

Configureer eBGP met Loopback-interface op beveiligde firewall

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[eBGP-configuratie met een terugkoppelingsinterface](#)

[Scenario](#)

[Netwerkdigram](#)

[Terugbelconfiguratie](#)

[Statische routeconfiguratie](#)

[BGP-configuratie](#)

[Verifiëren](#)

[Probleemoplossing](#)

Inleiding

Dit document beschrijft hoe u eBGP kunt configureren met behulp van een Loopback-interface in de Cisco Secure Firewall.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met dit onderwerp:

- BGP-protocol

Ondersteuning van Loopback-interface voor BGP is geïntroduceerd in versie 7.4.0, de minimumversie die vereist is voor Secure Firewall Management Center en Cisco Secure Firepower Threat Defence.

Gebruikte componenten

- Secure Firewall Management Center voor VMware versie 7.4.1
- 2 Cisco Secure Firepower Threat Defence voor VMware versie 7.4.1


De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

BGP is een gestandaardiseerd pad-vector routingprotocol (EGP) voor Exterior Gateway Protocol (BGP) dat schaalbaarheid, flexibiliteit en netwerkstabiliteit biedt. De BGP-sessie tussen twee peers met hetzelfde Autonomous System (AS) wordt Internal BGP (iBGP) genoemd. Een BGP-sessie tussen twee peers met verschillende Autonomous Systems (AS) wordt Externe BGP (eBGP) genoemd.

Meestal wordt de peer-relatie ingesteld met het IP-adres van de interface die het dichtst bij de peer staat, maar het gebruik van een Loopback-interface om de BGP-sessie op te zetten is nuttig omdat het de BGP-sessie niet omlaag brengt wanneer er meerdere paden zijn tussen BGP-peers.

 Opmerking: Het proces beschrijft het gebruik van een Loopback voor een eBGP-peer, maar het is hetzelfde proces voor een iBGP-peer, zodat het als referentie kan worden gebruikt.

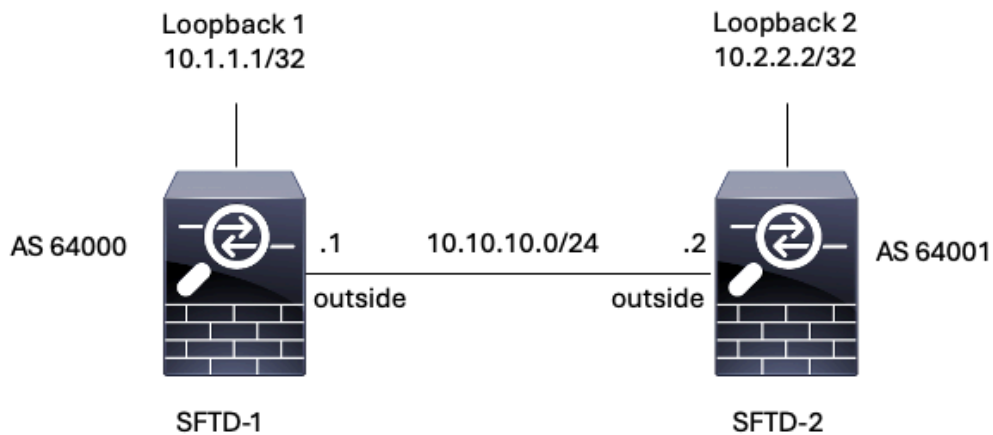
eBGP-configuratie met een terugkoppelingsinterface

Scenario

In deze configuratie heeft Firewall SFTD-1 een Loopback-interface met het IP-adres 10.1.1.1/32 en het AS-64000, heeft de Firewall SFTD-2 een Loopback-interface met het IP-adres 10.2.2.2/32 en het AS-64001. Beide firewalls gebruiken hun buiteninterface om de Loopback-interface van de andere firewall te bereiken (in dit scenario is de buiteninterface op beide firewalls vooraf geconfigureerd).

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Afbeelding 1. Schema van het scenario

Terugbelconfiguratie

Stap 1. Klik op Apparaten > Apparaatbeheer en selecteer vervolgens het apparaat waarop u de terugbelverbinding wilt configureren.

Stap 2. Klik op Interfaces > Alle interfaces.

