在ASA与FTD之间配置基于路由的站点到站点VPN，并使用BGP作为重叠

目录

简介

本文档介绍如何在自适应安全设备(ASA)与Firepower威胁防御(FTD)之间配置基于路由的站点到站点VPN隧道，该隧道由具有动态路由边界网关协议(BGP)的Firepower管理中心(FMC)管理。

先决条件

要求

Cisco 建议您了解以下主题：

- 对IPsec站点到站点VPN的基本了解
- FTD和ASA上的BGP配置
- 使用FMC的经验

使用的组件

- Cisco ASAv 9.20(2)2版
- 思科FMC版本7.4.1

- 思科FTD版本7.4.1

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

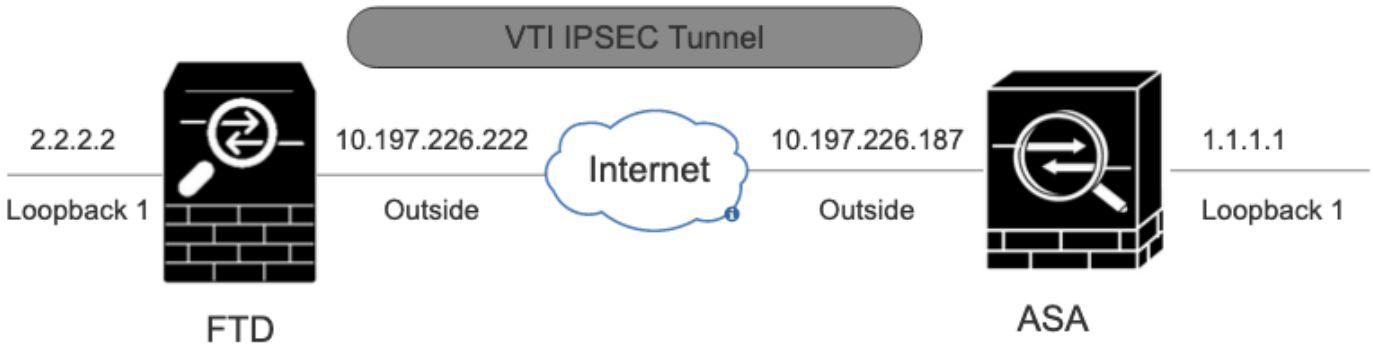
基于路由的VPN允许确定要加密或通过VPN隧道发送的相关流量，并且使用流量路由而不是策略/访问列表，就像在基于策略或基于加密映射的VPN中一样。 加密域设置为允许任何进入IPSec隧道的流量。IPsec本地和远程流量选择器设置为0.0.0.0/0.0.0.0。路由到IPsec隧道的所有流量都会被加密，无论源/目标子网如何。

