

# Configuración de VPN de sitio a sitio basada en ruta entre ASA y FTD

## 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 ASA y FTD por un FMC con ruteo dinámico BGP como superposición.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de VPN de sitio a sitio IPsec
- Configuraciones del protocolo de gateway fronterizo (BGP) en Firepower Threat Defence administrado (FTD) y Adaptive Security Appliance (ASA)
- Experiencia con Firepower Management Center (FMC)

### Componentes Utilizados

- Cisco ASAv versión 9.20(2)2

- Cisco FMC versión 7.4.1
- Cisco FTD versión 7.4.1

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 se configura para permitir cualquier tráfico que ingrese al túnel IPsec. Los selectores de tráfico local y remoto de IPsec se establecen 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 proximidad BGP a través de un túnel IPsec SVTI.

### Diagrama de la red

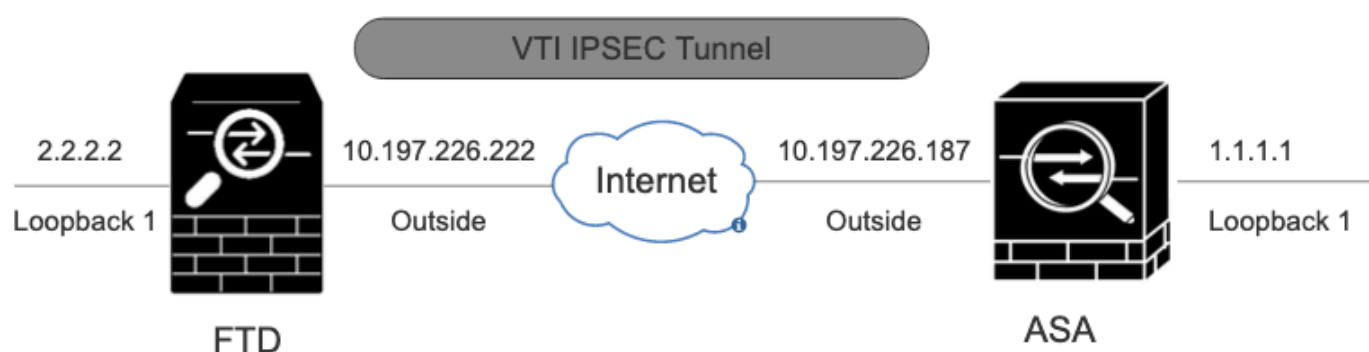


Diagrama de la red

## Configuraciones

### Configuración de VPN IPsec en FTD mediante FMC

Paso 1. Desplácese hasta **Devices > VPN > Site To Site**.

Paso 2. Haga clic en **+Site to Site VPN**.



VPN de sitio a sitio

Paso 3. Proporcione unTopology Namey seleccione el Tipo de VPN comoRoute Based (VTI). Elija la opciónIKE 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:

IKE Version:\* ☐ IKEv1 ☒ IKEv2

Topología de VPN

Paso 4. Elija elDeviceen 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 del 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
- IP Address: 169.254.2.1/24
- Origen 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)

