

Configuración de VPN basada en rutas con ruta estática en FTD administrada por FDM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Pasos de configuración en FDM](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar un túnel VPN de sitio a sitio basado en ruta estática en un FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de cómo funciona un túnel VPN.
- Conocimientos previos sobre la navegación por Firepower Device Manager (FDM).

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

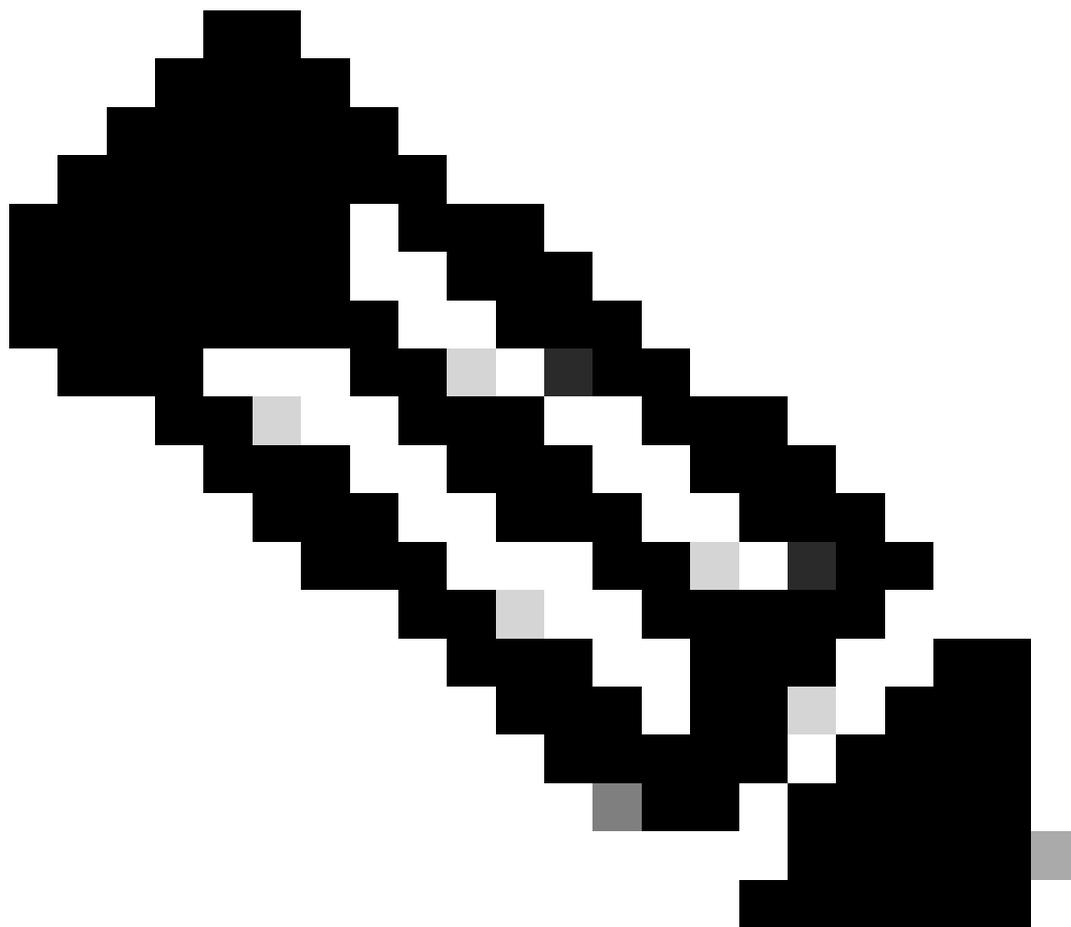
- Cisco Firepower Threat Defence (FTD) versión 7.0 gestionada por Firepower Device Manager (FDM).

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

Antecedentes

La VPN basada en rutas permite la determinación del tráfico interesante que se va a cifrar o enviar a través del túnel VPN, y utiliza el ruteo del tráfico en lugar de la política/lista de acceso como en la VPN basada en políticas o en el mapa criptográfico. El dominio de cifrado está configurado para permitir cualquier tráfico que ingrese al túnel IPsec. Los selectores de tráfico local y remoto de IPsec se establecen en 0.0.0.0/0.0.0.0. Esto significa que cualquier tráfico enrutado en el túnel IPsec se cifra independientemente de la subred de origen/destino.

