تكوين شبكة VPN المستندة إلى المسار المستندة إلى VRF على FTD المدارة بواسطة FDM

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين شبكة VPN المستندة إلى المسار من موقع إلى موقع على FTD المدارة بواسطة FDM.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- المفهوم الأساسي للشبكة الخاصة الظاهرية (VPN)
- المفهوم الأساسي للتوجيه الظاهري وإعادة التوجيه (VRF)
- تجربة إدارة fdm

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco FTDv، الإصدار 7.4.2
- Cisco FDM، الإصدار 7.4.2
- Cisco ASAv الإصدار 9.20.3

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.

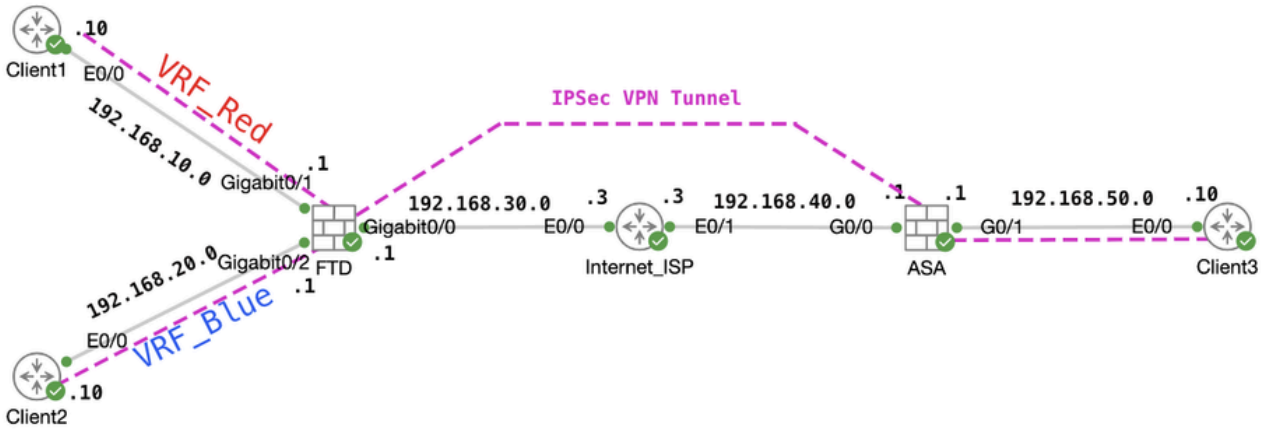
معلومات أساسية

يسمح لك التوجيه وإعادة التوجيه الظاهري (VRF) على FirePOWER Device Manager (FDM) بإنشاء العديد من مثيلات التوجيه المعزولة على جهاز واحد للدفاع عن تهديد الطاقة النارية (FTD). تعمل كل حالة من حالات التردد اللاسلكي (VRF) كموجه افتراضي منفصل مزود بجدول التوجيه الخاص به، مما يتيح إمكانية الفصل المنطقي لحركة مرور الشبكة ويوفر إمكانات محسنة للأمان وإدارة حركة مرور البيانات.

يشرح هذا المستند كيفية تكوين شبكة VPN المدركة لـ VRF باستخدام VTI. توجد شبكة VRF الحمراء وشبكة VRF الزرقاء خلف FTD. قد يتصل العميل1 في الشبكة الحمراء الخاصة بـ VRF والعميل 2 في VRF Blue بالعميل 3 خلف ASA من خلال نفق IPSec VPN.

التكوين

الرسم التخطيطي للشبكة

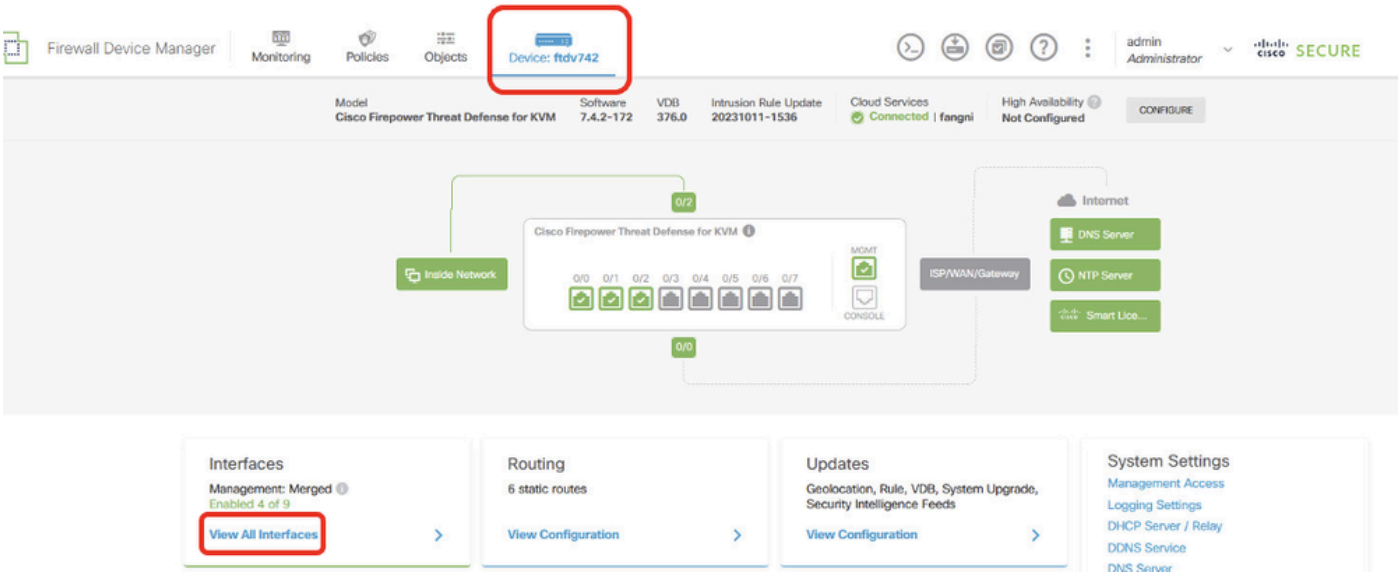


المخطط

تكوين FTD

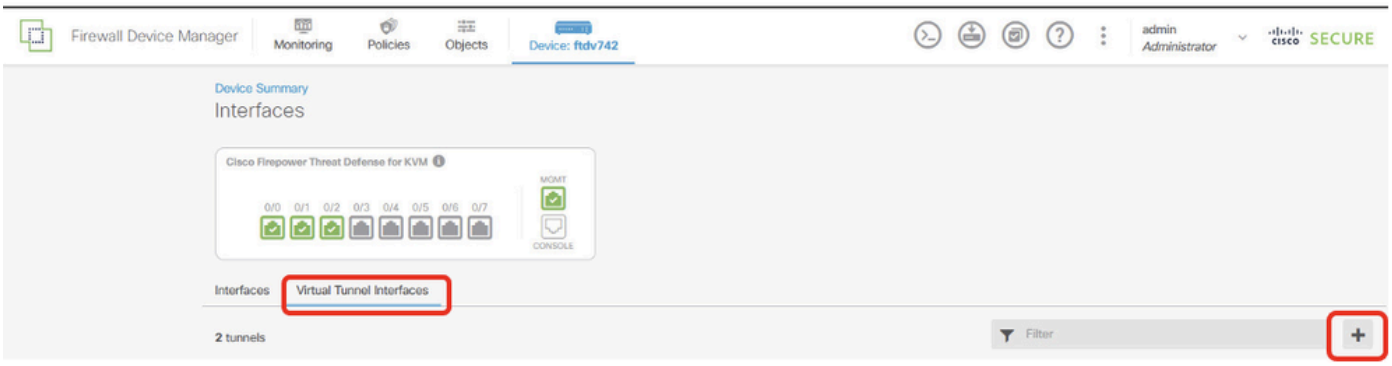
الخطوة 1. من الضروري التأكد من اكتمال التكوين الأولي لاتصال IP بين العقد بشكل صحيح. يكون Client1 و Client2 مع عنوان IP داخلي لـ FTD كبوابة. يكون العميل3 مع ASA داخل عنوان IP كبوابة.

الخطوة 2. قم بإنشاء واجهة النفق الظاهرية. قم بتسجيل دخول واجهة المستخدم الرسومية (GUI) لـ FTD لـ FTD. انتقل إلى الجهاز > الواجهات . انقر على عرض جميع الواجهات .



