

Configuración de eBGP con interfaz de loopback en firewall seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración de eBGP con una Interfaz de Loopback](#)

[Situación](#)

[Diagrama de la red](#)

[Configuración de loopback](#)

[Configuración de ruta estática](#)

[Configuración de BGP](#)

[Verificación](#)

[Resolución de problemas](#)

Introducción

Este documento describe cómo configurar eBGP usando una interfaz Loopback en Cisco Secure Firewall.

Prerequisites

Requirements

Cisco le recomienda que tenga conocimiento acerca de este tema:

- protocolo BGP

La compatibilidad con la interfaz de loopback para BGP se introdujo en la versión 7.4.0, que es la versión mínima requerida para Secure Firewall Management Center y Cisco Secure Firepower Threat Defense.

Componentes Utilizados

- Secure Firewall Management Center para VMware versión 7.4.1
- 2 Cisco Secure Firepower Threat Defense para VMware versión 7.4.1


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

El protocolo de gateway fronterizo (BGP) es un protocolo de routing de vector de ruta estandarizado de protocolo de gateway exterior (EGP) que proporciona escalabilidad, flexibilidad y estabilidad de red. La sesión BGP entre dos peers con el mismo sistema autónomo (AS) se denomina BGP interno (iBGP). Una sesión BGP entre dos peers con diferentes sistemas autónomos (AS) se denomina BGP externo (eBGP).

Generalmente, la relación de peer se establece con la dirección IP de la interfaz más cercana al peer, sin embargo, el uso de una interfaz Loopback para establecer la sesión BGP es útil ya que no hace caer la sesión BGP cuando hay múltiples trayectorias entre los peers BGP.

 Nota: El proceso describe el uso de un Loopback para un peer eBGP; sin embargo, es el mismo proceso para un peer iBGP, por lo que se puede utilizar como referencia.

Configuración de eBGP con una Interfaz de Loopback

Situación

En esta configuración, Firewall SFTD-1 tiene una interfaz de loopback con la dirección IP 10.1.1.1/32, y el AS 64000, Firewall SFTD-2 tiene una interfaz de loopback con la dirección IP 10.2.2.2/32 y el AS 64001. Ambos firewalls utilizan su interfaz externa para alcanzar la interfaz de bucle invertido del otro firewall (en este escenario, la interfaz externa está preconfigurada en ambos firewalls).

Diagrama de la red

En este documento, se utiliza esta configuración de red:

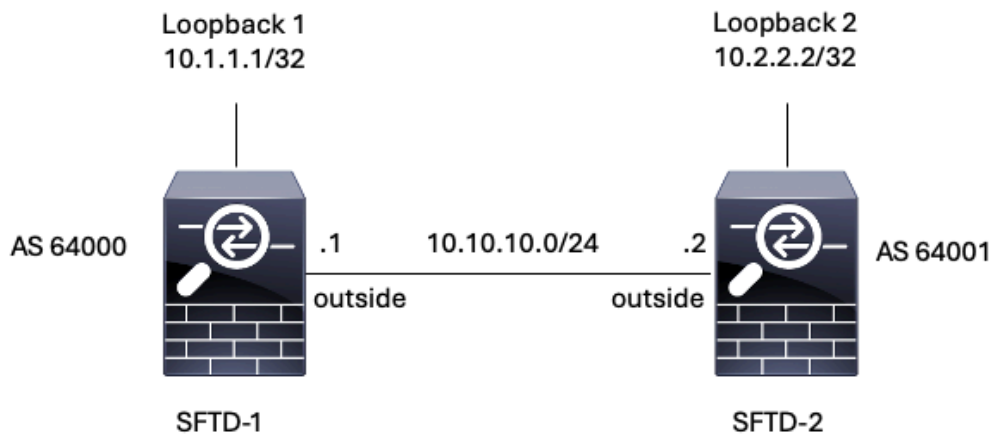


Imagen 1. Diagrama del escenario

Configuración de loopback

Paso 1. Haga clic en **Devices > Device Management**, luego seleccione el dispositivo donde desea configurar el loopback.

Paso 2. Haga clic en **Interfaces > All Interfaces**.

Paso 3. Haga clic en **Add Interface > Loopback Interface**.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical			10.10.10.1/24(Static)	Disabled	Global
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	

Imagen 2. Agregar loopback de interfaz

Paso 4. En la sección **General**, configure el nombre del Loopback, marque la casilla **Enabled** y configure el Loopback ID.

Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Imagen 3. Configuración básica de interfaz de loopback

Paso 5. En la sección IPv4, seleccione la opción Use Static IP en la sección IP Type, configure el Loopback IP y, a continuación, haga clic en OK para guardar los cambios.

Edit Loopback Interface



General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

10.1.1.1/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel

OK

Imagen 4. Configuración de dirección IP de loopback

Paso 6. Click Save.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin | cisco **SECURE**

FTD-1
Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

You have unsaved changes Save Cancel

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↶
GigabitEthernet0/0	outside	Physical			10.10.10.1/24(Static)	Disabled	Global	✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎
GigabitEthernet0/3		Physical				Disabled		✎
Loopback1	Loopback1	Loopback			10.1.1.1/32(Static)	Disabled	Global	✎ 🗑

Imagen 5. Guardar la Configuración de la Interfaz de Loopback

Paso 7. Repita el proceso con el segundo firewall.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical			10.10.10.2/24(Static)	Disabled	Global
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	
Loopback1	Loopback2	Loopback			10.2.2.2/32(Static)	Disabled	Global

Imagen 6. Configuración de la interfaz Loopback en peer

Configuración de ruta estática

Se debe configurar una ruta estática para garantizar que la dirección de peer remoto (Loopback) utilizada para el peering sea accesible a través de la interfaz deseada.

Paso 1. Haga clic en Devices > Device Management y seleccione el dispositivo que desea configurar para la ruta estática.

Paso 2. Haga clic en Routing > Manage Virtual Routers > Static Route y luego haga clic en Add Route.

The screenshot shows the 'Manage Virtual Routers' section with the 'Static Route' option selected in the left sidebar. The main area displays a table for adding routes, with the 'Add Route' button highlighted in red.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▶ IPv4 Routes						
▼ IPv6 Routes						

Imagen 7. Agregar nueva ruta estática

Paso 3. Verifique la opción IPv4 para Type. Seleccione la interfaz física utilizada para alcanzar el loopback del peer remoto en la opción Interface y luego especifique el siguiente salto para alcanzar el loopback en la sección Gateway.

Edit Static Route Configuration



Type: IPv4 IPv6

Interface*

outside

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

Add

any-ipv4

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Selected Network

Ensure that egress virtualrouter has route to that destination

Gateway

10.10.10.2

+

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

+

Cancel

OK

Imagen 8. Configuración de ruta estática

Paso 4. Haga clic en el icono (+) junto a la sección Red disponible.

Edit Static Route Configuration



Type: IPv4 IPv6

Interface*

outside

(interface starting with this icon  signifies it is available for route leak)

Available Network 



Selected Network

Search

Add

any-ipv4

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Ensure that egress virtualrouter has route to that destination

Gateway

10.10.10.2

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel

OK

Imagen 9. Agregar nuevo objeto de red

Paso 5. Configure un nombre para referencia y la IP del Looback del peer remoto y Save.

New Network Object



Name

Loopback-FTD2

Description

Network

Host Range Network FQDN

10.2.2.2

Allow Overrides

Cancel

Save

Imagen 10. Configuración del Destino de Red en la Ruta Estática

Paso 6. Busque el nuevo objeto creado en la barra de búsqueda, selecciónelo, haga clic en Agregar y, a continuación, haga clic en Aceptar.

Edit Static Route Configuration






Type: IPv4 IPv6

Interface*

outside

(Interface starting with this icon  signifies it is available for route leak)

Available Network 	+	Selected Network
<input type="text" value="Loopback-FTD2"/> 	<input type="button" value="Add"/>	Loopback-FTD2 
Loopback-FTD2		

Ensure that egress virtualrouter has route to that destination

Gateway

10.10.10.2 

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:



Cancel

OK

Imagen 1. Configuración del salto siguiente en la ruta estática

Paso 7. Click Save.