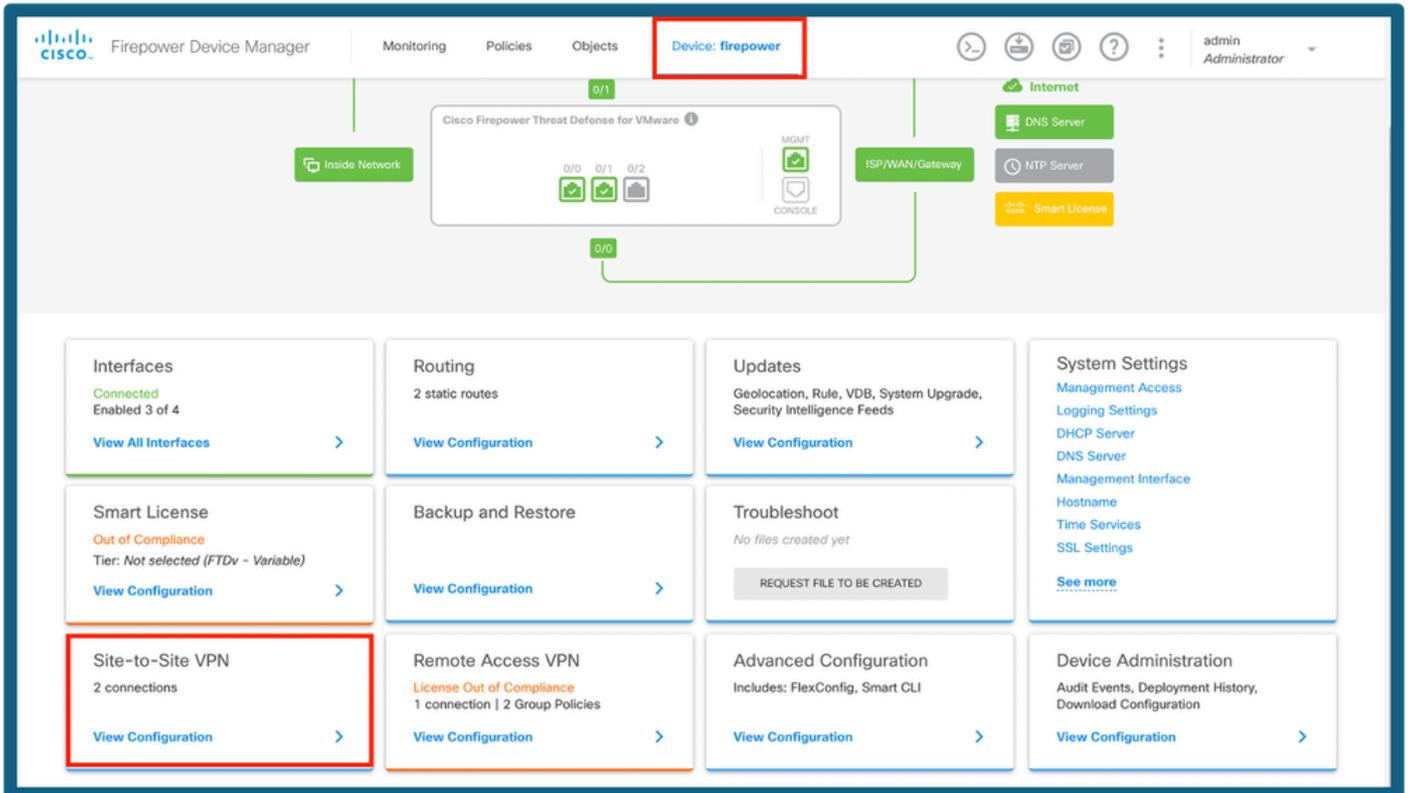
Este documento se centra en la configuración de la Interfaz de Túnel Virtual Estática (SVTI).



Nota: No se necesitan licencias adicionales, la VPN basada en rutas se puede configurar en los modos con licencia y de evaluación. Sin cumplimiento de cifrado (funciones controladas de exportación habilitadas), sólo se puede utilizar DES como algoritmo de cifrado.

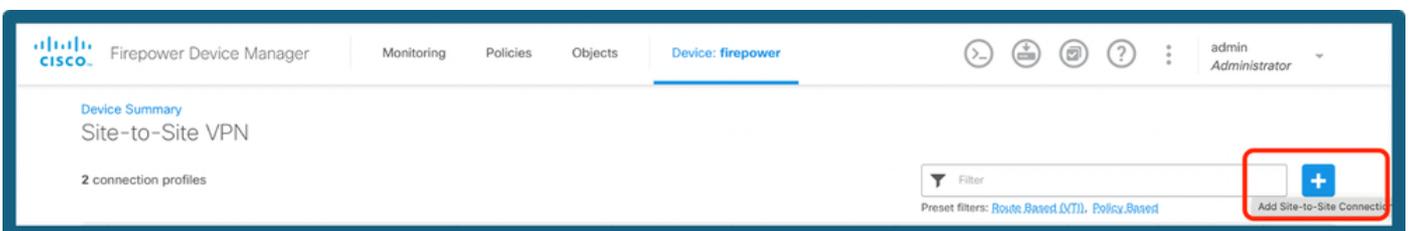
Pasos de configuración en FDM

Paso 1. Vaya a Dispositivo > Sitio a Sitio.



Panel de FDM

Paso 2. Haga clic en el icono + para agregar un nuevo sitio a la conexión del sitio.



Agregar una conexión S2S

Paso 3. Proporcione un nombre de topología y seleccione el tipo de VPN como basado en ruta (VTI).

Haga clic en Local VPN Access Interface, y luego haga clic en Create new Virtual Tunnel Interface o seleccione una de la lista que existe.

Firepower Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator

Local Network | FIREPOWER | VPN TUNNEL | INTERNET | PEER ENDPOINT | OUTSIDE INTERFACE | Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Type: Route Based (VTI) Policy Based

Sites Configuration

LOCAL SITE: Local VPN Access Interface:

REMOTE SITE: Remote IP Address:

[Create new Virtual Tunnel Interface](#)

Agregar interfaz de túnel

Paso 4. Defina los parámetros de la nueva interfaz de túnel virtual. Click OK.

