

# Configuración de BGP sobre VPN basada en ruta en FTD administrado por FDM

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones en VPN](#)

[Configuraciones en BGP](#)

[Verificación](#)

[Troubleshoot](#)

---

## Introducción

Este documento describe la configuración de BGP a través de VPN de sitio a sitio basada en ruta en FTDv administrado por FirePower Device Manager (FDM).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de VPN
- Configuraciones BGP en FTDv
- Experiencia con FDM

### Componentes Utilizados

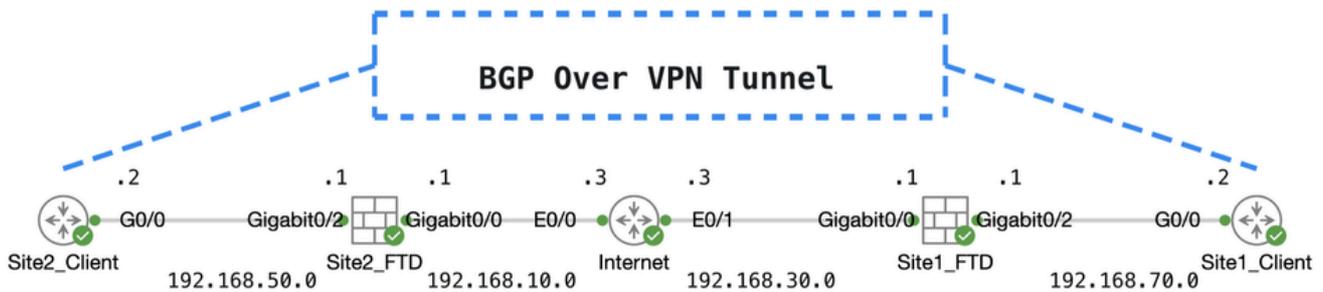
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTDv versión 7.4.2
- Cisco FDM versión 7.4.2

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.

# Configurar

## Diagrama de la red



Topo

## Configuraciones en VPN

Paso 1. Asegúrese de que la interconectividad IP entre nodos esté lista y estable. La licencia inteligente de FDM se ha registrado correctamente con la cuenta inteligente.

Paso 2. La puerta de enlace del cliente Site1 se configura con la dirección IP interna del FTD Site1 (192.168.70.1). La puerta de enlace del cliente Site2 se configura con la dirección IP interior del FTD Site2 (192.168.50.1). Además, asegúrese de que la ruta predeterminada en ambos FTD esté configurada correctamente después de la inicialización de FDM.

Inicie sesión en la GUI de cada FDM. Vaya a `.Device > Routing` Haga clic en `View Configuration`. Haga clic en la `Static Routing` pestaña para verificar la ruta estática predeterminada.

The screenshot shows the Firewall Device Manager (FDM) GUI for a device named 'ftdv742'. The 'Routing' section is active, and the 'Static Routing' tab is selected. A table displays the configured static routes. The first route is highlighted with a red box:

| # | NAME             | INTERFACE | IP TYPE | NETWORKS  | GATEWAY IP   | SLA MONITOR | METRIC | ACTIONS |
|---|------------------|-----------|---------|-----------|--------------|-------------|--------|---------|
| 1 | StaticRoute_IPv4 | outside   | IPv4    | 0.0.0.0/0 | 192.168.30.3 |             | 1      |         |

Site1\_FTD\_Gateway

Device Summary  
Routing

Add Multiple Virtual Routers

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

1 route

| # | NAME             | INTERFACE | IP TYPE | NETWORKS  | GATEWAY IP   | SLA MONITOR | METRIC | ACTIONS |
|---|------------------|-----------|---------|-----------|--------------|-------------|--------|---------|
| 1 | StaticRoute_IPv4 | outside   | IPv4    | 0.0.0.0/0 | 192.168.10.3 |             | 1      |         |

Site2\_FTD\_Gateway

Paso 3. Configure la VPN de sitio a sitio basada en rutas. En este ejemplo, configure primero el FTD Site1.

Paso 3.1. Inicie sesión en la GUI de FDM del FTD Site1. Cree un nuevo objeto de red para la red interna del FTD Site1. Desplácese hasta **Objects > Networks**, haga clic en el botón +.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: ftdv742

Object Types

Networks

Network Objects and Groups

9 objects

Filter

Preset filters: System defined, User defined

Create\_Network\_Object

Paso 3.2. Proporcione la información necesaria. Haga clic en el botón.

- Nombre: inside\_192.168.70.0
- Tipo: Red
- Red: 192.168.70.0/24

# Add Network Object



Name

inside\_192.168.70.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.70.0/24

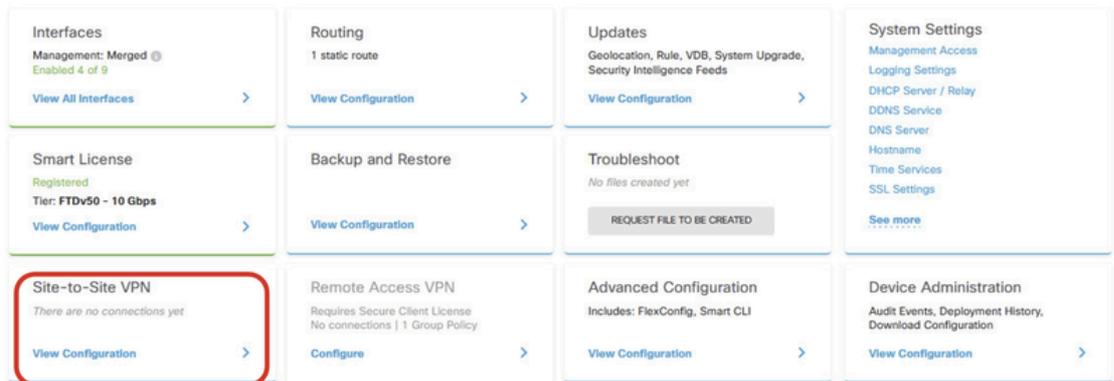
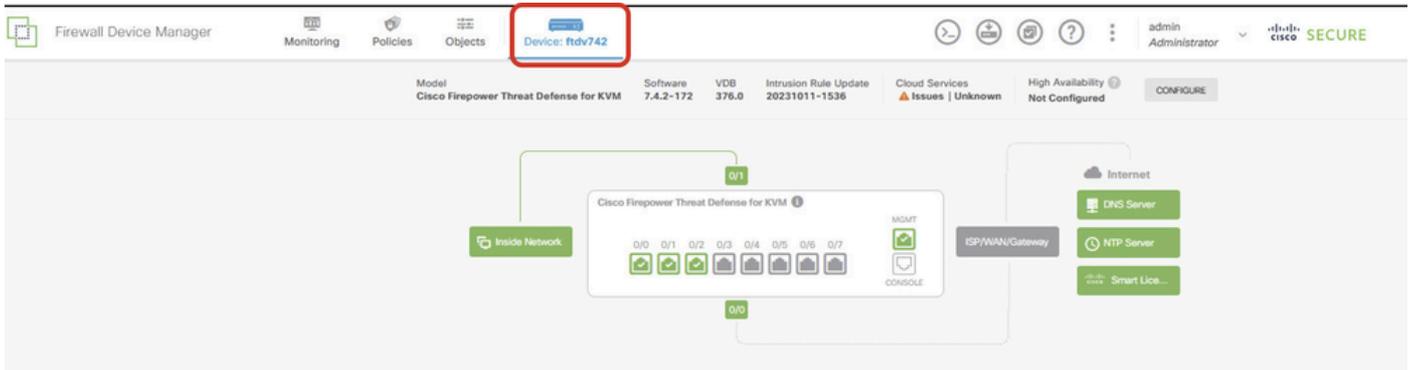
*e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60*

