

セキュアファイアウォール上のループバックインターフェイスを使用したeBGPの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ループバックインターフェイスを使用したeBGP設定](#)

[シナリオ](#)

[ネットワーク図](#)

[ループバック設定](#)

[スタティックルートの設定](#)

[BGPの設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、Cisco Secure Firewallのループバックインターフェイスを使用してeBGPを設定する方法について説明します。

前提条件

要件

次の項目に関する専門知識があることが推奨されます。

- BGPプロトコル

BGPのループバックインターフェイスのサポートは、バージョン7.4.0で導入されました。これは、Secure Firewall Management CenterおよびCisco Secure Firepower Threat Defenseに必要な最小バージョンです。

使用するコンポーネント

- Secure Firewall Management Center for VMwareバージョン7.4.1
- 2 Cisco Secure Firepower Threat Defense for VMwareバージョン7.4.1


このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ボーダーゲートウェイプロトコル(BGP)は、拡張性、柔軟性、およびネットワークの安定性を提供するExterior Gateway Protocol(EGP)標準パスベクタールーティングプロトコルです。同じ自律システム(AS)を持つ2つのピア間のBGPセッションは、内部BGP(iBGP)と呼ばれます。異なる自律システム(AS)を持つ2つのピア間のBGPセッションは、外部BGP(eBGP)と呼ばれます。

通常、ピア関係は、ピアに最も近いインターフェイスのIPアドレスで確立されますが、BGPセッションを確立するためにループバックインターフェイスを使用することは、BGPピア間に複数のパスが存在する場合にBGPセッションをダウンさせないために有用です。

 注：このプロセスでは、eBGPピアでのループバックの使用について説明します。ただし、iBGPピアでの同じプロセスであるため、参照として使用できます。

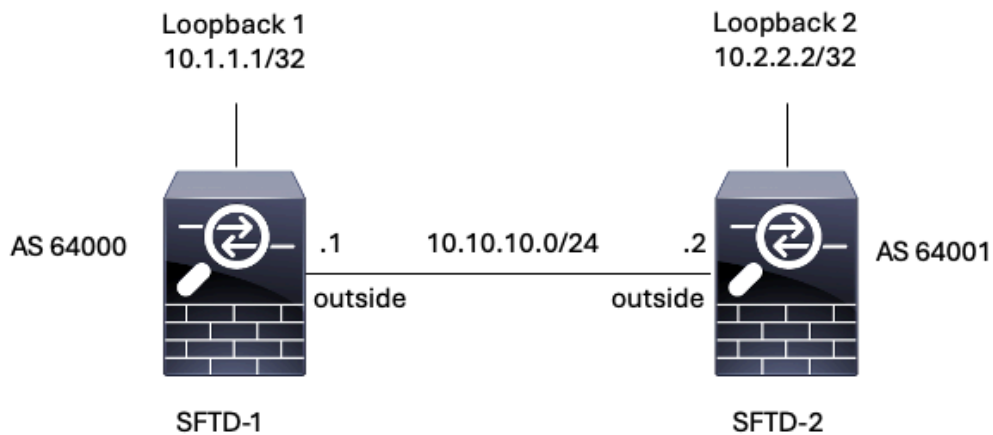
ループバックインターフェイスを使用したeBGP設定

シナリオ

この設定では、ファイアウォールSFTD-1にIPアドレス10.1.1.1/32およびAS 64000のループバックインターフェイスがあり、ファイアウォールSFTD-2にIPアドレス10.2.2.2/32およびAS 64001のループバックインターフェイスがあります。両方のファイアウォールは、他方のファイアウォールのループバックインターフェイスに到達するために外部インターフェイスを使用します(このシナリオでは、両方のファイアウォールで外部インターフェイスが事前に設定されています)。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



