在ASA和FTD之間使用BGP作為重疊配置基於路由的站點到站點VPN

目錄

簡介

本檔案介紹如何在具有動態路由邊界閘道通訊協定(BGP)的Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)與調適型安全裝置(ASA)之間設定路由型站點對站點VPN通道。

必要條件

需求

思科建議您瞭解以下主題：

- 對IPSec站點到站點VPN有基本的瞭解
- FTD和ASA上的BGP配置
- 體驗FMC

採用元件

- Cisco ASAv版本9.20(2)2
- Cisco FMC版本7.4.1

- Cisco FTD版本7.4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

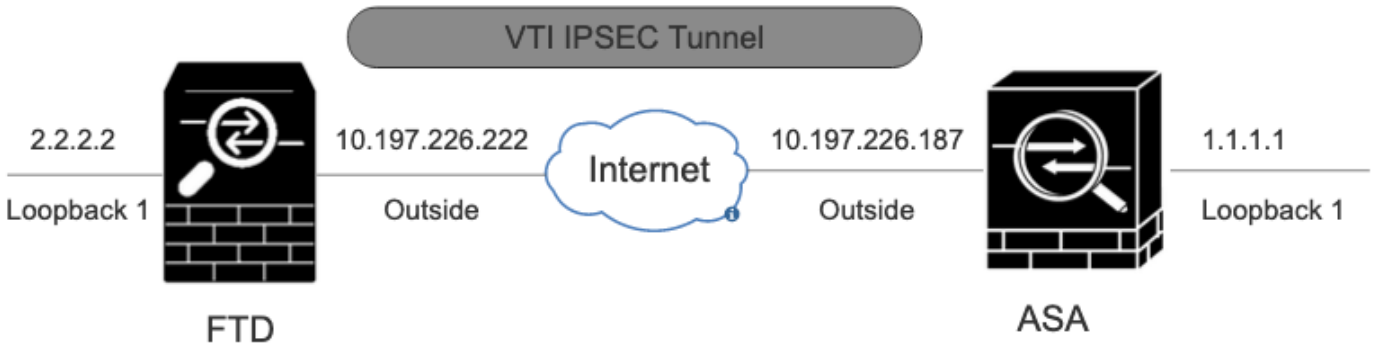
基於路由的VPN允許確定要加密或透過VPN隧道傳送的相關流量，並且使用流量路由而不是策略/訪問清單，就像在基於策略或基於加密對映的VPN中一樣。 加密域設定為允許任何進入IPSec隧道的流量。IPsec本地和遠端流量選擇器設定為0.0.0.0/0.0.0.0。任何路由到IPSec隧道的流量都會被加密，無論源/目標子網如何。