CANCEL

OK

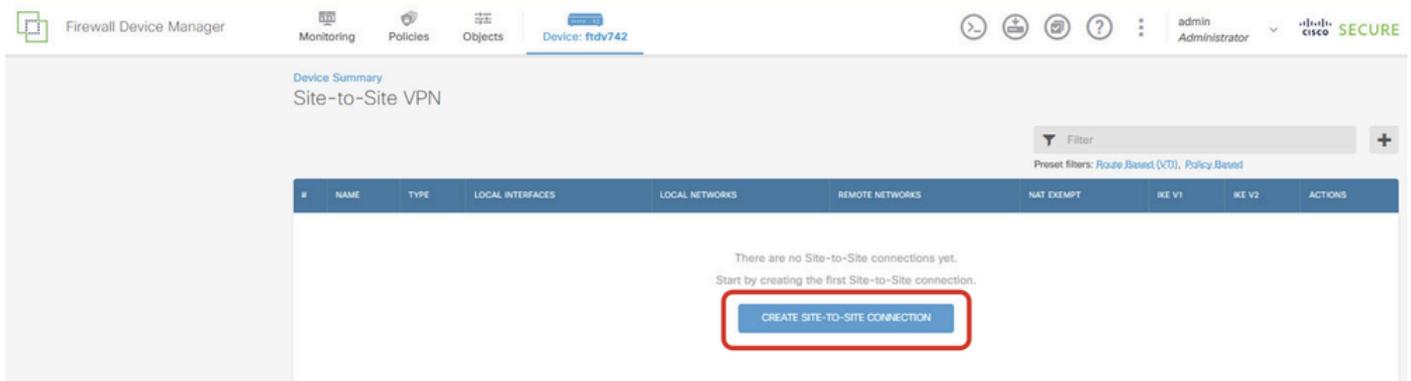
Sitio1\_Red\_interna

Paso 3.3. Vaya a **.Device > Site-to-Site VPN** Haga clic en **View Configuration** .



Ver VPN de sitio a sitio

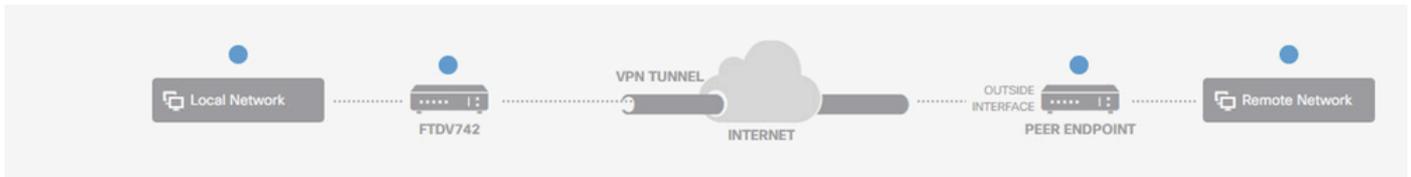
Paso 3.4. Comience a crear una nueva VPN de sitio a sitio. Haga clic en **CREATE SITE-TO-SITE CONNECTION**.



Create\_Site-to-Site\_Connection

Paso 3.5. Proporcione la información necesaria.

- Nombre del perfil de conexión: Demo\_S2S
- Tipo: basado en ruta (VTI)
- Interfaz de acceso VPN local: haga clic en la lista desplegable y, a continuación, haga clic en **Create new Virtual Tunnel Interface**.



## 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: Demo\_S2S

Type: Route Based (VTI) | Policy Based

### Sites Configuration

| LOCAL SITE  | REMOTE SITE       |
|---|-------------------|
| Local VPN Access Interface<br>Please select<br>Filter<br>Nothing found<br><a href="#">Create new Virtual Tunnel Interface</a> | Remote IP Address |

NEXT

Create\_VTI\_in\_VPN\_Wizard

Paso 3.6. Proporcione la información necesaria para crear una nueva VTI. Haga clic en el botón OK (Aceptar)

- Nombre: demovti
- ID de túnel: 1
- Fuente del túnel: exterior (GigabitEthernet0/0)
- Dirección IP Y Máscara De Subred: 169.254.10.1/24
- Estado: haga clic en el control deslizante hasta la posición Activado

Name Status

demovti

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

Description

Tunnel ID ? Tunnel Source ?

1 outside (GigabitEthernet0/0) v

0 - 10413

IP Address and Subnet Mask

169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

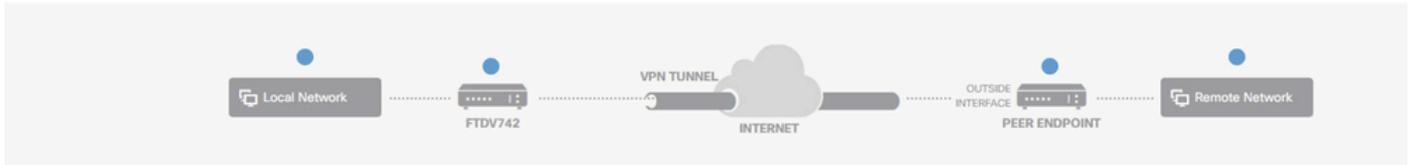
Create\_VTI\_Details

Paso 3.7. Continúe proporcionando la información necesaria. Haga clic en el botón NEXT.

- Interfaz de acceso VPN local: demovti (creada en el paso 3.6.1)
- Dirección IP remota: 192.168.10.1

## 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: Demo\_S2S

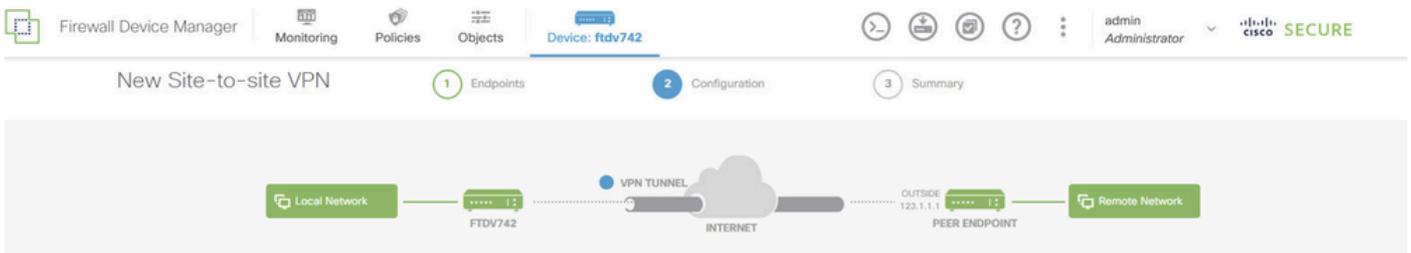
Type:  Route Based (VTI)  Policy Based

Sites Configuration

| LOCAL SITE                                      | REMOTE SITE                       |
|---|-----------------------------------|
| Local VPN Access Interface<br>demovti (Tunnel1) | Remote IP Address<br>192.168.10.1 |

VPN\_Wizard\_Endpoints\_Step1

Paso 3.8. Vaya a Política IKE. Haga clic en el botón Editar.



### Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

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

None selected  !

