

Configurar o eBGP com interface de loopback no firewall seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração do eBGP com uma interface de loopback](#)

[Cenário](#)

[Diagrama de Rede](#)

[Configuração de loopback](#)

[Configuração de rota estática](#)

[Configuração de BGP](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar o eBGP usando uma interface de loopback no Cisco Secure Firewall.

Pré-requisitos

Requisitos

A Cisco recomenda ter conhecimento deste tópico:

- protocolo BGP

O suporte à interface de loopback para BGP foi introduzido na versão 7.4.0, que é a versão mínima necessária para o Secure Firewall Management Center e o Cisco Secure Firepower Threat Defense.

Componentes Utilizados

- Secure Firewall Management Center for VMware versão 7.4.1
- 2 Cisco Secure Firepower Threat Defense for VMware versão 7.4.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O BGP (Border Gateway Protocol) é um protocolo de roteamento de vetor de caminho padronizado EGP (Exterior Gateway Protocol) que fornece escalabilidade, flexibilidade e estabilidade de rede. A sessão de BGP entre dois peers com o mesmo Sistema Autônomo (AS) é chamada de BGP Interno (iBGP). Uma sessão de BGP entre dois peers com sistemas autônomos (AS) diferentes é chamada de BGP externo (eBGP).

Normalmente, a relação de peer é estabelecida com o endereço IP da interface mais próxima do peer. No entanto, o uso de uma interface de loopback para estabelecer a sessão BGP é útil, já que não desativa a sessão BGP quando há vários caminhos entre os peers BGP.

 Observação: o processo descreve o uso de um Loopback para um peer eBGP, no entanto, é o mesmo processo para um peer iBGP para que possa ser usado como referência.

Configuração do eBGP com uma interface de loopback

Cenário

Nessa configuração, o Firewall SFTD-1 tem uma interface de Loopback com o endereço IP 10.1.1.1/32 e o AS 64000, o Firewall SFTD-2 tem uma interface de Loopback com o endereço IP 10.2.2.2/32 e o AS 64001. Ambos os firewalls usam sua interface externa para acessar a interface de loopback do outro firewall (nesse cenário, a interface externa é pré-configurada em ambos os firewalls).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

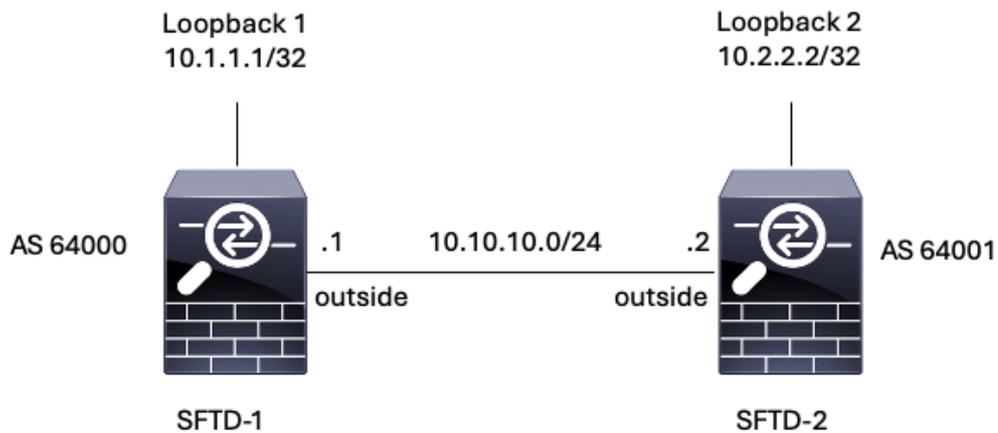


Imagem 1. Diagrama de Cenário

Configuração de loopback

Etapa 1. Clique em Devices > Device Management e, em seguida, selecione o dispositivo onde deseja configurar o Loopback.

Etapa 2. Clique em Interfaces > Todas as interfaces.

Etapa 3. Clique em Adicionar interface > Interface de loopback.

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	

Imagem 2. Adicionar Loopback de Interface

Etapa 4. Na seção Geral, configure o nome do Loopback, marque a caixa Habilitado e configure o ID de Loopback.

Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Imagem 3. Configuração básica de interface de loopback

Etapa 5. Na seção IPv4, selecione a opção Usar IP estático na seção Tipo de IP, configure o IP de loopback e clique em OK para salvar as alterações.

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

Imagem 4. Configuração de endereço IP de loopback

Etapa 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	✎ 🗑️

Imagem 5. Salvar a configuração da interface de loopback

Passo 7. Repita o processo com o segundo Firewall.

