# 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).

| Firewall Management Center<br>Devices / Secure Firewall Interfaces                    | Overview     | Analysis P | olicies Devices | Objects Integration          | D                     | eploy Q 🗘       | e 🛛         | dmin v dhale SECURE               |
|---|--------------|------------|-----------------|------------------------------|-----------------------|-----------------|-------------|-----------------------------------|
| FTD-1<br>Cisco Firepower Threat Defense for VMware<br>Device Routing Interfaces Inlin | ne Sets DHCP | VTEP       |                 |                              |                       |                 |             | Save Cancel                       |
| All Interfaces Virtual Tunnels  |              |            |                 |                              | Q. Search by name     |                 | Sync Device | Add Interfaces V<br>Sub Interface |
| Interface   | Logical Name | Туре       | Security Zones  | MAC Address (Active/Standby) | IP Address            | Path Monitoring | Virtual F   | Redundant Interface               |
| Management0/0   | management   | Physical   |                 |                              |                       | Disabled        | Global      | Virtual Tunnel Interface          |
| GigabitEthernet0/0  | outside      | Physical   |                 |                              | 10.10.10.1/24(Static) | Disabled        | Global      | VNI Interface                     |
| GigabitEthernet0/1  |              | Physical   |                 |                              |                       | Disabled        |             | /                                 |
| GigabitEthemet0/2   |              | 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

| Looback1    |     |  |  |  |
|-------------|-----|--|--|--|
| Enabled     |     |  |  |  |
| Loopback II | D:* |  |  |  |
| 1           |     |  |  |  |
| (1-1024)    |     |  |  |  |
| Description |     |  |  |  |
|             |     |  |  |  |
|             |     |  |  |  |
|             |     |  |  |  |

?

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



e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24



Immagine 4. Configurazione indirizzo IP di loopback

### Passaggio 6. Fare clic su Save (Salva).

| Firewall Management Center<br>Devices / Secure Firewall Interfaces   | Overview     | Analysis Po | licies Devices | Objects Integration          | Dep                   | loy Q 🔅         | admin ~ diadu  | SECURE    |
|--|--------------|-------------|----------------|------------------------------|-----------------------|-----------------|----------------|-----------|
| FTD-1     Cancel       Cisco Firepower Threat Defense for VMware     Device Routing Interfaces Inline Sets DHCP VTEP |              |             |                |                              |                       |                 |                |           |
| All Interfaces Virtual Tunnels   |              |             |                |                              | Q. Search by name     | s               | Add Inte       | erfaces * |
| Interface  | Logical Name | Туре        | Security Zones | MAC Address (Active/Standby) | IP Address            | Path Monitoring | Virtual Router |           |
| Management0/0  | management   | Physical    |                |                              |                       | Disabled        | Global         | ۹.⊄       |
| GigabitEthernet0/0   | outside      | Physical    |                |                              | 10.10.10.1/24(Static) | Disabled        | Global         | /         |
| GigabitEthernet0/1   |              | Physical    |                |                              |                       | Disabled        |                | /         |
| GigabitEthernet0/2   |              | Physical    |                |                              |                       | Disabled        |                | /         |
| GigabitEthernet0/3   |              | Physical    |                |                              |                       | Disabled        |                | 1         |
| Loopback1  | Loopback1    | Loopback    |                |                              | 10.1.1.1/32(Static)   | Disabled        | Global         | 11        |
|  |              |             |                |                              |                       |                 |                |           |

