# Configurar o eBGP com interface de loopback no firewall seguro

# Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configuração do eBGP com uma interface de loopback
Cenário
Diagrama de Rede
Configuração de loopback
Configuração de rota estática
Configuração de BGP
Verificar
Troubleshooting

## Introdução

Este documento descreve como configurar o eBGP usando uma interface de loopback no Cisco Secure Firewall.

## Pré-requisitos

## Requisitos

A Cisco recomenda ter conhecimento deste tópico:

• protocolo BGP

O suporte à interface de loopback para BGP foi introduzido na versão 7.4.0, que é a versão mínima necessária para o Secure Firewall Management Center e o Cisco Secure Firepower Threat Defense.

## **Componentes Utilizados**

- Secure Firewall Management Center for VMware versão 7.4.1
- 2 Cisco Secure Firepower Threat Defense for VMware versão 7.4.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

O BGP (Border Gateway Protocol) é um protocolo de roteamento de vetor de caminho padronizado EGP (Exterior Gateway Protocol) que fornece escalabilidade, flexibilidade e estabilidade de rede. A sessão de BGP entre dois peers com o mesmo Sistema Autônomo (AS) é chamada de BGP Interno (iBGP). Uma sessão de BGP entre dois peers com sistemas autônomos (AS) diferentes é chamada de BGP externo (eBGP).

Normalmente, a relação de peer é estabelecida com o endereço IP da interface mais próxima do peer. No entanto, o uso de uma interface de loopback para estabelecer a sessão BGP é útil, já que não desativa a sessão BGP quando há vários caminhos entre os peers BGP.

Observação: o processo descreve o uso de um Loopback para um peer eBGP, no entanto, é o mesmo processo para um peer iBGP para que possa ser usado como referência.

# Configuração do eBGP com uma interface de loopback

## Cenário

Nessa configuração, o Firewall SFTD-1 tem uma interface de Loopback com o endereço IP 10.1.1.1/32 e o AS 64000, o Firewall SFTD-2 tem uma interface de Loopback com o endereço IP 10.2.2.2/32 e o AS 64001. Ambos os firewalls usam sua interface externa para acessar a interface de loopback do outro firewall (nesse cenário, a interface externa é pré-configurada em ambos os firewalls).

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Imagem 1. Diagrama de Cenário

Configuração de loopback

Etapa 1. Clique em Devices > Device Management e, em seguida, selecione o dispositivo onde deseja configurar o Loopback.

Etapa 2. Clique em Interfaces > Todas as interfaces.

Etapa 3. Clique em Adicionar interface > Interface de loopback.

Firewall Management Center Devices / Secure Firewall Interfaces	er Overview	Analysis Po	licies Devices	Objects Integration	D	eploy Q 🛱	<b>0</b> a	dmin v dhale 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 Device	Add Interfaces   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
GigabitEthemet0/1		Physical				Disabled		/
GigabitEthernet0/2		Physical				Disabled		1
GigabitEthernet0/3		Physical				Disabled		/

Imagem 2. Adicionar Loopback de Interface

Etapa 4. Na seção Geral, configure o nome do Loopback, marque a caixa Habilitado e configure o ID de Loopback.

# Add Loopback Interface

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

?

Imagem 3. Configuração básica de interface de loopback

Etapa 5. Na seção IPv4, selecione a opção Usar IP estático na seção Tipo de IP, configure o IP de loopback e clique em OK para salvar as alterações.

## Edit Loopback Interface



e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

Imagem 4. Configuração de endereço IP de loopback

#### Etapa 6. Click Save.

Firewall Management Cente Devices / Secure Firewall Interfaces	Overview	Analysis Po	olicies Devices	Objects	Integration		Deplo	y Q 🌣	admin v	eisco SECURE
FTD-1 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP										
All Interfaces Virtual Tunnels						Q Sear	ch by name	S	ync Device Add	i Interfaces 🔻
Interface	Logical Name	Туре	Security Zones	MAC Add	ress (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		/
Loopback1	Loopback1	Loopback				10.1.1.1/32(Static)		Disabled	Global	11

