# Configureer eBGP met Loopback-interface op beveiligde firewall

# Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
eBGP-configuratie met een terugkoppelingsinterface
Scenario
Netwerkdiagram
Terugbelconfiguratie
Statische routeconfiguratie
BGP-configuratie
Verifiëren
Probleemoplossing

# Inleiding

Dit document beschrijft hoe u eBGP kunt configureren met behulp van een Loopback-interface in de Cisco Secure Firewall.

## Voorwaarden

## Vereisten

Cisco raadt u aan bekend te zijn met dit onderwerp:

BGP-protocol

Ondersteuning van Loopback-interface voor BGP is geïntroduceerd in versie 7.4.0, de minimumversie die vereist is voor Secure Firewall Management Center en Cisco Secure Firepower Threat Defence.

## Gebruikte componenten

- Secure Firewall Management Center voor VMware versie 7.4.1
- 2 Cisco Secure Firepower Threat Defence voor VMware versie 7.4.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrondinformatie

BGP is een gestandaardiseerd pad-vector routingprotocol (EGP) voor Exterior Gateway Protocol (BGP) dat schaalbaarheid, flexibiliteit en netwerkstabiliteit biedt. De BGP-sessie tussen twee peers met hetzelfde Autonomous System (AS) wordt Internal BGP (iBGP) genoemd. Een BGP-sessie tussen twee peers met verschillende Autonomous Systems (AS) wordt Externe BGP (eBGP) genoemd.

Meestal wordt de peer-relatie ingesteld met het IP-adres van de interface die het dichtst bij de peer staat, maar het gebruik van een Loopback-interface om de BGP-sessie op te zetten is nuttig omdat het de BGP-sessie niet omlaag brengt wanneer er meerdere paden zijn tussen BGP-peers.

Opmerking: Het proces beschrijft het gebruik van een Loopkack voor een eBGP-peer, maar het is hetzelfde proces voor een iBGP-peer, zodat het als referentie kan worden gebruikt.

# eBGP-configuratie met een terugkoppelingsinterface

## Scenario

In deze configuratie heeft Firewall SFTD-1 een Loopback-interface met het IP-adres 10.1.1.1/32 en het AS-64000, heeft de Firewall SFTD-2 een Loopback-interface met het IP-adres 10.2.2.2/32 en het AS-64001. Beide firewalls gebruiken hun buiteninterface om de Loopback-interface van de andere firewall te bereiken (in dit scenario is de buiteninterface op beide firewalls vooraf geconfigureerd).

## Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Afbeelding 1. Schema van het scenario

#### Terugbelconfiguratie

Stap 1. Klik op Apparaten > Apparaatbeheer en selecteer vervolgens het apparaat waarop u de terugbelverbinding wilt configureren.

Stap 2. Klik op Interfaces > Alle interfaces.

Stap 3. Klik op Add Interface > Loopback Interface.

SECURE
Cancel
rfaces 🔻
nface
nterface
nace
/
/
/
rface interf face

Afbeelding 2. Interfaceloopback toevoegen

Stap 4. In de Algemene sectie, vorm de naam van Loopback, controleer het Toegelaten vakje, en vorm Loopback ID.

# Add Loopback Interface

Looback1			
Enabled			
Loopback ID:	*		
1			
(1-1024)			
Description			

?

Afbeelding 3. Basisconfiguratie van loopback-interface

Stap 5. Selecteer in het gedeelte IPv4 de optie Statische IP gebruiken in het gedeelte IP-type, configureer de loopback-IP en klik vervolgens op OK om de wijzigingen op te slaan.

## Edit Loopback Interface



e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

Afbeelding 4. Configuratie van IP-adres voor terugbellen

#### Stap 6. Klik op Save (Opslaan).

Firewall Management Cente Devices / Secure Firewall Interfaces	f Overview	Analysis Po	licies Devices	Objects Integration	Dep	loy Q 🔅	admin v alkali	SECURE
FTD-1 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inlin	ne Sets DHCP V	TEP				You have un	saved changes Save	Cancel
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		/
Loopback1	Loopback1	Loopback			10.1.1.1/32(Static)	Disabled	Global	/1