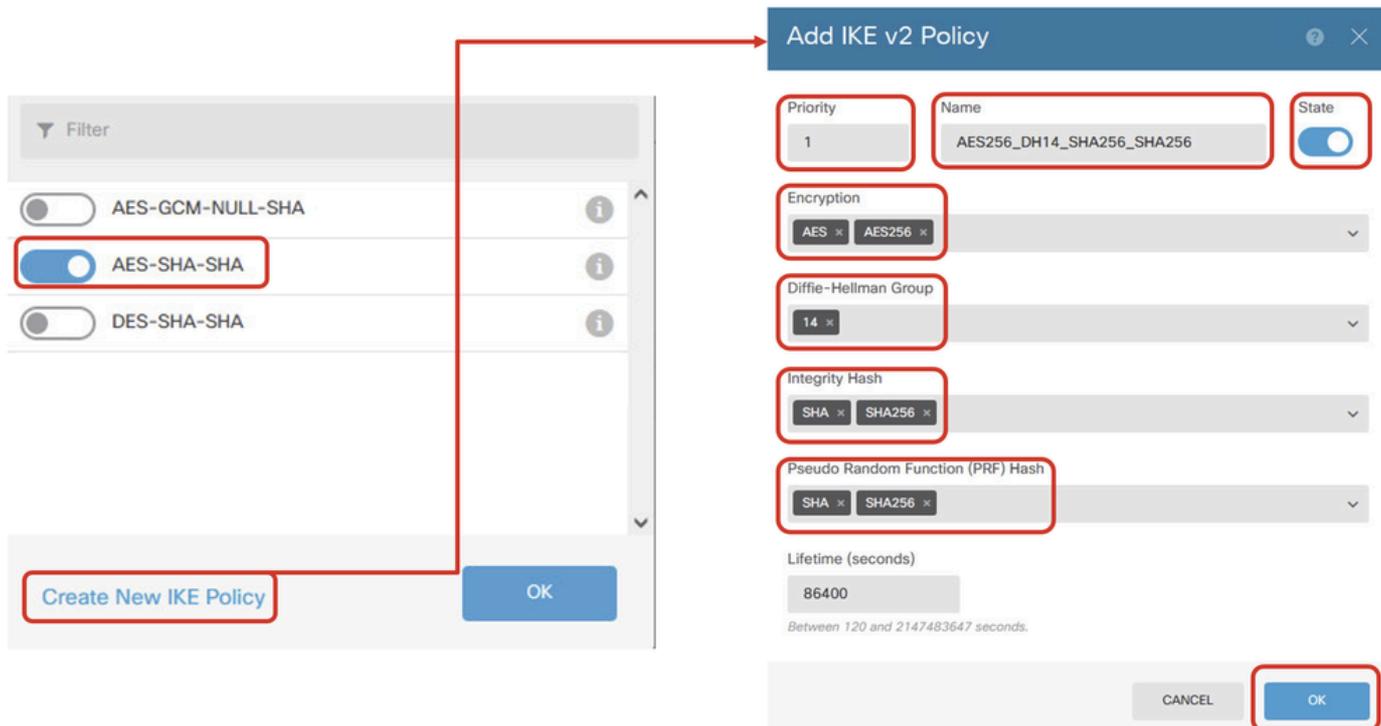
Edit\_IKE\_Policy

Paso 3.9. Para la política IKE, puede utilizar una predefinida o crear una nueva haciendo clic en Create New IKE Policy.

En este ejemplo, alterne una política IKE existente AES-SHA-SHA y cree una nueva para fines de

demostración. Haga clic en el botón OK para guardar.

- Nombre: AES256\_DH14\_SHA256\_SHA256
- Cifrado: AES, AES256
- Grupo DH: 14
- Hash de integridad: SHA, SHA256
- Hash PRF: SHA, SHA256
- Vida útil: 86400 (predeterminado)



Add\_New\_IKE\_Policy

Filter

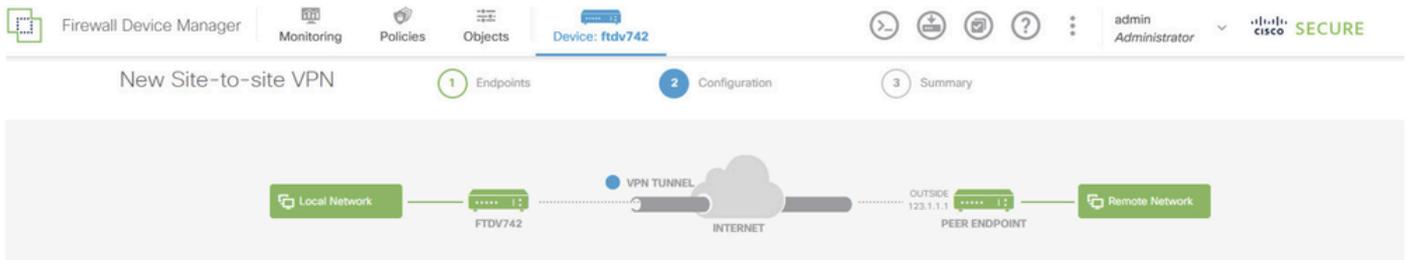
|                                     |                           |   |
|-------------------------------------|---------------------------|---|
| <input type="checkbox"/>            | AES-GCM-NULL-SHA          | i |
| <input checked="" type="checkbox"/> | AES-SHA-SHA               | i |
| <input type="checkbox"/>            | DES-SHA-SHA               | i |
| <input checked="" type="checkbox"/> | AES256_DH14_SHA256_SHA256 | i |

Create New IKE Policy

OK

Enable\_New\_IKE\_Policy

Paso 3.10. Vaya a la propuesta IPSec. Haga clic en el botón Editar.



### Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

#### IKE Policy

1 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

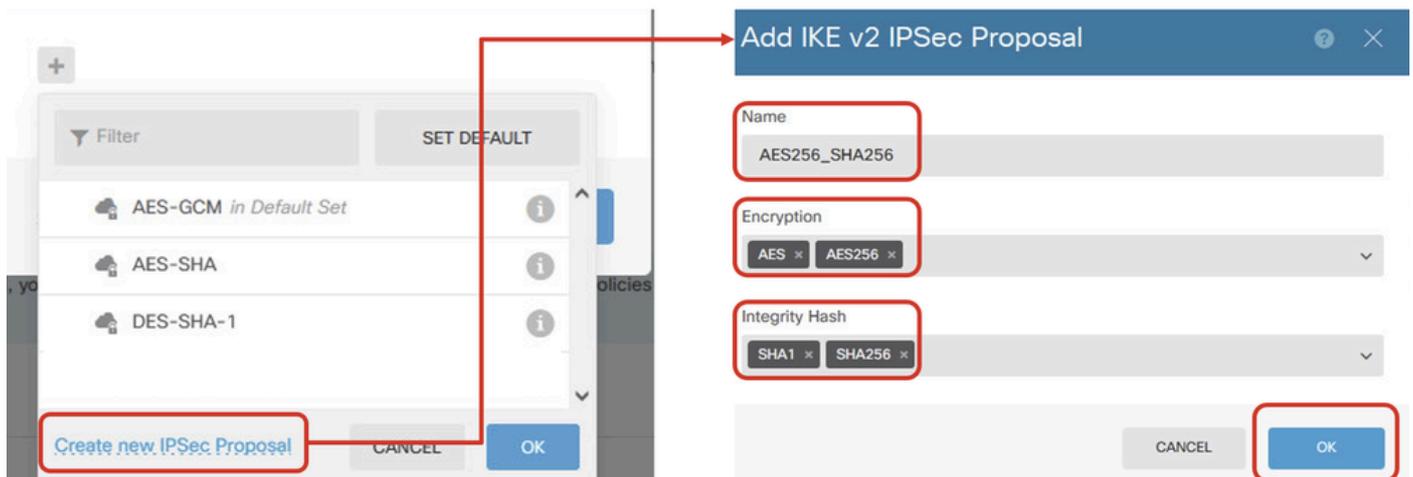
#### IPSec Proposal

None selected  !

