

Configuración de FTD BGP sobre VPN IPSec

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de VPN IPSec](#)

[Configuración de BGP](#)

[Configuración final en ambos dispositivos](#)

[FTD1](#)

[FTD2](#)

[Verificación](#)

[FTD1](#)

[FTD2](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar la vecindad BGP a través de un túnel VPN de sitio a sitio IPsec entre dos Cisco FirePower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuraciones BGP en FTD
- Configuraciones de túnel VPN de sitio a sitio IPsec en FTD

Componentes Utilizados

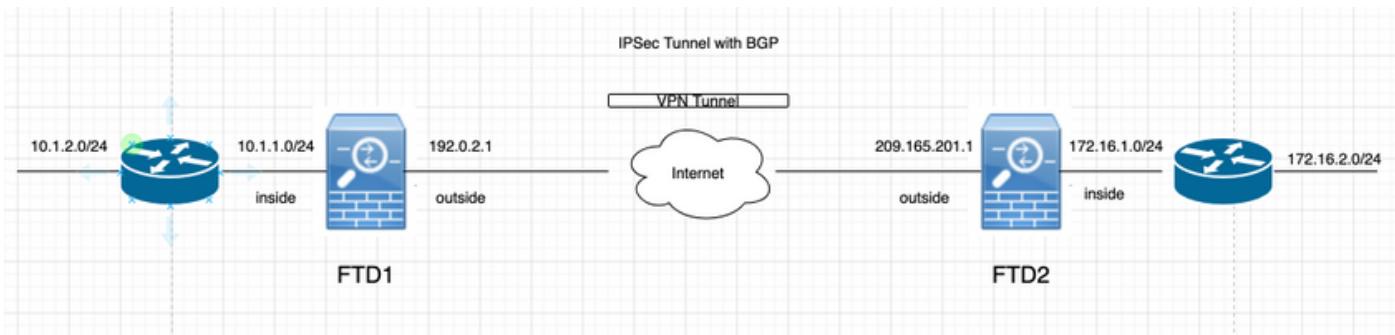
La información de este documento se basa en Cisco FTDrv que ejecuta 6.4.0.7 y 6.4.0.9.

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, make sure that you understand the potential impact of any command.

Configurar

Esta sección describe la configuración necesaria en los FTD para activar la vecindad BGP a través de un túnel IPSec.

Diagrama de la red



Configuración de VPN IPSec

Paso 1. Cree una nueva topología VPN punto a punto.

Navegue hasta **Devices > VPN > Site-to-Site** y agregue una nueva VPN de dispositivo FirePower Threat Defense.

