

Configurazione di eBGP con interfaccia di loopback su firewall protetto

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione eBGP con interfaccia di loopback](#)

[Scenario](#)

[Esempio di rete](#)

[Configurazione loopback](#)

[Configurazione route statica](#)

[Configurazione BGP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare eBGP utilizzando un'interfaccia di loopback su Cisco Secure Firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- protocollo BGP

Il supporto dell'interfaccia di loopback per BGP è stato introdotto nella versione 7.4.0, che è la versione minima richiesta per Secure Firewall Management Center e Cisco Secure Firepower Threat Defense.

Componenti usati

- Secure Firewall Management Center per VMware versione 7.4.1
- 2 Cisco Secure Firepower Threat Defense per VMware versione 7.4.1


Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Border Gateway Protocol (BGP) è un protocollo EGP (Exterior Gateway Protocol) standardizzato per il routing dei vettori di percorso che fornisce scalabilità, flessibilità e stabilità di rete. La sessione BGP tra due peer con lo stesso Autonomous System (AS) è chiamata Internal BGP (iBGP). Una sessione BGP tra due peer con sistemi autonomi diversi (AS) è chiamata BGP esterno (eBGP).

In genere, la relazione peer viene stabilita con l'indirizzo IP dell'interfaccia più vicina al peer. Tuttavia, l'utilizzo di un'interfaccia di loopback per stabilire la sessione BGP è utile in quanto non interrompe la sessione BGP quando vi sono più percorsi tra i peer BGP.

 Nota: il processo descrive l'utilizzo di un loopback per un peer eBGP; tuttavia, è lo stesso processo per un peer iBGP, quindi può essere utilizzato come riferimento.

Configurazione eBGP con interfaccia di loopback

Scenario

In questa configurazione, il firewall SFTD-1 ha un'interfaccia di loopback con l'indirizzo IP 10.1.1.1/32, mentre il firewall SFTD-2 ha un'interfaccia di loopback con l'indirizzo IP 10.2.2.2/32 e l'AS 64001. Entrambi i firewall utilizzano l'interfaccia esterna per raggiungere l'interfaccia di loopback dell'altro firewall (in questo scenario, l'interfaccia esterna è preconfigurata su entrambi i firewall).

Esempio di rete

Il documento usa la seguente configurazione di rete:

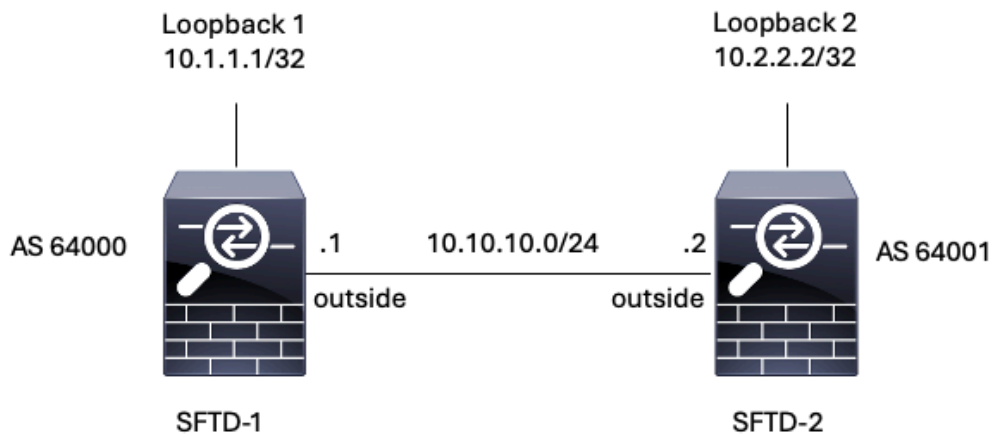


Immagine 1. Diagramma di Escenario

Configurazione loopback

Passaggio 1. Fare clic su Dispositivi > Gestione dispositivi, quindi selezionare il dispositivo in cui configurare il loopback.

Passaggio 2. Scegliere Interfacce > Tutte le interfacce.

Passaggio 3. Fare clic su Add Interface > Loopback Interface (Aggiungi interfaccia).

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	

Immagine 2. Aggiungi loopback interfaccia

Passaggio 4. Nella sezione Generale, configurare il nome del loopback, selezionare la casella Abilitato e configurare l'ID loopback.

Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Immagine 3. Configurazione di base dell'interfaccia di loopback

Passaggio 5. Nella sezione IPv4, selezionare l'opzione Use Static IP nella sezione IP Type, configurare l'indirizzo IP di loopback e fare clic su OK per salvare le modifiche.

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

Immagine 4. Configurazione indirizzo IP di loopback

Passaggio 6. Fare clic su Save (Salva).