本檔案將重點介紹以動態路由BGP作為重疊的靜態虛擬通道介面(SVTI)組態。

設定

本節介紹在ASA和FTD上透過SVTI IPSec隧道啟用BGP鄰居關係所需的配置。

網路圖表



網路圖表

組態

使用FMC在FTD上設定IPSec VPN

步驟 1.導航到Devices > VPN > Site To Site。

步驟 2.點選+Site to Site VPN。

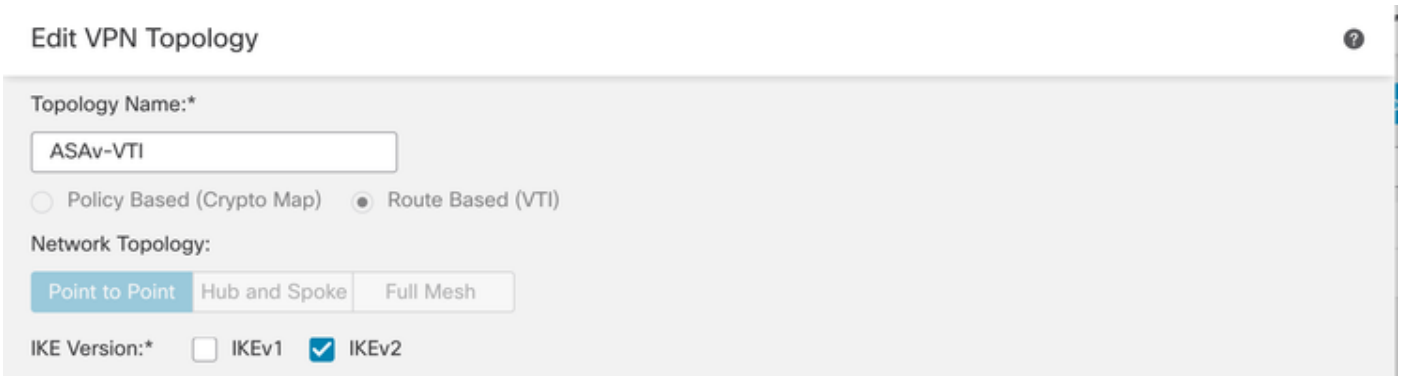
站點到站點*VPN*

步驟 3.提供Topology Name，並選擇VPN的型別Route Based (VTI)。選擇IKE Version。

在本演示中：

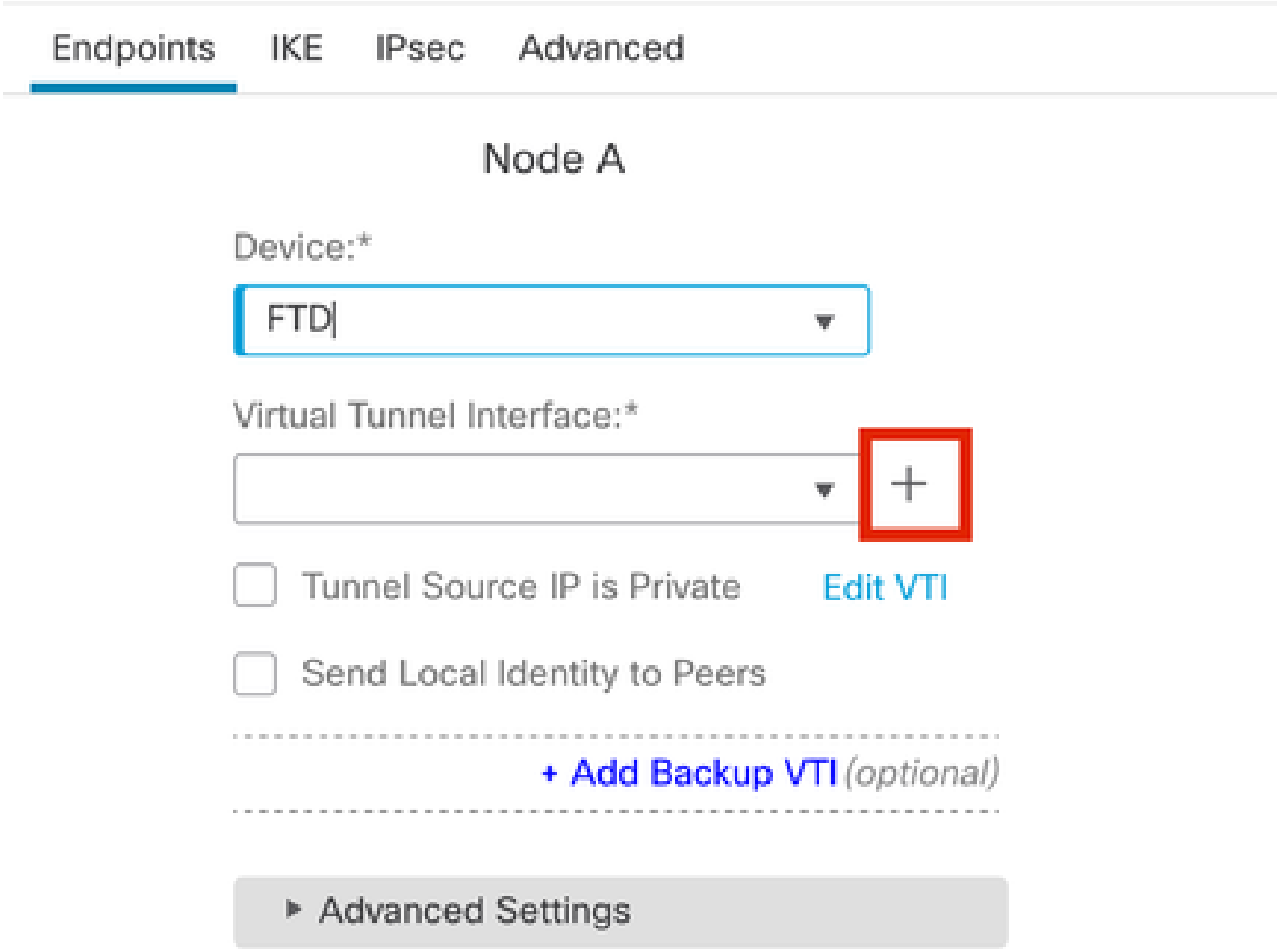
拓撲名稱：ASAv-VTI

IKE版本：IKEv2



*VPN*拓撲

步驟 4.選擇需要配置隧道的Device命令。您可以增加新的虛擬隧道介面(點選+圖示)，或從現有清單中選擇一個虛擬隧道介面。



步驟 5.定義New Virtual Tunnel Interface的引數。按一下Ok。

在本演示中：

名稱：ASA-VTI

說明（可選）：VTI隧道和外聯網ASA

安全區域：VTI-Zone

通道ID：1

IP地址：169.254.2.1/24

隧道源：GigabitEthernet0/1（外部）

IPsec通道模式：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:*

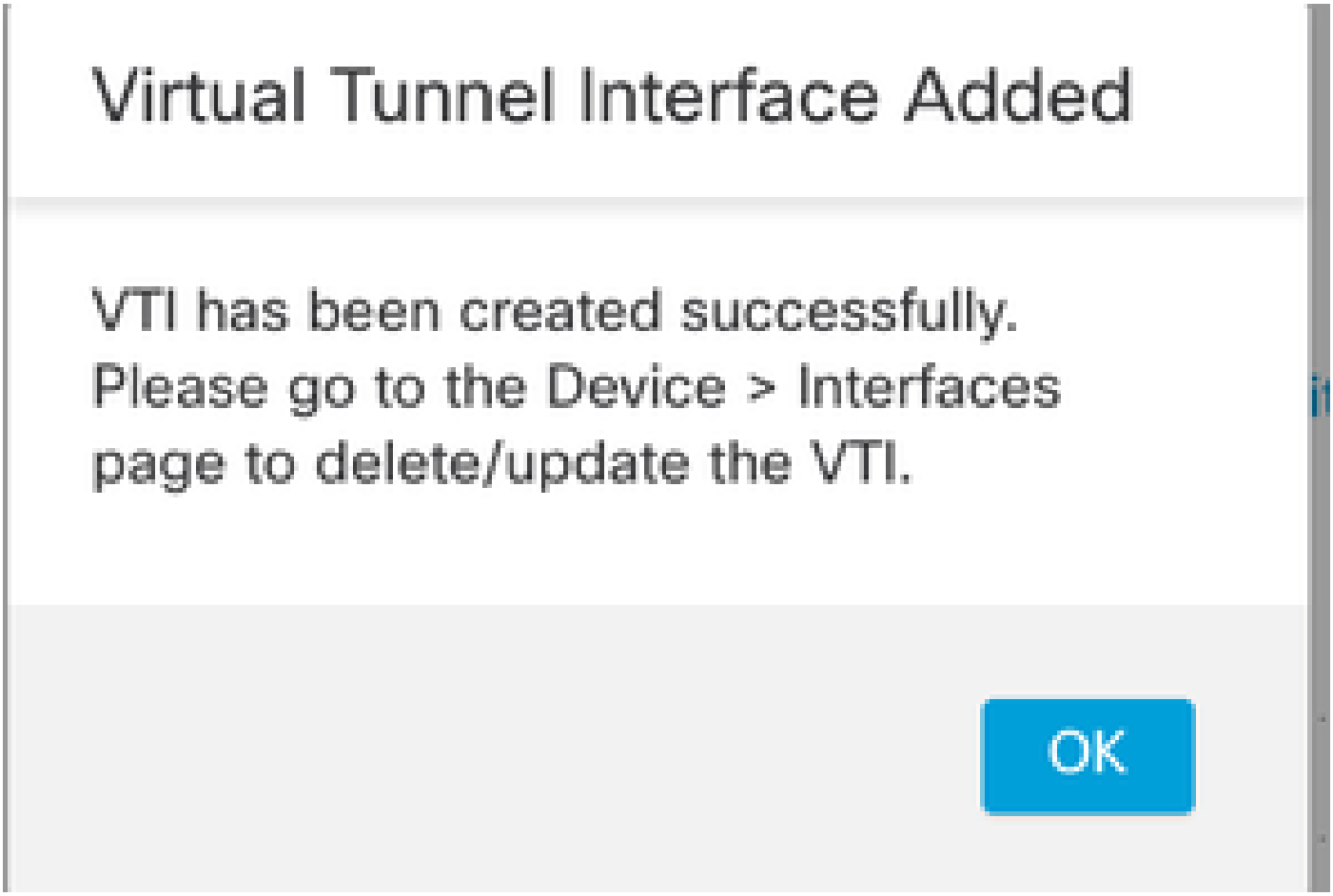
(•) Configure IP 169.254.2.1/24

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

Cancel OK

虛擬通道介面

步驟 6.點選OK，系統將顯示新的VTI已經建立。



已增加虛擬隧道介面

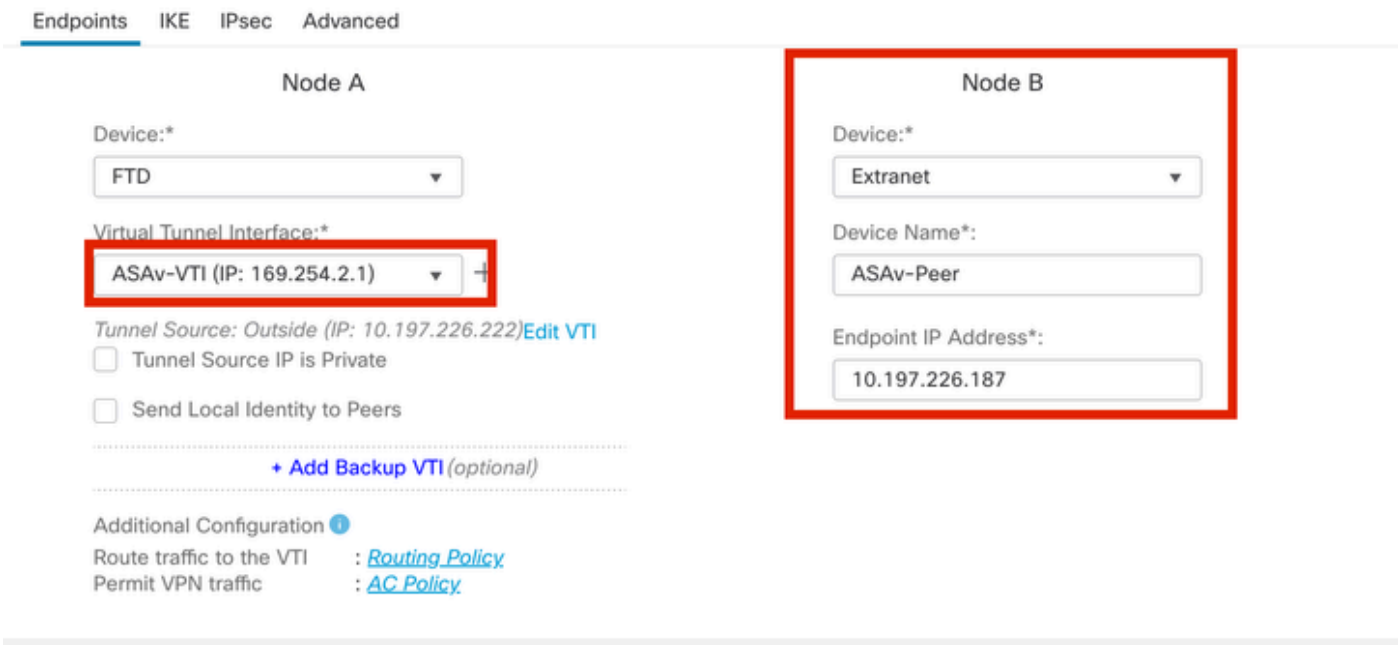
步驟 7.在Virtual Tunnel Interface下選擇新建立的VTI或VTI。提供節點B（對等裝置）的資訊。