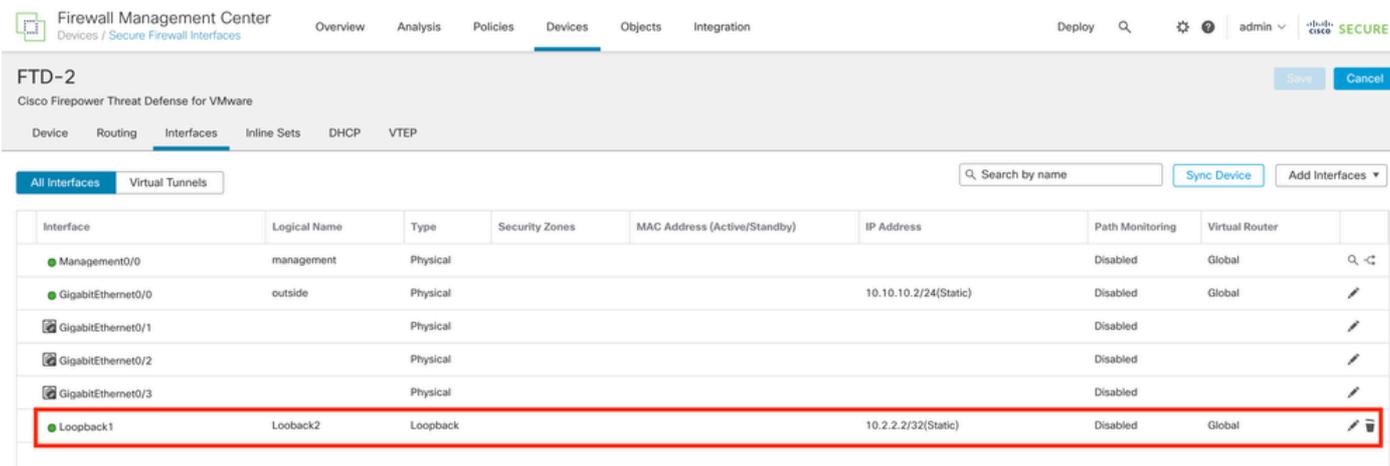


Imagem 6. Configuração de Interface de Loopback no par

Configuração de rota estática

Uma rota estática deve ser configurada para garantir que o endereço de peer remoto (loopback) usado para peering esteja acessível através da interface desejada.

Etapa 1. Clique em Devices > Device Management e selecione o dispositivo para o qual deseja configurar a rota estática.

Etapa 2. Clique em Roteamento > Gerenciar roteadores virtuais > Rota estática e clique em Adicionar rota.