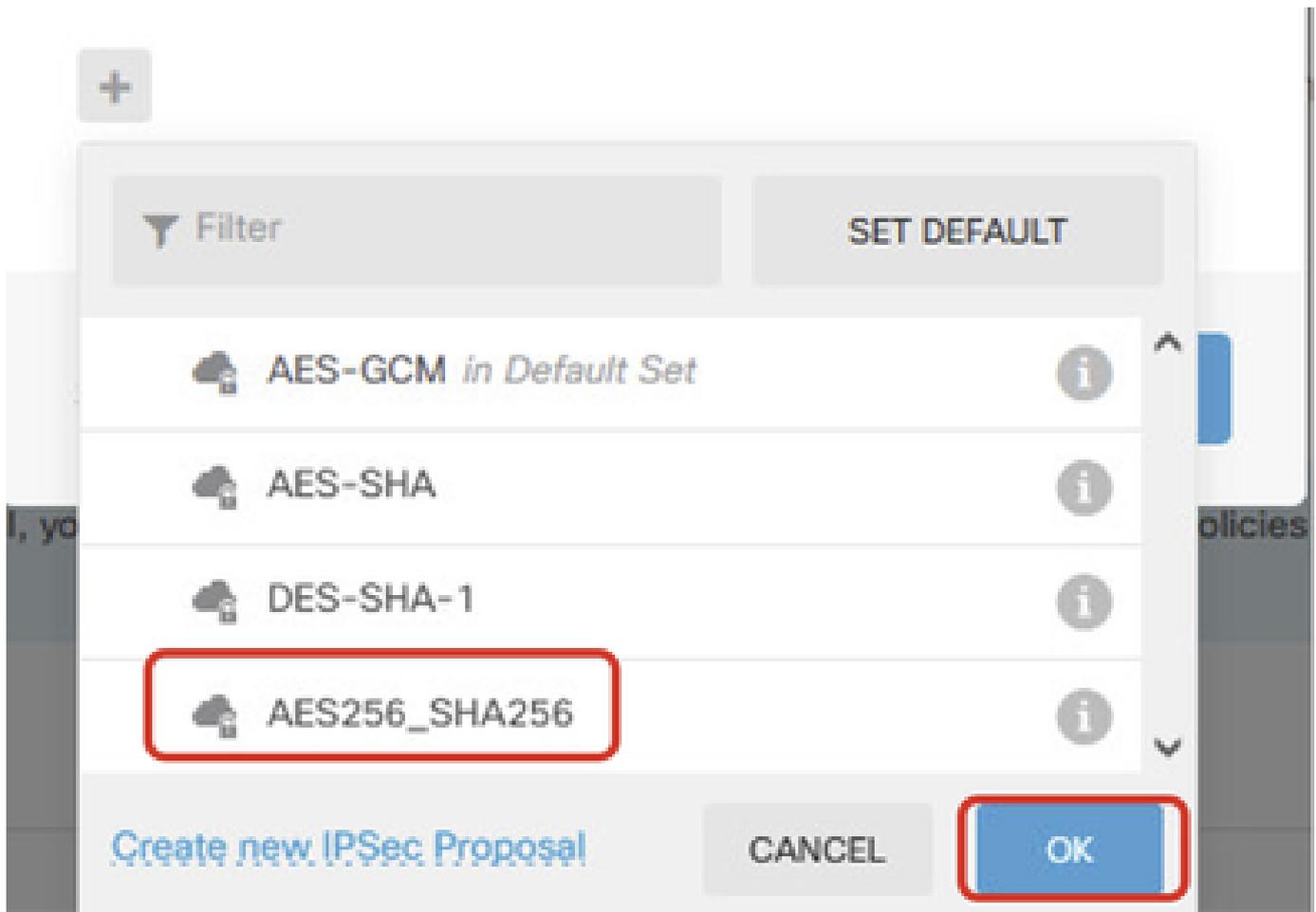
Editar\_IKE\_Propuesta

Paso 3.11. Para la propuesta IPsec, puede utilizar una propuesta predefinida o puede crear una nueva haciendo clic en Create new IPsec posed. En este ejemplo, cree uno nuevo con fines de demostración. Proporcione la información necesaria. Haga clic en el botón OK para guardar.

- Nombre: AES256\_SHA256
- Cifrado: AES, AES256
- Hash de integridad: SHA1, SHA256



Agregar\_nueva\_propuesta\_IPSec



Habilitar\_Nueva\_propuesta\_IPSec

Paso 3.12. Configure la clave previamente compartida. Haga clic en el botón NEXT.

Anote esta clave previamente compartida y configúrela en el FTD Site2 más adelante.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURI

FTDV742 | INTERNET | PEER ENDPOINT

### Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

#### 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

Authentication Type  
 Pre-shared Manual Key  Certificate

Local Pre-shared Key  
\*\*\*\*\*

Remote Peer Pre-shared Key  
\*\*\*\*\*

Configure\_Pre\_Shared\_Key

Paso 3.13. Revise la configuración de VPN. Si necesita modificar algo, haga clic en el botón BACK. Si todo está bien, haga clic en el botón FINISH.

## Demo\_S2S Connection Profile

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

**VPN Access Interface**

demovti (169.254.10.1)



**Peer IP Address**

192.168.10.1

### IKE V2

**IKE Policy**

aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14

**IPSec Proposal**

aes,aes-256-sha-1,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

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

VPN\_Wizard\_Complete

Paso 3.14. Cree una regla de control de acceso para permitir que el tráfico pase a través del FTD. En este ejemplo, permitir todos con fines de demostración. Modifique su política en función de sus necesidades reales.

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes "Firewall Device Manager", "Monitoring", "Policies", "Objects", and "Device: ftdv742". The "Policies" tab is active, and the breadcrumb trail is: "SSL Decryption" → "Identity" → "Security Intelligence" → "NAT" → "Access Control" → "Intrusion".

Under "Access Control", there is a section for "1 rule" with a "Filter" input field and a "Settings" icon. Below this is a table with the following columns: #, NAME, ACTION, ZONES, NETWORKS, PORTS, ZONES, NETWORKS, PORTS, APPLICATIONS, URLS, USERS, and ACTIONS.

| # | NAME       | ACTION | ZONES | NETWORKS | PORTS | ZONES | NETWORKS | PORTS | APPLICATIONS | URLS | USERS | ACTIONS |
|---|------------|--------|-------|----------|-------|-------|----------|-------|--------------|------|-------|---------|
| 1 | Demo_allow | Allow  | ANY   | ANY      | ANY   | ANY   | ANY      | ANY   | ANY          | ANY  | ANY   |         |

At the bottom, the "Default Action" is set to "Access Control" with a "Block" button and a dropdown menu.

Paso 3.15. (Opcional) Configure la regla de exención de NAT para el tráfico del cliente en FTD si se configura NAT dinámica para el cliente para acceder a Internet. En este ejemplo, no es necesario configurar una regla exenta de NAT porque no se configura ninguna NAT dinámica en cada FTD.

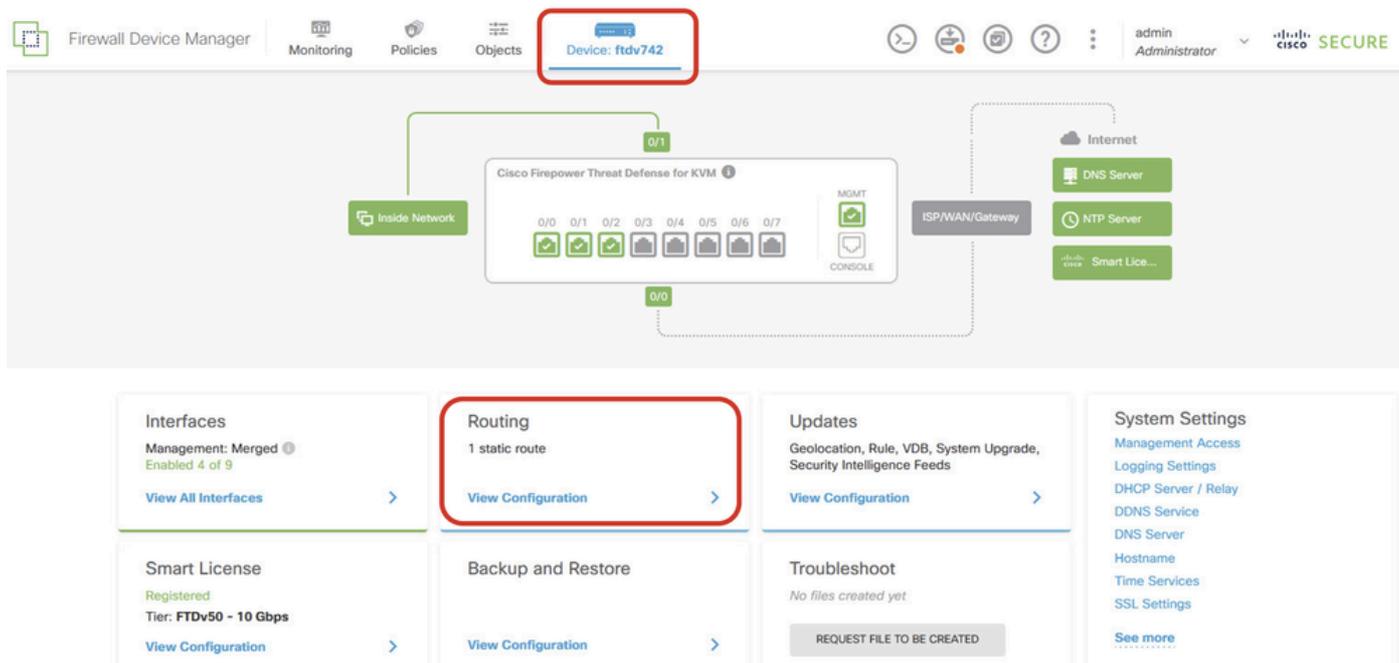
Paso 3.16. Implemente los cambios de configuración.