Immagine 5. Salvataggio della configurazione dell'interfaccia di loopback

#### Passaggio 7. Ripetere la procedura con il secondo firewall.



| Firewall Management Cente<br>Devices / Secure Firewall Interfaces                                 | r Overview   | Analysis Po | olicies Devices | Objects Integration          | D                     | Neploy Q 🔅      | ∂ admin ∨ dhah     cisco     cisco | SECURE    |  |  |
|---|--------------|-------------|-----------------|------------------------------|-----------------------|-----------------|------------------------------------|-----------|--|--|
| TD-2<br>Isco Firepower Threat Defense for VMware  Device Routing Interfaces Inline Sets DHCP VTEP |              |             |                 |                              |                       |                 |                                    |           |  |  |
| All Interfaces Virtual Tunnels  |              |             |                 |                              | Q. Search by name     | 9               | Sync Device Add Inte               | erfaces 🔻 |  |  |
| Interface   | Logical Name | Туре        | Security Zones  | MAC Address (Active/Standby) | IP Address            | Path Monitoring | Virtual Router                     |           |  |  |
| Management0/0   | management   | Physical    |                 |                              |                       | Disabled        | Global                             | ≎ ب       |  |  |
| GigabitEthernet0/0  | outside      | Physical    |                 |                              | 10.10.10.2/24(Static) | Disabled        | Global                             | /         |  |  |
| GigabitEthernet0/1  |              | Physical    |                 |                              |                       | Disabled        |                                    | /         |  |  |
| GigabitEthernet0/2  |              | Physical    |                 |                              |                       | Disabled        |                                    | /         |  |  |
| GigabitEthernet0/3  |              | Physical    |                 |                              |                       | Disabled        |                                    | 1         |  |  |
| Loopback1   | Looback2     | Loopback    |                 |                              | 10.2.2.2/32(Static)   | Disabled        | Global                             | 11        |  |  |

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.

| Firewall Management Center<br>Devices / Secure Firewall Routing                             | Overview Analysis Policies | Devices Objects               | Integration |          | Deploy Q | 🔅 🞯 🛛 admin 🗸 🖓 dividu SECURE |
|---|----------------------------|-------------------------------|-------------|----------|----------|-------------------------------|
| FTD-1<br>Cisco Firepower Threat Defense for VMware<br>Device Routing Interfaces Inline Sets | DHCP VTEP                  |                               |             |          |          | Save Cancel                   |
| Manage Virtual Routers  |                            |                               |             |          |          | + Add Route                   |
| Global   Network  | Interface                  | Leaked from Virtual<br>Router | Gateway     | Tunneled | Metric   | Tracked                       |
| Virtual Router Properties   IPv4 Route  | 15                         |                               |             |          |          |                               |
| ECMP V6 Route   | 15                         |                               |             |          |          |                               |
| BFD   |                            |                               |             |          |          |                               |
| OSPF  |                            |                               |             |          |          |                               |
| OSPEV3  |                            |                               |             |          |          |                               |
| RIP   |                            |                               |             |          |          |                               |
| Policy Based Routing  |                            |                               |             |          |          |                               |
| ∼ BGP   |                            |                               |             |          |          |                               |
| IPv4  |                            |                               |             |          |          |                               |
| IPv6  |                            |                               |             |          |          |                               |
| Static Route  |                            |                               |             |          |          |                               |
| V Multicast Routing   |                            |                               |             |          |          |                               |
| IGMP  |                            |                               |             |          |          |                               |
| PIM<br>Multicast Doutes   |                            |                               |             |          |          |                               |
| Multicast Boundary Filter   |                            |                               |             |          |          |                               |
|   |                            |                               |             |          |          |                               |
| General Settings  |                            |                               |             |          |          |                               |
| BGP   |                            |                               |             |          | 1.00     |                               |

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                            | ٣        |
| (Interface starting with this icon | Ssignifi |
| Available Network C                | +        |
| 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         |          |

#### Ensure that egress virtualrouter has route to that destination

| Gateway                            |       |
|------------------------------------|-------|
| 10.10.10.2 +                       | +     |
| Metric:                            |       |
| 1                                  |       |
| (1 - 254)                          |       |
| Tunneled: Used only for default Re | oute) |
| Route Tracking:                    |       |
|                                    | $^+$  |
|                                    |       |
|                                    |       |
|                                    |       |

Immagine 8. Configurazione route statica



Edit Static Route Configuration

| Type: (             | IPv4      | O IPv6         |                |                      |  |
|---------------------|-----------|----------------|----------------|----------------------|--|
| Interface*          |           |                |                |                      |  |
| outside             |           |                |                |                      |  |
| (Interface starting | with this | icon 🚳 signifi | es it is avail | able for route leak) |  |
| Available Network   | С         | +              |                | Selected Network     |  |
| Q. Search           |           |                | Add            |                      |  |
| any-ipv4            |           |                |                |                      |  |
| IPv4-Benchmark      | -Tests    |                |                |                      |  |
| IPv4-Link-Local     |           |                |                |                      |  |
| IPv4-Multicast      |           |                |                |                      |  |
| IPv4-Private-10.    | 0.0.0-8   |                |                |                      |  |
| IPv4-Private-172    | 2.16.0.0- | 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.

