Configure Route-Based Site-To-Site VPN Between ASA and FTD with BGP as Overlay

Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Background Information
<u>Configure</u>
Network Diagram
Configurations
Configure IPSec VPN on FTD using FMC
Configure Loopback Interface on FTD using FMC
Configure IPSec VPN on ASA
Configure Loopback Interface on ASA
Configure Overlay BGP on FTD using FMC
Configure Overlay BGP on ASA
<u>Verify</u>
Outputs on FTD
Outputs on ASA
Troubleshoot

Introduction

This document describes how to configure a route-based Site-to-Site VPN tunnel between Adaptive Security Appliance (ASA) and Firepower Threat Defense managed (FTD) by a Firepower Management Center (FMC) with dynamic routing Border Gateway Protocol (BGP) as an overlay.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of IPsec site-to-site VPN
- BGP configurations on FTD and ASA
- Experience with FMC

Components Used

- Cisco ASAv version 9.20(2)2
- Cisco FMC version 7.4.1
- Cisco FTD 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

Route-based VPN allows the determination of interesting traffic to be encrypted, or sent over a VPN tunnel, and uses traffic routing instead of policy/access-list as in a Policy-based or Crypto-map-based VPN. The encryption domain is set to allow any traffic which enters the IPsec tunnel. IPsec Local and remote traffic selectors are set to 0.0.0/0.0.0.0. Any traffic routed into the IPsec tunnel is encrypted regardless of the source/destination subnet.

This document focuses on Static Virtual Tunnel Interface (SVTI) configuration with dynamic routing BGP as an overlay.

Configure

This section describes the configuration needed on the ASA and FTD to bring up BGP neighborship through an SVTI IPSec Tunnel.

Network Diagram



Network Diagram

Configurations

Configure IPSec VPN on FTD using FMC

Step 1. Navigate to Devices > VPN > Site To Site .

Step 2. Click on +Site to Site VPN .



Site-To-Site VPN

Step 3. Provide a Topology Name and select the Type of VPN as Route Based (VTI). Choose the IKE Version.

For this demonstration:

Topology Name: ASAv-VTI

IKE Version: IKEv2

Edit VPN Topology
Topology Name:*

 Topology Name:*

 ASAv-VTI

 Policy Based (Crypto Map)

 Route Based (VTI)

 Network Topology:

 Point to Point

 Hub and Spoke

 Full Mesh

 IKE Version:*
 IKEv1

VPN-Topology

Step 4. Choose the Deviceon which the tunnel needs to be configured. You can add a new Virtual Tunnel Interface (click on the + icon), or select one from the existing list.

Endpoints	IKE	IPsec	Advanced	
		1	Node A	
	Device:	*		
	FTD			Ŧ
	Virtual '	Tunnel In	iterface:*	→ +
	U Tur	nnel Sou	rce IP is Private	Edit VTI
	Ser	nd Local	Identity to Peers	S
			+ Add Backup	p VTI (optional)
	► Ac	dvanced	Settings	

Endpoint Node A

Step 5. Define the parameters of the New Virtual Tunnel Interface. Click Ok.

For this demonstration:

Name: ASA-VTI

Description (Optional): VTI Tunnel with Extranet ASA

Security Zone: VTI-Zone

Tunnel ID: 1

IP Address: 169.254.2.1/24

Tunnel Source: GigabitEthernet0/1 (Outside)

IPsec Tunnel mode: IPv4

Add Virtual Tunnel Interface

General Path Monitoring	
Tunnol Tuno	
Tunnel Type	
Static Upynamic	
ASAv-VTI	
Enabled	
Description:	
VTI Tunnel with Extranet ASA	
Security Zone:	
VTI-Zone	*
Priority:	
0	(0 - 65535)
Virtual Tunnel Interface Details An interface named Tunnel <id> is config Tunnel ID:* 3</id>	ured. Tunnel Source is a physical interface where VPN tunnel terminates for the VT. (0 - 10413)
Tunnel Source:*	
GigabitEthernet0/1 (Outside)	▼ 10.197.226.222 ▼
IPsec Tunnel Details IPsec Tunnel mode is decided by VPN tra- IPsec Tunnel Mode:* IPsec Tunnel Psec Tunnel Mode:* IPsec Tunnel Psec Tunnel Mode:* IPsec Tunnel Psec Tunn	affic IP type. Configure IPv4 and IPv6 addresses accordingly. 169.254.2.1/24 • Loopback1 (loopback) •
	Cancel OK

0

Step 6. Clickok on the popup mentioning that the new VTI has been created.