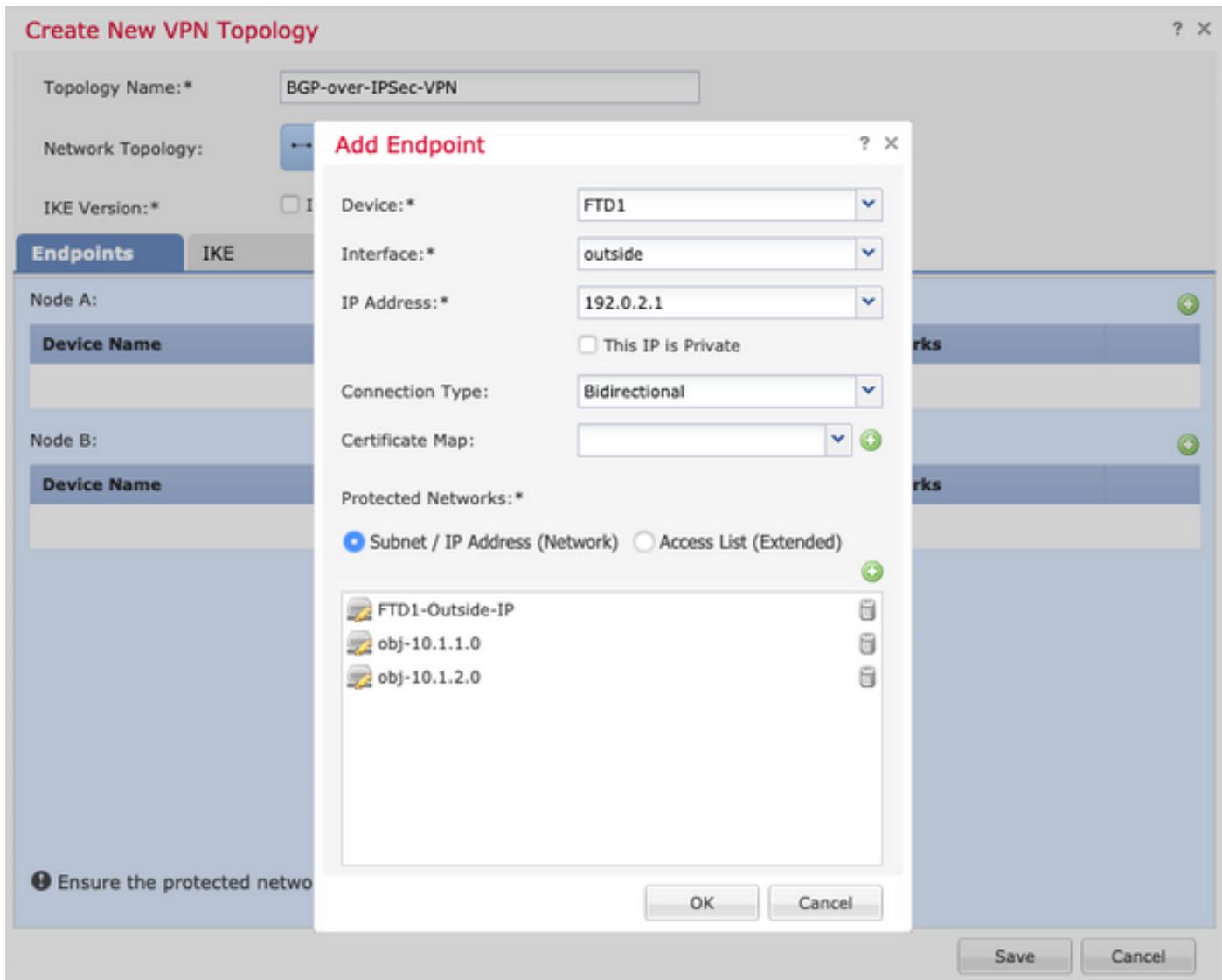
Create New VPN Topology

Topology Name:*	BGP-over-IPSec-VPN						
Network Topology:	<input checked="" type="radio"/> Point to Point <input type="radio"/> Hub and Spoke <input type="radio"/> Full Mesh						
IKE Version:*	<input type="checkbox"/> IKEv1 <input checked="" type="checkbox"/> IKEv2						
Endpoints IKE IPsec Advanced							
Node A:							
<table border="1"><thead><tr><th>Device Name</th><th>VPN Interface</th><th>Protected Networks</th></tr></thead><tbody><tr><td></td><td></td><td></td></tr></tbody></table>		Device Name	VPN Interface	Protected Networks			
Device Name	VPN Interface	Protected Networks					
Node B:							
<table border="1"><thead><tr><th>Device Name</th><th>VPN Interface</th><th>Protected Networks</th></tr></thead><tbody><tr><td></td><td></td><td></td></tr></tbody></table>		Device Name	VPN Interface	Protected Networks			
Device Name	VPN Interface	Protected Networks					

Nota: Ensure the protected networks are allowed by access control policy of each device.

