

Konfigurieren von eBGP mit Loopback-Schnittstelle in sicherer Firewall

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[eBGP-Konfiguration mit Loopback-Schnittstelle](#)

[Szenario](#)

[Netzwerkdiagramm](#)

[Loopback-Konfiguration](#)

[Statische Routenkonfiguration](#)

[BGP-Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie eBGP mithilfe einer Loopback-Schnittstelle auf der Cisco Secure Firewall konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- BGP-Protokoll

Die Loopback-Schnittstellenunterstützung für BGP wurde in Version 7.4.0 eingeführt. Dies ist die erforderliche Mindestversion für Secure Firewall Management Center und Cisco Secure Firepower Threat Defense.

Verwendete Komponenten

- Secure Firewall Management Center für VMware Version 7.4.1
- 2 Cisco Secure Firepower Threat Defense für VMware Version 7.4.1


Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Border Gateway Protocol (BGP) ist ein standardisiertes Pfad-Vektor-Routing-Protokoll für das Exterior Gateway Protocol (EGP), das Skalierbarkeit, Flexibilität und Netzwerkstabilität bietet. Die BGP-Sitzung zwischen zwei Peers mit demselben autonomen System (AS) wird als internes BGP (iBGP) bezeichnet. Eine BGP-Sitzung zwischen zwei Peers mit unterschiedlichen autonomen Systemen (AS) wird als externes BGP (eBGP) bezeichnet.

In der Regel wird die Peer-Beziehung mit der IP-Adresse der Schnittstelle hergestellt, die dem Peer am nächsten ist. Die Verwendung einer Loopback-Schnittstelle zum Einrichten der BGP-Sitzung ist jedoch sinnvoll, da die BGP-Sitzung nicht deaktiviert wird, wenn mehrere Pfade zwischen BGP-Peers vorhanden sind.

 Hinweis: Der Prozess beschreibt die Verwendung eines Loopbacks für einen eBGP-Peer, ist jedoch der gleiche Prozess für einen iBGP-Peer und kann daher als Referenz verwendet werden.

eBGP-Konfiguration mit Loopback-Schnittstelle

Szenario

64000 In dieser Konfiguration besitzt Firewall SFTD-1 eine Loopback-Schnittstelle mit der IP-Adresse 10.1.1.1/32 und die Firewall SFTD-2 eine Loopback-Schnittstelle mit der IP-Adresse 10.2.2.2/32 und der AS 64001. Beide Firewalls verwenden ihre externe Schnittstelle, um die Loopback-Schnittstelle der anderen Firewall zu erreichen (in diesem Szenario ist die externe Schnittstelle auf beiden Firewalls vorkonfiguriert).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

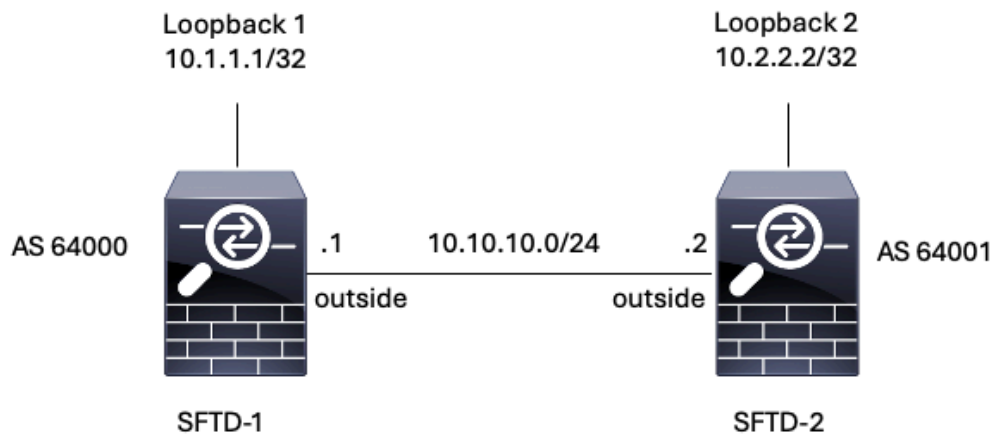


Bild 1. Diagramm des Eszenarios

Loopback-Konfiguration

Schritt 1: Klicken Sie auf Geräte > Geräteverwaltung, und wählen Sie dann das Gerät aus, dem Sie das Loopback konfigurieren möchten.

Schritt 2: Klicken Sie auf Schnittstellen > Alle Schnittstellen.