Stap 3. Klik op 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	

Afbeelding 2. Interfaceloopback toevoegen

Stap 4. In de Algemene sectie, vorm de naam van Loopback, controleer het Toegelaten vakje, en vorm Loopback ID.

Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Afbeelding 3. Basisconfiguratie van loopback-interface

Stap 5. Selecteer in het gedeelte IPv4 de optie Statische IP gebruiken in het gedeelte IP-type, configureer de loopback-IP en klik vervolgens op OK om de wijzigingen op te slaan.

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

Afbeelding 4. Configuratie van IP-adres voor terugbellen

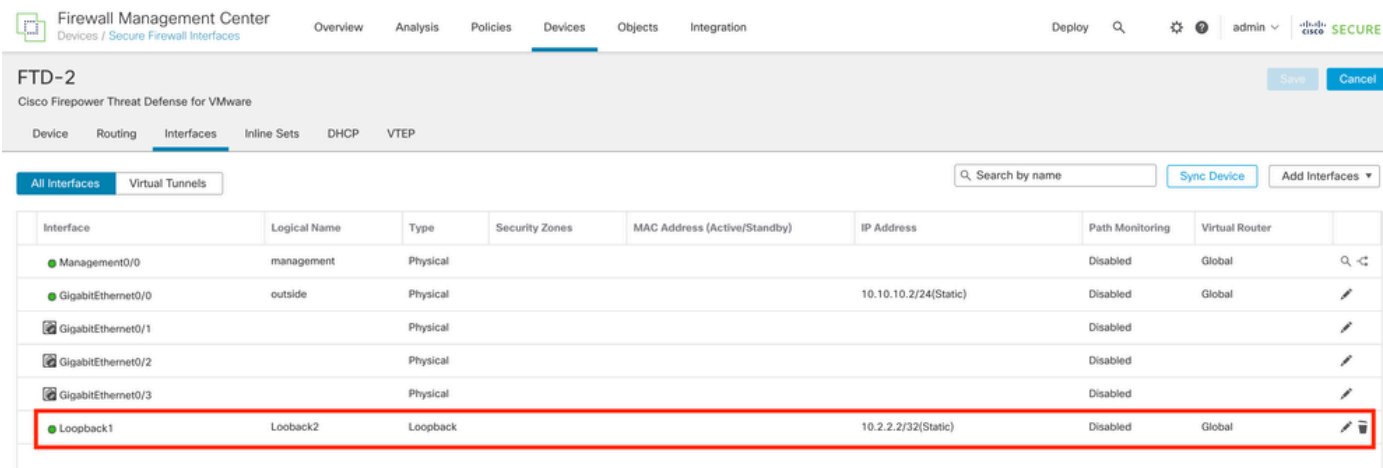
Stap 6. Klik op Save (Opslaan).

The screenshot shows the Firewall Management Center interface for a device named FTD-1. The 'Interfaces' tab is selected, and the 'Loopback1' interface is highlighted. The configuration for 'Loopback1' is shown in the table below:

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	✎ 🗑

Afbeelding 5. De configuratie van de Loopback-interface opslaan

Stap 7. Herhaal het proces met de tweede firewall.



