تكوين شبكة VPN المستندة إلى المسار من موقع إلى موقع بين ASA و FTD مع BGP عبر الإنترنت

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق VPN مستند إلى المسار من موقع إلى موقع بين جدار الحماية القابل للتكيف (ASA) والدفاع عن تهديد FirePOWER (FTD) بواسطة مركز إدارة FirePOWER (FMC) مع بروتوكول عبارة التوجيه الديناميكي (BGP) كتغشية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الفهم الأساسي لشبكة VPN من موقع إلى موقع IPsec
- تكوينات BGP على FTD و ASA
- تجربة مع FMC

المكونات المستخدمة

- Cisco ASAv الإصدار 9.20(2)2
- Cisco FMC، الإصدار 7.4.1
- Cisco FTD، الإصدار 7.4.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

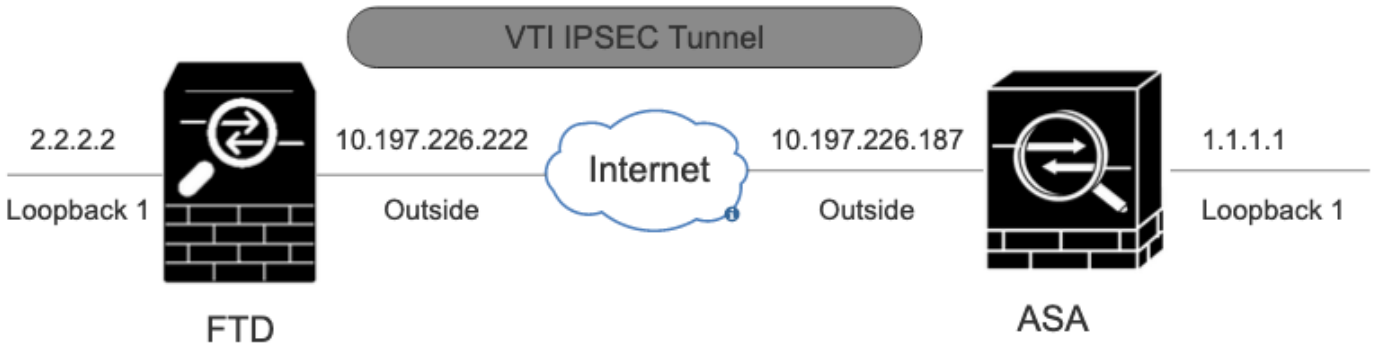
تسمح الشبكة الخاصة الظاهرية (VPN) المستندة إلى المسار بتشفير تحديد حركة مرور البيانات المفيدة، وإرسالها عبر نفق VPN، وتستخدم توجيه حركة مرور البيانات بدلا من قائمة الوصول/السياسة كما هو الحال في شبكة VPN المستندة إلى خريطة التشفير وأ القائمة على السياسة. تم تعيين مجال التشفير للسماح بأي حركة مرور تدخل نفق IPsec. تم تعيين محددات حركة مرور البيانات المحلية والبعيدة ل IPsec على 0.0.0.0/0.0.0.0. يتم تشفير أي حركة مرور يتم توجيهها إلى نفق IPsec بغض النظر عن الشبكة الفرعية للمصدر/الوجهة.

يركز هذا المستند على تكوين واجهة النفق الظاهرية الثابتة (SVTI) مع بروتوكول BGP للتوجيه الديناميكي كتغشية.

التكوين

يصف هذا القسم التكوين المطلوب على ASA و FTD لعرض جوار BGP من خلال نفق SVTI IPSec.

الرسم التخطيطي للشبكة



الرسم التخطيطي للشبكة

التكوينات

تكوين IPSec VPN على FTD باستخدام FMC

الخطوة 1. انتقل إلى Devices > VPN > Site To Site .

الخطوة 2. انقر فوق +Site to Site VPN .

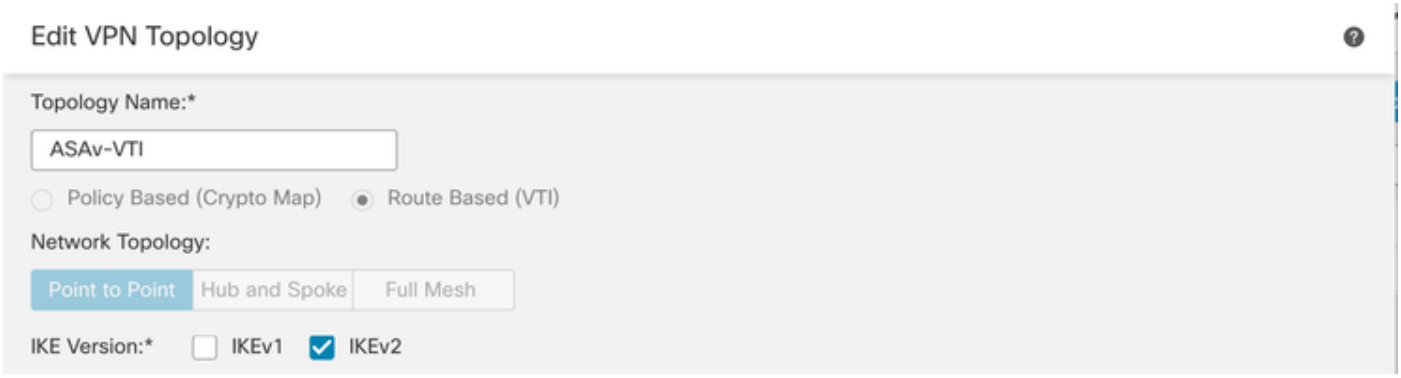
شبكة *VPN* من موقع إلى موقع

الخطوة 3. توفير Topology Name وتحديد نوع شبكة VPN باسم Route Based (VTI). أختر IKE Version.

من أجل هذا العرض التوضيحي:

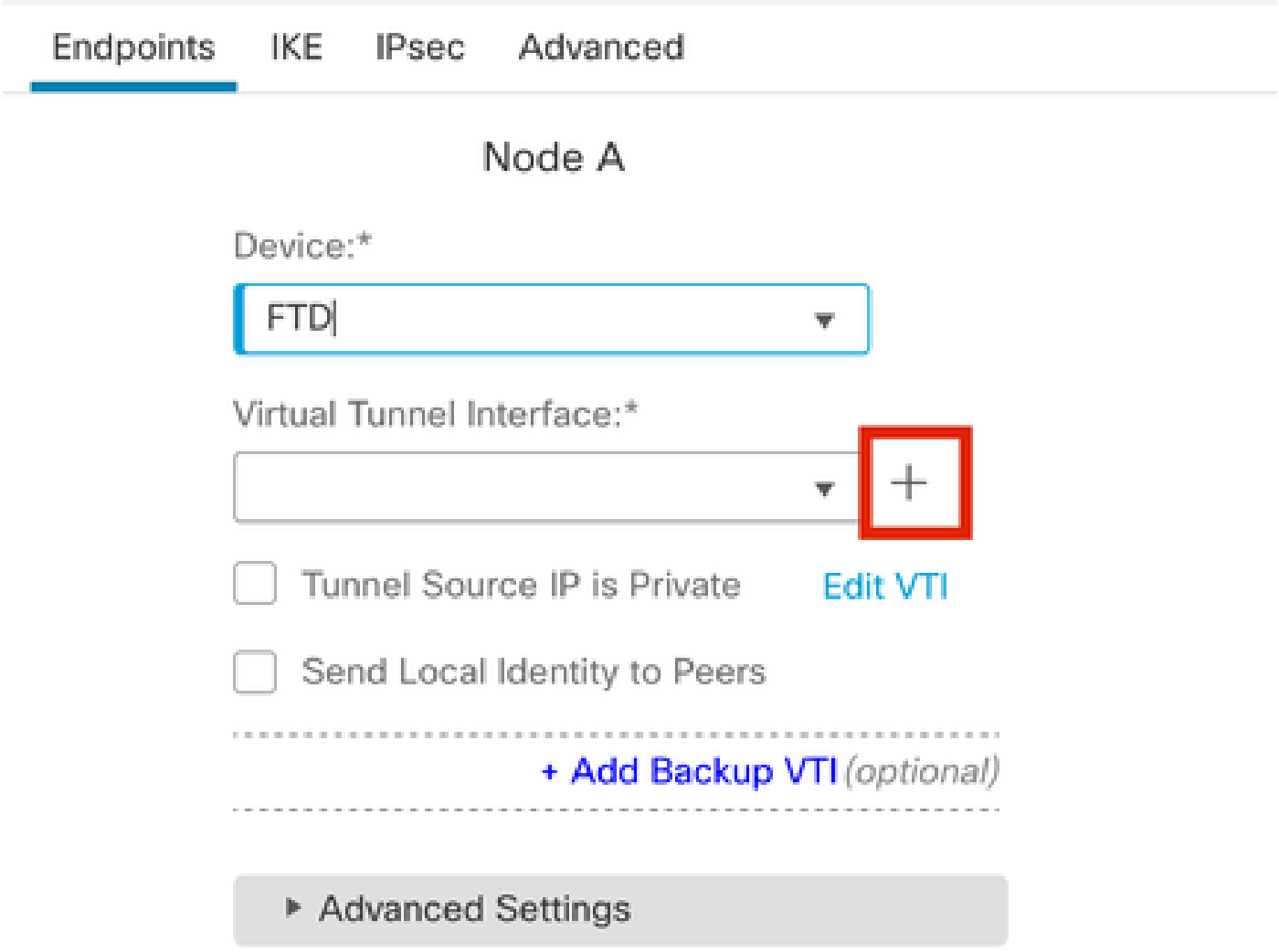
اسم المخطط: ASAv-VTI

إصدار IKE: IKEv2



طوبولوجيا *VPN*

الخطوة 4. أختر Deviceالنفق الذي يلزم تكوينه. يمكنك إضافة واجهة نفق ظاهري جديدة (انقر على + الرمز) أو تحديد واجهة من القائمة الموجودة.



عقدة نقطة النهاية A

الخطوة 5. قم بتحديد معلمات New Virtual Tunnel Interface. انقر.Ok

من أجل هذا العرض التوضيحي:

الاسم: ASA-VTI

الوصف (إختياري): نفق VTI مع Extranet ASA

المنطقة الأمنية: منطقة vTI-Zone

معرف النفق: 1

عنوان IP: 169.254.2.1/24

مصدر النفق: GigabitEthernet0/1 (خارجي)

وضع نفق IPsec: 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

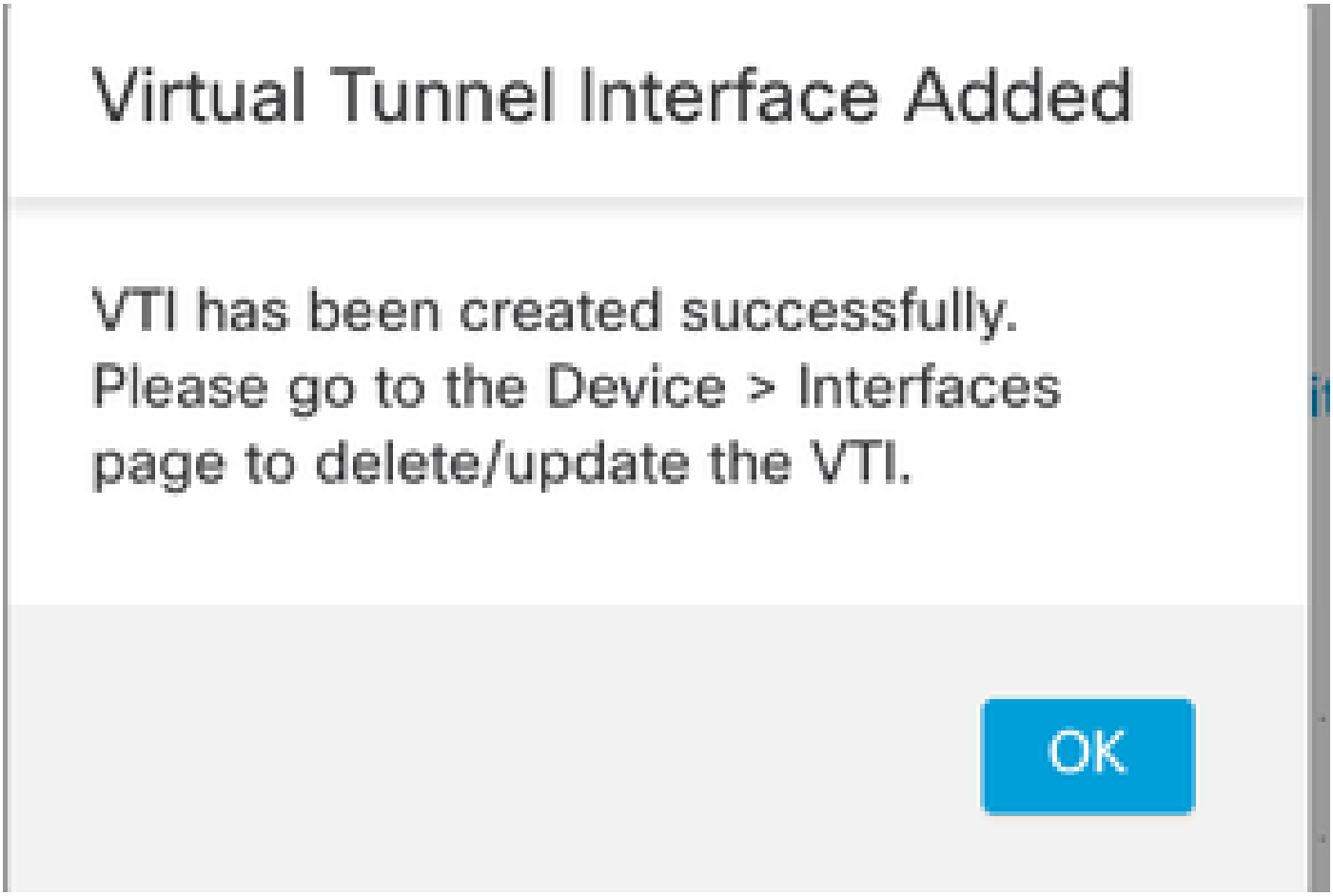
IP Address:*

(•) Configure IP 169.254.2.1/24

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

Cancel OK

الخطوة 6. طقطقتOK على المنبثق ذيكر أن ال VTI جديد خلقت.



تمت إضافة واجهة النفق الظاهري

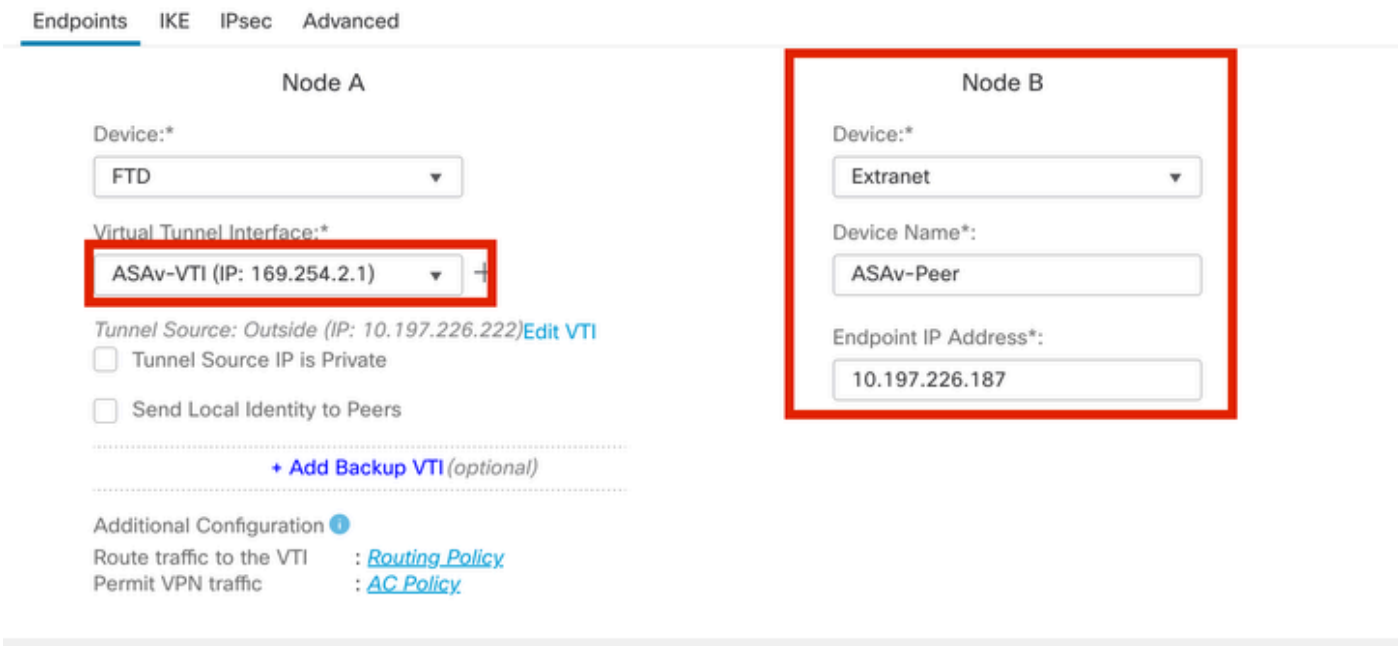
الخطوة 7. أخترت ال VTI newly created أو VTI تحت Virtual Tunnel Interface. قم بتوفير المعلومات للعقدة (والتي هي جهاز النظير).