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	✎ 🗑️

Immagine 5. Salvataggio della configurazione dell'interfaccia di loopback

Passaggio 7. Ripetere la procedura con il secondo firewall.

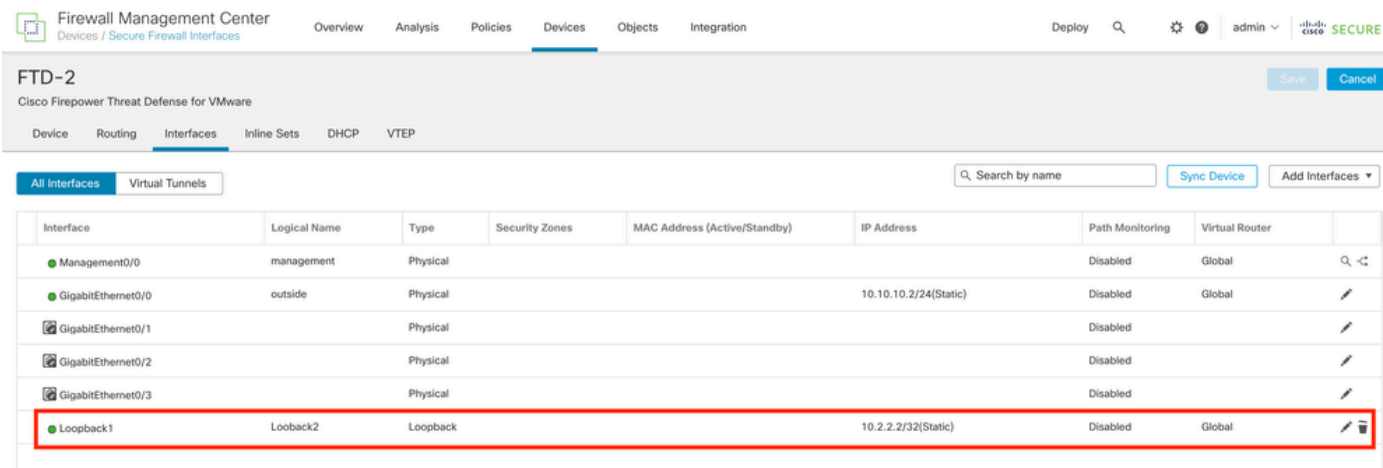


Immagine 6. Configurazione interfaccia di loopback nel peer

Configurazione route statica

È necessario configurare una route statica per garantire che l'indirizzo peer remoto (loopback) utilizzato per il peering sia raggiungibile tramite l'interfaccia desiderata.

Passaggio 1. Fare clic su Dispositivi > Gestione dispositivi, quindi selezionare il dispositivo per il quale si desidera configurare la route statica.

Passaggio 2. Fare clic su Routing > Gestisci router virtuali > Static Route, quindi fare clic su Add Route.

