# セキュアファイアウォール上のループバックイ ンターフェイスを使用したeBGPの設定

内容
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>ループバックインターフェイスを使用したeBGP設定</u>
シナリオ
<u>ネットワーク図</u>
<u>ループバック設定</u>
<u>スタティックルートの設定</u>
<u>BGPの設定</u>
<u>トラブルシューティング</u>

## はじめに

このドキュメントでは、Cisco Secure Firewallのループバックインターフェイスを使用して eBGPを設定する方法について説明します。

## 前提条件

要件

次の項目に関する専門知識があることが推奨されます。

• BGPプロトコル

BGPのループバックインターフェイスのサポートは、バージョン7.4.0で導入されました。これは 、Secure Firewall Management CenterおよびCisco Secure Firepower Threat Defenseに必要な最 小バージョンです。

使用するコンポーネント

- Secure Firewall Management Center for VMware  $\mathcal{N} = \mathcal{V}7.4.1$
- 2 Cisco Secure Firepower Threat Defense for VMware $\mathcal{N} \mathcal{V} \exists \mathcal{V} 7.4.1$

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

### 背景説明

ボーダーゲートウェイプロトコル(BGP)は、拡張性、柔軟性、およびネットワークの安定性を提 供するExterior Gateway Protocol(EGP)標準パスベクタールーティングプロトコルです。同じ自律 システム(AS)を持つ2つのピア間のBGPセッションは、内部BGP(iBGP)と呼ばれます。異なる自 律システム(AS)を持つ2つのピア間のBGPセッションは、外部BGP(eBGP)と呼ばれます。

通常、ピア関係は、ピアに最も近いインターフェイスのIPアドレスで確立されますが、BGPセッションを確立するためにループバックインターフェイスを使用することは、BGPピア間に複数の パスが存在する場合にBGPセッションをダウンさせないために有用です。

◆ 注:このプロセスでは、eBGPピアでのループバックの使用について説明します。ただし、 iBGPピアでの同じプロセスであるため、参照として使用できます。

### ループバックインターフェイスを使用したeBGP設定

シナリオ

この設定では、ファイアウォールSFTD-1にIPアドレス10.1.1.1/32およびAS 64000のループバッ クインターフェイスがあり、ファイアウォールSFTD-2にIPアドレス10.2.2.2/32およびAS 64001のループバックインターフェイスがあります。両方のファイアウォールは、他方のファイ アウォールのループバックインターフェイスに到達するために外部インターフェイスを使用しま す(このシナリオでは、両方のファイアウォールで外部インターフェイスが事前に設定されてい ます)。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



画像 1.シナリオ図

### ループバック設定

ステップ1: Devices > Device Managementの順にクリックし、ループバックを設定するデバイ スを選択します。

ステップ2: Interfaces > All Interfacesの順にクリックします。

ステップ3: Add Interface > Loopback Interfaceの順にクリックします。

(	Firewall Management Cente Devices / Secure Firewall Interfaces	r Overview	Analysis Po	licies Devices	Objects Integration	t	Xeploy Q 🔅 🖗	admin ~ diada SECURE			
ł	FTD-1 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP										
I	All Interfaces Virtual Tunnels					Q. Search by name	8 Sync	C Device Add Interfaces *			
	Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual I Reidgo 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	/			

画像 2.インターフェイスループバックの追加

ステップ 4: Generalセクションで、ループバックの名前を設定し、Enabledボックスにチェック マークを入れて、Loopback IDを設定します。

## Add Loopback Interface

General	IPv4	IPv6	
Name:			
Looback1			
Enabled			
Loopback ID	):*		
1			
(1-1024)			
Description			_
			_

画像 3.基本的なループバックインターフェイス設定

ステップ 5 : IPv4セクションのIP TypeセクションでUse Static IPオプションを選択し、ループバックIPを設定してから、OKをクリックして変更を保存します。

Cancel

OK.