Schritt 3: Klicken Sie auf Schnittstelle hinzufügen > Loopback-Schnittstelle.

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	

Bild 2. Schnittstellen-Loopback hinzufügen

Schritt 4: Konfigurieren Sie im Abschnitt Allgemein den Namen des Loopbacks, aktivieren Sie das Kontrollkästchen Aktiviert, und konfigurieren Sie die Loopback-ID.

Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Bild 3. Grundlegende Konfiguration der Loopback-Schnittstelle

Schritt 5: Wählen Sie im Abschnitt IPv4 die Option Statische IP verwenden im Abschnitt IP-Typ aus, konfigurieren Sie die Loopback-IP, und klicken Sie dann auf OK, um die Änderungen zu speichern.

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

Abbildung 4: Konfiguration der Loopback-IP-Adresse

Schritt 6: Klicken Sie auf Speichern.

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	✎ 🗑️

Bild 5. Speichern der Loopback-Schnittstellenkonfiguration

Schritt 7. Wiederholen Sie den Vorgang mit der zweiten Firewall.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 cisco **SECURE**

FTD-2
Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

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			10.10.10.2/24(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	✎ 🗑️

Bild 6. Loopback-Schnittstellenkonfiguration auf Peer

Statische Routenkonfiguration

Es muss eine statische Route konfiguriert werden, um sicherzustellen, dass die für das Peering verwendete Remote-Peer-Adresse (Loopback) über die gewünschte Schnittstelle erreichbar ist.

Schritt 1: Klicken Sie auf Geräte > Geräteverwaltung, und wählen Sie dann das Gerät aus, das Sie die statische Route konfigurieren möchten.

Schritt 2: Klicken Sie auf Routing > Virtuelle Router verwalten > Statische Route, und klicken Sie dann auf Route hinzufügen.

Firewall Management Center
Devices / Secure Firewall Routing

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

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

+ Add Route

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

Bild 7. Neue statische Route hinzufügen

Schritt 3: Aktivieren Sie die Option IPv4 für Type (Typ). Wählen Sie in der Option Interface (Schnittstelle) die physische Schnittstelle aus, über die das Loopback des Remote-Peers erreicht wird, und geben Sie dann den nächsten Hop an, über den das Loopback auf dem Gateway-Abschnitt erreicht werden soll.

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

Bild 8. Statische Routenkonfiguration

Schritt 4: Klicken Sie auf das Symbol (+) neben dem Abschnitt "Verfügbares Netzwerk".

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

Bild 9. Neues Netzwerkobjekt hinzufügen

Schritt 5: Konfigurieren Sie einen Referenznamen und die IP-Adresse des Loobacks des Remote-Peers, und speichern Sie.

New Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

Bild 10. Konfigurieren des Netzwerkziels in der statischen Route

Schritt 6: Suchen Sie das neue Objekt, das in der Suchleiste erstellt wurde, wählen Sie es aus, klicken Sie dann auf Hinzufügen und dann auf 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

Bild 11. Next-Hop in statischer Route konfigurieren

Schritt 7. Klicken Sie auf Speichern.