本文档重点介绍将动态路由BGP作为重叠的静态虚拟隧道接口(SVTI)配置。

配置

本节介绍在ASA和FTD上通过SVTI IPSec隧道建立BGP邻居关系所需的配置。

网络图



网络图

配置

使用FMC在FTD上配置IPSec VPN

步骤1:导航到Devices > VPN > Site To Site。

第二步：点击+Site to Site VPN。

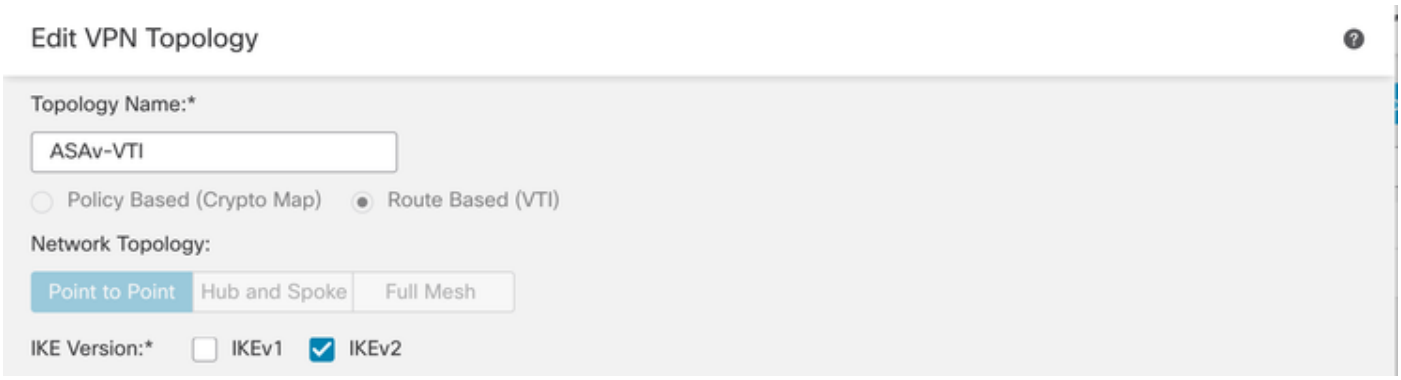
站点到站点 *VPN*

第三步：提供Topology NameRoute Based (VTI) ，然后选择Type of VPN（VPN类型）。选择IKE Version。

在本演示中：

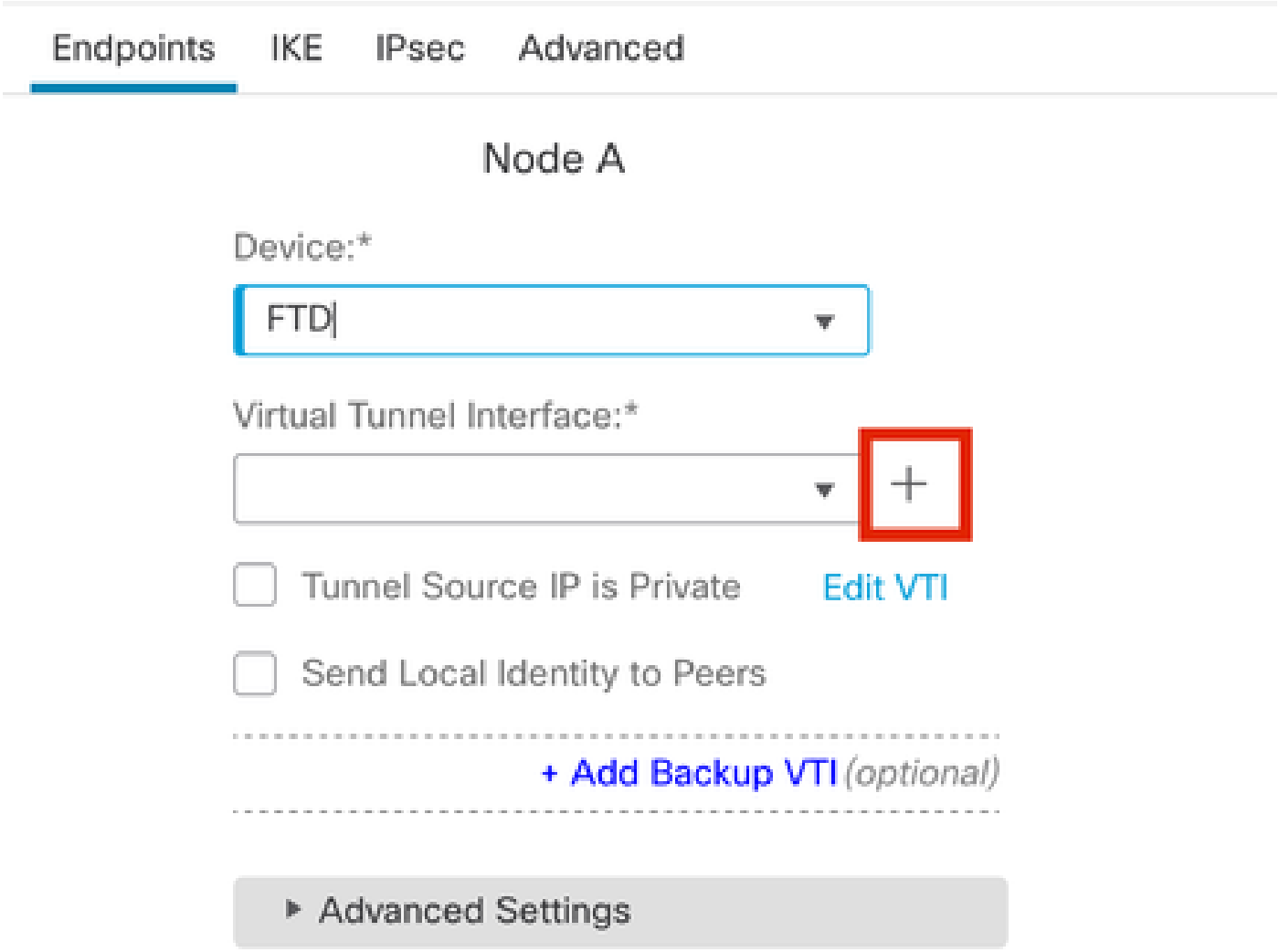
拓扑名称：ASAv-VTI

IKE版本：IKEv2



*VPN*拓扑

第四步：选择需要在其上配置隧道的Device。您可以添加新的虚拟隧道接口(点击+图标)，或从现有列表中选择一个虚拟隧道接口。



第五步：定义New Virtual Tunnel Interface的参数。单击。Ok

在本演示中：

名称：ASA-VTI

说明（可选）：使用外网ASA的VTI隧道

安全区域：VTI区域

隧道ID：1

IP地址：169.254.2.1/24

隧道源：GigabitEthernet0/1（外部）

IPsec隧道模式：IPv4

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

ASAv-VTI

[x] 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:*

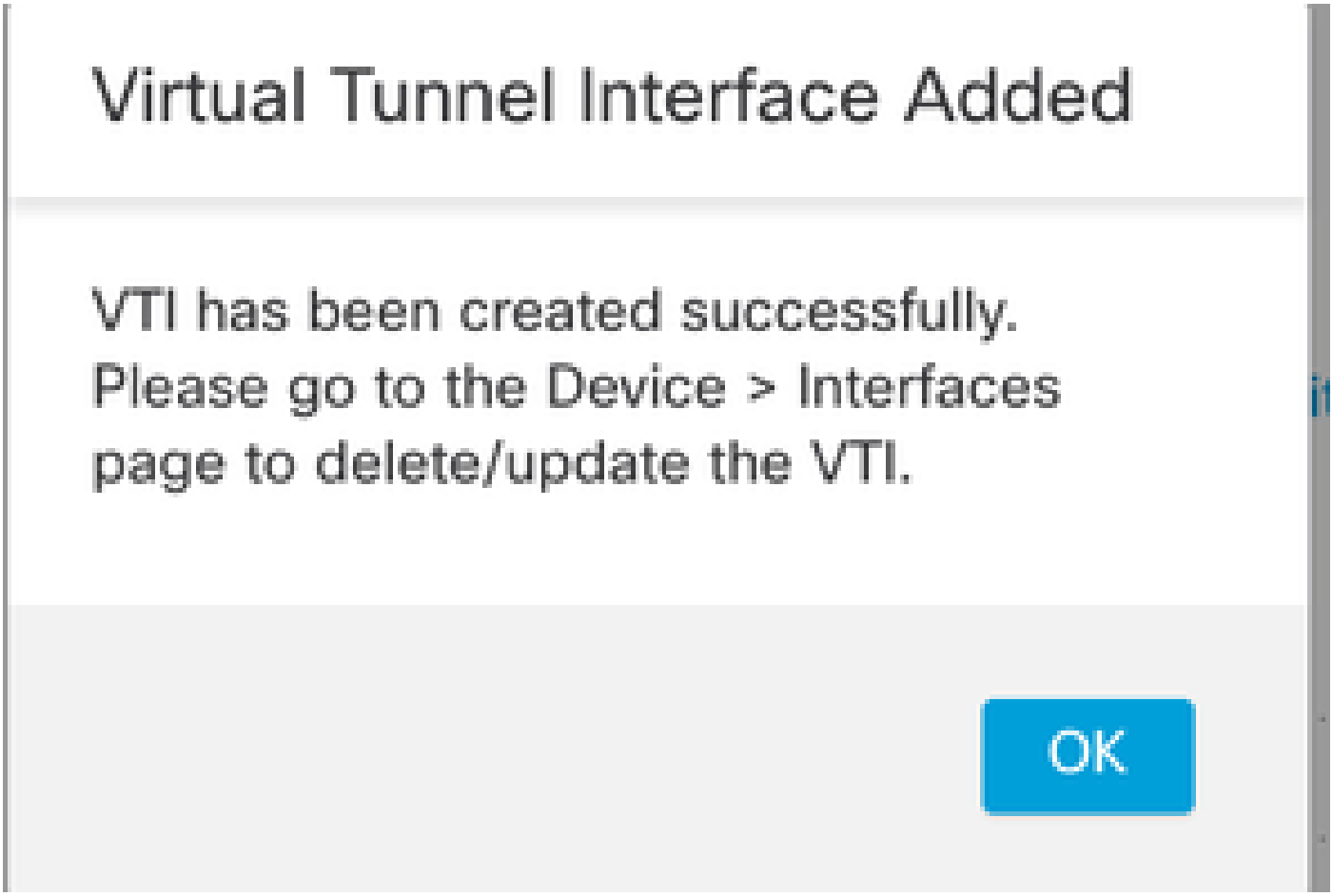
(•) Configure IP 169.254.2.1/24

( ) Borrow IP (IP unnumbered) Loopback1 (loopback)

Cancel OK

虚拟通道接口

第六步：点击OK弹出窗口，提示已创建新的VTI。



虚拟隧道接口已添加

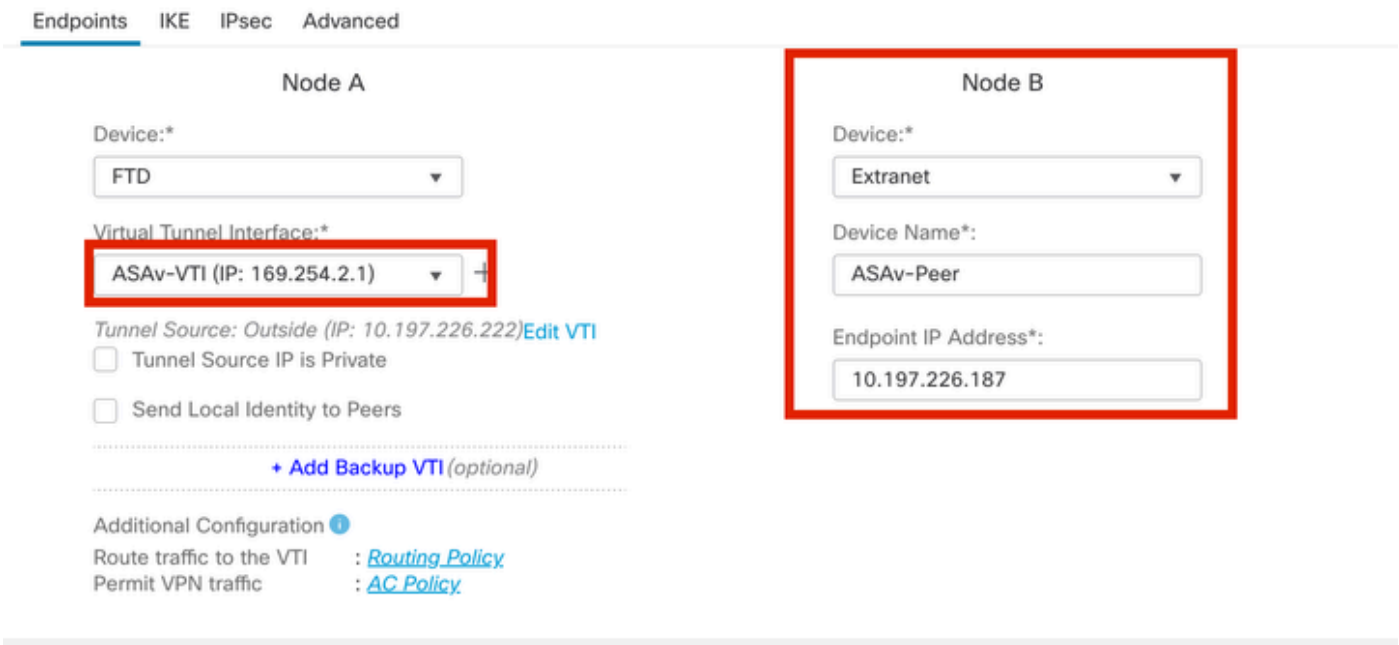
步骤 7.在Virtual Tunnel Interface下选择新创建的VTI或VTI。提供节点B（对等设备）的信息。