Imagem 5. Salvar a configuração da interface de loopback

#### Passo 7. Repita o processo com o segundo Firewall.

0

FTD-2   Cisco Firepower Threat Defense for VMware     Device   Routing   Interface   Ntuterface     Logical Name     Type   Security Zones   MAC Address (Active/Standby)   IP Address   Path Monitoring   Virtual Router   Interface   Logical Name   Type   Security Zones   MAC Address (Active/Standby)   IP Address   Path Monitoring   Virtual Router   Interface	Firewall Management Center Devices / Secure Firewall Interfaces	Overview A	Analysis Pol	icies Devices	Objects Integration	Depl	oy Q 🜣	admin v diadu	SECURE
All Interface       Logical Name       Type       Security Zones       MAC Address (Active/Standby)       IP Address       Path Monitoring       Virtual Router         • Management0/0       management       Physical       Disabled       Global       C         • GigabitEthernet0/0       outside       Physical       10.10.10.2/24(Static)       Disabled       Global       C         • GigabitEthernet0/1       Physical       Disabled       Global       C       C         • GigabitEthernet0/1       Physical       Disabled       C       C         • GigabitEthernet0/2       Physical       Disabled       C       C	TD-2 sco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP								
Interface         Logical Name         Type         Security Zones         MAC Address (Active/Standby)         IP Address         Path Monitoring         Virtual Router           • Management(0/0         management         Physical         -         Disabled         Global         <	All Interfaces Virtual Tunnels					Q. Search by name	S	Add Inte	rfaces ¥
Management()/p     management     Physical     Disabled     Global     Q.<       • GigabitEthernet()/p     • outside     Physical     10.10.10.2/24(Static)     Disabled     Global     ////////////////////////////////////	Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
• GigabitEthernet0/0       outside       Physical       10.10.2/24(Static)       Disabled       Global       /         I GigabitEthernet0/1       Physical       Disabled       Disabled       /         I GigabitEthernet0/2       Physical       Disabled       /       /	Management0/0	management	Physical				Disabled	Global	ର ⊲:
Image: Construction         Physical         Disabled         Image: Construction         Image: Con	GigabitEthernet0/0	outside	Physical			10.10.10.2/24(Static)	Disabled	Global	/
CinabiliFithemet0/2 Physical Disabled	GigabitEthernet0/1		Physical				Disabled		/
A allocation and a second	GigabitEthernet0/2		Physical				Disabled		/
GigabitEthernet0/3 Physical Disabled	GigabitEthernet0/3		Physical				Disabled		/
Loopback1     Looback2     Loopback     10.2.2.2/32(Static)     Disabled     Global	Loopback1	Looback2	Loopback			10.2.2.2/32(Static)	Disabled	Global	11

Imagem 6. Configuração de Interface de Loopback no par

#### Configuração de rota estática

Uma rota estática deve ser configurada para garantir que o endereço de peer remoto (loopback) usado para peering esteja acessível através da interface desejada.

Etapa 1. Clique em Devices > Device Management e selecione o dispositivo para o qual deseja configurar a rota estática.

Etapa 2. Clique em Roteamento > Gerenciar roteadores virtuais > Rota estática e clique em Adicionar rota.

Firewall Management Ce Devices / Secure Firewall Routing	overview	Analysis Policies	Devices Objects	Integration		Deploy Q	수 🕜 admin ~ ethods SECURE
FTD-1 Cisco Firepower Threat Defense for VMwa	ire	1/750					Save Cancel
Manage Virtual Routers	letwork +	Interface	Leaked from Virtual	Gateway	Tunneled	Metric	+ Add Route
Virtual Router Properties	IPv4 Routes  IPv6 Routes						
BFD OSPF							
EIGRP RIP							
Policy Based Routing V BGP							
IPv6 Static Route							
<ul> <li>Multicast Routing</li> <li>IGMP</li> </ul>							
PIM Multicast Routes Multicast Boundary Filter							
General Settings BGP							

Imagem 7. Adicionar nova rota estática

Etapa 3. Verifique a opção IPv4 para Type. Selecione a interface física usada para acessar o Loopback do peer remoto na opção Interface e, em seguida, especifique o próximo salto para acessar o Loopback na seção Gateway.

Type:      IPv4      IPv6	1
Interface*	
outside v	
(Interface starting with this icon Ssignif	es it is available for route leak)
Available Network C +	Selected Network
Q, Search	Add
any-ipv4	
IPv4-Benchmark-Tests	
IPv4-Link-Local	
IPv4-Multicast	
IPv4-Private-10.0.0-8	
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:	_
	+

Imagem 8. Configuração de rota estática

Etapa 4. Clique no ícone (+) próximo à seção Rede disponível.