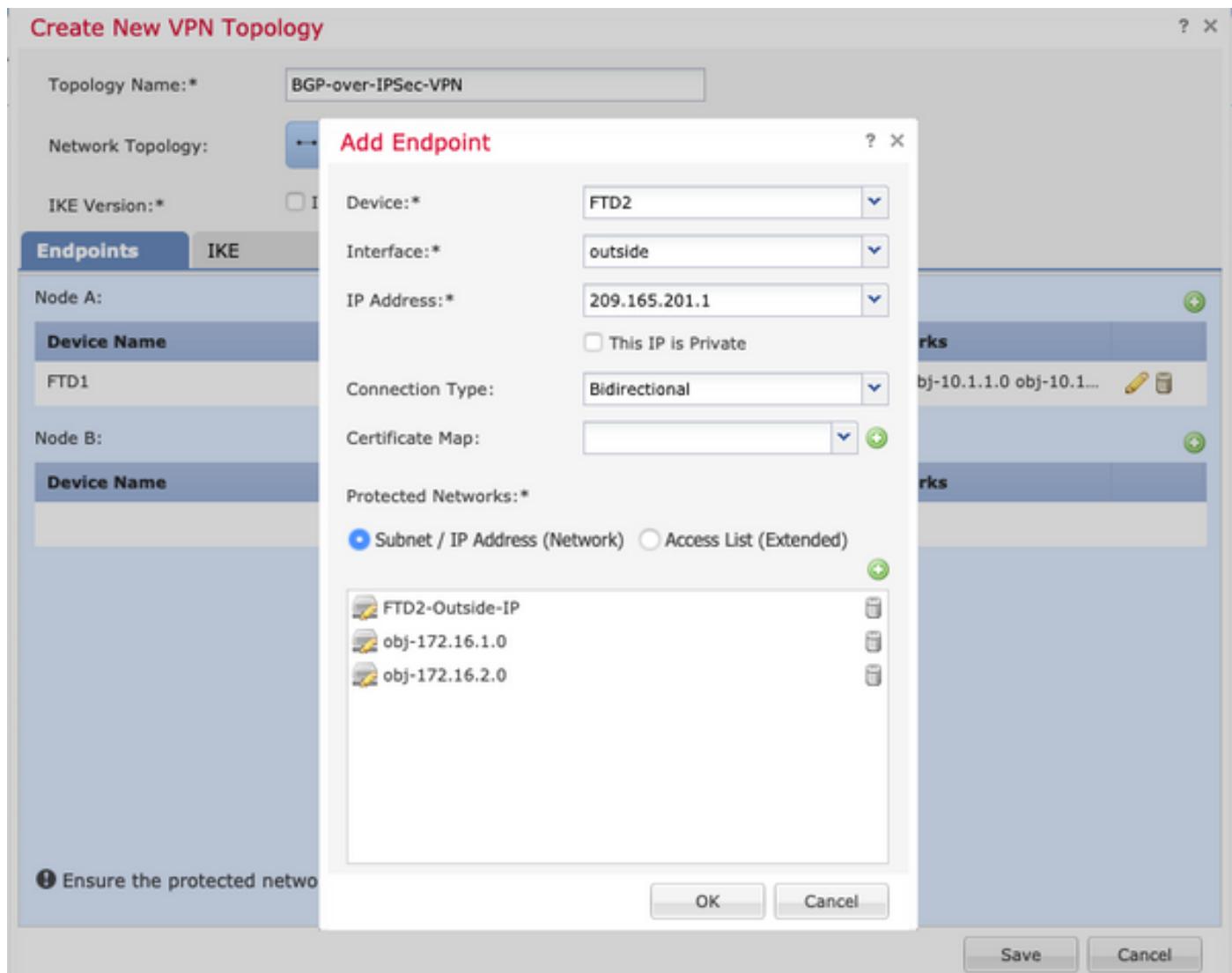
Save **Cancel**

Paso 2. Configure FTD1 como uno de los terminales.



- La red de objetos FTD1-Outside-IP contiene la dirección IP de la interfaz exterior del FTD1.
- Los objetos obj-10.1.1.0 y obj-10.1.2.0 contienen la subred 10.1.1.0/24 y 10.1.2.0/24 respectivamente. El tráfico VPN se genera a partir de estas subredes. En la sección de configuración de BGP aquí, BGP se configura para anunciar estas subredes a sus vecinos.

Paso 3. Configure FTD2 como el segundo terminal.



- La red de objetos FTD2-Outside-IP contiene la dirección IP de la interfaz exterior del FTD2.
- Los objetos obj-172.16.1.0 y obj-172.16.2.0 contienen la subred 172.16.1.0/24 y 172.16.2.0/24 respectivamente. El tráfico VPN se genera a partir de estas subredes. En la sección de configuración de BGP aquí, BGP se configura para anunciar estas subredes a sus vecinos.

Paso 4. Configure los parámetros IKE.

1. Configure la política IKEv2.
2. Configure el método de autenticación (PSK/Certificate).

Create New VPN Topology

Topology Name:

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:

Authentication Type:

Pre-shared Key Length: Characters (Range 1-127)

IKEv2 Settings

Policy:

Authentication Type:

Key:

Confirm Key:

Enforce hex-based pre-shared key only

Save **Cancel**

Paso 5. Configure los parámetros IPSec necesarios.

1. Configurar el tipo de mapa criptográfico (estático o dinámico)
2. Configuración del modo IKEv2 (túnel o transporte)
3. Configurar propuestas IPSec
4. Activar confidencialidad directa perfecta (opcional)
5. Habilitar inyección de ruta inversa (opcional)

Create New VPN Topology

Topology Name:

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel Transport

Transform Sets:

IKEv1 IPsec Proposals	IKEv2 IPsec Proposals*
tunnel_des_sha	DES_SHA-1

Enable Security Association (SA) Strength Enforcement
 Enable Reverse Route Injection
 Enable Perfect Forward Secrecy

