Configure eBGP with Loopback Interface on Secure Firewall

Contents

Introduction	
Prerequisites	
Requirements	
Components Used	
Background Information	
eBGP Configuration with a Loopback Interface	
Scenario	
Network Diagram	
Loopback Configuration	
Static Route Configuration	
BGP Configuration	
Verify	
Troubleshooting	

Introduction

This document describes how to configure eBGP using a Loopback interface on the Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recommends that you have knowledge of this topic:

• BGP protocol

Loopback interface support for BGP was introduced in version 7.4.0, which is the minimum version required for Secure Firewall Management Center and Cisco Secure Firepower Threat Defense.

Components Used

- Secure Firewall Management Center for VMware version 7.4.1
- 2 Cisco Secure Firepower Threat Defense for 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) standardized path-vector routing protocol that provides scalability, flexibility, and network stability. The BGP session between two peers with the same Autonomous System (AS) is called Internal BGP (iBGP). A BGP session between two peers with different Autonomous Systems (AS) is called External BGP (eBGP).

Typically, the peer relationship is established with the IP address of the interface closest to the peer, however, the use of a Loopback interface to establish the BGP session is useful since it not bring down the BGP session when there are multiple paths between BGP peers.

Note: The process describes the use of a Loopkack for an eBGP peer, however, is the same process for an iBGP peer so it can be used as a reference.

eBGP Configuration with a Loopback Interface

Scenario

In this configuration, Firewall SFTD-1 has a Loopback interface with the IP address 10.1.1.1/32, and the AS 64000, the Firewall SFTD-2 has a Loopback interface with the IP address 10.2.2.2/32 and the AS 64001. Both Firewalls use their outside interface to reach the Loopback interface of the other Firewall (in this scenario, the outside interface is preconfigured on both Firewalls).

Network Diagram

This document uses this network setup:



Image 1. Diagram of Escenario

Loopback Configuration

Step 1. Click **Devices** > **Device Management**, then select the device where you want to configure the Loopback.

Step 2. Click Interfaces > All Interfaces.

Step 3. Click Add Interface > Loopback Interface.

Firewall Management Cente Devices / Secure Firewall Interfaces	CVerview	Analysis Po	olicies Devices	Objects Integration	De	rploy Q 🛱	0	idmin ~ cisco SECURE	
FTD-1 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP									
All Interfaces Virtual Tunnels					Q. Search by name		Sync Devic	e Add Interfaces * Sub Interface	
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual	Redundant Interface Rridge Group Interface	
Management0/0	management	Physical				Disabled	Global	Virtual Tunnel Interface	
GigabitEthernet0/0	outside	Physical			10.10.10.1/24(Static)	Disabled	Global	VNI Interface	
GigabitEthemet0/1		Physical				Disabled		/	
GigabitEthernet0/2		Physical				Disabled		/	
GigabitEthernet0/3		Physical				Disabled		/	

Image 2. Add Interface Loopback

Step 4. In the **General** section, configure the name of the Loopback, check the **Enabled** box, and configure the **Loopback ID**.



Step 5. In the **IPv4** section, select the **Use Static IP** option in the **IP Type** section, configure the Loopback IP, then click **OK** to save the changes.



Image 5. Save the Loopback Interface Configuration

Step 7. Repeat the process with the second Firewall.

Firewall Management Cente Devices / Secure Firewall Interfaces	r Overview	Analysis Po	olicies Devices	Objects Integration	Dep	oloy Q 🗘	admin ∨ diado cisce cisce	SECURE
TD-2 Save Cancel Use 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	ي.⊲
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	Looback2	Loopback			10.2.2.2/32(Static)	Disabled	Global	11

Image 6. Loopback Interface Configuration on peer

Static Route Configuration

A static route must be configured to ensure the remote peer address (Loopback) used for peering is reachable through the desired interface.

Step 1. Click **Devices** > **Device Management**, then select the device you want to configure the static route.

Step 2. Click **Routing** > **Manage Virtual Routers** > **Static Route**, then click **Add Route**.

