

Configurer eBGP avec l'interface de bouclage sur Secure Firewall

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration eBGP avec une interface de bouclage](#)

[Scénario](#)

[Diagramme du réseau](#)

[Configuration de bouclage](#)

[Configuration de route statique](#)

[Configuration BGP](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer eBGP à l'aide d'une interface de bouclage sur le pare-feu sécurisé Cisco.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- protocole BGP

La prise en charge de l'interface de bouclage pour BGP a été introduite dans la version 7.4.0, qui est la version minimale requise pour Secure Firewall Management Center et Cisco Secure Firepower Threat Defense.

Composants utilisés

- Secure Firewall Management Center pour VMware version 7.4.1
- 2 Cisco Secure Firepower Threat Defense pour VMware version 7.4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le protocole BGP (Border Gateway Protocol) est un protocole de routage à vecteur de chemin normalisé EGP (Exterior Gateway Protocol) qui offre évolutivité, flexibilité et stabilité du réseau. La session BGP entre deux homologues avec le même système autonome (AS) est appelée BGP interne (iBGP). Une session BGP entre deux homologues avec différents systèmes autonomes (AS) est appelée BGP externe (eBGP).

Généralement, la relation d'homologue est établie avec l'adresse IP de l'interface la plus proche de l'homologue, cependant, l'utilisation d'une interface de bouclage pour établir la session BGP est utile car elle ne désactive pas la session BGP quand il y a plusieurs chemins entre les homologues BGP.



Remarque : le processus décrit l'utilisation d'un bouclage pour un homologue eBGP, cependant, est le même processus pour un homologue iBGP afin qu'il puisse être utilisé comme référence.

Configuration eBGP avec une interface de bouclage

Scénario

Dans cette configuration, le pare-feu SFTD-1 possède une interface de bouclage avec l'adresse IP 10.1.1.1/32, et le système autonome 64000, le pare-feu SFTD-2 possède une interface de bouclage avec l'adresse IP 10.2.2.2/32 et le système autonome 64001. Les deux pare-feu utilisent leur interface externe pour atteindre l'interface de bouclage de l'autre pare-feu (dans ce scénario, l'interface externe est préconfigurée sur les deux pare-feu).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

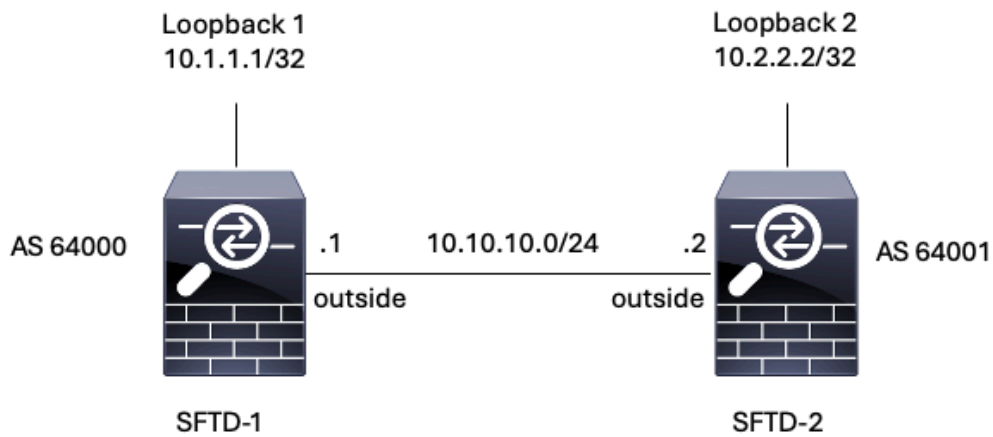


Image 1. Diagramme d'Escenario

Configuration de bouclage

Étape 1. Cliquez sur Périphériques > Gestion des périphériques, puis sélectionnez le périphérique où vous souhaitez configurer le bouclage.

Étape 2. Cliquez sur Interfaces > All Interfaces.