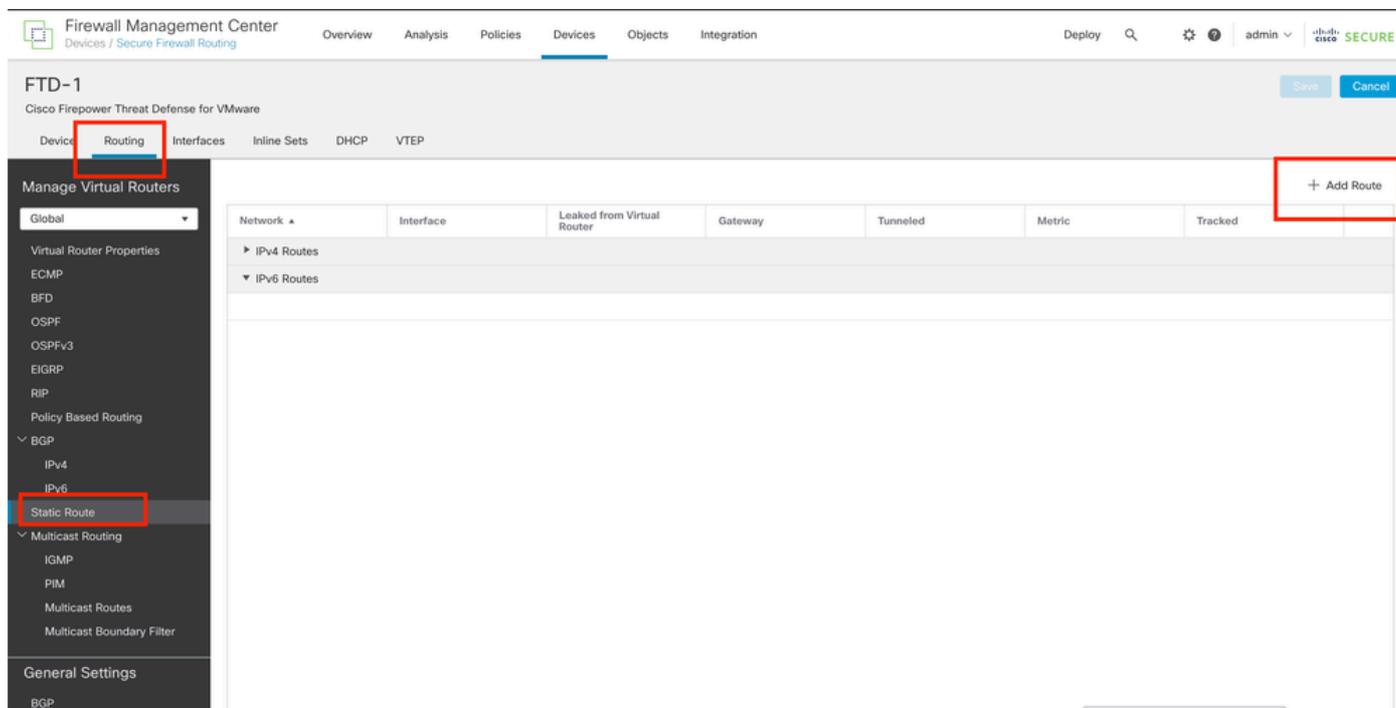


Imagem 7. Adicionar nova rota estática

Etapa 3. Verifique a opção IPv4 para Type. Selecione a interface física usada para acessar o Loopback do peer remoto na opção Interface e, em seguida, especifique o próximo salto para acessar o Loopback na seção Gateway.

Edit Static Route Configuration



Type: IPv4 IPv6

Interface*

outside

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

Available Network  

Q 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

Imagem 8. Configuração de rota estática

Etapa 4. Clique no ícone (+) próximo à seção Rede disponível.

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

Imagem 9. Adicionar novo objeto de rede

Etapa 5. Configure um nome para referência e o IP do Loopback do peer remoto e Save.

New Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

Imagem 10. Configure o destino da rede na rota estática

Etapa 6. Pesquise o novo objeto criado na barra de pesquisa, selecione-o, clique em Adicionar e em OK.

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

Imagem 11. Configurar o próximo salto na rota estática

Passo 7. Click Save.

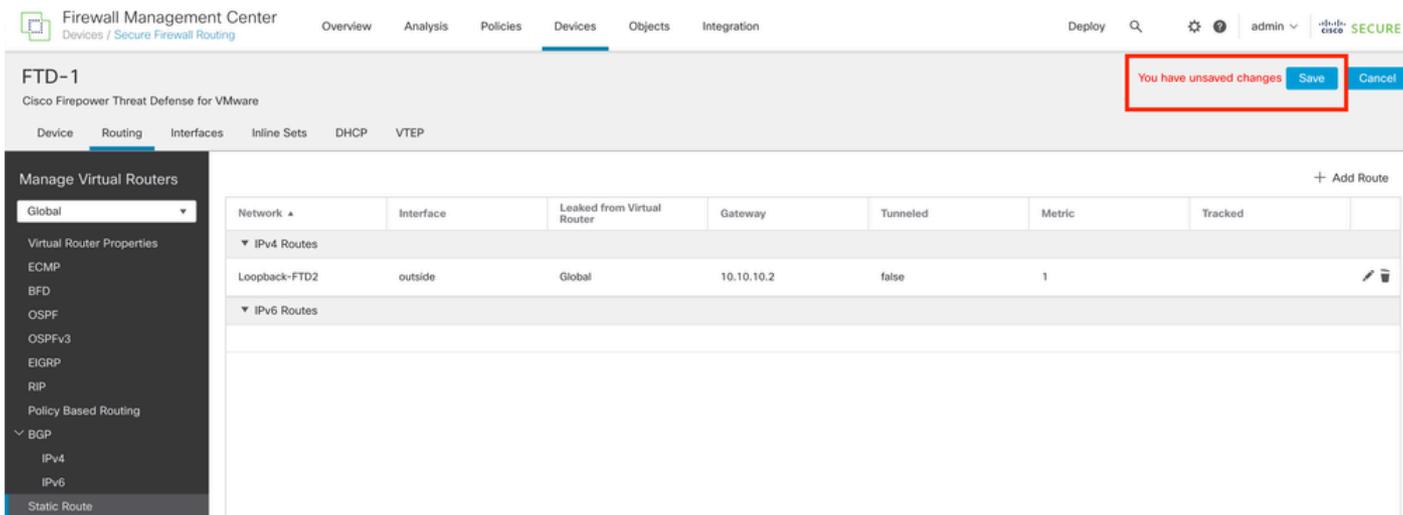


Imagem 12. Salvar a configuração da interface de rota estática

Etapa 8. Repita o processo com o segundo Firewall.