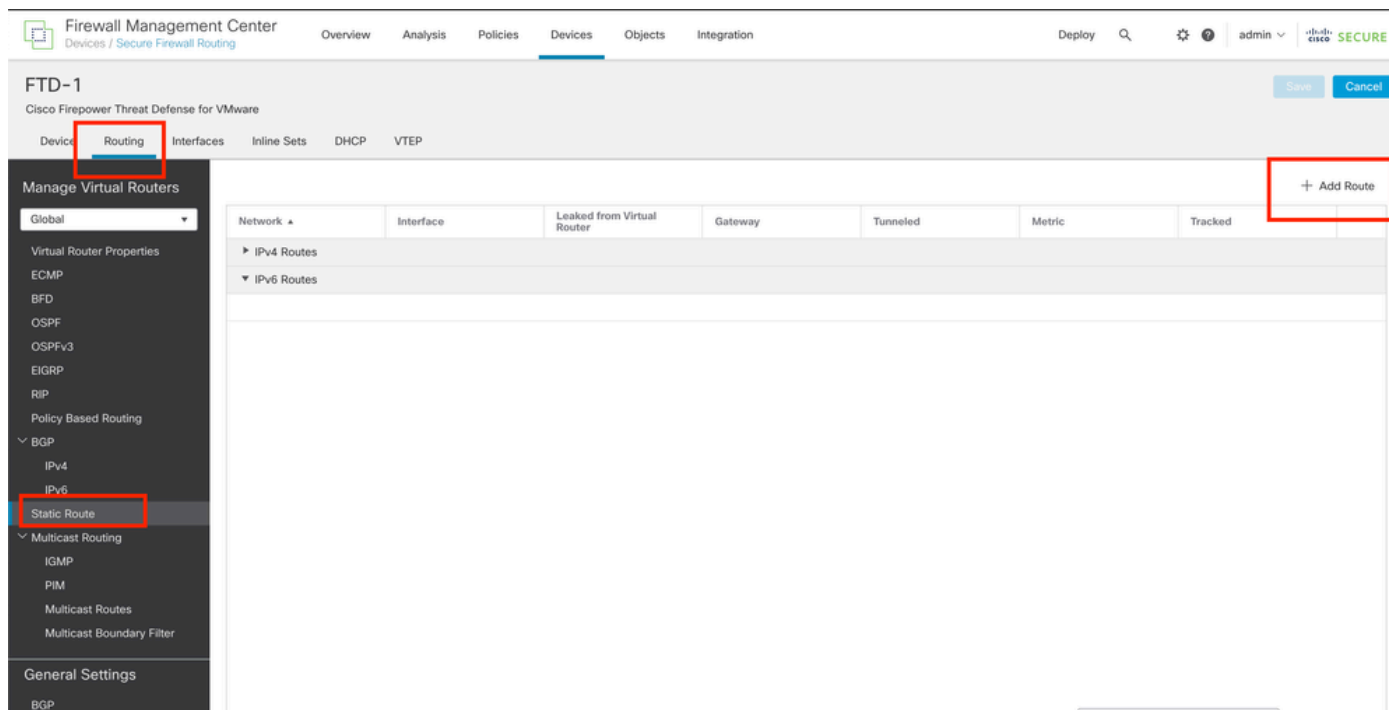


Immagine 7. Aggiungi nuova route statica

Passaggio 3. Selezionare l'opzione IPv4 per Type (Tipo). Selezionare l'interfaccia fisica utilizzata per raggiungere il loopback del peer remoto nell'opzione Interface, quindi specificare l'hop successivo per raggiungere il loopback nella sezione 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

Immagine 8. Configurazione route statica

Passaggio 4. Fare clic sull'icona (+) accanto alla sezione Rete disponibile.

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

Immagine 9. Aggiungi nuovo oggetto di rete

Passaggio 5. Configurare un nome di riferimento e l'indirizzo IP del looback del peer remoto e salvare.

New Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

Immagine 10. Configurare la destinazione di rete nella route statica

Passaggio 6. Cercare il nuovo oggetto creato nella barra di ricerca, selezionarlo, fare clic su Aggiungi e quindi su 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

Immagine 11. Configura hop successivo in route statica

Passaggio 7. Fare clic su Save (Salva).

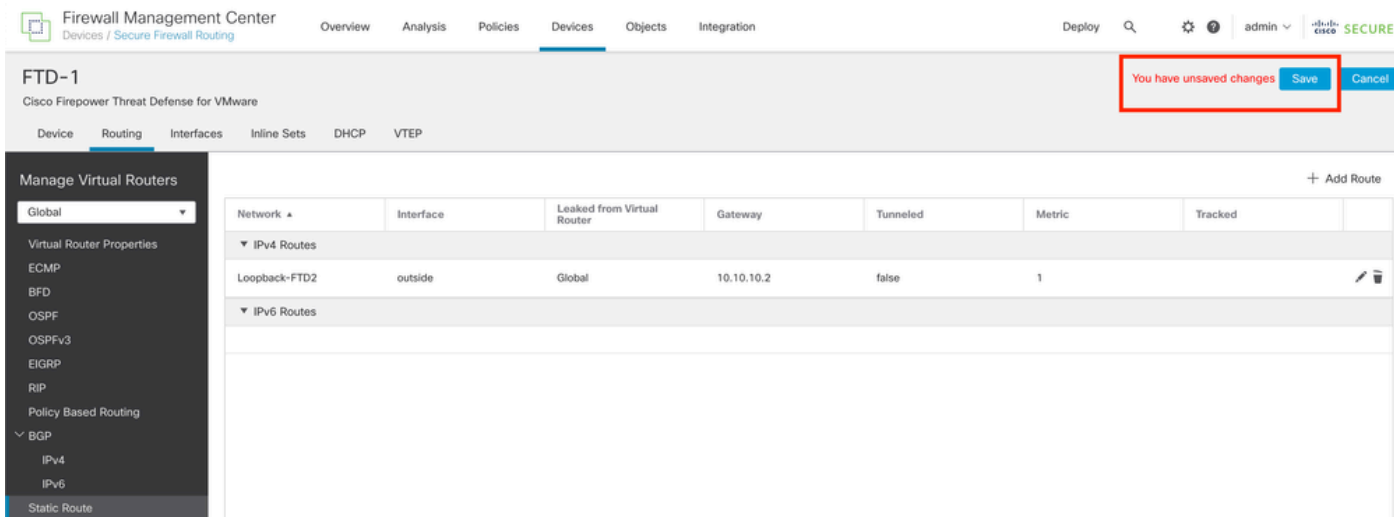


Immagine 12. Salvataggio della configurazione dell'interfaccia della route statica

Passaggio 8. Ripetere la procedura con il secondo firewall.