在本演示中：

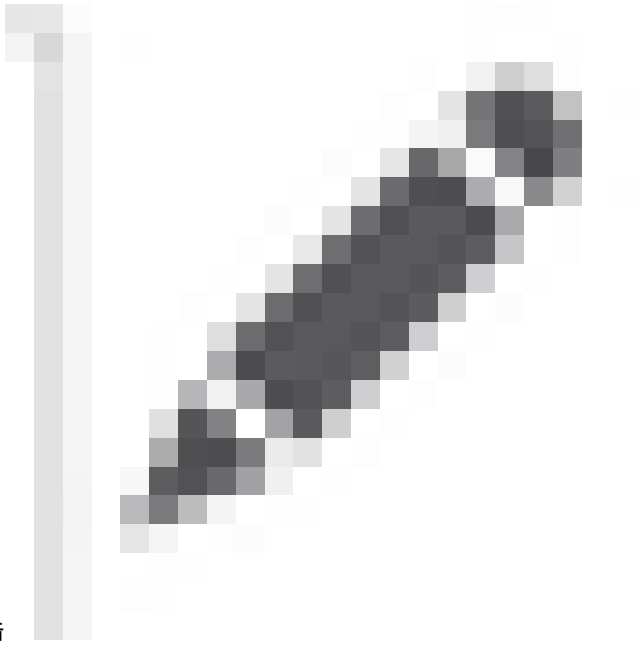
设备：外联网

设备名称：ASAv-Peer

终端IP地址：10.197.226.187



终端节点*B*



步骤 8导航到**IKE**选项卡。点击

。您可以选择使用预定义的Policy，或单击Policy选项卡旁边的+按钮以创建一个新按钮。

第9步（可选，如果创建新的IKEv2策略。）为策略提供Name并选择要在策略中使用的Algorithms。单击。Save

在本演示中：

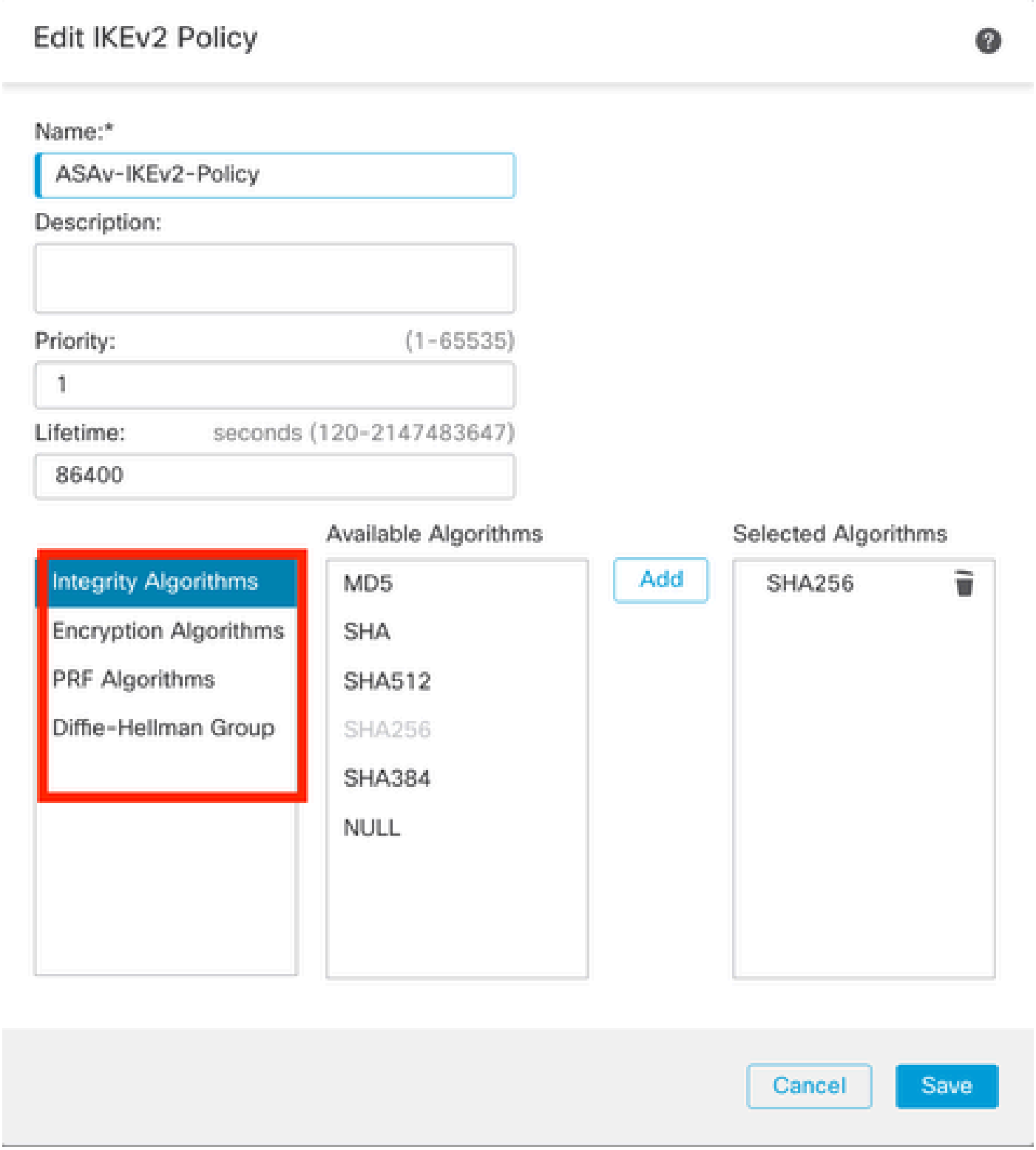
名称：ASAv-IKEv2-policy

完整性算法：SHA-256

加密算法：AES-256

PRF算法：SHA-256

Diffie-Hellman组：14



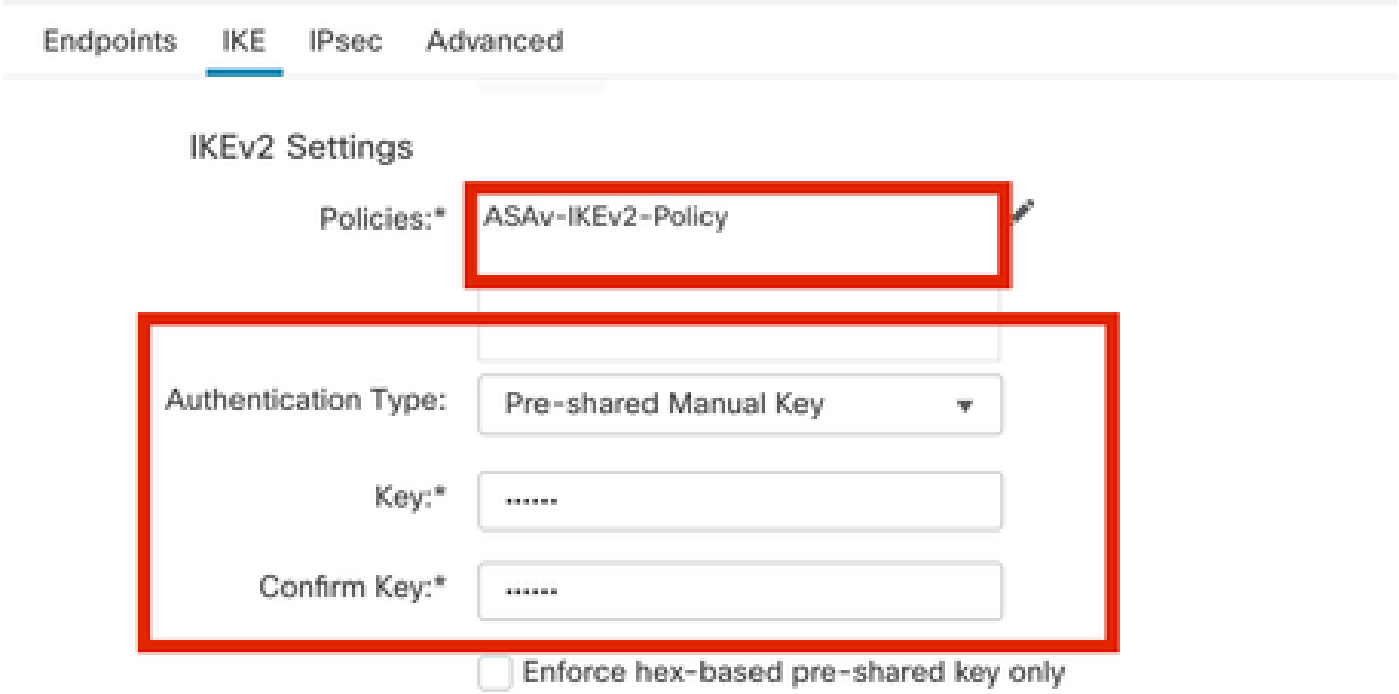