Étape 3. Cliquez sur 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	

Image 2. Ajouter un bouclage d'interface

Étape 4. Dans la section General, configurez le nom du bouclage, cochez la case Enabled, et configurez l'ID de bouclage.

Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Image 3. Configuration de base des interfaces de bouclage

Étape 5. Dans la section IPv4, sélectionnez l'option Use Static IP dans la section IP Type, configurez l'adresse IP de bouclage, puis cliquez sur OK pour enregistrer les modifications.

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

Image 4. Configuration des adresses IP de bouclage

Étape 6. Cliquez sur 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	✎ 🗑

Image 5. Enregistrer la configuration de l'interface de bouclage

Étape 7. Répétez le processus avec le deuxième pare-feu.

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

Image 6. Configuration de l'interface de bouclage sur homologue

Configuration de route statique

Une route statique doit être configurée pour garantir que l'adresse d'homologue distant (bouclage) utilisée pour l'appariage est accessible via l'interface souhaitée.

Étape 1. Cliquez sur Devices > Device Management, puis sélectionnez le périphérique que vous souhaitez configurer la route statique.

Étape 2. Cliquez sur Routing > Manage Virtual Routers > Static Route, puis cliquez sur Add Route.

The screenshot shows the 'Manage Virtual Routers' configuration page for 'FTD-1'. The 'Routing' tab is active. In the left sidebar, the 'Static Route' option is selected. The main area shows a table for configuring static routes with columns for Network, Interface, Leaked from Virtual Router, Gateway, Tunneled, Metric, and Tracked. A red box highlights the '+ Add Route' button in the top right corner.

Image 7. Ajouter une nouvelle route statique

Étape 3. Cochez l'option IPv4 pour Type. Sélectionnez l'interface physique utilisée pour atteindre le bouclage de l'homologue distant dans l'option Interface, puis spécifiez le saut suivant pour atteindre le bouclage sur la section 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

Image 8. Configuration de route statique

Étape 4. Cliquez sur l'icône (+) en regard de la section Available Network.

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

Image 9. Ajouter un nouvel objet réseau

Étape 5. Configurez un nom de référence et l'IP du bouclage de l'homologue distant et enregistrez.

New Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

Image 10. Configuration de la destination réseau dans la route statique

Étape 6. Recherchez le nouvel objet créé dans la barre de recherche, sélectionnez-le, puis cliquez sur Ajouter, puis cliquez sur 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

Image 11. Configuration du tronçon suivant dans la route statique

Étape 7. Cliquez sur Save.