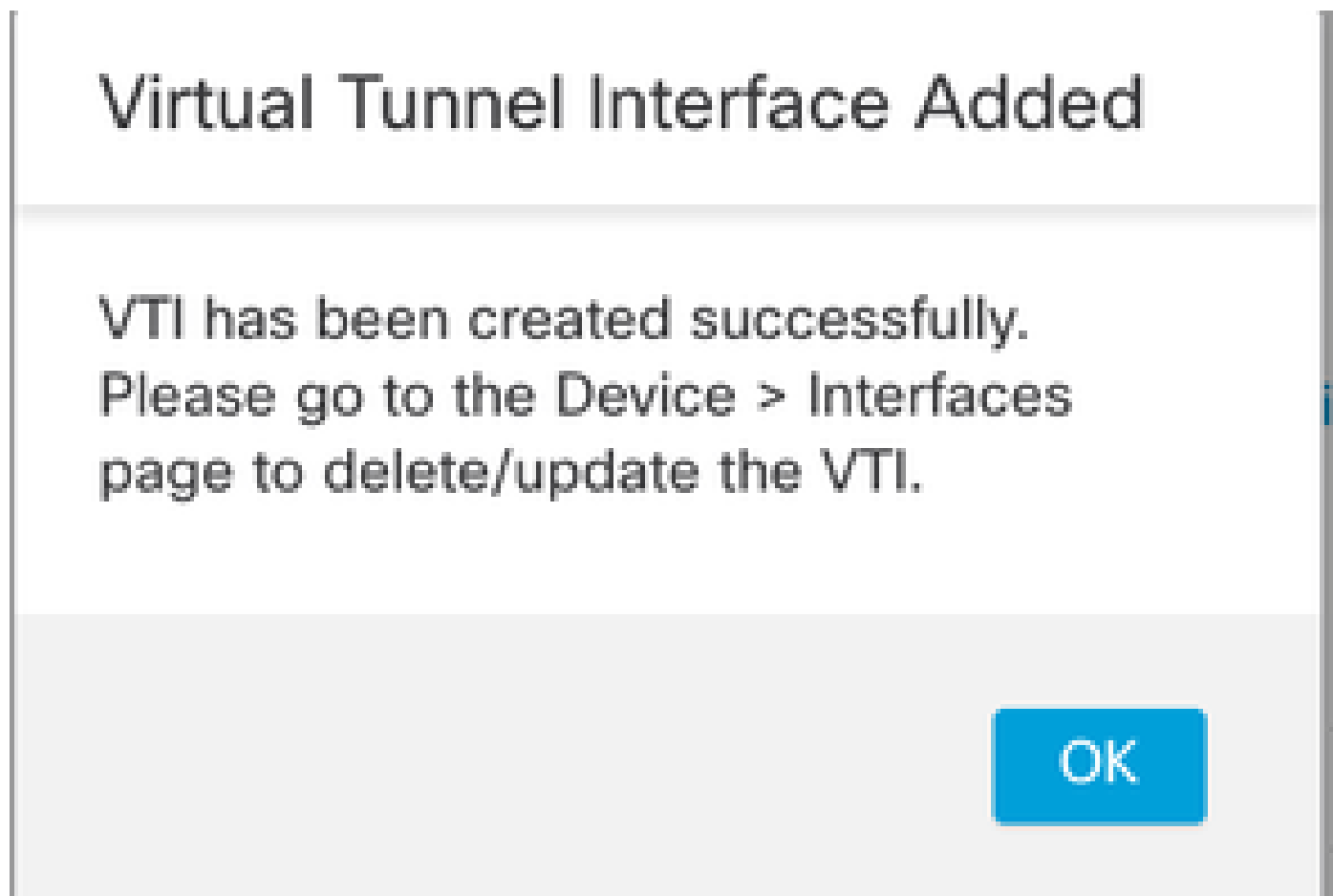
Loopback1 (loopback)



Cancel

OK

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



Interfaz de túnel virtual agregada

**Paso 7.** Seleccione 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: ASAv-Peer
- Dirección IP de 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 ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

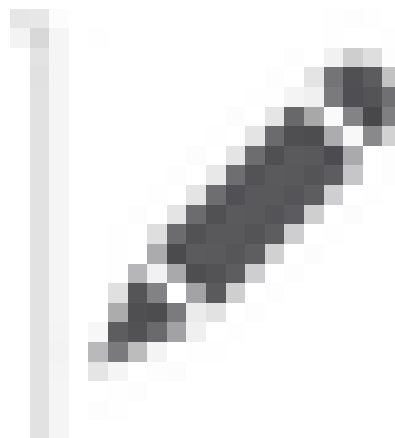
Node B

Device:\*  
Extranet

Device Name\*:  
ASAv-Peer

Endpoint IP Address\*:  
10.197.226.187

Nodo B de terminal



Paso 8. Acceda a la pestaña IKE. Haga clic en [Add](#). Puede optar por utilizar una ficha predefinida [Policy](#) o hacer clic en el [+](#) botón situado junto a la [Policy](#) ficha para crear una nueva.

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

Para esta demostración:

- Nombre: Política de ASAv-IKEv2
- 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

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

MD5

SHA

SHA512

SHA256

SHA384

NULL

Add

### Selected Algorithms

SHA256



Cancel

Save

IKEv2-Política

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

Para esta demostración:

- Política: ASAv-IKEv2-Política
- Tipo de autenticación: Clave manual precompartida

## IKEv2 Settings

Policies:\* ASAv-IKEv2-Policy

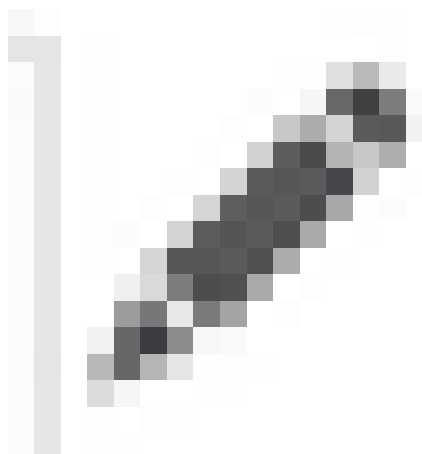
Authentication Type: Pre-shared Manual Key ▼

Key:\* .....

Confirm Key:\* .....

☐ Enforce hex-based pre-shared key only

## Autenticación



Paso 11. Acceda a la IPsec pestaña. Chasquido

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 un Name para 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:\*

ASAv-IPSec-Policy

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. Seleccione el **Proposal** o **Propuesta** recién creado de la lista de propuestas disponibles. Haga clic en **OK**.