Firewall Management Ce Devices / Secure Firewall Routing	overview	Analysis Policies	Devices Objects	Integration		Deploy Q	æ linetine secure
FTD-1 Cisco Firepower Threat Defense for VMwa Device Routing Interfaces	Inline Sets DHCP	VTEP					Save Cancel
Manage Virtual Routers							+ Add Route
Global 💌 N	etwork 🔺	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Virtual Router Properties	IPv4 Routes						
ECMP	/ IPv6 Routes						
BFD							
OSPF							
OSPFv3							
EIGRP							
Policy Based Routing							
∨ BGP							
IPv4							
IPv6							
Static Route							
✓ Multicast Routing							
IGMP							
PIM							
Multicast Routes							
Multicast Boundary Filter							
General Settings							
BGP						é na Ca	

Image 7. Add New Static Route

Step 3. Check the IPv4 option for **Type**. Select the physical interface used to reach the Loopback of the remote peer in the **Interface** option, and then specify the next hop to reach the Loopback on the **Gateway** section.

Type: IPv4	O IPv6	
Interface*		
outside	Ŧ	
(Interface starting with this	icon 🐔 signifie	s it is available for route leak)
Available Network C	+	Selected Network
Q, Search		Add
anv-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 i	Route
Route Tracking:	
· · · · · ·]+



Step 4. Click the icon (+) next to the **Available Network** section.

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 de	fault Route)	
Route Tracking:		
	• +	
		Cancel

Image 9. Add New Network Object

Step 5. Configure a name for reference and the IP of the Looback of the remote peer and Save.

0

New Network Object

Name			
Loopback-FTD2			
Description			
Network			
Host O Range	 Network 	O FQDN	
10.2.2.2			
Allow Overrides			
		Cancel	Save

?

Image 10. Configure Network Destination In the Static Route

Step 6. Search the new object created in the search bar, select it, then click Add, and then click OK.

Type: IPv4 O IPv6 Interface* (Interface starting with this icon signification)] gnifies it is availat	ble for route leak)
Available Network C - Q, Loopback-FTD2 X Loopback-FTD2	Add	Selected Network 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

Image 11. Configure Next Hop in Static Route

Step 7. Click Save.

Ø

Firewall Management Devices / Secure Firewall Routing	Center Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ ¢ (admin ~ dui	SECURE
FTD-1 Cisco Firepower Threat Defense for VI Device Routing Interfaces	Mware Inline Sets DHCP	VTEP							You have unsav	ed changes Save	Cancel
Manage Virtual Routers										+ 4	dd Route
Global 🔻	Network +	Interface		Leaked fr Router	om Virtual	Gateway	Tunneled	Metric	Tra	cked	
Virtual Router Properties	▼ IPv4 Routes										
ECMP	Loopback-FTD2	outside		Global		10.10.10.2	false	1			11
BFD	▼ IPv6 Routes										
OSPFv3											
EIGRP											
RIP											
Policy Based Routing											
∼ BGP											
IPv4											
IPv6											
Static Route											

Image 12. Save the Static Route Interface Configuration

Step 8. Repeat the process with the second Firewall.

Firewall Management Devices / Secure Firewall Routi	Center Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🌣 🔘 admin 🗸 👘 secure
FTD-2 Cisco Firepower Threat Defense for V Device Routing Interfaces	Mware s Inline Sets DHCP	VTEP					Save Cancel
Manage Virtual Routers							+ Add Route
Global v	Network +	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Virtual Router Properties	▼ IPv4 Routes						
ECMP	Loopback-FTD1	outside	Global	10.10.10.1	false	1	/1
OSPF	▼ IPv6 Routes						
OSPFv3							
EIGRP							
RIP Policy Based Pouting							
✓ BGP							
IPv4							
IPv6							
Static Route							

Image 13. Configure Static Route on Peer

BGP Configuration

Step 1. Click **Devices** > **Device Management**, and select the device you want to enable BGP.

Step 2. Click **Routing** > **Manage Virtual Routers** > **General Settings**, and then click **BGP**.

Step 3. Check the **Enable BGP** box, then configure the local AS of the Firewall into the **AS Number** section.

Firewall Management Devices / Secure Firewall Routin	Center Overview Analysis Policies Devices Objects	Integration	
FTD-1 Cisco Firepower Threat Defense for VI Device Routing Interfaces	Mware Inline Sets DHCP VTEP		
Manage Virtual Routers Global Virtual Router Properties ECMP BFD OSPF OSPFv3 FIGPP	Enable BGP: AS Number* 64000 Coverride BGP general settings router-id address: Router Id Automatic 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
IGMP	Enforce the first AS is peer's AS for EBGP routes	Yes	Address tracking
PIM	Use dot notation for AS number	No	Delay interval
Multicast Routes	Aggregate Timer	30	
Multicast Boundary Filter			
General Settings	Best Path Selection	1	Graceful Restart
RGP	Default local preference	100	Restart time
b di la			

Image 14. Enable BGP Globally

Step 4. Save the changes by clicking the **Save** button.

