

Configuración de VPN de Sitio a Sitio Basada en Ruta entre ASA y FTD con BGP como Overlay

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de VPN IPsec en FTD mediante FMC](#)

[Configuración de la interfaz de loopback en FTD mediante FMC](#)

[Configuración de VPN IPsec en ASA](#)

[Configuración de la interfaz de loopback en ASA](#)

[Configuración de BGP de superposición en FTD mediante FMC](#)

[Configuración de BGP de superposición en ASA](#)

[Verificación](#)

[Salidas en FTD](#)

[Salidas en ASA](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar un túnel VPN de sitio a sitio basado en ruta entre Adaptive Security Appliance (ASA) y Firepower Threat Defence gestionado (FTD) por un Firepower Management Center (FMC) con routing dinámico Border Gateway Protocol (BGP) como superposición.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de VPN de sitio a sitio IPsec
- Configuraciones BGP en FTD y ASA
- Experiencia con FMC

Componentes Utilizados

- Cisco ASA v9.2(2)2
- Cisco FMC v7.4.1
- Cisco FTD v7.4.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La VPN basada en rutas permite cifrar la determinación del tráfico interesante o enviarla a través de un túnel VPN, y utiliza el ruteo del tráfico en lugar de la política/lista de acceso como en una VPN basada en políticas o en mapas criptográficos. El dominio de cifrado está configurado para permitir el tráfico que entra en el túnel IPsec. Los selectores de tráfico local y remoto IPSec están configurados en 0.0.0.0/0.0.0.0. Cualquier tráfico enrutado en el túnel IPsec se cifra independientemente de la subred de origen/destino.

Este documento se centra en la configuración de la Interfaz de Túnel Virtual Estática (SVTI) con el ruteo dinámico BGP como superposición.

Configurar

Esta sección describe la configuración necesaria en ASA y FTD para activar la vecindad BGP a través de un túnel IPsec SVTI.

Diagrama de la red

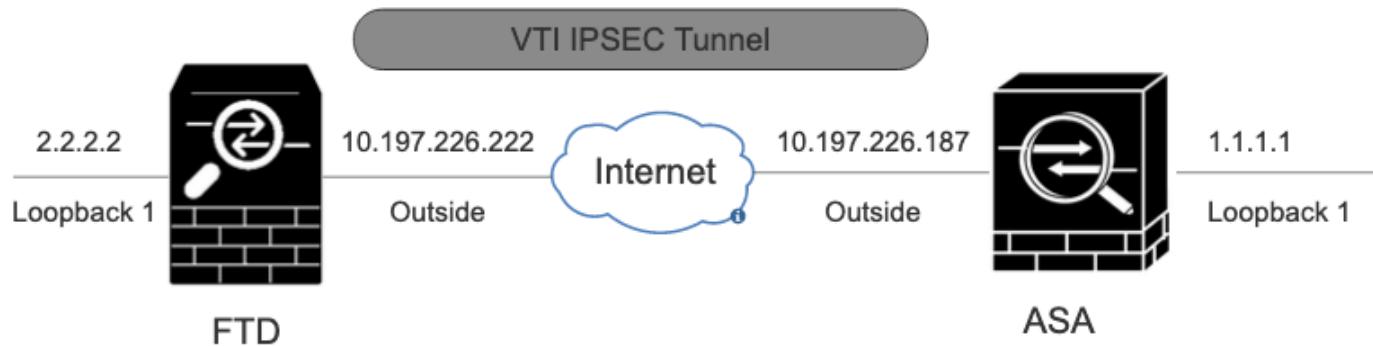


Diagrama de la red

Configuraciones

Configuración de VPN IPsec en FTD mediante FMC

Paso 1. Vaya a [Devices > VPN > Site To Site](#).

Paso 2. Haga clic en [+Site to Site VPN](#).



VPN de sitio a sitio

Paso 3. Proporcione un Topology Name y seleccione el tipo de VPN como Route Based (VTI). Elija el IKE Version.

Para esta demostración:

Nombre de topología: ASAv-VTI

Versión IKE: IKEv2

Edit VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

IKEv1 IKEv2

Topología de VPN

Paso 4. Elija el Device en el que debe configurarse el túnel. Puede agregar una nueva interfaz de túnel virtual (haga clic en el + icono) o seleccionar una de la lista existente.

Node A

Device:*

FTD

Virtual Tunnel Interface:*



Tunnel Source IP is Private

[Edit VTI](#)

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

[▶ Advanced Settings](#)

Nodo A de terminal

Paso 5. Defina los parámetros de New Virtual Tunnel Interface. Haga clic en Ok.