Create Virtual Tunnel Interface

Name: Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

Tunnel ID: Tunnel Source:

0 - 10413

IP Address and Subnet Mask: /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Configuración de VTI

Paso 5. Elija el VTI recién creado o un VTI que exista en la interfaz de túnel virtual. Proporcione la dirección IP remota.

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name:

Type: Route Based (VTI) Policy Based

Sites Configuration

| LOCAL SITE | REMOTE SITE |
|--|--|
| Local VPN Access Interface: <input type="text" value="tunnel10 (Tunnel10)"/> | Remote IP Address: <input type="text" value="10.106.63.23"/> |

Agregar IP de par

Paso 6. Elija la Versión IKE y elija el botón Editar para establecer los parámetros IKE e IPsec como se muestra en la imagen.

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 **IKE VERSION 1**

IKE Policy

Globally applied

IPSec Proposal

Custom set selected

Configurar la versión IKE

Paso 7a. Elija el botón IKE Policy como se muestra en la imagen y haga clic en el botón ok o en Create New IKE Policy, si desea crear una nueva política.

Edit Globally: IKE v2 Policy



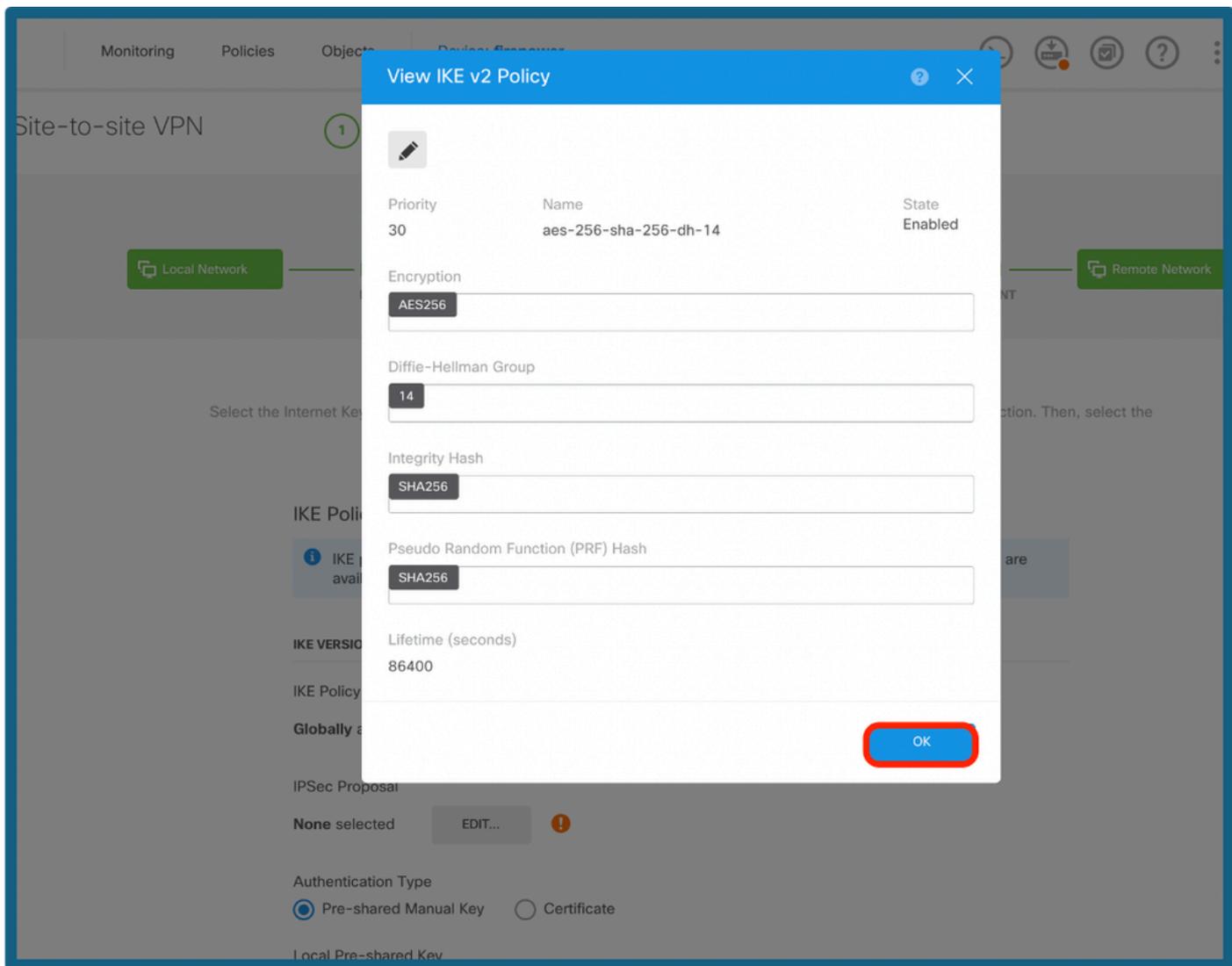
Filter

- AES-GCM-NULL-SHA 
- AES-SHA-SHA 
- DES-SHA-SHA 
- aes-256-sha-256-dh-14 
- ike2_policy 