Deploy\_VPN\_Configuration

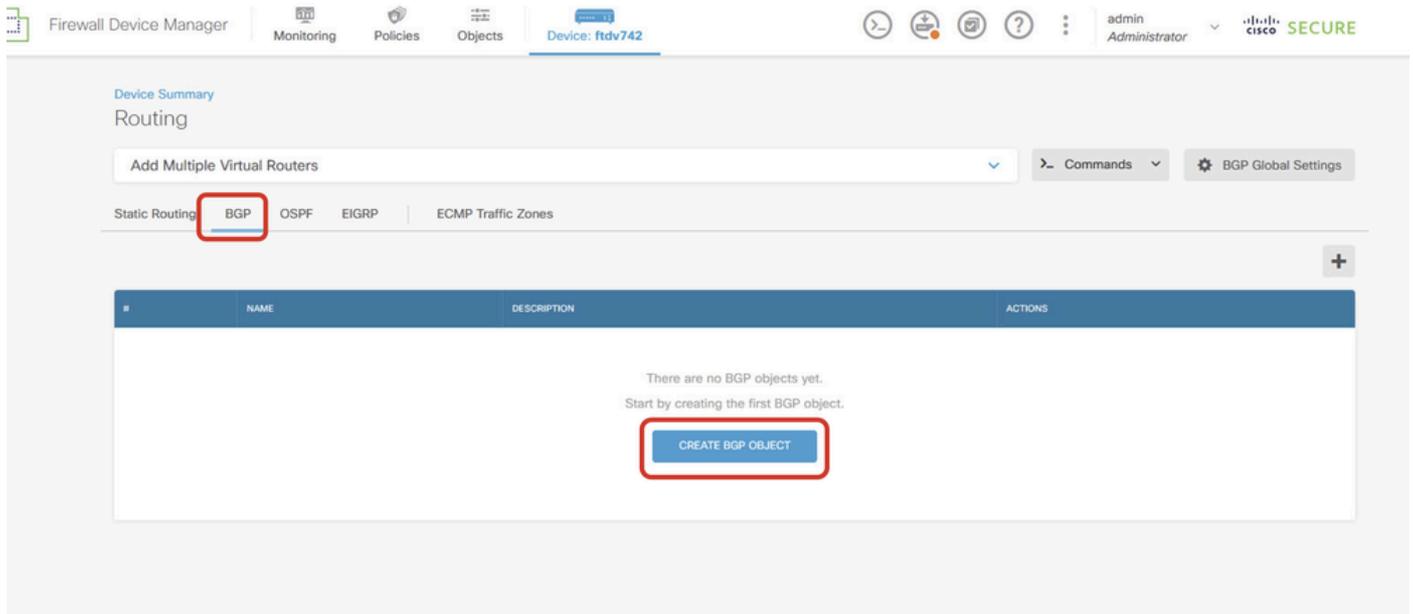
## Configuraciones en BGP

Paso 4. Vaya a Device > Routing. Haga clic en Ver configuración.



View\_Routing\_Configuration

Paso 5. Haga clic en la pestaña BGP y luego haga clic en CREATE BGP OBJECT.



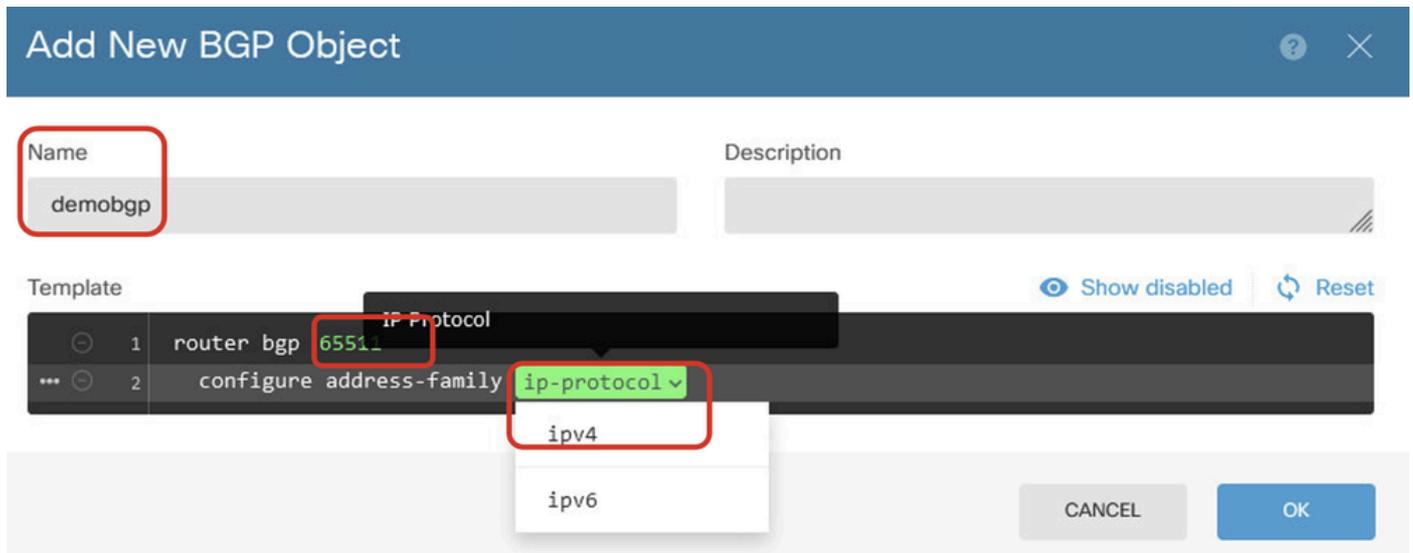
Create\_BGP\_Object

Paso 6. Proporcione el nombre del objeto. Navegue hasta Plantilla y configure. Haga clic en el botón OK para guardar.

Nombre: demobgp

Línea 1: Configure el número AS. Haga clic en as-number. Entrada manual del número AS local. En este ejemplo, el número AS 65511 para el FTD Site1.

Línea 2: Configure el protocolo IP. Haga clic en ip-protocol. Seleccione ipv4.



Create\_BGP\_Object\_ASNumber\_Protocol

Línea 4: Configure más parámetros. Haga clic en settings, elija general, y luego haga clic en Show disabled.

## Add New BGP Object

Name: demobgp

Description:

Template: Show disabled Reset

```

1 router bgp 65511
2   configure address-family ipv4
3   address-family ipv4 unicast
4   configure address-family ipv4 settings

```

Address Family IPv4 Settings

- general
- advanced

CANCEL OK

Create\_BGP\_Object\_AddressSetting

Línea 6: Haga clic en el icono + para habilitar la línea para configurar la red BGP. Haga clic en network-object. Puede ver los objetos disponibles existentes y elegir uno. En este ejemplo, elija el nombre de objeto inside\_192.168.70.0 (creado en el paso 3.2.).

## Add New BGP Object

Name: demobgp

Description:

Template: Hide disabled Reset

```

1 router bgp 65511
2   configure address-family ipv4
3   address-family ipv4 unicast
4   configure address-family ipv4 general
5   distance bgp 20 200 200
6   network network-object
7   network network-object route-map map-tag
8   bgp inject-map inject-map exist-map exist-map options
9   configure aggregate-address map-type
10  configure filter-rules direction
11  configure neighbor neighbor-address remote-as as-number config-options
12  configure ipv4 redistribution protocol identifier none
13  bgp router-id router-id

```

Create\_BGP\_Object\_Add\_Network

## Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 general
5     distance bgp 20 200 200
6   network
7   network
8   bgp inje
9   configur
10  configur
11  configur
12  configur
13  bgp router-i
```

IPV4 Network address

- OutsidelPv4DefaultRoute Network
- OutsidelPv4Gateway Host
- any-ipv4 Network
- any-ipv6 Network
- inside\_192.168.70.0 Network

inside\_192.168.70.0

Create\_BGP\_Object\_Add\_Network2

Línea 11: Haga clic en el icono + para habilitar la línea para configurar la información relacionada con el vecino BGP. Haga clic en neighbor-address, e ingrese manualmente la dirección de vecino BGP de peer. En este ejemplo, es 169.254.10.2 (dirección IP VTI del FTD Site2). Haga clic en as-number, e ingrese manualmente el número AS de peer. En este ejemplo, 65510 es para FTD Site2. Haga clic en config-options y elija properties.

## Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 config-options
12        configure ipv4 redistribution protocol identifier
13        bgp router-id router-id
```

Select Configuration Option

config-options

properties

Create\_BGP\_Object\_NeighborSetting

Línea 14: Haga clic en el icono + para habilitar la línea para configurar algunas propiedades del vecino. Haga clic en activate-options y elija properties.

## Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12          neighbor 169.254.10.2 remote-as 65510
13          configure neighbor 169.254.10.2 remote-as setting
14          configure neighbor 169.254.10.2 activate activate-options
15          configure ipv4 redistribution protocol id
16        bgp router-id router-id
```

Create\_BGP\_Object\_NeighborSetting\_Properties

Línea 13: Haga clic en el icono + para habilitar la línea para mostrar las opciones avanzadas. Haga clic en Settings y elija advanced.

## Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65511 properties
12        neighbor 169.254.10.2 remote-as 65511
13        configure neighbor 169.254.10.2 remote-as 65511 settings
14        configure neighbor 169.254.10.2 activate
15        neighbor 169.254.10.2 activate
16        configure neighbor 169.254.10.2 activate
17        configure ipv4 redistribution protocol identifier
18        bgp router-id router-id
```

Select Neighbor Settings

settings

general

advanced

migration

ha-mode

CANCEL

OK

Create\_BGP\_Object\_NeighborSetting\_Properties\_Advanced

Línea 18: Haga clic en options y elija disable para inhabilitar la detección de MTU de trayectoria.

## Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12        neighbor 169.254.10.2 remote-as 65510
13        configure neighbor 169.254.10.2 remote-as advanced
14        neighbor 169.254.10.2 password secret
15        configure neighbor 169.254.10.2 hops options
16        neighbor 169.254.10.2 version version-number options (optional)
17        neighbor 169.254.10.2 transport connection-mode options
18        neighbor 169.254.10.2 transport path-mtu-discovery options
19        configure neighbor 169.254.10.2 activate properties
20        neighbor 169.254.10.2 activate
21        configure neighbor 169.254.10.2 activate settings
22        configure ipv4 redistribution protocol identifier none
23        bgp router-id router-id
```

Create\_BGP\_Object\_NeighborSetting\_Properties\_Advanced\_PMD

Línea 14, 15, 16, 17: Haga clic en el - botón para desactivar las líneas. A continuación, haga clic en el botón OK para guardar el objeto BGP.

## Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6       network inside_192.168.70.0
7       network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor 169.254.10.2 remote-as 65510 properties
12    neighbor 169.254.10.2 remote-as 65510
13    configure neighbor 169.254.10.2 remote-as advanced
14    neighbor 169.254.10.2 password secret
15    configure neighbor 169.254.10.2 hops options
16    neighbor 169.254.10.2 version version-number
17    neighbor 169.254.10.2 transport connection-mode options
18    neighbor 169.254.10.2 transport path-mtu-discovery disable
19    configure neighbor 169.254.10.2 activate properties
20    neighbor 169.254.10.2 activate
21    configure neighbor 169.254.10.2 activate settings
22    configure ipv4 redistribution protocol identifier none
23  bgp router-id router-id
```

CANCEL

OK

Create\_BGP\_Object\_DisableLines

Esta es una descripción general de la configuración de BGP en este ejemplo. Puede configurar los otros parámetros de BGP en función de sus necesidades reales.