在本演示中：

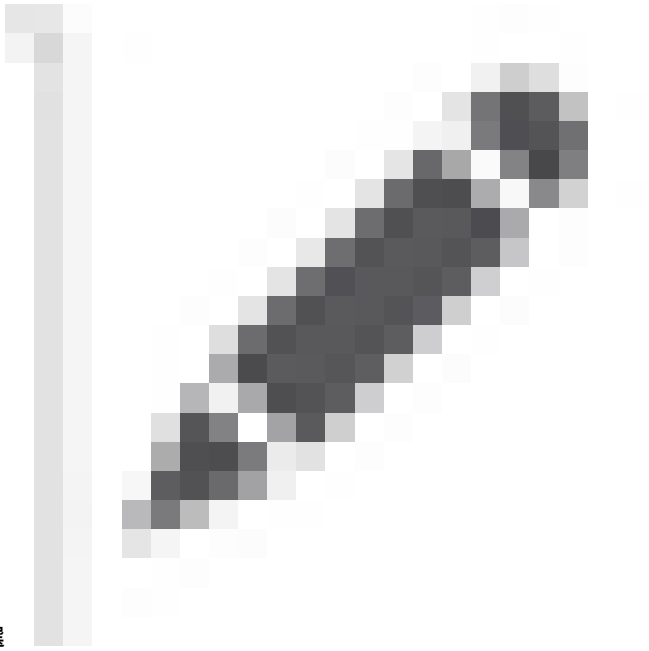
裝置：Extranet

裝置名稱：ASAv-Peer

終端IP地址：10.197.226.187



終端節點*B*



步驟 8.導航到**IKE** 頁籤。點選。您可以選擇使用預先定義的Policy，或按一下標Policy簽旁的按+鈕來建立新標籤。

第9步：（如果建立新的IKEv2策略，則可選。）為策略提供Name並選擇要在策略中使用的Algorithms。按一下Save。

在本演示中：

名稱：ASAv-IKEv2-policy

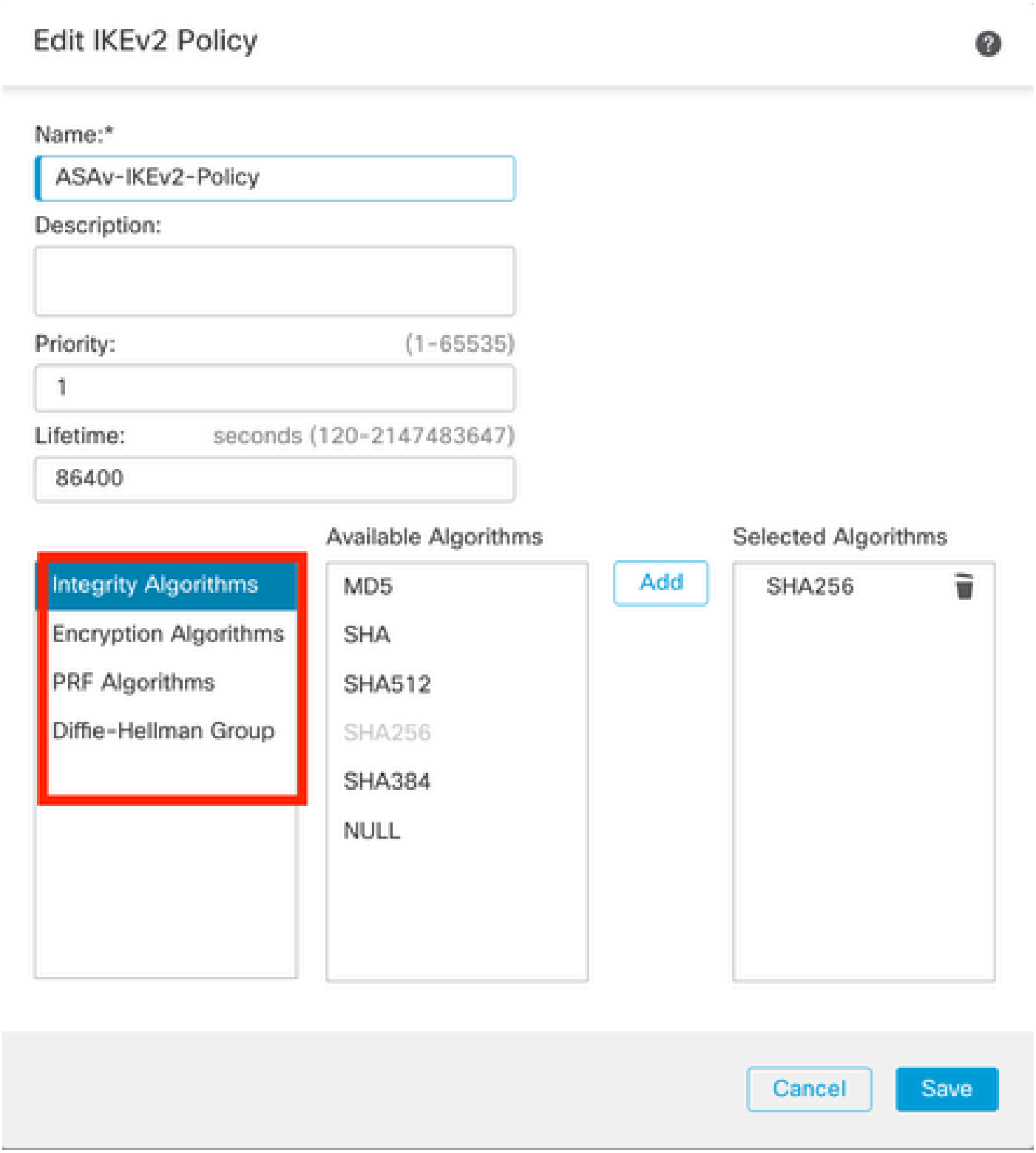
完整性演算法：SHA-256

加密演算法：AES-256

PRF演算法：SHA-256

Diffie-

Hellman組：14



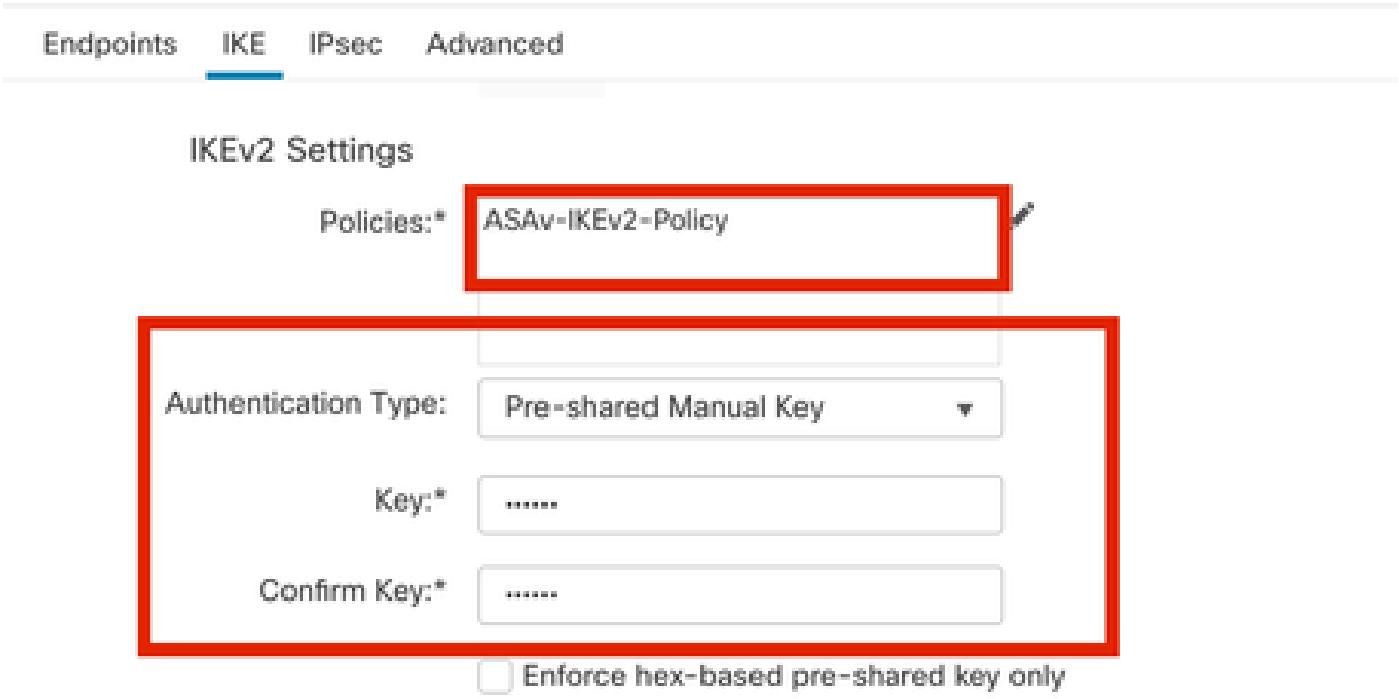