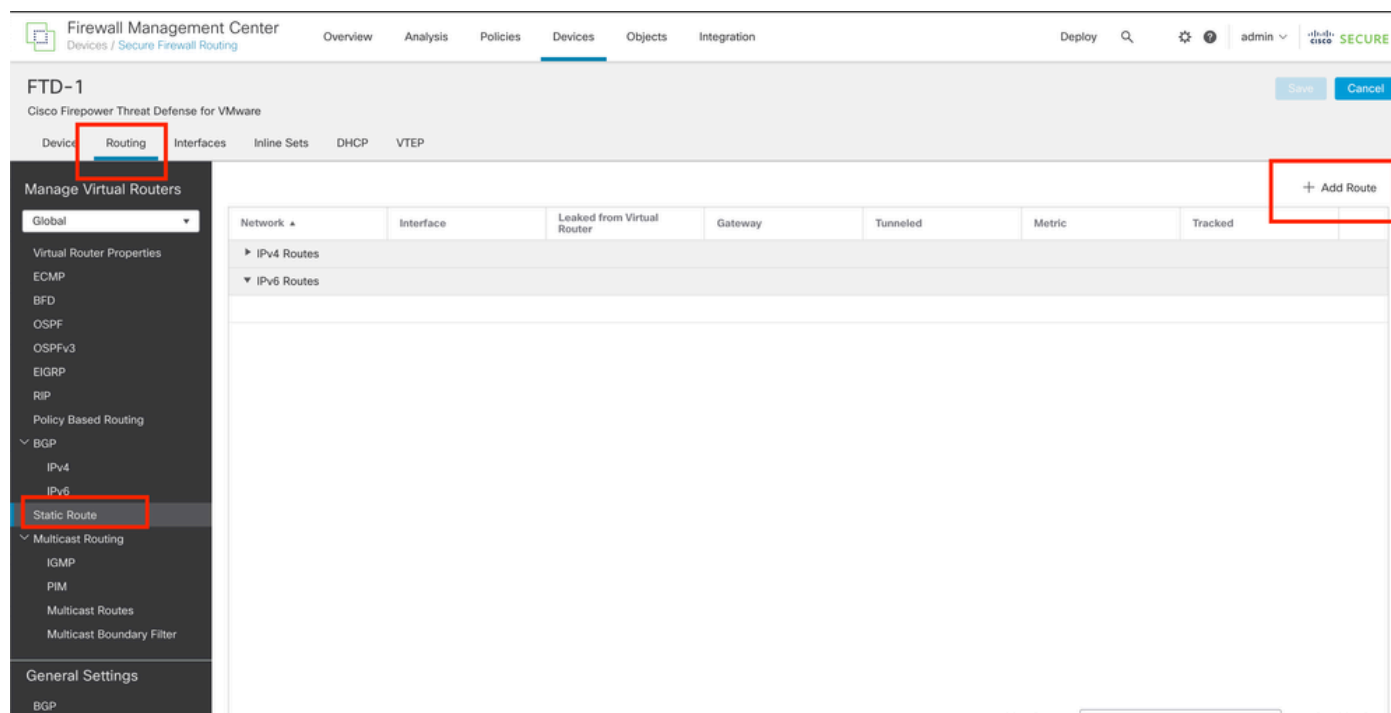
Afbeelding 6. Configuratie van Loopback-interface op peer

Statische routeconfiguratie

Een statische route moet worden geconfigureerd om ervoor te zorgen dat het externe peer-adres (Loopback) dat wordt gebruikt voor peering bereikbaar is via de gewenste interface.

Stap 1. Klik op Apparaten > Apparaatbeheer en selecteer vervolgens het apparaat dat u de statische route wilt configureren.

Stap 2. Klik op Routing > Virtual Routers beheren > Static Route en klik vervolgens op Add Route.



Afbeelding 7. Nieuwe statische route toevoegen

Stap 3. Controleer IPv4 op Type. Selecteer de fysieke interface die wordt gebruikt om de Loopback van de externe peer in de interfaceoptie te bereiken en specificeer vervolgens de volgende hop om de Loopback in de sectie Gateway te bereiken.

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

Afbeelding 8. Statische routeconfiguratie

Stap 4. Klik op het pictogram (+) naast de sectie Beschikbare netwerken.

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

Afbeelding 9. Nieuw netwerkobject toevoegen

Stap 5. Configureer een naam voor referentie en het IP van de Dekking van de externe peer en Sla op.

New Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

Afbeelding 10. Netwerkbestemming in de statische route configureren

Stap 6. Zoek het nieuwe object dat in de zoekbalk is gemaakt, selecteer het, klik vervolgens op Toevoegen en klik vervolgens op 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

Afbeelding 11. Configureer volgende hop in statische route

Stap 7. Klik op Save (Opslaan).

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

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
Loopback-FTD2	outside	Global	10.10.10.2	false	1	
IPv6 Routes						

You have unsaved changes Save Cancel

Afbeelding 12. De configuratie van de statische routeinterface opslaan

Stap 8. Herhaal het proces met de tweede firewall.