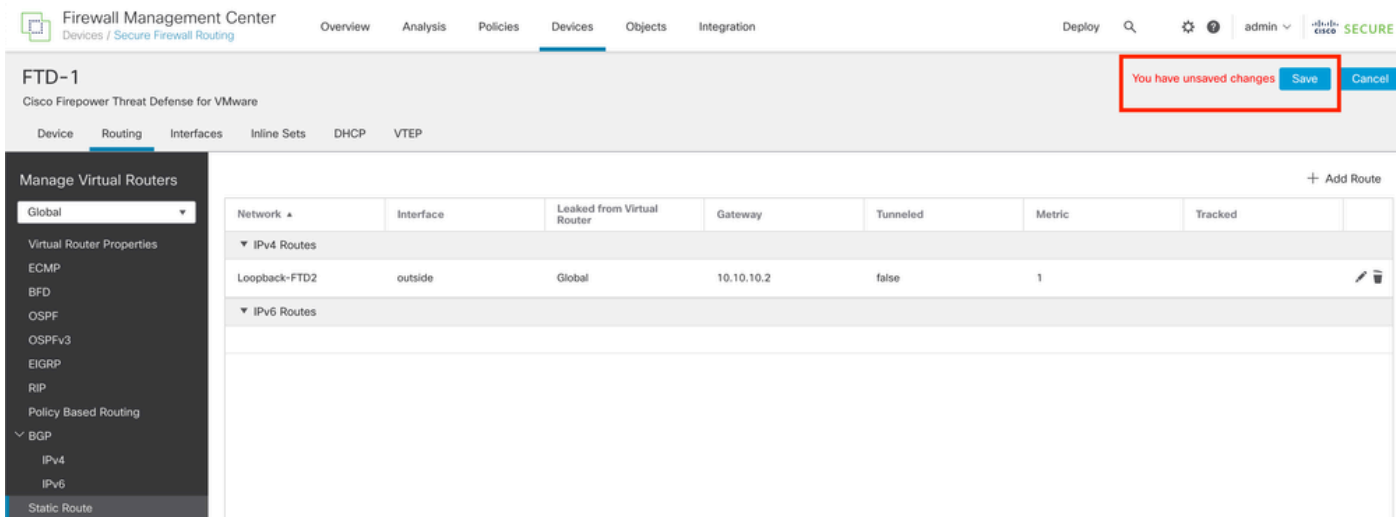


Bild 12. Speichern der Konfiguration der statischen Routenschnittstelle

Schritt 8: Wiederholen Sie den Vorgang mit der zweiten Firewall.

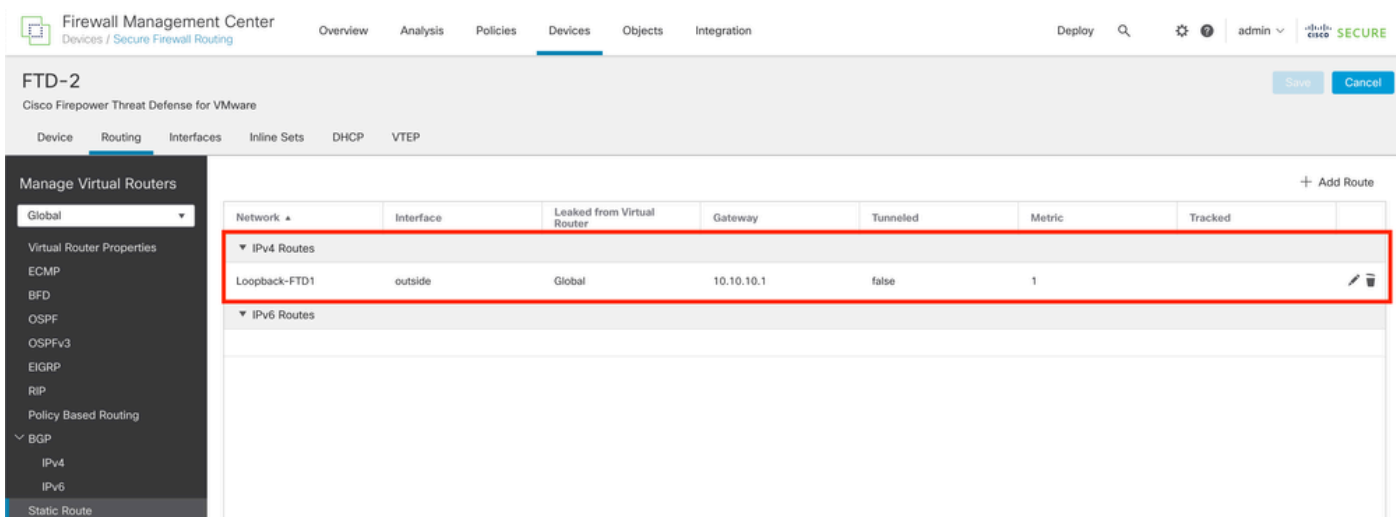


Bild 13. Statische Route auf Peer konfigurieren

BGP-Konfiguration

Schritt 1: Klicken Sie auf Devices > Device Management (Geräte > Geräteverwaltung), und wählen Sie das Gerät aus, das BGP aktivieren soll.

Schritt 2: Klicken Sie auf Routing > Virtuelle Router verwalten > Allgemeine Einstellungen, und klicken Sie dann auf BGP.

Schritt 3: Aktivieren Sie das Kontrollkästchen Enable BGP (BGP aktivieren), und konfigurieren Sie dann das lokale AS der Firewall im Abschnitt mit der AS-Nummer.