0

# New Network Object

| Name                   |             |
|------------------------|-------------|
| Loopback-FTD2          |             |
| Description            |             |
| Host O Range O Network | O FQDN      |
| 10.2.2.2               |             |
| 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.

0

| Type:      IPv4               | O IPv6           |                                   |   |
|-------------------------------|------------------|-----------------------------------|---|
| Interface*                    |                  |                                   |   |
| outside                       | Ψ                |                                   |   |
| (Interface starting with this | icon 🚳 signifie: | s it is available for route leak) |   |
| Available Network C           | +                | Selected Network                  |   |
| Q, Loopback-FTD2              | ×                | Add Loopback-FTD2                 | ĩ |
| 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 |

Immagine 11. Configura hop successivo in route statica

Passaggio 7. Fare clic su Save (Salva).

ø

| Firewall Management<br>Devices / Secure Firewall Routin                     | Center Overview           | Analysis Policies | Devices Objects I             | Integration |          | Deploy Q | 🔅 🕜 admin ~ 🕴                 |
|---|---------------------------|-------------------|-------------------------------|-------------|----------|----------|-------------------------------|
| FTD-1<br>Cisco Firepower Threat Defense for VI<br>Device Routing Interfaces | Mware<br>Inline Sets DHCP | VTEP              |                               |             |          | You have | a unsaved changes Save Cancel |
| Manage Virtual Routers  |                           |                   |                               |             |          |          | + Add Route                   |
| Global 🔻  | Network .                 | Interface         | Leaked from Virtual<br>Router | Gateway     | Tunneled | Metric   | Tracked                       |
| Virtual Router Properties   | ▼ IPv4 Routes             |                   |                               |             |          |          |                               |
| ECMP  | Loopback-FTD2             | outside           | Global                        | 10.10.10.2  | false    | 1        | /1                            |
| OSPF  | ▼ IPv6 Routes             |                   |                               |             |          |          |                               |
| OSPFv3  |                           |                   |                               |             |          |          |                               |
| EIGRP   |                           |                   |                               |             |          |          |                               |
| RIP   |                           |                   |                               |             |          |          |                               |
| Policy Based Routing  |                           |                   |                               |             |          |          |                               |
| ∀ BGP   |                           |                   |                               |             |          |          |                               |
| IPv4  |                           |                   |                               |             |          |          |                               |
| IPv6  |                           |                   |                               |             |          |          |                               |
| Static Route  |                           |                   |                               |             |          |          |                               |

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

#### Passaggio 8. Ripetere la procedura con il secondo firewall.

| Firewall Management (<br>Devices / Secure Firewall Routin                   | Center c<br>9        | Verview | Analysis  | Policies | Devices              | Objects    | Integration |          | Deploy | ۹ | 🗘 🕜 adm | nin v dudu<br>cisco | SECURE  |
|---|----------------------|---------|-----------|----------|----------------------|------------|-------------|----------|--------|---|---------|---------------------|---------|
| FTD-2<br>Cisco Firepower Threat Defense for VN<br>Device Routing Interfaces | /ware<br>Inline Sets | DHCP    | VTEP      |          |                      |            |             |          |        |   |         | Save                | Cancel  |
| Manage Virtual Routers  |                      |         |           |          |                      |            |             |          |        |   |         | + Ad                | d Route |
| Global v  | Network .            |         | Interface |          | Leaked fre<br>Router | om Virtual | Gateway     | Tunneled | Metric |   | Tracked |                     |         |
| Virtual Router Properties   | ▼ IPv4 Routes        |         |           |          |                      |            |             |          |        |   |         |                     |         |
| ECMP  | Loopback-FTD1        |         | outside   |          | Global               |            | 10.10.10.1  | false    | 1      |   |         |                     | 11      |
| OSPF  | ▼ IPv6 Routes        |         |           |          |                      |            |             |          |        |   |         |                     |         |
| OSPFv3  |                      |         |           |          |                      |            |             |          |        |   |         |                     |         |
| EIGRP   |                      |         |           |          |                      |            |             |          |        |   |         |                     |         |
| RIP<br>Policy Pared Policipa  |                      |         |           |          |                      |            |             |          |        |   |         |                     |         |
| ✓ BGP   |                      |         |           |          |                      |            |             |          |        |   |         |                     |         |
| IPv4  |                      |         |           |          |                      |            |             |          |        |   |         |                     |         |
| IPv6  |                      |         |           |          |                      |            |             |          |        |   |         |                     |         |
| Static Route  |                      |         |           |          |                      |            |             |          |        |   |         |                     |         |