FTD-2
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

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
Loopback-FTD1	outside	Global	10.10.10.1	false	1	
IPv6 Routes						

Save Cancel

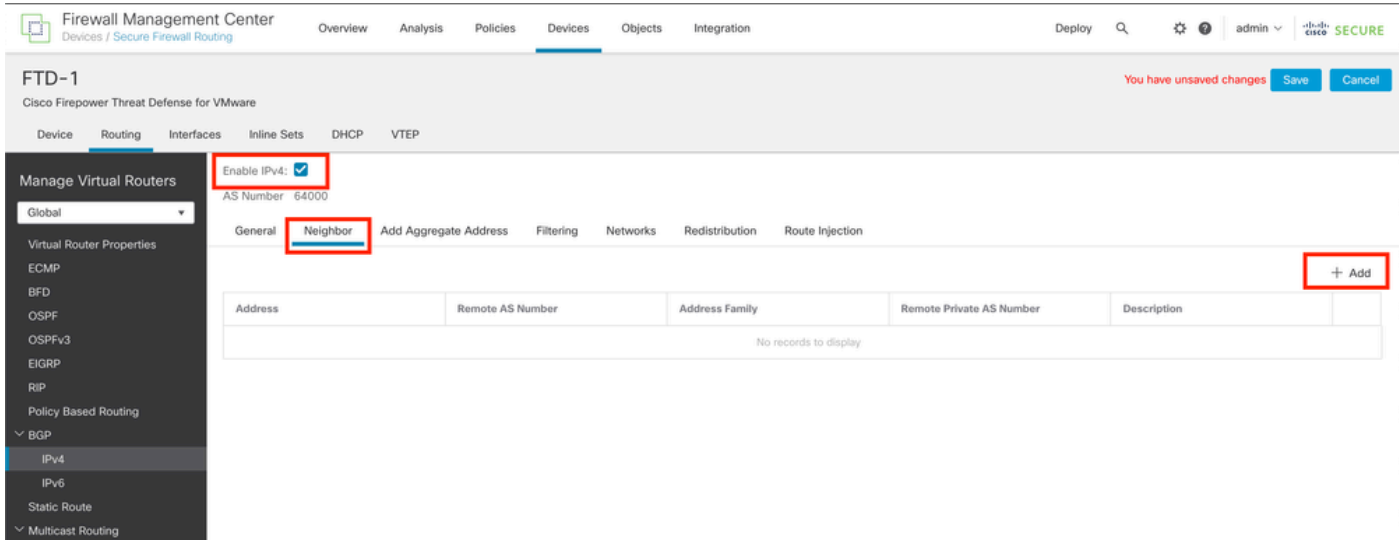
Afbeelding 13. Statische route op peer configureren

BGP-configuratie

Stap 1. Klik op Apparaten > Apparaatbeheer en selecteer het apparaat dat u BGP wilt inschakelen.

Stap 2. Klik op Routing > Virtual Routers beheren > Algemene instellingen en klik vervolgens op BGP.