Create New IKE Policy

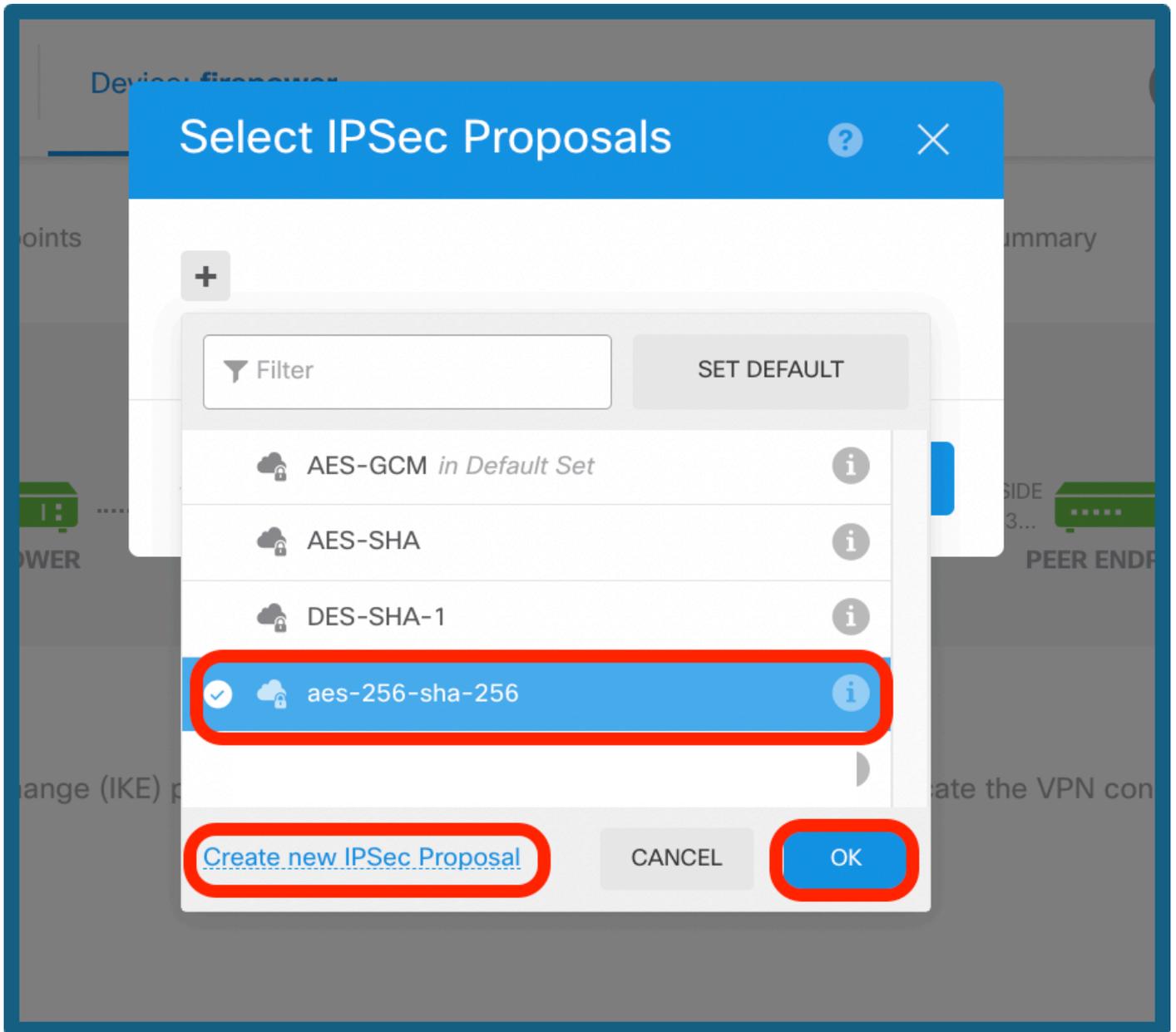
OK

Elija la política IKE



Configuración de la política IKE

Paso 7b. Elija el botón IPsec Policy como se muestra en la imagen y haga clic en el botón ok o en Create New IPsec Propuesta, si desea crear una nueva propuesta.



Seleccionar propuesta de IPsec

IKE v2 IPsec Proposal

Name
aes-256-sha-256

Encryption
AES256

Integrity Hash
SHA256

OK

Configuración de la propuesta de IPsec

Paso 8a. Seleccione el Tipo de autenticación. Si se utiliza una clave manual previamente compartida, proporcione la clave previamente compartida local y remota.

Paso 8b. (Opcional) Elija la configuración Perfect Forward Secrecy. Configure IPsec Lifetime Duration and Lifetime Size y, a continuación, haga clic en Next (Siguiete).

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

Custom set selected

Authentication Type

Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

IPSEC SETTINGS

Lifetime Duration seconds
120 - 2147483647; (Default: 28800)

Lifetime Size kilobytes
10 - 2147483647; (Default: 4608000).
Leave empty for Unlimited.

Additional Options

Diffie-Hellman Group for Perfect Forward Secrecy

PSK y configuración de por vida

Paso 9. Revise la configuración y haga clic en Finish.

Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

Vti-Ipsec Connection Profile

i Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface IP tunnel10 (1.1.1.1)



Peer IP Address 10.106.63.23

IKE V2

IKE Policy aes-256-sha256-sha256-14

IPSec Proposal aes-256-sha-256

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

Diffie-Hellman Group Null (not selected)

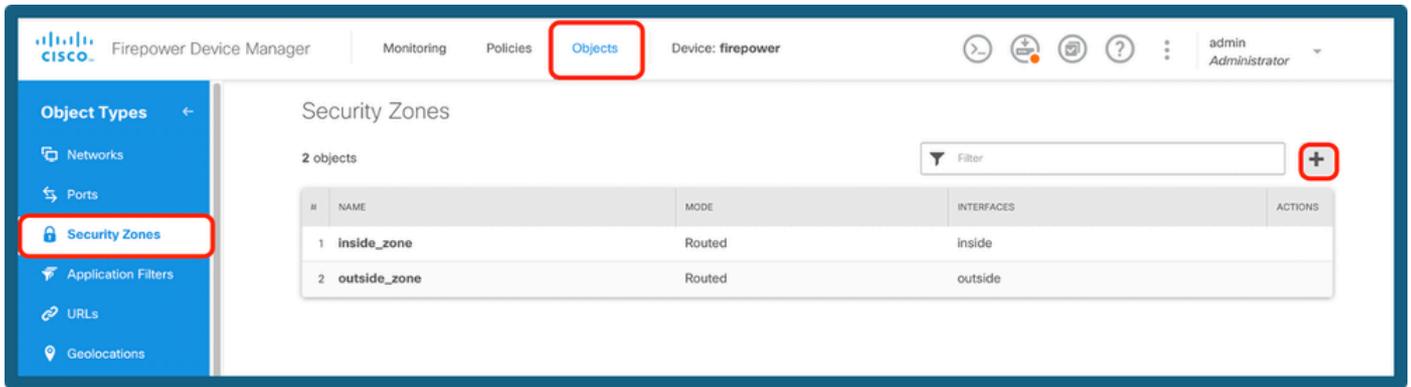
i Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

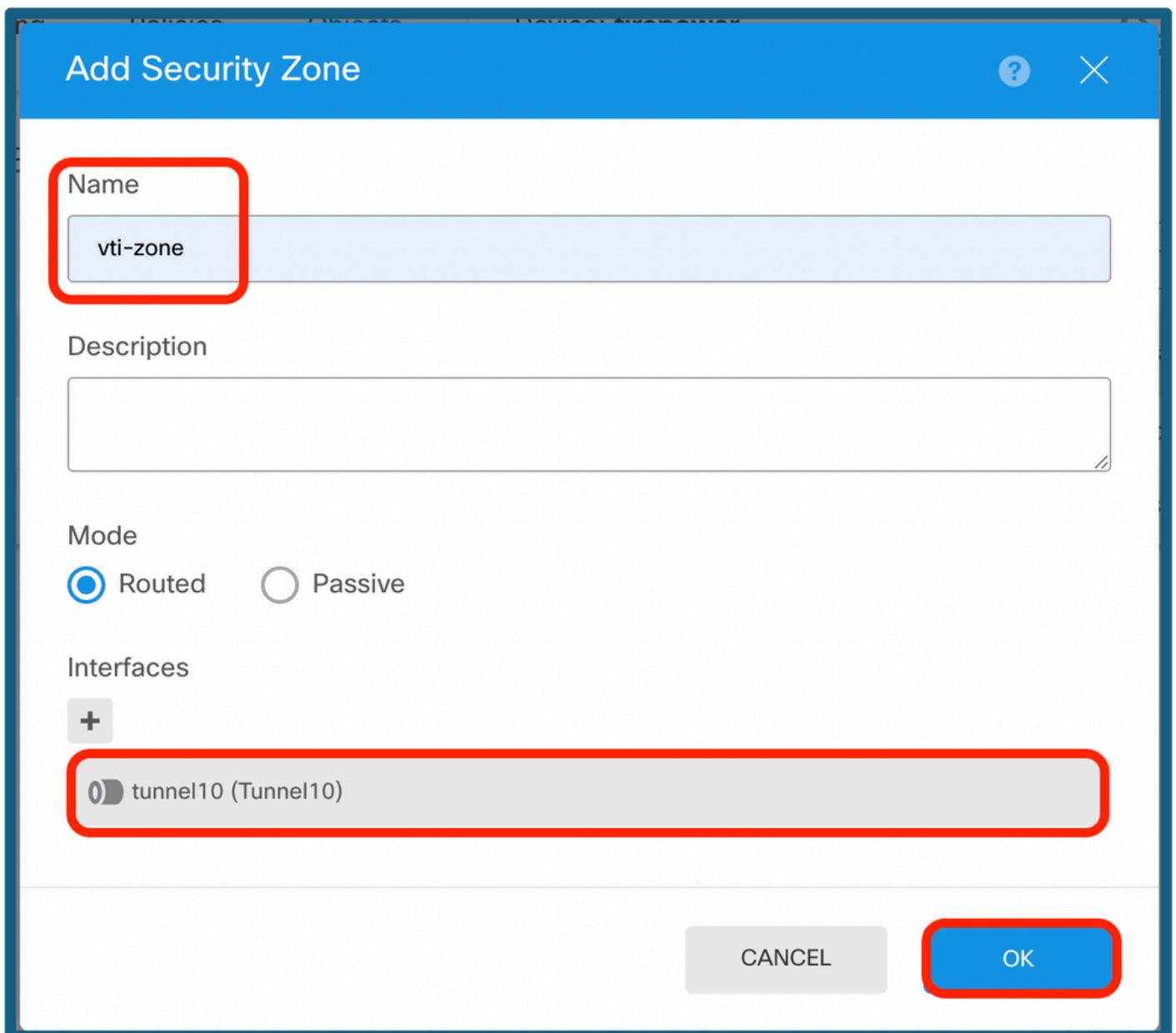
Resumen de la configuración

Paso 10a. Navegue hasta Objetos > Zonas de seguridad y luego haga clic en el icono +.