من أجل هذه العرض التوضيحي:

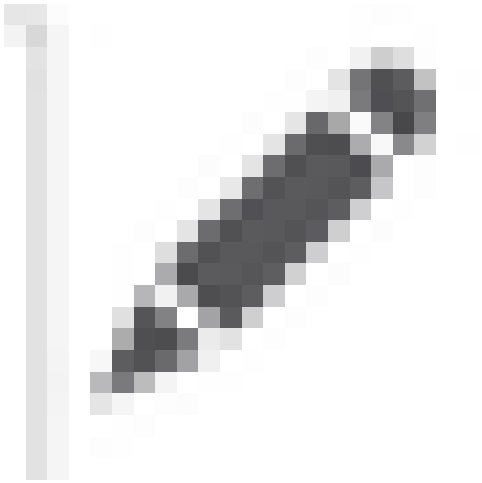
الجهاز: إكسترانت

اسم الجهاز: ASAv-Peer

عنوان IP لنقطة النهاية: 10.197.226.187



عقدة نقطة النهاية *B*



الخطوة 8. انتقل إلى علامة التبويب **IKE**. انقر فوق علامة التبويب Policy جواز الموجود +الزر فوق النقر مسبقا Policy أو معرف استخدام إختياري، يمكنك إنشاء واحد جديد.

الخطوة 9. (إختياري، إذا قمت بإنشاء سياسة IKEv2 جديدة.) قم بتوفير Name للنهج وحدد النهج Algorithms الذي سيتم إستخدامه في النهج. انقر Save.

من أجل هذا العرض التوضيحي:

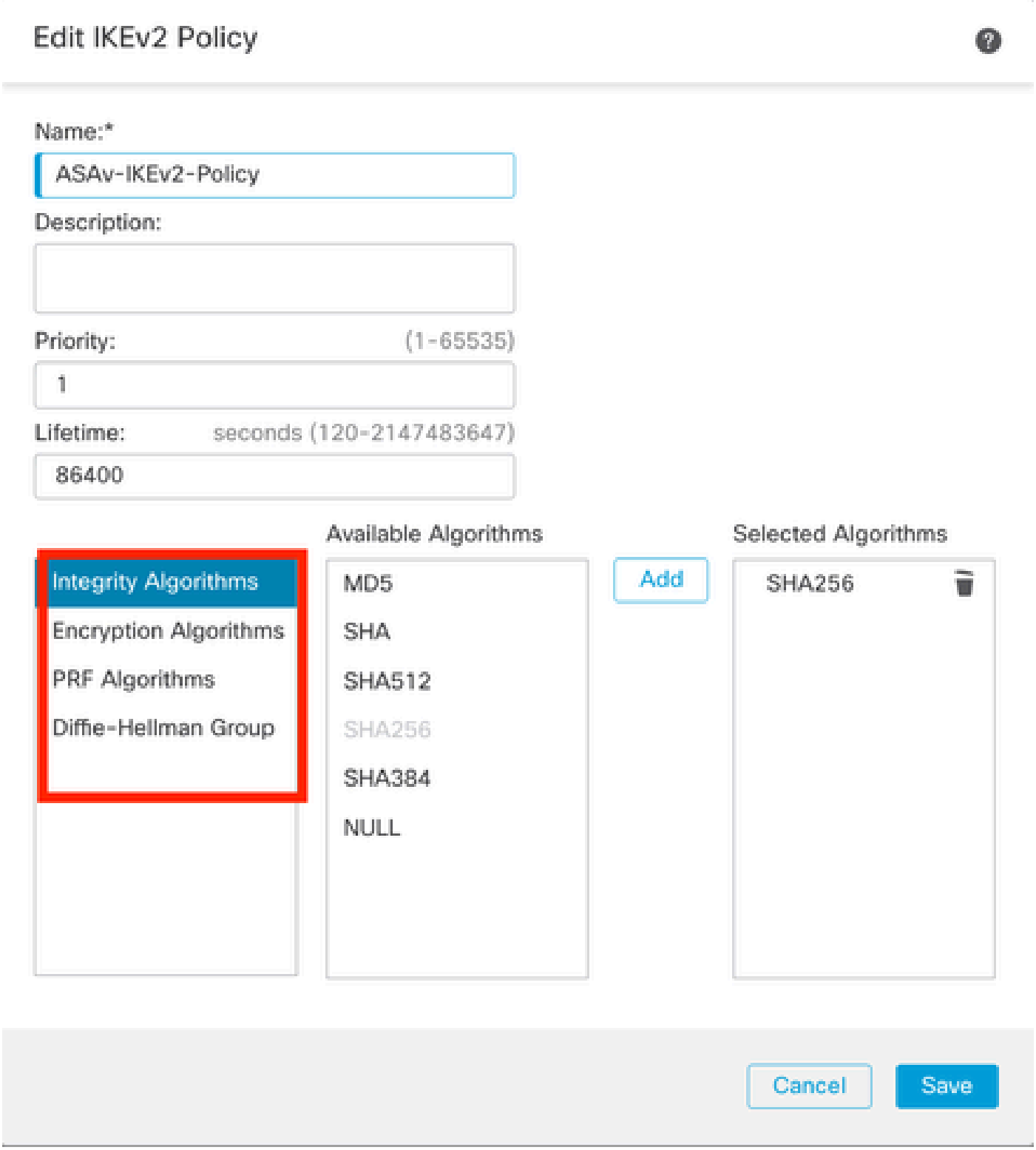
الاسم: ASAv-IKEv2-policy

خوارزميات التكامل: SHA-256

خوارزميات التشفير: AES-256

خوارزميات PRF: SHA-256

مجموعة Diffie-Hellman: 14



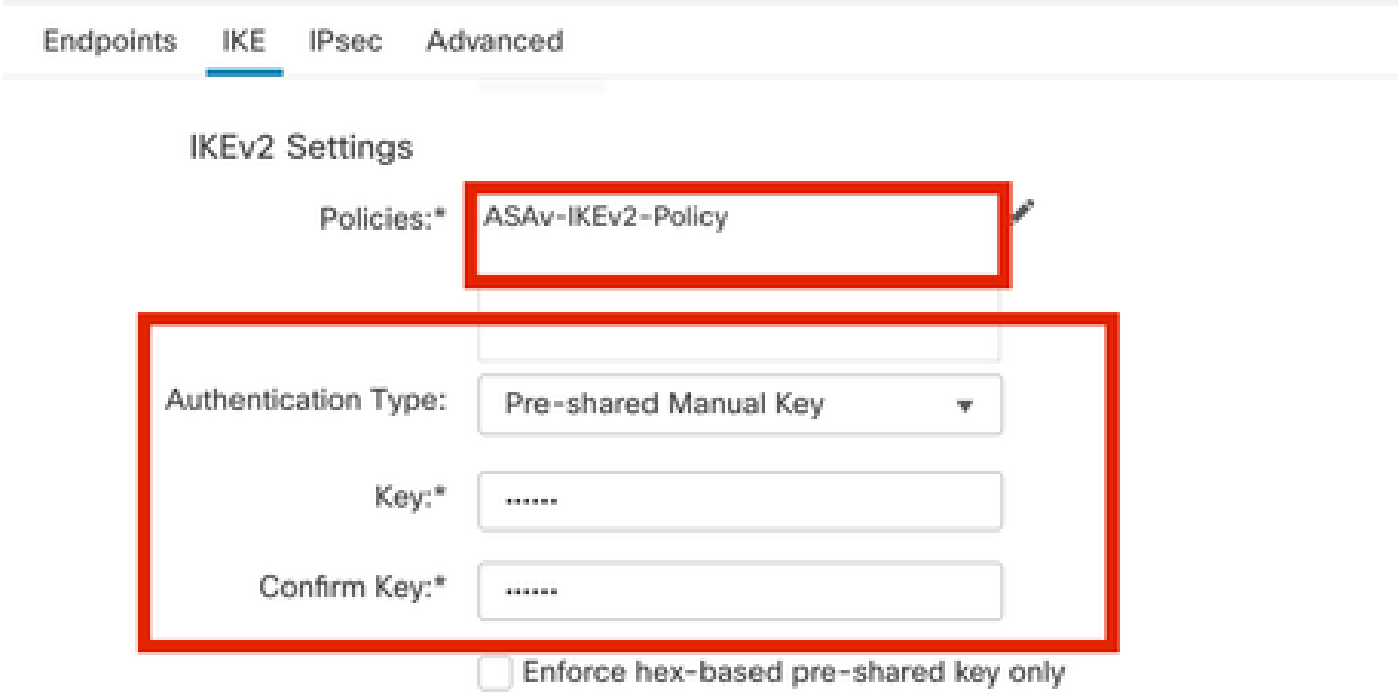
IKEv2-Policy

الخطوة 10. أخترت ال newly created Policy أو ال Policyأن يتواجد. حدد Authentication Type. إذا تم إستخدام مفتاح يدوي مشترك مسبقا، فأدخل المفتاح في KeyConfirm Key المربع.

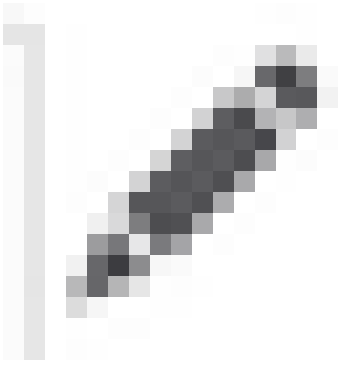
من أجل هذا العرض التوضيحي:

السياسة: ASAv-IKEv2-Policy

نوع المصادقة: مفتاح يدوي مشترك مسبقا



المصادقة



الخطوة 11. انتقل إلى IPsec عالمة التبويب. يمكن أن يختار النقر فوق إستخدام مقترح IPsec المعرف مسبقا أو إنشاء مقترح جديد. انقر فوق +الزر الموجود بجوار IKEv2 IPsec Proposal عالمة التبويب.

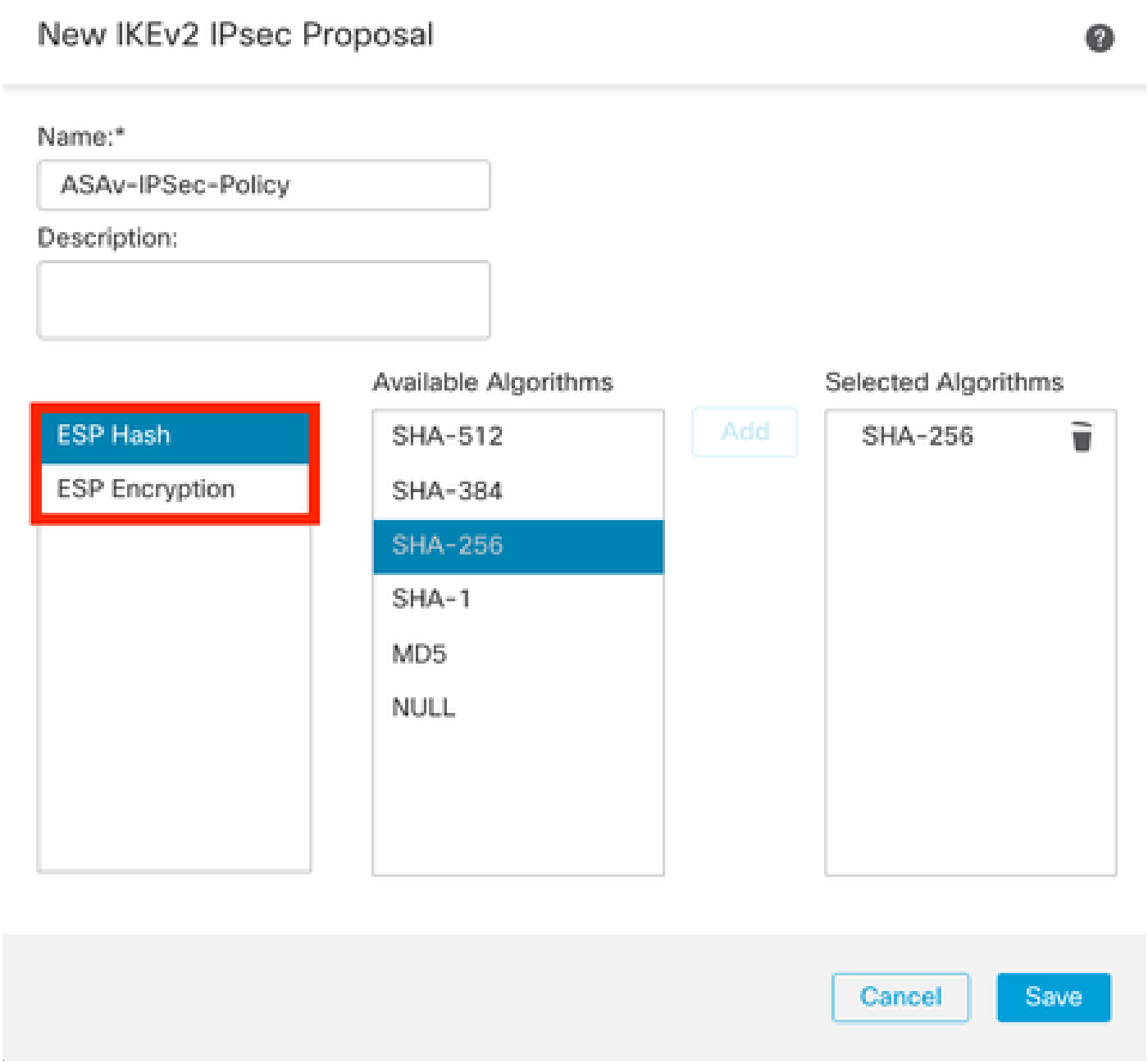
الخطوة 12. (إختياري، إذا قمت بإنشاء اقتراح IKEv2 IPsec جديد.) أدخل Nameلمقترح وحدد العرض الذيAlgorithms سيتم إستخدامه في العرض. انقر.Save

من أجل هذا العرض التوضيحي:

الاسم: ASAv-IPSec-Policy

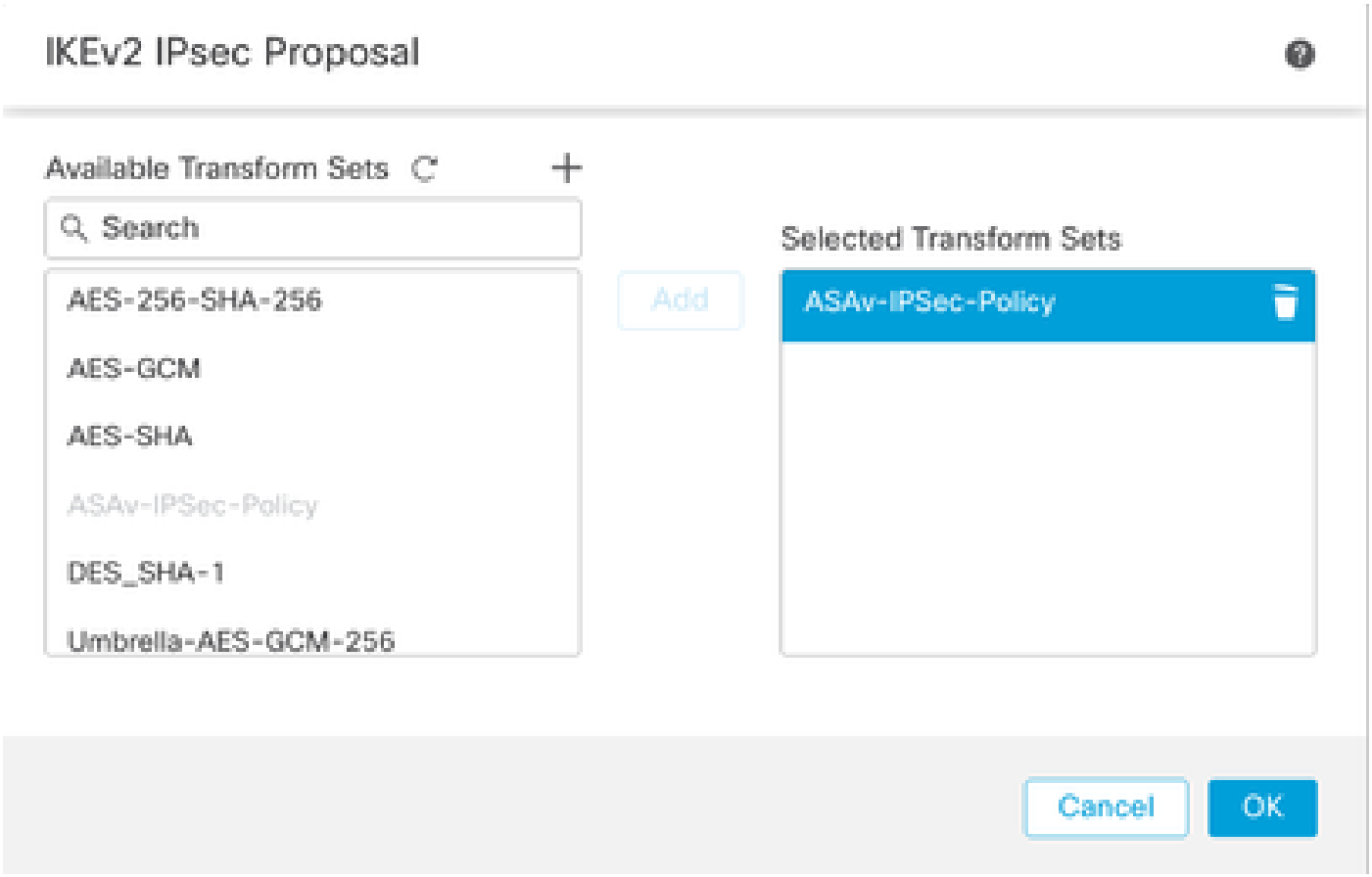
تجزئة ESP: SHA-256

تشفير ESP: AES-256



مقترح *IKEv2-IPsec*

الخطوة 13. أختر أوProposal Proposalلموجود من قائمة الاقتراحات المتوفرة. انقر.OK



مجموعة تحويل

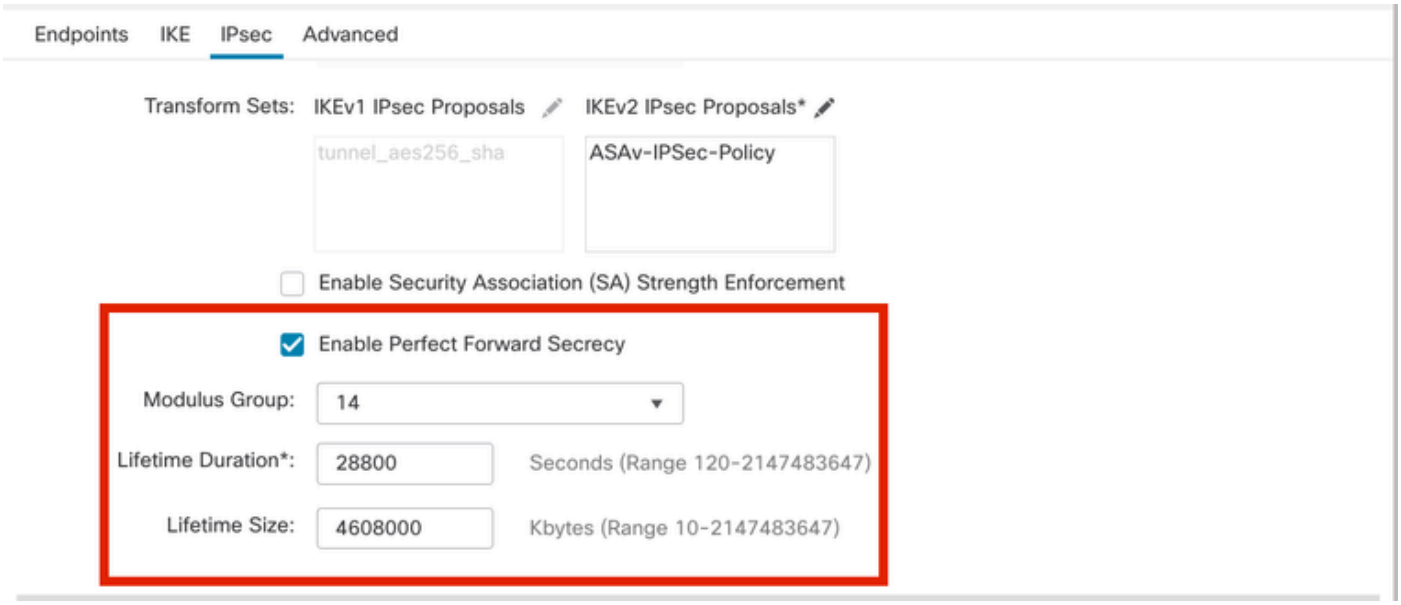
الخطوة 14. (إختياري) أخترPerfect Forward Secrecy الإعدادات. قم بتكوين IPsec Lifetime Duration and Lifetime Size.

من أجل هذا العرض التوضيحي:

سرية إعادة التوجيه المثالية: مجموعة المعاملات 14

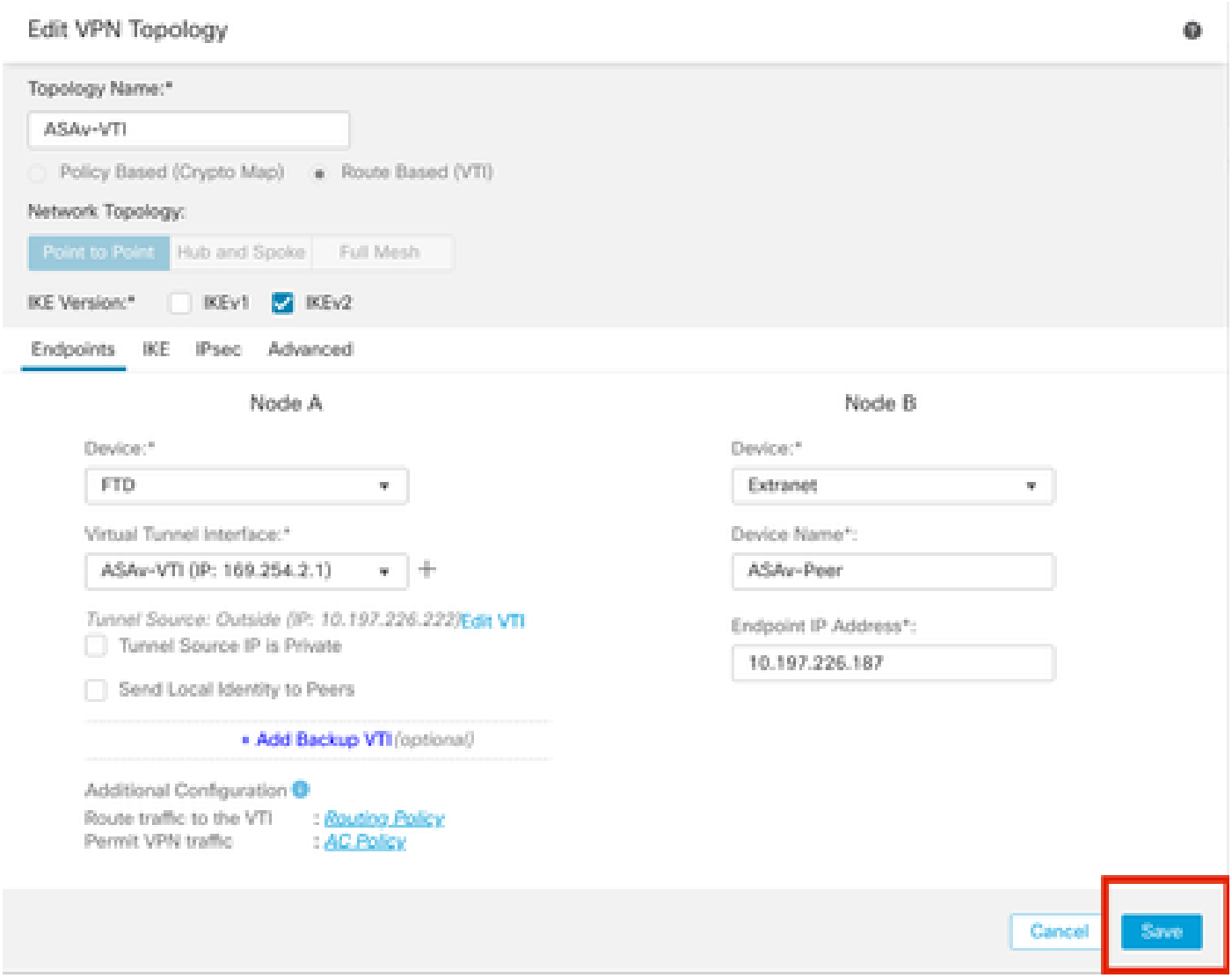
مدة العمر: 28800 (الافتراضي)

