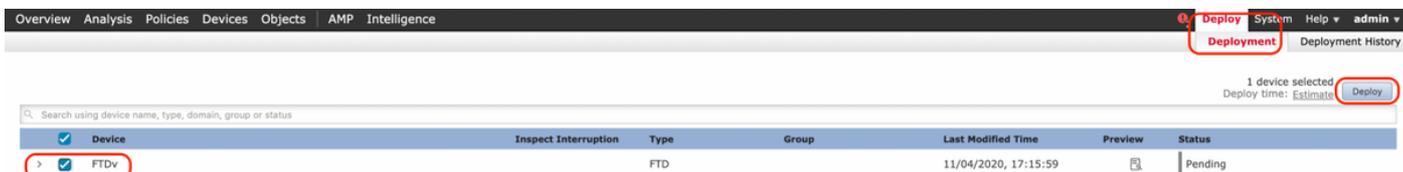
Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

**NAT\_Exempt**  
Enter Description Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	
1		Static	LAN	WAN	LOCAL_PROXY	REMOTE_PROXY	LOCAL_PROXY	REMOTE_PROXY	Dns: false route-lookup no-proxy-arp

Paso 4. Una vez finalizada la configuración, guarde e implemente la configuración en el FTD.



## Verificación

Inicie el tráfico interesante desde la máquina LAN o puede ejecutar el siguiente comando packet-tracer en el ASA.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

**Nota:** Aquí Type = 128 y Code=0 representa ICMPv6 "Echo Request".

La siguiente sección describe los comandos que puede ejecutar en ASA o FTD LINA CLI para verificar el estado del túnel IKEv2.

Este es un ejemplo de un resultado del ASA:

```
ciscoasa# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Status Role Remote
6638313 2001:bbbb::1/500
READY INITIATOR 2001:cccc::1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/224 sec
Child sa: local selector 2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8
```

```
ciscoasa# show crypto ipsec sa detail
```

```
interface: outside
```

```
Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1
```

```
access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
current_peer: 2001:cccc::1
```

```
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #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
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

#pkts invalid pad (rcv): 0,  
#pkts invalid ip version (rcv): 0,  
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0  
#pkts replay failed (rcv): 0  
#pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0  
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500  
path mtu 1500, ipsec overhead 94(64), media mtu 1500  
PMTU time remaining (sec): 0, DF policy: copy-df  
ICMP error validation: disabled, TFC packets: disabled  
current outbound spi: D95ECDB8  
current inbound spi : A0FD3FE6

inbound esp sas:

spi: 0xA0FD3FE6 (2700951526)  
transform: esp-aes-256 esp-sha-hmac no compression  
in use settings =(L2L, Tunnel, IKEv2, )  
slot: 0, conn\_id: 1937408, crypto-map: VP  
sa timing: remaining key lifetime (kB/sec): (4055040/28535)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001

outbound esp sas:

spi: 0xD95ECDB8 (3646868920)  
transform: esp-aes-256 esp-sha-hmac no compression  
in use settings =(L2L, Tunnel, IKEv2, )  
slot: 0, conn\_id: 1937408, crypto-map: VPN  
sa timing: remaining key lifetime (kB/sec): (4193280/28535)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001

ciscoasa# **show vpn-sessiondb detail l2l filter name 2001:cccc::1**

Session Type: LAN-to-LAN Detailed

Connection : 2001:cccc::1  
Index : 473 IP Addr : 2001:cccc::1  
Protocol : IKEv2 IPsec  
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256  
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA1  
Bytes Tx : 352 Bytes Rx : 352  
Login Time : 12:27:36 UTC Sun Apr 12 2020  
Duration : 0h:06m:40s

IKEv2 Tunnels: 1  
IPsec Tunnels: 1

IKEv2:

Tunnel ID : 473.1  
UDP Src Port : 500 UDP Dst Port : 500  
Rem Auth Mode: preSharedKeys  
Loc Auth Mode: preSharedKeys  
Encryption : AES256 Hashing : SHA256  
Rekey Int (T): 86400 Seconds Rekey Left(T): 86000 Seconds  
PRF : SHA256 D/H Group : 14  
Filter Name :

IPsec:

Tunnel ID : 473.2

```
Local Addr   : 2001:aaaa::/64/0/0
Remote Addr  : 2001:dddd::/64/0/0
Encryption   : AES256                Hashing      : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds          Rekey Left (T): 28400 Seconds
Rekey Int (D): 4608000 K-Bytes        Rekey Left (D): 4608000 K-Bytes
Idle Time Out: 30 Minutes             Idle TO Left  : 23 Minutes
Bytes Tx     : 352                    Bytes Rx     : 352
Pkts Tx     : 11                      Pkts Rx     : 11
```

## Troubleshoot

Para resolver problemas de establecimiento de túnel IKEv2 en ASA y FTD, ejecute los siguientes comandos de depuración:

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

A continuación se muestra un ejemplo de depuración IKEv2 que se está utilizando como referencia:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debug.html>

## Referencias

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html>