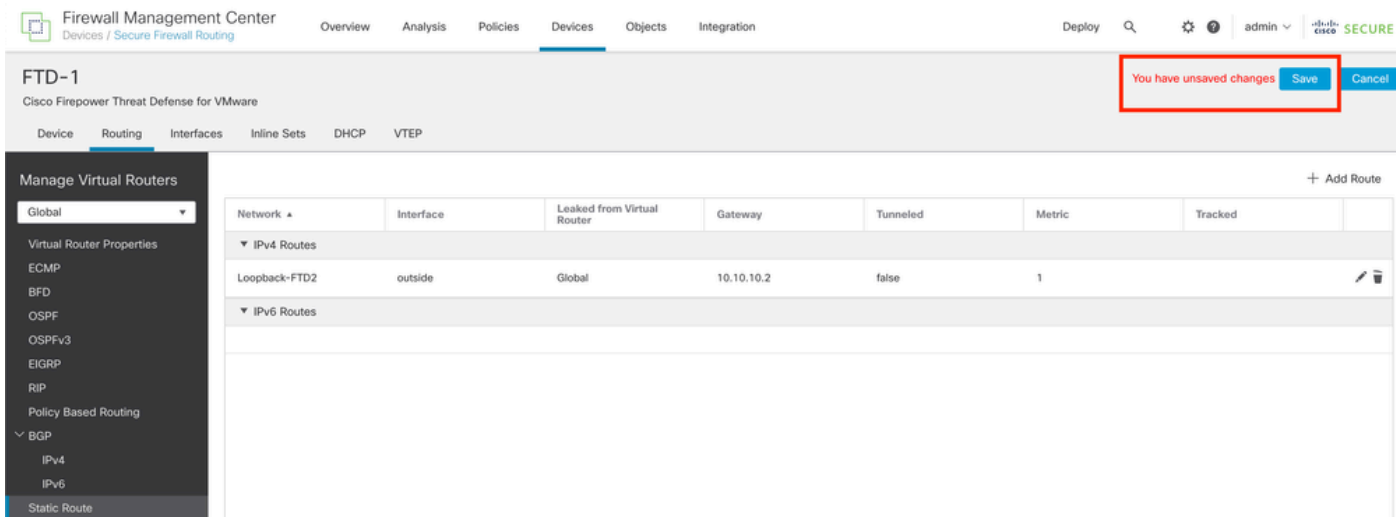


Imagen 12. Guardar la Configuración de la Interfaz de Ruta Estática

Paso 8. Repita el proceso con el segundo firewall.

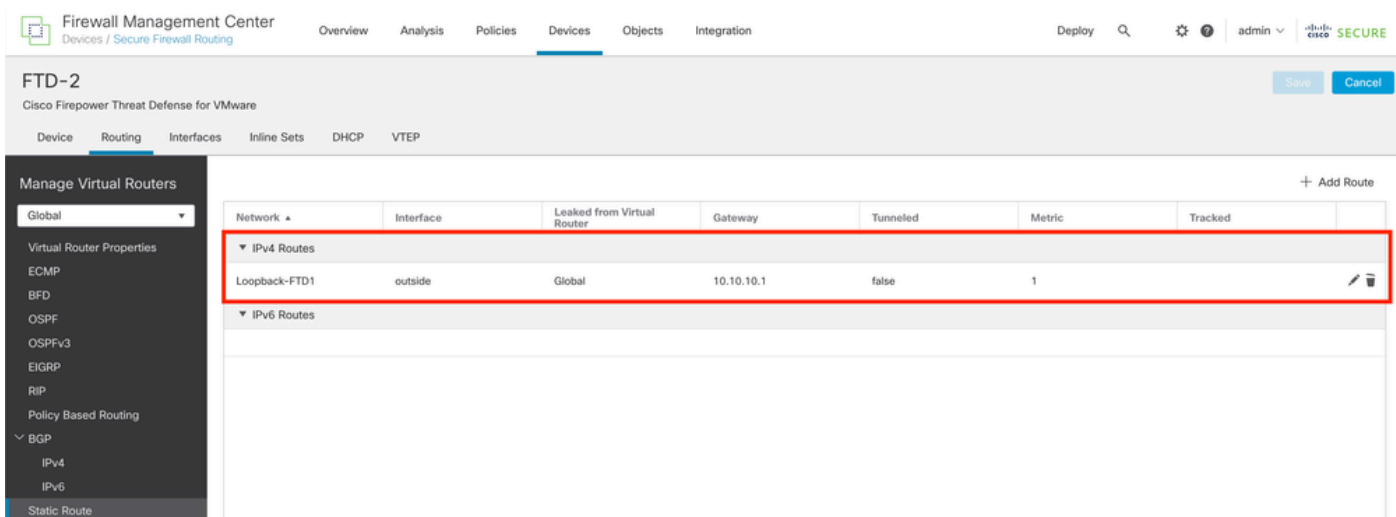


Imagen 13. Configurar ruta estática en par

Configuración de BGP

Paso 1. Haga clic en Devices > Device Management, y seleccione el dispositivo que desea habilitar BGP.