Virtual Tunnel Interface Added

Step 7. Choose the newly created VTI or a VTI under Virtual Tunnel Interface. Provide the information for Node B (which is the peer device).

For this demonstration:

Device: Extranet

Device Name: ASAv-Peer

Endpoint IP Address: 10.197.226.187

Node A	Node B
Device:*	Device:*
FTD 🔻	Extranet 👻
Virtual Tunnel Interface:*	Device Name*:
ASAv-VTI (IP: 169.254.2.1) 🔻 🕂	ASAv-Peer
Tunnel Source: Outside (IP: 10.197.226.222)Edit VTI	Endpoint IP Address*:
Tunnel Source IP is Private	10.197.226.187
Send Local Identity to Peers	
+ Add Backup VTI (optional)	
Additional Configuration 🕕	
Route traffic to the VTI : <u>Routing Policy</u>	



Endpointe

IVE

IDeee

Advanced



Step 8. Navigate to the IKE tab. Click on

. You can choose to use a pre-defined Policy or click the +button next to the Policytab to create a new one.

Step 9. (Optional, if you create a new IKEv2 Policy.) Provide a Namefor the Policy and select the Algorithms to be used in the policy. Click Save.

For this demonstration:

Name: ASAv-IKEv2-policy

Integrity Algorithms: SHA-256

Encryption Algorithms: AES-256

PRF Algorithms: SHA-256

Diffie-Hellman Group: 14

Edit IKEv2 Policy



Cancel Save

IKEv2-Policy

Step 10. Choose the newly created Policy or the Policythat exists. Select the Authentication Type. If a Pre-shared Manual Key is used, enter the key in the Keyand Confirm Key box.

For this demonstration:

Policy: ASAv-IKEv2-Policy

Authentication Type: Pre-shared Manual Key

2

Endpoir	nts IKE IPsec Adv	vanced	
	IKEv2 Settings		
	Policies:*	ASAv-IKEv2-Policy	
	Authentication Type:	Pre-shared Manual Key	
	Key:*		
	Confirm Key:*		
		Enforce hex-based pre-shared key only	-

Authentication



Step 11. Navigate to the IPsec tab. Click on

can choose to use a pre-defined IKEv2 IPsec Proposal or create a new one. Click the +button next to the IKEv2 IPsec Proposal tab.

Step 12. (Optional, if you create a new IKEv2 IPsec Proposal.) Enter a Namefor the Proposal and select the Algorithms to be used in the Proposal. Click Save.

For this demonstration:

Name: ASAv-IPSec-Policy

ESP Hash: SHA-256

ESP Encryption: AES-256



Ø

IKEv2-IPsec-Proposal

Step 13. Choose the newly created Proposal or Proposalthat exists from the list of proposals available. Click OK.

२. Search	Selected Transform Sets
AES-256-SHA-256	Add ASAv-IPSec-Policy
AES-GCM	
AES-SHA	
ASAv-IPSec-Policy	
DES_SHA-1	
Umbrella-AES-GCM-256	

Transform Set

Step 14. (Optional) Choose the Perfect Forward Secrecy settings. Configure the IPsec Lifetime Duration and Lifetime Size.