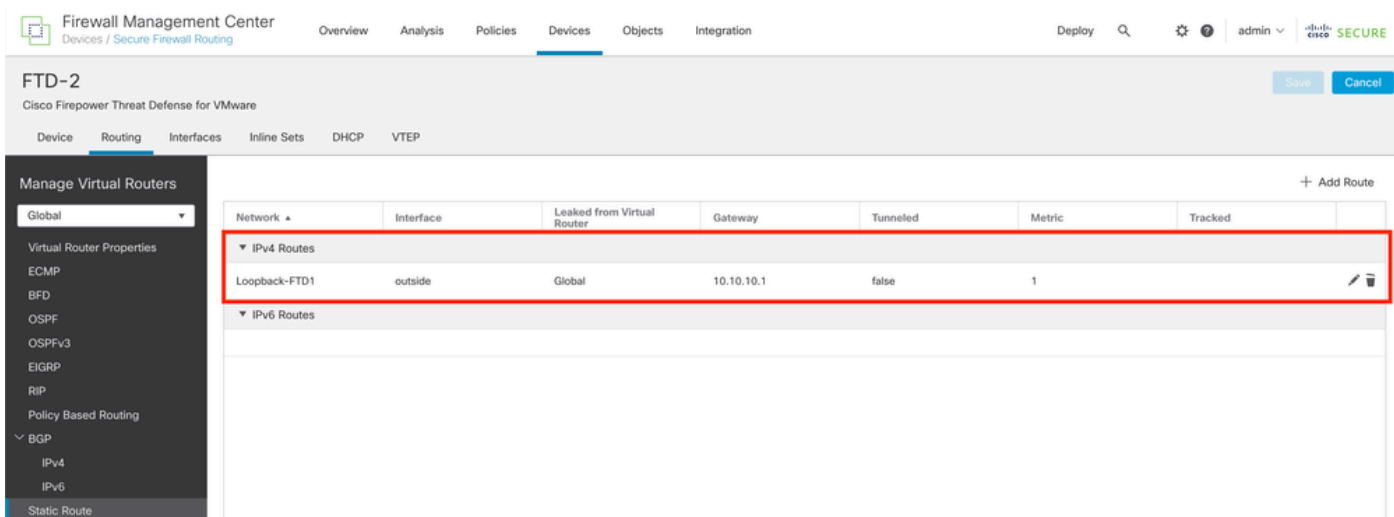


Immagine 13. Configura route statica su peer

Configurazione BGP

Passaggio 1. Fare clic su Dispositivi > Gestione dispositivi e selezionare il dispositivo che si desidera abilitare BGP.

Passaggio 2. Fare clic su Routing > Gestisci router virtuali > Impostazioni generali, quindi fare clic su BGP.

Passaggio 3. Selezionare la casella Enable BGP (Abilita BGP), quindi configurare l'appliance ASA locale del firewall nella sezione AS Number (Numero ASA).

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
--------------------------	-----

Immagine 14. Abilita BGP a livello globale

Passaggio 4. Salvare le modifiche facendo clic sul pulsante Salva.

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

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

You have unsaved changes Save Cancel

Immagine 15. Salva la modifica dell'abilitazione BGP

Passaggio 5. Nella sezione Gestione router virtuali, selezionare l'opzione BGP, quindi fare clic su IPv4.

Passaggio 6. Selezionare la casella Enable IPv4 (Abilita IPv4), fare clic su Adiacente (Adiacente), quindi fare clic su + Add (Aggiungi).