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<br>Devices / Secure Firewall Routin   | Center Overview Analysis Policies Devices Objects   | Integration |                    |
|---|---|-------------|--------------------|
| FTD-1<br>Cisco Firepower Threat Defense for VI<br>Device Routing Interfaces                           | Mware<br>Inline Sets DHCP VTEP  |             |                    |
| Manage Virtual Routers<br>Global  Virtual Router Properties<br>ECMP<br>BFD<br>OSPF<br>OSPFv3<br>FIGRP | Enable BGP:<br>AS Number*<br>64000<br>C-4294967295 or 1.0-65535.65535)<br>Override BGP general settings router-id address:<br>Router Id<br>Automatic<br>IP Address* |             |                    |
| RIP   | General   | 1           | Neighbor Timers    |
| Policy Based Routing  | Scanning Interval   | 60          | Keepalive Interval |
| ∽ BGP   | Number of AS numbers in AS_PATH attribute of received routes  | None        | Hold time          |
| IPv4  | Log Neighbor Changes  | Yes         | Min hold time      |
| IPv6  | Use TCP path MTU discovery  | Yes         |                    |
| Static Route  | Reset session upon failover   | Yes         | Next Hop           |
| <ul> <li>Multicast Routing</li> <li>IGMP</li> </ul>   | Enforce the first AS is peer's AS for EBGP routes   | Yes         | Address tracking   |
| PIM   | Lise dot notation for AS number   | No          | Delay interval     |
| Multicast Routes  |   | 30          |                    |
| Multicast Boundary Filter   | Aggregate timer   | 50          |                    |
| General Settings  | Best Path Selection   | 1           | Graceful Restart   |
| BGP   | Default local preference  | 100         | Restart time       |
|   |   |             |                    |

Immagine 14. Abilita BGP a livello globale

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

| Firewall Management   | nt Center Overview Analysis Policies Devices Objects  | Integration | Deploy             | Q ✿ admin ∽ dealer SECURE            |
|---|---|-------------|--------------------|--------------------------------------|
| FTD-1<br>Cisco Firepower Threat Defense for<br>Device Routing Interfac                                | VMware<br>es Inline Sets DHCP VTEP  |             |                    | You have unsaved changes Save Cancel |
| Manage Virtual Routers<br>Global  Virtual Router Properties<br>ECMP<br>BFD<br>OSPF<br>OSPFv3<br>EICPP | Enable BGP:<br>AS Number*<br>64000<br>Override BGP general settings router~id address:<br>Router Id<br>Automatic<br>IP Address* |             |                    |                                      |
| RIP   | General   | 1           | Neighbor Timers    | 1                                    |
| Policy Based Routing  | Scanning Interval   | 60          | Keepalive Interval | 60                                   |
| ∼ BGP   | Number of AS numbers in AS_PATH attribute of received routes  | None        | Hold time          | 180                                  |
| IPv4  | Log Neighbor Changes  | Yes         | Min hold time      | 0                                    |
| IPv6<br>Static Route  | Use TCP path MTU discovery  | Yes         |                    |                                      |

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).

