

# 通过IPSec VPN配置FTD BGP

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置IPSec VPN](#)

[配置BGP](#)

[两台设备的最终配置](#)

[FTD1](#)

[FTD2](#)

[验证](#)

[FTD1](#)

[FTD2](#)

[故障排除](#)

## 简介

本文档介绍如何在两个Cisco FirePower威胁防御(FTD)之间通过IPsec站点到站点VPN隧道配置边界网关协议(BGP)邻居关系。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- FTD上的BGP配置
- FTD上的IPsec站点到站点VPN隧道配置

### 使用的组件

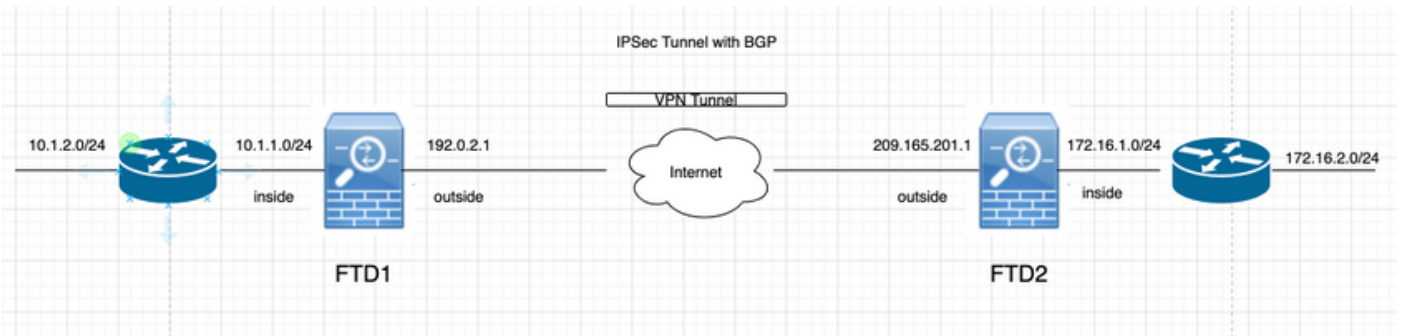
本文档中的信息基于运行6.4.0.7和6.4.0.9的Cisco FTDv。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