Paso 2. Haga clic en Routing > Manage Virtual Routers > General Settings, y luego haga clic en BGP.

Paso 3. Marque la casilla Enable BGP, luego configure el AS local del firewall en la sección AS Number.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

FTD-1
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter

General Settings
BGP

Enable BGP:

AS Number*
64000 (1-4294967295 or 1.0-65535.65535)

Override BGP general settings router-id address:

Router Id
Automatic

IP Address*

General		Neighbor Timers	
Scanning Interval	60	Keepalive Interval	
Number of AS numbers in AS_PATH attribute of received routes	None	Hold time	
Log Neighbor Changes	Yes	Min hold time	
Use TCP path MTU discovery	Yes	Next Hop	
Reset session upon failover	Yes	Address tracking	
Enforce the first AS is peer's AS for EBGp routes	Yes	Delay interval	
Use dot notation for AS number	No	Graceful Restart (use in f	
Aggregate Timer	30	Graceful Restart	
Best Path Selection		Restart time	
Default local preference	100		

Imagen 14. Habilitar BGP globalmente

Paso 4. Guarde los cambios haciendo clic en el botón Save.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy Q ⚙️ ? admin | Cisco SECURE

FTD-1
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6
Static Route

Enable BGP:

AS Number*
64000 (1-4294967295 or 1.0-65535.65535)

Override BGP general settings router-id address:

Router Id
Automatic

IP Address*

General		Neighbor Timers	
Scanning Interval	60	Keepalive Interval	60
Number of AS numbers in AS_PATH attribute of received routes	None	Hold time	180
Log Neighbor Changes	Yes	Min hold time	0
Use TCP path MTU discovery	Yes		

You have unsaved changes Save Cancel

Imagen 15. Guarde el cambio de habilitación de BGP

Paso 5. En la sección Administrar routers virtuales, vaya a la opción BGP y, a continuación, haga clic en IPv4.

Paso 6. Marque la casilla Enable IPv4, luego haga clic en Neighbor, y luego haga clic en + Add.

The screenshot shows the 'Neighbor' configuration page in the Firewall Management Center. The 'Enable IPv4' checkbox is checked. The 'AS Number' is set to 64000. The 'Neighbor' tab is selected, and the '+ Add' button is highlighted. The table below is empty, indicating no records to display.

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
No records to display				

Imagen 16. Agregar un nuevo par BGP

Paso 7. Configure la dirección IP del peer remoto en la sección Dirección IP, luego configure el AS del peer remoto en la sección AS remoto y marque la casilla Enable address.

Paso 8. Seleccione el loopback de la interfaz local en la sección Actualizar Origen.

The screenshot shows the 'Edit Neighbor' configuration page. The 'IP Address' field is set to 10.0.2.2, the 'Remote AS' field is set to 64001, and the 'Update Source' dropdown is set to 'Loopback1'. The 'Enabled address' checkbox is checked. The 'BFD Follower' is set to 'none'. The 'Description' field is empty. The 'Filtering Routes' tab is selected, and the 'Incoming' and 'Outgoing' sections are visible.