واجهات FTD_VIEW_INTERFACES

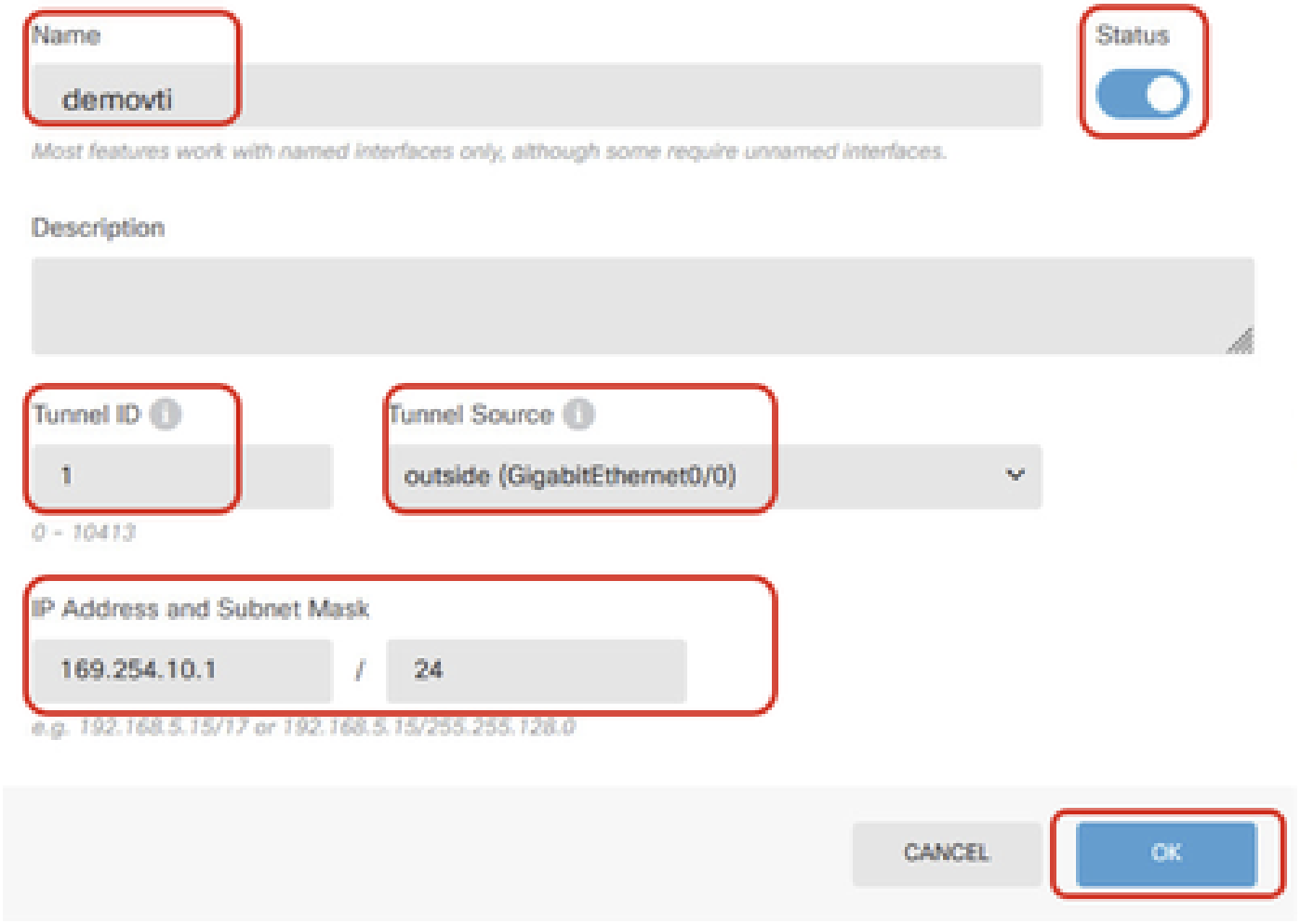
الخطوة 2.1. انقر فوق علامة التبويب واجهات النفق الظاهري. انقر فوق + زر.



FTD_Create_VTI

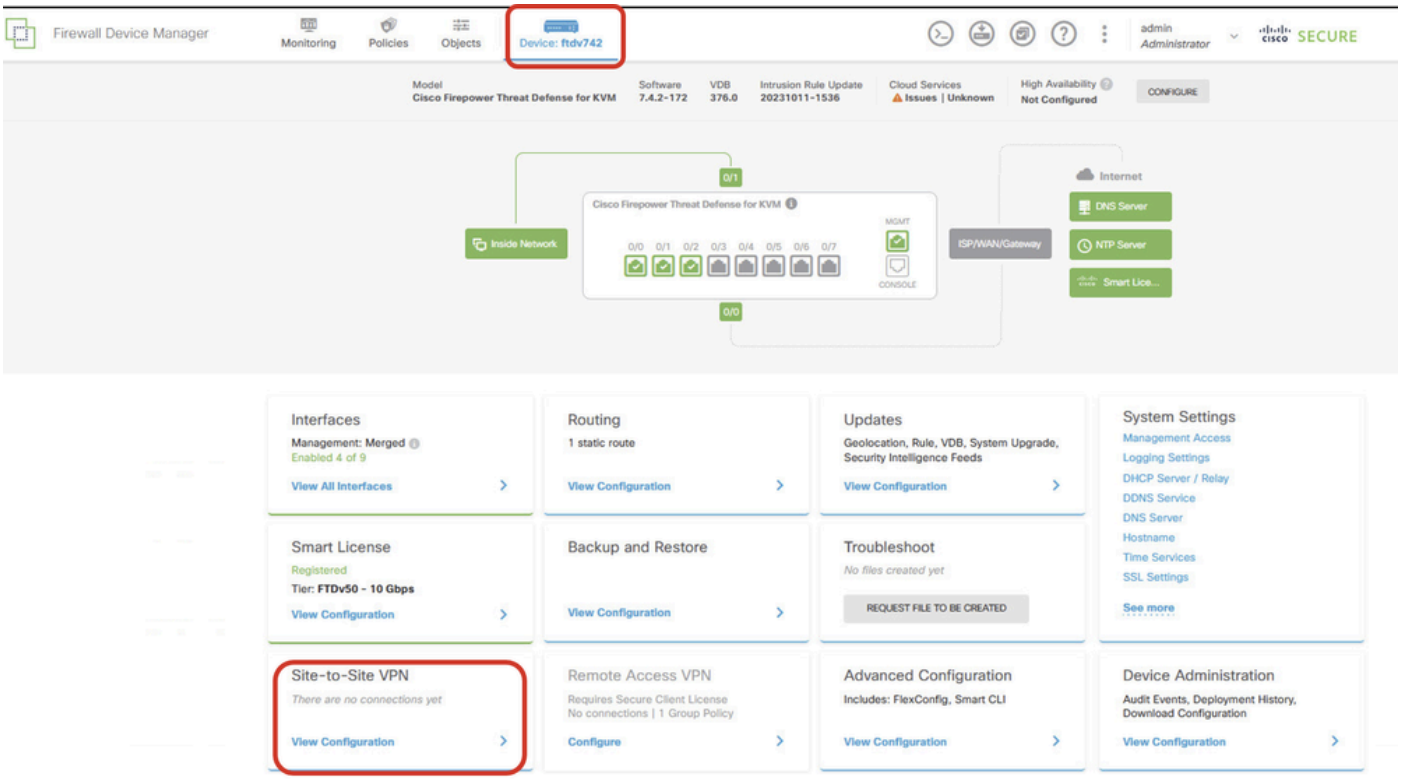
الخطوة 2-2- توفير المعلومات اللازمة. طقطقت ok زر.

- الاسم: ديموفتي
- معرف النفق: 1
- مصدر النفق: خارج (GigabitEthernet0/0)
- عنوان IP وقناع الشبكة الفرعية: 169.254.10.1/24
- الحالة: انقر المنزلق على الموضع المتاح



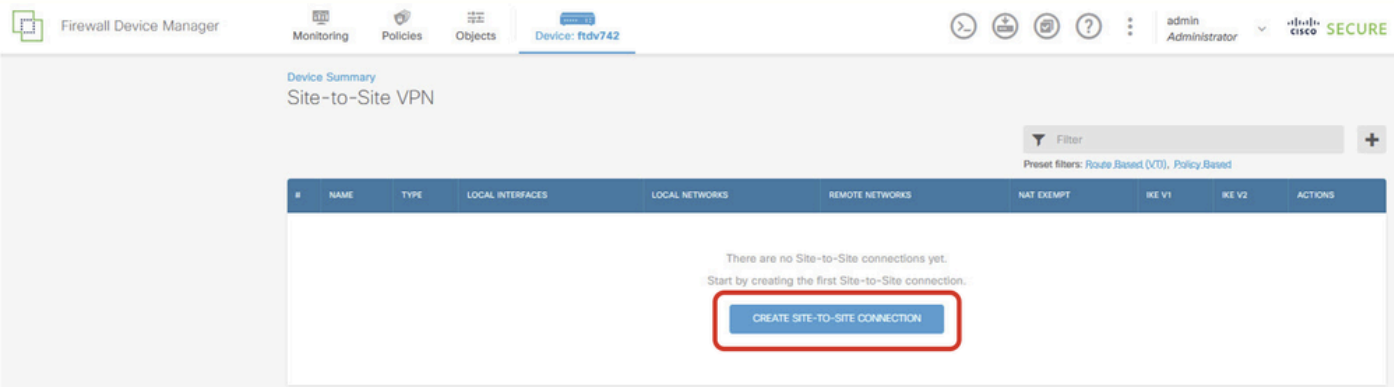
تفاصيل FTD_Create_VTI_Details

الخطوة 3. انتقل إلى جهاز > شبكة VPN من موقع إلى موقع . انقر فوق الزر عرض التكوين.