IKEv2-策略

步骤 10选择新创建的Policy或Policy存在的。选择Authentication Type。如果使用预共享手动密钥，请在Key和Confirm Key 框中输入密钥。

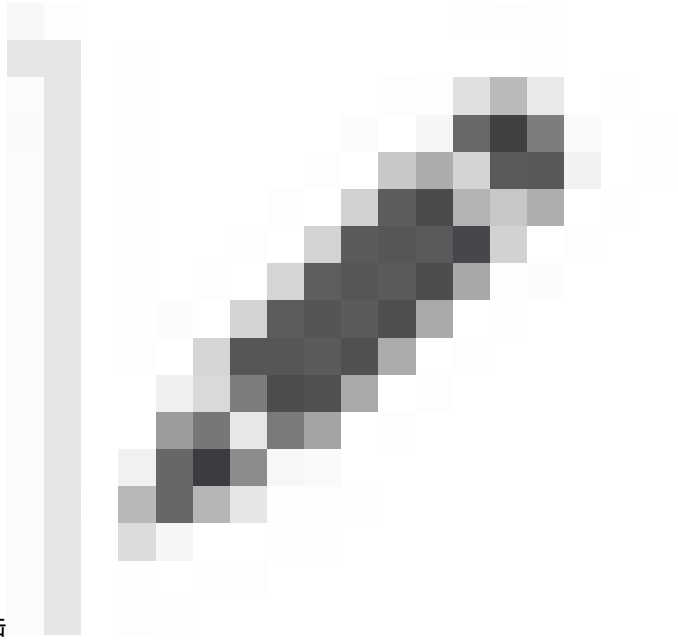
在本演示中：

策略：ASAv-IKEv2-Policy

身份验证类型：预共享手动密钥



身份验证



步骤 11导航到选IPsec 项卡。点击

，可选择使用预定义的IKEv2 IPsec建议或创建一个新建议。单击选IKEv2 IPsec Proposal 项卡旁边的+按钮。

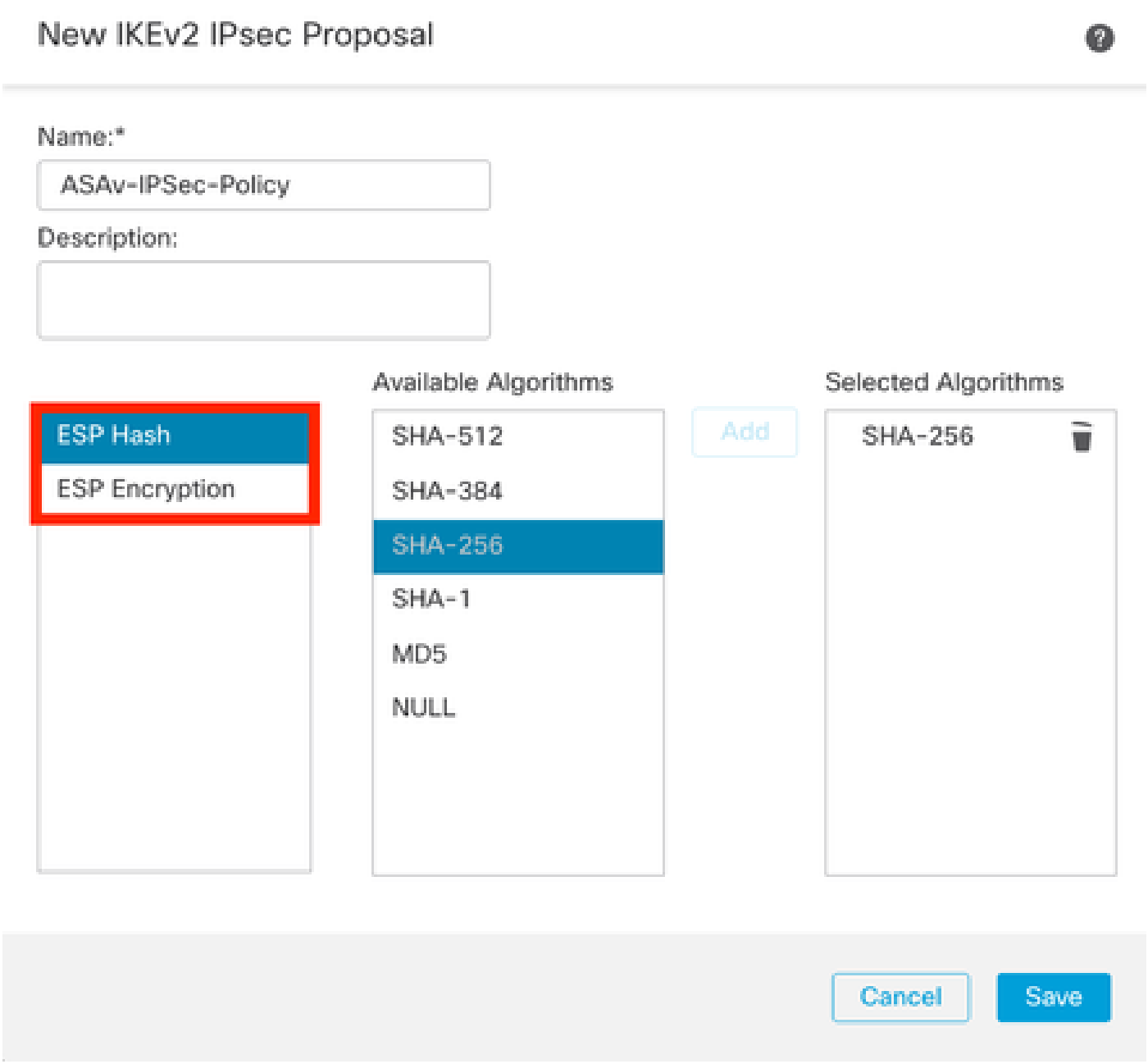
第12步（可选，如果创建新的IKEv2 IPsec提议。）输入建议书的Name命令，并选择要在建议书中使用的Algorithms。单击。Save