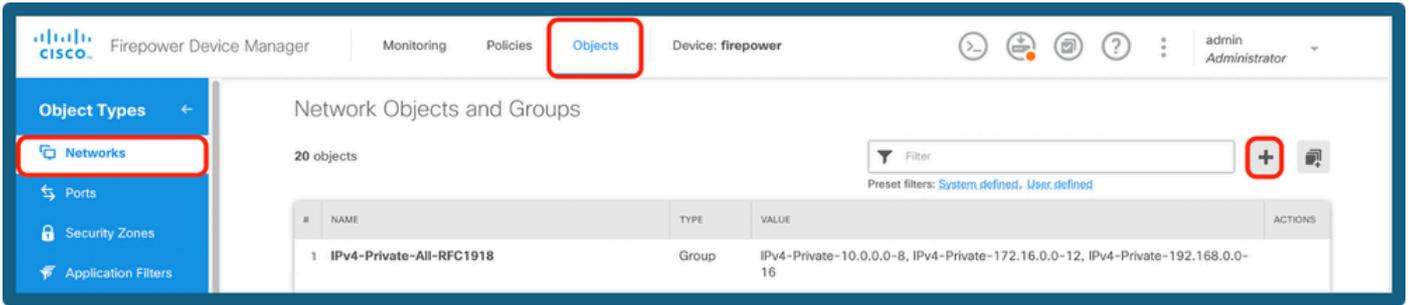
Agregar una zona de seguridad

Paso 10b. Cree una zona y seleccione la interfaz VTI como se muestra a continuación.



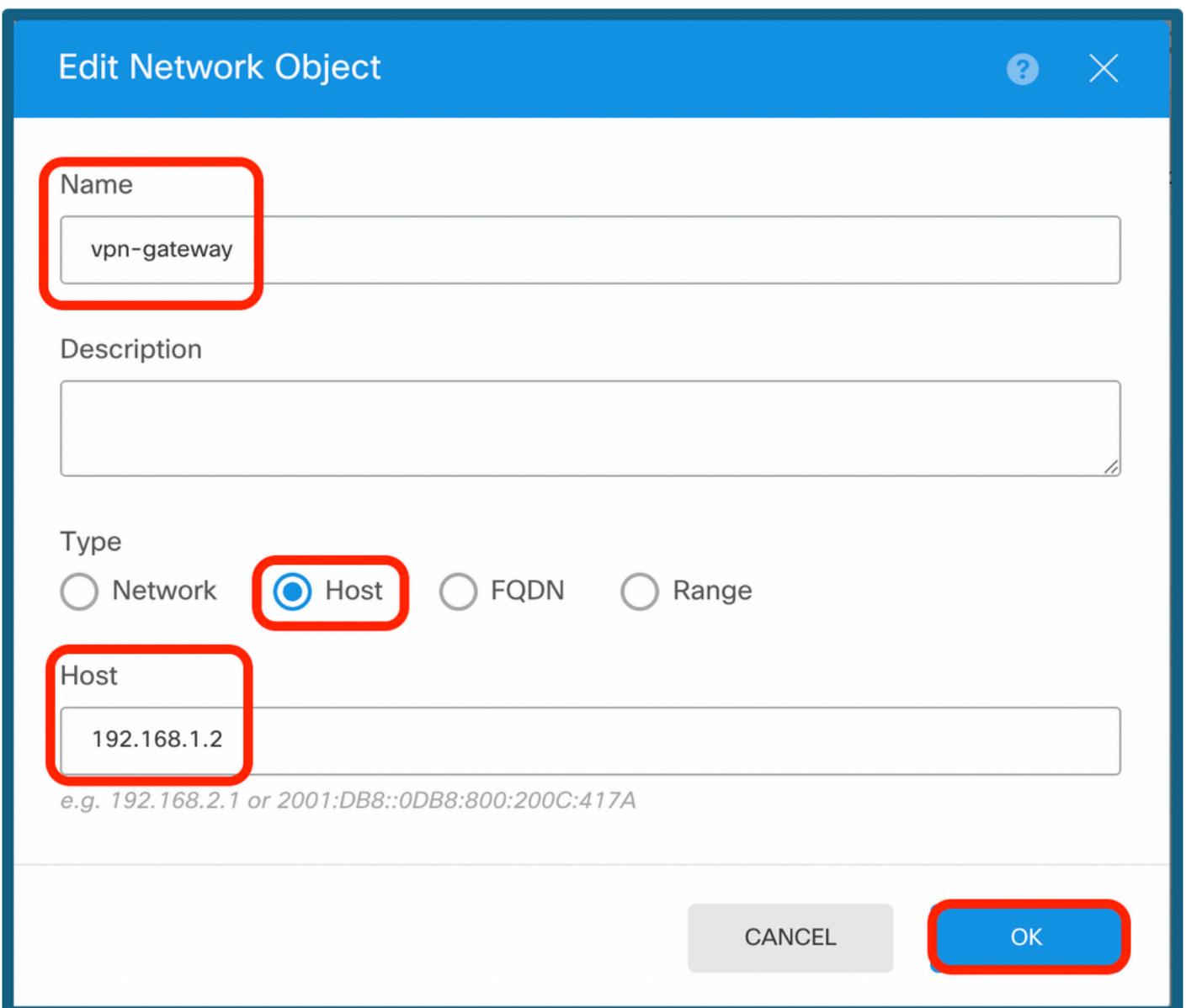
Configuración de la zona de seguridad

Paso 11a. Navegue hasta Objetos > Redes, haga clic en el icono +.