## Edit Loopback Interface



e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

図 4.ループバックIPアドレスの設定

### 手順 6 : [Save] をクリックします。

Firewall Management Center Devices / Secure Firewall Interfaces	er Overview	Analysis Po	olicies Devices	Objects Integration	Dep	loy Q 🔅	admin ~ diadu	SECURE	
FTD-1     You have unsaved changes     Save     Cancel       Claco Firepower Threat Defense for VMware     Device     Routing     Interfaces     Inline Sets     DHCP     VTEP									
All Interfaces Virtual Tunnels	All Interfaces Virtual Tunnels Q, Search by name Sync Device Add Interfaces •								
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	11	

図 5.ループバックインターフェイス設定の保存

手順7:2つ目のファイアウォールでこのプロセスを繰り返します。



Firewall Management Cente Devices / Secure Firewall Interfaces	r Overview	Analysis Po	olicies Devices	Objects Integration	Dep	loy Q 🔅	admin ~ diado     cisco	SECURE		
TD-2 Sisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP										
All Interfaces Virtual Tunnels Add Interfaces T										
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router			
Management0/0	management	Physical				Disabled	Global	୦. ଏ		
GigabitEthernet0/0	outside	Physical			10.10.10.2/24(Static)	Disabled	Global	/		
GigabitEthernet0/1	GigabitEthernet0/1 Physical					Disabled		/		
GigabitEthernet0/2 Physical					Disabled		/			
GigabitEthernet0/3		Physical				Disabled		/		
Loopback1	Looback2	Loopback			10.2.2.2/32(Static)	Disabled	Global	11		

図 6.ピアのループバックインターフェイス設定

### スタティックルートの設定

スタティックルートは、ピアリングに使用されるリモートピアアドレス(ループバック)が目的 のインターフェイスを介して到達可能であることを確認するように設定する必要があります。

ステップ1: Devices > Device Management の順にクリックし、スタティックルートを設定する デバイスを選択します。

ステップ2.Routing > Manage Virtual Routers > Static Routeの順にクリックし、Add Routeをクリックします。

Firewall Managemen Devices / Secure Firewall Rout	t Center Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🗘 🞯 admin	esco SECURE		
FTD-1 Cisco Firepower Threat Defense for	FTD-1 Save Cancel Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP									
Manage Virtual Routers	s mine orts Unor	VIEP	Leaked from Virtual					+ Add Route		
Virtual Router Properties	<ul> <li>Network *</li> <li>IPv4 Routes</li> </ul>	Interface	Router	Gateway	Tunneled	Metric	Tracked			
ECMP BFD	▼ IPv6 Routes									
OSPF OSPFv3										
EIGRP RIP										
Policy Based Routing										
IPv4 IPv6										
Static Route										
IGMP										
PIM Multicast Routes										
Multicast Boundary Filter										
BGP						1.000				

図 7.新しいスタティックルートの追加

手順3:TypeのIPv4オプションをチェックします。Interfaceオプションでリモートピアのループ バックに到達するために使用する物理インターフェイスを選択してから、Gatewayセクションで 、ループバックに到達するためのネクストホップを指定します。 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

Sateway	
10.10.10.2 *	]+
Metric:	
1	]
(1 - 254)	_
Tunneled: 🗌 (Used only for default	Route
Route Tracking:	
*	]+

図 8.スタティックルートの設定

ステップ4. Available Networkセクションの横にあるアイコン(+)をクリックします。

Edit Static Route Configuration

Type:	IPv4	O IPv6
Interface*		
outside		٠
(Interface starting	g with this	icon 🔏 signifi
Available Networ	k C	+
Q, Search		
any-ipv4		
IPv4-Benchmar	rk-Tests	
IPv4-Link-Loca	d	
IPv4-Multicast		
IPv4-Private-10	8-0.0.0	
IPv4-Private-12	72.16.0.0-	12

Ensure that egress virtualrouter has route to that destination

100				
6 B. A.	8 m.			a 10
SC 1997		1000	NR.	199 H
The local division of	the literature		Test.	UR -

10.10.10.2	+
Metric:	

1

(1 - 254)

Tunneled:	(Used	only for	default.	Route)
-----------	-------	----------	----------	--------

Route Tracking:

• | +

Cancel	OK
<u> </u>	

図 9.新しいネットワークオブジェクトの追加

ステップ5:参照用に名前を設定し、リモートピアのループバックのIPを設定して、保存します。

0

## New Network Object

0

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

図 10.スタティックルートでのネットワーク宛先の設定

ステップ 6:検索バーで作成した新しいオブジェクトを検索して選択し、AddをクリックしてからOKをクリックします。

## Edit Static Route Configuration

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

Ensure that egress virtualrouter has route to that destination

#### Gateway

10.10.10.2	٠	+	
Metric:			
1			
(1 - 254)			
Tunneled: 🗌 (Used only for defa	iult F	loute)	
Route Tracking:			
	۳	+	

図 11.スタティックルートでのネクストホップの設定

### 手順7: [Save] をクリックします。

ø

Cancel

Firewall Management Devices / Secure Firewall Routin	Center Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🗘 🕜 admin 🗸 🖏	SECURE
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	d 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		11
BFD	▼ IPv6 Routes							
OSPFv3								
EIGRP								
RIP								
Policy Based Routing								
∼ BGP								
IPv4								
IPv6								
Static Route								

図 12.スタティックルートインターフェイス設定の保存

### ステップ8:2つ目のファイアウォールでこのプロセスを繰り返します。

Firewall Management Devices / Secure Firewall Routin	Center Overview	Analysis Policies	Devices Objects	Integration		Deploy Q	🔅 🙆 admin 🗸 diada	SECURE
FTD-2 Cisco Firepower Threat Defense for VM Device Routing Interfaces	Mware Inline Sets DHCP	VTEP						Cancel
Manage Virtual Routers							+ Ac	dd Route
Global 🔻	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		11
BFD	W ID-0 Decision							
OSPF	<ul> <li>IPV6 Routes</li> </ul>							
OSPFv3								
EIGRP								
Policy Based Routing								
✓ BGP								
IPv4								
IPv6								
Static Route								

図 13.ピアでのスタティックルートの設定

### BGPの設定

ステップ1: Devices > Device Managementの順にクリックし、BGPをイネーブルにするデバイ スを選択します。

ステップ2. Routing > Manage Virtual Routers > General Settingsの順にクリックし、BGPをクリックします。

手順 3: Enable BGPボックスにチェックマークを入れてから、ファイアウォールのローカル ASをAS Numberセクションで設定します。

Firewall Management Devices / Secure Firewall Routin	Center Overview Analysis Policies Devices Objects	Integration	
FTD-1			
Cisco Firepower Threat Defense for V	Mware		
Device Pouting Interfaces			
Device Routing Interfaces			
Manage Virtual Routers	Enable BGP: 🗹		
Global	AS Number*		
	64000 (-4294967295 or 1.0-65535.65535)		
Virtual Router Properties	Override BGP general settings router-id address:		
ECMP	Automatio		
BFD	Automatic		
OSPF	IP Address*		
OSPFv3			
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		Vee	Min hald line
IPv6	Log Neighbor Changes	res	Min hold time
Static Route	Use TCP path MTU discovery	Yes	
✓ Multicast Routing	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
BGP	Default local preference	100	Restart time

図 14.BGPをグローバルに有効にする

### ステップ4.Saveボタンをクリックして、変更を保存します。

Firewall Manageme Devices / Secure Firewall Ro	nt Center Overview Analysis Policies Devices Objects	Integration	Deploy	Q ✿ admin ∽ secure
FTD-1 Cisco Firepower Threat Defense fo	VMware			You have unsaved changes Save Cancel
Device Routing Internal     Manage Virtual Routers     Global     Virtual Router Properties     ECMP     BFD     OSPF     OSPFFv3     EIGRP	es mine Sets DRCP VIEP Enable BGP:  AS Number*  G4000  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		

図 15.BGP有効化の変更の保存

ステップ 5 : Manage Virtual Routersセクションで、BGP オプションに移動し、IPv4をクリック します。

手順 6 : Enable IPv4ボックスにチェックマークを入れてから、Neighborをクリックし、+ Addを クリックする。

Firewall Manageme Devices / Secure Firewall Ro	nt Center Overview An	lysis Policies Devices Obje	Integration	Deploy	Q 🔅 🖉 admin 🗸 👘
FTD-1 Cisco Firepower Threat Defense fo Device Routing Interfac	r VMware ces Inline Sets DHCP VTEF				You have unsaved changes Save Cancel
Manage Virtual Routers Global • Virtual Router Properties ECMP	Enable IPv4: AS Number 64000 General Neighbor Add A	gregate Address Filtering Networ	ks Redistribution Route Injection		+ Add
BFD OSPF	Address	Remote AS Number	Address Family	Remote Private AS Number	Description
OSPFv3			No records to display		
EIGRP					
RIP Policy Based Routing					
∨ BGP					
IPv6					
Static Route					
Multicast Routing					