FTD_SITE-to-SITE_VPN_VIEW_CONFIGURATION

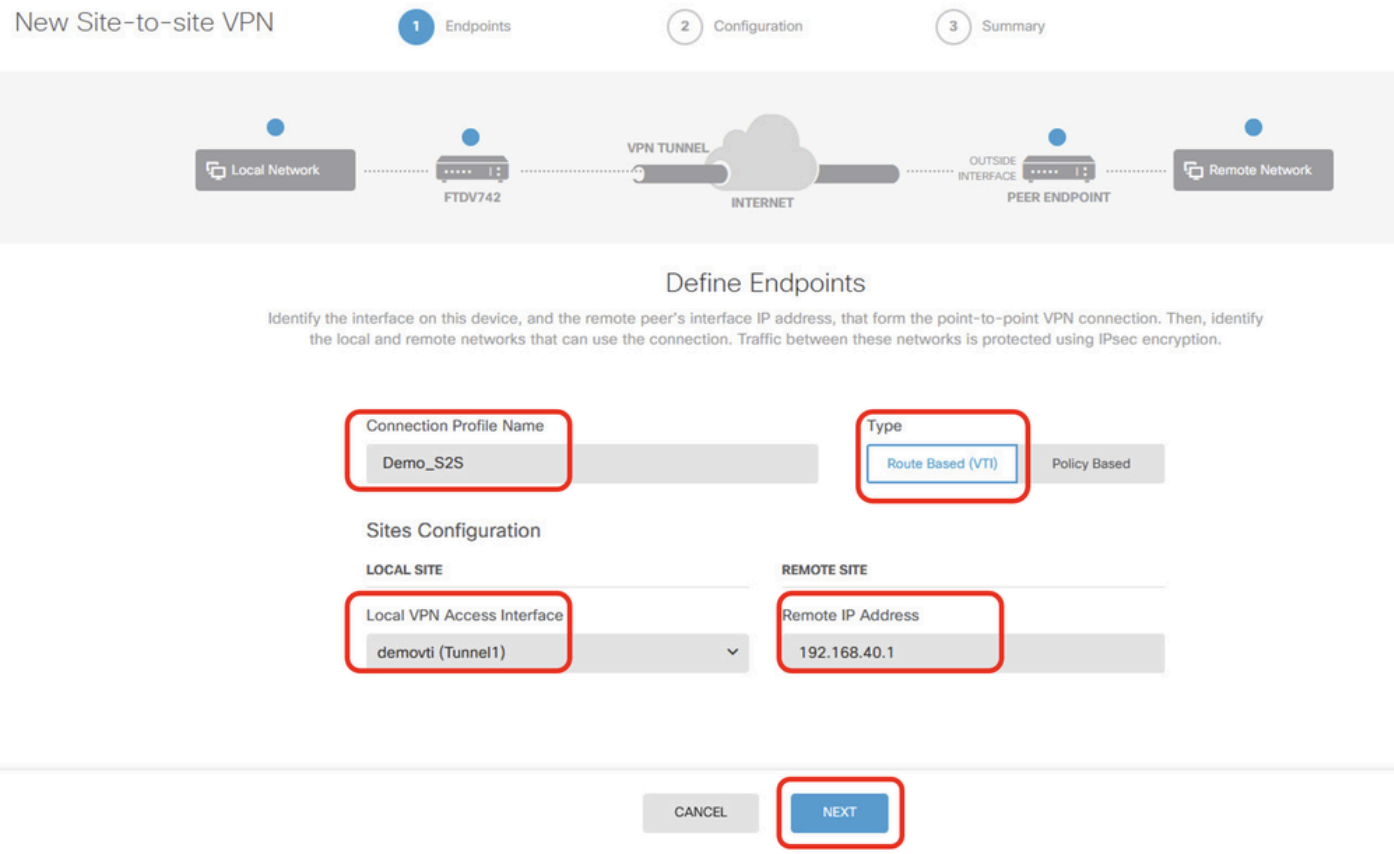
الخطوة 3.1. بدء إنشاء شبكة VPN جديدة من موقع إلى موقع. انقر على زر إنشاء اتصال من موقع إلى موقع. أو انقر فوق + زر.



FTD_CREATE_SITE2SITE_CONNECTION

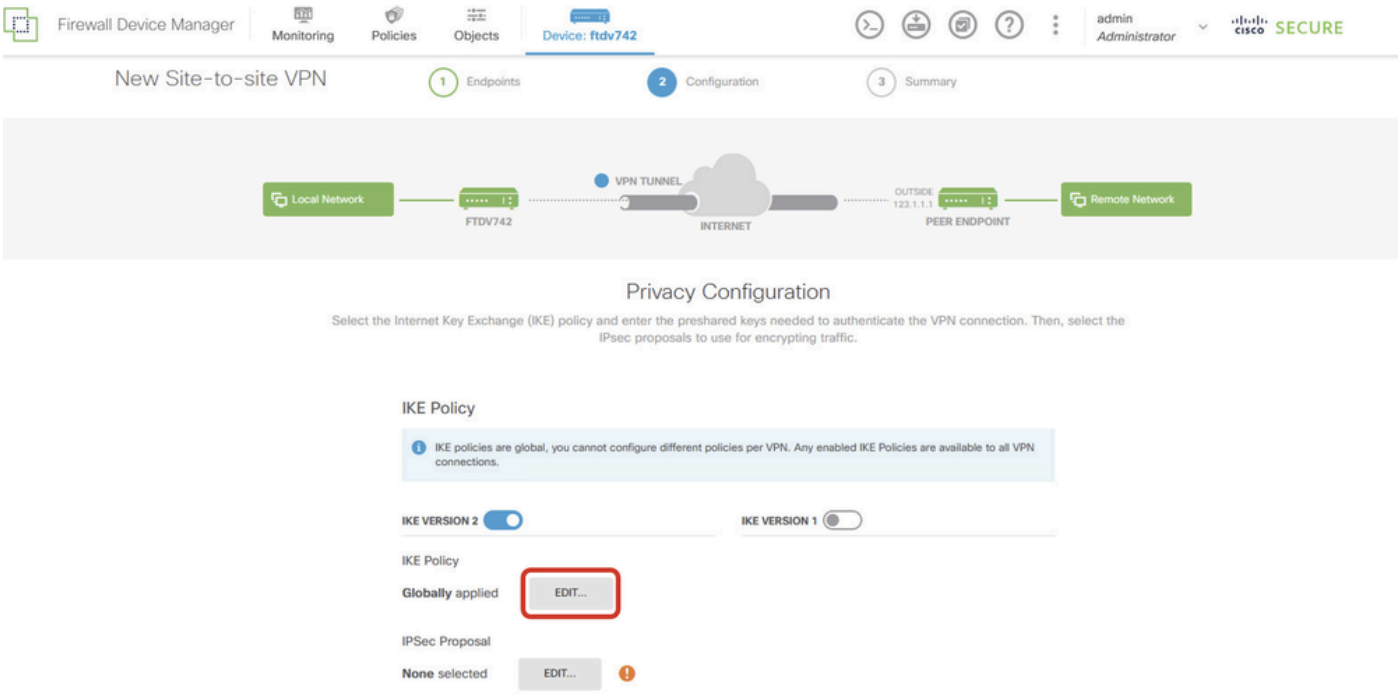
الخطوة 3.2. توفير المعلومات الضرورية. طقطقت بعد ذلك زر.