在本演示中：

名称：ASAv-IPSec-Policy

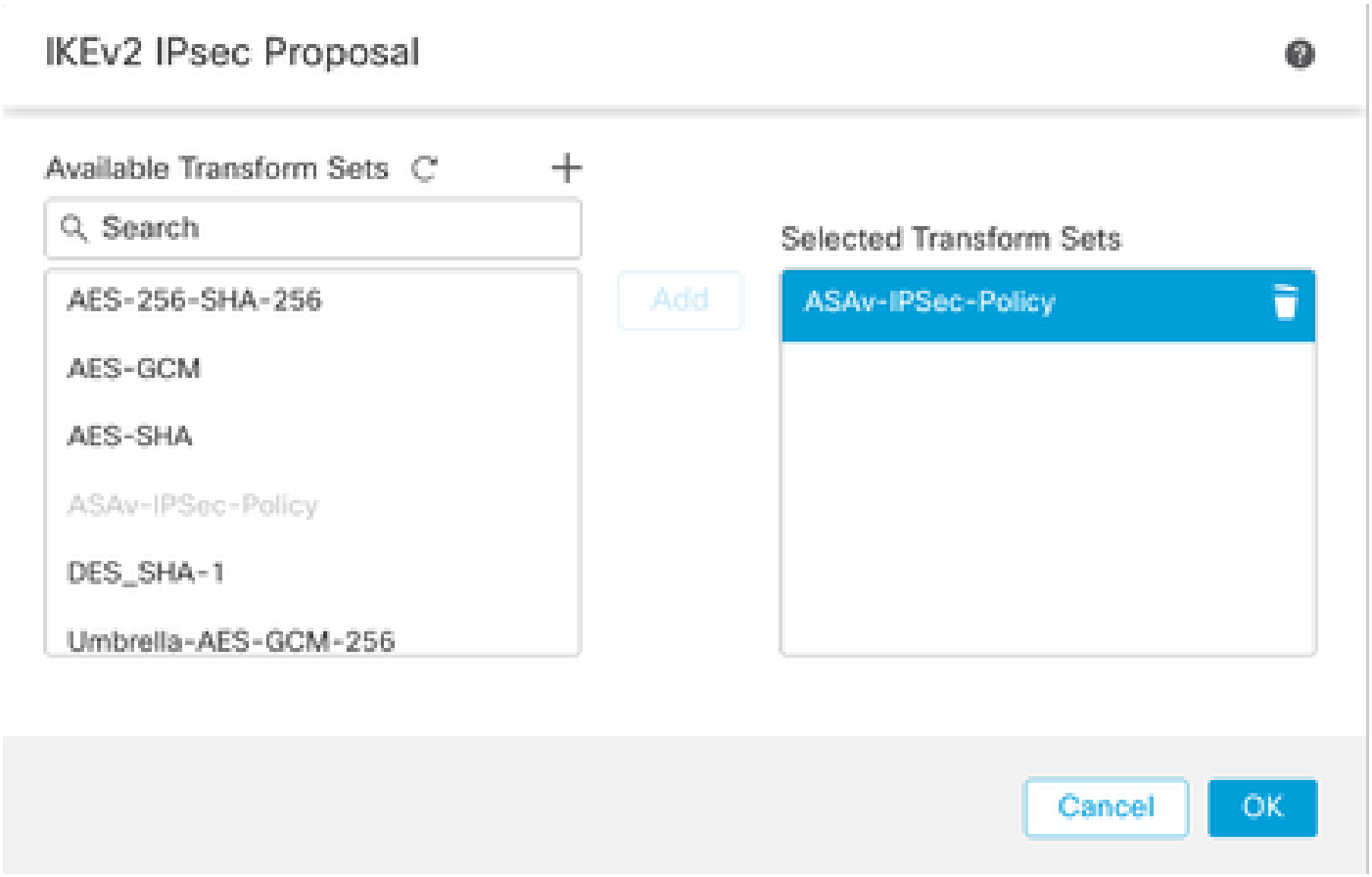
ESP哈希：SHA-256

ESP加密：AES-256



IKEv2-IPsec-Proposal

步骤 13 从可用建议列表中选择新创建的Proposal或Proposal。单击。OK



变换集

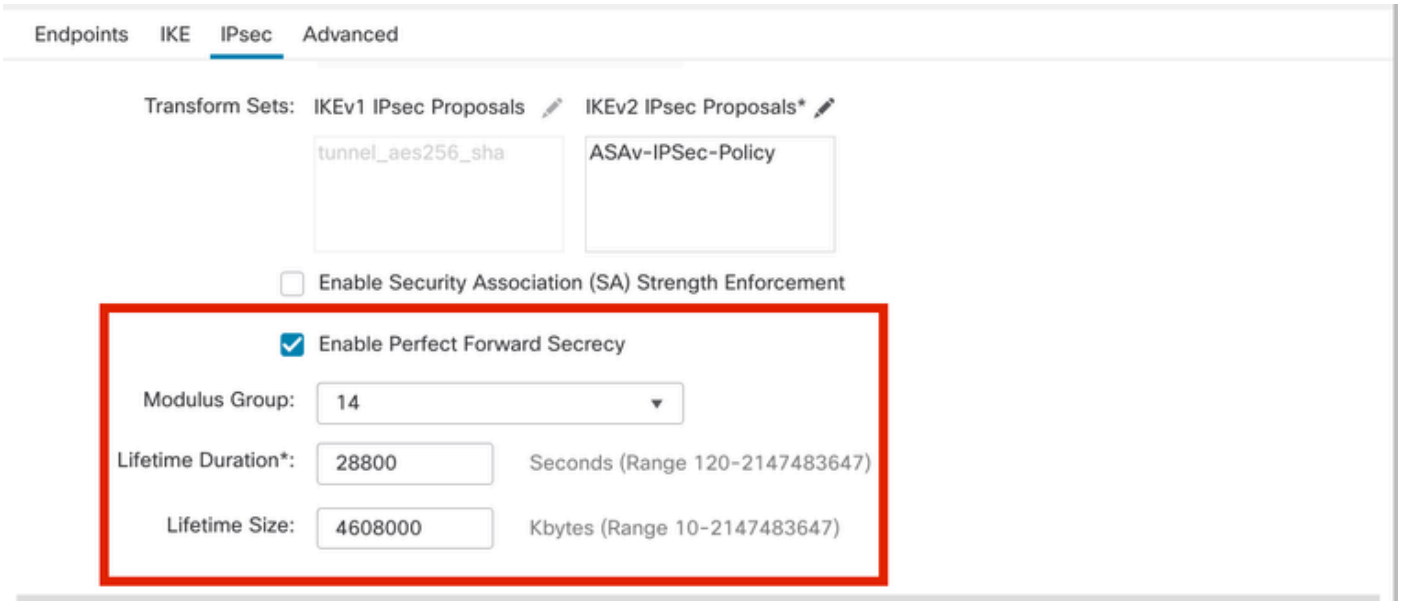
第14步：（可选）选择Perfect Forward Secrecy设置。配置IPsec Lifetime Duration and Lifetime Size。