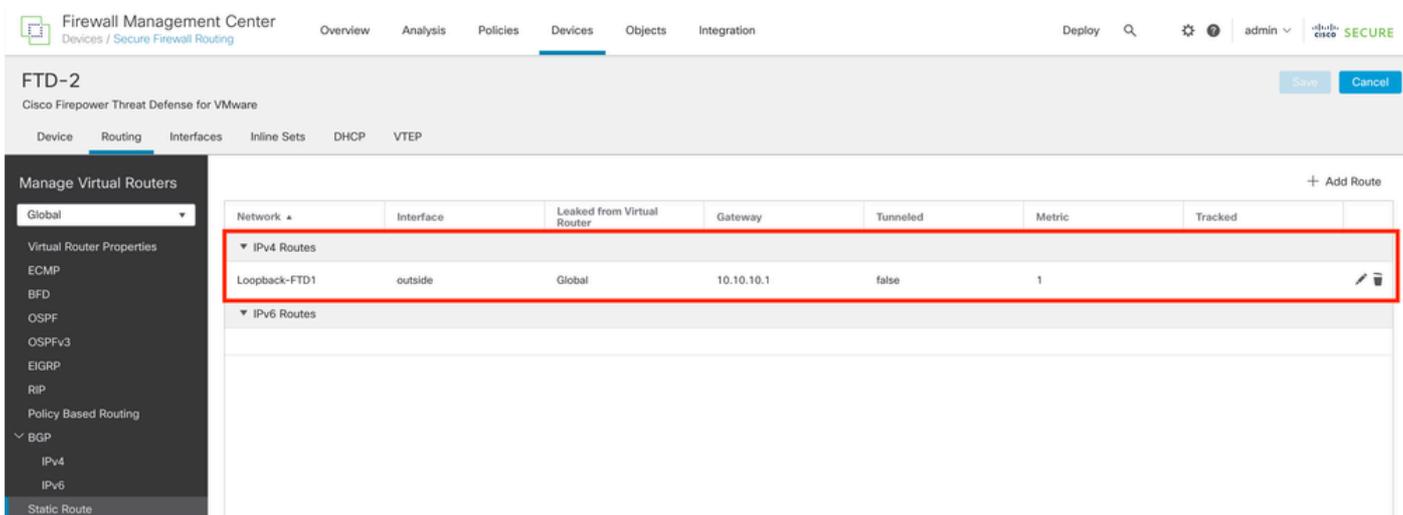


Imagem 13. Configurar Rota Estática no Peer

Configuração de BGP

Etapa 1. Clique em Devices > Device Management e selecione o dispositivo que deseja habilitar o BGP.

Etapa 2. Clique em Roteamento > Gerenciar roteadores virtuais > Configurações gerais e clique em BGP.

Etapa 3. Marque a caixa Enable BGP e configure o AS local do Firewall na seção AS Number.