Modulus Group: 2 5 14 18 20 23 24 26 31 35 51 71 89 103 139 167 179 193 223 233 239 251 283 317 337 367 397 431 463 503 541 571 601 631 653 683 701 727 751 781 809 839 863 881 907 931 961 991 1021 1031 1051 1061 1081 1103 1123 1143 1163 1183 1201 1223 1243 1261 1283 1301 1321 1343 1361 1383 1401 1423 1443 1461 1483 1501 1523 1543 1561 1583 1601 1623 1643 1661 1683 1701 1723 1743 1761 1783 1801 1823 1843 1861 1883 1901 1923 1943 1961 1983 2001 2023 2043 2061 2083 2101 2123 2143 2161 2183 2201 2223 2243 2261 2283 2301 2323 2343 2361 2383 2401 2423 2443 2461 2483 2501 2523 2543 2561 2583 2601 2623 2643 2661 2683 2701 2723 2743 2761 2783 2801 2823 2843 2861 2883 2901 2923 2943 2961 2983 3001 3023 3043 3061 3083 3101 3123 3143 3161 3183 3201 3223 3243 3261 3283 3301 3323 3343 3361 3383 3401 3423 3443 3461 3483 3501 3523 3543 3561 3583 3601 3623 3643 3661 3683 3701 3723 3743 3761 3783 3801 3823 3843 3861 3883 3901 3923 3943 3961 3983 4001 4023 4043 4061 4083 4101 4123 4143 4161 4183 4201 4223 4243 4261 4283 4301 4323 4343 4361 4383 4401 4423 4443 4461 4483 4501 4523 4543 4561 4583 4601 4623 4643 4661 4683 4701 4723 4743 4761 4783 4801 4823 4843 4861 4883 4901 4923 4943 4961 4983 5001 5023 5043 5061 5083 5101 5123 5143 5161 5183 5201 5223 5243 5261 5283 5301 5323 5343 5361 5383 5401 5423 5443 5461 5483 5501 5523 5543 5561 5583 5601 5623 5643 5661 5683 5701 5723 5743 5761 5783 5801 5823 5843 5861 5883 5901 5923 5943 5961 5983 6001 6023 6043 6061 6083 6101 6123 6143 6161 6183 6201 6223 6243 6261 6283 6301 6323 6343 6361 6383 6401 6423 6443 6461 6483 6501 6523 6543 6561 6583 6601 6623 6643 6661 6683 6701 6723 6743 6761 6783 6801 6823 6843 6861 6883 6901 6923 6943 6961 6983 7001 7023 7043 7061 7083 7101 7123 7143 7161 7183 7201 7223 7243 7261 7283 7301 7323 7343 7361 7383 7401 7423 7443 7461 7483 7501 7523 7543 7561 7583 7601 7623 7643 7661 7683 7701 7723 7743 7761 7783 7801 7823 7843 7861 7883 7901 7923 7943 7961 7983 8001 8023 8043 8061 8083 8101 8123 8143 8161 8183 8201 8223 8243 8261 8283 8301 8323 8343 8361 8383 8401 8423 8443 8461 8483 8501 8523 8543 8561 8583 8601 8623 8643 8661 8683 8701 8723 8743 8761 8783 8801 8823 8843 8861 8883 8901 8923 8943 8961 8983 9001 9023 9043 9061 9083 9101 9123 9143 9161 9183 9201 9223 9243 9261 9283 9301 9323 9343 9361 9383 9401 9423 9443 9461 9483 9501 9523 9543 9561 9583 9601 9623 9643 9661 9683 9701 9723 9743 9761 9783 9801 9823 9843 9861 9883 9901 9923 9943 9961 9983 10001 10023 10043 10061 10083 10101 10123 10143 10161 10183 10201 10223 10243 10261 10283 10301 10323 10343 10361 10383 10401 10423 10443 10461 10483 10501 10523 10543 10561 10583 10601 10623 10643 10661 10683 10701 10723 10743 10761 10783 10801 10823 10843 10861 10883 10901 10923 10943 10961 10983 11001 11023 11043 11061 11083 11101 11123 11143 11161 11183 11201 11223 11243 11261 11283 11301 11323 11343 11361 11383 11401 11423 11443 11461 11483 11501 11523 11543 11561 11583 11601 11623 11643 11661 11683 11701 11723 11743 11761 11783 11801 11823 11843 11861 11883 11901 11923 11943 11961 11983 12001 12023 12043 12061 12083 12101 12123 12143 12161 12183 12201 12223 12243 12261 12283 12301 12323 12343 12361 12383 12401 12423 12443 12461 12483 12501 12523 12543 12561 12583 12601 12623 12643 12661 12683 12701 12723 12743 12761 12783 12801 12823 12843 12861 12883 12901 12923 12943 12961 12983 13001 13023 13043 13061 13083 13101 13123 13143 13161 13183 13201 13223 13243 13261 13283 13301 13323 13343 13361 13383 13401 13423 13443 13461 13483 13501 13523 13543 13561 13583 13601 13623 13643 13661 13683 13701 13723 13743 13761 13783 13801 13823 13843 13861 13883 13901 13923 13943 13961 13983 14001 14023 14043 14061 14083 14101 14123 14143 14161 14183 14201 14223 14243 14261 14283 14301 14323 14343 14361 14383 14401 14423 14443 14461 14483 14501 14523 14543 14561 14583 14601 14623 14643 14661 14683 14701 14723 14743 14761 14783 14801 14823 14843 14861 14883 14901 14923 14943 14961 14983 15001 15023 15043 15061 15083 15101 15123 15143 15161 15183 15201 15223 15243 15261 15283 15301 15323 15343 15361 15383 15401 15423 15443 15461 15483 15501 15523 15543 15561 15583 15601 15623 15643 15661 15683 15701 15723 15743 15761 15783 15801 15823 15843 15861 15883 15901 15923 15943 15961 15983 16001 16023 16043 16061 16083 16101 16123 16143 16161 16183 16201 16223 16243 16261 16283 16301 16323 16343 16361 16383 16401 16423 16443 16461 16483 16501 16523 16543 16561 16583 16601 16623 16643 16661 16683 16701 16723 16743 16761 16783 16801 16823 16843 16861 16883 16901 16923 16943 16961 16983 17001 17023 17043 17061 17083 17101 17123 17143 17161 17183 17201 17223 17243 17261 17283 17301 17323 17343 17361 17383 17401 17423 17443 17461 17483 17501 17523 17543 17561 17583 17601 17623 17643 17661 17683 17701 17723 17743 17761 17783 17801 17823 17843 17861 17883 17901 17923 17943 17961 17983 18001 18023 18043 18061 18083 18101 18123 18143 18161 18183 18201 18223 18243 18261 18283 18301 18323 18343 18361 18383 18401 18423 18443 18461 18483 18501 18523 18543 18561 18583 18601 18623 18643 18661 18683 18701 18723 18743 18761 18783 18801 18823 18843 18861 18883 18901 18923 18943 18961 18983 19001 19023 19043 19061 <input type="