Incoming

Access List: [] +

Route Map: [] +

Prefix List: [] +

AS path filter: [] +

Outgoing

Access List: [] +

Route Map: [] +


Prefix List: [] +

AS path filter: [] +

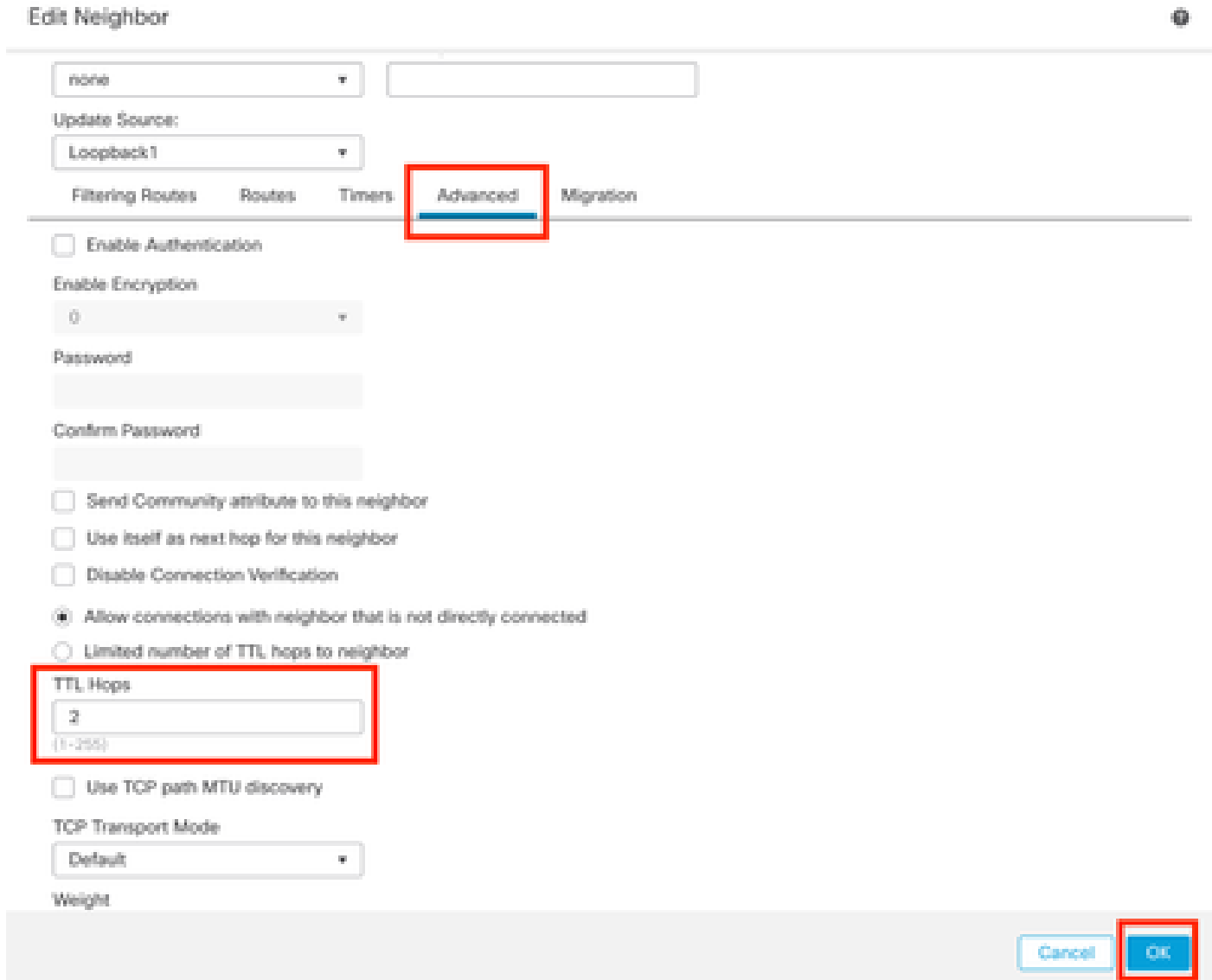
Limit the number of prefixes allowed from the neighbor

Imagen 17. Parámetros de Peer BGP Básicos

Nota: La opción Update Source habilita el comando neighbor update-source, que se utiliza

 para permitir cualquier interfaz operativa (incluidos los loopbacks). Este comando se puede especificar para establecer conexiones TCP.

Paso 9. Haga clic en Advanced, luego configure el número 2 en la opción TTL Hops, y haga clic en OK.



Edit Neighbor ⊙

none

Update Source:
Loopback1

Filtering Routes Routes Timers **Advanced** Migration

Enable Authentication

Enable Encryption
0

Password

Confirm Password

Send Community attribute to this neighbor

Use itself as next hop for this neighbor

Disable Connection Verification

Allow connections with neighbor that is not directly connected

Limited number of TTL hops to neighbor


TTL Hops
2
(1-255)

Use TCP path MTU discovery

TCP Transport Mode
Default

Weight

Imagen 18. Configurar el número de salto de TTL

 Nota: La opción TTL Hops habilita el comando ebgp-multihop, que se utiliza para cambiar el valor TTL para permitir que el paquete alcance el peer BGP externo que no está conectado directamente o que tiene una interfaz que no es la interfaz conectada directamente.