在本演示中：

完全正向保密：模数组14

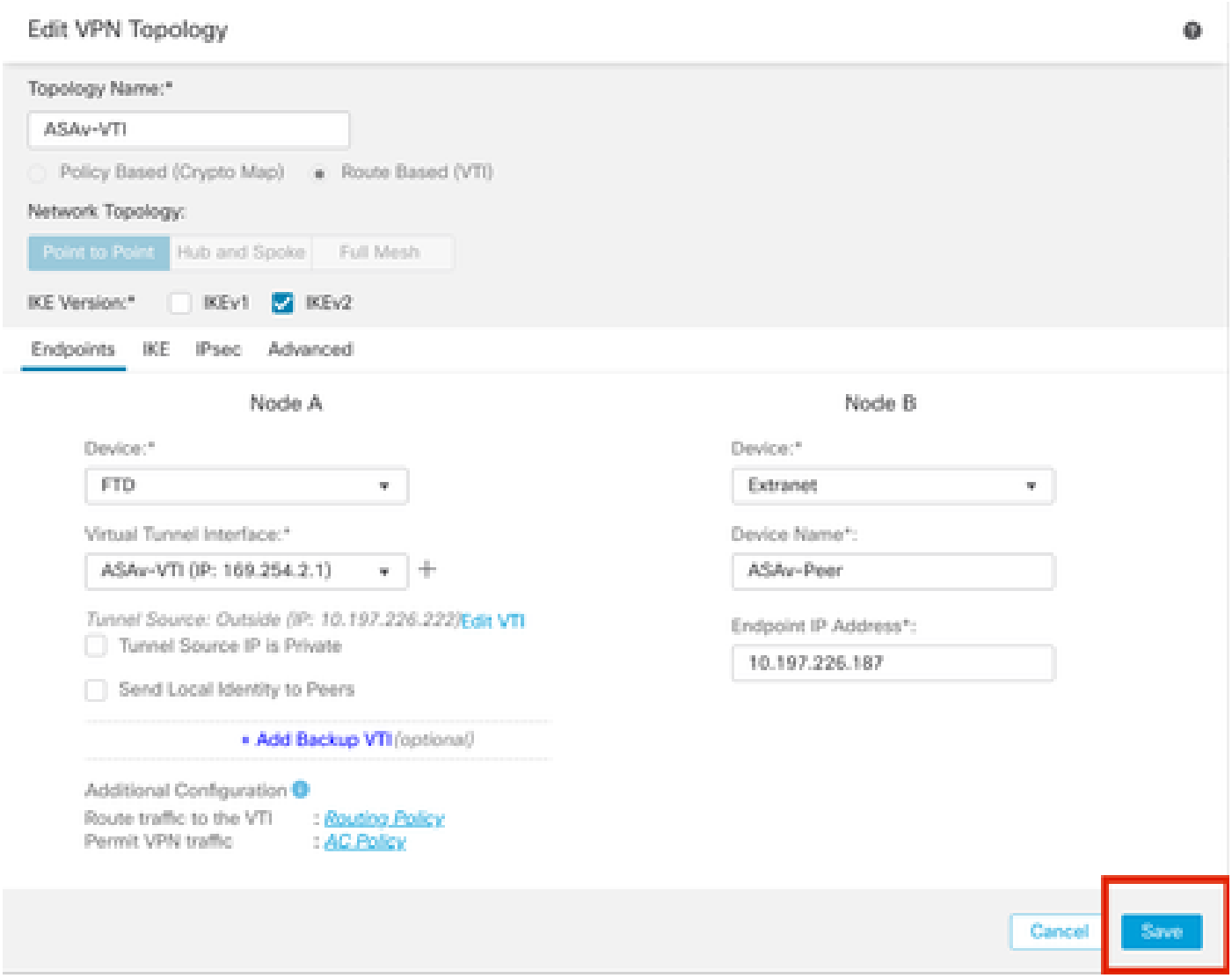
生存期持续时间：28800（默认值）

生存期大小：4608000（默认值）



*PFS*配置

步骤 15检查配置的设置。单击Save，如图所示。



保存配置

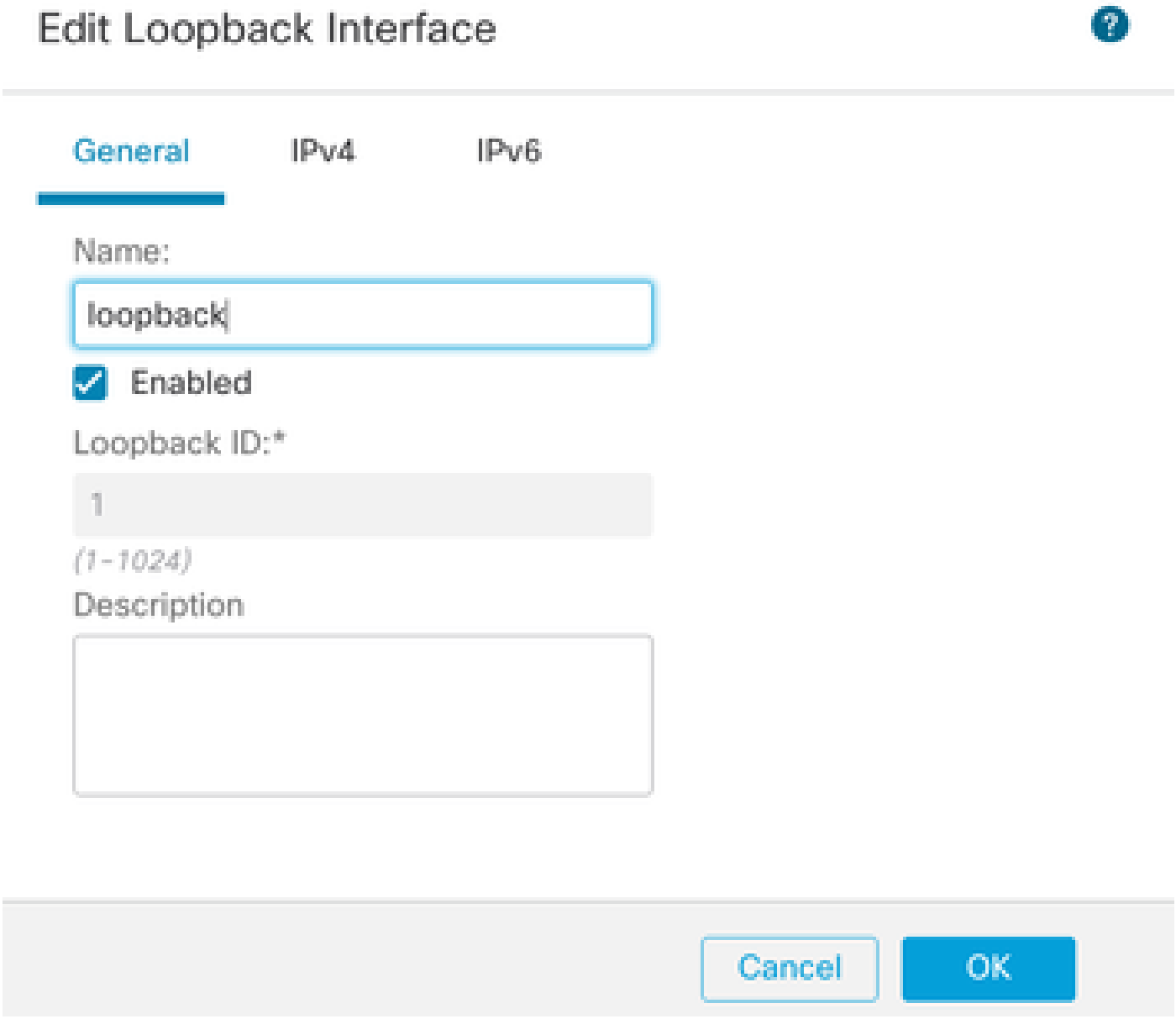
使用FMC在FTD上配置环回接口

导航到Devices > Device Management。编辑需要配置环回的设备。

步骤1:转到访问 。Interfaces > Add Interfaces > Loopback Interface

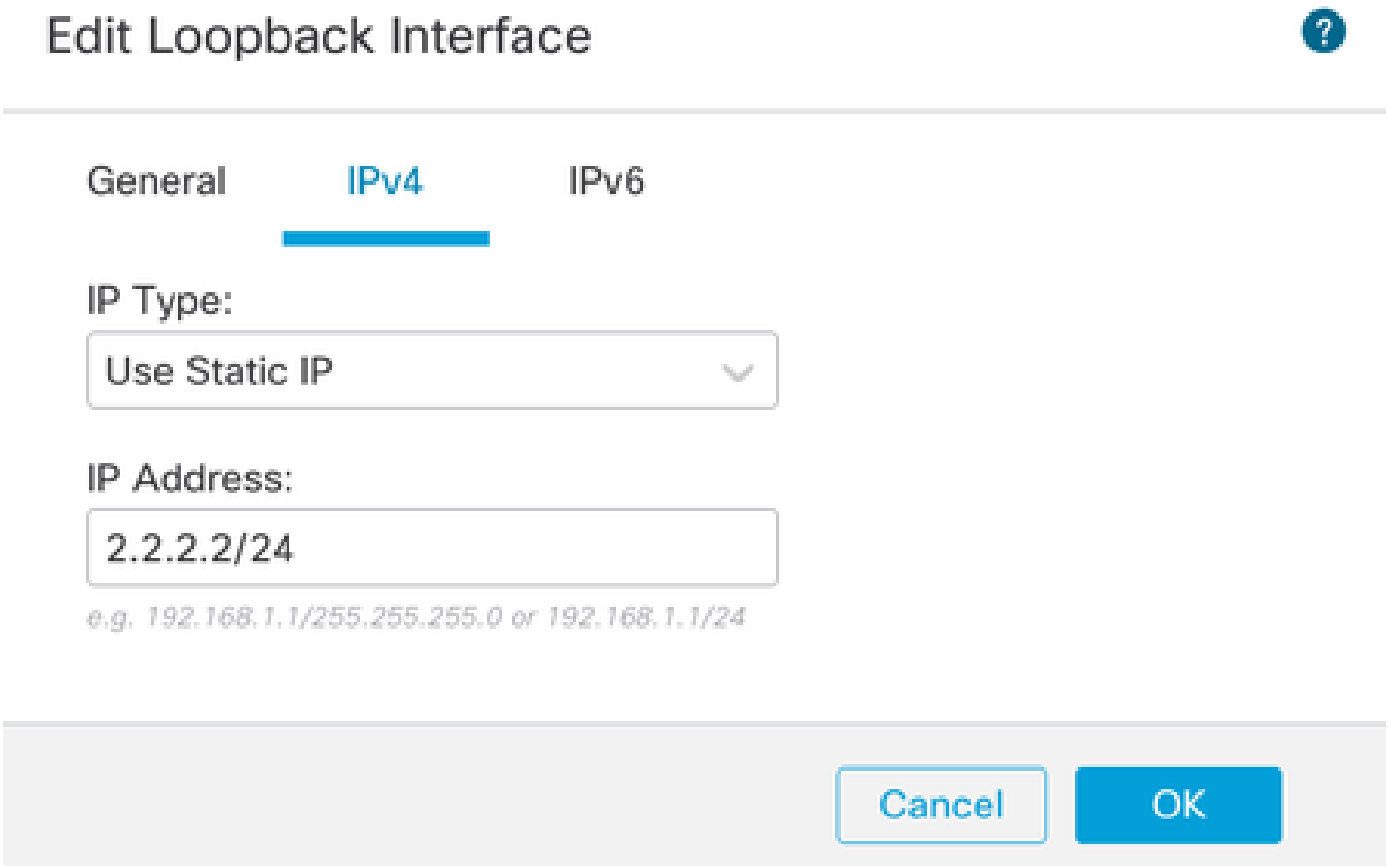
导航到环回接口