画像 1.シナリオ図

ループバック設定

ステップ 1 : Devices > Device Managementの順にクリックし、ループバックを設定するデバイスを選択します。

ステップ 2 : Interfaces > All Interfacesの順にクリックします。

ステップ 3 : Add Interface > Loopback Interfaceの順にクリックします。

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	

画像 2.インターフェイスループバックの追加

ステップ 4 : Generalセクションで、ループバックの名前を設定し、Enabledボックスにチェックマークを入れて、Loopback IDを設定します。

Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

画像 3. 基本的なループバックインターフェイス設定

ステップ 5 : IPv4セクションのIP TypeセクションでUse Static IPオプションを選択し、ループバックIPを設定してから、OKをクリックして変更を保存します。

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

図 4. ループバックIPアドレスの設定

手順 6 : [Save] をクリックします。

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	✎ 🗑️

図 5. ループバックインターフェイス設定の保存

手順 7 : 2つ目のファイアウォールでこのプロセスを繰り返します。

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

図 6.ピアのループバックインターフェイス設定

スタティックルートの設定

スタティックルートは、ピアリングに使用されるリモートピアアドレス（ループバック）が目的のインターフェイスを介して到達可能であることを確認するように設定する必要があります。

ステップ 1 : Devices > Device Management の順にクリックし、スタティックルートを設定するデバイスを選択します。

ステップ2.Routing > Manage Virtual Routers > Static Routeの順にクリックし、Add Routeをクリックします。

図 7.新しいスタティックルートの追加


手順 3 : TypeのIPv4オプションをチェックします。Interfaceオプションでリモートピアのループバックに到達するために使用する物理インターフェイスを選択してから、Gatewayセクションで、ループバックに到達するためのネクストホップを指定します。


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

any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12

Add

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

図 8.スタティックルートの設定

ステップ4. Available Networkセクションの横にあるアイコン(+)をクリックします。

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

図 9.新しいネットワークオブジェクトの追加

ステップ5:参照用に名前を設定し、リモートピアのループバックのIPを設定して、保存します。

New Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

図 10.スタティックルートでのネットワーク宛先の設定

ステップ 6 : 検索バーで作成した新しいオブジェクトを検索して選択し、AddをクリックしてからOKをクリックします。

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

図 11.スタティックルートでのネクストホップの設定

手順 7 : [Save] をクリックします。

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **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

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

+ Add Route

You have unsaved changes **Save** **Cancel**

図 12.スタティックルートインターフェイス設定の保存

ステップ 8 : 2つ目のファイアウォールでこのプロセスを繰り返します。

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

FTD-2

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						

+ Add Route

Save **Cancel**

図 13.ピアでのスタティックルートの設定

BGPの設定

ステップ 1 : Devices > Device Managementの順にクリックし、BGPをイネーブルにするデバイスを選択します。

ステップ2. Routing > Manage Virtual Routers > General Settingsの順にクリックし、BGPをクリックします。

手順 3 : Enable BGPボックスにチェックマークを入れてから、ファイアウォールのローカルASをAS Numberセクションで設定します。

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* (1-4294967295 or 1.0-65535.65535)

Override BGP general settings router-id address:

Router Id

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

図 14.BGPをグローバルに有効にする

ステップ4.Saveボタンをクリックして、変更を保存します。

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ▾ **SECURE**

FTD-1 You have unsaved changes [Save](#) [Cancel](#)

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* (1-4294967295 or 1.0-65535.65535)

Override BGP general settings router-id address:

Router Id

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		

図 15.BGP有効化の変更の保存

ステップ 5 : Manage Virtual Routersセクションで、BGP オプションに移動し、IPv4をクリックします。

手順 6 : Enable IPv4ボックスにチェックマークを入れてから、Neighborをクリックし、+ Addをクリックする。

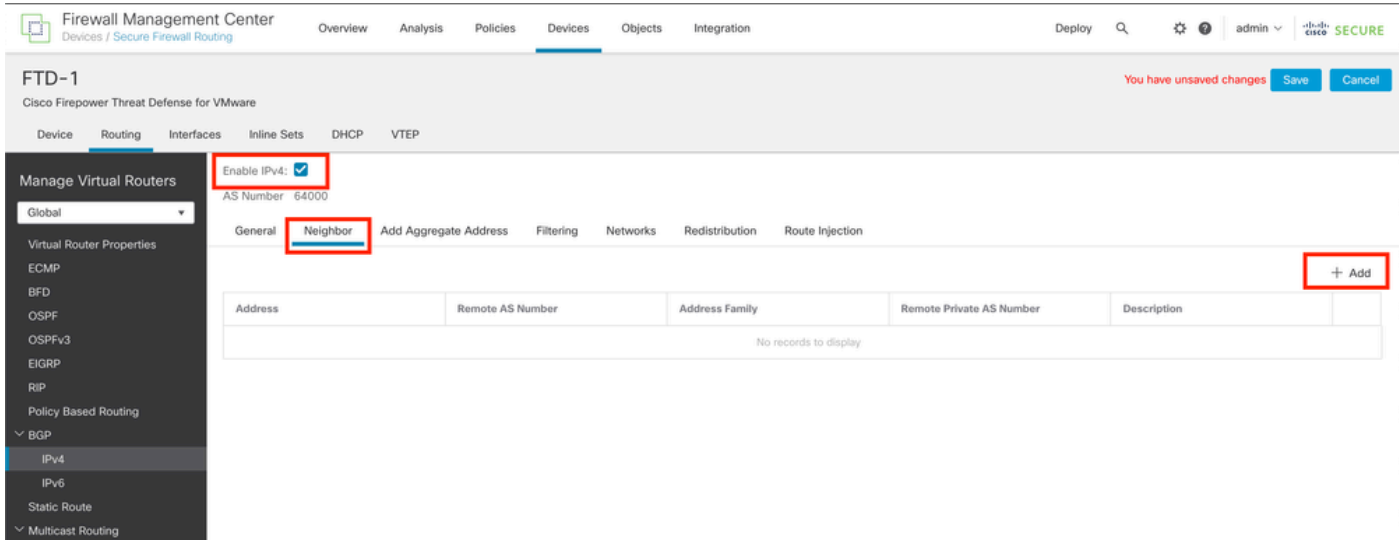


図 16.新しいBGPピアの追加

手順 7 : 「IP Address」 セクションでリモートピアのIPアドレスを設定し、「Remote AS」 セクションでリモートピアのASを設定して、「Enable address」 ボックスにチェックマークを入れます。