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

Scanning Interval	60
Number of AS numbers in AS_PATH attribute of received routes	None
Log Neighbor Changes	Yes
Use TCP path MTU discovery	Yes
Reset session upon failover	Yes
Enforce the first AS is peer's AS for EBGp routes	Yes
Use dot notation for AS number	No
Aggregate Timer	30

Neighbor Timers

Keepalive Interval	
Hold time	
Min hold time	

Next Hop

Address tracking	
Delay interval	

Graceful Restart (use in f...)

Graceful Restart	
Restart time	

Best Path Selection

Default local preference	100
--------------------------	-----

Bild 14. BGP global aktivieren

Schritt 4: Speichern Sie die Änderungen, indem Sie auf die Schaltfläche Speichern klicken.

Firewall Management Center
Devices / Secure Firewall Routing

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

Manage Virtual Routers
Global

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

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

Scanning Interval	60
Number of AS numbers in AS_PATH attribute of received routes	None
Log Neighbor Changes	Yes
Use TCP path MTU discovery	Yes

Neighbor Timers

Keepalive Interval	60
Hold time	180
Min hold time	0

Best Path Selection

Default local preference	100
--------------------------	-----

You have unsaved changes Save Cancel

Bild 15. Speichern der BGP-Aktivierungsänderung

Schritt 5: Gehen Sie im Abschnitt Manage Virtual Routers (Virtuelle Router verwalten) zur BGP-Option, und klicken Sie dann auf IPv4.

Schritt 6: Aktivieren Sie das Kontrollkästchen IPv4 aktivieren, klicken Sie dann auf Neighbor und dann auf + Hinzufügen.

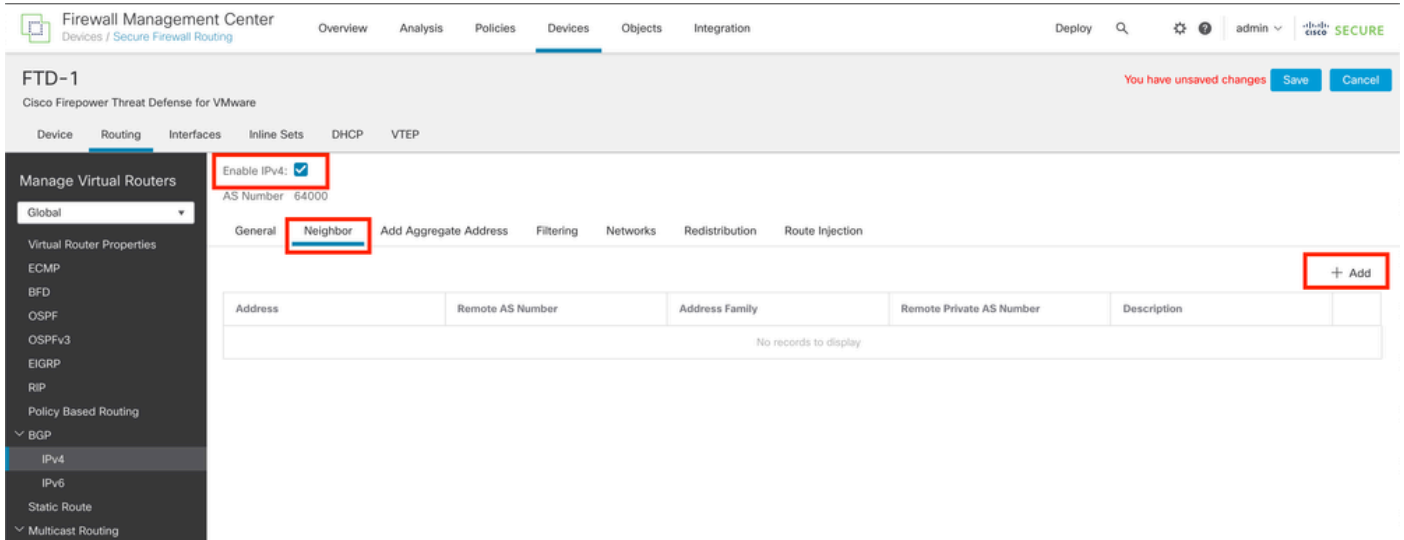


Bild 16. Neuen BGP-Peer hinzufügen

Schritt 7. Konfigurieren Sie die IP-Adresse des Remote-Peers im Abschnitt "IP Address" (IP-Adresse), konfigurieren Sie dann das AS des Remote-Peers im Abschnitt "Remote AS", und aktivieren Sie das Kontrollkästchen Enable address.

Schritt 8: Wählen Sie im Abschnitt Update Source (Update-Quelle) die lokale Schnittstelle Loopback aus.