- اسم ملف تعريف الاتصال: العرض التوضيحي_S2S
- النوع: مستند إلى المسار (VTI)
- واجهة الوصول إلى شبكة VPN المحلية: Demovti (تم إنشاؤها في الخطوة 2)
- عنوان IP البعيد: 192.168.40.1 (هذا هو ASA النظير خارج عنوان IP)



FTD_SITE-to-SITE_VPN_ENDPOINTS

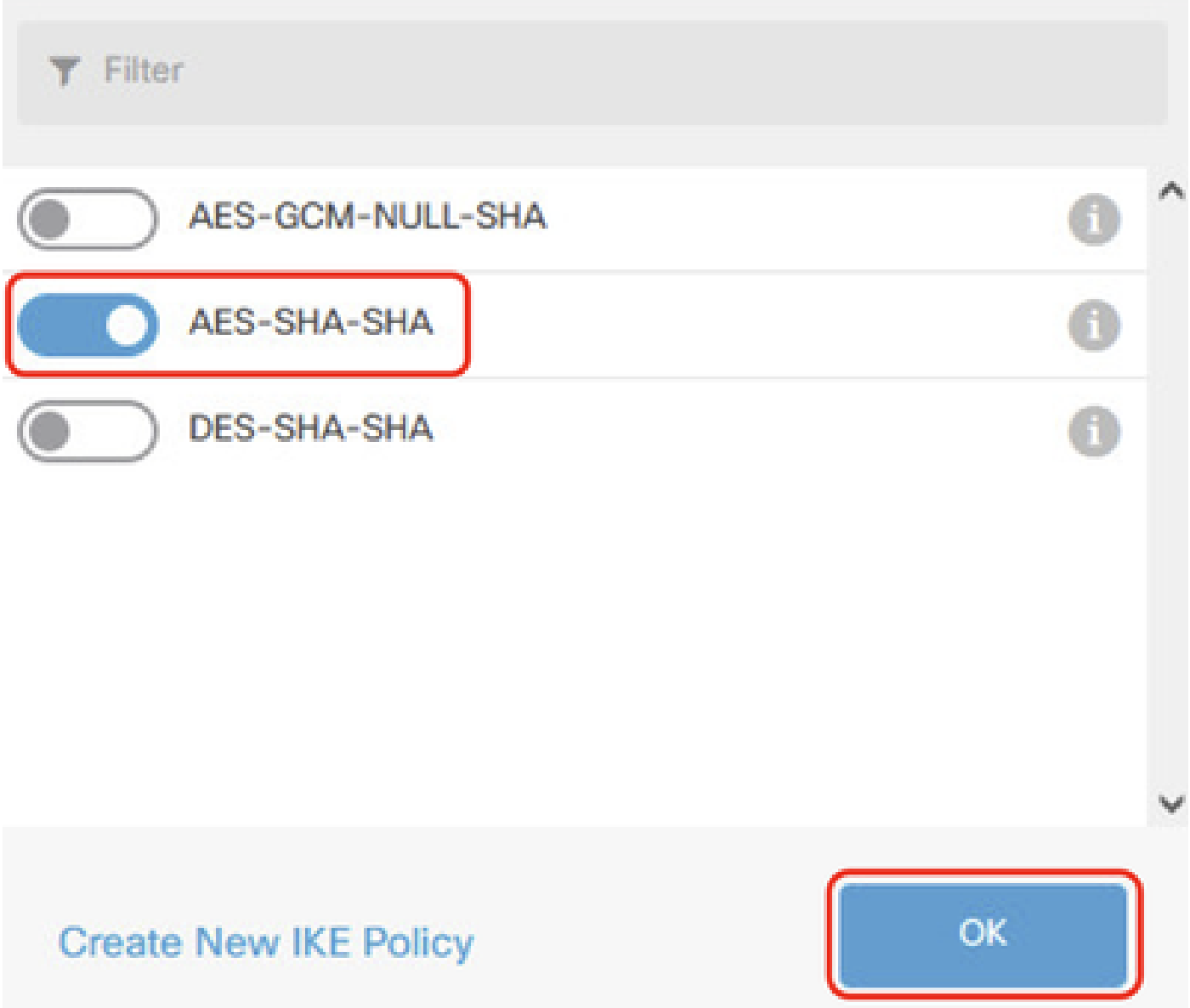
الخطوة 3.3. انتقل إلى سياسة IKE. طقطقة يحرر زر.



FTD_Edit_IKE_Policy

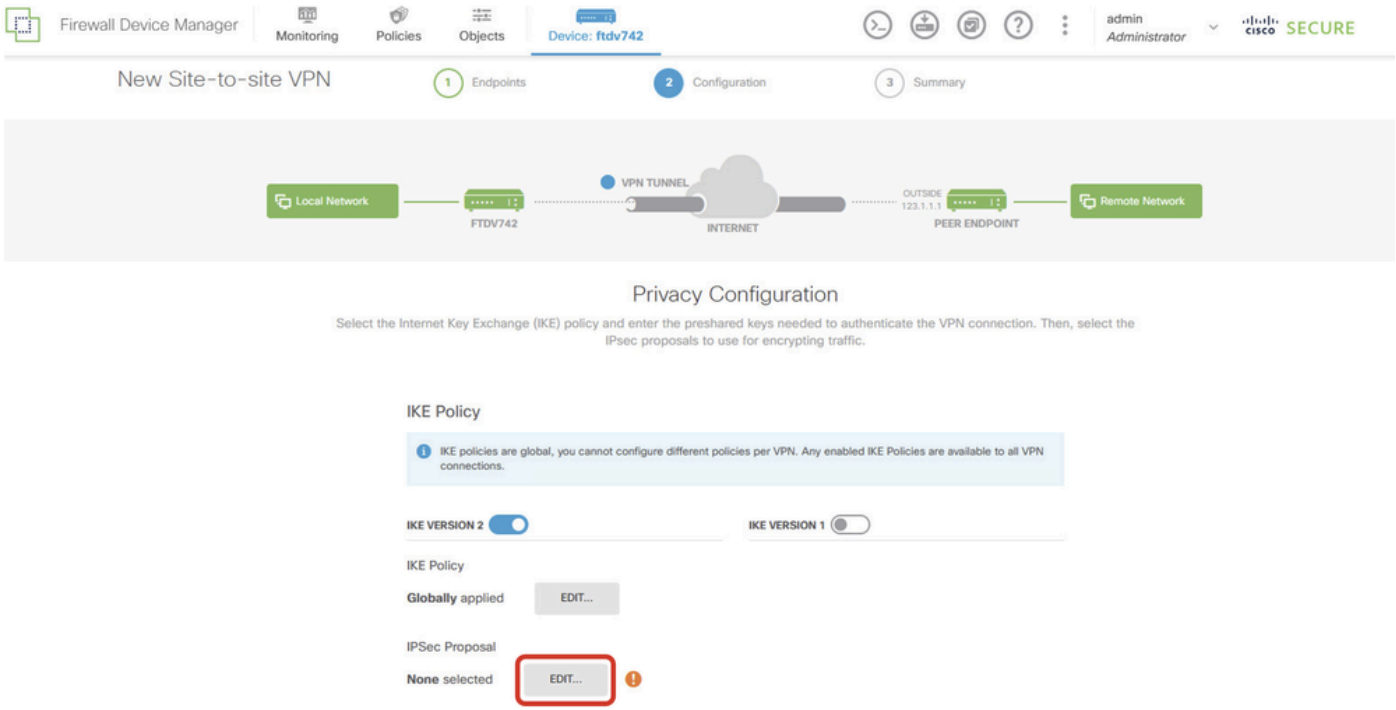
الخطوة 3.4. لنهج IKE، يمكنك إستخدام معرف مسبقا أو يمكنك إنشاء نهج جديد بالنقر فوق إنشاء نهج IKE جديد .

في هذا المثال، تبديل اسم سياسة IKE موجود AES-SHA . انقر فوق الزر موافق للحفظ.