## IKEv2 IPsec Proposal



Available Transform Sets  

 Search

AES-256-SHA-256

AES-GCM

AES-SHA

ASAv-IPSec-Policy

DES\_SHA-1

Umbrella-AES-GCM-256

Add

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 (Default)
- Tamaño de vida: 4608000 (Default)

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: 14 ▼

Lifetime Duration\*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

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

**Edit VPN Topology**

Topology Name: ASA-v-FTI

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version: ☐ IKEv1 ☒ IKEv2

**Endpoints** IKE IPsec Advanced

**Node A**

Device: FTD

Virtual Tunnel Interface: ASA-v-FTI (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 ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [ACL Policy](#)

**Node B**

Device: Extranet

Device Name: ASA-v-Peer

Endpoint IP Address: 10.197.226.187

**Save**

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**.

| 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         |                              | 10.197.226.227(23)(Static) | Disabled        | Global         |  |

Vaya a la interfaz de bucle invertido

Paso 2. Introduzca el nombre "loopback", proporcione un ID de loopback "1" y habilite 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 para la interfaz, 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**. Edite el dispositivo donde está configurado el túnel VTI, luego navegue hasta **Routing > General Settings > BGP**.

Paso 1. Habilite BGP y configure el número de sistema autónomo (AS) y el ID de 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.

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

Enable BGP: ☒

AS Number\*: 1000 (1-65535 or 1-4294967295)

Override BGP general settings router-id address: ☐

Router ID: Manual

IP Address\*: 10.1.1.1

General

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 EGP routes: Yes

Use dot notation for AS number: No

Aggregate Timer: 30

Neighbor Timers

Keepalive Interval: 60

Hold time: 180

Min hold time: 0

Next Hop

Address tracking: Yes

Delay interval: 5

Graceful Restart (Only in Release or Restarted Neighbor mode)

Graceful Restart: No

Restart time: 120

Stalepath time: 180

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

Vaya a configurar BGP

Paso 2. Desplácese hasta **BGP > IPv4 BGP IPv4** y habilítelo en el FTD.

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General

Neighbor

Add Aggregate Address

Filtering

Networks

Redistribution

Route Injection

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 BGP 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. Debajo de **Neighbor** la ficha, agregue la dirección IP del túnel VTI de ASAv como vecino y habilite el vecino.