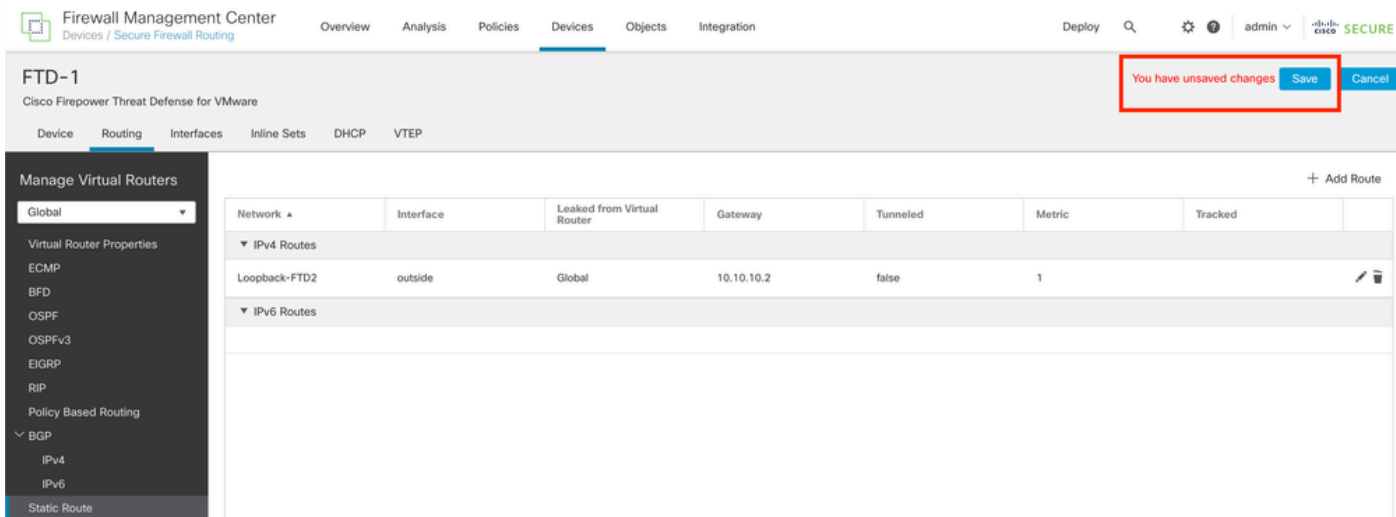


Image 12. Enregistrement de la configuration d'interface de route statique

Étape 8. Répétez le processus avec le deuxième pare-feu.

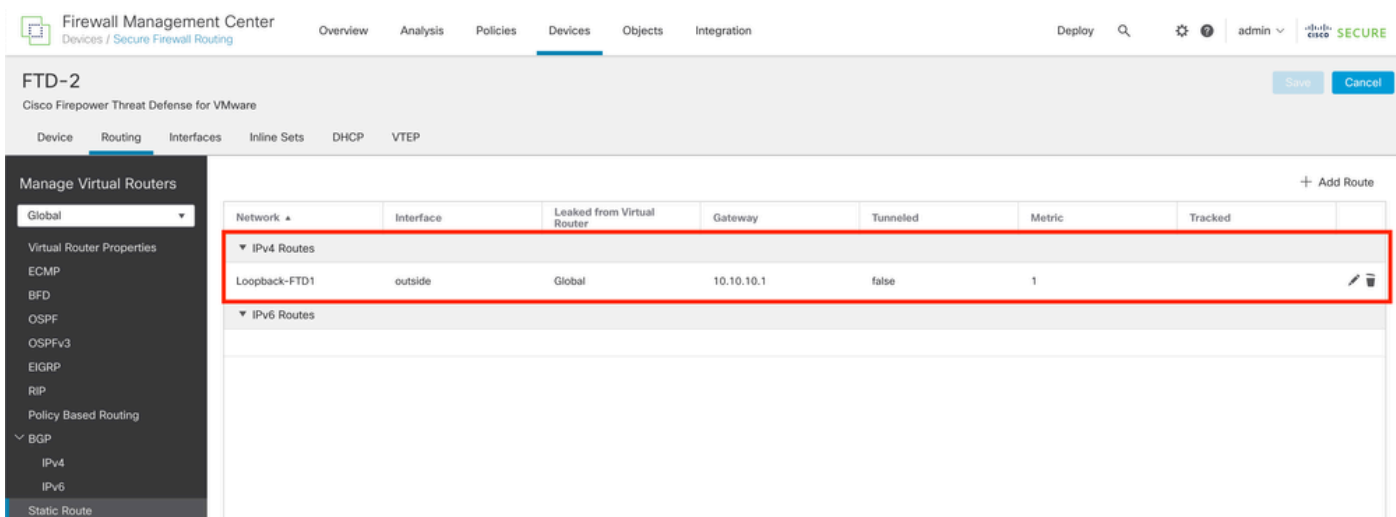


Image 13. Configuration du routage statique sur l'homologue

Configuration BGP

Étape 1. Cliquez sur **Devices > Device Management**, et sélectionnez le périphérique que vous voulez activer BGP.

Étape 2. Cliquez sur **Routing > Manage Virtual Routers > General Settings**, puis cliquez sur **BGP**.