Paso 10. Haga clic en Guardar e implemente los cambios.

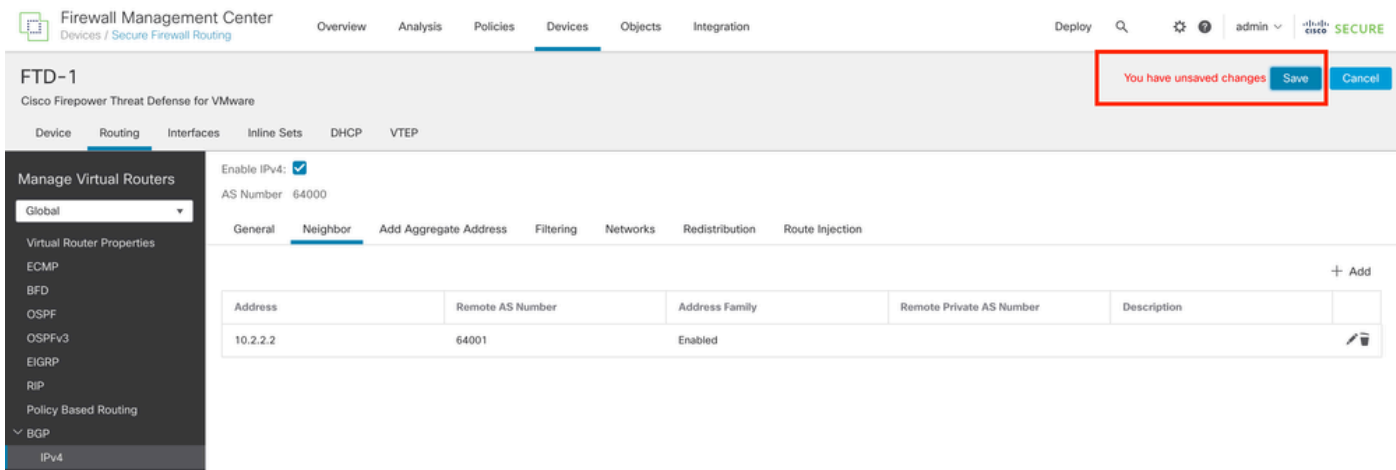


Imagen 19. Guarde la configuración BGP

Paso 11. Repita el proceso con el segundo firewall.