Afbeelding 5. De configuratie van de Loopback-interface opslaan

#### Stap 7. Herhaal het proces met de tweede firewall.

Firewall Management Cente Devices / Secure Firewall Interfaces	r Overview	Analysis Po	licies Devices	Objects Integration		Deploy Q 🔅		SECURE
FTD-2 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Initir	ie Sets DHCP V	TEP						Cancel
All Interfaces Virtual Tunnels					Q. Search by na	ime	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	≎ ک
GigabitEthemet0/0	outside	Physical			10.10.10.2/24(Static)	Disabled	Global	/
GigabitEthemet0/1		Physical				Disabled		/
GigabitEthemet0/2		Physical				Disabled		/
GigabitEthernet0/3		Physical				Disabled		1
Loopback1	Looback2	Loopback			10.2.2.2/32(Static)	Disabled	Global	11

Afbeelding 6. Configuratie van Loopback-interface op peer

#### Statische routeconfiguratie

Een statische route moet worden geconfigureerd om ervoor te zorgen dat het externe peer-adres (Loopback) dat wordt gebruikt voor peering bereikbaar is via de gewenste interface.

Stap 1. Klik op Apparaten > Apparaatbeheer en selecteer vervolgens het apparaat dat u de statische route wilt configureren.

Stap 2. Klik op Routing > Virtual Routers beheren > Static Route en klik vervolgens op Add Route.

Firewall Management Devices / Secure Firewall Routin	Center Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🔅 🕐 admin 🗸 👘 SECURE
FTD-1 Cisco Firepower Threat Defense for VM Device Routing Interfaces	/ware Inline Sets DHCP	VTEP					Save Cancel
Manage Virtual Routers							+ Add Route
Global 🔻	Network +	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Virtual Router Properties	▶ IPv4 Routes						
ECMP	▼ IPv6 Routes						
BFD							
OSPF							
EIGRP							
RIP							
Policy Based Routing							
∨ BGP							
IPv4							
IPv6							
Static Route							
Mulacast Routing     IGMP							
PIM							
Multicast Routes							
Multicast Boundary Filter							
General Settings							
BGP						2 m	

Afbeelding 7. Nieuwe statische route toevoegen

Stap 3. Controleer IPv4 op Type. Selecteer de fysieke interface die wordt gebruikt om de Loopback van de externe peer in de interfaceoptie te bereiken en specificeer vervolgens de volgende hop om de Loopback in de sectie Gateway te bereiken.

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 i	Route
Route Tracking:	
· · · · · ·	]+

Afbeelding 8. Statische routeconfiguratie



Edit Static Route Configuration

Type: 💿 IPv4 🔿	) IPv6	
Interface*		
outside		
(Interface starting with this ico	n 🕾 signifi	hes 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 Route)	
Route Tracking:		
	• +	
		Cancel

Afbeelding 9. Nieuw netwerkobject toevoegen

Stap 5. Configureer een naam voor referentie en het IP van de Dekking van de externe peer en Sla op.

0

# New Network Object

Name	
Loopback-FTD2	
Description          Description         Network            • Host         • Range         • Network         • N	○ FQDN
	0.400
10.2.2.2	
Allow Overrides	
	Cancel Save

Afbeelding 10. Netwerkbestemming in de statische route configureren

Stap 6. Zoek het nieuwe object dat in de zoekbalk is gemaakt, selecteer het, klik vervolgens op Toevoegen en klik vervolgens op OK.

0

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 de	efault Route)		
Route Tracking:			
	• +		
		(	Cancel

Afbeelding 11. Configureer volgende hop in statische route

Stap 7. Klik op Save (Opslaan).

0

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							

Afbeelding 12. De configuratie van de statische routeinterface opslaan

#### Stap 8. Herhaal het proces met de tweede firewall.

Firewall Management ( Devices / Secure Firewall Routin	Center c 9	Verview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	🗘 🕜 adm	nin v dudu cisco	SECURE
FTD-2 Cisco Firepower Threat Defense for VN Device Routing Interfaces	/ware Inline Sets	DHCP	VTEP									Save	Cancel
Manage Virtual Routers												+ Ad	d Route
Global v	Network .		Interface		Leaked fre 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 Policy Pared Policipa													
✓ BGP													
IPv4													
IPv6													
Static Route													

Afbeelding 13. Statische route op peer configureren

#### **BGP-configuratie**

Stap 1. Klik op Apparaten > Apparaatbeheer en selecteer het apparaat dat u BGP wilt inschakelen.