Étape 3. Cochez la case **Enable BGP**, puis configurez le système autonome local du pare-feu dans la section **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
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
Best Path Selection	100

Neighbor Timers
Keepalive Interval
Hold time
Min hold time

Next Hop
Address tracking
Delay interval

Graceful Restart (use in f...)
Graceful Restart
Restart time

Image 14. Activer BGP globalement

Étape 4. Enregistrez les modifications en cliquant sur le bouton Enregistrer.

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

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
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
Hold time
Min hold time

You have unsaved changes Save Cancel

Image 15. Enregistrer la modification d'activation BGP

Étape 5. Dans la section Gérer les routeurs virtuels, accédez à l'option BGP, puis cliquez sur IPv4.

Étape 6. Cochez la case Enable IPv4, puis cliquez sur Neighbor, puis cliquez sur + Add.

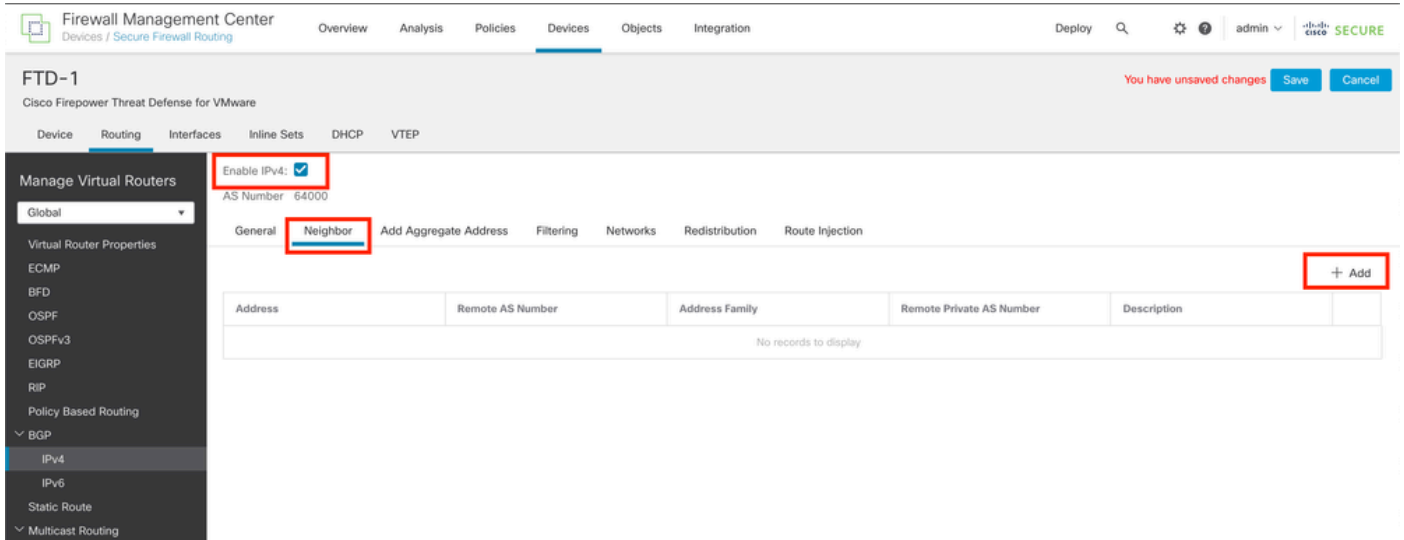


Image 16. Ajouter un nouvel homologue BGP

Étape 7. Configurez l'adresse IP de l'homologue distant dans la section IP Address, puis configurez le système autonome de l'homologue distant dans la section Remote AS et cochez la case Enable address.

Étape 8. Sélectionnez le bouclage de l'interface locale dans la section Update Source.