Create New VPN Topology

Topology Name:

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints **IKE** **IPsec** **Advanced**

IKE

ISAKAMP Settings

IKE Keepalive: Enable

Threshold: Seconds (Range 10 - 3600)

Retry Interval: Seconds (Range 2 - 10)

Identity Sent to Peers: autoOrDN

Peer Identity Validation: Required

Enable Aggressive Mode

Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

Threshold to Challenge Incoming Cookies: %

Number of SAs Allowed in Negotiation: %

Maximum number of SAs Allowed: Device maximum

Save **Cancel**

Configuración de BGP

Este es el procedimiento para configurar FTD1 y FTD2.

En **Administración de dispositivos** y seleccione el dispositivo, navegue hasta **Ruteo > BGP**.

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

BGP

Enable BGP:

AS Number*: (1-4294967295 or 1.0-65535-65535)

General	Neighbor Timers
Router ID	Keepalive Interval
Number of AS numbers in AS_PATH attribute of received routes	Hold time
Log Neighbor Changes	Min hold time
Use TCP path MTU discovery	Graceful Restart (use in failover or spanned cluster mode)
Reset session upon failover	Graceful Restart
Enforce the first AS is peer's AS for EBGP routes	Restart time
Use dot notation for AS number	Stalepath time
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

2. Navegue hasta **BGP > IPv4** y habilite BGP IPv4 en el FTD, como se muestra en esta imagen.

Enable IPv4:

AS Number: 100

General **Neighbor** **Add Aggregate Address** **Filtering** **Networks** **Redistribution** **Route Injection**

Setting

Learned Route Map	<input type="button" value="Edit"/>
Scanning Interval	60

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

General 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	No

(Use filtering to limit the number of prefixes that are redistributed)

Next Hop

Address tracking	Yes
Delay interval	5

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

3. En la pestaña Vecino, agregue el otro FTD como vecino y habilite al vecino, como se muestra en esta imagen.

Enable IPv4:

AS Number: 100

General **Neighbor** **Add Aggregate Address** **Filtering** **Networks** **Redistribution** **Route Injection**

Address **Remote AS Number** **Address Family** **Remote Private AS Number** **Description**

209.165.201.1	100	Enabled		
---------------	-----	---------	--	--

4. En la pestaña Redes, agregue las redes que desea anunciar a través de BGP.

Enable IPv4:

AS Number: 100

General **Neighbor** **Add Aggregate Address** **Filtering** **Networks** **Redistribution** **Route Injection**

Network **RouteMap**

obj-10.1.1.0	<input type="button" value="Edit"/>
obj-10.1.2.0	<input type="button" value="Edit"/>