IKEv2-策略

步驟 10.選擇新建立的Policy或Policy現有的。選擇Authentication Type。如果使用預共用手動金鑰，請在Key和Confirm Key 框中輸入金鑰。

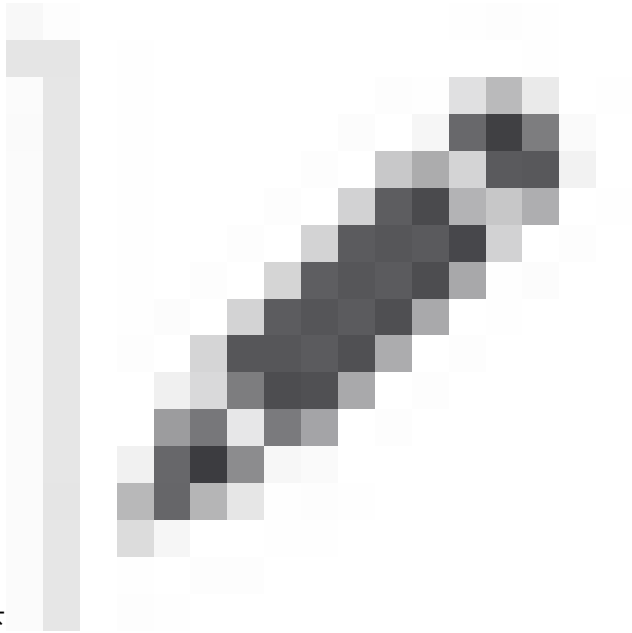
在本演示中：

策略：ASAv-IKEv2-Policy

驗證型別：預先共用手動金鑰



驗證



步驟 11.瀏覽至標IPsec 簽。按一下

可選擇使用預定義的IKEv2 IPsec建議或建立一個新建議。按一下IKEv2 IPsec Proposal 頁籤旁邊的+按鈕。

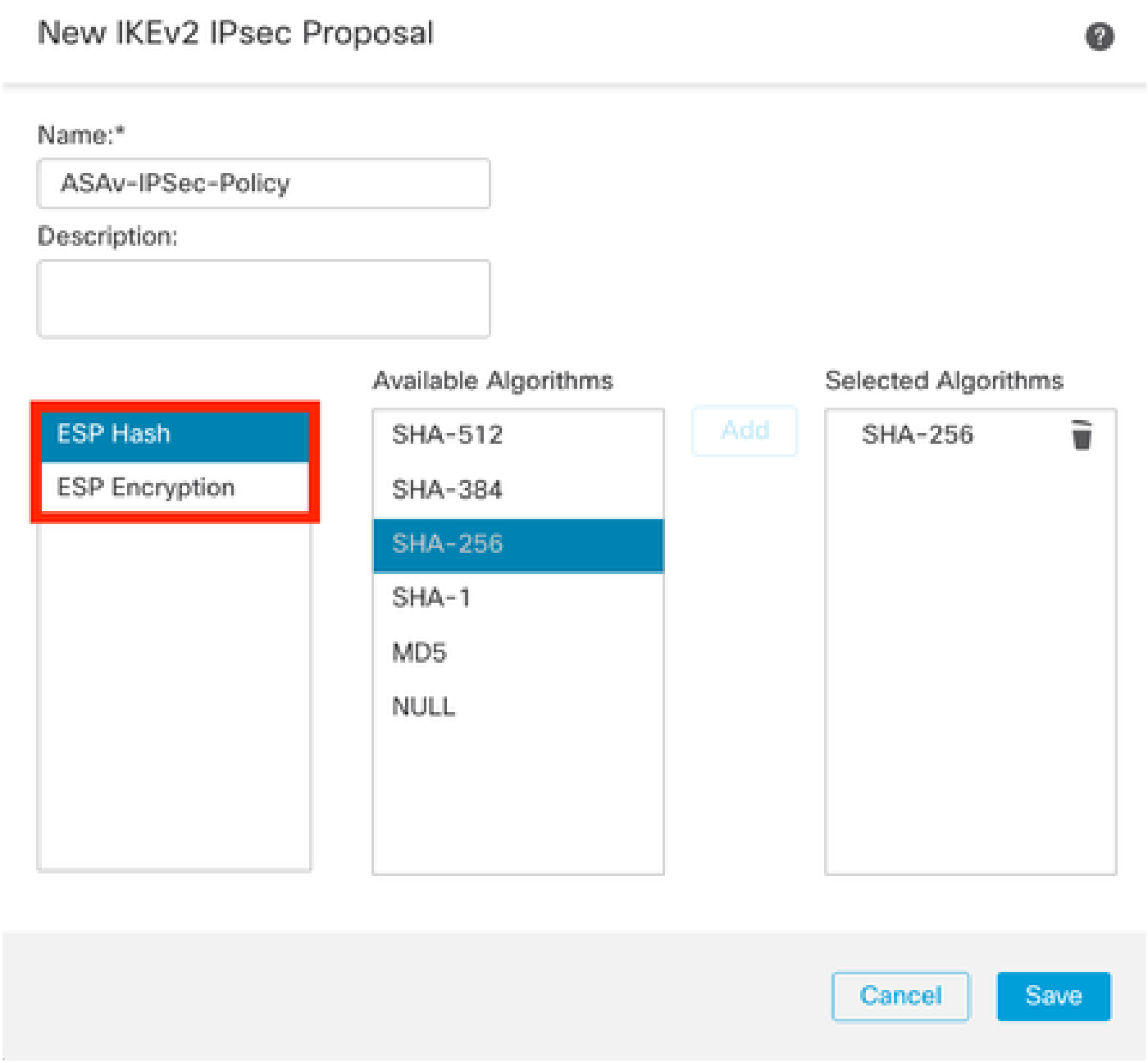
第12步：（可選，如果您建立新的IKEv2 IPsec提議。）輸入Name提案的編號，並選擇要在提案中使用的Algorithms。按一下Save。