حجم العمر الافتراضي: 4608000 (الافتراضي)



تهيئة *PFS*

الخطوة 15. تحقق من الإعدادات التي تم تكوينها. انقر Save، كما هو موضح في هذه الصورة.



حفظ التكوين

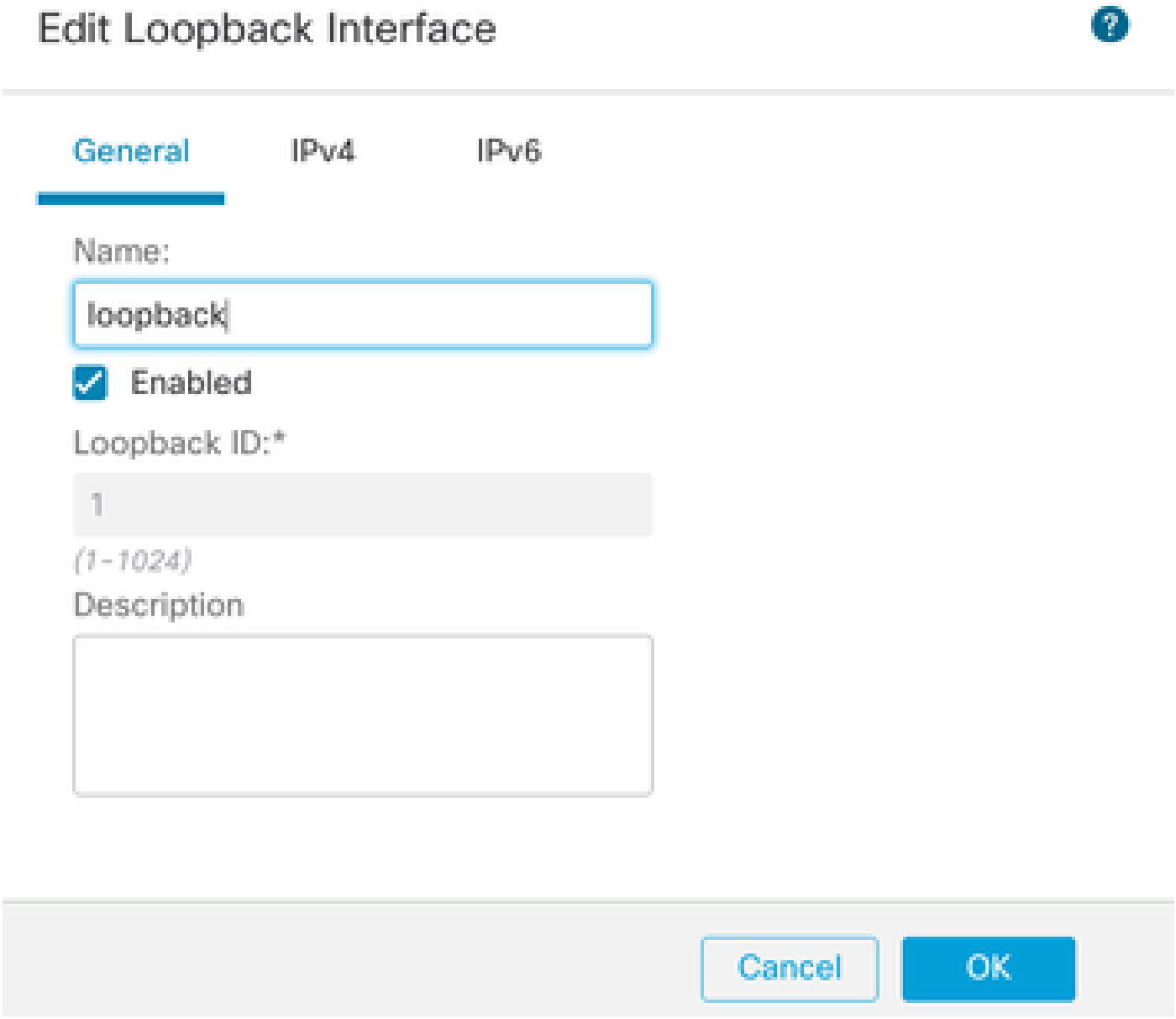
تكوين واجهة الاسترجاع على FTD باستخدام FMC

انتقل إلى Devices > Device Management . قم بتحرير الجهاز حيث يلزم تكوين الاسترجاع.

الخطوة 1. انتقل إلى Interfaces > Add Interfaces > Loopback Interface .