ステップ 8 : Update Source セクションでローカルインターフェイスループバックを選択します。

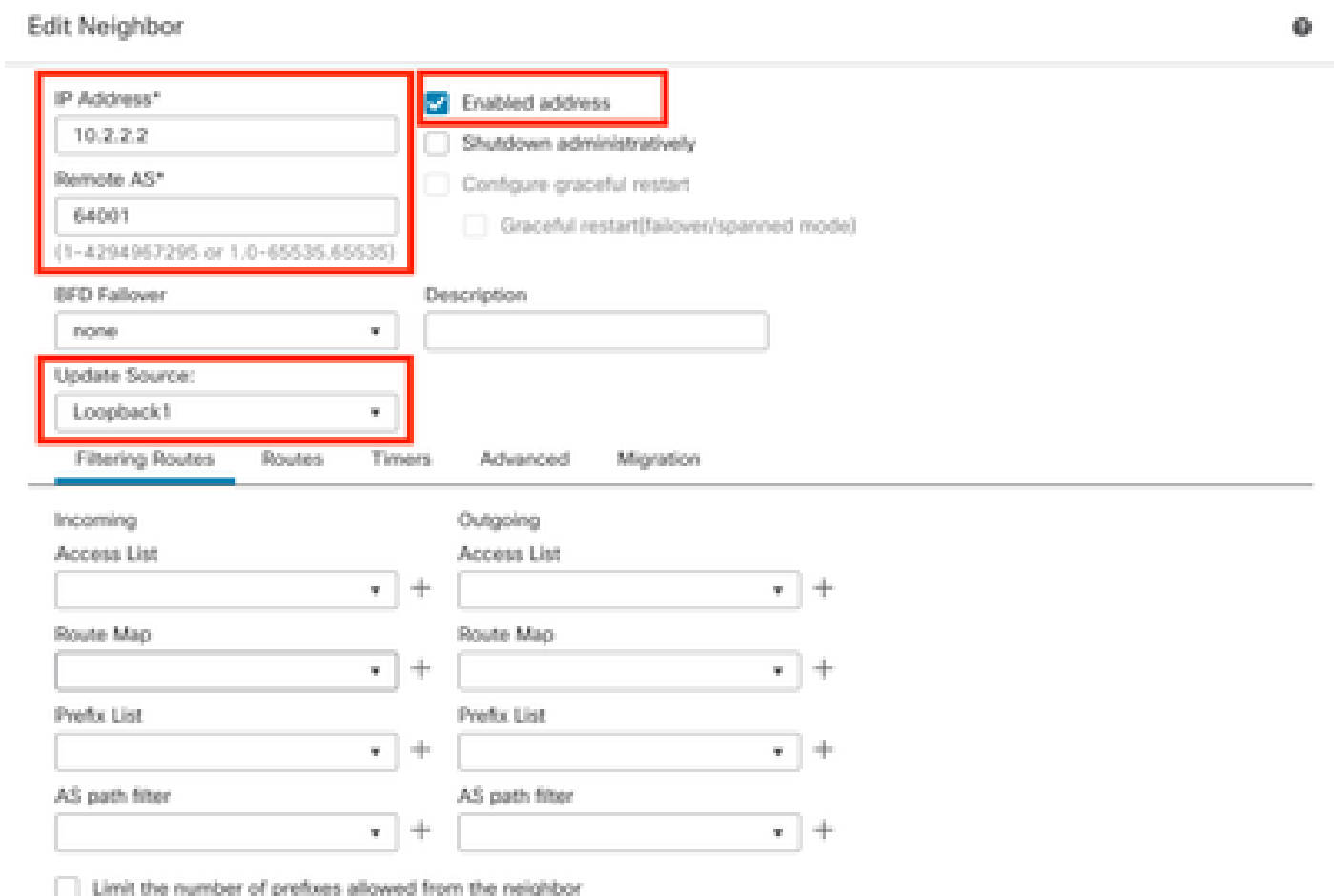

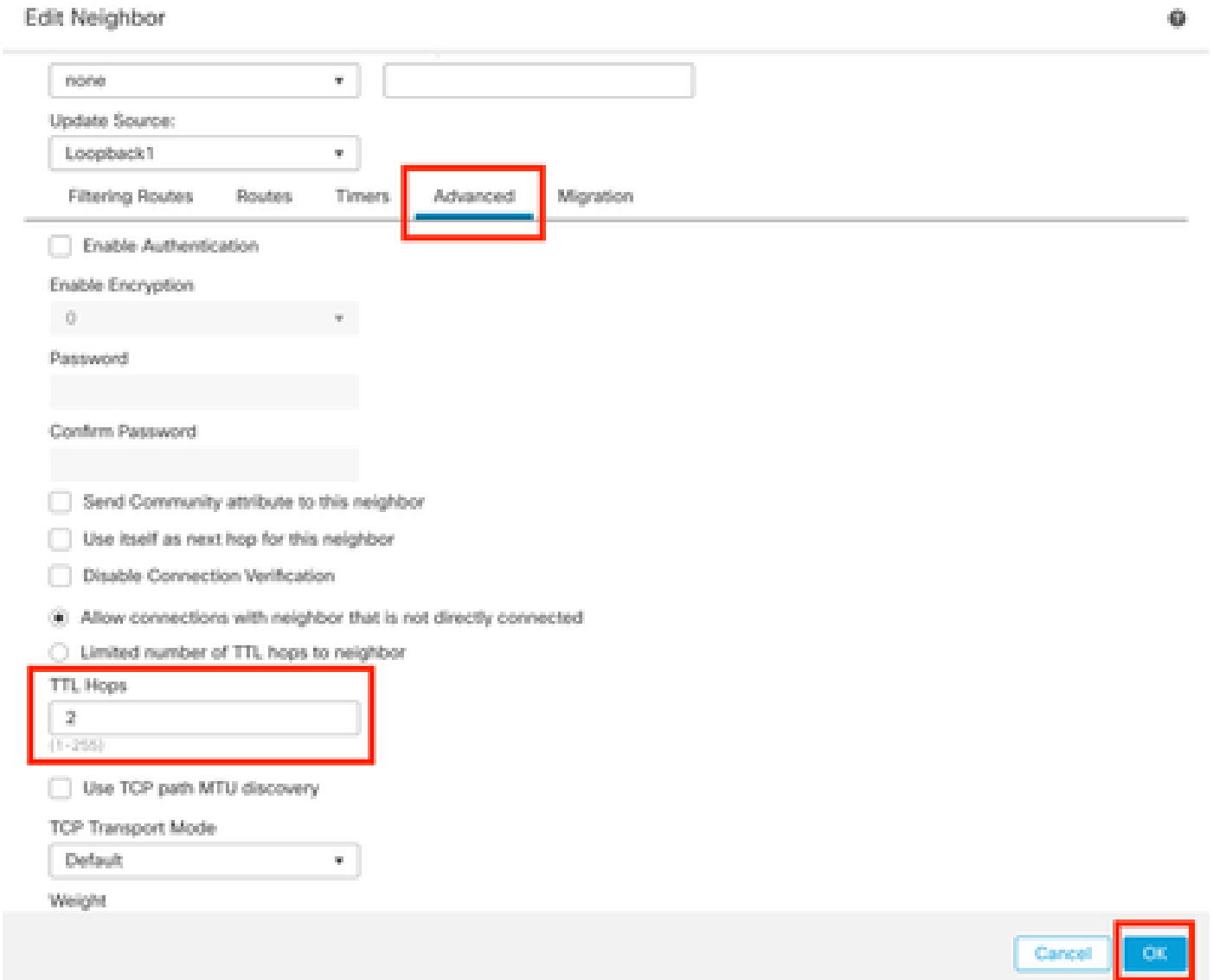


図 17.基本的なBGPピアパラメータ

 注：Update Source オプションにより、neighbor update-source コマンドがイネーブルになり、（ループバックを含む）動作しているすべてのインターフェイスを許可するために使用されます。このコマンドは、TCP接続を確立するために指定できます。

ステップ 9：Advancedをクリックし、TTL Hopsオプションに番号2を設定して、OKをクリックします。



Edit Neighbor

none

Update Source:
Loopback 1

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

図 18. TTLsホップ番号の設定

 注:TTL Hops オプションによりebgp-multihop コマンドがイネーブルになります。このコマンドを使用してTTL値を変更すると、直接接続されていない外部BGPピア、または直接接続されたインターフェイス以外のインターフェイスを持つ外部BGPピアにパケットが到達できるようになります。