本节介绍在FTD上通过IPSec隧道建立BGP邻居关系所需的配置。

## 网络图



## 配置IPSec VPN

步骤1.创建新的点对点VPN拓扑。

导航至Devices > VPN > Site-to-Site，然后添加新的FirePower威胁防御设备VPN。

**Create New VPN Topology**

Topology Name: \*

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version: \*  IKEv1  IKEv2

**Endpoints** | IKE | IPsec | Advanced

Node A: +

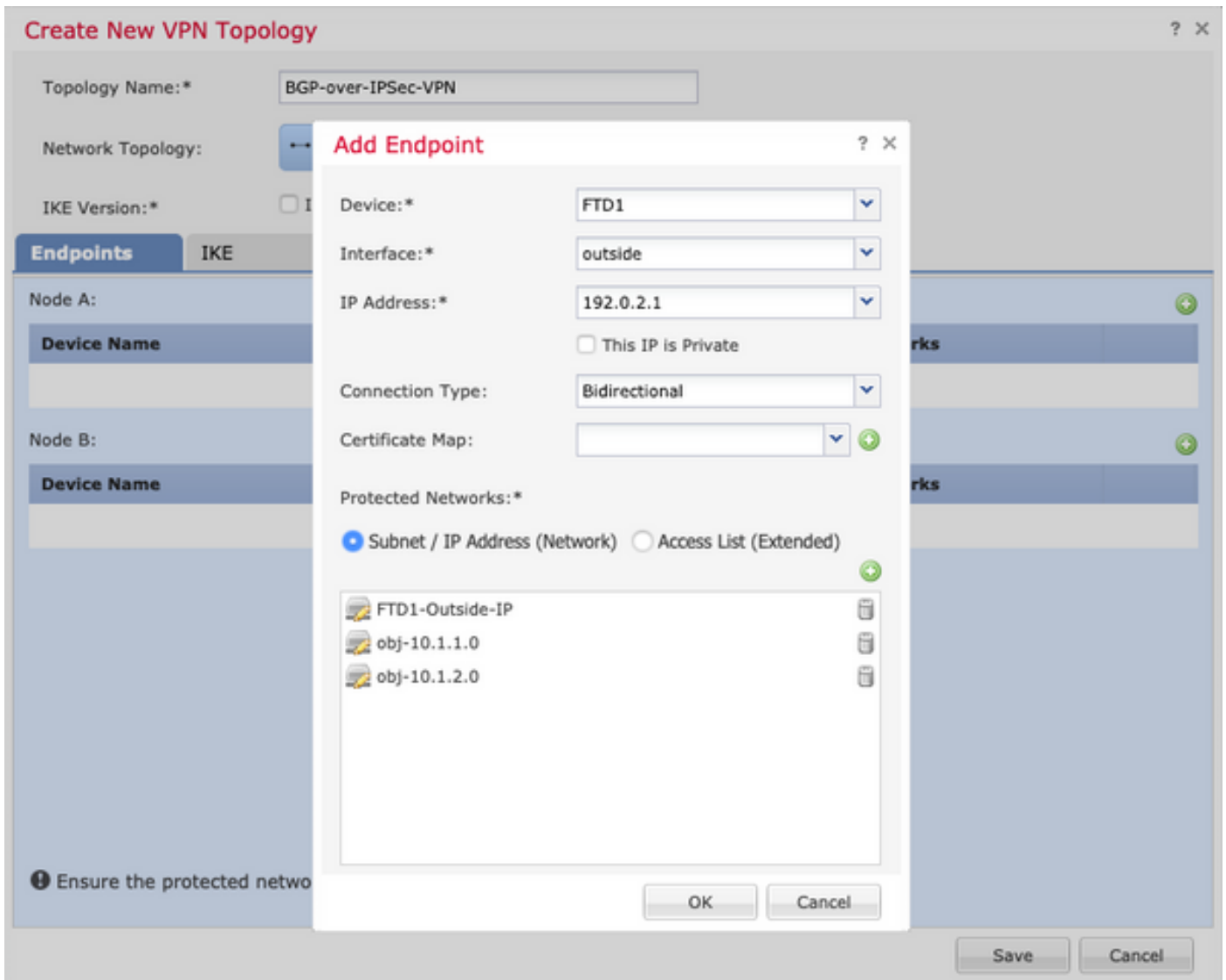
Device Name	VPN Interface	Protected Networks