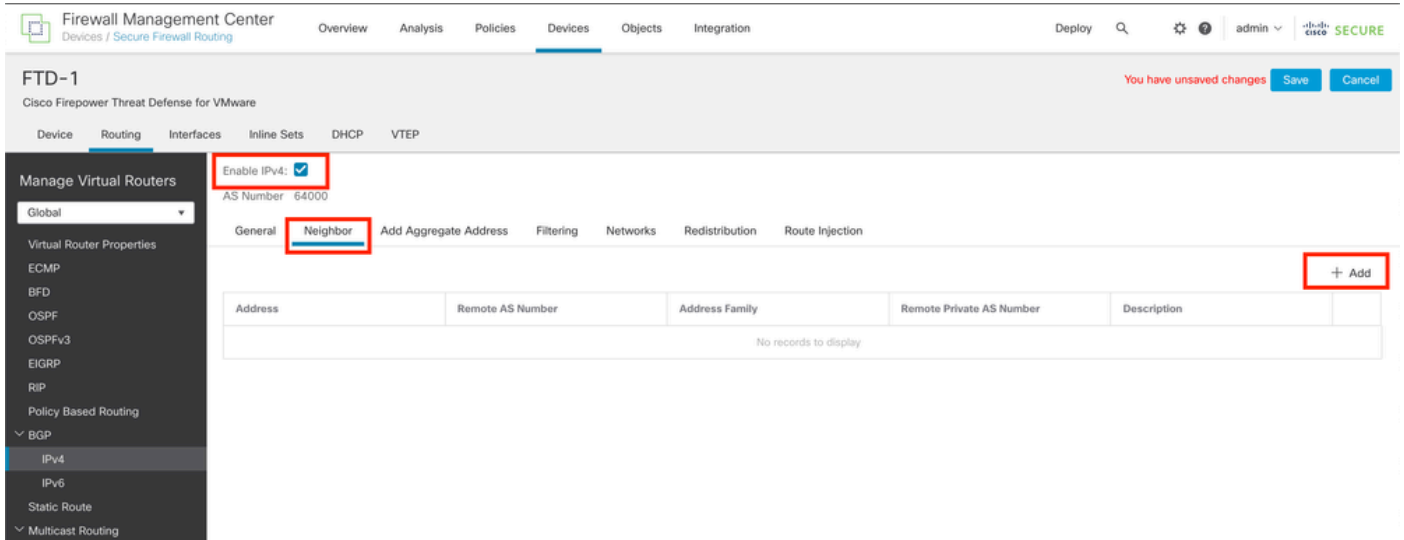


Immagine 16. Aggiungi nuovo peer BGP

Passaggio 7. Configurare l'indirizzo IP del peer remoto nella sezione Indirizzo IP, quindi configurare l'AS del peer remoto nella sezione AS remoto e selezionare la casella Abilita indirizzo.

Passaggio 8. Selezionare l'interfaccia locale Loopback nella sezione Aggiorna origine.