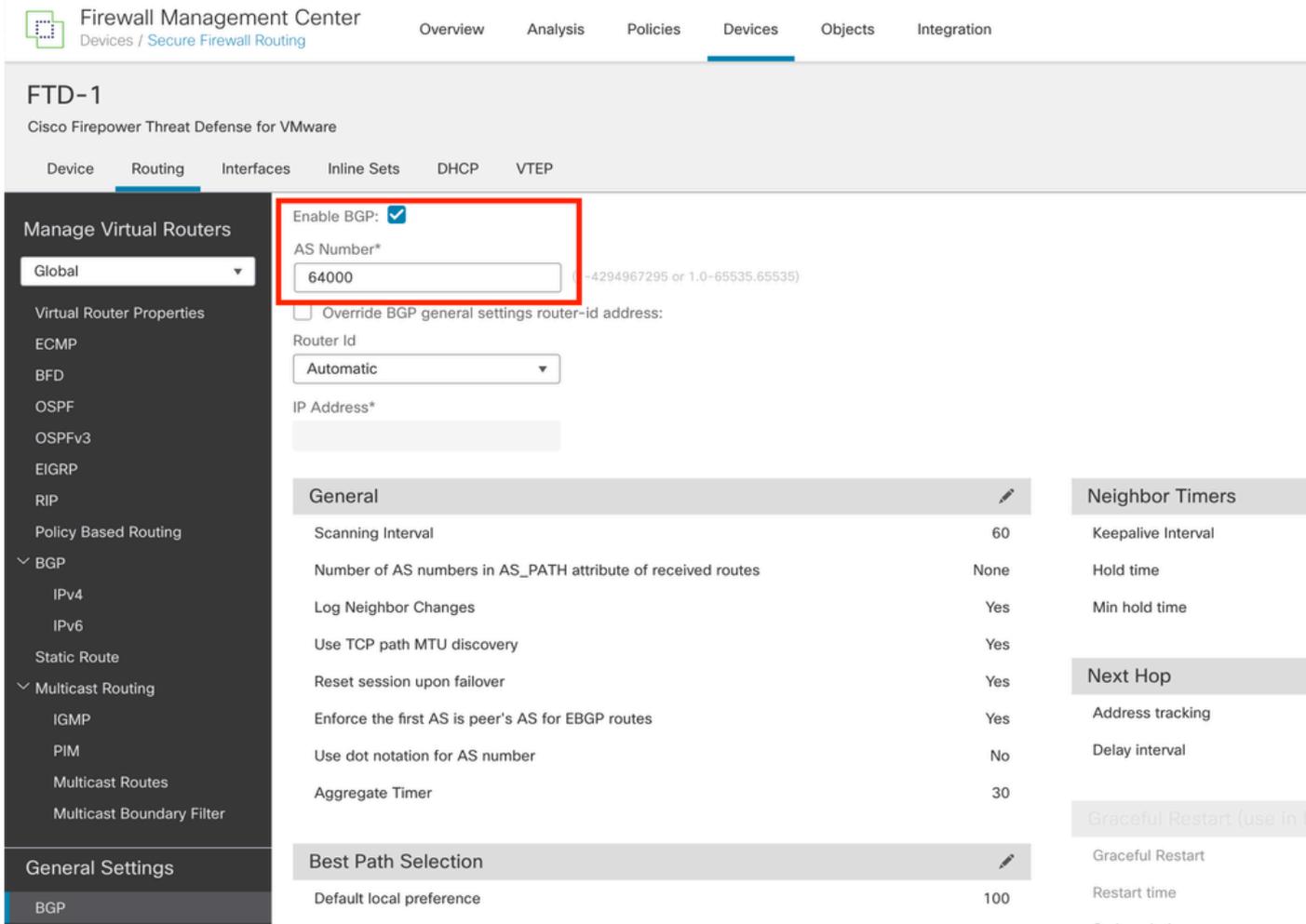


Imagem 14. Ativar o BGP globalmente

Etapa 4. Salve as alterações clicando no botão Save.

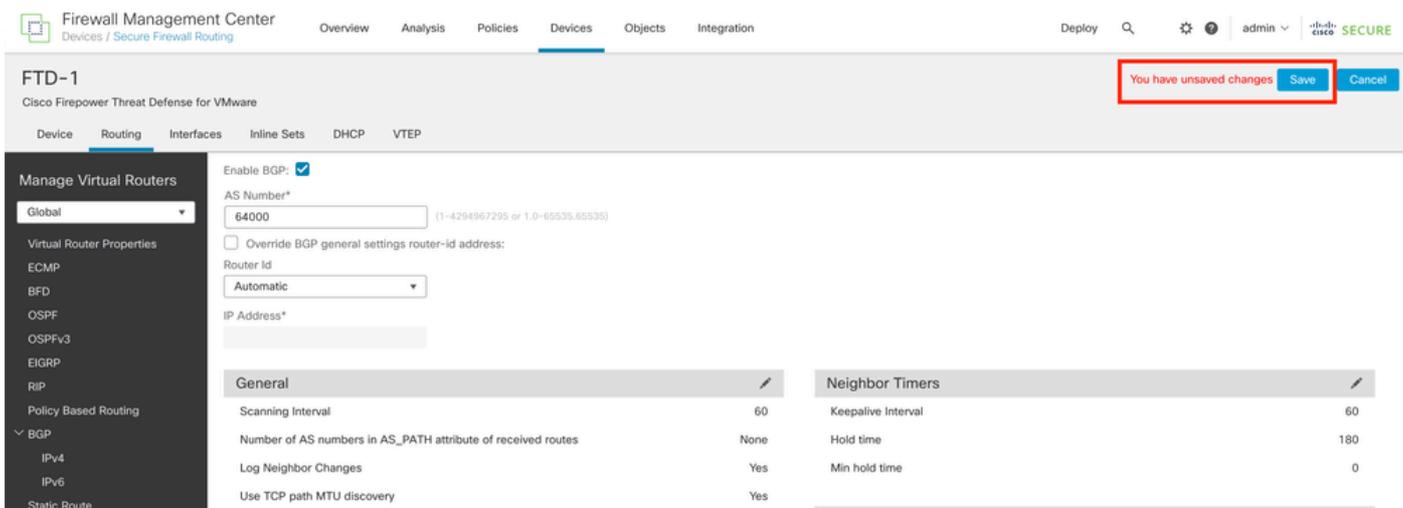


Imagem 15. Salve a alteração de ativação do BGP

Etapa 5. Na seção Manage Virtual Routers, vá para a opção BGP e clique em IPv4.