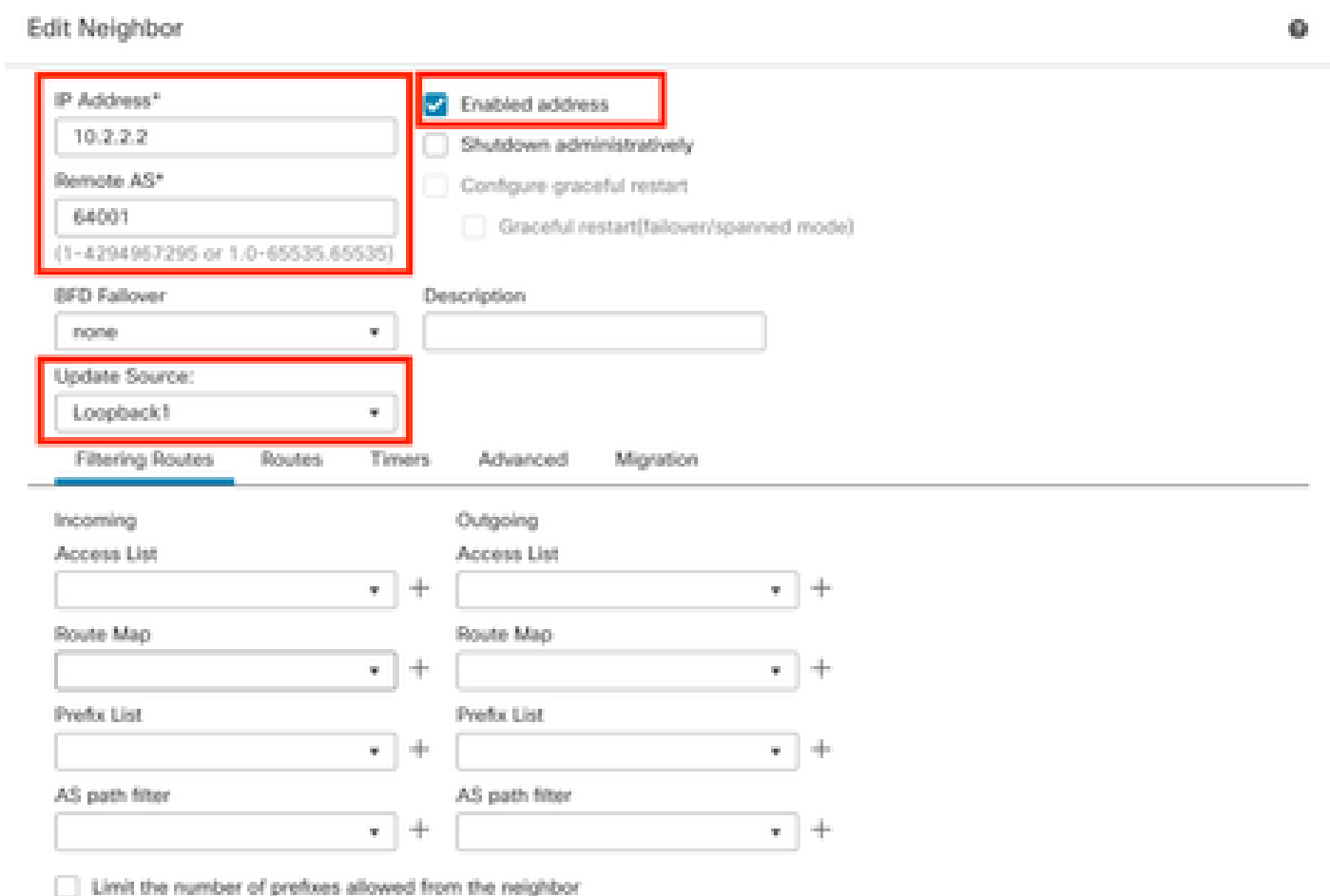
Stap 3. Controleer het vakje BGP inschakelen en configureer vervolgens de lokale AS van de firewall in het gedeelte AS-nummer.




Afbeelding 16. Voeg een nieuwe BGP-peer toe

Stap 7. Configureer het IP-adres van de externe peer in de sectie IP-adres, configureer vervolgens het AS van de externe peer in de sectie Remote AS en controleer het vakje Adres inschakelen.