Para esta demostración:

Nombre: ASA-VTI

Descripción (opcional): Túnel VTI con Extranet ASA

Zona de seguridad: VTI-Zone

ID de túnel: 1

Dirección IP: 169.254.2.1/24

Fuente del túnel: GigabitEthernet0/1 (exterior)

Modo de túnel IPsec: IPv4

Add Virtual Tunnel Interface



General Path Monitoring

Tunnel Type

Static Dynamic

Name:*

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 configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VT.

Tunnel ID:*

3

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/1 (Outside)

10.197.226.222

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

IPv4 IPv6

IP Address:*

Configure IP

169.254.2.1/24

Borrow IP (IP unnumbered)

Loopback1 (loopback)

Cancel

OK

Interfaz de túnel virtual

Paso 6. Haga OK clic en la ventana emergente que indica que se ha creado el nuevo VTI.

Virtual Tunnel Interface Added

VTI has been created successfully.
Please go to the Device > Interfaces
page to delete/update the VTI.

OK

Interfaz de túnel virtual agregada

Paso 7. Elija la VTI recién creada o una VTI en Virtual Tunnel Interface. Proporcione la información para el Nodo B (que es el dispositivo par).

Para esta demostración:

Dispositivo: Extranet

Nombre del dispositivo: ASA-V-Peer

Dirección IP del terminal: 10.197.226.187

Node A

Device:*

FTD

Virtual Tunnel Interface:*

ASAv-VTI (IP: 169.254.2.1)

Tunnel Source: Outside (IP: 10.197.226.222) [Edit VTI](#) Tunnel Source IP is Private Send Local Identity to Peers[+ Add Backup VTI \(optional\)](#)Additional Configuration (1)Route traffic to the VTI : [Routing Policy](#)Permit VPN traffic : [AC Policy](#)

Node B

Device:*

Extranet

Device Name:*

ASAv-Peer

Endpoint IP Address:*

10.197.226.187

Nodo B de terminal

Paso 8. Vaya a la pestaña **IKE**. Haga clic en

. Puede optar por utilizar una ficha predefinida Policy o hacer clic en el +botón situado junto a la Policyficha para crear una nueva.

Paso 9. (Opcional, si crea una nueva política IKEv2.) Proporcione un Namepara la política y seleccione el Algorithms que se utilizará en la política. Haga clic en Save.

Para esta demostración:

Nombre: ASAv-IKEv2-policy

Algoritmos de integridad: SHA-256

Algoritmos de cifrado: AES-256

Algoritmos PRF: SHA-256

Grupo Diffie-Hellman: 14

Edit IKEv2 Policy



Name:*

ASAv-IKEv2-Policy

Description:

Priority: (1-65535)

1

Lifetime: seconds (120-2147483647)

86400

Available Algorithms	Selected Algorithms
Integrity Algorithms	SHA256
Encryption Algorithms	
PRF Algorithms	
Diffie-Hellman Group	
MD5	
SHA	
SHA512	
SHA256	
SHA384	
NULL	

Add



Cancel

Save

IKEv2-Política

Paso 10. Elija el recién creado Policy o el Policy que existe. Seleccione el Authentication Type. Si utiliza una clave manual precompartida, introduzcalo en el cuadro Key Confirm Key de.

Para esta demostración:

Política: ASA-IKEv2-Política

Tipo de autenticación: clave manual previamente compartida

IKEv2 Settings

Policies:* 

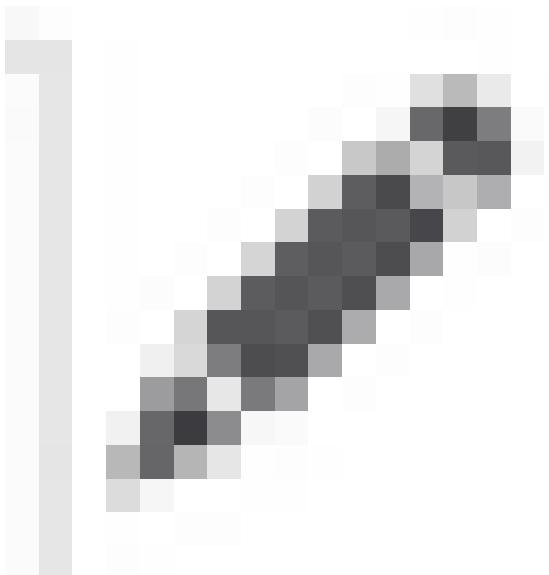
Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Autenticación



Paso 11. Vaya a la IPsec pestaña. Haga clic en  puede elegir utilizar una propuesta IPsec IKEv2 predefinida o crear una nueva. Haga clic en el +botón situado junto a la IKEv2 IPsec Proposal ficha.