ステップ 10：Saveをクリックして、変更を展開します。

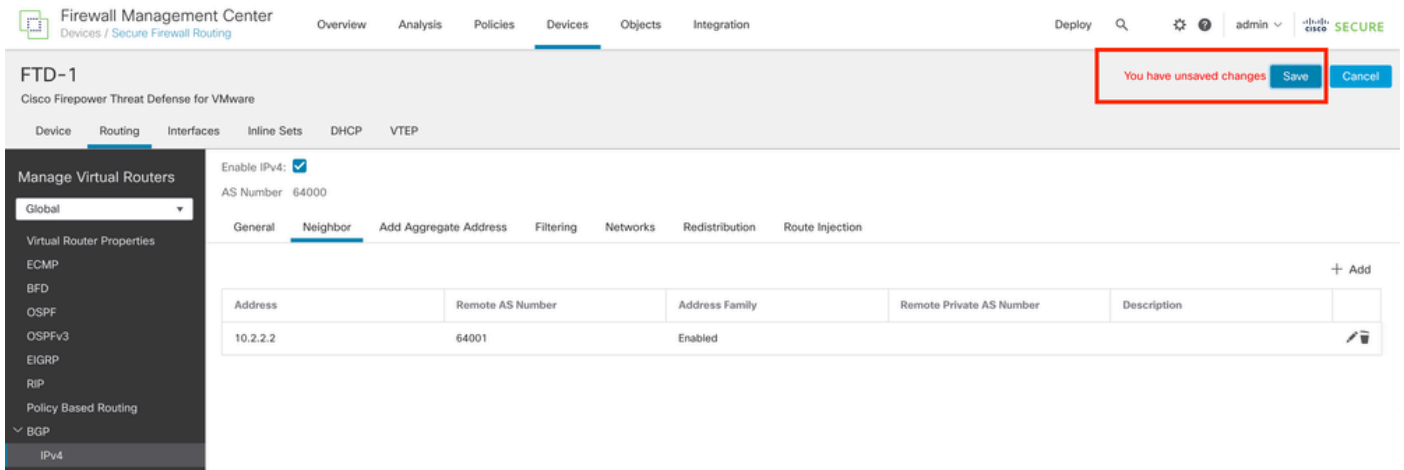


図 19.BGP設定の保存

ステップ 112つ目のファイアウォールでこのプロセスを繰り返します。

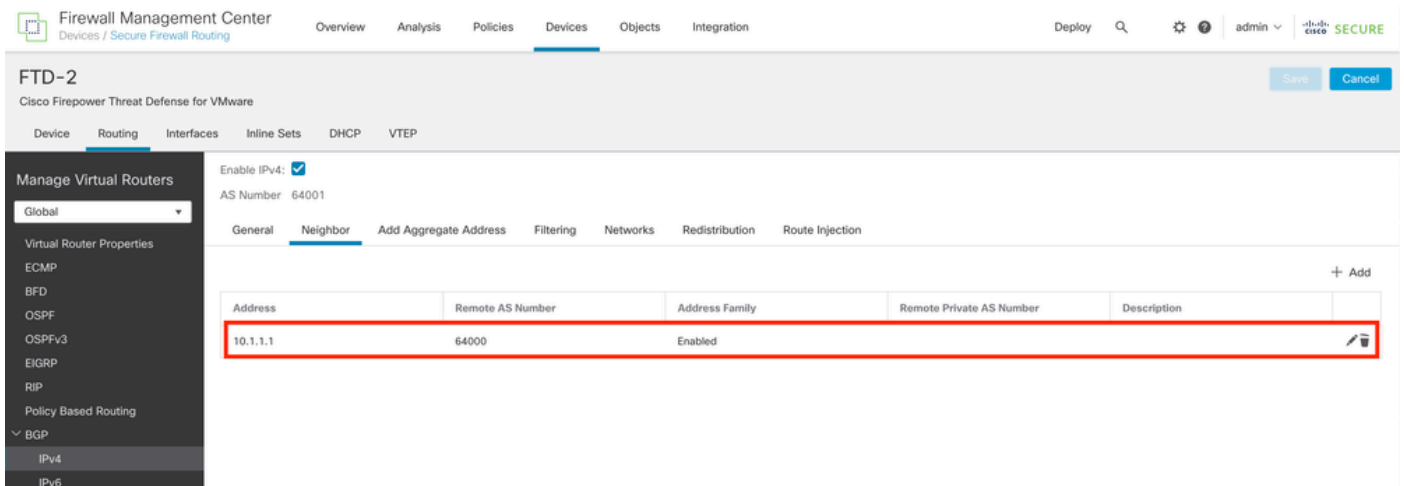


図 20.ピアでのBGPの設定

確認

ステップ 1： ループバックとスタティックルートの設定を確認し、pingテストを使用してBGPピア間の接続を確認します。

show running-config interface interface_name (隠しコマンド)

show running-config route

show destination_ip(宛先IPの表示)