FTD_ENABLE_IKE_POLICY

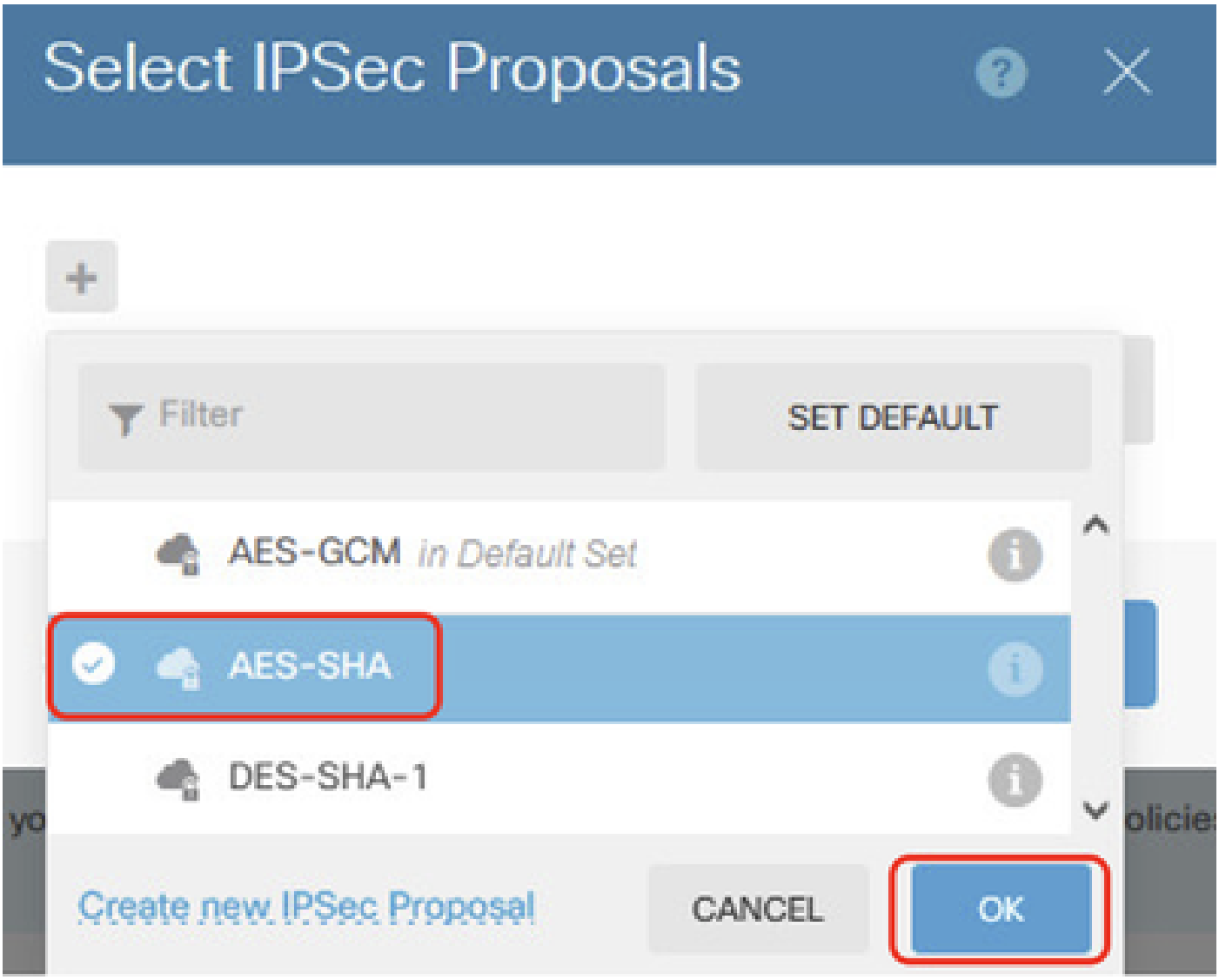
الخطوة 3.5. انتقل إلى اقتراح IPSec. طقطقة يحرر زر.



FTD_Edit_IPSec_Proposal

الخطوة 3.6. بالنسبة لاقتراح IPSec، يمكنك إستخدام مع رف مسبق أو يمكنك إنشاء اقتراح جديد من خلال النقر فوق إنشاء مقترح IPSec جديد .

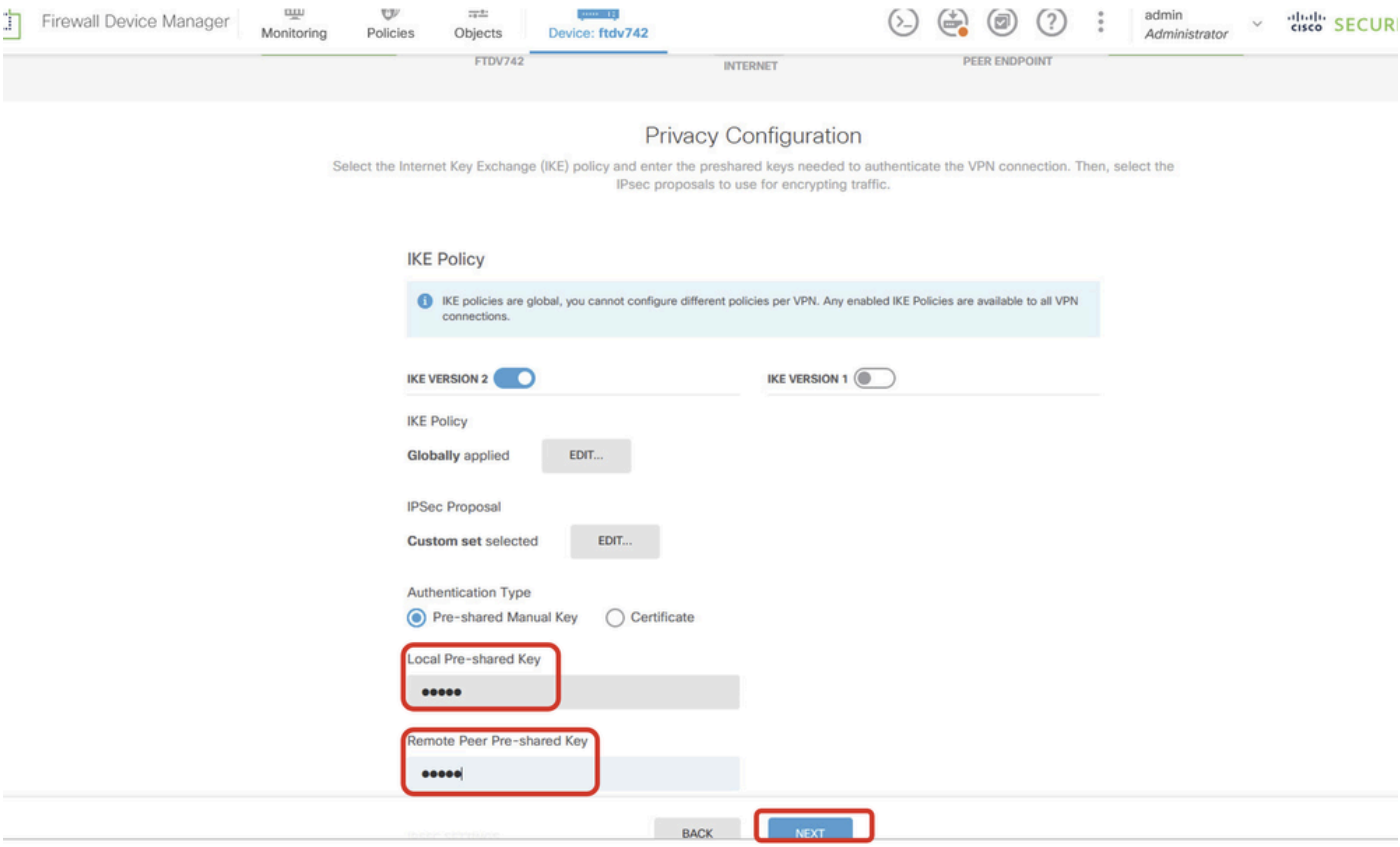
في هذا المثال، بدل اسم اقتراح IPSec الموجود AES-SHA . انقر موافق زر للحفظ.