| Firewall Management<br>Devices / Secure Firewall Ro | nt Center Overvi                                    | ew Analysis | Policies    | Devices   | Objects  | Integration    |                    |                          | Deploy | ۹         | 🔅 🞯 admin 🗸        | cisco SECURE |
|---|---|-------------|-------------|-----------|----------|----------------|--------------------|--------------------------|--------|-----------|--------------------|--------------|
| FTD-1<br>Cisco Firepower Threat Defense for         | · VMware  |             |             |           |          |                |                    |                          |        | You have  | unsaved changes Sa | ve Cancel    |
| Device Routing Interfac                             | es Inline Sets DHO                                  | P VTEP      |             |           |          |                |                    |                          |        |           |                    |              |
| Manage Virtual Routers<br>Global                    | Enable IPv4:<br>AS Number 64000<br>General Neighbor | Add Aggreç  | ate Address | Filtering | Networks | Redistribution | Route Injection    |                          |        |           |                    |              |
| ECMP  |   | -           |             |           |          |                |                    |                          |        |           |                    | + Add        |
| BFD   |   |             |             |           |          |                |                    |                          |        |           |                    |              |
| OSPF  | Address   |             | Remote AS N | umber     |          | Address Family |                    | Remote Private AS Number |        | Descripti | an                 |              |
| OSPFv3  |   |             |             |           |          | No             | records to display |                          |        |           |                    |              |
| EIGRP   |   |             |             |           |          |                |                    |                          |        |           |                    |              |
| RIP   |   |             |             |           |          |                |                    |                          |        |           |                    |              |
| Policy Based Routing                                |   |             |             |           |          |                |                    |                          |        |           |                    |              |
| Y BGP   |   |             |             |           |          |                |                    |                          |        |           |                    |              |
| IPv4  |   |             |             |           |          |                |                    |                          |        |           |                    |              |
| IPv6  |   |             |             |           |          |                |                    |                          |        |           |                    |              |
| Static Route<br>V Multicast Routing                 |   |             |             |           |          |                |                    |                          |        |           |                    |              |

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.

0

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

| Edit | Neighbor |  |
|------|----------|--|
|      |          |  |

| - FT2-0-1-22  | Chapter accress   |
|---|---|
| 10.2.2.2  | Shutdown administratively   |
| Remote AS*  | Configure graceful restart  |
| 64001   | Graceful restart(failover/snanned mode)   |
| (1-4294967295 or 1.0-65535.65535)   |   |
| BFD Fallover  | Description   |
| none v  |   |
| Update Source:  |   |
|   |   |
| Loopbeck1 •   |   |
| Electron Brutes Brutes Timer  | n Advanced Ministro   |
| Filtering Routes Routes Timer   | rs Advanced Migration   |
| Filtering Routes Routes Timer   | rs Advanced Migration Outgoing  |
| Filtering Routes Routes Timer Incoming Access List  | rs Advanced Migration Outgoing Access List  |
| Incoming<br>Access List   | rs Advanced Migration Outgoing Access List +  |
| Loopbeck1  Filtering Routes Routes Timer Incoming Access List Route Map                                     | rs Advanced Migration Outgoing Access List + Route Map  |
| Loopbeck1  Filtering Routes Routes Timer Incoming Access List Route Map                                     | rs Advanced Migration Outgoing Access List + Route Map + V + V + V + V + V + V + V + V + V +                                  |
| Loopbeck1   Filtering Routes Routes Timer Incoming Access List  Route Map  Prefx List                       | Advanced Migration Outgoing Access List + Route Map + Prefix List   |
| Loopbeck1   Filtering Routes Routes Timer Incoming Access List  Route Map  Prefix List                      | rs Advanced Migration Outgoing Access List + Route Map + Prefix List + V + V + V + V + V + V + V + V + V +                    |
| Loopbeck1   Filtering Routes Routes Timer Incoming Access List  Route Map  Prefix List  AS path filter      | Advanced Migration Outgoing Access List + Route Map + Prefix List + AS path fitter  |
| Loopbeck1   Filtering Routes Routes Timer Incoming Access List  Route Map  Prefix List  AS path filter  v 4 | rs Advanced Migration Outgoing Access List + Route Map + Prefix List + AS path filter + + Y + Y + Y + Y + Y + Y + Y + Y + Y + |

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                                     |                                 |           | 0      |
|---|---------------------------------|-----------|--------|
| none  | •                               |           |        |
| Update Source:                                    |                                 |           |        |
| Loopback1   | *                               |           |        |
| Filtering Routes Routes                           | Timers Advanced                 | Migration |        |
| Enable Authentication                             |                                 |           |        |
| Enable Encryption                                 |                                 |           |        |
| 0   | *                               |           |        |
| Password  |                                 |           |        |
| Confirm Password                                  |                                 |           |        |
| Send Community attribute t                        | ) this neighbor                 |           |        |
| Use itself as next hop for th                     | s neighbor                      |           |        |
| <ul> <li>Disable Connection Verifica</li> </ul>   | ion                             |           |        |
| <ol> <li>Allow connections with neight</li> </ol> | hbor that is not directly conne | cted      |        |
| <ul> <li>Limited number of TTL hope</li> </ul>    | to neighbor                     |           |        |
| TTL Hops  |                                 |           |        |
| (1-255)   | _                               |           |        |
| Use TCP path MTU discove                          | v                               |           |        |
| TCP Transport Mode                                |                                 |           |        |
| Default   | •                               |           |        |
| Weight  |                                 |           |        |
|   |                                 |           | Cancel |
|   |                                 |           |        |
|   |                                 |           |        |