For this demonstration:

Perfect Forward Secrecy: Modulus Group 14

Lifetime Duration: 28800 (Default)

Lifetime Size:	4608000	(Default)
----------------	---------	-----------

oints	IKE IPsec	Advanced	
	Transform Sets:	IKEv1 IPsec Proposals 🥒	IKEv2 IPsec Proposals* 🖋
		tunnel_aes256_sha	ASAv-IPSec-Policy
г		Enable Security Associatio	on (SA) Strength Enforcement
I	Modulus Group:	14	*
L	ifetime Duration*:	28800 Sec	onds (Range 120-2147483647)
		4000000	(Deere 10, 0147400047)

PFS-Configuration

Step 15. Check the configured settings. Click Save, as shown in this image.

dit VPN Topology	6
spology Name:*	
ASAw-VTI	
Policy Based (Crypto Map) Route Based (VTI)	
etwork Topology:	
Point to Point Hub and Spoke Full Mesh	
E Version:" 📃 IKEv1 💆 IKEv2	
indpoints IKE IPsec Advanced	
Node A	Node B
Device:*	Device:*
FTD *	Extranet •
Virtual Tunnel Interface:*	Device Name*:
ASAn-VTI (IP: 169.254.2.1) +	Adjara-Peer
Tunnel Source: Outside (IP: 10.197.226.222)Edit VTI	Endpoint IP Address*:
Tunnel Source IP is Private	10.197.226.187
Send Local Identity to Peers	
 Add Backup VTI (optional) 	
Additional Configuration ()	
Route traffic to the VTI : <u>Boution Policy</u> Permit VPN traffic : <u>AC Policy</u>	
	Cancel

Saving the configuration

Configure Loopback Interface on FTD using FMC

Navigate to Devices > Device Management . Edit the device where the loopback needs to be configured.

 $Step \ 1. \ Go \ to \ \ Interfaces > {\sf Add \ Interfaces} > {\sf Loopback \ Interface} \ .$

Device	Routing Interfaces Inline Sets DHCP	VTEP								
All Interface	S Virtual Tunnels						O, Searc	h by name	Sync Device	Add Interfaces +
	Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router		Redundant Interface Bridge Group Interface
	Management0/0	management	Physical				Disabled	Global	9.4	Loopback Interface
	GigabitEthemet0/0	Inside	Physical	Inside		10.197.224.227/23(Static)	Disabled	Global	/	

Navigate to Loopback interface

Step 2. Enter the name "loopback", provide a loopback ID "1" and enable the interface.

Edit Loopback Interface





Enabling Loopback interface

Step 3. Configure the IP address for the interface, click OK.



Edit Loopback Interface



Cancel

OK.

Provide Ip address to loopback interface

Configure IPSec VPN on ASA

!--- Configure IKEv2 Policy ---!

crypto ikev2 policy 1 encryption aes-256 integrity sha256 group 14 prf sha256 lifetime seconds 86400

!--- Enable IKEv2 on the outside interface ---!

crypto ikev2 enable outside

!---Configure Tunnel-Group with pre-shared-key---!

tunnel-group 10.197.226.222 type ipsec-121 tunnel-group 10.197.226.222 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****



```
!--- Configure IPSec Policy ---!
crypto ipsec ikev2 ipsec-proposal ipsec_proposal_for_FTD
protocol esp encryption aes-256
protocol esp integrity sha-256
!--- Configure IPSec Profile ---!
crypto ipsec profile ipsec_profile_for_FTD
set ikev2 ipsec-proposal FTD-ipsec-proposal
set pfs group14
!--- Configure VTI ---!
interface Tunnel1
nameif FTD-VTI
ip address 169.254.2.2 255.255.255.0
tunnel source interface outside
tunnel destination 10.197.226.222
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile_for_FTD
!--- Configure the WAN routes ---!
```

Configure Loopback Interface on ASA

route outside 0.0.0.0 0.0.0.0 10.197.226.1 1

interface Loopback1
nameif loopback
ip address 1.1.1.1 255.255.255.0

Configure Overlay BGP on FTD using FMC

Navigate to Devices > Device Management.Edit the device where the VTI tunnel is configured, then navigate to Routing >General Settings > BGP.

Step 1. Enable BGP and configure the Autonomous System (AS) Number and Router ID, as shown in this image.

AS number needs to be the same on both the devices FTD and ASA.

Router ID is used to identify each router participating in BGP.