Stap 2. Klik op Routing > Virtual Routers beheren > Algemene instellingen en klik vervolgens op BGP.

Stap 3. Controleer het vakje BGP inschakelen en configureer vervolgens de lokale AS van de firewall in het gedeelte AS-nummer.

Firewall Management Devices / Secure Firewall Routin	Center Overview Analysis Policies Devices Objects	Integration									
FTD-1         Cisco Firepower Threat Defense for VMware         Device       Routing       Interfaces       DHCP       VTEP											
Manage Virtual Routers Global v Virtual Router Properties ECMP BFD OSPF OSPFv3 EIGRP	Enable BGP: AS Number* 64000 Override 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									
V Multicast Routing	Reset session upon failover	Yes	Next Hop								
IGMP	Enforce the first AS is peer's AS for EBGP routes	Yes	Address tracking								
РІМ	Use dot notation for AS number	No	Delay interval								
Multicast Routes Multicast Boundary Filter	Aggregate Timer	30									
General Settings	Best Path Selection	1	Graceful Restart								
BGP	Default local preference	100	Restart time								

Afbeelding 14. BGP wereldwijd inschakelen

#### Stap 4. Sla de wijzigingen op door op de knop Opslaan te klikken.

Firewall Manageme Devices / Secure Firewall Ro	nt Center Overview Analysis Policies Devices Objects	Integration	D	Deploy	Q ☆ Ø admin ∨ sliedu SECURE
FTD-1 Cisco Firepower Threat Defense fo Device Routing Interface	r VMware es Inline Sets DHCP VTEP				You have unsaved changes Save Cancel
Manage Virtual Routers Global  Virtual Router Properties ECMP BFD OSPF OSPFV3 ECOP	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 Static Route	Use TCP path MTU discovery	Yes			

Afbeelding 15. BGP opslaan Wijzigingen inschakelen

Stap 5. In de sectie Virtuele routers beheren gaat u naar de BGP-optie en klikt u vervolgens op IPv4.

Stap 6. Controleer het vakje IPv4 inschakelen, klik vervolgens op Buren en klik vervolgens op + Toevoegen.

Firewall Management Devices / Secure Firewall Ro	nt Center <sup>uting</sup>	Overview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹	٥	admin ~	cisco SI	ECURE
FTD-1 Cisco Firepower Threat Defense for	r VMware										You t	nave unsa	aved changes	iave (	Cancel
Device Routing Interfac	es Inline Sets	DHCP	VTEP												
Manage Virtual Routers	Enable IPv4: AS Number 640 General N	000 Veighbor	Add Aggrega	te Address	Filtering	Networks	Redistribution	Route Injection							
Virtual Router Properties														_	_
ECMP														+	Add
BFD	Address			Remote AS Nu	mber		Address Family		Remote Private AS Numb	er	Desc	ription			
OSPF															
EIGPR							NG	records to display							
RIP															
Policy Based Routing															
∽ BGP															
IPv4															
IPv6															
Static Route															
✓ Multicast Routing															

Afbeelding 16. Voeg een nieuwe BGP-peer toe

Stap 7. Configureer het IP-adres van de externe peer in de sectie IP-adres, configureer vervolgens het AS van de externe peer in de sectie Remote AS en controleer het vakje Adres inschakelen.

Stap 8. Selecteer de lokale interface Loopback in de sectie Update Source.