SFTD-1	SFTD-2
show running-config interfaceループバック1 interface Loopback1	show running-config interfaceループバック1 interface Loopback1

<pre> nameifループバック1 ip address 10.1.1.1 255.255.255.255 show running-config route 10.2.2.2 255.255.255.255 10.10.10.2 1以外のル ート 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 10.1.1.1 255.255.255.255 10.10.1.1以外のルー ト 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>
---	--

ステップ 2 : BGP設定を確認し、BGPピアリングが確立されていることを確認します。

show running-config router bgpコマンド

show bgp neighbors (隠しコマンド)

show bgp summary

SFTD-1	SFTD-2
<pre> show running-config router bgpコマンド router bgp 64000 bgp log-neighbor-changes bgp router-id vrf auto-assign (VRF自動割り当て) address-family ipv4 unicast neighbor 10.2.2.2 remote-as 64001 ネイバー10.2.2.2 ebgpマルチホップ2 neighbor 10.2.2.2 transport path-mtu- discoveryの無効化 neighbor 10.2.2.2 update-sourceループバック1 </pre>	<pre> show running-config router bgpコマンド router bgp 64001 bgp log-neighbor-changes bgp router-id vrf auto-assign (VRF自動割り当て) address-family ipv4 unicast neighbor 10.1.1.1 remote-as 64000 ネイバー10.1.1.1 ebgp-multihop 2 neighbor 10.1.1.1 transport path-mtu-discovery disable (ネイバー10.1.1.1 transport path-mtu- discoveryがデイスレーブル) neighbor 10.1.1.1 update-source Looback2 </pre>

<pre>neighbor 10.2.2.2 activate no auto-summary no synchronization exit-address-family !</pre>	<pre>neighbor 10.1.1.1 activate no auto-summary no synchronization exit-address-family !</pre>
<pre>show bgp neighbors (隠しコマンド) i BGP(i BGP)</pre>	<pre>show bgp neighbors (隠しコマンド) i BGP(i BGP)</pre>
<p>BGPネイバーは10.2.2.2、vrf single_vf、リモートAS 64001、外部リンク</p>	<p>BGPネイバーは10.1.1.1、vrf single_vf、リモートAS 64000、外部リンク</p>
<p>BGPバージョン4、リモートルータID 10.2.2.2</p>	<p>BGPバージョン4、リモートルータID 10.1.1.1</p>
<p>BGP状態= Established、アップ(1d15h)</p>	<p>BGP状態= Established、アップ(1d16h用)</p>
<p>BGPテーブルバージョン7、ネイバーバージョン7/0</p>	<p>BGPテーブルバージョン1、ネイバーバージョン1/0</p>
<p>外部BGPネイバーは最大2ホップ離れている可能性があります。</p>	<p>外部BGPネイバーは最大2ホップ離れている可能性があります。</p>
<pre>show bgp summary</pre>	<pre>show bgp summary</pre>
<p>BGP router identifier 10.1.1.1, local AS number 64000</p>	<p>BGP router identifier 10.2.2.2, local AS number 64001</p>
<p>BGPテーブルバージョン7、メインルーティングテーブルバージョン7</p>	<p>BGP table version is 1, main routing table version 1</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 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>

トラブルシューティング

処理中に問題が発生した場合は、次の記事を参照してください。

- Border Gateway Protocol (BGP)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。