Edit Static Route Configuration

Type:	IPv4	O IPv6
Interface*		
outside		•
(Interface starting	g with this	icon Signifi
Available Networ	k C	+
Q, Search		
any-ipv4		
IPv4-Benchma	rk-Tests	
IPv4-Link-Loca	d	
IPv4-Multicast		
IPv4-Private-10	0.0.0.0-8	
IPv4-Private-1	72.16.0.0-	12

Ensure that egress virtualrouter has route to that destination

Gateway		
10.10.10.2	• +	
Metric:		
1		
(1 - 254)		
Tunneled: 🗌 (Used or	ily for default Route)	
Route Tracking:		
	* +	
		Cancel OK

Imagem 9. Adicionar novo objeto de rede

Etapa 5. Configure um nome para referência e o IP do Loopback do peer remoto e Save.

0

# New Network Object

Name			
Loopback-FTD2			
Description			
Network			
Host O Range	<ul> <li>Network</li> </ul>	O FQDN	
10.2.2.2			
Allow Overrides			
		Cancel	Save

Imagem 10. Configure o destino da rede na rota estática

Etapa 6. Pesquise o novo objeto criado na barra de pesquisa, selecione-o, clique em Adicionar e em OK.

3

Type:  IPv4 O IPv6 Interface*  Outside  (Interface starting with this icon signature)	iffes it is available for route	leak)
Available Network C + Q, Loopback-FTD2 X Loopback-FTD2	Add Loopback-	twork FTD2

Ensure that egress virtualrouter has route to that destination

#### Gateway

10.10.10.2	• +	
Metric:		
1		
(1 - 254)		
Tunneled: [] (Used on	ly for default Route)	
Route Tracking:		
	• +	
		Cancel O

Imagem 11. Configurar o próximo salto na rota estática

Passo 7. Click Save.

ø

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

Imagem 12. Salvar a configuração da interface de rota estática

#### Etapa 8. Repita o processo com o segundo Firewall.

Firewall Management Cen Devices / Secure Firewall Routing	iter Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🌣 🚱 admin ~ 🖏 admin secure
FTD-2 Cisco Firepower Threat Defense for VMware Device Routing Interfaces I	e nline Sets DHCP	VTEP					Save Cancel
Manage Virtual Routers							+ Add Route
Global v Net	twork 🔺	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Virtual Router Properties	IPv4 Routes						
ECMP Loo	opback-FTD1	outside	Global	10.10.10.1	false	1	/1
OSPF V	IPv6 Routes						
OSPFv3							
EIGRP							
RIP Policy Based Routing							
✓ BGP							
IPv4							
IPv6							
Static Route							

Imagem 13. Configurar Rota Estática no Peer

#### Configuração de BGP

Etapa 1. Clique em Devices > Device Management e selecione o dispositivo que deseja habilitar o BGP.

Etapa 2. Clique em Roteamento > Gerenciar roteadores virtuais > Configurações gerais e clique em BGP.

Etapa 3. Marque a caixa Enable BGP e configure o AS local do Firewall na seção AS Number.

Firewall Management Devices / Secure Firewall Routi	Center Overview Analysis Policies Devices Objects Ir	ntegration	
FTD-1 Cisco Firepower Threat Defense for V Device Routing Interfaces	Mware Inline Sets DHCP VTEP		
Manage Virtual Routers Global  Virtual Router Properties ECMP BFD OSPF OSPFv3 EIGPP	Enable BGP: AS Number* 64000 Cverride BGP general settings router-id address: Router Id Automatic IP Address*		
RIP	General		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		30	
Multicast Boundary Filter	Aggregate filler	30	
General Settings	Best Path Selection	1	Graceful Restart
BGP	Default local preference	100	Restart time

Imagem 14. Ativar o BGP globalmente

#### Etapa 4. Salve as alterações clicando no botão Save.

Firewall Managemen Devices / Secure Firewall Rou	t Center Overview Analysis Policies Devices Objects	Integration	Deploy	Q, IC @ admin ~ "hells SECURE
FTD-1 Cisco Firepower Threat Defense for Device Routing Interface	VMware is Inline Sets DHCP VTEP			You have unsaved changes Save Cancel
Manage Virtual Routers Global Virtual Router Properties ECMP BFD OSPF OSPFv3 EICPO	Enable BGP: AS Number* 64000 (1-4294967295 or 1.0-65535.65535) Override BGP general settings router~ld address: Router Id Automatic • IP Address*			
RIP	General	Neight	bor Timers	1
Policy Based Routing	Scanning Interval	60 Keepali	ve Interval	60
∼ BGP	Number of AS numbers in AS_PATH attribute of received routes	None Hold tin	ne	180
IPv4	Log Neighbor Changes	Yes Min hol	d time	0
IPv6 Static Route	Use TCP path MTU discovery	Yes		



Etapa 5. Na seção Manage Virtual Routers, vá para a opção BGP e clique em IPv4.