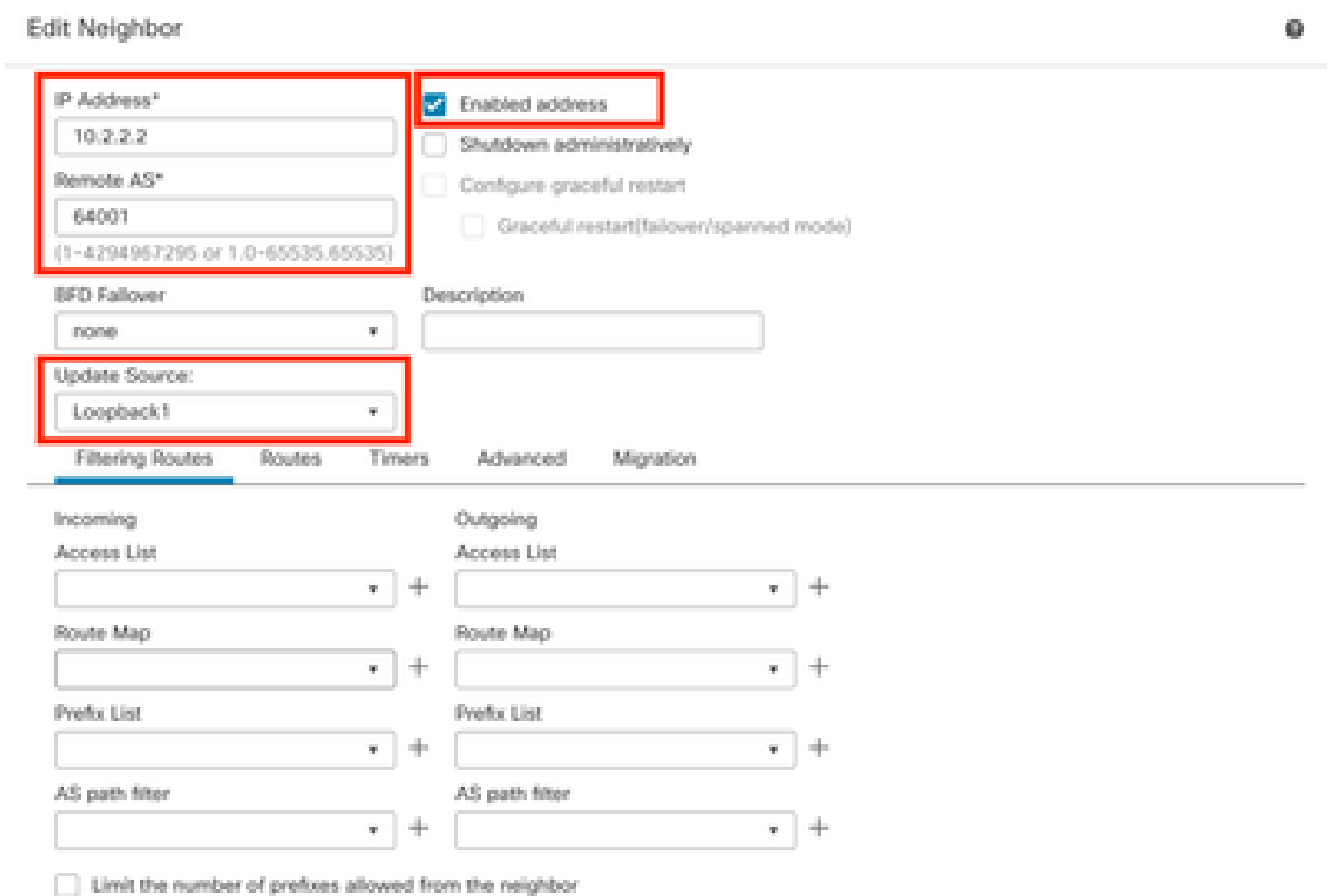

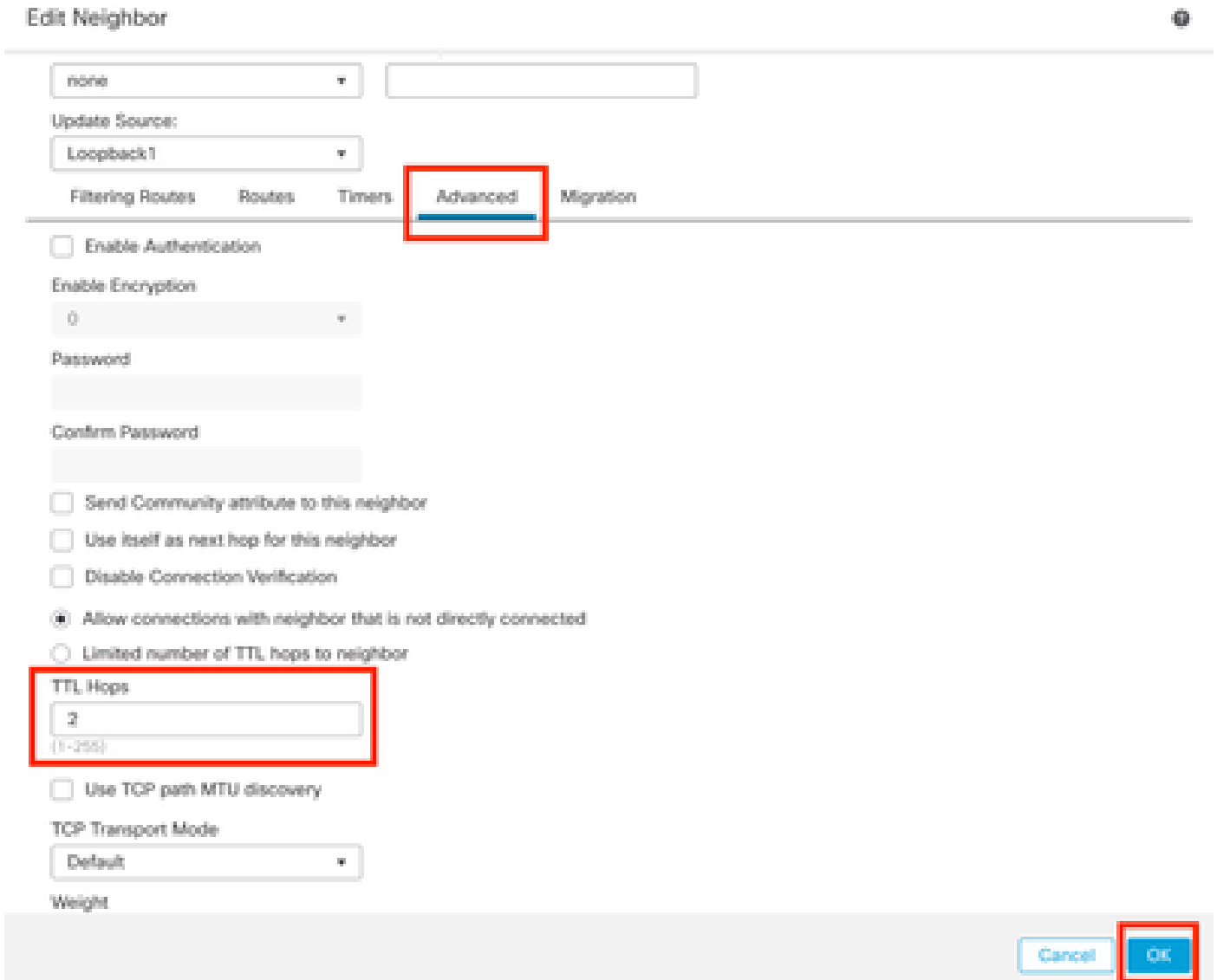


Image 17. Paramètres d'homologue BGP de base

 Remarque : l'option Update Source active la commande neighbor update-source, utilisée pour autoriser toute interface opérationnelle (y compris les boucles). Cette commande peut être spécifiée pour établir des connexions TCP.

Étape 9. Cliquez sur Advanced, puis configurez le numéro 2 dans l'option TTL Hops, et cliquez sur 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


(1-255)

Use TCP path MTU discovery

TCP Transport Mode
Default

Weight

Image 18. Configuration du numéro de saut TTL

 Remarque : l'option TTL Hops active la commande ebgp-multihop, utilisée pour modifier la valeur TTL pour permettre au paquet d'atteindre l'homologue BGP externe qui n'est pas directement connecté ou qui a une interface autre que l'interface directement connectée.