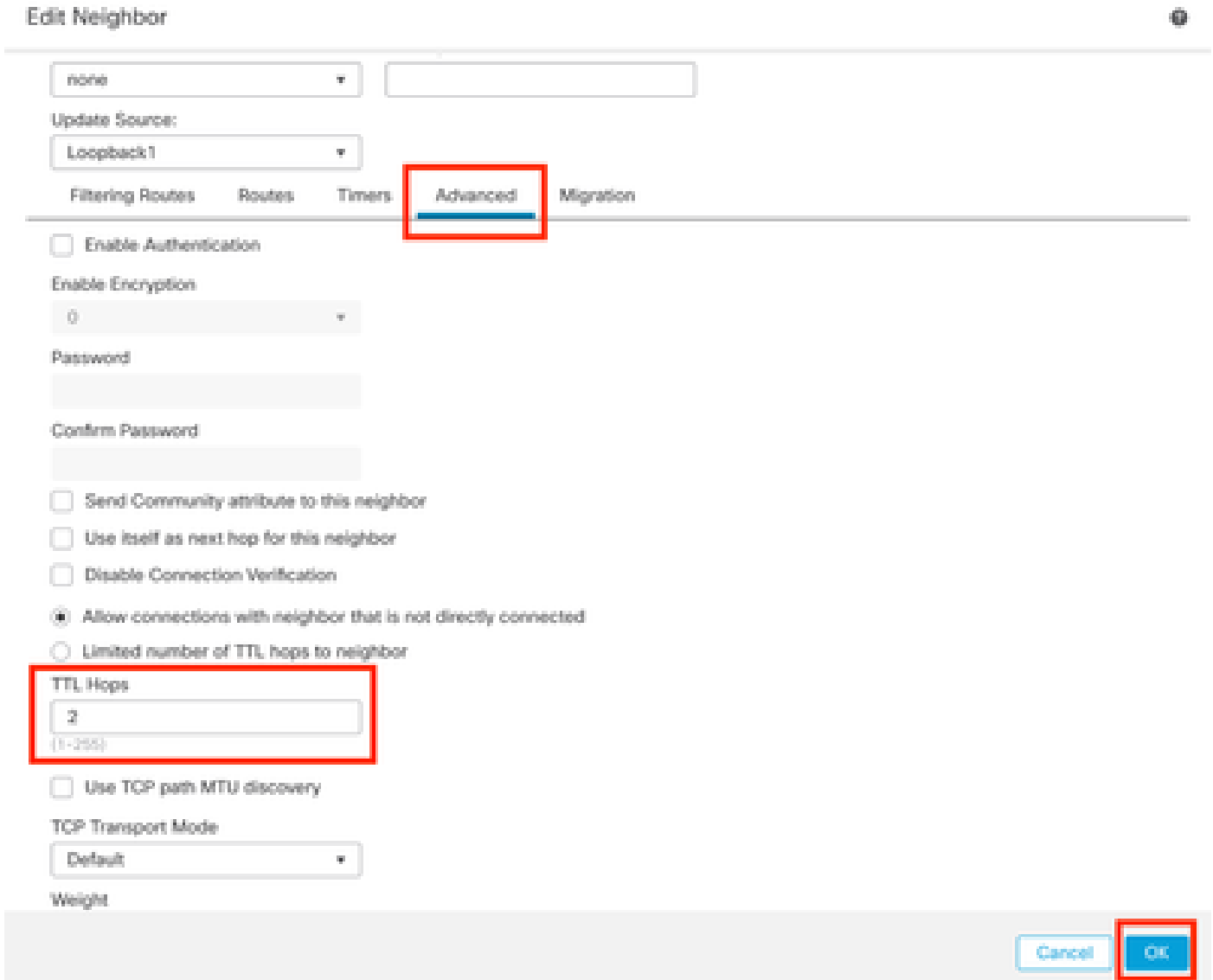
Stap 8. Selecteer de lokale interface Loopback in de sectie Update Source.



Afbeelding 17. Basis BGP-peer parameters

 **Opmerking:** De Update Source optie maakt het buurupdate-bron commando, gebruikt om elke operationele interface (inclusief Loopbacks) toe te staan. Deze opdracht kan worden gespecificeerd om TCP-verbindingen tot stand te brengen.

Stap 9. Klik op Advanced, configureer vervolgens nummer 2 in de optie TTL Hops en klik op 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