| Name    | Description |
|---------|-------------|
| demobgp |             |

Template

Hide disabled

Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6       network inside_192.168.70.0
7     network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor 169.254.10.2 remote-as 65510 properties
12      neighbor 169.254.10.2 remote-as 65510
13      configure neighbor 169.254.10.2 remote-as advanced
14        neighbor 169.254.10.2 password secret
15        configure neighbor 169.254.10.2 hops options
16        neighbor 169.254.10.2 version version-number
17        neighbor 169.254.10.2 transport connection-mode options
18        neighbor 169.254.10.2 transport path-mtu-discovery disable
19        configure neighbor 169.254.10.2 activate properties
20        neighbor 169.254.10.2 activate
21        configure neighbor 169.254.10.2 activate settings
22        configure ipv4 redistribution protocol identifier none
23    bgp router-id router-id

```

CANCEL

OK

Create\_BGP\_Object\_Final\_Overview

Paso 7. Implemente los cambios de configuración de BGP.

The screenshot shows the Cisco Firewall Device Manager interface. At the top, there are navigation tabs: Firewall Device Manager, Monitoring, Policies, Objects, and Device: ftdv742. The main content area is titled 'Device Summary Routing'. Below this, there is a search bar for 'Add Multiple Virtual Routers' and a 'Commands' dropdown menu. The 'BGP' tab is selected, showing a list of BGP objects. The table below has columns for '#', 'NAME', 'DESCRIPTION', and 'ACTIONS'. There is one object listed: '1 demobgp'.

Deploy\_BGP\_Configuration

Paso 8. Ahora se ha completado la configuración del FTD Site1.

Para configurar Site2 FTD VPN y BGP, repita los pasos 3 a 7 con los parámetros correspondientes de Site2 FTD.

Descripción general de la configuración del FTD del sitio 1 y del FTD del sitio 2 en CLI.

| FTD del sitio 1   | FTD del sitio 2   |
|---|---|
| <pre> NGFW versión 7.4.2  interface GigabitEthernet0/0 nameif outside manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 IP address 192.168.30.1 255.255.255.0  interface GigabitEthernet0/2 nameif inside security-level 0 IP address 192.168.70.1 255.255.255.0  interface Tunnel1 nameif demovti IP address 169.254.10.1 255.255.255.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile e4084d322d  Red de objetos OutsideIPv4Gateway host 192.168.30.3 Red de objetos inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0  access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group  acSvcg-268435457 ifc dentro de cualquier ifc fuera de cualquier rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: </pre> | <pre> NGFW versión 7.4.2  interface GigabitEthernet0/0 nameif outside manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 IP address 192.168.10.1 255.255.255.0  interface GigabitEthernet0/2 nameif inside security-level 0 IP address 192.168.50.1 255.255.255.0  interface Tunnel1 nameif demovti25 IP address 169.254.10.2 255.255.255.0 tunnel source interface outside tunnel destination 192.168.30.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile e4084d322d  Red de objetos OutsideIPv4Gateway host 192.168.10.3 Red de objetos inside_192.168.50.0 subnet 192.168.50.0 255.255.255.0  access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group  acSvcg-268435457 ifc dentro de cualquier ifc fuera de cualquier rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow </pre> |

|   |   |
|---|---|
| <pre> L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object- group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1  router bgp 65511 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 169.254.10.2 remote-as 65510 neighbor 169.254.10.2 transport path-mtu-discovery disable neighbor 169.254.10.2 activate network 192.168.70.0 no auto-summary sin sincronización exit-address-family  route outside 0.0.0.0 0.0.0.0 192.168.30.3 1  crypto ipsec ikev2 ipsec-offer AES256_SHA256 protocol esp encryption aes-256 aes protocol esp integration sha-256 sha-1  crypto ipsec profile ipsec_profile e4084d322d set ikev2 ipsec-offer AES256_SHA256 set security-association lifetime kilobytes 4608000 set security-association lifetime seconds 28800  crypto ipsec security-association pmtu-aging infinite  crypto ikev2 policy 1 encryption aes-256 aes Integrity sha256 sha grupo 14 prf sha256 sha lifetime seconds 86400  crypto ikev2 policy 20 encryption aes-256 aes-192 aes integridad sha512 sha384 sha256 sha grupo 21 20 16 15 14 </pre> | <pre> access-list NGFW_ONBOX_ACL advanced permit object- group lacSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1  router bgp 65510 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 169.254.10.1 remote-as 65511 neighbor 169.254.10.1 transport path-mtu-discovery disable neighbor 169.254.10.1 activate network 192.168.50.0 no auto-summary sin sincronización exit-address-family  route outside 0.0.0.0 0.0.0.0 192.168.10.3 1  crypto ipsec ikev2 ipsec-offer AES256_SHA256 protocol esp encryption aes-256 aes protocol esp integration sha-256 sha-1  crypto ipsec profile ipsec_profile e4084d322d set ikev2 ipsec-offer AES256_SHA256 set security-association lifetime kilobytes 4608000 set security-association lifetime seconds 28800  crypto ipsec security-association pmtu-aging infinite  crypto ikev2 policy 1 encryption aes-256 aes Integrity sha256 sha grupo 14 prf sha256 sha lifetime seconds 86400  crypto ikev2 policy 20 encryption aes-256 aes-192 aes integridad sha512 sha384 sha256 sha grupo 21 20 16 15 14 </pre> |
|---|---|

|  |  |
|--|--|
| <pre>prf sha512 sha384 sha256 sha lifetime seconds 86400  crypto ikev2 enable outside  política de grupo  s2sGP 192.168.10.1 internal política de grupo Atributos  s2sGP 192.168.10.1 vpn-tunnel-protocol ikev2  tunnel-group 192.168.10.1 type ipsec-l2l tunnel-group 192.168.10.1 general-attributes default-group-policy  s2sGP 192.168.10.1  tunnel-group 192.168.10.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****</pre> | <pre>prf sha512 sha384 sha256 sha lifetime seconds 86400  crypto ikev2 enable outside  política de grupo  s2sGP 192.168.30.1 internal política de grupo Atributos  s2sGP 192.168.30.1 vpn-tunnel-protocol ikev2  tunnel-group 192.168.30.1 type ipsec-l2l tunnel-group 192.168.30.1 general-attributes default-group-policy  s2sGP 192.168.30.1  tunnel-group 192.168.30.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****</pre> |
|--|--|

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Navegue hasta la CLI de cada FTD a través de la consola o SSH para verificar el estado de VPN de la fase 1 y la fase 2 a través de los comandos `show crypto ikev2 sa` y `show crypto ipsec sa`.

| FTD del sitio 1   | FTD del sitio 2  |
|---|--|
| <pre>ftdv742# show crypto ikev2 sa  SA IKEv2:  Session-id:134, Status:UP-ACTIVE, IKE count:1, CHILD count:1  Función de estado de FVRF/IVRF remoto local de ID de túnel  563984431 192.168.30.1/500 192.168.10.1/500 Global/Global READY RESPONDER  Encr: AES-CBC, tamaño de clave: 256, hash: SHA256, DH Grp:14, signo de autenticación: PSK, verificación de autenticación: PSK  Vida/Tiempo activo: 86400/5145 s  Child sa: selector local 0.0.0.0/0 - 255.255.255.255/65535</pre> | <pre>ftdv742# show crypto ikev2 sa  SA IKEv2:  Id. de sesión:13, Estado:ACTIVO- ASCENDENTE, recuento IKE:1, recuento HIJO:1  Función de estado de FVRF/IVRF remoto local de ID de túnel  339797985 192.168.10.1/500 192.168.30.1/500 INICIADOR DE PREPARACIÓN global/global Encr: AES-CBC, tamaño de clave: 256, hash: SHA256, DH Grp:14, signo de autenticación: PSK, verificación de autenticación: PSK Vida/Tiempo activo: 86400/74099 s Child sa: selector local 0.0.0.0/0 - 255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255.255/65535 Entrada/salida SPI ESP:</pre> |

|   |  |
|---|--|
| <p>remote selector 0.0.0.0/0 -<br/>255.255.255.255/65535</p> <p>Entrada/salida SPI ESP:<br/>0xf0c4239d/0xb7b5b38b</p>   | <p>0xb7b5b38b/0xf0c4239d</p>   |
| <p>ftdv742# show crypto ipsec sa</p> <p>interfaz: demovti<br/>Etiqueta de mapa criptográfico: __vti-crypto-<br/>map-Tunnel1-0-1, número de secuencia: 65280,<br/>dirección local: 192.168.30.1</p> <p>vrf protegido (ivrf): global<br/>ident local (addr/mask/port/port):<br/>(0.0.0.0/0.0.0.0/0/0)<br/>ident remoto (addr/mask/port/port):<br/>(0.0.0.0/0.0.0.0/0/0)<br/>current_peer: 192.168.10.1</p> <p>#pkts encaps: 5720, #pkts encrypt: 5720, #pkts<br/>digest: 5720<br/>#pkts decaps: 5717, #pkts decrypt: 5717, #pkts<br/>verify: 5717<br/>#pkts comprimido: 0, #pkts descomprimido: 0<br/>#pkts sin comprimir: 5720, error en la<br/>compilación de #pkts: 0, error en la<br/>descomposición de #pkts: 0<br/>#pre-frag éxitos: 0, #pre-frag fracasos: 0,<br/>#fragments creado: 0<br/>#PMTUs enviado: 0, #PMTUs recibido: 0,<br/>#decapsulated frgs que necesitan<br/>reensamblado: 0<br/>#TFC recibido: 0, #TFC enviado: 0<br/>#Valid Errores ICMP recibidos: 0, #Invalid<br/>Errores ICMP recibidos: 0<br/>#send errores: 0, #recv errores: 0</p> <p>local crypto endpt.: 192.168.30.1/500, remote<br/>crypto endpt.: 192.168.10.1/500<br/>path mtu 1500, ipsec overhead 78(44), media<br/>mtu 1500<br/>Tiempo restante de PMTU (s): 0, directiva DF:<br/>copy-df<br/>Validación de error ICMP: deshabilitada,<br/>paquetes TFC: deshabilitados</p> | <p>ftdv742# show crypto ipsec sa</p> <p>interfaz: demovti25<br/>Etiqueta de mapa criptográfico: __vti-crypto-<br/>map-Tunnel1-0-1, número de secuencia: 65280,<br/>dirección local: 192.168.10.1</p> <p>vrf protegido (ivrf): global<br/>ident local (addr/mask/port/port):<br/>(0.0.0.0/0.0.0.0/0/0)<br/>ident remoto (addr/mask/port/port):<br/>(0.0.0.0/0.0.0.0/0/0)<br/>current_peer: 192.168.30.1</p> <p>#pkts encaps: 5721, #pkts encrypt: 5721, #pkts<br/>digest: 5721<br/>#pkts decaps: 5721, #pkts decrypt: 5721, #pkts<br/>verify: 5721<br/>#pkts comprimido: 0, #pkts descomprimido: 0<br/>#pkts sin comprimir: 5721, error de comp #pkts:<br/>0, error de descomp #pkts: 0<br/>#pre-frag éxitos: 0, #pre-frag fracasos: 0,<br/>#fragments creado: 0<br/>#PMTUs enviado: 0, #PMTUs recibido: 0,<br/>#decapsulated frgs que necesitan<br/>reensamblado: 0<br/>#TFC recibido: 0, #TFC enviado: 0<br/>#Valid Errores ICMP recibidos: 0, #Invalid<br/>Errores ICMP recibidos: 0<br/>#send errores: 0, #recv errores: 0</p> <p>local crypto endpt.: 192.168.10.1/500, remote<br/>crypto endpt.: 192.168.30.1/500<br/>path mtu 1500, ipsec overhead 78(44), media<br/>mtu 1500<br/>Tiempo restante de PMTU (s): 0, directiva DF:<br/>copy-df<br/>Validación de error ICMP: deshabilitada,<br/>paquetes TFC: deshabilitados<br/>spi de salida actual: F0C4239D</p> |