Étape 10. Cliquez sur Save et déployez les modifications.

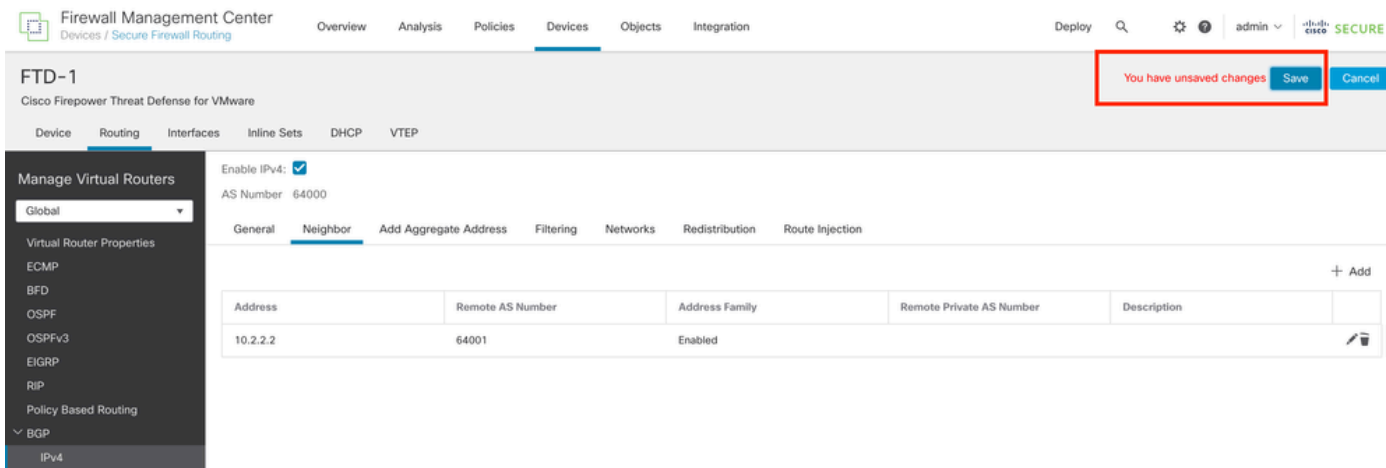


Image 19. Enregistrer la configuration BGP

Étape 11. Répétez le processus avec le deuxième pare-feu.