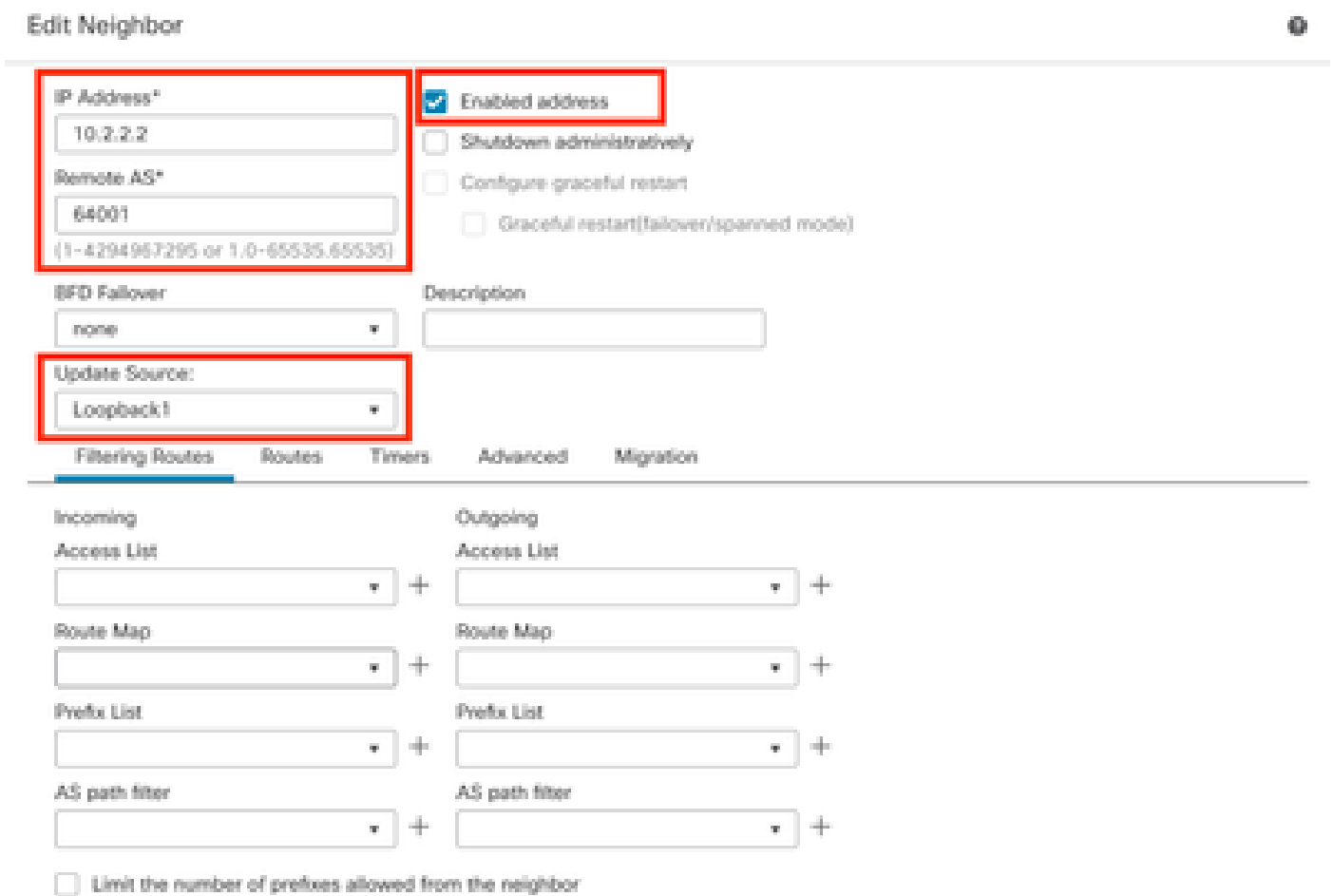


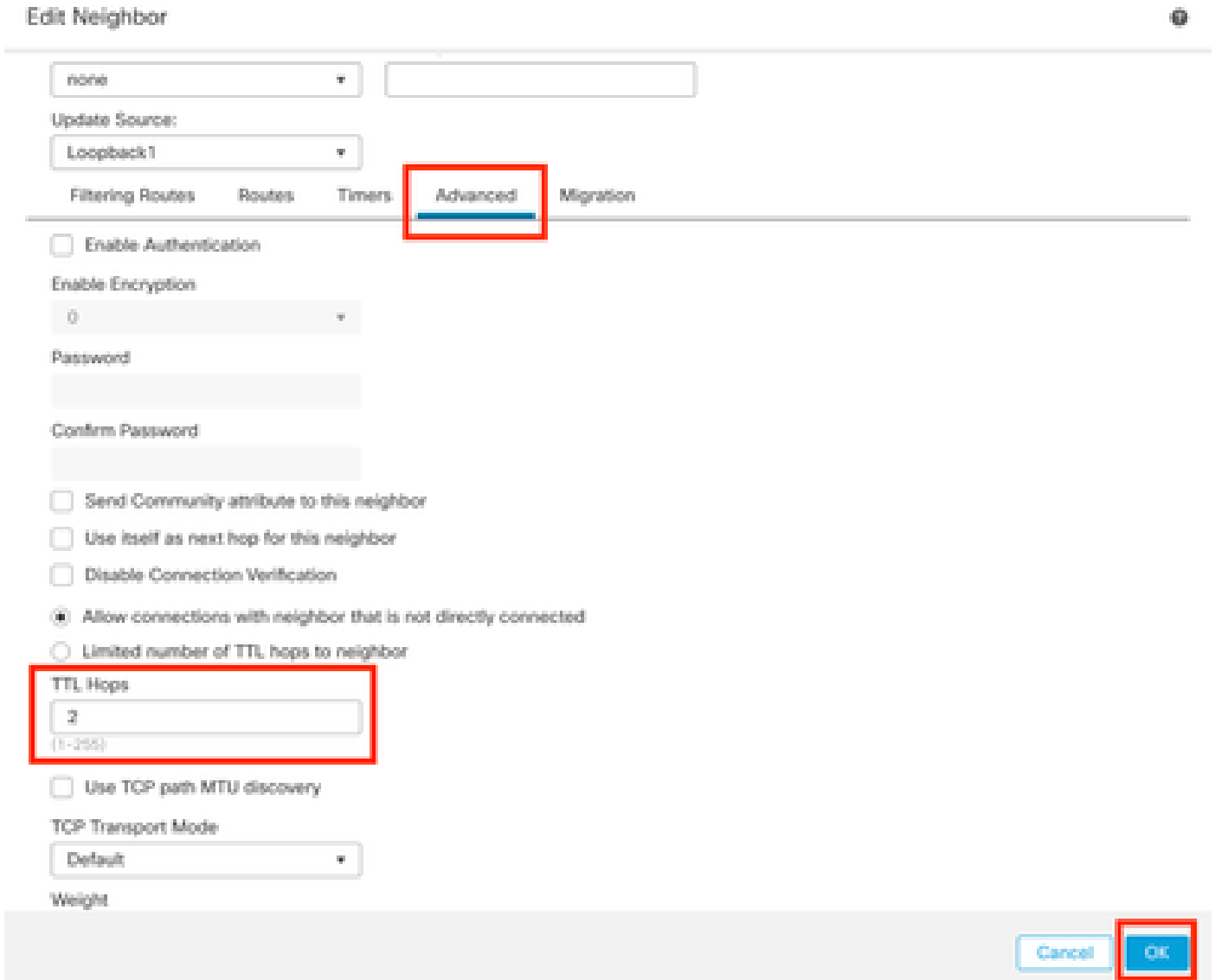


Immagine 17. Parametri peer BGP di base

 Nota: l'opzione Aggiorna origine abilita il comando neighbors update-source, utilizzato per

 consentire qualsiasi interfaccia operativa (inclusi i loopback). È possibile specificare questo comando per stabilire connessioni TCP.