FTD_ENABLE_IPSec_Proposal

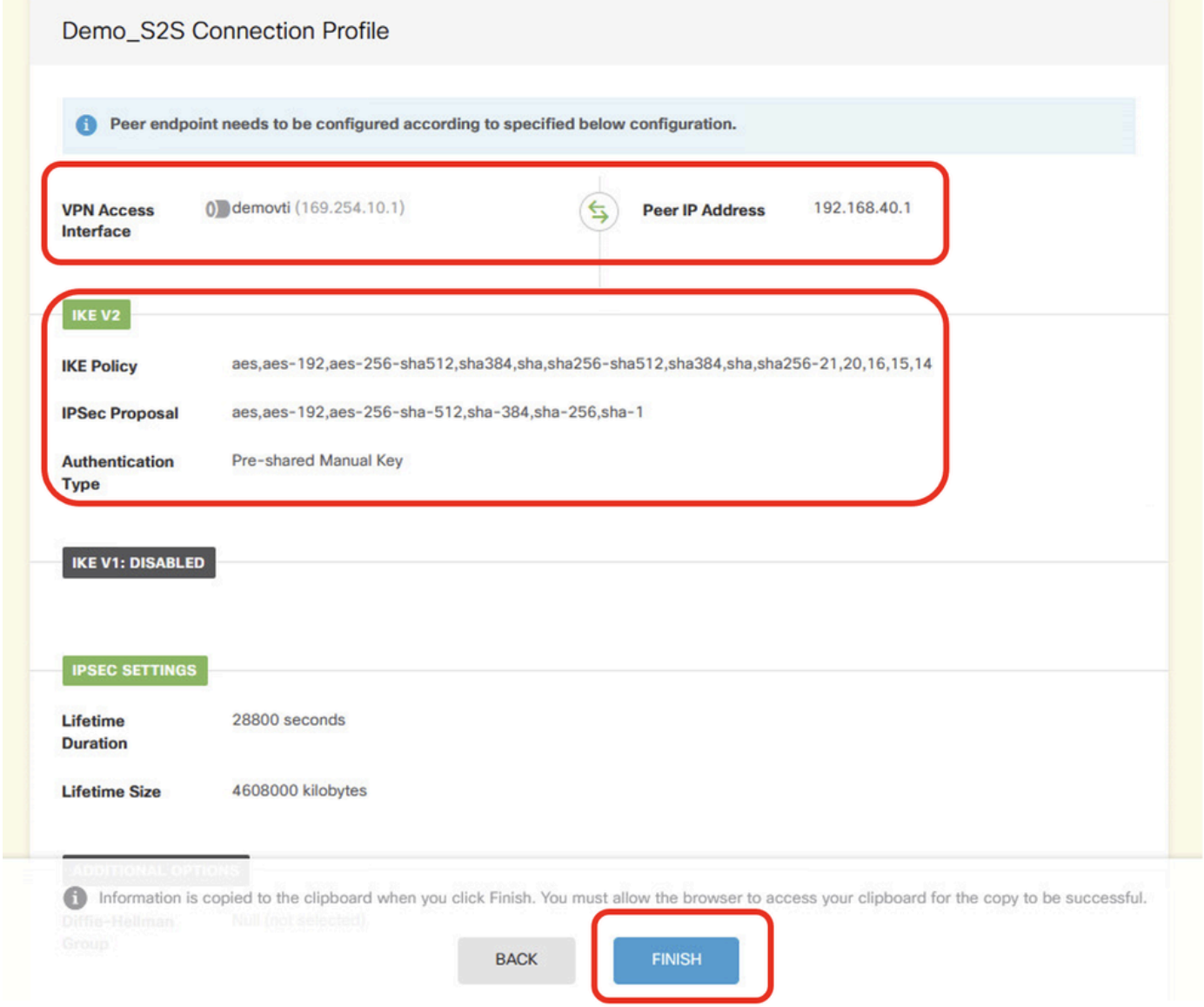
الخطوة 3.7. قم بالتمرير لأسفل الصفحة وتكوين المفتاح المشترك مسبقا. طقطقت بعد ذلك زر.

الرجاء ملاحظة هذا المفتاح المشترك مسبقا وتكوينه على ASA لاحقا.



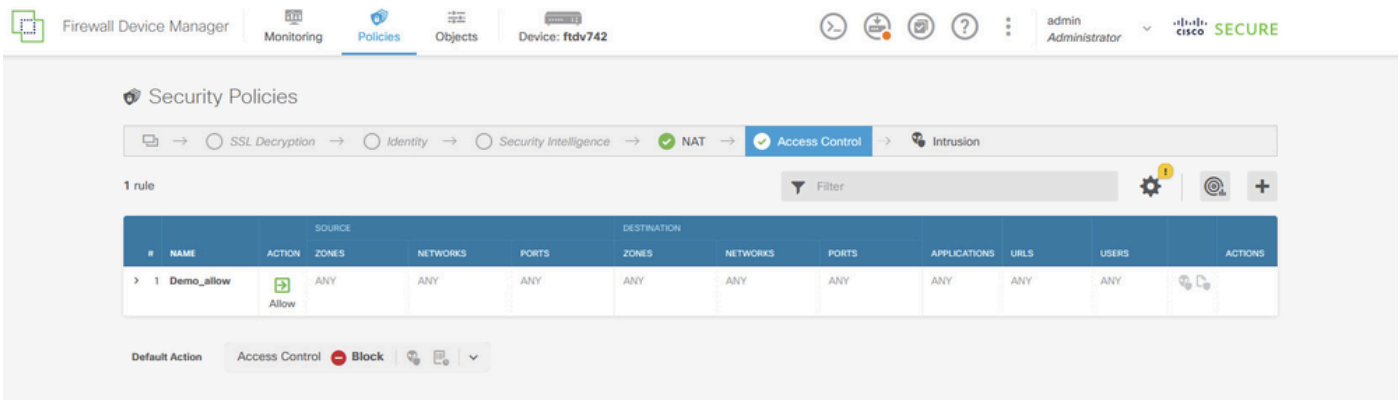
FTD_CONFIGURE_PRE_SHARED_KEY

الخطوة 3.8. راجع تكوين شبكة VPN. إذا كان هناك أي شيء بحاجة إلى التعديل، انقر فوق الزر السابق. إذا كان كل شيء جيدا، انقر فوق إنهاء الزر.



FTD_REVIEW_VPN_CONFIGURATION

الخطوة 3.9. قم بإنشاء قاعدة التحكم في الوصول للسماح لحركة المرور عبر FTD. في هذا المثال، قم بالسماح للجميع بهدف العرض التوضيحي. الرجاء تعديل النهج الخاص بك استنادا إلى إحتياجاتك الفعلية.

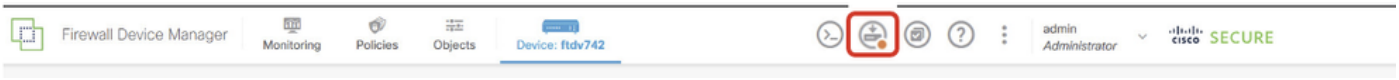


FTD_ACP_Example

الخطوة 3.10. (إختياري) قم بتكوين قاعدة إستثناء NAT لحركة مرور العميل على FTD إذا كان

هناك NAT ديناميكي تم تكوينه للعميل للوصول إلى الإنترنت. في هذا المثال، لا توجد حاجة لتكوين قاعدة إستثناء NAT بسبب عدم تكوين NAT ديناميكي على FTD.

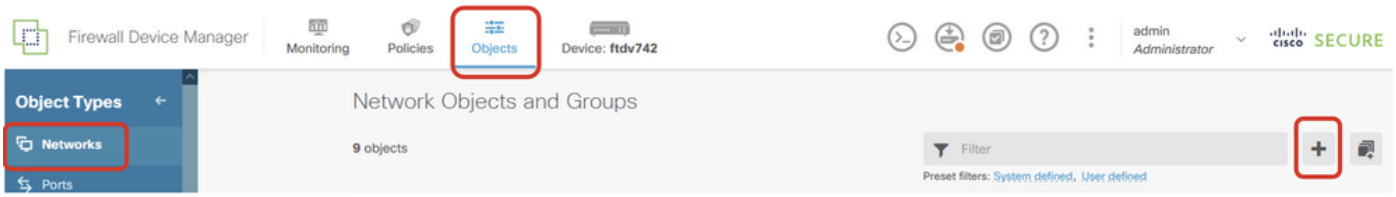
الخطوة 3.11. نشر تغييرات التكوين.



FTD_DEPLOYMENT_CHANGES

الخطوة 4. تكوين الموجهات الظاهرية.