Device Routing Interta	ces initie Sets DHCP VTEP			
Davice Routing Waters Manage Virtual Routers <u>Global</u> Virtual Router Virtual Router Properties ECAP BFD OSPF- OSPF- OSPF-V3 EGAP	Evadors BOP: Control			
RP				
Policy Based Routing	General	/	Neighbor Timers	/
∼ BGP	Scanning Interval	60	Keepalive Interval	60
IPv4	Number of AS numbers in AS_PATH attribute of received routes	None	Hold time	180
Pv6	Log Neighbor Changes	Yes	Min hold time	0
Static Route	Use TCP path MTU discovery	Yes		
V Multicast Routing	Reset session upon failover	Yes	Next Hop	1
KGMP DNA	Enforce the first AS is peer's AS for EBGP routes	Yes	Address tracking	Yes
Multicast Routes	Use dot notation for AS number	No	Delay Interval	5
Multicast Boundary Filter	Anneantin Timer	30		
	Addition and			1
General Settings	Best Path Selection	1	Graceful Restart	
BGP	Default local preference	100	Restart time	
	Allow comparing MFD from different naiobhors	No	Stalepath time	
	Compare Reviter ID for Identical EBCP paths	No		
	Sompare novem to no reprinter coor parts	No		
	The start was a set of the set of	No.		
	irreat missing MiLU as the best preterred path	NO		

Navigate to configure BGP

Step 2. Navigate to BGP > IPv4 and enable BGP IPv4 on the FTD.

Device Routing Interfac	ces Inline Sets DHCP VTEP			
Manage Virtual Routers Global •	Enable IPvit. 22 AS Number 1000 General Neighbor Add Aggregate Address Filtering Networks Redistribution Route hijection			
ECMP BFD	Setting	1	Administrative Route Distances	1
OSPF	Learned Route Map		External	20
OSPFv3			Internal	200
EIGRP			Local	200
RIP				
Policy Based Routing	Routes and Synchronization	1	Forward Packets Over Multiple Paths	1
~ BQP	Generate default routes	No	Number of Paths	1
Pv4	Summarize subnet routes into network level routes	No	IBOP number of paths	1
PV6	Advertise inactive routes	Yes		
V Multicast Roution	Synchronize between BQP and IQP systems	No		
ISMP	Redistribute INOP into IGP	No		
PIM	(Use filtering to limit the number of prefixes that are redistributed)			
Multicast Routes				
Multicast Boundary Filter				
	-			

Enable BGP

Step 3. Under the Neighbor Tab, add the ASAv VTI tunnel ip address as a neighbor and enable the neighbor.

Device Routing Interfac	es Inline Sets DHCP VTEP					
Manage Virtual Routers	Enable IPv4: 2 AS Number 1000					
Virtual Router Properties	General Neighbor Add Aggregat	te Address Filtering Networks Redistribution	n Route Injection			
ECMP						+ Add
BFD	Address	Remote AS Number	Address Family	Remote Private AS Number	Description	
OSPFv3	169.254.2.2	1000	Enabled		/	
EIGRP						
RIP Policy Based Decting						
✓ BGP						
Pv4						

Add BGP neighbor

Step 4. Under Networks , add the networks you want to advertise through BGP that need to go through the VTI tunnel, in this case, loopback1.

Device Routing Interfac	es Inline Sets DHCP VTEP	
Manage Virtual Routers Global • Virtual Router Properties	Enable III-vi. 💆 AS Number 1000 General Neighbor Add Aggregate Address Filtering <u>Networks</u> Redistribution Route Injection	
ECMP		+ Add
BFD	Normal Business	
OSPF	Hatana Hatana	
OSPFv3	2220	/1
EIGRP		
RIP		
Policy Based Routing		
∽ BGP		
IPv4		
IPv6		

Add BGP Networks

Step 5. All other BGP settings are optional and you may configure them as per your environment. Verify the configuration and Click _{Save}.