Node B: +

Device Name	VPN Interface	Protected Networks

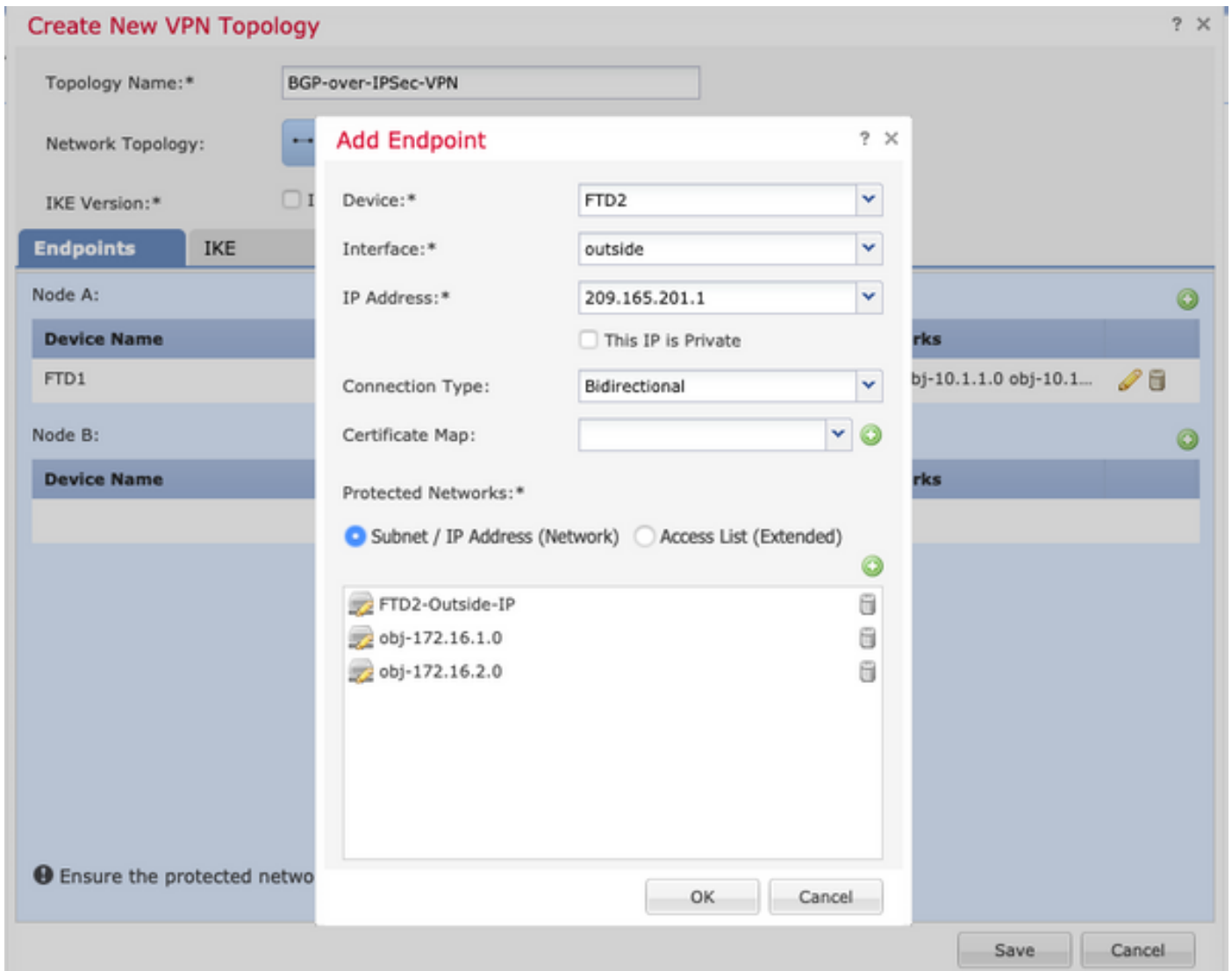
**i** Ensure the protected networks are allowed by access control policy of each device.

步骤2.将FTD1配置为终端之一。



- 对象网络FTD1-Outside-IP包含FTD1的外部接口IP地址。
- 对象obj-10.1.1.0和obj-10.1.2.0分别包含子网10.1.1.0/24和10.1.2.0/24。VPN流量从这些子网生成。在此处的BGP配置部分，BGP配置为向其邻居通告这些子网。

步骤3.将FTD2配置为第二个终端。



- 对象网络FTD2-Outside-IP包含FTD2的外部接口IP地址。
- 对象obj-172.16.1.0和obj-172.16.2.0分别包含子网172.16.1.0/24和172.16.2.0/24。VPN流量从这些子网生成。在此处的BGP配置部分，BGP配置为向其邻居通告这些子网。