Firewall Managemen	nt Center Overview Analysis Policies Devices Objects In	itegration	Deploy	Q ☆ Ø admin ∨ thethe SECURE
FTD-1 Cisco Firepower Threat Defense for Device Routing Interfac	r VMware es Inline Sets DHCP VTEP			You have unsaved changes Save Cancel
Manage Virtual Routers Global • Virtual Router Properties ECMP BFD OSPF OSPFFv3 FICRP	Enable BGP: AS Number* 64000 Override BGP general settings router-id address: Router Id Automatic 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	Use TCP path MTU discovery	Yes		
Static Route				

Image 15. Save the BGP Enable Change

Step 5. In the Manage Virtual Routers section, go to the BGP option, and then click IPv4.

Step 6. Check the **Enable IPv4** box, then click **Neighbor**, and then click + **Add**.

Firewall Managemer Devices / Secure Firewall Ro	nt Center ov	verview Ana	ysis Policie	s Devices	Objects	Integration			Deploy	۹	🗘 🕜 ədmi	a 🗠 🔤 diado SECU	JRE
FTD-1 Cisco Firepower Threat Defense for Device Routing Interfac	VMware es Inline Sets	DHCP VTEP								You hav	e unsaved change	Save Can	icel
Manage Virtual Routers Global v Virtual Router Properties ECMP	Enable IPv4: AS Number 64000 General Neigh	hbor Add Ag	gregate Address	Filtering	Networks	Redistribution	Route Injection					+ Ad	id b
BFD OSPF	Address		Remote A	S Number		Address Family		Remote Private AS Number		Descrip	tion		Τ.
OSPFv3						No	records to display						
EIGRP													
Policy Based Routing													
IPv4													
IPv6													
Static Route V Multicast Routing													

Image 16. Add a New BGP Peer

Step 7. Configure the IP address of the remote peer in the **IP Address** section, then configure the AS of the remote peer in the **Remote AS** section, and check the **Enable address** box.

0

Step 8. Select the local interface Loopback in the Update Source section.

Edit Neighbor

P Address*		Enabled address					
10.2.2.2		Shutdown administratively					
Remote AS*	note AS* Confoure oraceful restart						
64001		Graceful restart(failover/spanned mode)					
(1-4294967295 or 1.0-65535.65535	6						
BFD Fallover	De	escription					
none v	3 0						
Update Source:							
Loopback1 v	٦.						
Filtering Routes T	Imers	Advanced Migration					
Filtering Routes Routes T Incoming	imers	Advanced Migration Outgoing Access List					
Filtering Routes T Incoming Access List	imers	Advanced Migration Outgoing Access List					
Filtering Routes T Incoming Access List	imers	Advanced Migration Outgoing Access List					
Filtering Routes T Incoming Access List Route Map) +] +	Advanced Migration Outgoing Access List Route Map +					
Filtering Routes Routes T Incoming Access List Route Map) +] +] +	Advanced Migration Outgoing Access List					
Filtering Routes T Incoming Access List Route Map) +] +] +	Advanced Migration Outgoing Access List					
Filtering Routes Routes T Incoming Access List Route Map Prefix List AS path filter) +] +] +] +	Advanced Migration Outgoing Access List					

Image 17. Basic BGP Peer Parameters

Note: The **Update Source** option enables the **neighbor update-source** command, used to permit any operational interface (including Loopbacks). This command can be specified to establish TCP



Step 9. Click Advanced, then configure the number 2 in the TTL Hops option, and click OK.

Edit Neighbor	e
none •	
Update Source:	
Loopback1 v	
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

Image 18. Configure the TTLs Hop Number

Note: The **TTL Hops** option enables the **ebgp-multihop** command, used to change the TTL value to allow the packet to reach the external BGP peer that is not directly connected or has an interface other than the directly connected interface.

Step 10. Click Save and deploy the changes.