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.

| Firewall Managemen<br>Devices / Secure Firewall Roo     | t Center                                     | Overview        | Analysis    | Policies    | Devices   | Objects  | Integration    |                         | 1                        | Deploy | ۹           | 0 0        | admin $\sim$ | cisco SECURE |
|---|--|-----------------|-------------|-------------|-----------|----------|----------------|-------------------------|--------------------------|--------|-------------|------------|--------------|--------------|
| FTD-1<br>Cisco Firepower Threat Defense for             | VMware                                       |                 |             |             |           |          |                |                         |                          |        | You ha      | ve unsaved | I changes S  | ave Cancel   |
| Device Routing Interface                                | es Inline Sets                               | DHCP            | VTEP        |             |           |          |                |                         |                          |        |             |            |              |              |
| Manage Virtual Routers Global Virtual Router Properties | Enable IPv4: 🗹<br>AS Number 640<br>General N | 000<br>leighbor | Add Aggrega | ite Address | Filtering | Networks | Redistribution | Route Injection         |                          |        |             |            |              |              |
| ECMP  |  |                 |             |             |           |          |                |                         |                          |        |             |            |              | + Add        |
| BFD   | Address                                      |                 |             | Remote AS N | umber     |          | Address Family |                         | Remote Private AS Number |        | Descrit     | otion      |              |              |
| OSPF  | 100000                                       |                 |             | 6 1001      | 111001    |          | Franking       | Remote Physic A3 Humber |                          |        | Description |            |              | 12           |
| EIGRP   | 10.2.2.2                                     |                 |             | 64001       |           |          | Enabled        |                         |                          |        |             |            |              | /            |
| RIP   |  |                 |             |             |           |          |                |                         |                          |        |             |            |              |              |
| Policy Based Routing                                    |  |                 |             |             |           |          |                |                         |                          |        |             |            |              |              |
| ✓ BGP   |  |                 |             |             |           |          |                |                         |                          |        |             |            |              |              |
| IPv4  |  |                 |             |             |           |          |                |                         |                          |        |             |            |              |              |

Immagine 19. Salvataggio della configurazione BGP

#### Passaggio 11. Ripetere la procedura con il secondo firewall.

| Firewall Manageme<br>Devices / Secure Firewall Ro                      | nt Center Overv                                       | ew Analysis | Policies     | Devices   | Objects  | Integration    |                 |                          | Deploy | ۹ ۽         | ¢ 0 | admin ~ doubt SEC | URE  |
|--|---|-------------|--------------|-----------|----------|----------------|-----------------|--------------------------|--------|-------------|-----|-------------------|------|
| FTD-2<br>Cisco Firepower Threat Defense fo<br>Device Routing Interface | r VMware<br>ces Inline Sets DHI                       | CP VTEP     |              |           |          |                |                 |                          |        |             |     | Save              | ncel |
| Manage Virtual Routers<br>Global •                                     | Enable IPv4: 🗹<br>AS Number 64001<br>General Neighbor | Add Aggre   | gate Address | Filtering | Networks | Redistribution | Route Injection |                          |        |             |     |                   |      |
| ECMP<br>BFD  |   |             |              |           |          |                |                 |                          |        |             |     | + A               | dd   |
| OSPF<br>OSPFv3   | 10.1.1.1  |             | 64000        | umber     |          | Enabled        |                 | Remote Private AS Number |        | Description | 1   | /                 | Ŧ    |
| RIP<br>Policy Based Routing  |   |             |              |           |          |                |                 |                          |        |             |     |                   |      |
| ✓ BGP<br>IPv4<br>IPv6  |   |             |              |           |          |                |                 |                          |        |             |     |                   |      |

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 | show running-config interface - Loopback1 |  |  |  |  |  |  |
| interfaccia Loopback1                     | interfaccia Loopback1                     |  |  |  |  |  |  |

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

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

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

## 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).