在本演示中：

名稱：ASAv-IPSec-Policy

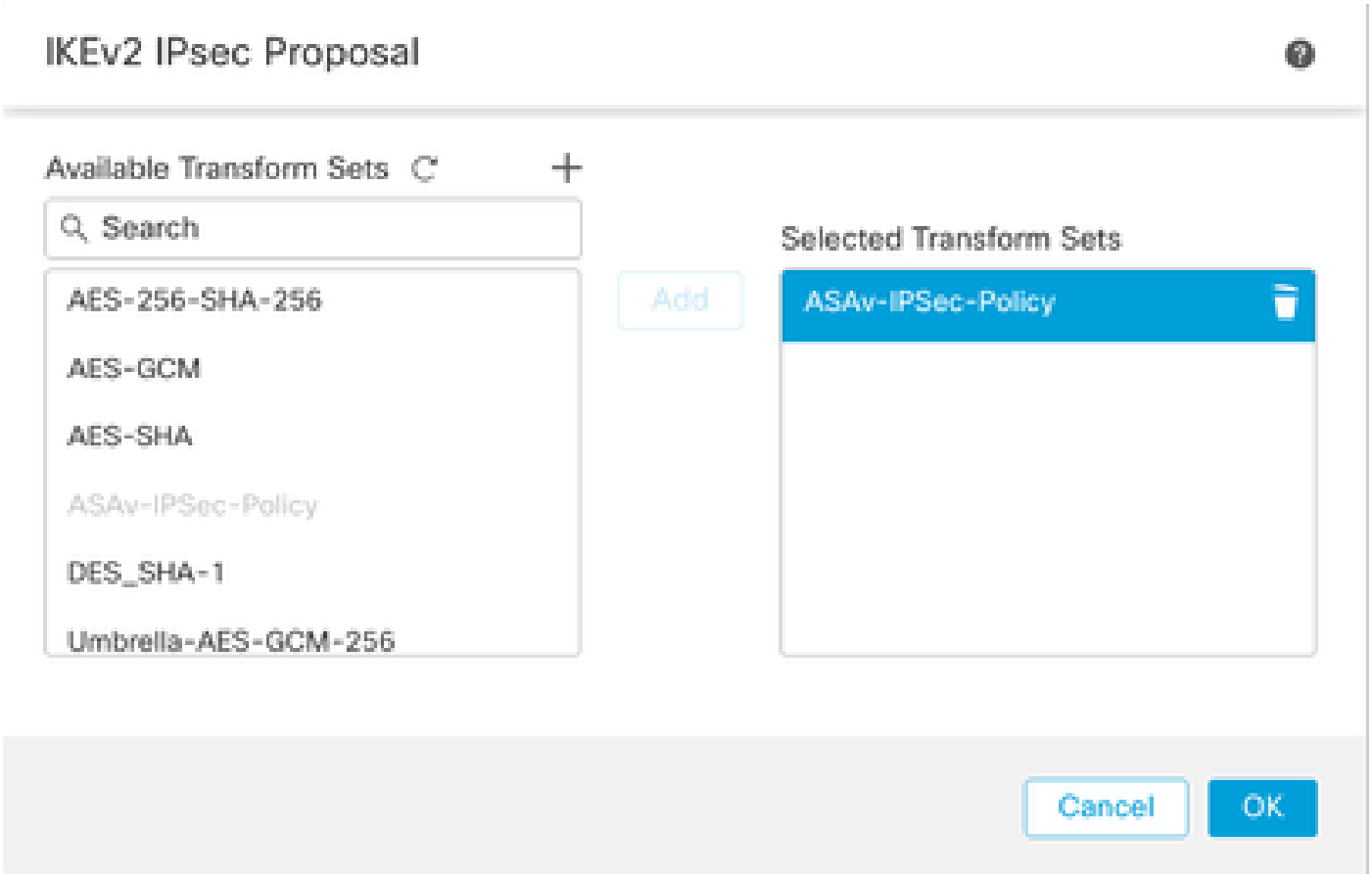
ESP雜湊：SHA-256

ESP加密：AES-256



IKEv2-IPsec-提議

步驟 13. 從可用提案清單中選擇新建立的Proposal或Proposal者。按一下OK。



轉換集

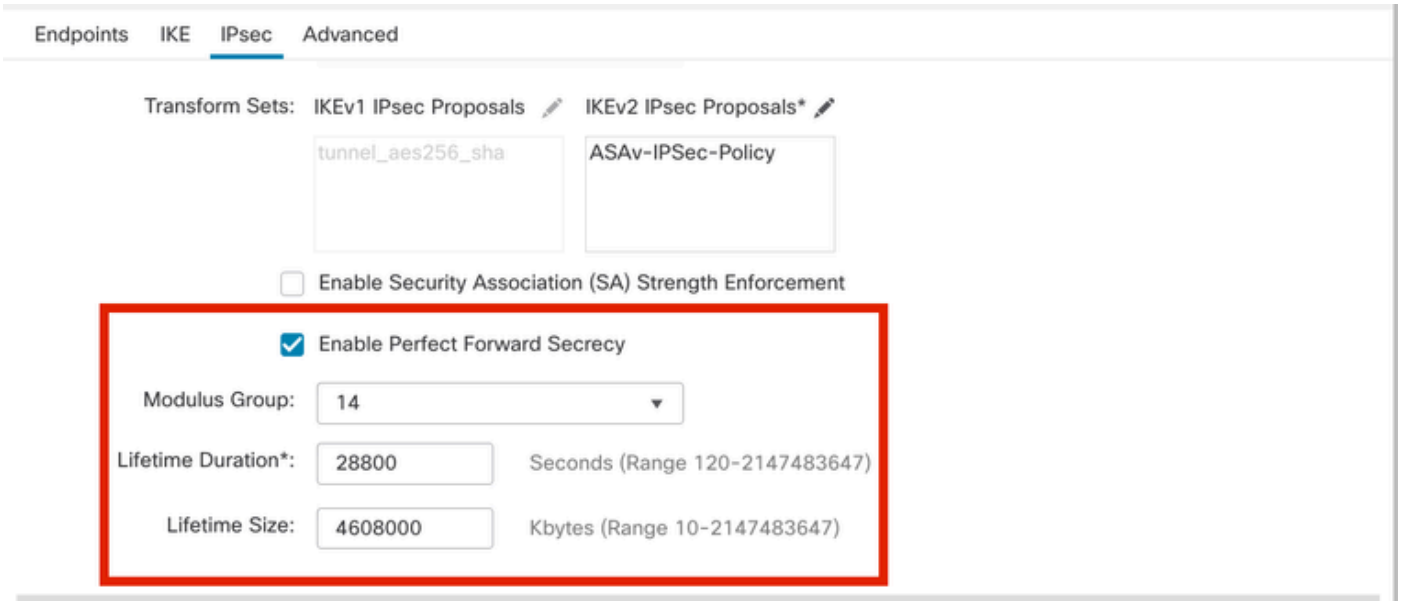
步驟14.（選擇性）選擇Perfect Forward Secrecy設定。配置IPSecLifetime Duration and Lifetime Size。