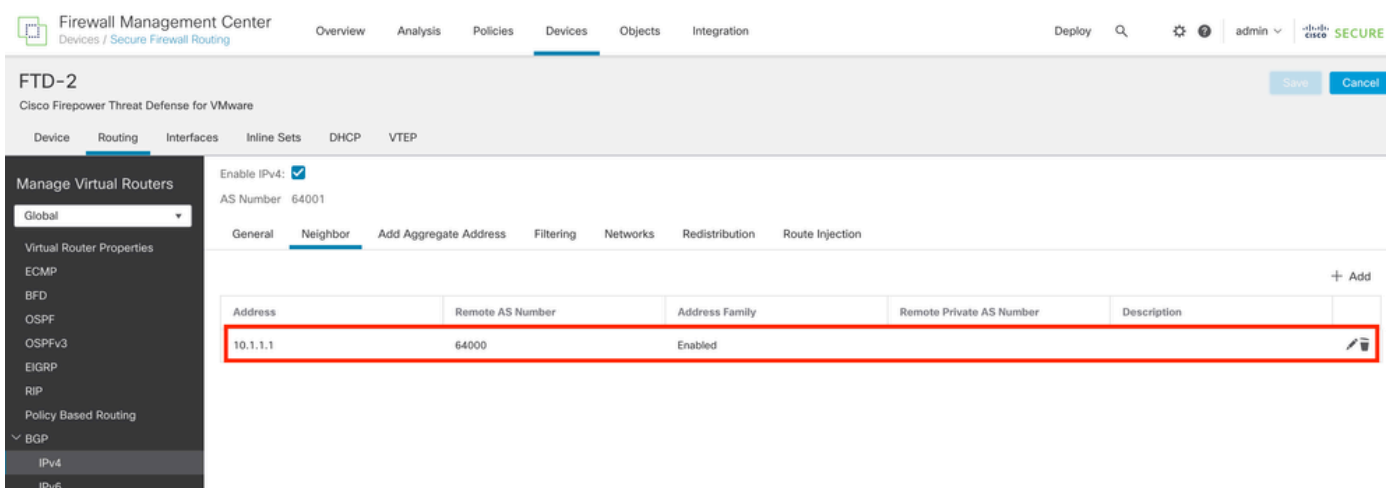


Image 20. Configurer BGP sur l'homologue

Vérifier

Étape 1. Vérifiez la configuration du bouclage et de la route statique, puis vérifiez la connectivité entre les homologues BGP à l'aide d'un test ping.

```
show running-config interface nom_interface
```

```
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 Bouclage1 adresse ip 10.1.1.1 255.255.255.255 show running-config route route en dehors de 10.2.2.2 255.255.255.255 10.10.10.2 1 ping 10.2.2.2 Envoi d'écho ICMP de 5 octets, 100 octets vers 10.2.2.2, délai d'attente de 2 secondes : !!!! Taux de réussite de 100 % (5/5), aller-retour min/moy/max = 1/1/1 ms </pre>	<pre> nameif Looback2 adresse ip 10.2.2.2 255.255.255.255 show running-config route route en dehors de 10.1.1.1 255.255.255.255 10.10.10.1 1 ping 10.1.1.1 Envoi d'écho ICMP de 5 octets, 100 octets vers 10.1.1.1, délai d'attente de 2 secondes : !!!! Taux de réussite de 100 % (5/5), aller-retour min/moy/max = 1/1/1 ms </pre>
---	--

Étape 2. Vérifiez la configuration BGP, puis assurez-vous que l'appairage BGP est établi.

```
show running-config router bgp
```

```
show bgp neighbors
```

```
show bgp summary
```

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

<p>no auto-summary</p> <p>aucune synchronisation</p> <p>exit-address-family</p> <p>!</p> <p>show bgp neighbors i BGP</p> <p>Le voisin BGP est 10.2.2.2, vrf single_vf, remote AS 64001, liaison externe</p> <p>BGP version 4, ID de routeur distant 10.2.2.2</p> <p>État BGP = Établi, jusqu'à 1j15h</p> <p>Table BGP version 7, voisin version 7/0</p> <p>Le voisin BGP externe peut se trouver à 2 sauts au maximum.</p> <p>show bgp summary</p> <p>Identificateur de routeur BGP 10.1.1.1, numéro de système autonome local 64000</p> <p>Version 7 de la table BGP, version 7 de la table de routage principale</p> <p>Voisin V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd</p> <p>10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0</p>	<p>no auto-summary</p> <p>aucune synchronisation</p> <p>exit-address-family</p> <p>!</p> <p>show bgp neighbors i BGP</p> <p>Le voisin BGP est 10.1.1.1, vrf single_vf, remote AS 64000, liaison externe</p> <p>BGP version 4, ID de routeur distant 10.1.1.1</p> <p>État BGP = Établi, jusqu'à 1d16h</p> <p>Table BGP version 1, voisin version 1/0</p> <p>Le voisin BGP externe peut se trouver à 2 sauts au maximum.</p> <p>show bgp summary</p> <p>Identificateur de routeur BGP 10.2.2.2, numéro de système autonome local 64001</p> <p>La version de la table BGP est 1, la version 1 de la table de routage principale</p> <p>Voisin V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd</p> <p>10.1.1.1 4 64000 2168 2173 1 0 0 1d16h 0</p>
--	--

Dépannage

Si vous rencontrez des problèmes au cours du processus, lisez cet article :

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.