第二步：输入名称“loopback”，提供环回ID“1”并启用接口。



启用环回接口

第三步：配置接口的IP地址，点击OK 。



为环回接口提供*IP*地址

在ASA上配置IPSec VPN

```
!--- 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
```

在ASA上配置环回接口

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

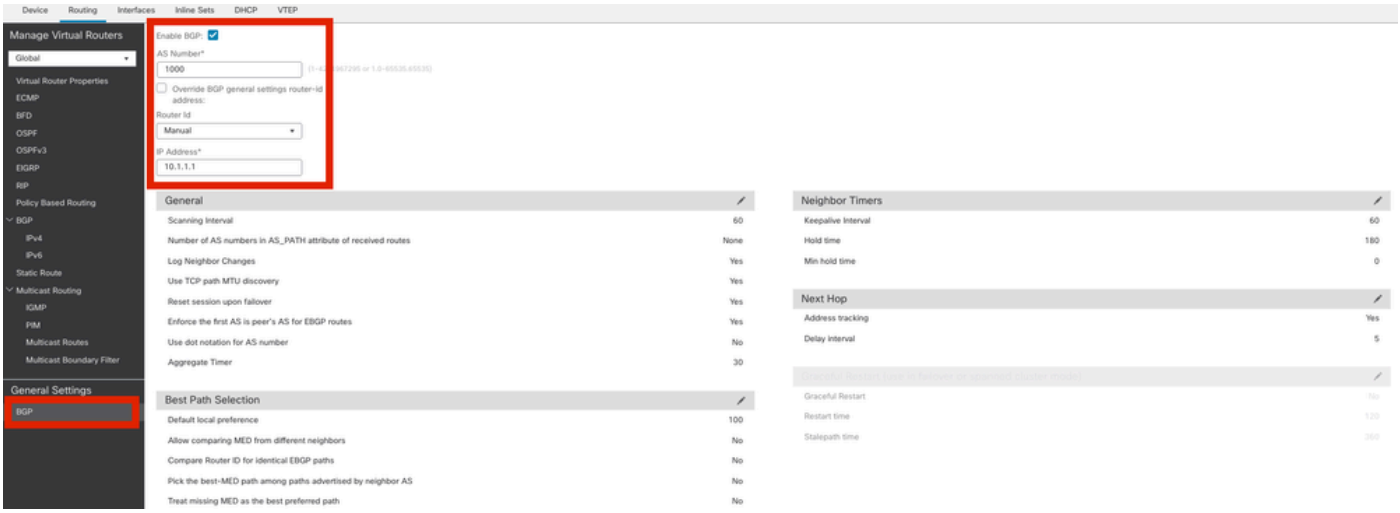
使用FMC在FTD上配置重叠BGP

导航到配置VTI隧道的设备Devices > Device Management.Edit，然后导航到Routing >General Settings > BGP。