図 16.新しいBGPピアの追加

手順 7:「IP Address」セクションでリモートピアのIPアドレスを設定し、「Remote AS」セク ションでリモートピアのASを設定して、「Enable address」ボックスにチェックマークを入れま す。

ステップ 8:Update Source セクションでローカルインターフェイスループバックを選択します。

0

Edit Neighbor

IP Address*		Enabled addres	55		
10.2.2.2		Shutdown adm	inistratively		
Remote AS*		Configure grad	eful restart		
64001		Graceful re	istart[failover/spann	ed model	
(1-4294957295 or 1.0+6553	(5.65535)				
BFD Failover	D	escription			
none	• •				
Update Source:					
Loopback1					
Filtering Routes Route	is Timers	Advanced	Migration		
Filtering Routes Route	is Timers	Advanced	Migration		
Filtering Routes Route	s Timers	Advanced	Migration		
Filtering Routes Route Incoming Access List	is Timers	Advanced Outgoing Access List	Migration		
Filtering Routes Route Incoming Access List	• Timers	Advanced Outgoing Access List	Migration	• +	
Filtering Routes Route Incoming Access List Route Map	v +	Advanced Outgoing Access List Route Map	Migration	• +	
Filtering Routes Route Incoming Access List Route Map	• +	Advanced Outgoing Access List Route Map	Migration	• +	
Filtering Routes Route Incoming Access List Route Map Prefix List	• +	Advanced Outgoing Access List Route Map Prefix List	Migration	• + • +	
Filtering Routes Route Incoming Access List Route Map Prefix List	• + • + • +	Advanced Outgoing Access List Route Map Prefix List	Migration	• + • + • +	
Filtering Routes Route Incoming Access List Route Map Prefix List AS path filter	• + • + • +	Advanced Outgoing Access List Route Map Prefix List AS path filter	Migration	• + • + • +	

図 17.基本的なBGPピアパラメータ

注: Update Source オプションにより、neighbor update-source コマンドがイネーブルになり、(ループバックを含む)動作しているすべてのインターフェイスを許可するために使用されます。このコマンドは、TCP接続を確立するために指定できます。

ステップ 9: Advancedをクリックし、TTL Hopsオプションに番号2を設定して、OKをクリックします。

ø

Edit Neighbor

none	•		
Update Source:			
Loopback1	w.	_	
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 thi	s neichbor		
Disable Connection Verificat	ion		
() ••••••••••••••••••••••••••••••••••••			
Allow connections with neight	soor that is not directly conn	RDC10rd	
United number of TTL hops	to neighbor		
3			
(1-255)			
Use TCP path MTU discover	Y		
TCP Transport Mode			
Default	•		
Weight			
			Cancel

図 18.TTLsホップ番号の設定

◆ 注:TTL Hops オプションによりebgp-multihop コマンドがイネーブルになります。このコマンドを使用してTTL値を変更すると、直接接続されていない外部BGPピア、または直接接続されたインターフェイス以外のインターフェイスを持つ外部BGPピアにパケットが到達できるようになります。

ステップ 10: Saveをクリックして、変更を展開します。

Firewall Management Center Devices / Secure Firewall Routing	erview Analysis	Policies	Devices	Objects	Integration		Dep	oloy	۹ ۱	0	${\rm admin} \sim$	cisco S	ECURE
FTD-1 Cisco Firepower Threat Defense for VMware									You have a	unsaved o	:hanges Sa	we	Cancel
Device Routing Interfaces Inline Sets I	DHCP VTEP												
Manage Virtual Routers Global Global General Neigh	ibor Add Aggregati	e Address	Filtering	Networks	Redistribution	Route Injection							
Virtual Router Properties												4	Add
BFD												-	AUU
OSPF Address		Remote AS Num	nber		Address Family		Remote Private AS Number		Description	n			
OSPFv3 10.2.2.2		64001			Enabled								1
EIGRP													
RIP													
Policy Based Routing													
0 BCb													