5. Todos los demás parámetros de BGP son opcionales y puede configurarlos según su entorno.

Configuración final en ambos dispositivos

FTD1

```
!---- FTD Version ---! ftd1# show version -----[ ftd1 ]-----
Model : Cisco Firepower Threat Defense for VMWare (75) Version 6.4.0.7 (Build 53) UUID :
cbd4966c-daf4-11ea-8637-c8977622bc2d Rules update version : 2018-10-10-001-vrt VDB version : 309
----- Cisco Adaptive Security Appliance Software
Version 9.12(2)151 !--- Configure the Inside and outside interface ---! interface
GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag policy static sgt
disabled trusted security-level 0 ip address 192.0.2.1 255.255.255.0 ! interface
GigabitEthernet0/1 nameif inside cts manual propagate sgt preserve-untag policy static sgt
disabled trusted security-level 0 ip address 10.1.1.1 255.255.255.0 !--- Configure VPN ---! !---
Configure IPSec Policy ---! crypto ipsec ikev2 ipsec-proposal CSM_IP_1 protocol esp encryption
des protocol esp integrity sha-1 !--- Configure Crypto Map ---! crypto map CSM_outside_map 1
match address CSM_IPSEC_ACL_2 crypto map CSM_outside_map 1 set peer 209.165.201.1 crypto map
CSM_outside_map 1 set ikev2 ipsec-proposal CSM_IP_1 crypto map CSM_outside_map 1 set reverse-
route !--- Apply the Crypto Map to the outside interface ---! crypto map CSM_outside_map
interface outside !--- Configure IKEv2 policy ---! crypto ikev2 policy 80 encryption des
integrity sha group 5 prf sha lifetime seconds 86400 !--- Enable IKEv2 on the outside interface
---! crypto ikev2 enable outside !--- Configure BGP Router Process ---! router bgp 100 bgp log-
neighbor-changes bgp router-id 10.127.248.35 address-family ipv4 unicast neighbor 209.165.201.1
remote-as 100 neighbor 209.165.201.1 transport path-mtu-discovery disable neighbor 209.165.201.1
```

```
activate network 10.1.1.0 mask 255.255.255.0 network 10.1.2.0 mask 255.255.255.0 no auto-summary  
no synchronization exit-address-family ! --- Configure the necessary routes ---! route outside  
0.0.0.0 0.0.0.0 192.0.2.100 1 route inside 10.1.2.0 255.255.255.0 10.1.1.100 1
```

FTD2

```
!--- FTD Version ---! ftd2# show version -----[ ftd2 ]-----  
Model : Cisco Firepower Threat Defense for VMWare (75) Version 6.4.0.9 (Build 62) UUID :  
4ebe8e3a-dd8d-11ea-a599-a348a450d5ff Rules update version : 2018-10-10-001-vrt VDB version : 309  
----- Cisco Adaptive Security Appliance Software  
Version 9.12(2)33 !--- Configure the Inside and outside interface ---! interface  
GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag policy static sgt  
disabled trusted security-level 0 ip address 209.165.201.1 255.255.255.0 ! interface  
GigabitEthernet0/1 nameif inside cts manual propagate sgt preserve-untag policy static sgt  
disabled trusted security-level 0 ip address 172.16.1.1 255.255.255.0 !--- Configure VPN ---! !--  
Configure IPSec Policy ---! crypto ipsec ikev2 ipsec-proposal CSM_IP_1 protocol esp  
encryption des protocol esp integrity sha-1 !--- Configure Crypto Map ---! crypto map  
CSM_outside_map 2 match address CSM_IPSEC_ACL_2 crypto map CSM_outside_map 2 set peer 192.0.2.1  
crypto map CSM_outside_map 2 set ikev2 ipsec-proposal CSM_IP_1 crypto map CSM_outside_map 2 set  
reverse-route !--- Apply the Crypto Map to the outside interface ---! crypto map CSM_outside_map  
interface outside !--- Configure IKEv2 policy ---! crypto ikev2 policy 80 encryption des  
integrity sha group 5 prf sha lifetime seconds 86400 !--- Enable IKEv2 on the outside interface  
---! crypto ikev2 enable outside !--- Configure BGP Router Process ---! router bgp 100 bgp log-  
neighbor-changes bgp router-id 10.127.248.36 address-family ipv4 unicast neighbor 192.0.2.1  
remote-as 100 neighbor 192.0.2.1 transport path-mtu-discovery disable neighbor 192.0.2.1  
activate network 172.16.1.0 mask 255.255.255.0 network 172.16.2.0 mask 255.255.255.0 no auto-  
summary no synchronization exit-address-family !--- Configure the necessary routes ---! route  
outside 0.0.0.0 0.0.0.0 209.165.201.100 1 route inside 172.16.2.0 255.255.255.0 172.16.1.100 1
```