Passaggio 9. Fare clic su Avanzate, quindi configurare il numero 2 nell'opzione TTL Hops e fare clic su 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

Immagine 18. Configurazione del numero di hop TTL

 Nota: l'opzione TTL Hops abilita il comando ebgp-multihop, usato per modificare il valore TTL per consentire al pacchetto di raggiungere il peer BGP esterno che non è connesso direttamente o che ha un'interfaccia diversa da quella connessa direttamente.

Passaggio 10. Fare clic su Save (Salva) e distribuire le modifiche.

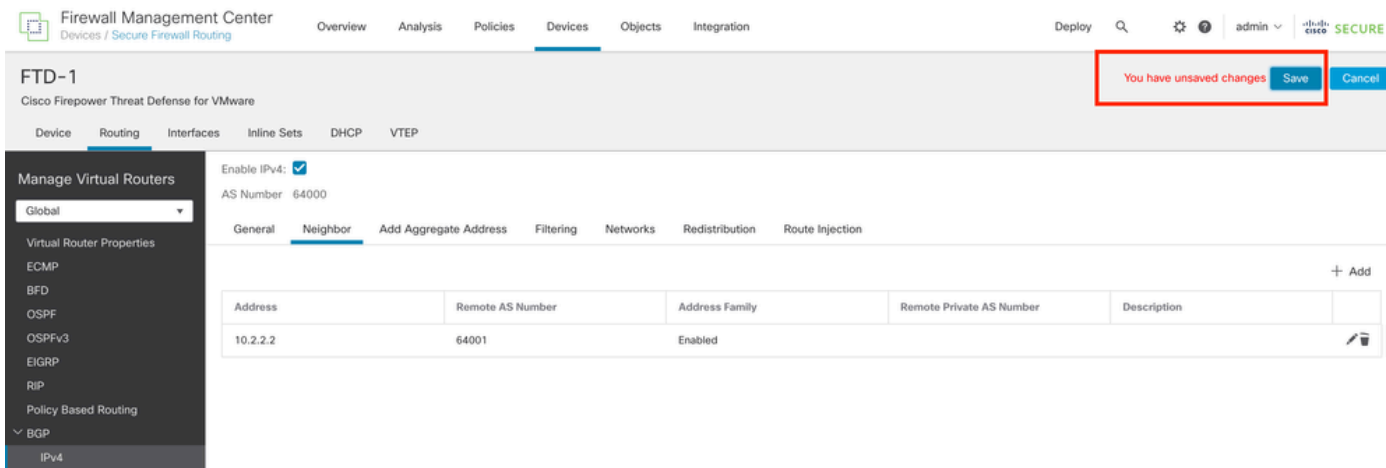


Immagine 19. Salvataggio della configurazione BGP

Passaggio 11. Ripetere la procedura con il secondo firewall.

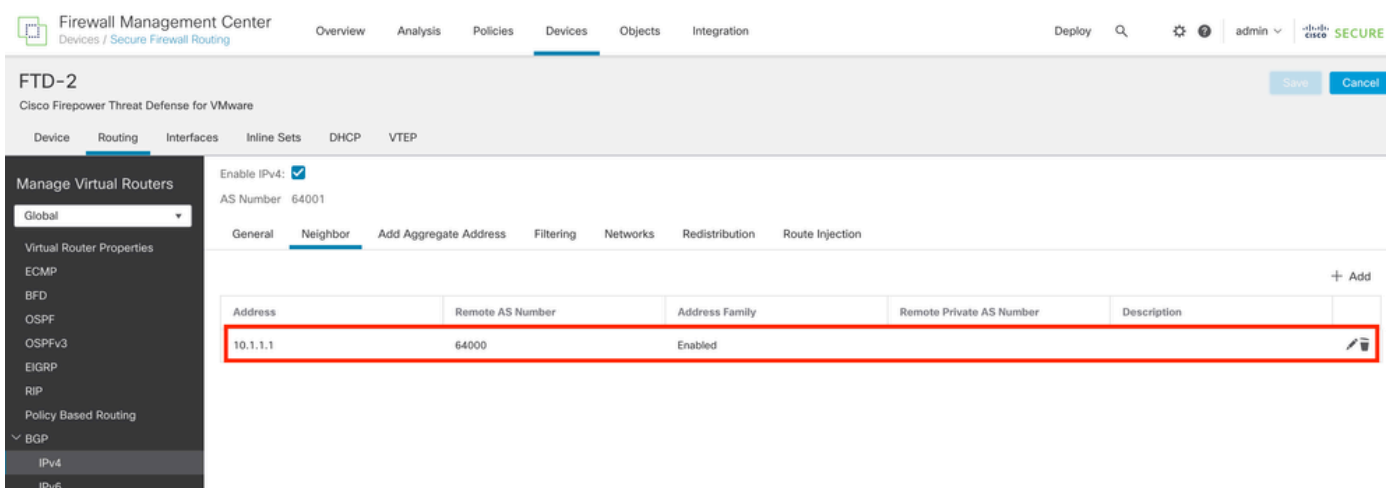


Immagine 20. Configurazione di BGP sul peer

Verifica

Passaggio 1. Verificare la configurazione del loopback e della route statica, quindi controllare la connettività tra i peer BGP con un test ping.