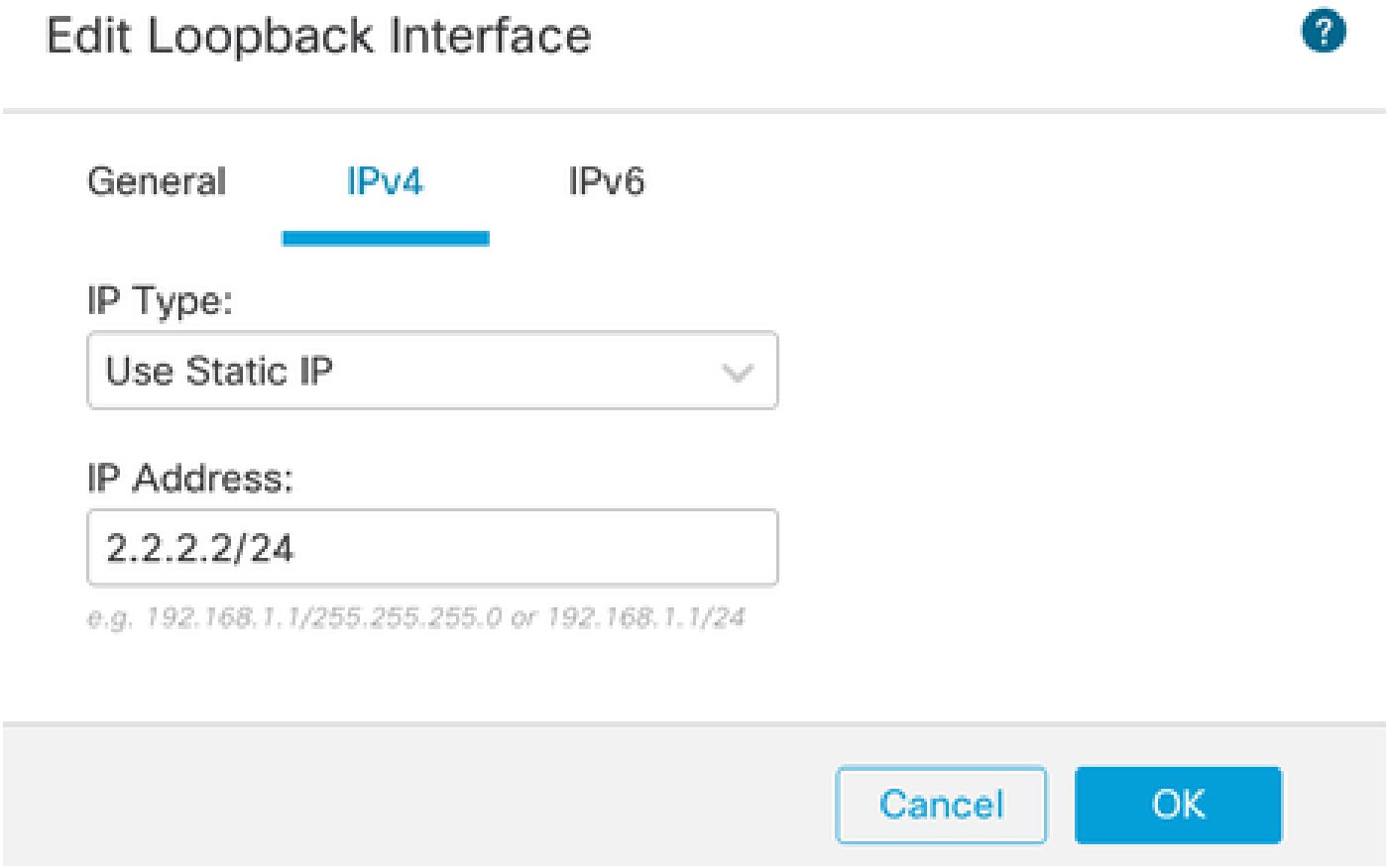
انتقل إلى واجهة الاسترجاع

الخطوة 2. أدخل الاسم "loopback"، وقم بتوفير معرف الاسترجاع "1" وتمكين الواجهة.



تمكين واجهة الاسترجاع

الخطوة 3. شكلت العنوان للقارن، طقطقت OK .



توفير عنوان IP لواجهة الاسترجاع

تكوين IPSec VPN على ASA

```
!--- Configure IKEv2 Policy ---!

crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400



!--- Enable IKEv2 on the outside interface ---!

crypto ikev2 enable outside



!---Configure Tunnel-Group with pre-shared-key---!

tunnel-group 10.197.226.222 type ipsec-l2l
tunnel-group 10.197.226.222 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

```
!--- Configure IPSec Policy ---!

crypto ipsec ikev2 ipsec-proposal ipsec_proposal_for_FTD
protocol esp encryption aes-256
protocol esp integrity sha-256



!--- Configure IPSec Profile ---!

crypto ipsec profile ipsec_profile_for_FTD
set ikev2 ipsec-proposal FTD-ipsec-proposal
set pfs group14



!--- Configure VTI ---!

interface Tunnel1
nameif FTD-VTI
ip address 169.254.2.2 255.255.255.0
tunnel source interface outside
tunnel destination 10.197.226.222
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile_for_FTD



!--- Configure the WAN routes ---!