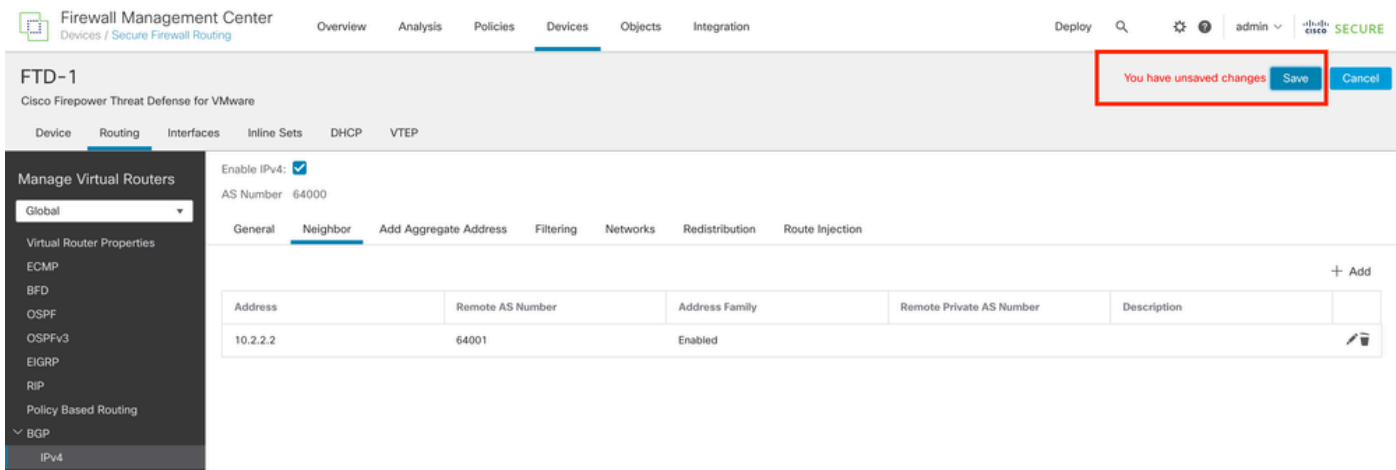
Weight

Cancel OK

Afbeelding 18. Het hopnummer van TTL's configureren

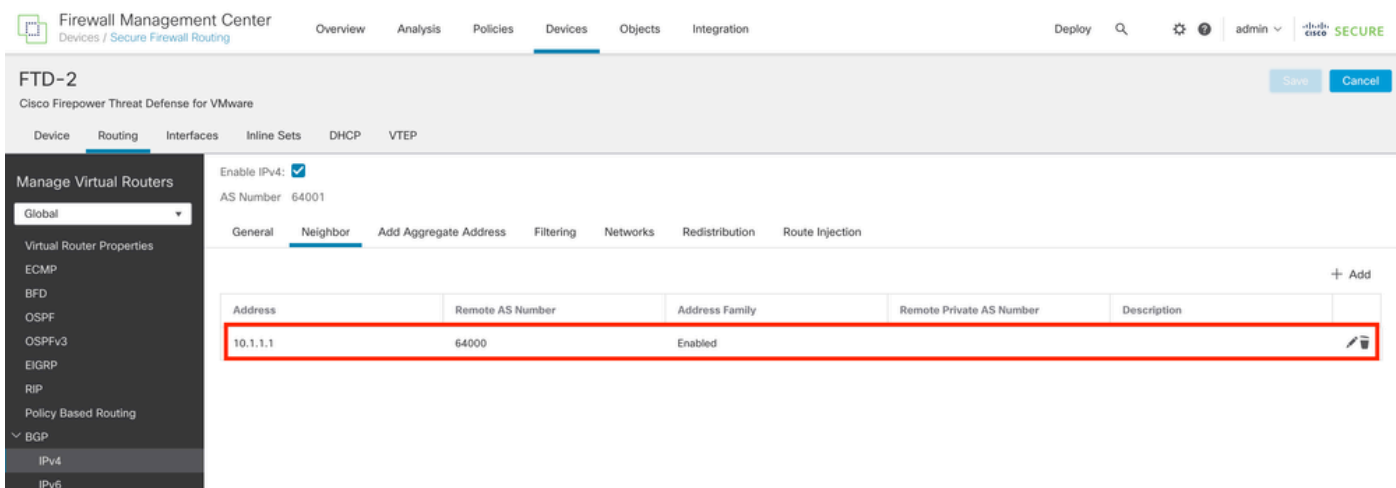
 **Opmerking:** de optie TTL Hops schakelt de ebgp-multihop-opdracht in, die wordt gebruikt om de TTL-waarde te wijzigen, zodat het pakket de externe BGP-peer kan bereiken die niet direct verbonden is of een andere interface heeft dan de direct verbonden interface.

Stap 10. Klik op Opslaan en voer de wijzigingen in.



Afbeelding 19. De BGP-configuratie opslaan

Stap 11. Herhaal het proces met de tweede firewall.