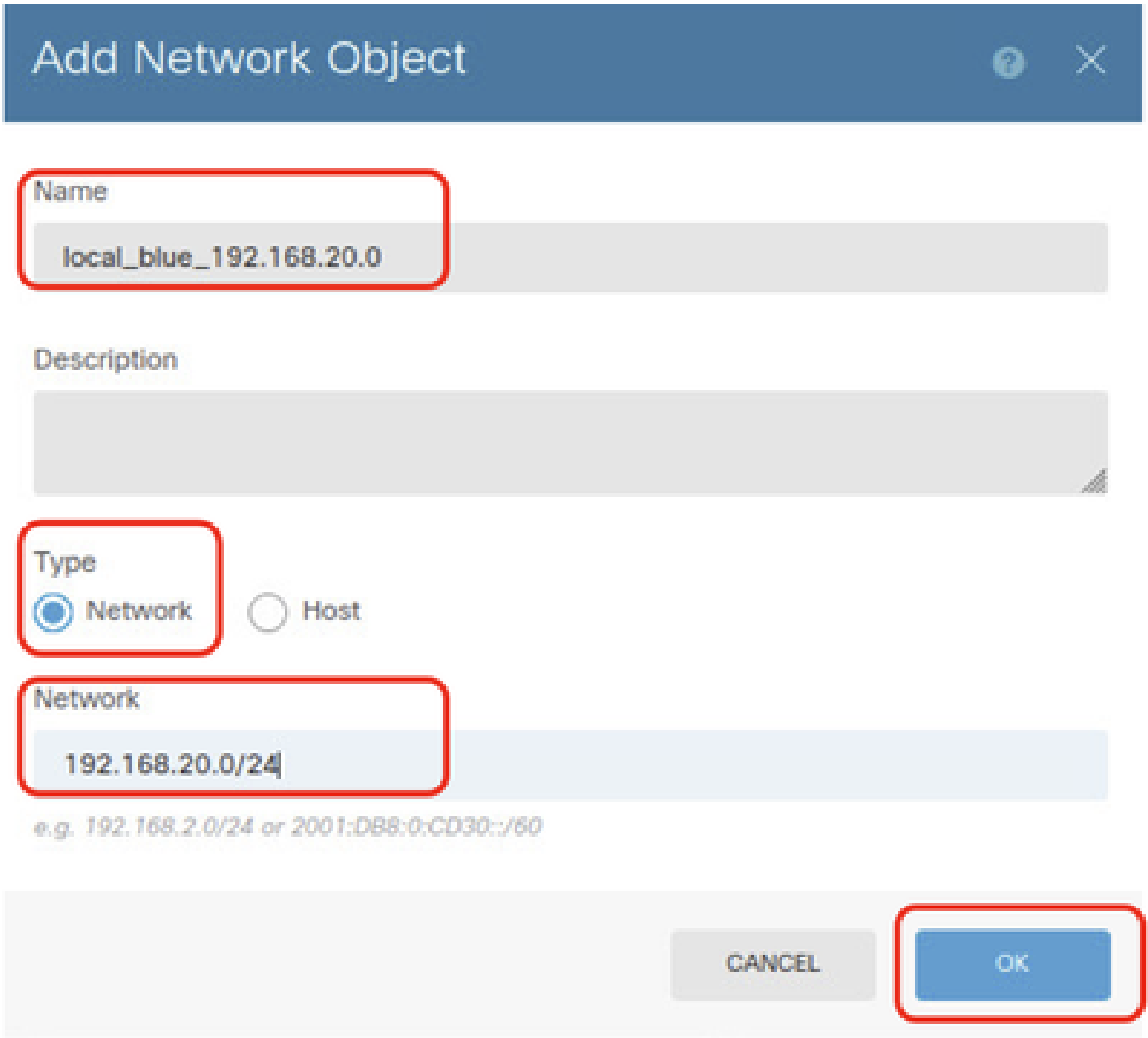
الخطوة 4.1. إنشاء كائنات شبكة للمسار الثابت. انتقل إلى كائنات > شبكات ، انقر فوق + زر.



FTD_Create_NetObjects

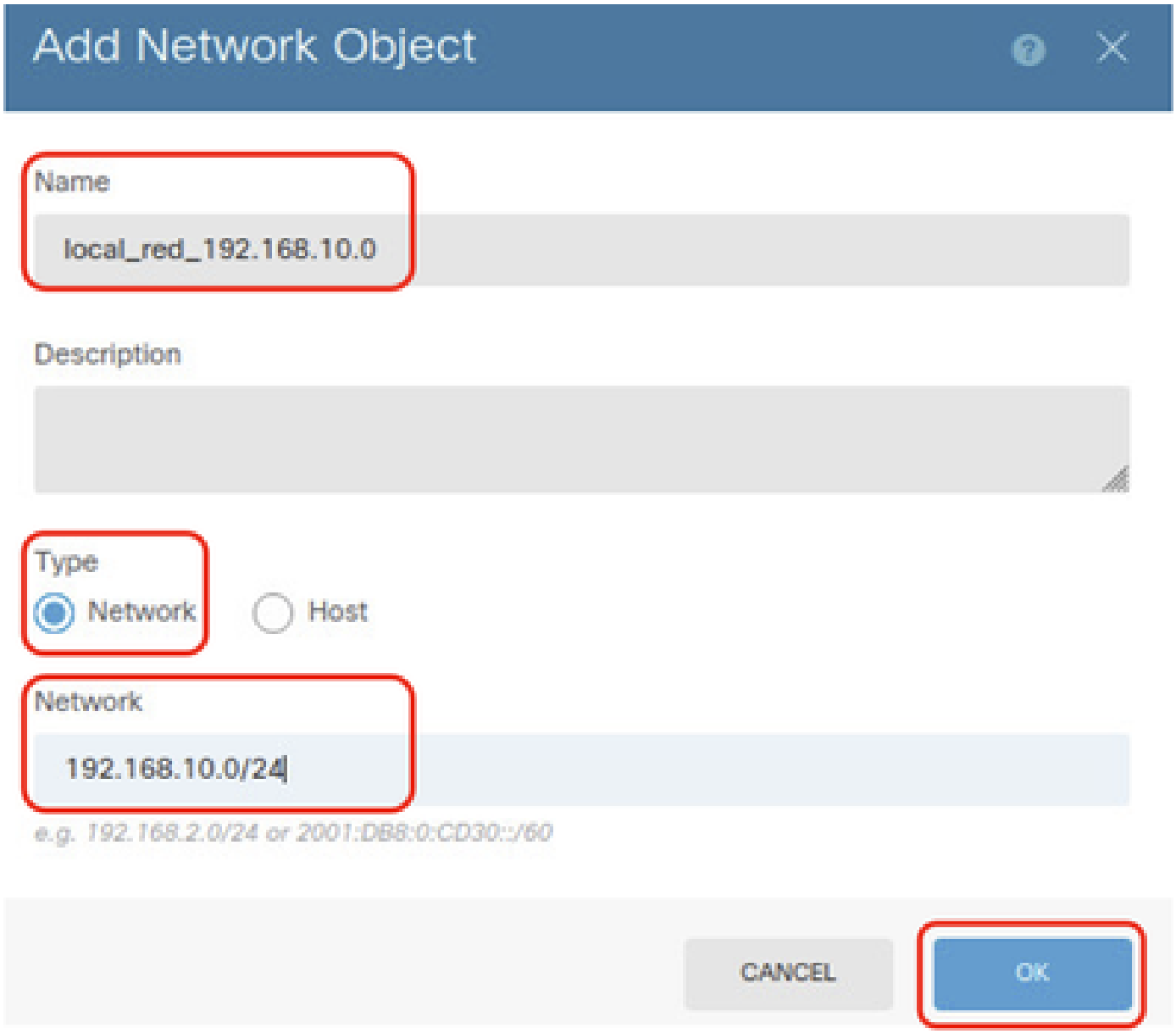
الخطوة 4.2. توفير المعلومات اللازمة لكل كائن شبكة. طقطقت ok زر.