Etapa 6. Marque a caixa Enable IPv4, clique em Neighbor e clique em + Add.

The screenshot shows the 'FTD-1' configuration page in the Firewall Management Center. The 'Neighbor' tab is active, and the 'Add' button is highlighted. The 'Enable IPv4' checkbox is checked, and the 'AS Number' is set to 64000. The table below the tabs is empty, with a '+ Add' button in the top right corner.

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

Imagem 16. Adicionar um Novo Par BGP

Passo 7. Configure o endereço IP do peer remoto na seção Endereço IP, configure o AS do peer remoto na seção AS Remoto e marque a caixa Ativar endereço.

Etapa 8. Selecione o loopback da interface local na seção Atualizar origem.

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 'Filtering Routes' tab is selected, and the 'Incoming' and 'Outgoing' sections are visible.

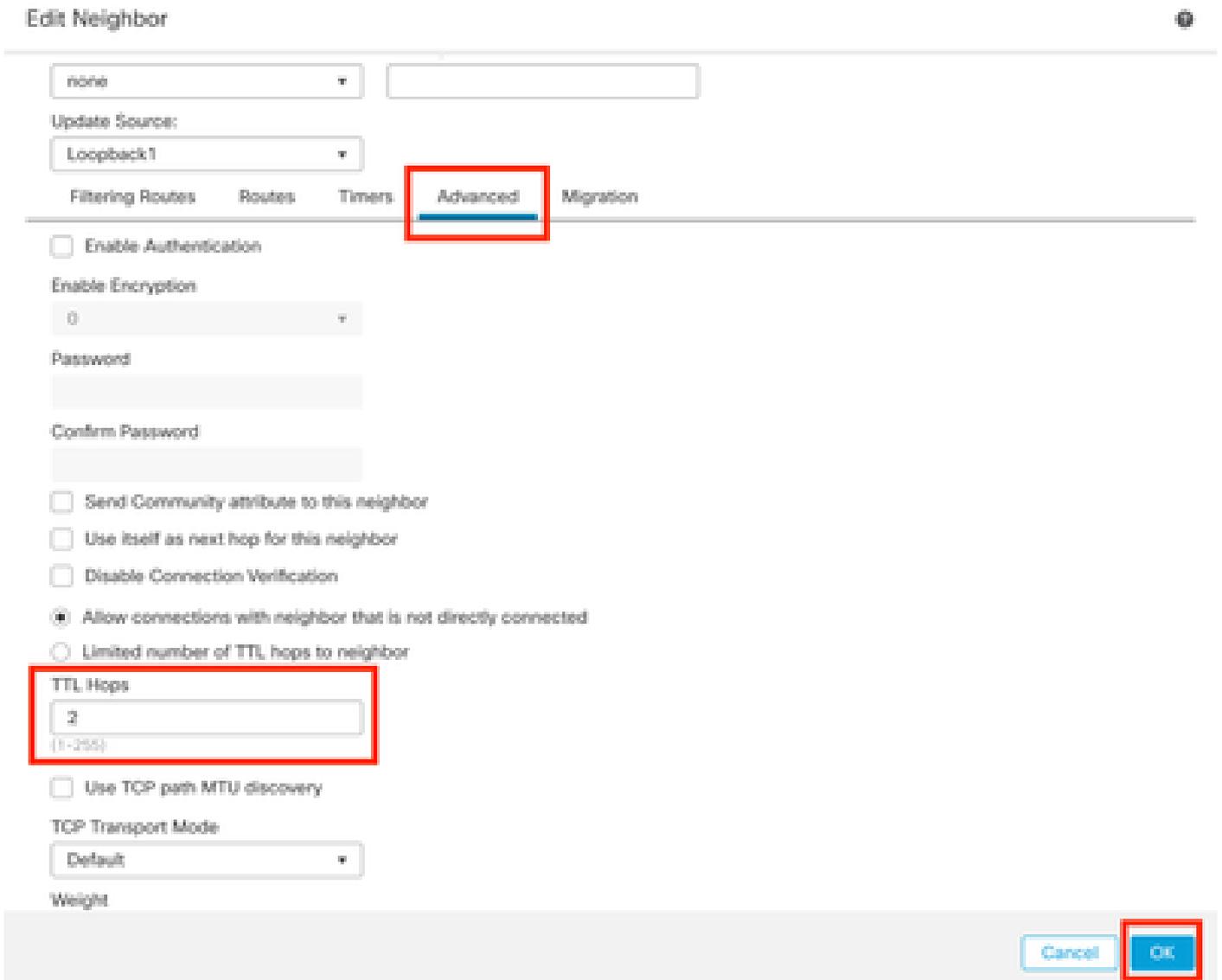
Incoming	Outgoing
Access List	Access List
Route Map	Route Map
Prefix List	Prefix List
AS path filter	AS path filter