在本演示中：

完全正向保密：模陣列14

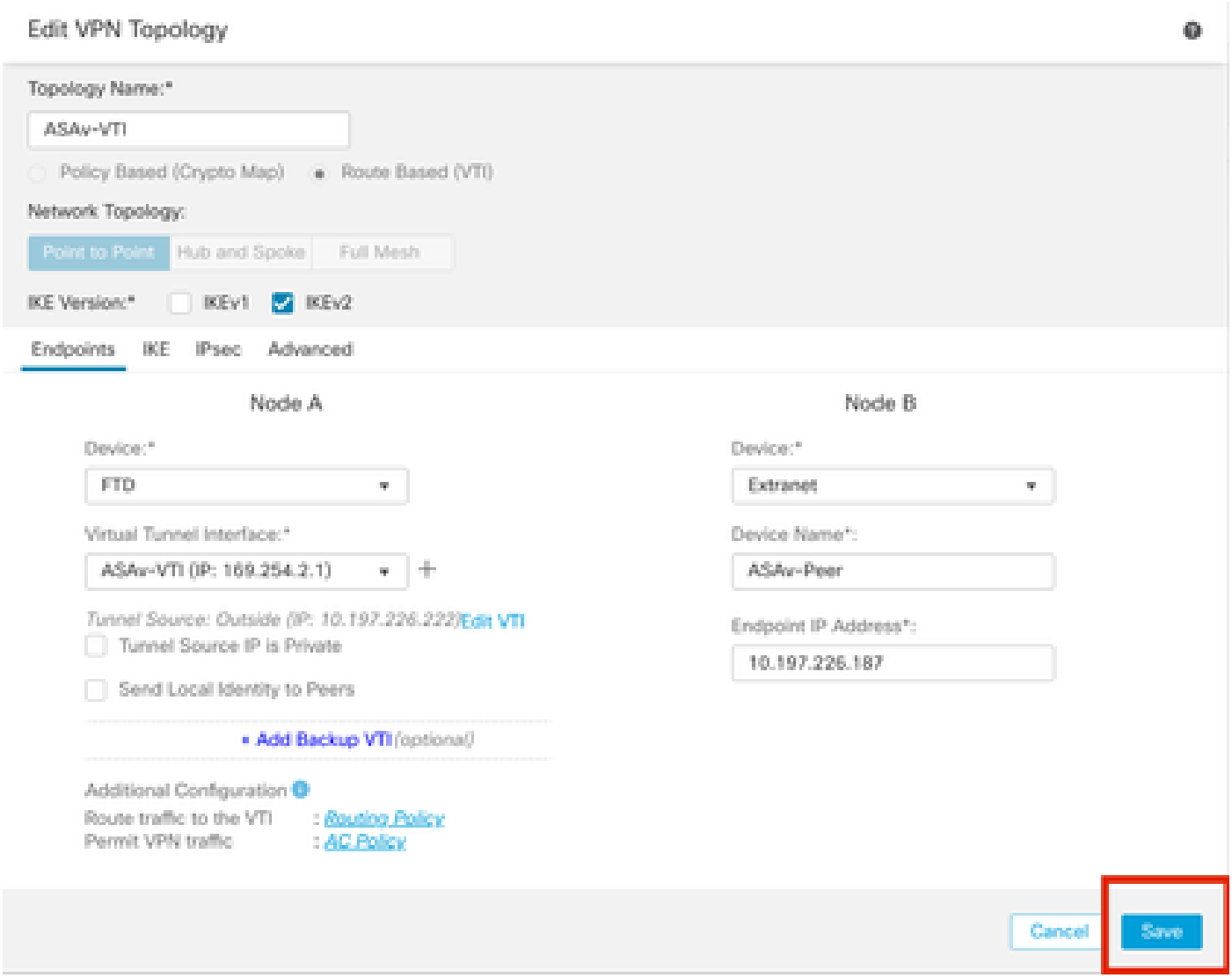
存留期期間：28800（預設）

存留時間大小： 4608000（預設）



*PFS*配置

步驟 15.檢查配置的設定。按一下Save（如圖所示）。



儲存組態

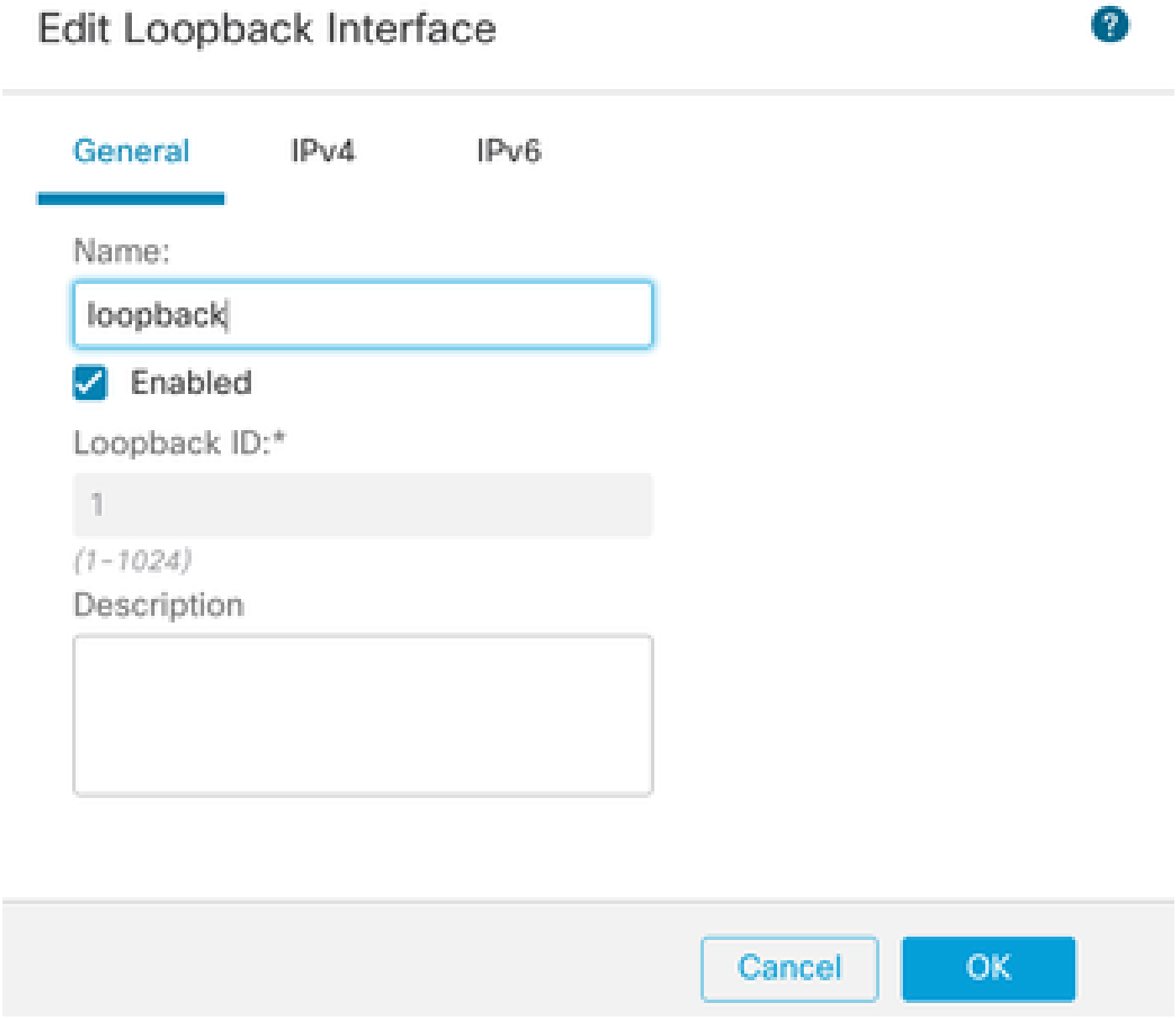
使用FMC設定FTD上的回送介面

導航到Devices > Device Management。編輯需要配置環回的裝置。

步驟 1.轉至Interfaces > Add Interfaces > Loopback Interface。

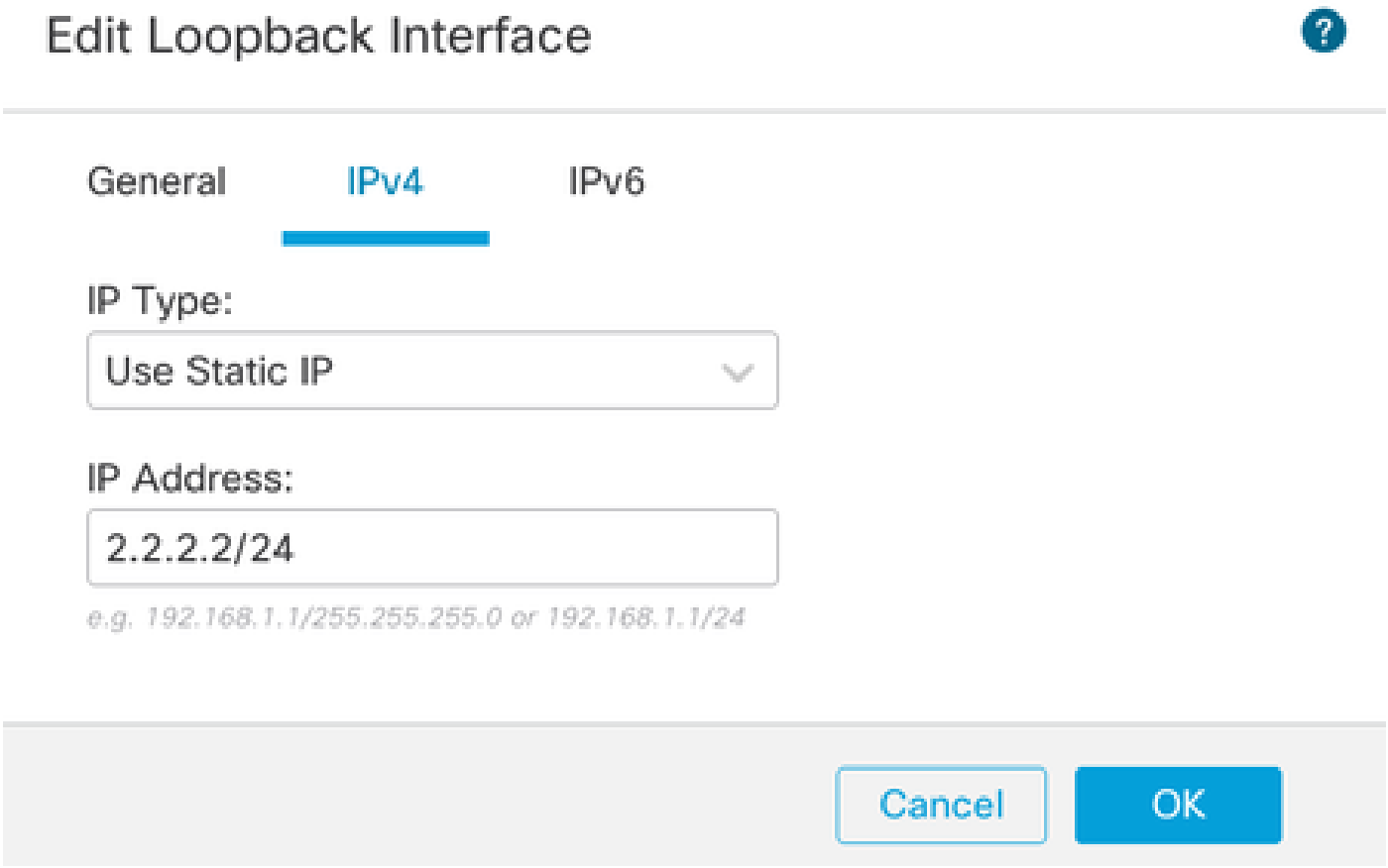
導航到*Loopback*介面