図 19.BGP設定の保存

### ステップ 112つ目のファイアウォールでこのプロセスを繰り返します。

Firewall Manageme Devices / Secure Firewall Ro	nt Center o	verview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹	° 0	admin ~ divide SECURE	E
FTD-2 Cisco Firepower Threat Defense fo Device Routing Interface	r VMware ces Inline Sets	DHCP 1	VTEP										Save Cancel	
Manage Virtual Routers Global ¥ Virtual Router Properties	Enable IPv4: 🗹 AS Number 64001 General Neig	hbor Ad	id Aggregate	Address	Filtering	Networks	Redistribution	Route Injection						
ECMP BFD	Address		5	Remote AS N	umber		Address Family		Remote Private AS Number		Descriptio	m	+ Add	
OSPFv3 EIGRP	10.1.1.1		e	54000			Enabled						/1	
RIP Policy Based Routing														
iPv6														

図 20.ピアでのBGPの設定

### 確認

ステップ1:ループバックとスタティックルートの設定を確認し、pingテストを使用してBGPピア間の接続を確認します。

show running-config interface interface\_name (隠しコマンド)

show running-config route

show destination\_ip(宛先IPの表示)

SFTD-1	SFTD-2
show running-config interfaceループバック1	show running-config interfaceループバック1
Interface Loopback1	Interface Loopback1

nameifループバック1	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
10.2.2.2 255.255.255.255 10.10.10.2 1以外のル ート	10.1.1.1 255.255.255.255 10.10.1.1以外のルー ト
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	!!!!!
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

ステップ2:BGP設定を確認し、BGPピアリングが確立されていることを確認します。

```
show running-config router bgp \exists \, \overline{\prec} \, \succ \, \check{\kappa}
```

```
show bgp neighbors (隠しコマンド)
```

show bgp summary

SFTD-1	SFTD-2
show running-config router bgpコマンド	show running-config router bgpコマンド
router bgp 64000	router bgp 64001
bgp log-neighbor-changes	bgp log-neighbor-changes
bgp router-id vrf auto-assign(VRF自動割り当て )	bgp router-id vrf auto-assign(VRF自動割り当て )
address-family ipv4 unicast	address-family ipv4 unicast
neighbor 10.2.2.2 remote-as 64001	neighbor 10.1.1.1 remote-as 64000
ネイバー10.2.2.2 ebgpマルチホップ2	ネイバー10.1.1.1 ebgp-multihop 2
neighbor 10.2.2.2 transport path-mtu- discoveryの無効化 neighbor 10.2.2.2 update-sourceループバック1	neighbor 10.1.1.1 transport path-mtu-discovery disable(ネイバー10.1.1.1 transport path-mtu- discoveryがディセーブル) 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(隠しコマンド)  i BGP(i BGP)	show bgp neighbors(隠しコマンド)  i BGP(i BGP)				
BGPネイバーは10.2.2.2、vrf single_vf、リモー トAS 64001、外部リンク	BGPネイバーは10.1.1.1、vrf single_vf、リモー トAS 64000、外部リンク				
BGPバージョン4、リモートルータID 10.2.2.2	BGPバージョン4、リモートルータID 10.1.1.1				
BGP状態= Established、アップ(1d15h)	BGP状態= Established、アップ(1d16h用)				
BGPテーブルバージョン7、ネイバーバージョ ン7/0	BGPテーブルバージョン1、ネイバーバージョ ン1/0				
外部BGPネイバーは最大2ホップ離れている可 能性があります。	外部BGPネイバーは最大2ホップ離れている可 能性があります。				
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テーブルバージョン7、メインルーティン グテーブルバージョン7	BGP table version is 1, main routing table version 1				
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ	Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ				
Up/Down State/PfxRcd	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				

## トラブルシューティング

処理中に問題が発生した場合は、次の記事を参照してください。

•Border Gateway Protocol ( BGP )

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。