Verificación

FTD1

```
!--- Check the IKEv2 sa with remote peer ---! ftd1# show crypto ikev2 sa IKEv2 SAs: Session-  
id:34, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote Status Role 315310279  
192.0.2.1/500 209.165.201.1/500 READY INITIATOR Encr: DES, Hash: SHA96, DH Grp:5, Auth sign:  
PSK, Auth verify: PSK Life/Active Time: 86400/32514 sec Child sa: local selector 192.0.2.1/0 -  
192.0.2.1/65535 remote selector 209.165.201.1/0 - 209.165.201.1/65535 ESP spi in/out:  
0xd8ba0545/0x4b6beb6c !--- Check the IPsec sa with remote peer and check the number of encrypts  
and decrypts---! ftd1# show crypto ipsec sa interface: outside Crypto map tag: CSM_outside_map,  
seq num: 1, local addr: 192.0.2.1 access-list CSM_IPSEC_ACL_2 extended permit ip host 192.0.2.1  
host 209.165.201.1 local ident (addr/mask/prot/port): (192.0.2.1/255.255.255.255/0/0) remote  
ident (addr/mask/prot/port): (209.165.201.1/255.255.255.255/0/0) current_peer: 209.165.201.1  
#pkts encaps: 1110, #pkts encrypt: 1110, #pkts digest: 1110 #pkts decaps: 1111, #pkts decrypt:  
1111, #pkts verify: 1111 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 1110,  
#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.: 192.0.2.1/500, remote crypto endpt.:  
209.165.201.1/500 path mtu 1500, ipsec overhead 58(36), media mtu 1500 PMTU time remaining  
(sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current  
outbound spi: 4B6BEB6C current inbound spi : D8BA0545 inbound esp sas: spi: 0xD8BA0545  
(3636069701) SA State: active transform: esp-des esp-sha-hmac no compression in use settings  
={L2L, Tunnel, IKEv2, } slot: 0, conn_id: 1515, crypto-map: CSM_outside_map sa timing: remaining  
key lifetime (kB/sec): (4101105/21619) IV size: 8 bytes replay detection support: Y Anti replay  
bitmap: 0xFFFFFFFF 0xFFFFFFFF outbound esp sas: spi: 0x4B6BEB6C (1265363820) SA State: active  
transform: esp-des esp-sha-hmac no compression in use settings ={L2L, Tunnel, IKEv2, } slot: 0,  
conn_id: 1515, crypto-map: CSM_outside_map sa timing: remaining key lifetime (kB/sec):  
(4239345/21619) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0x00000000  
0x00000001 !--- Check the BGP router summary ---! ftd1# show bgp summary BGP router identifier
```

10.127.248.35, local AS number 100 BGP table version is 43, main routing table version 43 4
 network entries using 800 bytes of memory 4 path entries using 320 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 1536 total
 bytes of memory BGP activity 20/16 prefixes, 26/22 paths, scan interval 60 secs Neighbor V AS
 MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 209.165.201.1 4 100 494 488 43 0 0 09:01:15
 2 !--- Check the BGP neighborship ---! ftd1# show bgp neighbors BGP neighbor is 209.165.201.1,
 context single_vf, remote AS 100, internal link BGP version 4, remote router ID 10.127.248.36
 BGP state = Established, up for 09:01:18 Last read 00:00:52, last write 00:00:12, 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: 3 3 Keepalives: 484 490 Route Refresh: 0 0 Total: 488 494 Default
 minimum time between advertisement runs is 0 seconds For address family: IPv4 Unicast Session:
 209.165.201.1 BGP table version 43, neighbor version 43/0 Output queue size : 0 Index 19 19
 update-group member Sent Rcvd Prefix activity: ---- Prefixes Current: 2 2 (Consumes 160
 bytes) Prefixes Total: 2 2 Implicit Withdraw: 0 0 Explicit Withdraw: 0 0 Used as bestpath: n/a 2
 Used as multipath: n/a 0 Outbound Inbound Local Policy Denied Prefixes: -----
 Bestpath from this peer: 2 n/a Invalid Path: 1 n/a Total: 3 0 Number of NLRI's in the update
 sent: max 1, min 0 Address tracking is enabled, the RIB does have a route to 209.165.201.1
 Connections established 2; dropped 1 Last reset 09:01:34, due to Peer closed the session of
 session 1 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled !--- Check
 the routes learned from BGP ---! ftd1# sh 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 Gateway of last resort is 192.0.2.100 to network
 0.0.0.0 B 172.16.1.0 255.255.255.0 [200/0] via 209.165.201.1, 00:00:57 B 172.16.2.0
 255.255.255.0 [200/0] via 172.16.1.100, 09:01:23