Agregar objetos de red

Paso 11b. Agregue un objeto host y cree una gateway con IP de túnel del extremo del par.



Configurar puerta de enlace VPN

Paso 11c. Agregue la subred remota y la subred local.

Edit Network Object



Name

remote-vpn-network

Description

Type



Network



Host



FQDN



Range

Network

172.16.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Configuración de IP remota

Edit Network Object ? ×

Name
inside-network

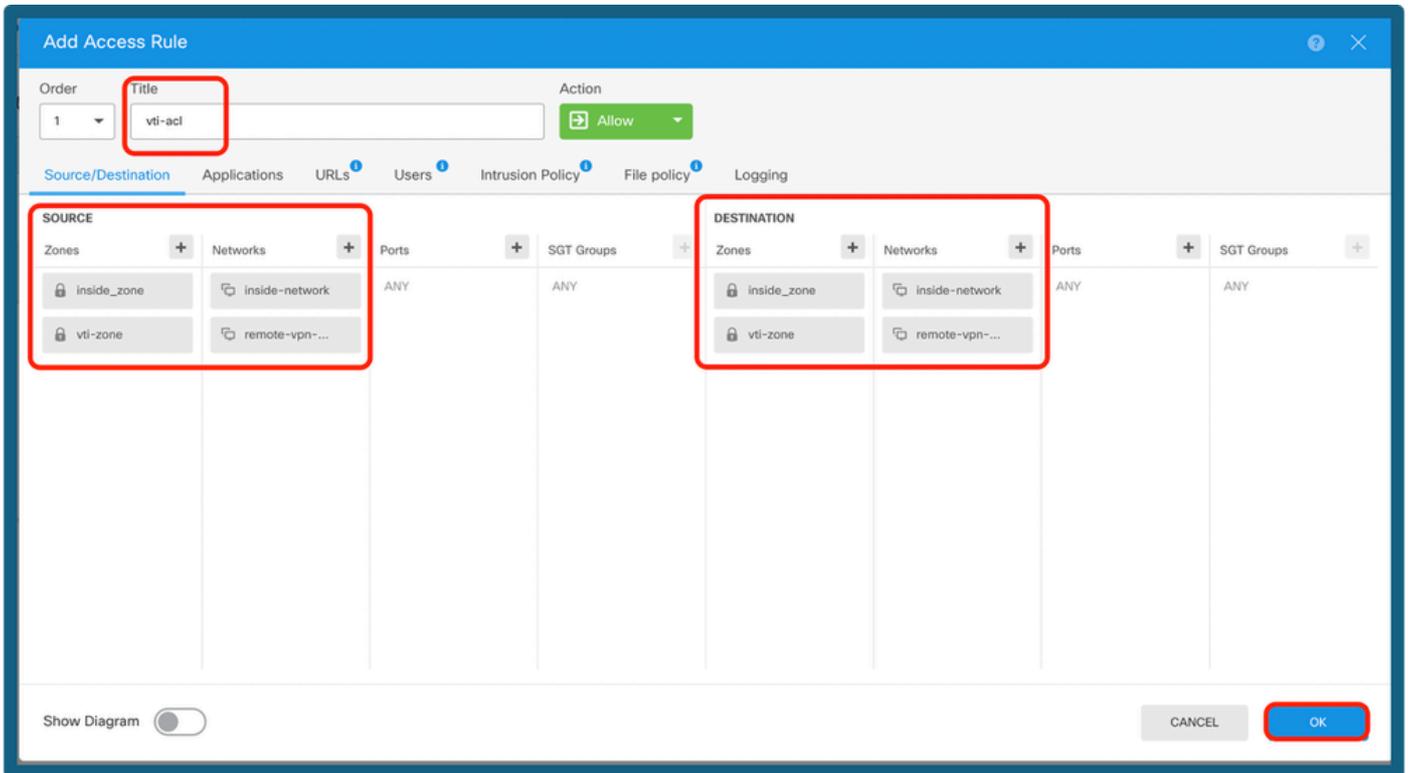
Description

Type
 Network Host FQDN Range

Network
10.10.10.0/24
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

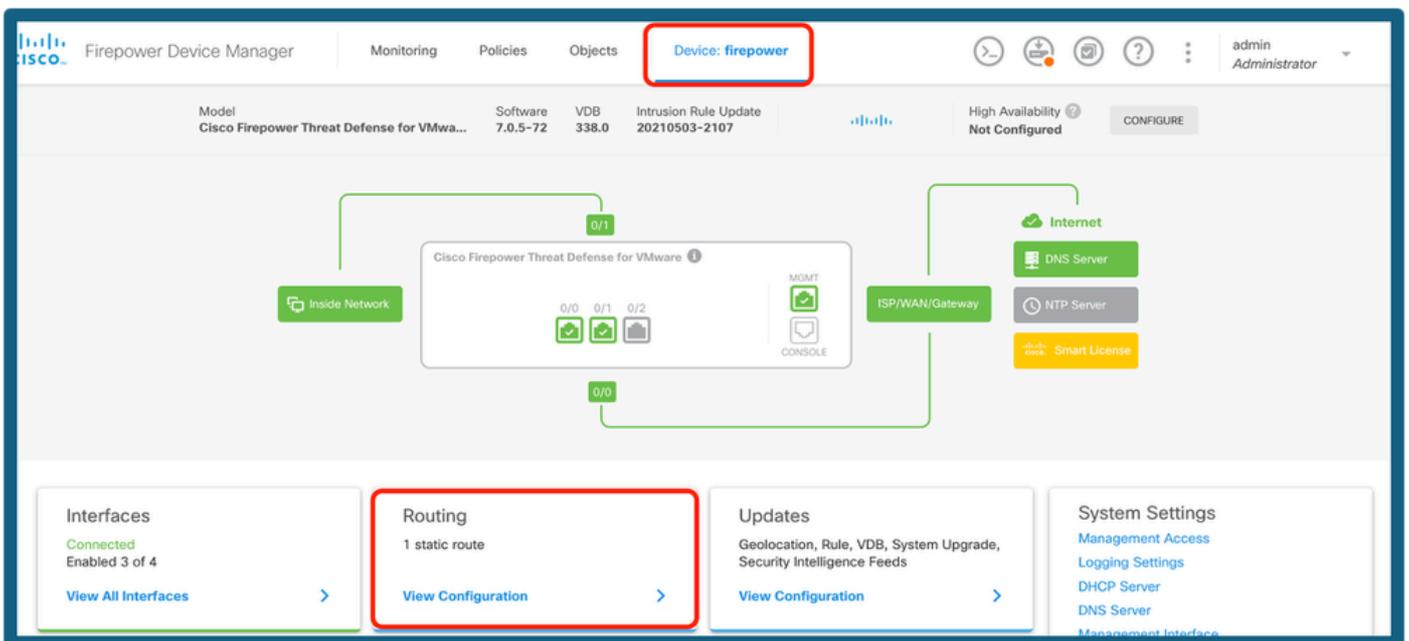
Configuración de IP local

Paso 12. Navegue hasta Dispositivo > Políticas, y configure la Política de Control de Acceso.



Agregar política de control de acceso

Paso 13a. Agregue el ruteo sobre el túnel VTI. Vaya a Device > Routing.



Seleccionar enrutamiento

Paso 13b. Vaya a Static Route en la pestaña Routing. Haga clic en el icono +.

Device Summary
Routing

Add Multiple Virtual Routers ▾ Commands ▾ BGP Global Settings

Static Routing | BGP | OSPF | EIGRP | ECMP Traffic Zones

1 route Filter +

| # | NAME | INTERFACE | IP TYPE | NETWORKS | GATEWAY IP | SLA MONITOR | METRIC | ACTIONS |
|---|---------|-----------|---------|-----------|-------------|-------------|--------|---------|
| 1 | default | outside | IPv4 | 0.0.0.0/0 | 10.106.52.1 | | 1 | |

Agregar ruta

Paso 13c. Proporcione la interfaz, elija la red, proporcione la puerta de enlace. Click OK.

Add Static Route

Name
vti-route

Description

Interface
tunnel10 (Tunnel10)

Protocol
 IPv4 IPv6

Networks
+
remote-vpn-network

Gateway
vpn-gateway

Metric
1

SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor

CANCEL OK