Etapa 6. Marque a caixa Enable IPv4, clique em Neighbor e clique em + Add.

Firewall Management Devices / Secure Firewall Routing	Center Overview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹	🗘 🕜 admin 🗸	cisco SECURE
FTD-1 Cisco Firepower Threat Defense for Vi	Mware									You hav	e unsaved changes	Save Cancel
Device Routing Interfaces	Inline Sets DHCP	VTEP										
Manage Virtual Routers Global	Enable IPv4: AS Number 64000 General Neighbor	Add Aggreg	ate Address	Filtering	Networks	Redistribution	Route Injection					
Virtual Router Properties												
BED												+ Add
OSPF	Address		Remote AS N	umber		Address Family		Remote Private AS Number		Descrip	tion	
OSPFv3						N	records to display					
EIGRP												
RIP												
Policy Based Routing												
Y BGP												
IPv4												
IPv6												
Static Route												
✓ Multicast Routing												

Imagem 16. Adicionar um Novo Par BGP

Passo 7. Configure o endereço IP do peer remoto na seção Endereço IP, configure o AS do peer remoto na seção AS Remoto e marque a caixa Ativar endereço.

0

Etapa 8. Selecione o loopback da interface local na seção Atualizar origem.

Edit Neighbor

IP Address*		Enabled address					
10.2.2.2		Shutdown administratively					
Remote AS*		Configure graceful restart					
64001	Graceful restart(fallover/spanned mode)						
(1-4294967295 or 1.0-65535.65535)							
BFD Fallover	De	Iscription					
none •							
Update Source:							
Loopbeck1 ·							
Filtering Routes Routes Tin	ners	Advanced Migration					
Filtering Routes Routes Tin	ners	Advanced Migration					
Filtering Routes Routes Tin	ners	Advanced Migration Outgoing					
Filtering Routes Routes Tin Incoming Access List	ners	Advanced Migration Outgoing Access List					
Filtering Routes Routes Tin Incoming Access List	+	Advanced Migration Outgoing Access List  +					
Filtering Routes Routes Tin Incoming Access List Route Map	+	Advanced Migration Outgoing Access List  Route Map					
Filtering Routes Routes Tin Incoming Access List Route Map	) + ) +	Advanced Migration Outgoing Access List  Route Map  +					
Filtering Routes Routes Tin Incoming Access List Route Map Prefix List	) + ) +	Advanced Migration Outgoing Access List					
Filtering Routes Routes Tin Incoming Access List Route Map Prefix List	+   +   +	Advanced Migration Outgoing Access List					
Filtering Routes Routes Tin Incoming Access List Route Map Prefix List AS path filter	) + ) + ) +	Advanced Migration Outgoing Access List					

Imagem 17. Parâmetros Básicos de Pares BGP

Not servação: a opção Update Source ativa o comando neighbor update-source, usado para

permitir qualquer interface operacional (incluindo loopbacks). Esse comando pode ser especificado para estabelecer conexões TCP.

Etapa 9. Clique em Avançado e configure o número 2 na opção Saltos TTL e clique em OK.

Edit Neighbor	0
none v	
Update Source:	
Loopbeck1 v	
Filtering Routes Routes Timers Advanced Migration	
Enable Authentication	
Enable Encryption	
0 v	
Password	
Confirm Password	
Send Community attribute to this neighbor	
<ul> <li>Use itself as next hop for this neighbor</li> </ul>	
Disable Connection Verification	
<ul> <li>Allow connections with neighbor that is not directly connected</li> </ul>	
<ul> <li>Limited number of TTL hops to neighbor</li> </ul>	
TTL Hops	
2	
(1-255)	
Use TCP path MTU discovery	
TCP Transport Mode	
Default •	
Weight	
	Cancel
magam 18. Captigurar o púmoro do colto TTL s	

Noservação: a opção TTL Hops habilita o comando ebgp-multihop , usado para alterar o valor TTL para permitir que o pacote acesse o par BGP externo que não está diretamente conectado ou tem uma interface diferente da interface diretamente conectada.