步驟 2.輸入名稱「loopback」，提供環回ID「1」並啟用介面。



啟用環回介面

步驟 3.配置介面的IP地址，然後按一下OK 。



向環回介面提供*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上配置環回介面

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

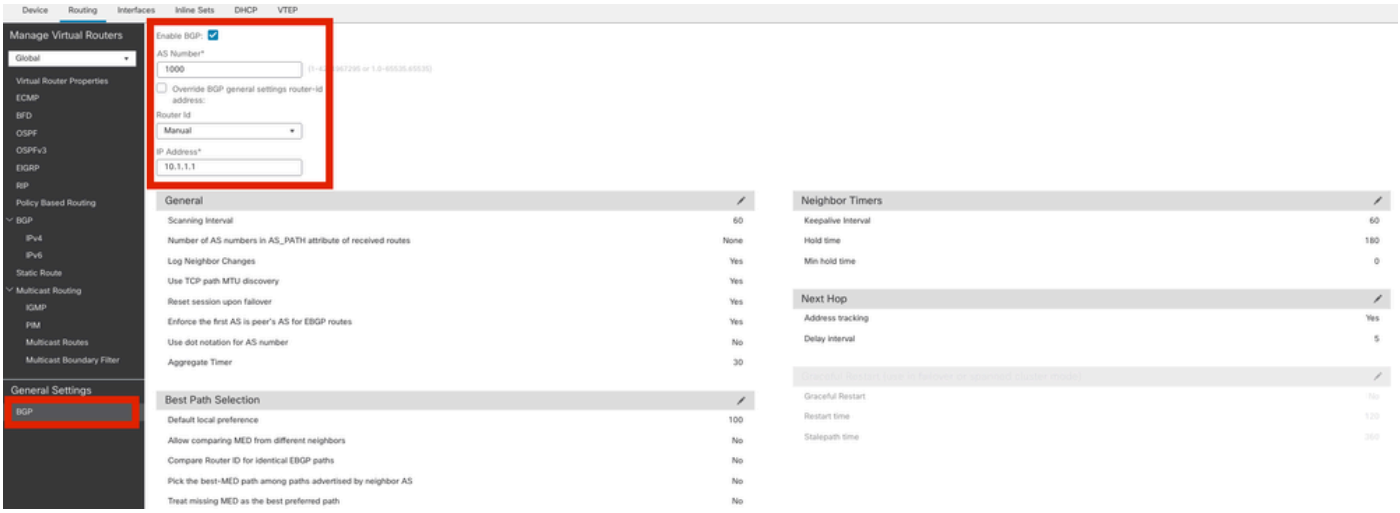
使用FMC在FTD上設定重疊BGP

導航到Devices > Device ManagementEdit 。**導航到配置**VTI**隧道的裝置，然後導航到**Routing >General Settings > BGP。