步骤1:启用BGP并配置自治系统(AS)编号和路由器ID，如此图中所示。

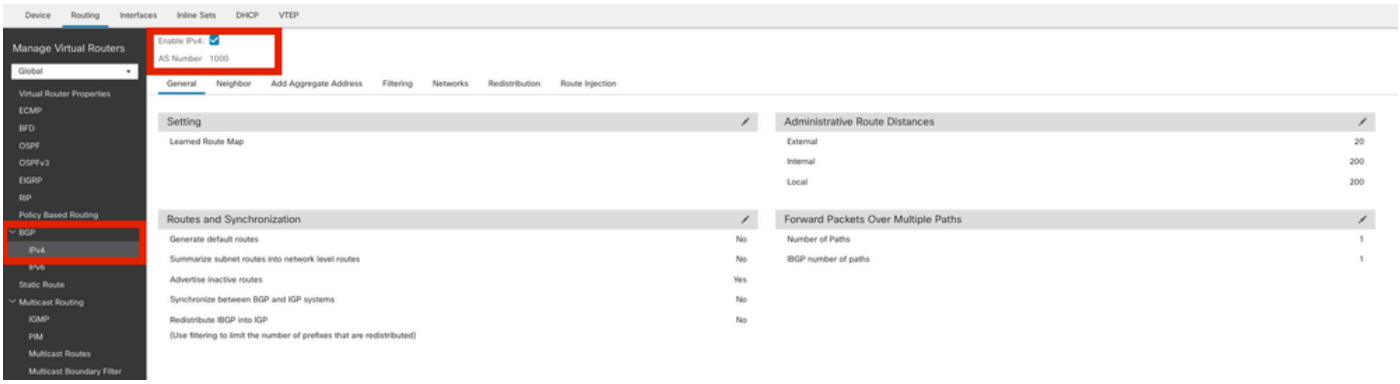
设备FTD和ASA上的AS编号必须相同。

路由器ID用于标识参与BGP的每个路由器。



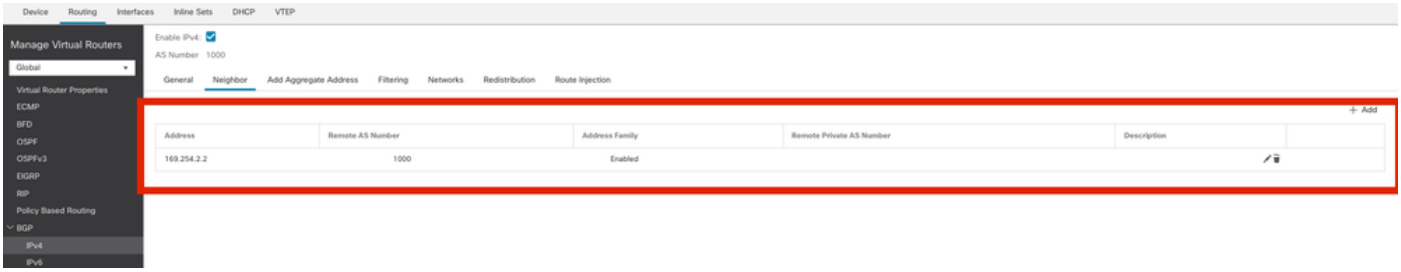
导航到配置*BGP*

第二步：导航到BGP > IPv4(CDP)并在FTD上启用BGP IPv4。



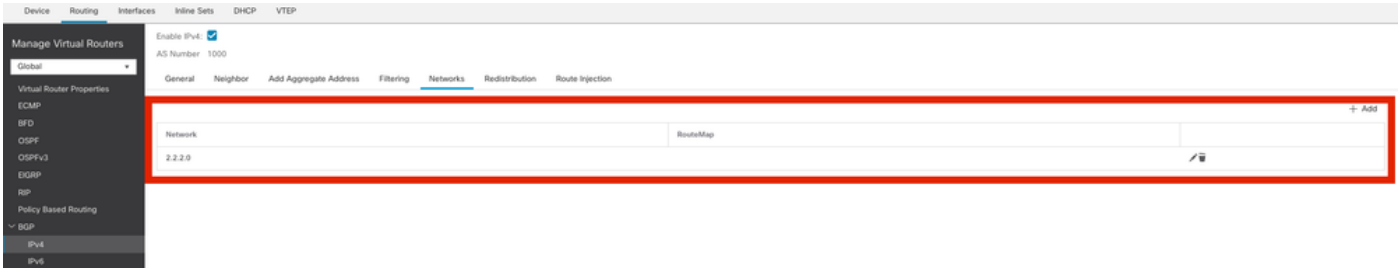
启用*BGP*

第三步：在Neighbor选项卡下，添加ASAv VTI隧道IP地址作为邻居并启用邻居。



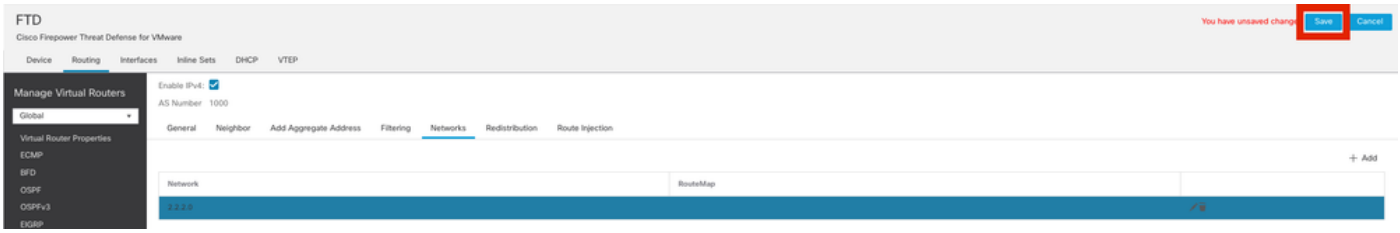
添加*BGP*邻居

第四步：在Networks下，添加要通过BGP通告但需要通过VTI隧道的网络，在本例中为loopback1。



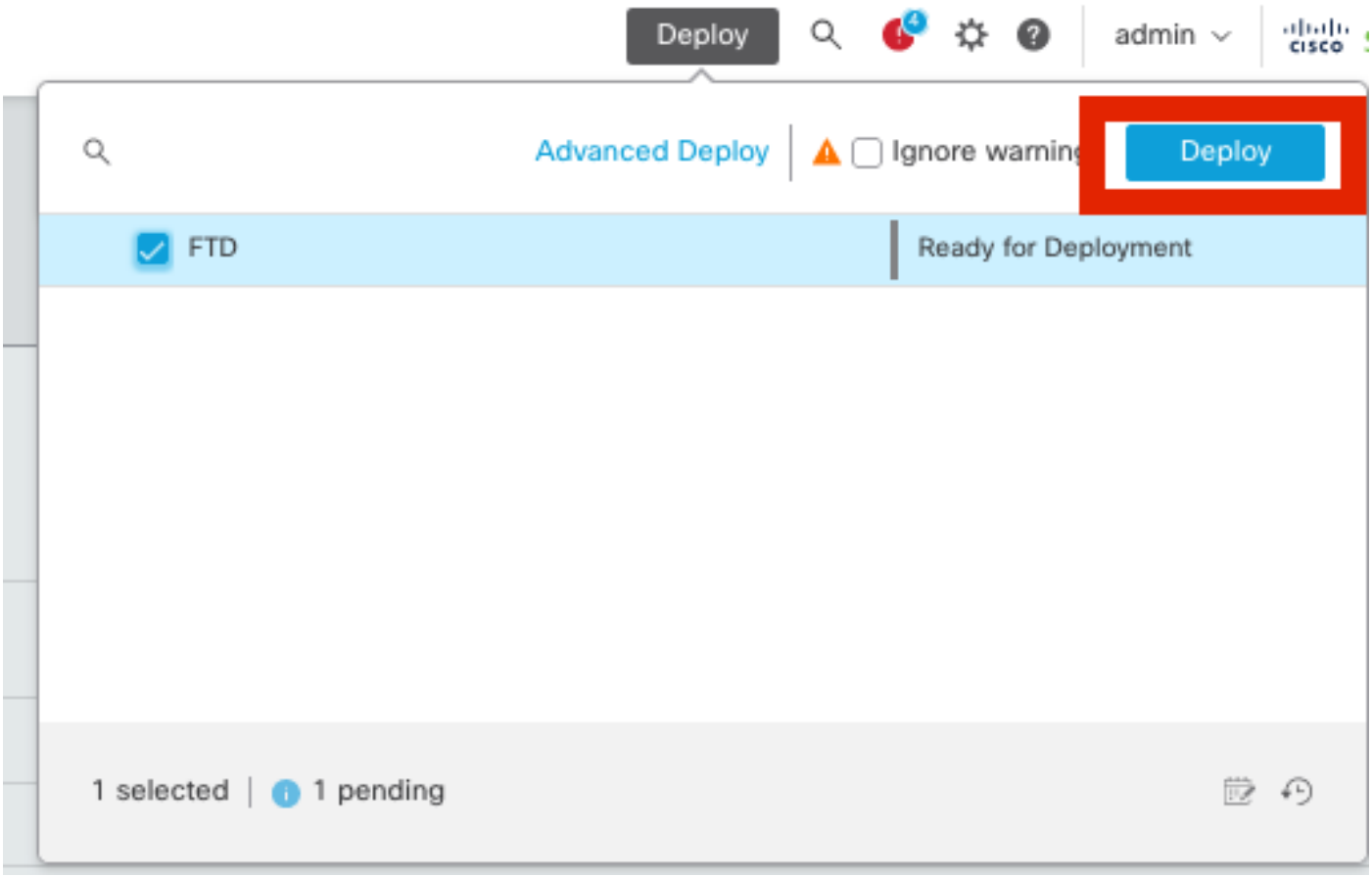
添加*BGP*网络

第五步：所有其他BGP设置都是可选的，您可以根据您的环境对其进行配置。验证配置并单击Save。



保存*BGP*配置

第六步：部署所有配置。



部署

在ASA上配置重叠BGP

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

验证

使用本部分可确认配置能否正常运行。

FTD上的输出

```
<#root>
```

#show crypto ikev2 sa

```
IKEv2 SAs:
Session-id:20, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id         Local                  Remote                fvrf/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: ASAv-VTI
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.222

  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  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 NLRIs in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a route to 169.254.2.2
Connections established 7; dropped 6
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
```

#show route bgp

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
            D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
            N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
            E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
            i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
            ia - IS-IS inter area, * - candidate default, U - per-user static route
            o - ODR, P - periodic downloaded static route, + - replicated route
            SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.197.226.1 to network 0.0.0.0

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

ASA上的输出

<#root>

#show crypto ikev2 sa

```
IKEv2 SAs:

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

Tunnel-id    Local                    Remote                   fvrf/ivrf            Status
442126361    10.197.226.187/500       10.197.226.222/500       Global/Global         READY
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1200 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x8540d49e/0xa14edaf6
```

#show crypto ipsec sa

```
interface: FTD-VTI
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.187

  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
  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 NLRIs in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a route to 169.254.2.1
Connections established 5; dropped 4
```

```
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
```

#show route bgp

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
           i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
           ia - IS-IS inter area, * - candidate default, U - per-user static route
           o - ODR, P - periodic downloaded static route, + - replicated route
           SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.197.226.1 to network 0.0.0.0

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

故障排除

本部分提供了可用于对配置进行故障排除的信息。

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

- 仅支持IPv4接口以及IPv4、受保护网络或VPN负载（不支持IPv6）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。