show running-config interface nome_interfaccia

show running-config route

show destination_ip

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

<pre> nameif Loopback1 indirizzo ip 10.1.1.1 255.255.255.255 show running-config route rotta esterna a 10.2.2.2 255.255.255.255 10.10.10.2.1 ping 10.2.2.2 Invio di 5 echo ICMP da 100 byte a 10.2.2.2, il timeout è di 2 secondi: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms </pre>	<pre> nameif Looback2 indirizzo ip 10.2.2.2 255.255.255.255 show running-config route rotta esterna a 10.1.1.1 255.255.255.255 10.10.10.1.1 ping 10.1.1.1 Invio di 5 echo ICMP da 100 byte a 10.1.1.1, il timeout è 2 secondi: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms </pre>
---	---

Passaggio 2. Verificare la configurazione BGP, quindi accertarsi che il peering BGP sia stato stabilito.

show running-config router bgp

mostra vicini bgp

mostra riepilogo bgp

SFTD-1	SFTD-2
<pre> show running-config router bgp router bgp 6400 bgp log-neighbor-changes bgp router-id vrf auto-assign unicast ipv4 famiglia di indirizzi neighbors 10.2.2.2 remote-as 64001 adiacente 10.2.2.2 ebgp-multihop 2 neighbors 10.2.2.2 transport path-mtu- discovery disable router adiacente 10.2.2.2 update-source Loopback1 </pre>	<pre> show running-config router bgp router bgp 6401 bgp log-neighbor-changes bgp router-id vrf auto-assign unicast ipv4 famiglia di indirizzi neighbors 10.1.1.1 remote-as 64000 adiacente 10.1.1.1 ebgp-multihop 2 neighbors 10.1.1.1 transport path-mtu- discovery disable update-source Looback2 adiacente 10.1.1.1 </pre>

<p>adiacente 10.2.2.2 attivare</p> <p>nessun riepilogo automatico</p> <p>nessuna sincronizzazione</p> <p>exit-address-family</p> <p>!</p> <p>mostra vicini bgp i BGP</p> <p>Il sistema BGP adiacente è 10.2.2.2, vrf single_vf, remoto AS 64001, collegamento esterno</p> <p>BGP versione 4, ID router remoto 10.2.2.2</p> <p>Stato BGP = Stabilito, attivo per 1 d15 h</p> <p>Tabella BGP versione 7, versione adiacente 7/0</p> <p>Il router adiacente BGP esterno può essere a una distanza massima di 2 hop.</p> <p>mostra riepilogo bgp</p> <p>Identificatore router BGP 10.1.1.1, numero AS locale 6400</p> <p>La versione della tabella BGP è 7, versione 7 della tabella di routing principale</p> <p>Router adiacente V AS MsgRcvd MsgSent TblVer InQ OutQ Stato attivo/inattivo/PfxRcd</p> <p>10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0</p>	<p>adiacente 10.1.1.1 attivare</p> <p>nessun riepilogo automatico</p> <p>nessuna sincronizzazione</p> <p>exit-address-family</p> <p>!</p> <p>mostra vicini bgp i BGP</p> <p>Il sistema BGP adiacente è 10.1.1.1, vrf single_vf, remoto AS 64000, collegamento esterno</p> <p>BGP versione 4, ID router remoto 10.1.1.1</p> <p>Stato BGP = Stabilito, attivo per 1 d16 h</p> <p>Tabella BGP versione 1, router adiacente versione 1/0</p> <p>Il router adiacente BGP esterno può essere a una distanza massima di 2 hop.</p> <p>mostra riepilogo bgp</p> <p>Identificatore router BGP 10.2.2.2, numero AS locale 64001</p> <p>La versione della tabella BGP è 1, la versione 1 della tabella di routing principale</p> <p>Router adiacente V AS MsgRcvd MsgSent TblVer InQ OutQ Stato attivo/inattivo/PfxRcd</p> <p>10.1.1.1 4 6400 2168 2173 1 0 0 1d16h 0</p>
--	--

Risoluzione dei problemi

Se si verificano problemi durante il processo, leggere questo articolo:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).