route outside 0.0.0.0 0.0.0.0 10.197.226.1 1
```

تكوين واجهة الاسترجاع على ASA

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

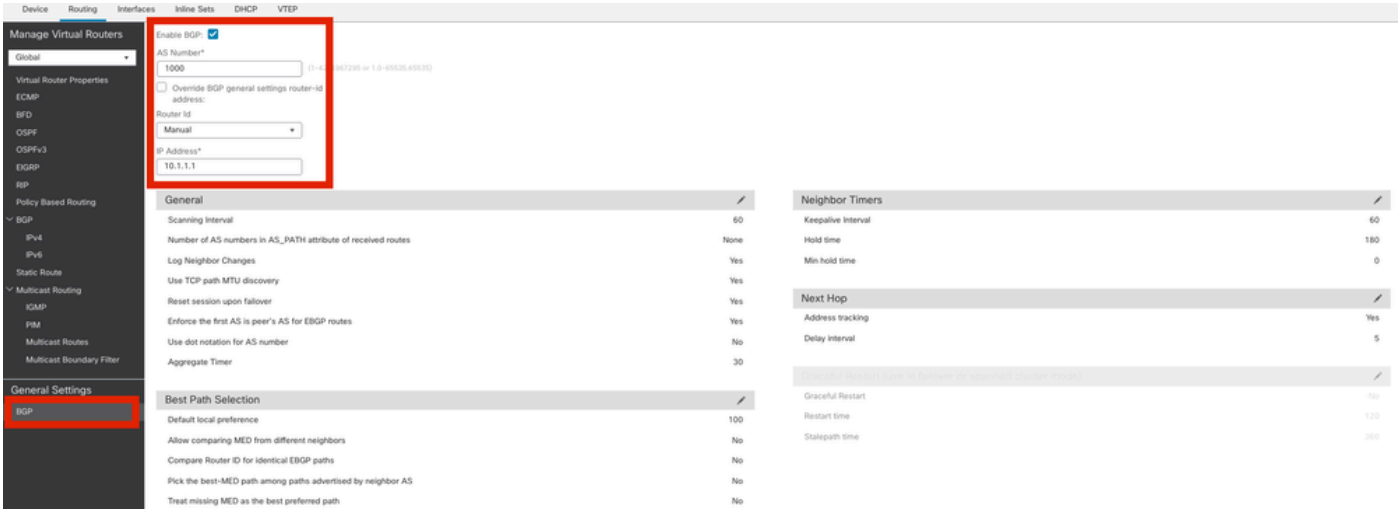
تكوين BGP التخطيطي على FTD باستخدام FMC

انتقل إلى Devices > Device Management.Edit الجهاز الذي تم تكوين نفق VTI به، ثم انتقل إلى Routing >General Settings > BGP.

الخطوة 1. قم بتمكين BGP وتكوين رقم النظام الذاتي (AS) ومعرف الموجه، كما هو موضح في هذه الصورة.

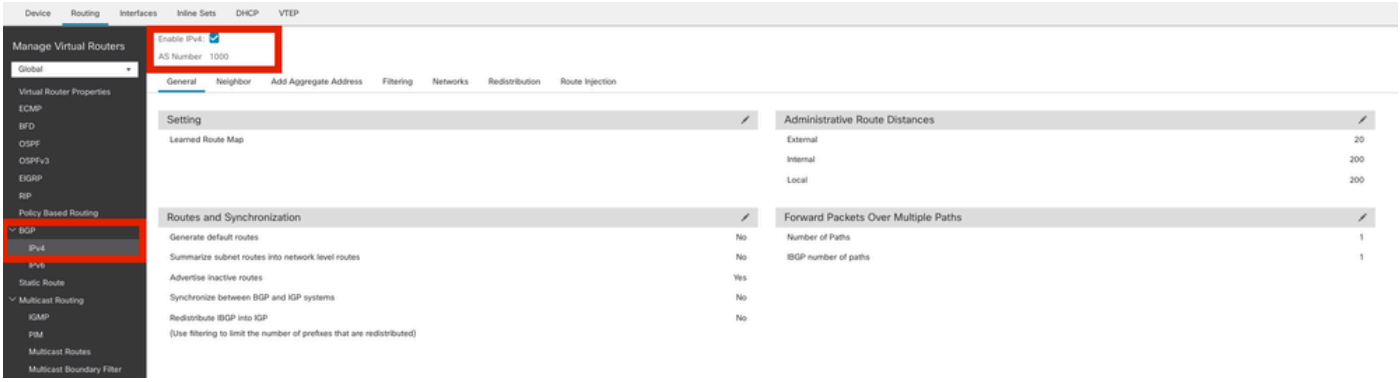
يجب أن يكون الرقم هو نفسه على كل من الجهازين FTD و ASA.

يتم إستخدام معرف الموجه لتحديد كل موجه مشارك في BGP.



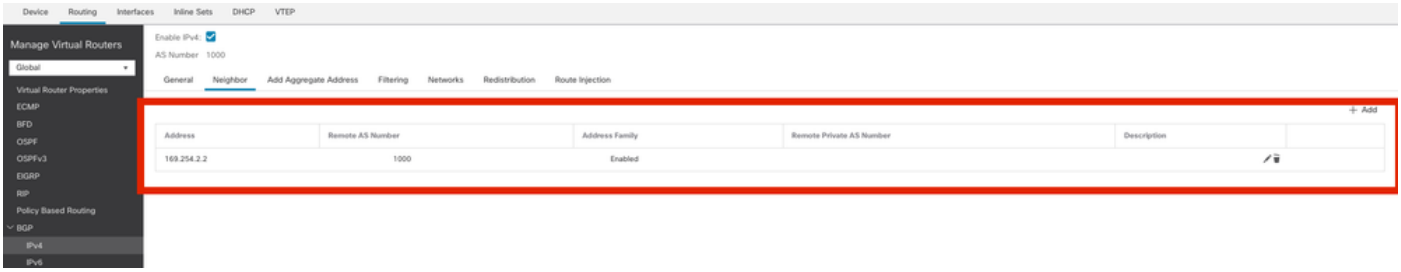
انتقل لتكوين *BGP*

الخطوة 2. انتقل إلى BGP > IPv4 BGP IPv4 وتمكينه على FTD.



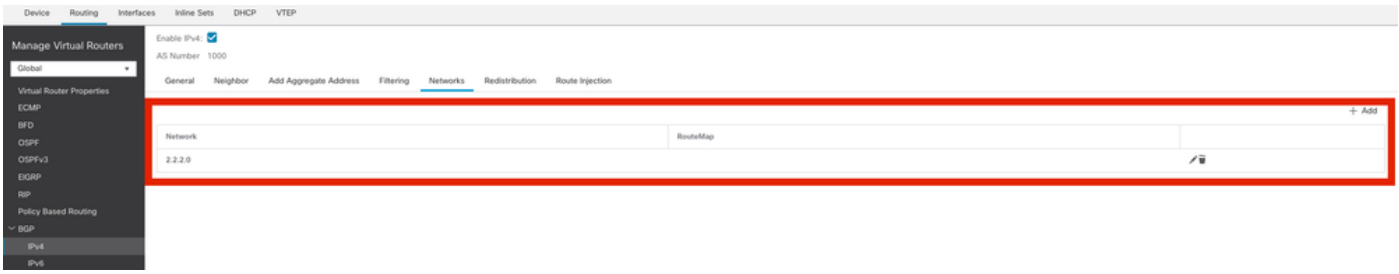
تمكين *BGP*

الخطوة 3. تحتNeighbor علامة التبويب، أضف عنوان IP لنفق ASAv VTI كجار وتمكين المجاور.



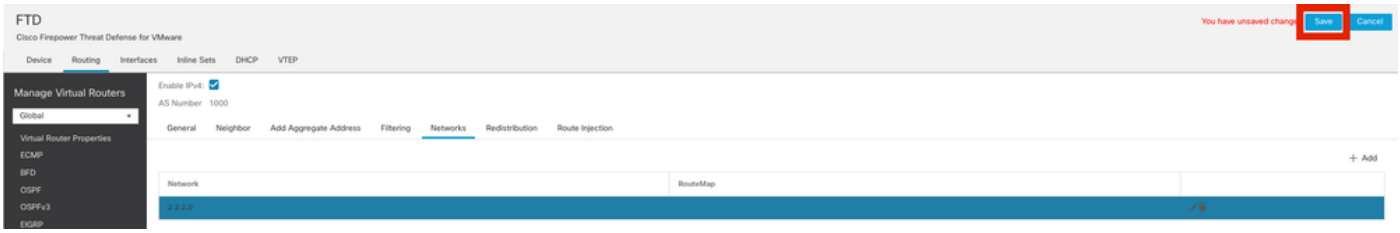
إضافة جار *BGP*

الخطوة 4. تحت Networks ، أضف الشبكات التي تريد الإعلان عنها من خلال BGP التي تحتاج إلى المرور عبر نفق VTI، في هذه الحالة، loopback1.



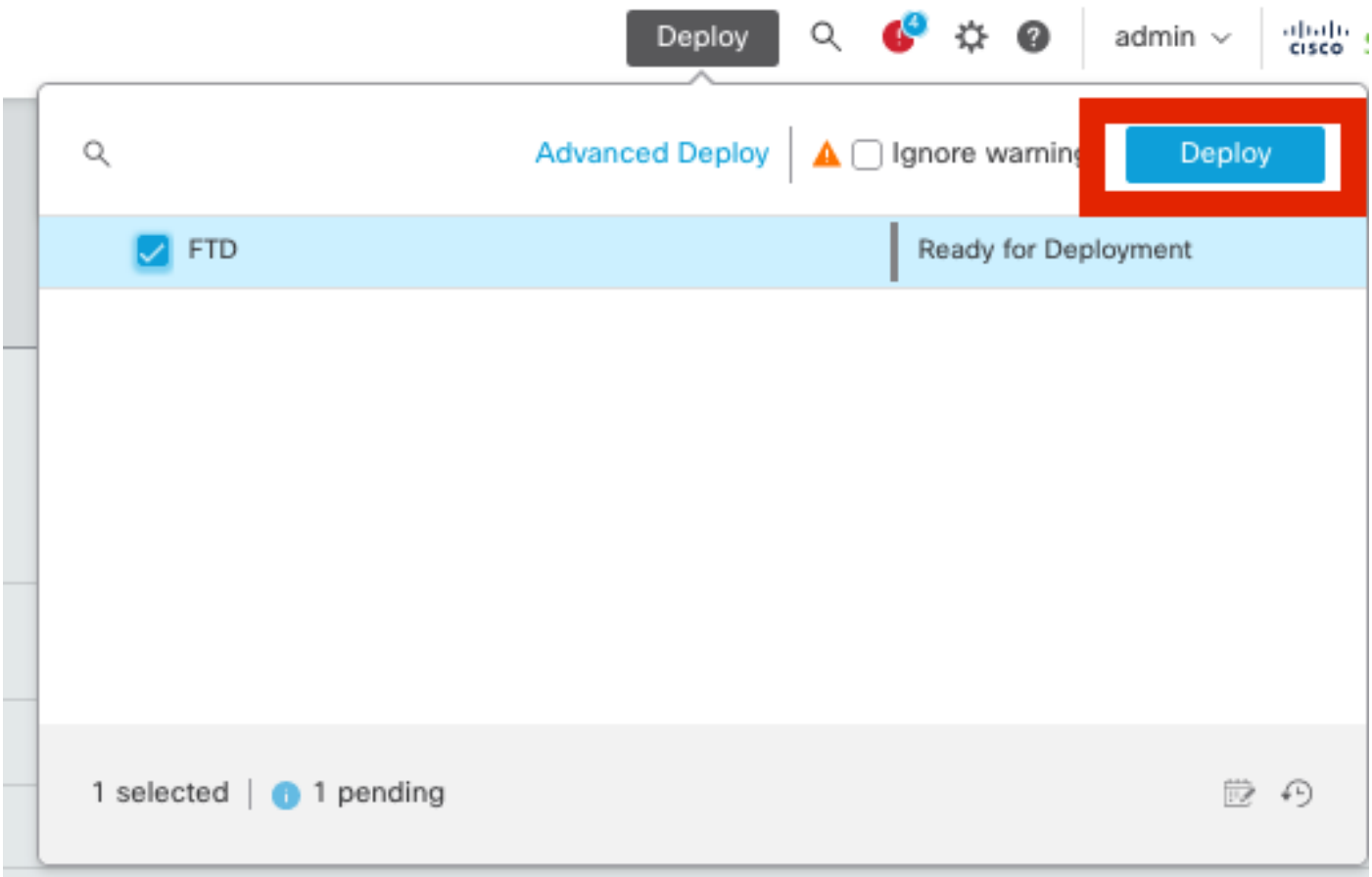
إضافة شبكات *BGP*

الخطوة 5. تكوين جميع إعدادات BGP الأخرى الإختيارية ويمكنك تكوينها طبقا للبيئة الخاصة بك. تحقق من التكوين وانقر Save فوق.



حفظ تكوين *BGP*

الخطوة 6. قم بنشر جميع التكوينات.



النشر

تكوين BGP التخطي على ASA

```
router bgp 1000
bgp log-neighbor-changes
bgp router-id 10.1.1.2
address-family ipv4 unicast
neighbor 169.254.2.1 remote-as 1000
neighbor 169.254.2.1 transport path-mtu-discovery disable
neighbor 169.254.2.1 activate
network 1.1.1.0 mask 255.255.255.0
no auto-summary
```

no synchronization
exit-address-family

التحقق من الصحة

استخدم هذه القسم لتأكيد عمل التكوين بشكل صحيح.

النواتج في إطار برنامج الإرسال فائق السرعة

<#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
```

النواتج المتعلقة بمؤشر الأداء الموحد

<#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
```

استكشاف الأخطاء وإصلاحها

يوفر هذه القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

- يدعم واجهات IPv4 فقط، بالإضافة إلى IPv4 أو الشبكات المحمية أو حمولة الشبكة الخاصة الظاهرية (لا يوجد دعم لـ IPv6).

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).