步驟 1.啟用BGP並配置自治系統(AS)編號和路由器ID，如此圖中所示。

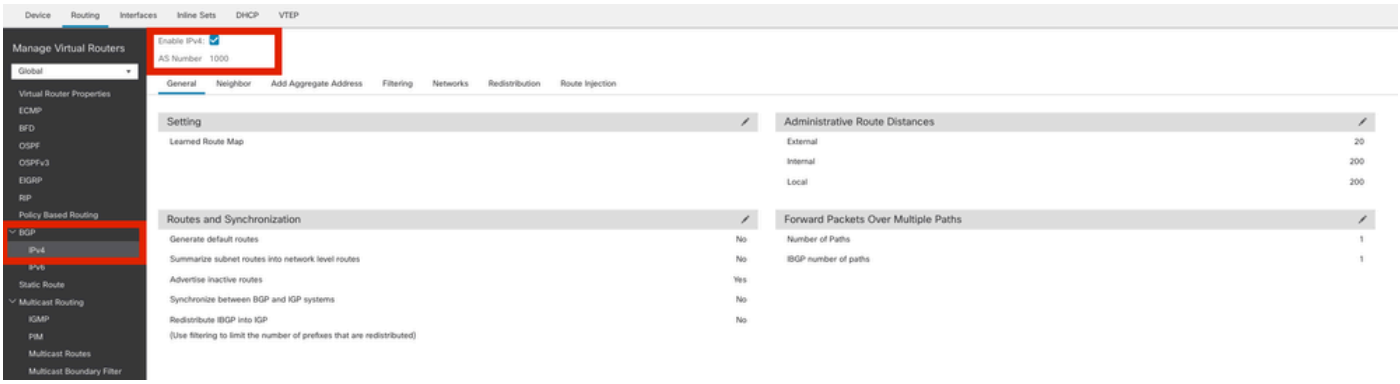
裝置FTD和ASA上的AS編號必須相同。

路由器ID用於標識參與BGP的每個路由器。



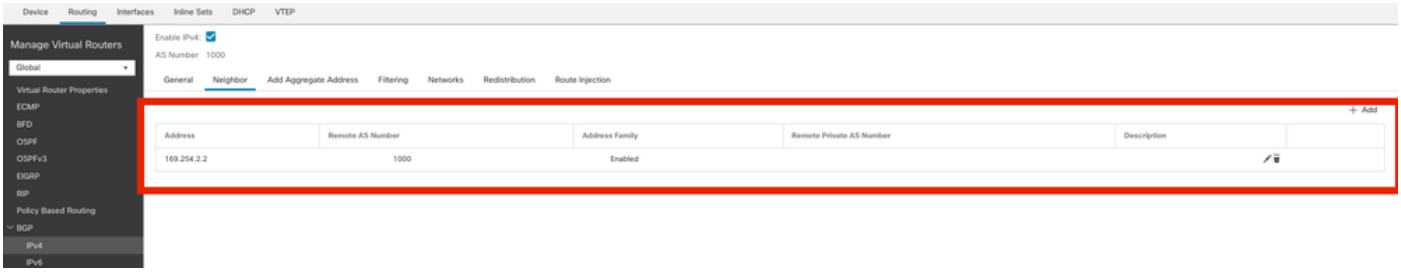
導航到配置*BGP*

步驟 2.導覽至BGP > IPv4，並在FTD上啟用BGP IPv4。



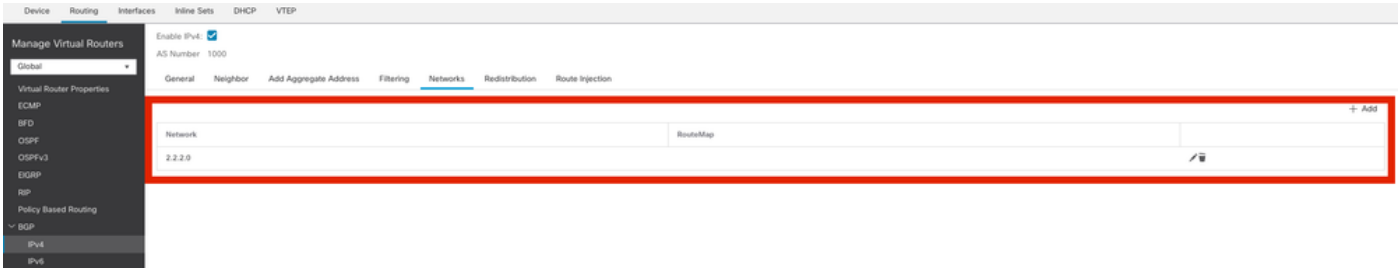
啟用*BGP*

步驟 3.在Neighbor頁籤下，增加ASAv VTI隧道IP地址作為鄰居並啟用鄰居。



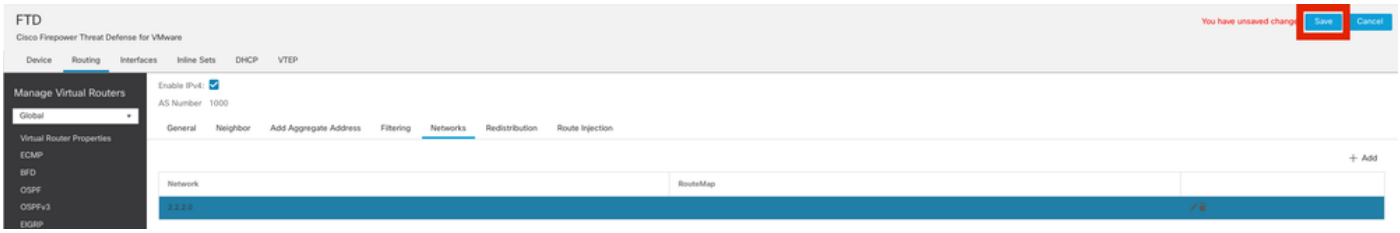
增加*BGP*鄰居

步驟 4.在Networks下，增加要透過BGP通告但需要透過VTI隧道的網路（在本例中為loopback1）。



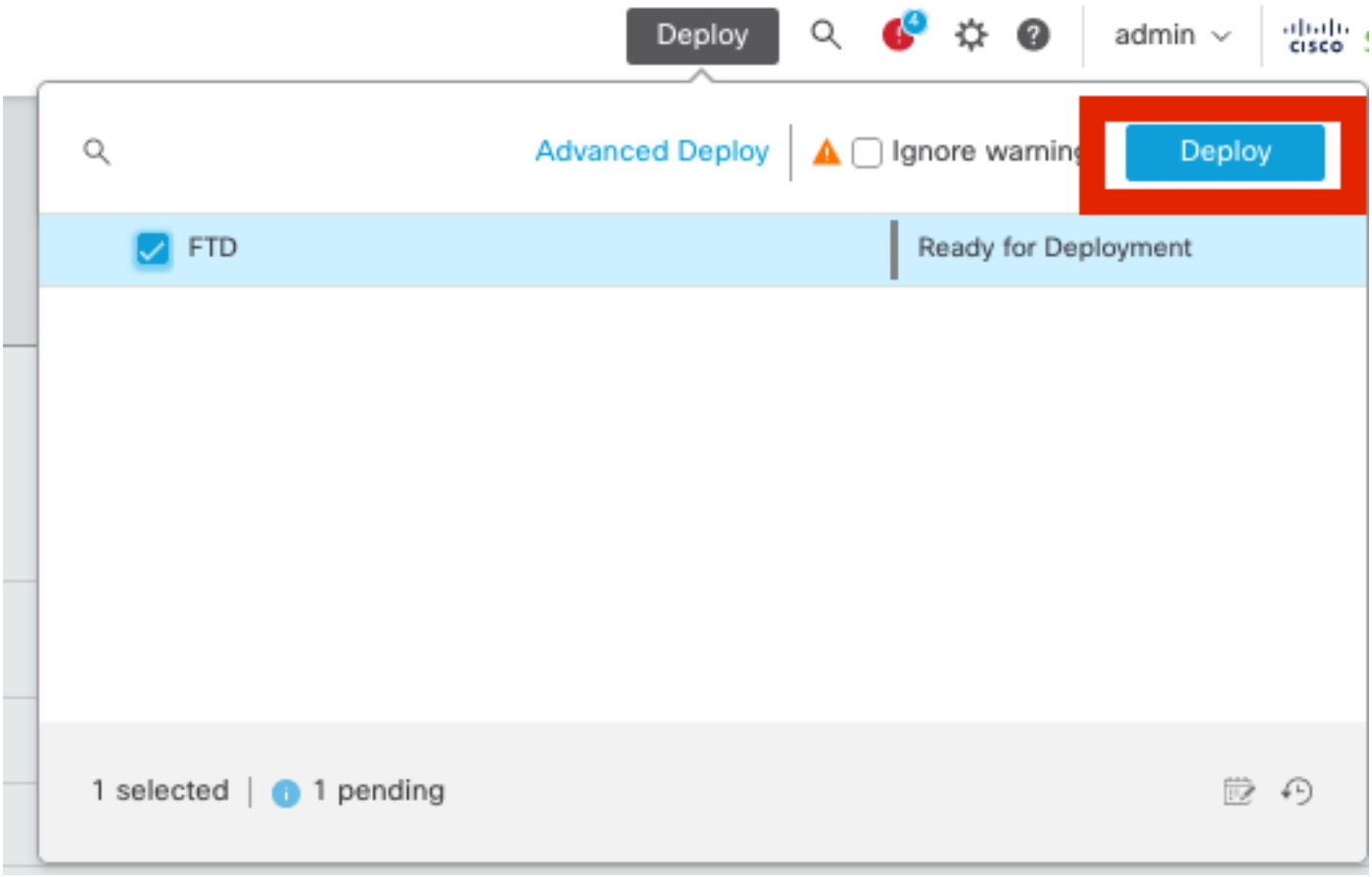
增加*BGP*網路

步驟 5.所有其他BGP設定都是可選的，您可以根據您的環境對其進行配置。驗證配置並按一下Save。



儲存*BGP*配置

步驟 6.部署所有配置。



部署

在ASA上配置重疊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

驗證

使用本節內容，確認您的組態是否正常運作。

FTD上的輸出

```
<#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上的輸出

<#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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

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

- **僅支援IPv4介面，以及IPv4、受保護的網路或VPN負載（不支援IPv6）。**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。