Afbeelding 20. BGP op peer configureren

Verifiëren

Stap 1. Controleer de Loopback- en statische routeconfiguratie en controleer vervolgens de connectiviteit tussen BGP-peers met een ping-test.

toon in werking stellen-config interface interface_name

toon in werking stelt -in werking stellen-configuratieinterface

toon destinatie_ip

SFTD-1	SFTD-2
tonen in werking stelt -in werking stellen-configuratieinterface Loopback1	tonen in werking stelt -in werking stellen-configuratieinterface Loopback1
interface-loopback1	interface-loopback1

naam Loopback1 IP-adres 10.1.1.1 255.255.255.255 toon in werking stelt -in werking stellen- configuratieroute route buiten 10.2.2.2 255.255.255.255 10.10.10.2 1 ping 10.2.2.2 Verzend 5, 100-byte ICMP Echos naar 10.2.2.2, tijd is 2 seconden: !!!! Succespercentage is 100 procent (5/5), ronde- trip min/avg/max = 1/1/1 ms	nameif Looback2 IP-adres 10.2.2.2 255.255.255.255 toon in werking stelt -in werking stellen- configuratieroute route buiten 10.1.1.1 255.255.255.255 10.10.10.1 1 ping 10.1.1.1 Verzend 5, 100-byte ICMP Echos naar 10.1.1.1, tijd is 2 seconden: !!!! Succespercentage is 100 procent (5/5), ronde- trip min/avg/max = 1/1/1 ms
--	---

Stap 2. Controleer de BGP-configuratie en zorg er vervolgens voor dat de BGP-peer is ingesteld.

tonen in werking stelt -in werking stellen-configuratierouter bgp

Toon bgp burens

bgp-overzicht tonen

SFTD-1	SFTD-2
tonen in werking stelt -in werking stellen- configuratierouter bgp router bgp 64000 bgp log-buurwijzigingen bgp router-id vrf automatisch toewijzen IPv4-unicast voor adresfamilie buur 10.2.2.2 op afstand 64001 buurman 10.2.2.2 bgp-multihop 2 buur 10.2.2.2 transportpad-mtu-discovery uitschakelen buur 10.2.2.2 update-bron Loopback1	tonen in werking stelt -in werking stellen- configuratierouter bgp router bgp 64001 bgp log-buurwijzigingen bgp router-id vrf automatisch toewijzen IPv4-unicast voor adresfamilie buur 10.1.1.1 afstandsbediening als 64000 buurman 10.1.1.1 bgp-multihop 2 buur 10.1.1.1 transportpad-mtu-discovery uitschakelen buur 10.1.1.1 update-bron Looback2

<p>buur 10.2.2.2 activeren</p> <p>geen automatische samenvatting</p> <p>geen synchronisatie</p> <p>exit-address-family</p> <p>!</p> <p>Toon bgp buren i BGP-software</p> <p>BGP-buur is 10.2.2.2, vrf single_vf, extern AS-64001, externe link</p> <p>BGP versie 4, externe router-ID 10.2.2.2</p> <p>BGP-staat = ingesteld, tot 1 d15 uur</p> <p>BGP-tabelversie 7, buurversie 7/0</p> <p>De externe buur van BGP kan tot 2 hop weg zijn.</p> <p>bgp-overzicht tonen</p> <p>BGP-router-id 10.1.1.1, lokaal AS-nummer 64000</p> <p>BGP-tabelversie 7, hoofdrouteringstabel versie 7</p> <p>Neighbour V ASmsgRcvd MSG Verzonden Tb Ver InQ OutQ Up/Down State/PFXRCD</p> <p>10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0</p>	<p>buur 10.1.1.1 activeren</p> <p>geen automatische samenvatting</p> <p>geen synchronisatie</p> <p>exit-address-family</p> <p>!</p> <p>Toon bgp buren i BGP-software</p> <p>BGP-buur is 10.1.1.1, vrf single_vf, extern AS-64000, externe link</p> <p>BGP versie 4, externe router-ID 10.1.1.1</p> <p>BGP-staat = ingesteld, tot 1d16h</p> <p>BGP-tabelversie 1, buurversie 1/0</p> <p>De externe buur van BGP kan tot 2 hop weg zijn.</p> <p>bgp-overzicht tonen</p> <p>BGP-router-id 10.2.2.2, lokaal AS-nummer 64001</p> <p>BGP-tabelversie 1, hoofdrouteringstabel versie 1</p> <p>Neighbour V ASmsgRcvd MSG Verzonden Tb Ver InQ OutQ Up/Down State/PFXRCD</p> <p>10.1.1.4 64000 2168 2173 1 0 0 1d16h 0</p>
---	---

Probleemoplossing

Als u problemen ondervindt tijdens het proces, kunt u dit artikel bekijken:

· [BGP-protocol \(border gateway protocol\)](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.