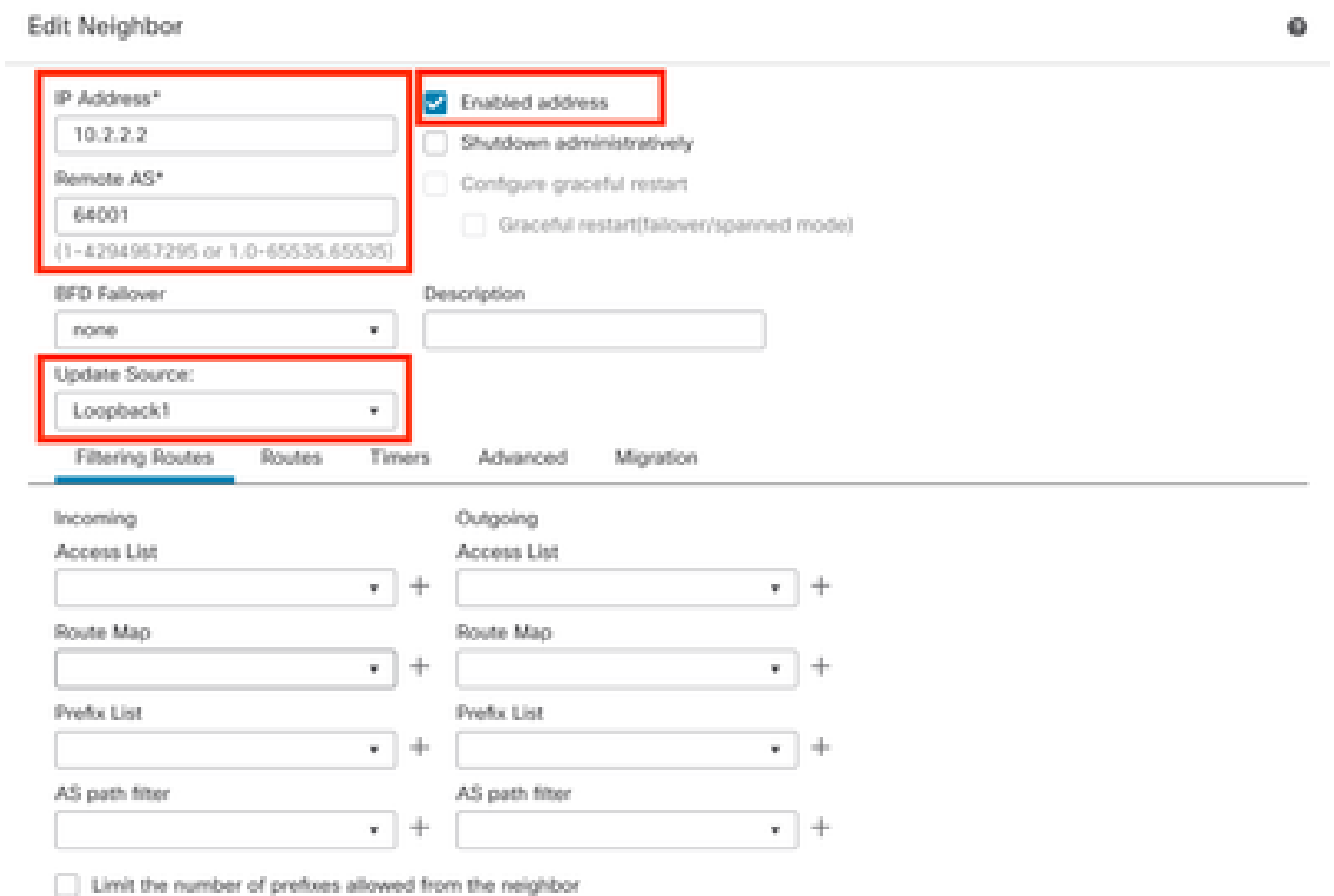

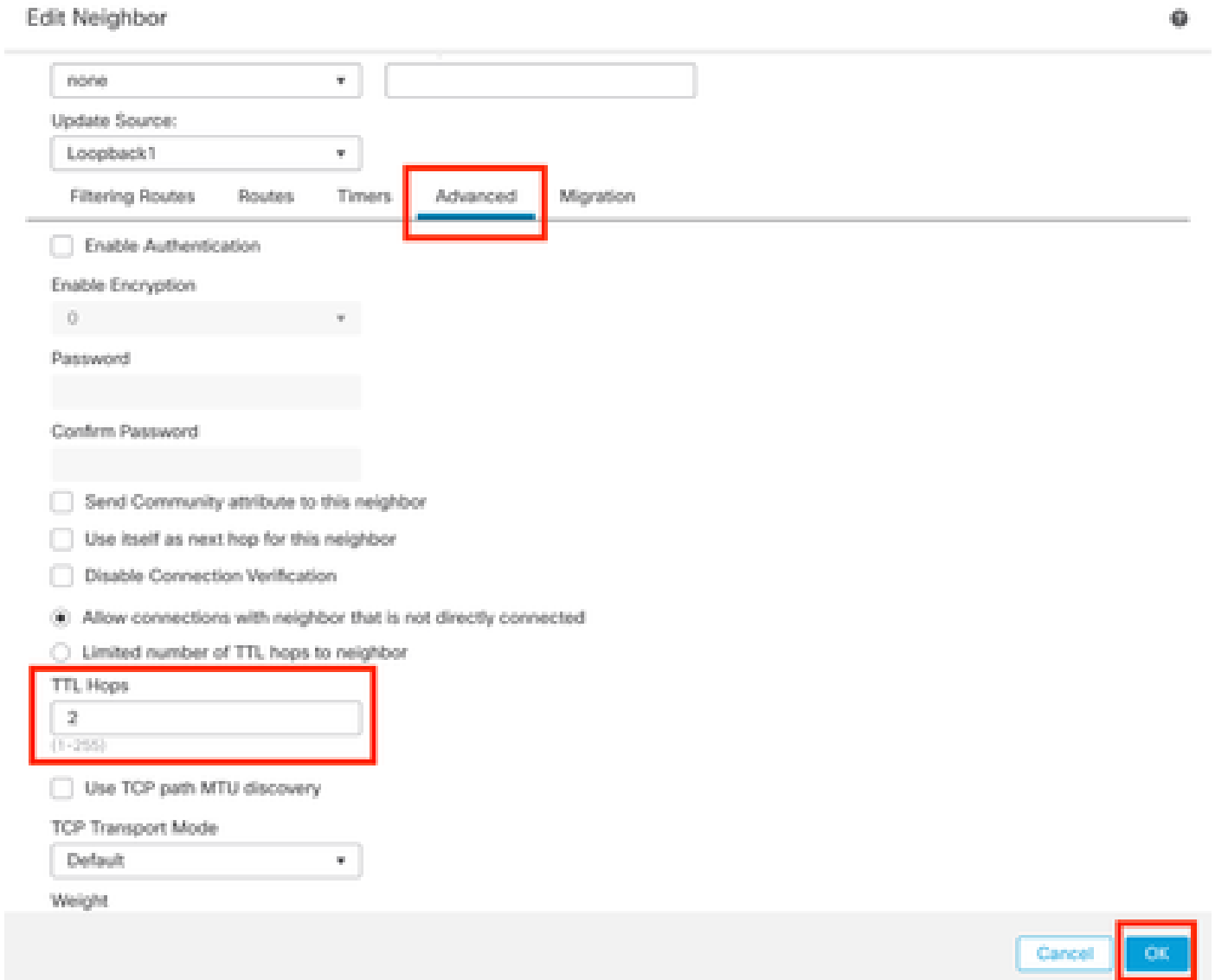


Bild 17. Grundlegende BGP-Peer-Parameter

 Hinweis: Mit der Option Update Source (Update-Quelle) wird der Befehl neighbor update-source aktiviert, der verwendet wird, um eine beliebige betriebliche Schnittstelle (einschließlich Loopbacks) zuzulassen. Mit diesem Befehl können TCP-Verbindungen hergestellt werden.

Schritt 9. Klicken Sie auf Erweitert, konfigurieren Sie die Nummer 2 in der Option TTL-Hops, und klicken Sie auf 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**

Bild 18. Konfigurieren der TTLs-Hop-Nummer

 Hinweis: Die Option TTL Hops aktiviert den Befehl ebgp-multihop, mit dem der TTL-Wert geändert wird, damit das Paket den externen BGP-Peer erreichen kann, der nicht direkt verbunden ist oder über eine andere Schnittstelle als die direkt verbundene Schnittstelle verfügt.

Schritt 10. Klicken Sie auf Speichern und die Änderungen bereitstellen.