Paso 12. (Opcional, si crea una nueva propuesta IKEv2 IPsec.) Introduzca una Namepara la propuesta y seleccione la Algorithms que se utilizará en la propuesta. Haga clic en Save.

Para esta demostración:

Nombre: ASAv-IPSec-Policy

Hash ESP: SHA-256

Cifrado ESP: AES-256

New IKEv2 IPsec Proposal



Name:*

Description:

Available Algorithms

ESP Hash

ESP Encryption

SHA-512

SHA-384

SHA-256

SHA-1

MD5

NULL

Add

Selected Algorithms

SHA-256



[Cancel](#)

[Save](#)

IKEv2-IPsec-Propuesta

Paso 13. Elija el Proposal o Proposalel recién creado existente de la lista de propuestas disponibles. Haga clic en OK.

IKEv2 IPsec Proposal



Available Transform Sets C +

Search

AES-256-SHA-256

Add

AES-GCM

AES-SHA

ASAv-IPSec-Policy

DES-SHA-1

Umbrella-AES-GCM-256

Selected Transform Sets

ASAv-IPSec-Policy



Cancel

OK

Transforme la configuración:

Paso 14. (Opcional) Elija los Perfect Forward Secrecy parámetros. Configure el IPSec Lifetime Duration and Lifetime Size.

Para esta demostración:

Confidencialidad directa perfecta: grupo de módulos 14

Duración de la vida útil: 28800 (Predeterminado)

Tamaño de vida útil: 4608000 (predeterminado)

Endpoints IKE IPsec Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha	ASAv-IPSec-Policy
-------------------	-------------------

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

Configuración de PFS

Paso 15. Compruebe los parámetros configurados. Haga clic en Save, como se muestra en esta imagen.

Edit VPN Topology

Topology Name:
ASAv-vTI

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Versions:
 IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:
FTD

Virtual Tunnel Interface:
ASAv-vTI (IP: 10.197.226.222) [Edit VTI](#)
 Tunnel Source IP is Private
 Send Local Identity to Peers
[+ Add Backup VTI \(optional\)](#)

Tunnel Source: Outside (IP: 10.197.226.222) [Edit VTI](#)

Additional Configuration
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

Node B

Device:
Extranet

Device Name:
ASAv-Peer

Endpoint IP Address:
10.197.226.187

[Cancel](#) [Save](#)

The 'Save' button is highlighted with a red box.

Saving the configuration

Configuración de la interfaz de loopback en FTD mediante FMC

Vaya a Devices > Device Management . Edite el dispositivo en el que debe configurarse el bucle invertido.

Paso 1. Vaya a Interfaces > Add Interfaces > Loopback Interface

Device Routing **Interfaces** Inline Sets DHCP VTEP

All Interfaces Virtual Tunnels

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	Inside	Physical	Inside		10.197.224.227/23(Static)	Disabled	Global

[Search by name](#) [Sync Device](#) [Add Interfaces](#) [Loopback Interface](#)

Vaya a la interfaz de bucle invertido

Paso 2. Introduzca el nombre "loopback", proporcione un ID de loopback "1" y active la interfaz.

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Habilitación de la interfaz Loopback

Paso 3. Configure la dirección IP de la interfaz y haga clic en OK .

Edit Loopback Interface



General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

2.2.2.2/24

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel

OK

Proporcione la dirección IP a la interfaz de bucle invertido

Configuración de VPN IPSec en 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-l2l
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 ---!

route outside 0.0.0.0 0.0.0.0 10.197.226.1 1
```

Configuración de la interfaz de loopback en ASA