|  |  |
|--|--|
| <p>spi saliente actual: B7B5B38B<br/>spi de entrada actual: F0C4239D</p> <p>sas esp de entrada:<br/>spi: 0xF0C4239D (4039386013)<br/>Estado de SA: activo<br/>transform: esp-aes-256 esp-sha-256-hmac no<br/>compression<br/>configuración en uso ={L2L, Túnel, IKEv2, VTI, }<br/>slot: 0, conn_id: 266, crypto-map: __vti-crypto-<br/>map-Tunnel1-0-1<br/>tiempo de sa: duración restante de la clave<br/>(kB/s): (4285389/3722)<br/>Tamaño IV: 16 bytes<br/>compatibilidad con detección de repetición: S<br/>Anti replay bitmap:<br/>0xFFFFFFFF 0xFFFFFFFF<br/>sas esp salientes:<br/>spi: 0xB7B5B38B (3082138507)<br/>Estado de SA: activo<br/>transform: esp-aes-256 esp-sha-256-hmac no<br/>compression<br/>configuración en uso ={L2L, Túnel, IKEv2, VTI, }<br/>slot: 0, conn_id: 266, crypto-map: __vti-crypto-<br/>map-Tunnel1-0-1<br/>tiempo de sa: duración restante de la clave<br/>(kB/s): (4147149/3722)<br/>Tamaño IV: 16 bytes<br/>compatibilidad con detección de repetición: S<br/>Anti replay bitmap:<br/>0x00000000 0x00000001</p> | <p>spi entrante actual: B7B5B38B</p> <p>sas esp de entrada:<br/>spi: 0xB7B5B38B (3082138507)<br/>Estado de SA: activo<br/>transform: esp-aes-256 esp-sha-256-hmac no<br/>compression<br/>configuración en uso ={L2L, Túnel, IKEv2, VTI, }<br/>slot: 0, conn_id: 160, crypto-map: __vti-crypto-<br/>map-Tunnel1-0-1<br/>tiempo de sa: duración restante de la clave<br/>(kB/s): (3962829/3626)<br/>Tamaño IV: 16 bytes<br/>compatibilidad con detección de repetición: S<br/>Anti replay bitmap:<br/>0xFFFFFFFF 0xFFFFFFFF<br/>sas esp salientes:<br/>spi: 0xF0C4239D (4039386013)<br/>Estado de SA: activo<br/>transform: esp-aes-256 esp-sha-256-hmac no<br/>compression<br/>configuración en uso ={L2L, Túnel, IKEv2, VTI, }<br/>slot: 0, conn_id: 160, crypto-map: __vti-crypto-<br/>map-Tunnel1-0-1<br/>tiempo de sa: duración restante de la clave<br/>(kB/s): (4101069/3626)<br/>Tamaño IV: 16 bytes<br/>compatibilidad con detección de repetición: S<br/>Anti replay bitmap:<br/>0x00000000 0x00000001</p> |
|--|--|

Paso 2. Navegue hasta la CLI de cada FTD a través de la consola o SSH para verificar el estado de BGP mediante los comandos show bgp neighbors y show route bgp.

| FTD del sitio 1   | FTD del sitio 2   |
|---|---|
| <p>ftdv742# show bgp neighbors</p> <p>El vecino BGP es 169.254.10.2, vrf single_vf,<br/>AS 65510 remoto, link externo<br/>BGP versión 4, ID de router remoto<br/>192.168.50.1<br/>Estado BGP = Establecido, hasta 1d20h<br/>Última lectura 00:00:25, última escritura<br/>00:00:45, tiempo de espera es 180, intervalo de</p> | <p>ftdv742# show bgp neighbors</p> <p>El vecino BGP es 169.254.10.1, vrf single_vf,<br/>AS 65511 remoto, link externo<br/>BGP versión 4, ID de router remoto<br/>192.168.70.1<br/>Estado BGP = Establecido, hasta 1d20h<br/>Última lectura 00:00:11, última escritura<br/>00:00:52, tiempo de espera es 180, intervalo de</p> |

keepalive es 60 segundos  
Sesiones de vecino:  
1 activo, no admite multisesión (deshabilitado)  
Capacidades del vecino:  
Actualización de ruta: anunciada y recibida  
(nueva)  
Capacidad de ASN de cuatro octetos:  
anunciada y recibida  
Unidifusión IPv4 de la familia de direcciones:  
anunciada y recibida  
Capacidad multisesión:  
Estadísticas de mensajes:  
La profundidad de InQ es 0  
La profundidad de salida es 0

Enviados y recibidos  
Aperturas: 1 1  
Notificaciones: 0 0  
Actualizaciones: 2 2  
Keepalives: 2423 2427  
Actualización de ruta: 0 0  
Total: 2426 2430  
El tiempo mínimo predeterminado entre  
ejecuciones de anuncios es de 30 segundos

Para la familia de direcciones: unidifusión IPv4  
Sesión: 169.254.10.2  
Tabla BGP versión 3, versión vecina 3/0  
Tamaño de la cola de salida: 0  
Índice 1  
1 miembro del grupo de actualización  
Enviados y recibidos  
Actividad de prefijo: ---- ----  
Prefijos actuales: 1 1 (consume 80 bytes)  
Prefijos totales: 1 1  
Retirada implícita: 0 0  
Retirada explícita: 0 0  
Se utiliza como bestpath: n/a 1  
Se utiliza como ruta múltiple: n/a 0

Saliente entrante  
Prefijos denegados de directiva local: ----- ----  
--  
Mejor trayectoria desde este par: 1 n/a  
Total: 1 0  
Número de NLRI en la actualización enviada:

keepalive es 60 segundos  
Sesiones de vecino:  
1 activo, no admite multisesión (deshabilitado)  
Capacidades del vecino:  
Actualización de ruta: anunciada y recibida  
(nueva)  
Capacidad de ASN de cuatro octetos:  
anunciada y recibida  
Unidifusión IPv4 de la familia de direcciones:  
anunciada y recibida  
Capacidad multisesión:  
Estadísticas de mensajes:  
La profundidad de InQ es 0  
La profundidad de salida es 0

Enviados y recibidos  
Aperturas: 1 1  
Notificaciones: 0 0  
Actualizaciones: 2 2  
Keepalives: 2424 a 2421  
Actualización de ruta: 0 0  
Total: 2427 2424  
El tiempo mínimo predeterminado entre  
ejecuciones de anuncios es de 30 segundos

Para la familia de direcciones: unidifusión IPv4  
Sesión: 169.254.10.1  
tabla BGP versión 9, versión vecina 9/0  
Tamaño de la cola de salida: 0  
Índice 4  
4 miembro del grupo de actualización  
Enviados y recibidos  
Actividad de prefijo: ---- ----  
Prefijos actuales: 1 1 (consume 80 bytes)  
Prefijos totales: 1 1  
Retirada implícita: 0 0  
Retirada explícita: 0 0  
Se utiliza como bestpath: n/a 1  
Se utiliza como ruta múltiple: n/a 0

Saliente entrante  
Prefijos denegados de directiva local: ----- ----  
--  
Mejor trayectoria desde este par: 1 n/a  
Total: 1 0  
Número de NLRI en la actualización enviada:

|   |   |
|---|---|
| <p>máx. 1, mín. 0</p> <p>El rastreo de direcciones está habilitado, el RIB tiene una ruta a 169.254.10.2</p> <p>Conexiones establecidas 1; descartadas 0</p> <p>Último restablecimiento nunca</p> <p>Transport(tcp) path-mtu-discovery is disabled</p> <p>Graceful-Restart está desactivado</p>   | <p>máx. 1, mín. 0</p> <p>El rastreo de direcciones está habilitado, el RIB tiene una ruta a 169.254.10.1</p> <p>Conexiones establecidas 4; descartadas 3</p> <p>Último reinicio 1d21h, debido a la inestabilidad de la interfaz de la sesión 1</p> <p>Transport(tcp) path-mtu-discovery is disabled</p> <p>Graceful-Restart está desactivado</p>  |
| <p>ftdv742# show route bgp</p> <p>Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP</p> <p>D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas</p> <p>N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2</p> <p>E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, V - VPN</p> <p>i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2</p> <p>ia - IS-IS inter area, * - candidate default, U - per-user static route</p> <p>o - ODR, P - ruta estática descargada periódicamente, + - ruta replicada</p> <p>SI - InterVRF estático, BI - InterVRF BGP</p> <p>El gateway de último recurso es 192.168.30.3 para la red 0.0.0.0</p> <p>B 192.168.50.0 255.255.255.0 [20/0] vía 169.254.10.2, 1d20h</p> | <p>ftdv742# show route bgp</p> <p>Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP</p> <p>D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas</p> <p>N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2</p> <p>E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, V - VPN</p> <p>i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2</p> <p>ia - IS-IS inter area, * - candidate default, U - per-user static route</p> <p>o - ODR, P - ruta estática descargada periódicamente, + - ruta replicada</p> <p>SI - InterVRF estático, BI - InterVRF BGP</p> <p>El gateway de último recurso es 192.168.10.3 para la red 0.0.0.0</p> <p>B 192.168.70.0 255.255.255.0 [20/0] vía 169.254.10.1, 1d20h</p> |

Paso 3. El cliente Site1 y el cliente Site2 se hacen ping entre sí correctamente.

Cliente del sitio 1:

```
Site1_Client#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/90 ms
```

Cliente de Site2:

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Puede utilizar esos comandos debug para resolver problemas de la sección VPN.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

Puede utilizar esos comandos debug para resolver problemas de la sección BGP.

```
ftdv742# debug ip bgp ?
```

```
A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range     BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpn4       Address family
vpn6       Address family
vrf        VRF scope
<cr>
```

## 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).