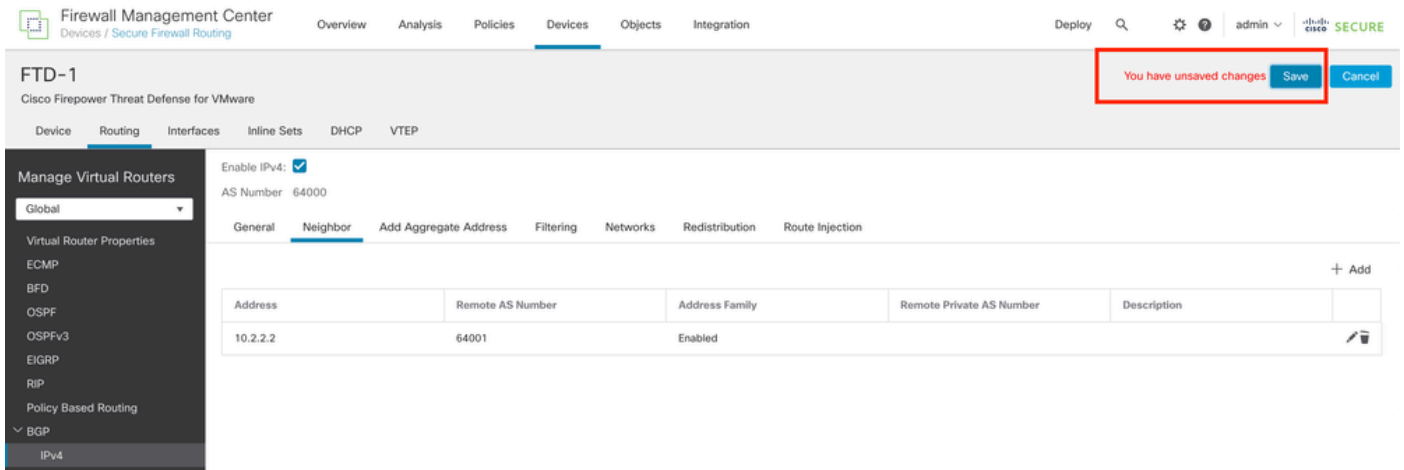


Bild 19. Speichern der BGP-Konfiguration

Schritt 11. Wiederholen Sie den Vorgang mit der zweiten Firewall.

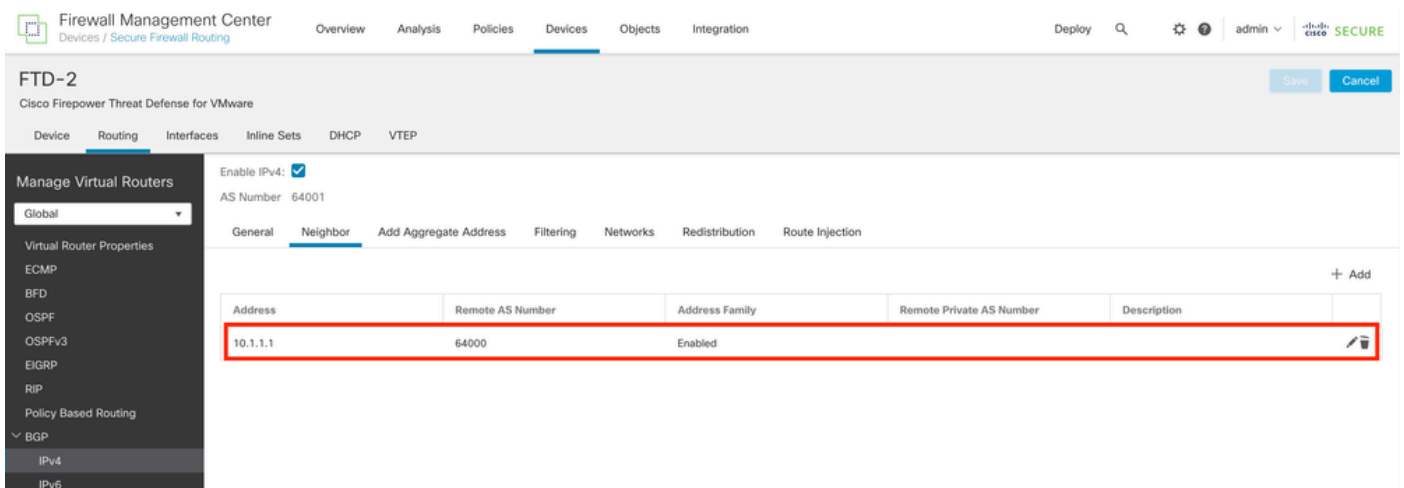


Bild 20. Konfigurieren von BGP auf Peer

Überprüfung

Schritt 1: Überprüfen Sie die Konfiguration von Loopback und statischer Route, und überprüfen Sie anschließend die Verbindung zwischen BGP-Peers mithilfe eines Ping-Tests.