```
interface Loopback1
nameif loopback
ip address 1.1.1.1 255.255.255.0
```

Configuración de BGP de superposición en FTD mediante FMC

Navegue hasta Devices > Device Management. Edit el dispositivo donde está configurado el túnel VTI, luego navegue hasta Routing > General Settings > BGP.

Paso 1. Habilite BGP y configure el número del sistema autónomo (AS) y la ID del router, como se muestra en esta imagen.

El número de AS debe ser el mismo tanto en el FTD del dispositivo como en el ASA.

El ID de router se utiliza para identificar cada router que participa en BGP.

BGP Settings:

- Enable BGP:
- AS Number*: 1000
- Override BGP general settings router-id address:
 - Router Id: Manual
 - IP Address*: 10.1.1.1

General Settings (BGP):

- Scanning Interval: 60
- Number of AS numbers in AS_PATH attribute of received routes: None
- Log Neighbor Changes: Yes
- Use TCP path MTU discovery: Yes
- Reset session upon fallover: Yes
- Enforce the first AS is peer's AS for EBGP routes: Yes
- Use dot notation for AS number: No
- Aggregate Timer: 30

Best Path Selection:

- Default local preference: 100
- Allow comparing MED from different neighbors: No
- Compare Router ID for identical EBGP paths: No
- Pick the best-MED path among paths advertised by neighbor AS: No
- Treat missing MED as the best preferred path: No

Neighbor Timers:

- Keepalive Interval: 60
- Hold time: 180
- Min hold time: 0

Next Hop:

- Address tracking: Yes
- Delay interval: 5

Graceful Restart:

- Restart time: 120
- Stalepath time: 360

Vaya a configurar BGP

Paso 2. Navegue hasta BGP > IPv4 BGP IPv4 y actívelo en el FTD.

BGP Settings:

- Enable IPv4:
- AS Number: 1000

Setting:

- Learned Route Map

Administrative Route Distances:

- External: 20
- Internal: 200
- Local: 200

Routes and Synchronization:

- Generate default routes: No
- Summarize subnet routes into network level routes: No
- Advertise inactive routes: Yes
- Synchronize between BGP and IGP systems: No
- Redistribute IBGP into IGP (Use filtering to limit the number of prefixes that are redistributed): No

Forward Packets Over Multiple Paths:

- Number of Paths: 1
- IBGP number of paths: 1

Activar BGP

Paso 3. En laNeighbor pestaña, agregue la dirección IP del túnel VTI de ASA v como un vecino y habilite el vecino.

Manage Virtual Routers (Global):

- Virtual Router Properties: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, IPv4, IPv6.

Neighbor Tab:

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.2.2	1000	Enabled		

Agregar vecino BGP

Paso 4. En Networks , agregue las redes que desea anunciar a través de BGP que necesitan pasar a través del túnel VTI, en este caso, loopback1.

Manage Virtual Routers (Global):

- Virtual Router Properties: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, IPv4, IPv6.

Networks Tab:

Network	RouteMap
2.2.2.0	

Agregar redes BGP

Paso 5. El resto de las configuraciones de BGP son opcionales y puede configurarlas según su entorno. Verifique la configuración y haga clic en Save.

The screenshot shows the Cisco FTD interface with the 'Routing' tab selected. On the left, there's a sidebar for 'Manage Virtual Routers' with options like Global, Virtual Router Properties, ECMP, BFD, OSPF, OSPFv3, and EIGRP. The main area shows a table with columns: Network, RouteMap, and Action. One row is visible with the network '2.2.2.0'. At the top right, a message says 'You have unsaved changes' with 'Save' and 'Cancel' buttons, where 'Save' is highlighted with a red box.

Guardar configuración BGP

Paso 6. Implemente todas las configuraciones.

The screenshot shows the deployment interface of the Cisco FTD. At the top, there's a toolbar with 'Deploy', a search icon, and user information ('admin'). Below it is a search bar and an 'Advanced Deploy' section with an 'Ignore warning' checkbox. A large red button labeled 'Deploy' is prominent. In the center, there's a status bar with 'Ready for Deployment' and '1 selected | 1 pending'. At the bottom, there are date and time controls.

Implementación

Configuración de BGP de superposición en 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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Salidas en FTD

```
<#root>
```

```
#show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:20, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	fvrif/ivrf	Status	Role
666846307	10.197.226.222/500	10.197.226.187/500	Global/Global	READY	RESPONDER
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: ASA-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): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
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:
0x00000000 0x00000001

```

```
#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
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 976 total bytes of memory
BGP activity 21/19 prefixes, 24/22 paths, scan interval 60 secs

```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
169.254.2.2	4	1000	22	22	5		0	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
      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: 169.254.2.2
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: n/a       0
      Outbound      Inbound
Local Policy Denied Prefixes: -----
Bestpath from this peer:    1           n/a
Invalid Path:              1           n/a
Total:                     2           0
Number of NLRI's 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

Salidas en ASA

<#root>

#show crypto ikev2 sa

IKEv2 SAs:

Session-id:7, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvrif/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): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
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:
0x00000000 0x007FFFFF

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
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
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory

```

```
BGP using 976 total bytes of memory
BGP activity 5/3 prefixes, 7/5 paths, scan interval 60 secs

Neighbor      V     AS      MsgRcvd      MsgSent      TblVer      InQ      OutQ      Up/Down      State/Pf
169.254.2.1   4     1000    22          22          7          0          0          00:19:42      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

	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:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
Bestpath from this peer:	1	n/a
Invalid Path:	1	n/a
Total:	2	0

Number of NLRI's 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
```

```
B      2.2.2.0 255.255.255.0 [200/0] via 169.254.2.1, 00:19:55
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

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

- Solo admite interfaces IPv4, así como IPv4, redes protegidas o carga útil de VPN (sin compatibilidad con IPv6).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).