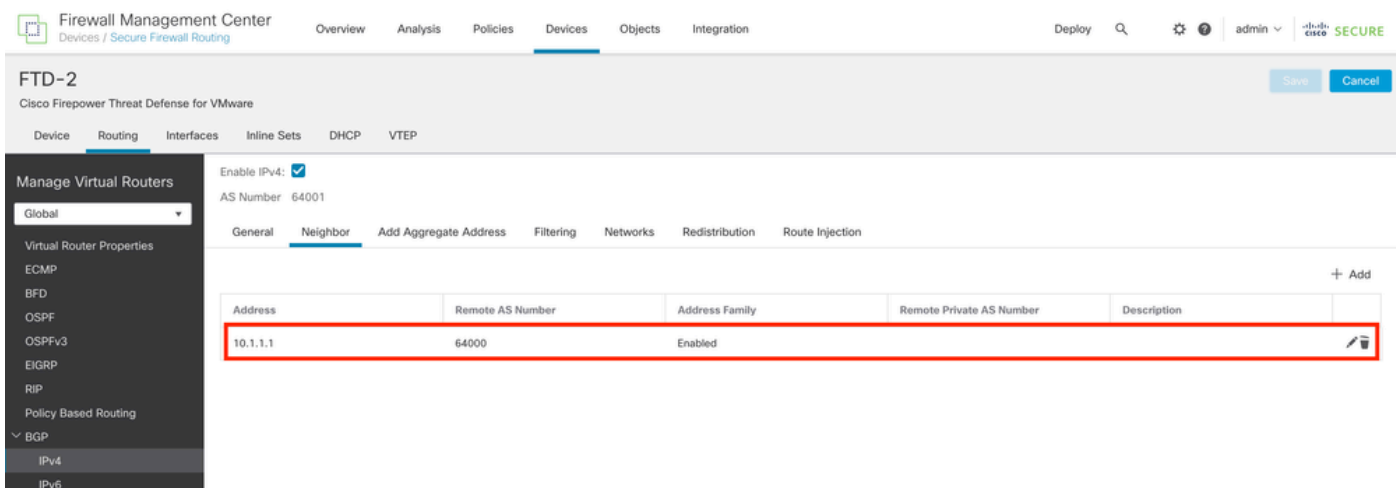


Imagen 20. Configuración de BGP en Peer

Verificación

Paso 1. Verifique la configuración de loopback y ruta estática, luego verifique la conectividad entre los peers BGP con una prueba de ping.

```
show running-config interface interface_name
```

```
show running-config route
```

```
show destination_ip
```

SFTD-1	SFTD-2
<pre>show running-config interface Loopback1</pre> <pre>interface Loopback1</pre>	<pre>show running-config interface Loopback1</pre> <pre>interface Loopback1</pre>

<pre> nameif Loopback1 ip address 10.1.1.1 255.255.255.255 show running-config route route outside 10.2.2.2 255.255.255.255 10.10.10.2 1 ping 10.2.2.2 Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms </pre>	<pre> nameif Looback2 ip address 10.2.2.2 255.255.255.255 show running-config route route outside 10.1.1.1 255.255.255.255 10.10.10.1 1 ping 10.1.1.1 Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms </pre>
---	--

Paso 2. Verifique la configuración de BGP y, a continuación, asegúrese de que se ha establecido el peering BGP.

show running-config router bgp

show bgp neighbors

show bgp summary

SFTD-1	SFTD-2
<pre> show running-config router bgp router bgp 64000 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 10.2.2.2 remote-as 64001 neighbor 10.2.2.2 ebgp-multihop 2 neighbor 10.2.2.2 transport path-mtu-discovery disable neighbor 10.2.2.2 update-source Loopback1 </pre>	<pre> show running-config router bgp router bgp 64001 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 10.1.1.1 remote-as 64000 neighbor 10.1.1.1 ebgp-multihop 2 neighbor 10.1.1.1 transport path-mtu-discovery disable neighbor 10.1.1.1 update-source Looback2 </pre>

<pre>neighbor 10.2.2.2 activate no auto-summary sin sincronización exit-address-family !</pre> <pre>show bgp neighbors i BGP</pre> <p>El vecino BGP es 10.2.2.2, vrf single_vf, AS 64001 remoto, link externo</p> <p>BGP versión 4, ID del router remoto 10.2.2.2</p> <p>estado BGP = Establecido, hasta 1d15h</p> <p>tabla BGP versión 7, versión vecina 7/0</p> <p>El vecino BGP externo puede estar hasta a 2 saltos de distancia.</p> <pre>show bgp summary</pre> <p>Identificador de router BGP 10.1.1.1, número AS local 64000</p> <p>La versión de la tabla BGP es 7, la tabla de ruteo principal es 7</p> <pre>Neighbor V AS MsgRcvd MsgSent TbIVer InQ OutQ Up/Down State/PfxRcd</pre> <pre>10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0</pre>	<pre>neighbor 10.1.1.1 activate no auto-summary sin sincronización exit-address-family !</pre> <pre>show bgp neighbors i BGP</pre> <p>El vecino BGP es 10.1.1.1, vrf single_vf, AS 64000 remoto, link externo</p> <p>BGP versión 4, ID del router remoto 10.1.1.1</p> <p>estado BGP = Establecido, hasta 1d16h</p> <p>tabla BGP versión 1, versión vecina 1/0</p> <p>El vecino BGP externo puede estar hasta a 2 saltos de distancia.</p> <pre>show bgp summary</pre> <p>Identificador de router BGP 10.2.2.2, número AS local 64001</p> <p>La versión de la tabla BGP es 1, la tabla de ruteo principal es 1</p> <pre>Neighbor V AS MsgRcvd MsgSent TbIVer InQ OutQ Up/Down State/PfxRcd</pre> <pre>10.1.1.1 4 64000 2168 2173 1 0 0 1d16h 0</pre>
---	---

Resolución de problemas

Si experimenta algún problema durante el proceso, revise este artículo:

- Border Gateway Protocol (BGP)

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).