FTD2

!--- Check the IKEv2 sa with remote peer ---! ftd2# show crypto ikev2 sa IKEv2 SAs: Session-
 id:34, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote Status Role 862624945
 209.165.201.1/500 192.0.2.1/500 READY RESPONDER Encr: DES, Hash: SHA96, DH Grp:5, Auth sign:
 PSK, Auth verify: PSK Life/Active Time: 86400/32429 sec Child sa: local selector 209.165.201.1/0
 - 209.165.201.1/65535 remote selector 192.0.2.1/0 - 192.0.2.1/65535 ESP spi in/out:
 0x4b6beb6c/0xd8ba0545 !--- Check the IPsec sa with remote peer and check the number of encrypts
 and decrypts---! ftd2# show crypto ipsec sa interface: outside Crypto map tag: CSM_outside_map,
 seq num: 2, local addr: 209.165.201.1 access-list CSM_IPSEC_ACL_2 extended permit ip host
 209.165.201.1 host 192.0.2.1 local ident (addr/mask/prot/port):
 (209.165.201.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port):
 (192.0.2.1/255.255.255.255/0/0) current_peer: 192.0.2.1 #pkts encaps: 1107, #pkts encrypt: 1107,
 #pkts digest: 1107 #pkts decaps: 1106, #pkts decrypt: 1106, #pkts verify: 1106 #pkts compressed:
 0, #pkts decompressed: 0 #pkts not compressed: 1107, #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.:
 209.165.201.1/500, remote crypto endpt.: 192.0.2.1/500 path mtu 1500, ipsec overhead 58(36),
 media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled,
 TFC packets: disabled current outbound spi: D8BA0545 current inbound spi : 4B6BEB6C inbound esp
 sas: spi: 0x4B6BEB6C (1265363820) SA State: active transform: esp-des esp-sha-hmac no
 compression in use settings ={L2L, Tunnel, IKEv2, } slot: 0, conn_id: 1516, crypto-map:
 CSM_outside_map sa timing: remaining key lifetime (kB/sec): (4008945/21713) IV size: 8 bytes
 replay detection support: Y Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF outbound esp sas: spi:
 0xD8BA0545 (3636069701) SA State: active transform: esp-des esp-sha-hmac no compression in use
 settings ={L2L, Tunnel, IKEv2, } slot: 0, conn_id: 1516, crypto-map: CSM_outside_map sa timing:
 remaining key lifetime (kB/sec): (4239345/21713) IV size: 8 bytes replay detection support: Y
 Anti replay bitmap: 0x00000000 0x00000001 !--- Check the BGP router summary ---! ftd2# show bgp
 summary BGP router identifier 10.127.248.36, local AS number 100 BGP table version is 44, main

```
routing table version 44 3 network entries using 600 bytes of memory 3 path entries using 240
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 1256 total bytes of memory BGP activity 20/17 prefixes, 26/23 paths, scan
interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 192.0.2.1 4
100 486 492 44 0 0 08:59:40 2 !--- Check the BGP neighborship ---! ftd2# show bgp neighbors BGP
neighbor is 192.0.2.1, context single_vf, remote AS 100, internal link BGP version 4, remote
router ID 10.127.248.35 BGP state = Established, up for 08:59:42 Last read 00:00:53, 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 3 Keepalives: 489 482 Route Refresh: 0 0
Total: 492 486 Default minimum time between advertisement runs is 0 seconds For address family:
IPv4 Unicast Session: 192.0.2.1 BGP table version 44, neighbor version 44/0 Output queue size :
0 Index 19 19 update-group member Sent Rcvd Prefix activity: ---- ----- Prefixes Current: 1 2
(Consumes 160 bytes) Prefixes Total: 1 2 Implicit Withdraw: 0 0 Explicit Withdraw: 0 0 Used as
bestpath: n/a 2 Used as multipath: n/a 0 Outbound Inbound Local Policy Denied Prefixes: -----
----- Bestpath from this peer: 2 n/a Invalid Path: 2 n/a Total: 4 0 Number of NLRIs in the
update sent: max 1, min 0 Address tracking is enabled, the RIB does have a route to 192.0.2.1
Connections established 2; dropped 1 Last reset 08:59:57, due to Peer closed the session of
session 1 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled !--- Check
the routes learned from BGP ---! ftd2# 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 Gateway of last resort is 209.165.201.100
to network 0.0.0.0 B 10.1.1.0 255.255.255.0 [200/0] via 192.0.2.1, 08:59:46 B 10.1.2.0
255.255.255.0 [200/0] via 10.1.1.100, 08:59:46
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.