IP Address*			Enabled address						
10.2.2.2			Shutdown administratively						
Remote AS*			Configure graceful restart						
64001			Graceful restart(failover/spanned mode)						
(1-4294957295 or 1.0-655	535.65535)								
BFD Fallover		De	escription						
none	٠								
Update Source:		1							
Loopbeck1	٠								
Filtering Routes Rout	tes Tin	ners	Advanced Migration						
Filtering Routes Rout	tes Tin	ners	Advanced Migration Outgoing						
Filtering Routes Rout Incoming Access List	tes Tin	ners	Advanced Migration Outgoing Access List						
Filtering Routes Rout Incoming Access List	tes Tin	ners +	Advanced Migration Outgoing Access List						
Filtering Routes Rout Incoming Access List Route Map	tes Tin	+	Advanced Migration Outgoing Access List						
Filtering Routes Rout Incoming Access List Route Map	tes Tin V	+	Advanced Migration Outgoing Access List  Route Map  +						
Filtering Routes Rout Incoming Access List Route Map Prefix List	res Tin	+	Advanced Migration Outgoing Access List    Route Map						
Filtering Routes Rout Incoming Access List Route Map Prefix List	tes Tin •	++++++	Advanced Migration Outgoing Access List						
Filtering Routes Rout Incoming Access List Route Map Prefix List AS path filter	tes Tin • •	+ + +	Advanced Migration Outgoing Access List    Poute Map     Prefix List						

Afbeelding 17. Basis BGP-peer parameters

Opmerking: De Update Source optie maakt het buurupdate-bron commando, gebruikt om elke operationele interface (inclusief Loopbacks) toe te staan. Deze opdracht kan worden gespecificeerd om TCP-verbindingen tot stand te brengen.

Stap 9. Klik op Advanced, configureer vervolgens nummer 2 in de optie TTL Hops en klik op OK.

Edit Neighbor	Θ
none v	
Update Source:	
Loopback1 *	
Filtering Routes Routes Timers Advanced Migration	
Enable Authentication	
Enable Encryption	
0 *	
Password	
Confirm Password	
Use itself as next hop for this neighbor	
Disable Connection Verification	
<ul> <li>Allow connections with neighbor that is not directly connected</li> </ul>	
<ul> <li>United number of TTL hops to neighbor</li> </ul>	
TTL Hops	
(1-255)	
Use TCP path MTU discovery	
TCP Transport Mode	
Default •	
Weight	
	Carcel

Afbeelding 18. Het hopnummer van TTL's configureren

Opmerking: de optie TTL Hops schakelt de ebgp-multihop-opdracht in, die wordt gebruikt om de TTL-waarde te wijzigen, zodat het pakket de externe BGP-peer kan bereiken die niet direct verbonden is of een andere interface heeft dan de direct verbonden interface.

Stap 10. Klik op Opslaan en voer de wijzigingen in.

Firewall Managemer	nt Center Overview	Analysis	Policies	Devices	Objects	Integration		D	eploy	۹	0	admin $\sim$	cisco SECURE
FTD-1 Cisco Firepower Threat Defense for	r VMware									You hav	e unsaved	changes Sa	ve Cancel
Device Routing Interfac	es Inline Sets DHCP	VTEP											
Manage Virtual Routers	Enable IPv4: 🗹 AS Number 64000												
Virtual Router Properties	General Neighbor	Add Aggreg	ate Address	Filtering	Networks	Redistribution	Route Injection						
ECMP													+ Add
BFD OSPF	Address		Remote AS N	umber		Address Family		Remote Private AS Number		Descrip	tion		
OSPFv3	10.2.2.2		64001			Enabled							/1
EIGRP RIP													
Policy Based Routing													
IPv4													

Afbeelding 19. De BGP-configuratie opslaan

#### Stap 11. Herhaal het proces met de tweede firewall.

Firewall Managemer	nt Center Overview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹	¢ 0	admin ~ diat	SECURE
FTD-2 Cisco Firepower Threat Defense for Device Routing Interfac	r VMware es Inline Sets DHCP	VTEP											Cancel
Manage Virtual Routers Global v Virtual Router Properties	Enable IPv4: 🗹 AS Number 64001 General Neighbor	Add Aggrega	ite Address	Filtering	Networks	Redistribution	Route Injection						
ECMP													+ Add
BFD OSPF	Address		Remote AS N	umber		Address Family		Remote Private AS Number		Descript	on		
OSPFv3	10.1.1.1		64000			Enabled							18
EIGRP RIP													
Policy Based Routing													
V BGP													
IPv6													

Afbeelding 20. BGP op peer configureren

#### Verifiëren

Stap 1. Controleer de Loopback- en statische routeconfiguratie en controleer vervolgens de connectiviteit tussen BGP-peers met een ping-test.