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

```
show running-config-route
```

```
show destination_ip
```

SFTD-1	SFTD-2
show running-config interface Loopback1	show running-config interface Loopback1
Schnittstelle Loopback1	Schnittstelle Loopback1

NameEIF-Loopback1 ip address 10.1.1.1 255.255.255.255 show running-config-route Strecke außerhalb 10.2.2.2 255.255.255.255 10.10.10.2 1 ping 10.2.2.2 Senden von 5 100-Byte-ICMP-Echos an 10.2.2.2, Zeitüberschreitung beträgt 2 Sekunden: !!!! Erfolgsrate: 100 Prozent (5/5), Round-Trip-Wert (min/durchschn/max) = 1/1/1 ms	NameEIF Looback2 ip address 10.2.2.2 255.255.255.255 show running-config-route Strecke außerhalb 10.1.1.1 255.255.255.255 10.10.10.1 1 ping 10.1.1.1 Senden von 5 100-Byte-ICMP-Echos an 10.1.1.1, Zeitüberschreitung beträgt 2 Sekunden: !!!! Erfolgsrate: 100 Prozent (5/5), Round-Trip-Wert (min/durchschn/max) = 1/1/1 ms
---	--

Schritt 2: Überprüfen Sie die BGP-Konfiguration, und stellen Sie dann sicher, dass das BGP-Peering eingerichtet ist.

show running-config router bgp

BGP-Nachbarn anzeigen

BGP-Übersicht anzeigen

SFTD-1	SFTD-2
show running-config router bgp Router BGP 64000 bgp log-neighbor-änderungen bgp router-id vrf automatisch zuweisen 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 Transportpfad-mtu-discovery disable neighbor 10.2.2.2 update-source Loopback1	show running-config router bgp Router BGP 64001 bgp log-neighbor-änderungen bgp router-id vrf automatisch zuweisen 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 Transportpfad-mtu-discovery disable neighbor 10.1.1.1 update-source Looback2

Nachbar 10.2.2.2 aktivieren	Nachbar 10.1.1.1 aktivieren
keine automatische Zusammenfassung	keine automatische Zusammenfassung
keine Synchronisierung	keine Synchronisierung
Ausgangsadressenfamilie	Ausgangsadressenfamilie
!	!
BGP-Nachbarn anzeigen i BGP	BGP-Nachbarn anzeigen i BGP
Der BGP-Nachbar ist 10.2.2.2, vrf single_vf, remote AS 64001, externe Verbindung.	Der BGP-Nachbar ist 10.1.1.1, vrf single_vf, remote AS 64000, externe Verbindung.
BGP-Version 4, Remote-Router-ID 10.2.2.2	BGP-Version 4, Remote-Router-ID 10.1.1.1
BGP-Status = etabliert, bis zu 1 d15 h	BGP-Status = etabliert, bis zu 1 d16 h
BGP-Tabelle Version 7, Nachbarversion 7/0	BGP-Tabelle Version 1, Nachbarversion 1/0
Der externe BGP-Nachbar kann bis zu 2 Hops entfernt sein.	Der externe BGP-Nachbar kann bis zu 2 Hops entfernt sein.
BGP-Übersicht anzeigen	BGP-Übersicht anzeigen
BGP-Router-ID 10.1.1.1, lokale AS-Nummer 64000	BGP-Router-ID 10.2.2.2, lokale AS-Nummer 64001
Version der BGP-Tabelle ist 7, Version 7 der Haupt-Routing-Tabelle	Version der BGP-Tabelle ist 1, Version 1 der Haupt-Routing-Tabelle
Neighbor V AS MsgRcvd MsgSent TbIVer InQ OutQ Up/Down State/PfxRcd	Neighbor V AS MsgRcvd MsgSent TbIVer InQ OutQ Up/Down State/PfxRcd
10.2.2.2 4 64001 2167 2162 7 0 0 1 d15 h 0	10.1.1.1 4 64000 2168 2173 1 0 0 1 d16h 0

Fehlerbehebung

Wenn während des Vorgangs Probleme auftreten, lesen Sie bitte diesen Artikel:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.