FTI Cisci	D Firepower Threat Defense for VMware rvice Routing Interfaces Inline Sets DHCP VTEP	You have unsaved charge	Cancel					
Man Glot Vin	age Virtual Routers A5 Number 1000 bil General Neighbor Add Aggregate Add	Iress Filtering Networks Redistribution Route Injection						
ECM BFD OSF	pp b pr pr pr ph 2220 pp	BostsMap / B	+ Add					
Sav	ve BGP configuration							
Step 6. Deploy all the configurations.								
		Deploy Q 💕 🌣 🕐 admin ~ 🖞						
	٩	Advanced Deploy 🔺 🗌 Ignore warning Deploy						
	🛃 FTD	Ready for Deployment						
	1 selected 🕕 1	pending 😥 💬						

Deployment

Configure Overlay BGP on ASA

```
router bgp 1000
bgp log-neighbor-changes
bgp router-id 10.1.1.2
address-family ipv4 unicast
neighbor 169.254.2.1 remote-as 1000
neighbor 169.254.2.1 transport path-mtu-discovery disable
neighbor 169.254.2.1 activate
network 1.1.1.0 mask 255.255.255.0
no auto-summary
no synchronization
exit-address-family
```

Verify

Use this section in order to confirm that your configuration works properly.

Outputs on FTD

<#root>

#show crypto ikev2 sa

IKEv2 SAs: Session-id:20, Status:UP-ACTIVE, IKE count:1, CHILD count:1 fvrf/ivrf Tunnel-id Loca] Remote Status Role 666846307 10.197.226.222/500 10.197.226.187/500 Global/Global READY RESPOND Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/1201 sec Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255.255/65535 ESP spi in/out: 0xa14edaf6/0x8540d49e #show crypto ipsec sa interface: ASAv-VTI Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.222 Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) current_peer: 10.197.226.187 #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45 #pkts decaps: 44, #pkts decrypt: 44, #pkts verify: 44 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed:0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.197.226.222/500, remote crypto endpt.: 10.197.226.187/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: 8540D49E current inbound spi : A14EDAF6 inbound esp sas: spi: 0xA14EDAF6 (2706299638) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, } slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4331517/27595) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 000001FFF 0xFFFFFFFF outbound esp sas: spi: 0x8540D49E (2235618462) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, } slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4101117/27595) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x0000001 #show bgp summary BGP router identifier 10.1.1.1, local AS number 1000 BGP table version is 5, main routing table version 5 2 network entries using 400 bytes of memory 2 path entries using 160 bytes of memory 2/2 BGP path/bestpath attribute entries using 416 bytes of memory 0 BGP route-map cache entries using 0 bytes of memory O BGP filter-list cache entries using O bytes of memory BGP using 976 total bytes of memory BGP activity 21/19 prefixes, 24/22 paths, scan interval 60 secs Neighbor MsgSent Tb1Ver V AS MsgRcvd InQ OutQ 169.254.2.2 4 1000 22 22 5 0 #show bgp neighbors BGP neighbor is 169.254.2.2, vrf single_vf, remote AS 1000, internal link BGP version 4, remote router ID 10.1.1.2 BGP state = Established, up for 00:19:49 Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds Neighbor sessions: 1 active, is not multisession capable (disabled) Neighbor capabilities: Route refresh: advertised and received(new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Multisession Capability:

Message statistics: InQ depth is 0 OutQ depth is 0 Up/Down

0

Rcvd Sent **Opens** 1 1 Notifications: 0 0 2 2 Updates: 19 19 Keepalives: Route Refresh: 0 0 Total: 22 22 Default minimum time between advertisement runs is 0 seconds For address family: IPv4 Unicast Session: 169.254.2.2 BGP table version 5, neighbor version 5/0 Output queue size : 0 Index 15 15 update-group member Sent Rcvd Prefix activity: ____ ____ Prefixes Current: 1 1 (Consumes 80 bytes) Prefixes Total: 1 1 Implicit Withdraw: 0 0 Explicit Withdraw: 0 0 Used as bestpath: n/a 1 Used as multipath: 0 n/a Outbound Inbound Local Policy Denied Prefixes: _____ ____ Bestpath from this peer: 1 n/a Invalid Path: 1 n/a Total: 2 0 Number of NLRIs in the update sent: max 1, min 0 Address tracking is enabled, the RIB does have a route to 169.254.2.2 Connections established 7; dropped 6 Last reset 00:20:06, due to Peer closed the session of session 1 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled #show route bgp Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF Gateway of last resort is 10.197.226.1 to network 0.0.0.0