Imagem 17. Parâmetros Básicos de Pares BGP

Observação: a opção Update Source ativa o comando neighbor update-source , usado para

 permitir qualquer interface operacional (incluindo loopbacks). Esse comando pode ser especificado para estabelecer conexões TCP.

Etapa 9. Clique em Avançado e configure o número 2 na opção Saltos TTL e clique em 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

Cancel OK

Imagem 18. Configurar o número de salto TTLs

 Observação: a opção TTL Hops habilita o comando `ebgp-multihop`, usado para alterar o valor TTL para permitir que o pacote acesse o par BGP externo que não está diretamente conectado ou tem uma interface diferente da interface diretamente conectada.

Etapa 10. Clique em Salvar e implante as alterações.

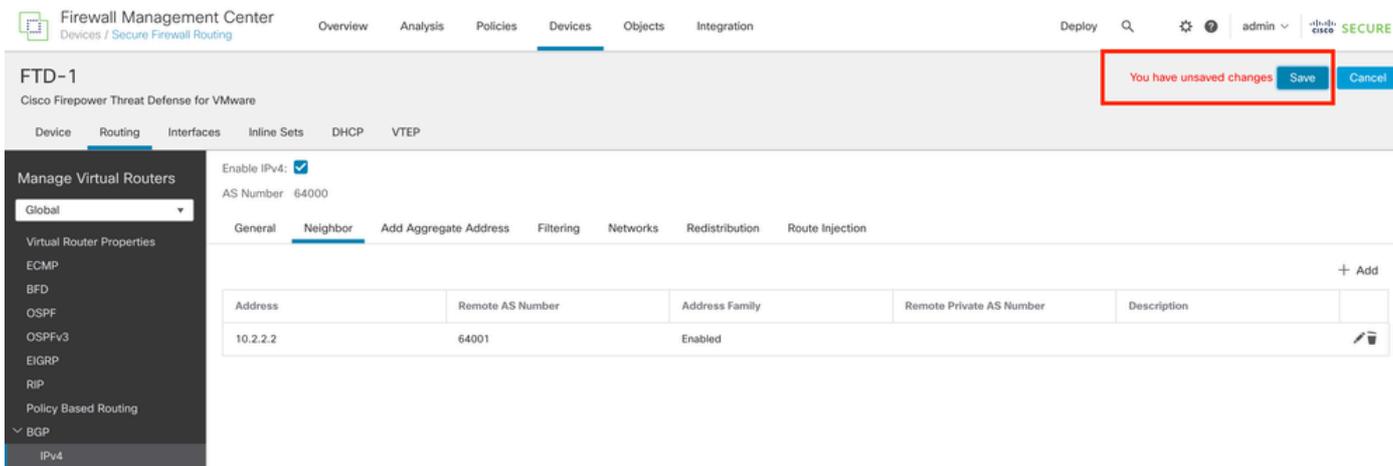


Imagem 19. Salvar a configuração do BGP

Etapa 11. Repita o processo com o segundo Firewall.