Etapa 10. Clique em Salvar e implante as alterações.

Firewall Managemen Devices / Secure Firewall Roo	t Center Overview	Analysis Policie	s Devices	Objects	Integration		Deploy	, Q	° 0	admin v	dialle SECURE
FTD-1 Cisco Firepower Threat Defense for Device Routing Interface	VMware as Inline Sets DHCP	VTEP						You	have unsaved	changes Save	Cancel
Manage Virtual Routers Global • Virtual Router Properties ECMP	Enable IPv4: AS Number 64000 General Neighbor	Add Aggregate Address	Filtering	Networks	Redistribution	Route Injection					+ Add
BFD OSPF	Address	Remote A	S Number		Address Family		Remote Private AS Number	Des	cription		
OSPFv3 EIGRP BIP	10.2.2.2	64001			Enabled						/1
Policy Based Routing ~ BGP IPv4											

Imagem 19. Salvar a configuração do BGP

#### Etapa 11. Repita o processo com o segundo Firewall.

Firewall Managemen Devices / Secure Firewall Ro	nt Center Overview	Analysis	Policies Devices	Objects	Integration			Deploy	۹	° 0	admin ~ dials SECURE
FTD-2 Cisco Firepower Threat Defense for Device Routing Interfac	r VMware es Inline Sets DHCP	VTEP									Save Cancel
Manage Virtual Routers Global 🗸	Enable IPv4: 🗹 AS Number 64001 General Neighbor	Add Aggregate A	Address Filtering	Networks	Redistribution	Route Injection					
ECMP BFD											+ Add
OSPF	Address	Re	mote AS Number		Address Family		Remote Private AS Number		Descriptio	n	
OSPFv3	10.1.1.1	64	000		Enabled						/1
EIGRP RIP Policy Based Routing											
∨ BGP IPv4											
IPv6											

Imagem 20. Configurar BGP no Peer

#### Verificar

Etapa 1. Verifique a configuração do Loopback e da rota estática e, em seguida, verifique a conectividade entre os peers BGP com um teste de ping.

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
rota externa 10.2.2.2 255.255.255.255 10.10.10.2 1	rota externa 10.1.1.1 255.255.255.255 10.10.10.1 1
ping 10.2.2.2	ping 10.1.1.1
Enviando Echos ICMP de 5.100 bytes para 10.2.2.2, o tempo limite é de 2 segundos:	Enviando Echos ICMP de 5.100 bytes para 10.1.1.1, o tempo limite é de 2 segundos:
	!!!!!
A taxa de sucesso é de 100% (5/5), round-trip min/avg/max = 1/1/1 ms	A taxa de sucesso é de 100% (5/5), round-trip min/avg/max = 1/1/1 ms

Etapa 2. Verifique a configuração do BGP e, em seguida, assegure-se de que o peering de BGP esteja estabelecido.

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 autoassign	bgp router-id vrf autoassign
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 ativate	neighbor 10.1.1.1 ativate
no autossummary	no autossummary
sem sincronização	sem sincronização
exit-address-family	exit-address-family
<u>!</u>	!
show bgp neighbors   i BGP	show bgp neighbors   i BGP
O vizinho BGP é 10.2.2.2, vrf single_vf, AS 64001 remoto, link externo	O vizinho BGP é 10.1.1.1, vrf single_vf, AS 64000 remoto, link externo
BGP versão 4, ID do roteador remoto 10.2.2.2	BGP versão 4, ID do roteador remoto 10.1.1.1
Estado de BGP = Estabelecido, para 1d15h	Estado de BGP = Estabelecido, para 1d16h
Tabela BGP versão 7, versão vizinha 7/0	Tabela BGP versão 1, versão vizinha 1/0
O vizinho BGP externo pode estar a até 2 saltos de distância.	O vizinho BGP externo pode estar a até 2 saltos de distância.
show bgp summary	show bgp summary
Identificador do roteador BGP 10.1.1.1, número AS local 64000	Identificador do roteador BGP 10.2.2.2, número AS local 64001
A versão da tabela de BGP é 7, a versão 7 da tabela de roteamento principal	A versão da tabela de BGP é 1, a versão da tabela de roteamento principal é 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

Se você tiver algum problema durante o processo, leia este artigo:

· BGP (Border Gateway Protocol)

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.