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General

Neighbor

Add Aggregate Address

Filtering

Networks

Redistribution

Route Injection

Enable IPv4: ☒

AS Number: 1000

Neighbor

Address: 169.254.2.2

Remote AS Number: 1000

Address Family: Enabled

Remote Private AS Number

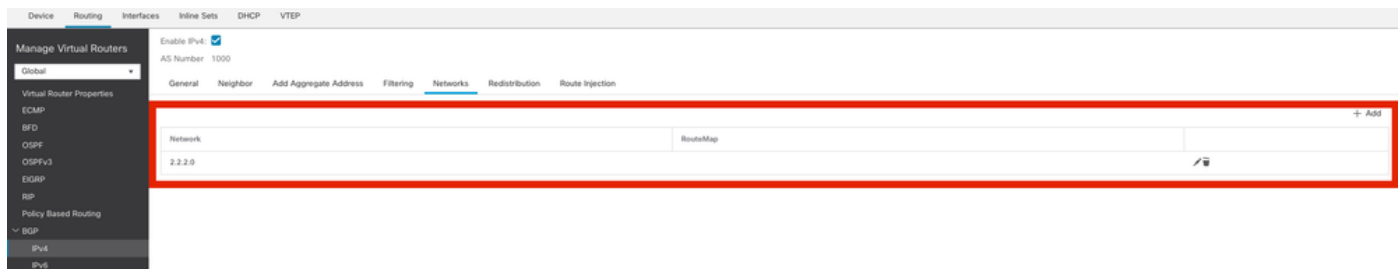
Description

+

Add

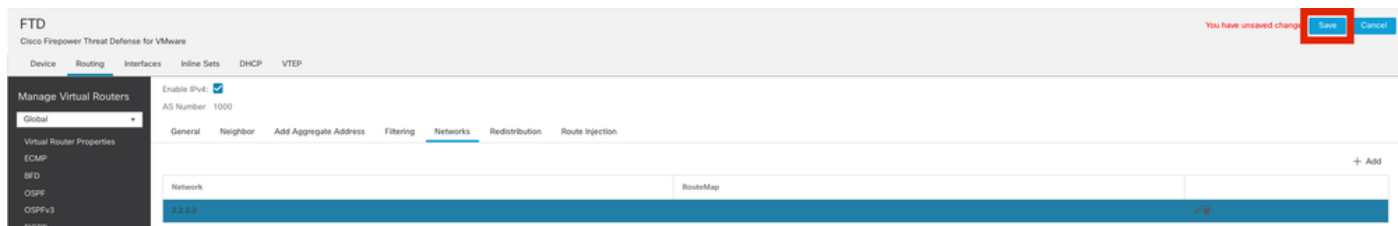
Agregar vecino BGP

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



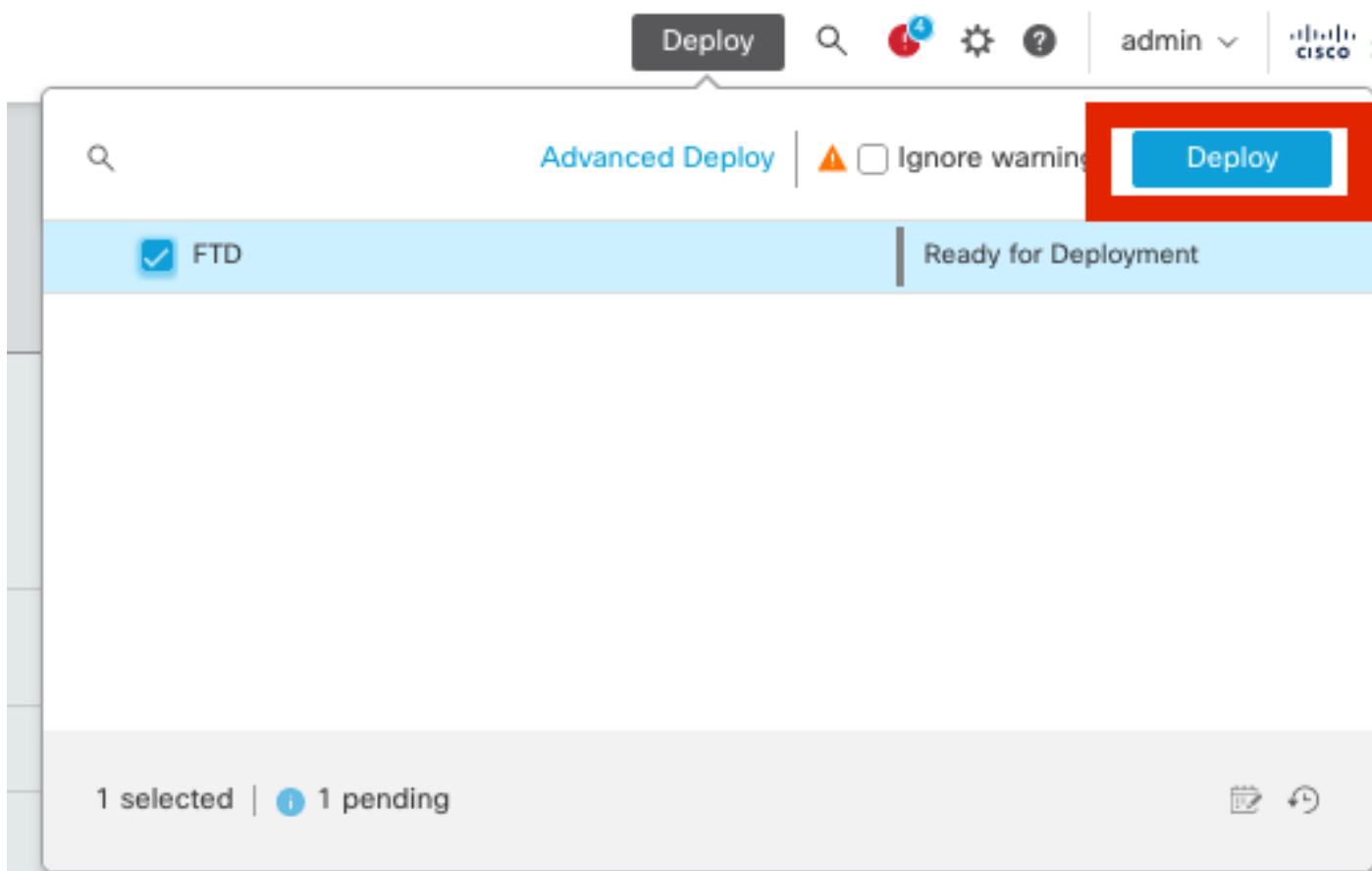
Agregar redes BGP

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**.



Guardar configuración BGP

Paso 6. Implemente todas las configuraciones.



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             | fvr/fivr      | 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 (ivr): 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             | fvr/fivr/f    | 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 (ivr/f): 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 multiseession capable (disabled)

Neighbor capabilities:  
Route refresh: advertised and received(new)  
Four-octets ASN Capability: advertised and received  
Address family IPv4 Unicast: advertised and received  
Multiseession 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).