Firewall Managemen Devices / Secure Firewall Ro	nt Center Overv	iew Analysis	Policies	Devices	Objects	Integration			Deploy	۹	° 0	admin ~	SECURE
FTD-1 Cisco Firepower Threat Defense for	r VMware									You have	unsaved	changes Save	Cancel
Device Routing Interfac	es Inline Sets DH Enable IPv4: 🗹 AS Number 64000 General Neighbor	CP VTEP	ate Address	Filtering	Networks	Redistribution	Route Injection						
ECMP													+ Add
BFD OSPF	Address		Remote AS N	umber		Address Family		Remote Private AS Number		Descripti	on		
OSPFv3 EIGRP	10.2.2.2		64001			Enabled							/1
RIP Policy Based Routing													
IPv4													

Image 19. Save the BGP Configuration

Step 11. Repeat the process with the second Firewall.

Firewall Manageme Devices / Secure Firewall R	ent Center Overview	w Analysis	Policies Dev	ces Objects	Integration			Deploy	٩ \$	8 0	admin ~ disto	SECURE
FTD-2 Cisco Firepower Threat Defense fo Device Routing Interfa	or VMware ces Inline Sets DHCP	VTEP									Save	Cancel
Manage Virtual Routers Global Virtual Router Properties ECMP	Enable IPv4: 🗹 AS Number 64001 General Neighbor	Add Aggregate	e Address Filterin	g Networks	Redistribution	Route Injection					4	+ Add
BFD OSPF	Address	1	Remote AS Number		Address Family		Remote Private AS Number		Description			
OSPFv3	10.1.1.1		64000		Enabled							/1
RIP Policy Based Routing V BGP												
IPv4 IPv6												

Image 20. Configure BGP on Peer

Verify

Step 1. Verify the Loopback and static route configuration, then check the connectivity between BGP peers with a ping test.

show running-config interface interface_name

show running-config route

show destination_ip

SFTD-1	SFTD-2
show running-config interface Loopback1	show running-config interface Loopback1
interface Loopback1	interface Loopback1
nameif Loopback1	nameif Looback2

ip address 10.1.1.1 255.255.255.255	ip address 10.2.2.2 255.255.255.255
show running-config route	show running-config route
route outside 10.2.2.2 255.255.255.255 10.10.10.2 1	route outside 10.1.1.1 255.255.255.255 10.10.10.1 1
ping 10.2.2.2	ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:	Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
11111	11111
Success rate is 100 percent (5/5), round-trip $min/avg/max = 1/1/1 ms$	Success rate is 100 percent (5/5), round-trip $min/avg/max = 1/1/1 ms$

Step 2. Verify the BGP configuration, then ensure that the BGP peering is established.

show running-config router bgp

show bgp neighbors

show bgp summary

SFTD-1	SFTD-2
show running-config router bgp	show running-config router bgp
router bgp 64000	router bgp 64001
bgp log-neighbor-changes	bgp log-neighbor-changes
bgp router-id vrf auto-assign	bgp router-id vrf auto-assign
address-family ipv4 unicast	address-family ipv4 unicast
neighbor 10.2.2.2 remote-as 64001	neighbor 10.1.1.1 remote-as 64000
neighbor 10.2.2.2 ebgp-multihop 2	neighbor 10.1.1.1 ebgp-multihop 2
neighbor 10.2.2.2 transport path-mtu-discovery disable	neighbor 10.1.1.1 transport path-mtu-discovery disable
neighbor 10.2.2.2 update-source Loopback1	neighbor 10.1.1.1 update-source Looback2
neighbor 10.2.2.2 activate	neighbor 10.1.1.1 activate
no auto-summary	no auto-summary
no synchronization	no synchronization
exit-address-family	exit-address-family
!	!

show bgp neighbors i BGP	show bgp neighbors i BGP							
BGP neighbor is 10.2.2.2 , vrf single_vf, remote AS 64001, external link	BGP neighbor is 10.1.1.1 , vrf single_vf, remote AS 64000, external link							
BGP version 4, remote router ID 10.2.2.2	BGP version 4, remote router ID 10.1.1.1							
BGP state = Established , up for 1d15h	BGP state = Established , up for 1d16h							
BGP table version 7, neighbor version 7/0	BGP table version 1, neighbor version 1/0							
External BGP neighbor may be up to 2 hops away.	External BGP neighbor may be up to 2 hops away.							
show bgp summary	show bgp summary							
BGP router identifier 10.1.1.1, local AS number 64000	BGP router identifier 10.2.2.2, local AS number 64001							
BGP table version is 7, main routing table version 7	BGP table version is 1, main routing table version 1							
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd	Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd							
10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0	10.1.1.1 4 64000 2168 2173 1 0 0 1d16h 0							

Troubleshooting

If you are experiencing any issues during the process, please review this article:

<u>Border Gateway Protocol (BGP)</u>