#### 步骤4. 配置IKE参数。

1. 配置IKEv2策略。
2. 配置身份验证方法(PSK/Certificate)。

**Create New VPN Topology** ? X

Topology Name:\* BGP-over-IPSec-VPN

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

IKE Version:\*  IKEv1  IKEv2

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

**IKEv1 Settings**

Policy:\* preshared\_sha\_des\_dh5\_160 +

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

**IKEv2 Settings**

Policy:\* DES-SHA-SHA +

Authentication Type: Pre-shared Manual Key

Key:\* \*\*\*\*\*

Confirm Key:\* \*\*\*\*\*

Enforce hex-based pre-shared key only

Save Cancel

步骤5.配置必要的IPSec参数。

1. 配置加密映射类型 ( 静态或动态 )
2. 配置IKEv2模式 ( 隧道或传输 )
3. 配置IPSec建议
4. 启用完全向前保密 ( 可选 )
5. 启用反向路由注入 ( 可选 )

### 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:

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

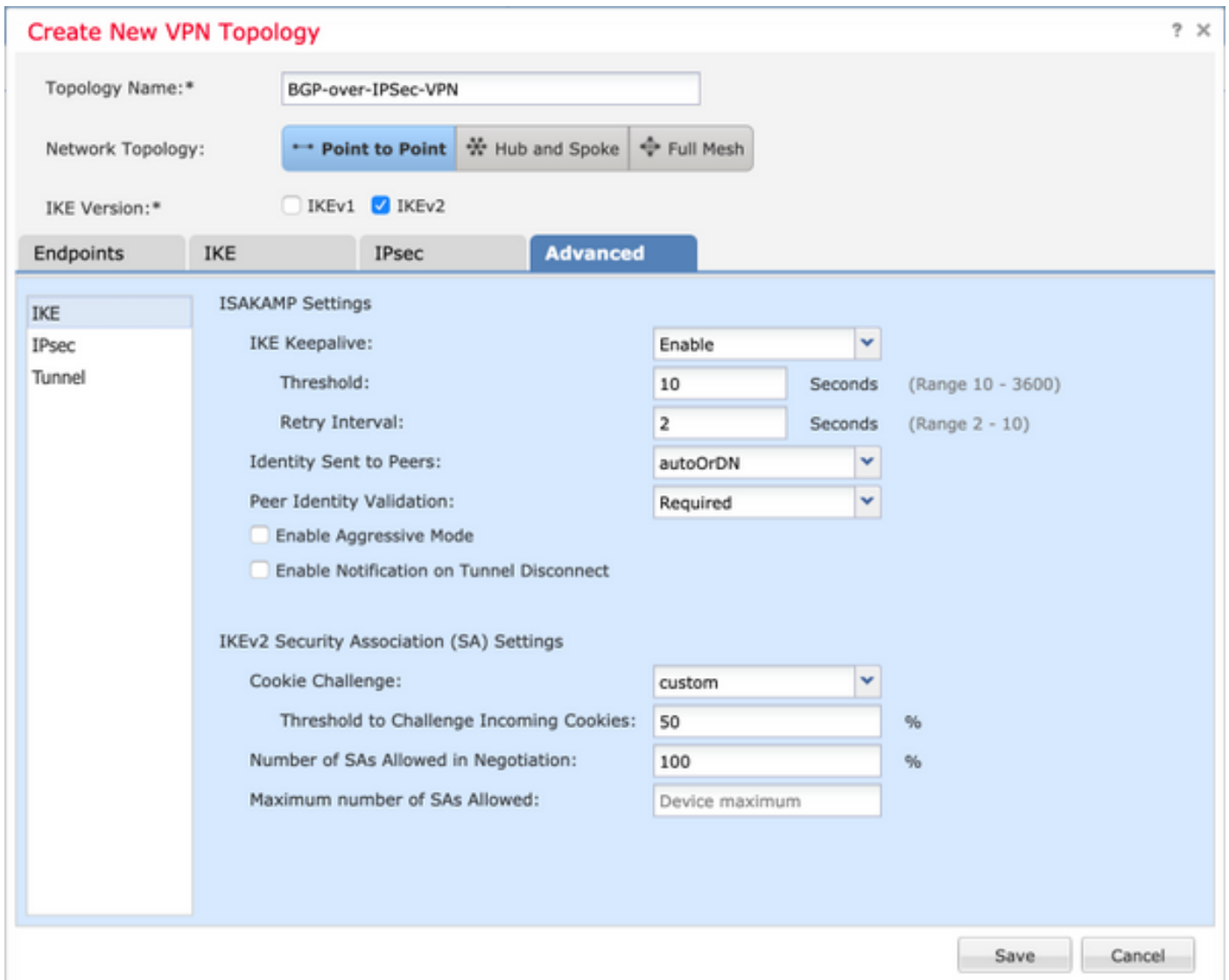
Modulus Group:

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

Lifetime Size:  Kbytes (Range 10-2147483647)

**ESPv3 Settings**

步骤6. 根据需要配置高级设置。

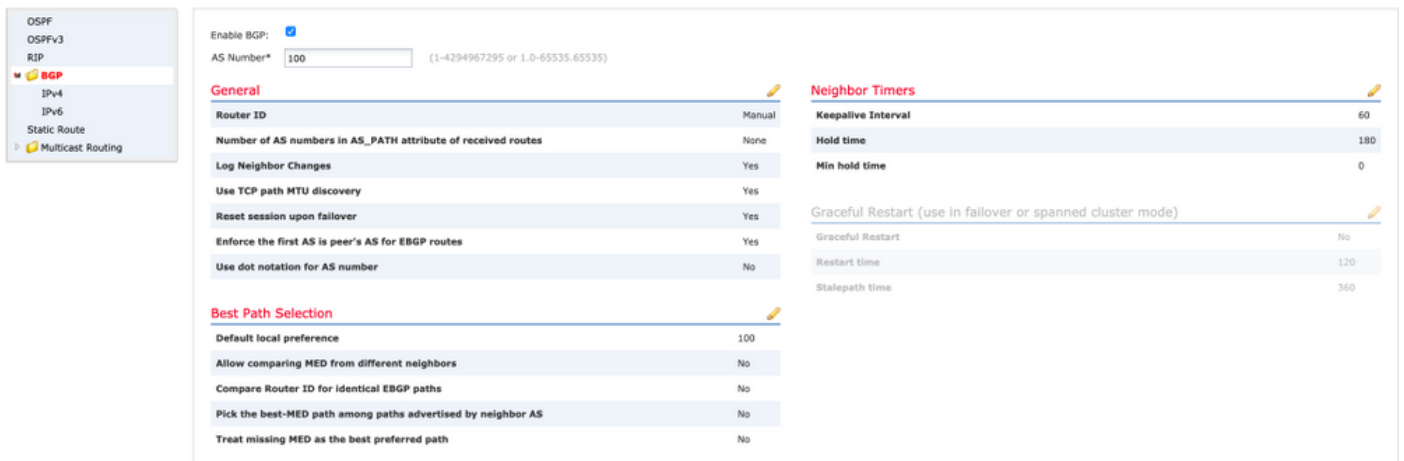


## 配置BGP

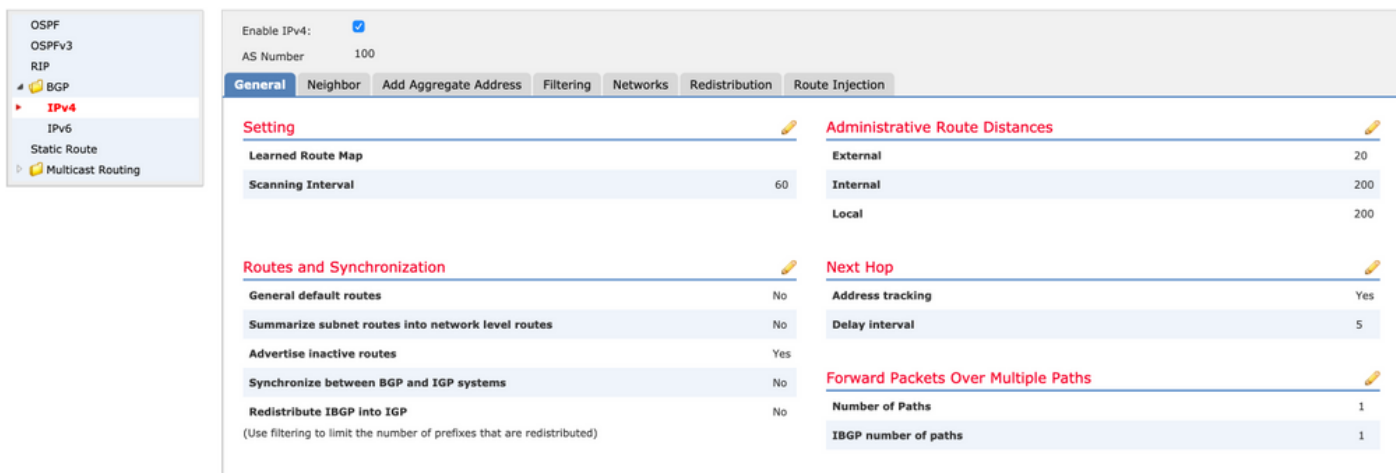
这是配置FTD1和FTD2的步骤。

在Device Management下，选择设备，然后导航至Routing > BGP。

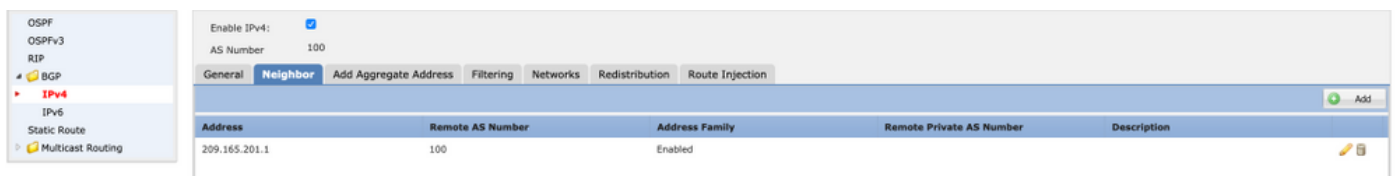
1. 启用BGP并配置自治系统(AS)编号，如下图所示。



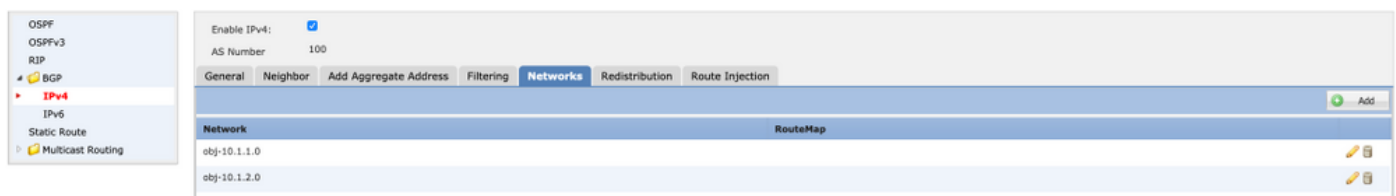
2. 导航到BGP > IPv4并在FTD上启用BGP IPv4，如此图所示。



3.在“邻居”选项卡下，添加另一个FTD作为邻居并启用邻居，如下图所示。



4.在Networks选项卡下，添加要通过BGP通告的网络。



5.所有其他BGP设置都是可选的，您可以根据您的环境配置这些设置。

## 两台设备的最终配置

### 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
```

## 验证

### 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 neighborhood ---! 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 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 NLRI 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
```

## 故障排除

目前没有针对此配置的故障排除信息。