B 1.1.1.0 255.255.255.0 [200/0] via 169.254.2.2, 00:19:55

Outputs on ASA

<#root>

#show crypto ikev2 sa

Session-id:7, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status 442126361 10.197.226.187/500 10.197.226.222/500 Global/Global READY Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/1200 sec Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255.255/65535 ESP spi in/out: 0x8540d49e/0xa14edaf6 #show crypto ipsec sa interface: FTD-VTI Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.187 Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) current_peer: 10.197.226.222 #pkts encaps: 44 #pkts encrypt: 44, #pkts digest: 44 #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed:0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.197.226.187/500, remote crypto endpt.: 10.197.226.222/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: A14EDAF6 current inbound spi : 8540D49E inbound esp sas: spi: 0x8540D49E (2235618462) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, } slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4147198/27594) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x007FFFF outbound esp sas: spi: 0xA14EDAF6 (2706299638) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, } slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (3916798/27594) IV size: 16 bytes replay detection support: Y

IKEv2 SAs:

Anti replay bitmap: 0x00000000 0x00000001

#show bgp summary

BGP router identifier 10.1.1.2, local AS number 1000 BGP table version is 7, main routing table version 7 2 network entries using 400 bytes of memory 2 path entries using 160 bytes of memory 2/2 BGP path/bestpath attribute entries using 416 bytes of memory O BGP route-map cache entries using O bytes of memory O BGP filter-list cache entries using O bytes of memory BGP using 976 total bytes of memory BGP activity 5/3 prefixes, 7/5 paths, scan interval 60 secs MsqRcvd Tb1Ver Up/Down State/Pf Neighbor V AS MsgSent InQ OutQ 169.254.2.1 1000 00:19:42 4 22 22 7 0 0 1 #show bgp neighbors BGP neighbor is 169.254.2.1, context single_vf, remote AS 1000, internal link BGP version 4, remote router ID 10.1.1.1 BGP state = Established, up for 00:19:42 Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds Neighbor sessions: 1 active, is not multisession capable (disabled) Neighbor capabilities: Route refresh: advertised and received(new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Multisession Capability: Message statistics: InQ depth is 0 OutQ depth is 0 Sent Rcvd Opens: 1 1 Notifications: 0 0 Updates: 2 2 Keepalives: 19 19 Route Refresh: 0 0 Total: 22 22 Default minimum time between advertisement runs is 0 seconds For address family: IPv4 Unicast Session: 169.254.2.1 BGP table version 7, neighbor version 7/0 Output queue size : 0 Index 5 5 update-group member Rcvd Sent Prefix activity: ____ ____ Prefixes Current: (Consumes 80 bytes) 1 1 Prefixes Total: 1 1 Implicit Withdraw: 0 0 Explicit Withdraw: 0 0 Used as bestpath: n/a 1 Used as multipath: 0 n/a

```
Outbound
```

```
Local Policy Denied Prefixes:
                                  _____
                                                  _____
Bestpath from this peer:
                                  1
                                                  n/a
Invalid Path:
                                  1
                                                  n/a
                                   2
Total:
                                                  0
Number of NLRIs in the update sent: max 1, min 0
Address tracking is enabled, the RIB does have a route to 169.254.2.1
Connections established 5; dropped 4
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
#show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
           i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
           ia - IS-IS inter area, * - candidate default, U - per-user static route
           o - ODR, P - periodic downloaded static route, + - replicated route
          SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.197.226.1 to network 0.0.0.0
       2.2.2.0 255.255.255.0 [200/0] via 169.254.2.1, 00:19:55
В
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug ip bgp all
```

• Supports only IPv4 interfaces, as well as IPv4, protected networks, or VPN payload (No Support for IPv6).