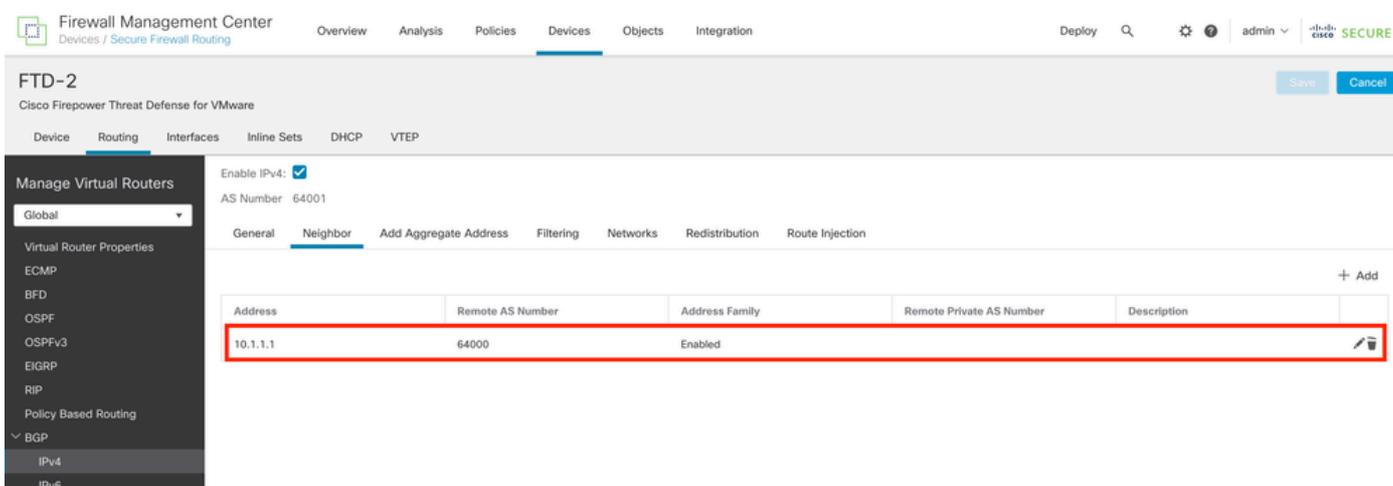


Imagem 20. Configurar BGP no Peer

Verificar

Etapa 1. Verifique a configuração do Loopback e da rota estática e, em seguida, verifique a conectividade entre os peers BGP com um teste 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 rota externa 10.2.2.2 255.255.255.255 10.10.10.2 1 ping 10.2.2.2 Enviando Echos ICMP de 5.100 bytes para 10.2.2.2, o tempo limite é de 2 segundos: !!!! A taxa de sucesso é de 100% (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 rota externa 10.1.1.1 255.255.255.255 10.10.10.1 1 ping 10.1.1.1 Enviando Echos ICMP de 5.100 bytes para 10.1.1.1, o tempo limite é de 2 segundos: !!!! A taxa de sucesso é de 100% (5/5), round-trip min/avg/max = 1/1/1 ms </pre>
--	---

Etapa 2. Verifique a configuração do BGP e, em seguida, assegure-se de que o peering de BGP esteja estabelecido.

```
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 autoassign 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 autoassign 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 ativate no autossommary sem sincronização exit-address-family ! show bgp neighbors i BGP</pre> <p>O vizinho BGP é 10.2.2.2, vrf single_vf, AS 64001 remoto, link externo</p> <p>BGP versão 4, ID do roteador remoto 10.2.2.2</p> <p>Estado de BGP = Estabelecido, para 1d15h</p> <p>Tabela BGP versão 7, versão vizinha 7/0</p> <p>O vizinho BGP externo pode estar a até 2 saltos de distância.</p> <pre>show bgp summary</pre> <p>Identificador do roteador BGP 10.1.1.1, número AS local 64000</p> <p>A versão da tabela de BGP é 7, a versão 7 da tabela de roteamento principal</p> <pre>Neighbor V AS MsgRcvd MsgSent TbIVer InQ OutQ Up/Down State/PfxRcd 10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0</pre>	<pre>neighbor 10.1.1.1 ativate no autossommary sem sincronização exit-address-family ! show bgp neighbors i BGP</pre> <p>O vizinho BGP é 10.1.1.1, vrf single_vf, AS 64000 remoto, link externo</p> <p>BGP versão 4, ID do roteador remoto 10.1.1.1</p> <p>Estado de BGP = Estabelecido, para 1d16h</p> <p>Tabela BGP versão 1, versão vizinha 1/0</p> <p>O vizinho BGP externo pode estar a até 2 saltos de distância.</p> <pre>show bgp summary</pre> <p>Identificador do roteador BGP 10.2.2.2, número AS local 64001</p> <p>A versão da tabela de BGP é 1, a versão da tabela de roteamento principal é 1</p> <pre>Neighbor V AS MsgRcvd MsgSent TbIVer InQ OutQ Up/Down State/PfxRcd 10.1.1.1 4 64000 2168 2173 1 0 0 1d16h 0</pre>
--	--

Troubleshooting

Se você tiver algum problema durante o processo, leia este artigo:

· [BGP \(Border Gateway Protocol\)](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.