toon in werking stellen-config interface interface\_name

toon in werking stelt -in werking stellen-configuratieroute

toon destinatie\_ip

SFTD-1	SFTD-2
onen in werking stelt -in werking stellen- configuratieinterface Loopback1	tonen in werking stelt -in werking stellen- configuratieinterface Loopback1
nterface-loopback1	interface-loopback1

naam Loopback1	nameif Looback2
IP-adres 10.1.1.1 255.255.255.255	IP-adres 10.2.2.2 255.255.255.255
toon in werking stelt -in werking stellen- configuratieroute	toon in werking stelt -in werking stellen- configuratieroute
route buiten 10.2.2.2 255.255.255.255 10.10.10.2 1	route buiten 10.1.1.1 255.255.255.255 10.10.10.1 1
ping 10.2.2.2	ping 10.1.1.1
Verzend 5, 100-byte ICMP Echos naar 10.2.2.2, tijd is 2 seconden:	Verzend 5, 100-byte ICMP Echos naar 10.1.1.1, tijd is 2 seconden:
!!!!!	!!!!!
Succespercentage is 100 procent (5/5), ronde- trip min/avg/max = 1/1/1 ms	Succespercentage is 100 procent (5/5), ronde- trip min/avg/max = 1/1/1 ms

Stap 2. Controleer de BGP-configuratie en zorg er vervolgens voor dat de BGP-peer is ingesteld.

tonen in werking stelt -in werking stellen-configuratierouter bgp

Toon bgp buren

bgp-overzicht tonen

SFTD-1	SFTD-2
tonen in werking stelt -in werking stellen- configuratierouter bgp	tonen in werking stelt -in werking stellen- configuratierouter bgp
router bgp 64000	router bgp 64001
bgp log-buurwijzigingen	bgp log-buurwijzigingen
bgp router-id vrf automatisch toewijzen	bgp router-id vrf automatisch toewijzen
IPv4-unicast voor adresfamilie	IPv4-unicast voor adresfamilie
buur 10.2.2.2 op afstand 64001	buur 10.1.1.1 afstandsbediening als 64000
buurman 10.2.2.2 bgp-multihop 2	buurman 10.1.1.1 bgp-multihop 2
buur 10.2.2.2 transportpad-mtu-discovery uitschakelen	buur 10.1.1.1 transportpad-mtu-discovery uitschakelen
buur 10.2.2.2 update-bron Loopback1	buur 10.1.1.1 update-bron Looback2

buur 10.2.2.2 activeren	buur 10.1.1.1 activeren
geen automatische samenvatting	geen automatische samenvatting
geen synchronisatie	geen synchronisatie
exit-address-family	exit-address-family
!	!
Toon bgp buren   i BGP-software	Toon bgp buren   i BGP-software
BGP-buur is 10.2.2.2, vrf single_vf, extern AS- 64001, externe link	BGP-buur is 10.1.1.1, vrf single_vf, extern AS- 64000, externe link
BGP versie 4, externe router-ID 10.2.2.2	BGP versie 4, externe router-ID 10.1.1.1
BGP-staat = ingesteld, tot 1 d15 uur	BGP-staat = ingesteld, tot 1d16h
BGP-tabelversie 7, buurversie 7/0	BGP-tabelversie 1, buurversie 1/0
De externe buur van BGP kan tot 2 hop weg zijn.	De externe buur van BGP kan tot 2 hop weg zijn.
bgp-overzicht tonen	bgp-overzicht tonen
BGP-router-id 10.1.1.1, lokaal AS-nummer 64000	BGP-router-id 10.2.2.2, lokaal AS-nummer 64001
BGP-tabelversie 7, hoofdrouteringstabel versie 7	BGP-tabelversie 1, hoofdrouteringstabel versie 1
Neighbour V ASmsgRcvd MSG Verzonden TblVer InQ OutQ Up/Down State/PFXRCD	Neighbour V ASmsgRcvd MSG Verzonden TblVer InQ OutQ Up/Down State/PFXRCD
10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0	10.1.1.4 64000 2168 2173 1 0 0 1d16h 0

## Probleemoplossing

Als u problemen ondervindt tijdens het proces, kunt u dit artikel bekijken:

· BGP-protocol (border gateway protocol)

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.