Configurar ruta estática

Paso 14. Vaya a Desplegar. Revise los cambios y, a continuación, haga clic en Deploy Now.

Pending Changes
? X

✔ Last Deployment Completed Successfully
 26 Jun 2025 05:27 PM. [See Deployment History](#)

| Deployed Version (26 Jun 2025 05:27 PM) | Pending Version |
|--|--------------------------|
| + Static Route Added: vti-route | |
| - | metricValue: 1 |
| - | ipType: IPv4 |
| - | name: vti-route |
| iface: | |
| - | tunnel10 |
| gateway: | |
| - | vpn-gateway |
| networks: | |
| - | remote-vpn-network |
| + Access Rule Added: vti-acl | |
| - | logFiles: false |
| - | eventLogAction: LOG_NONE |
| - | ruleId: 268435458 |
| - | name: vti-acl |
| sourceZones: | |
| - | vti-zone |
| - | inside_zone |
| destinationZones: | |
| - | vti-zone |
| - | inside_zone |
| sourceNetworks: | |
| - | remote-vpn-network |
| - | inside-network |
| destinationNetworks: | |

MORE ACTIONS ▼
CANCEL
DEPLOY NOW ▼

Implementación de la configuración

Verificación

Una vez completada la implementación, puede verificar el estado del túnel en la CLI mediante los siguientes comandos:

1. show crypto ikev2 sa
2. show crypto ipsec sa <peer-ip>

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote Status Role
3294213359 10.106.52.222/500 10.106.63.23/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/141 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x26a14554/0xd5db88bc
```

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.106.63.23
```

Comandos show

Información Relacionada

Para obtener más información sobre las VPN de sitio a sitio en el FTD gestionado por FDM, puede encontrar la guía de configuración completa aquí:

[Guía de configuración de FDM Administrado por FDM](#)

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).