- الاسم: local_blue_192.168.20.0
- النوع: الشبكة
- الشبكة: 192.168.20.0/24



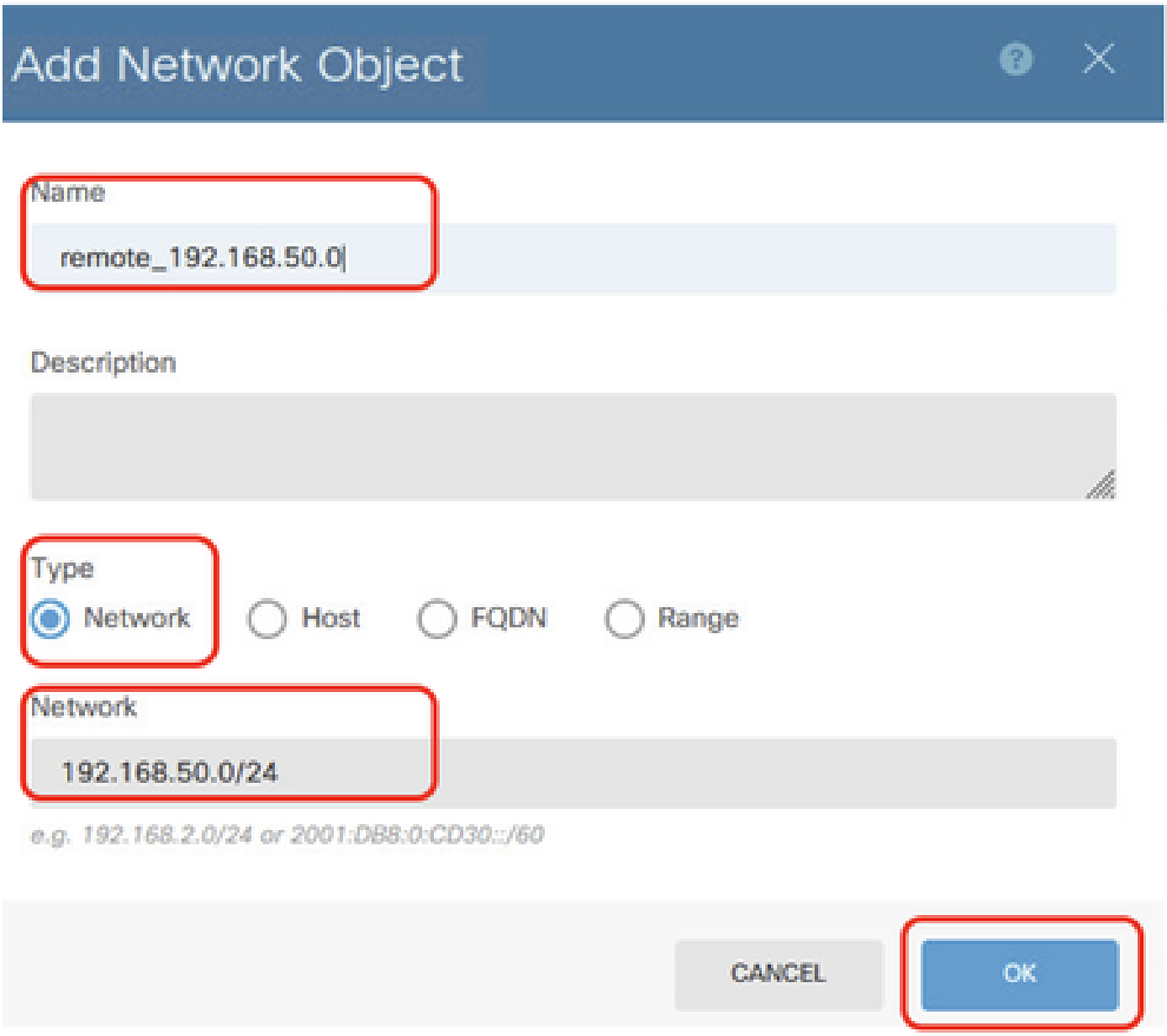
FTD_VRF_BLUE_Network

- الاسم: local_red_192.168.10.0
- النوع: الشبكة
- الشبكة: 192.168.10.0/24



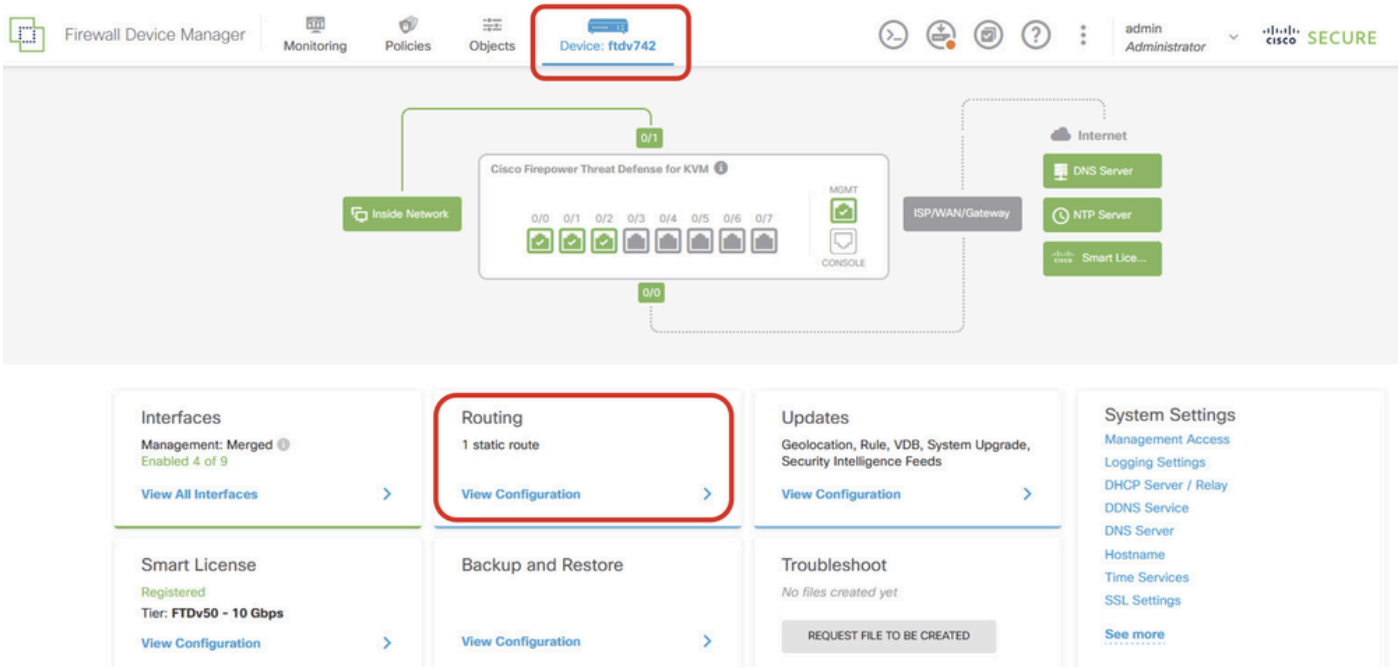
FTD_VRF_RED_Network

- الاسم: remote_192.168.50.0
- النوع: الشبكة
- الشبكة: 192.168.50.0/24



FTD_REMOTE_NETWORK

الخطوة 4.3. إنشاء الموجه الظاهري الأول. انتقل إلى الجهاز > التوجيه . طقطقة عرض تشكيل .



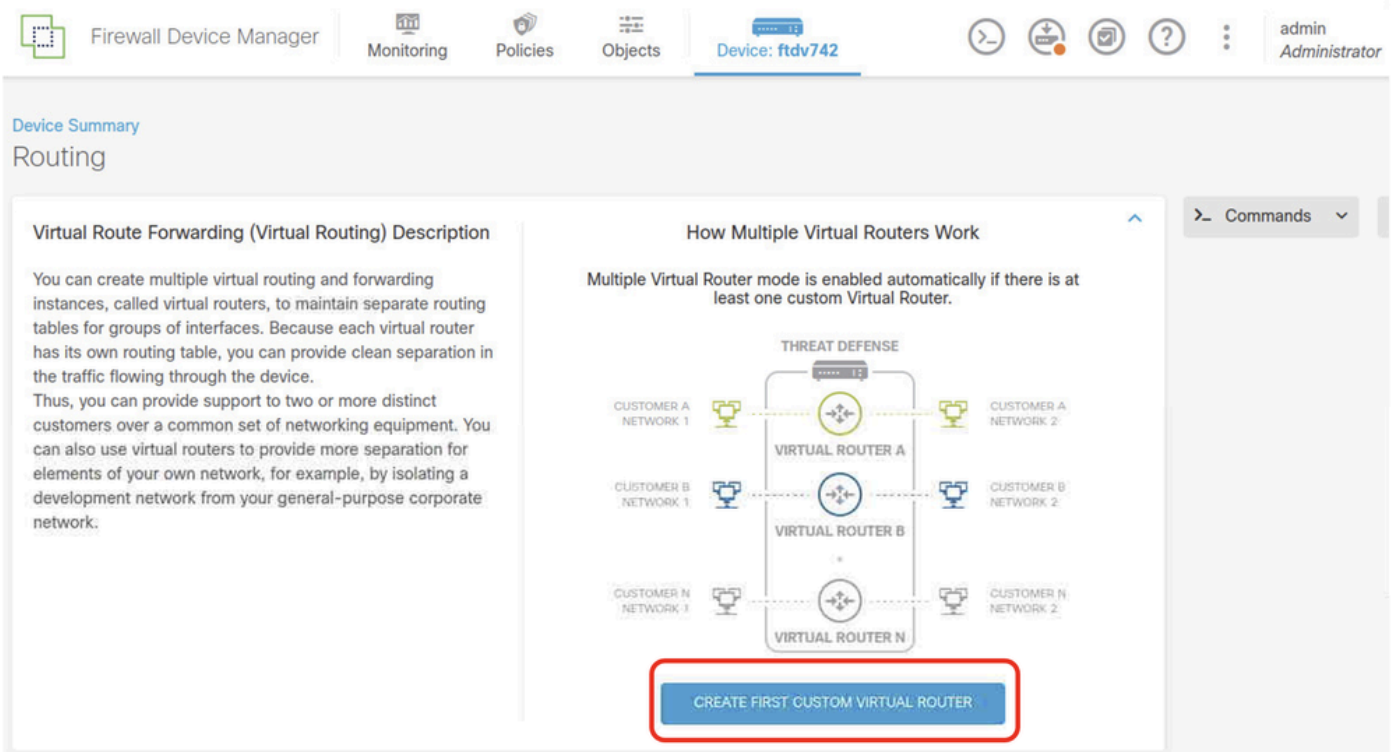
FTD_VIEW_ROUTING_Configuration

الخطوة 4.4. انقر فوق إضافة العديد من الموجهات الظاهرية .

ملاحظة: تم تكوين مسار ثابت من خلال الواجهة الخارجية أثناء تهيئة FDM. إذا لم تكن لديك، فيرجى تكوينها يدويا.

FTD_ADD_FIRST_VIRTUAL_ROUTER1

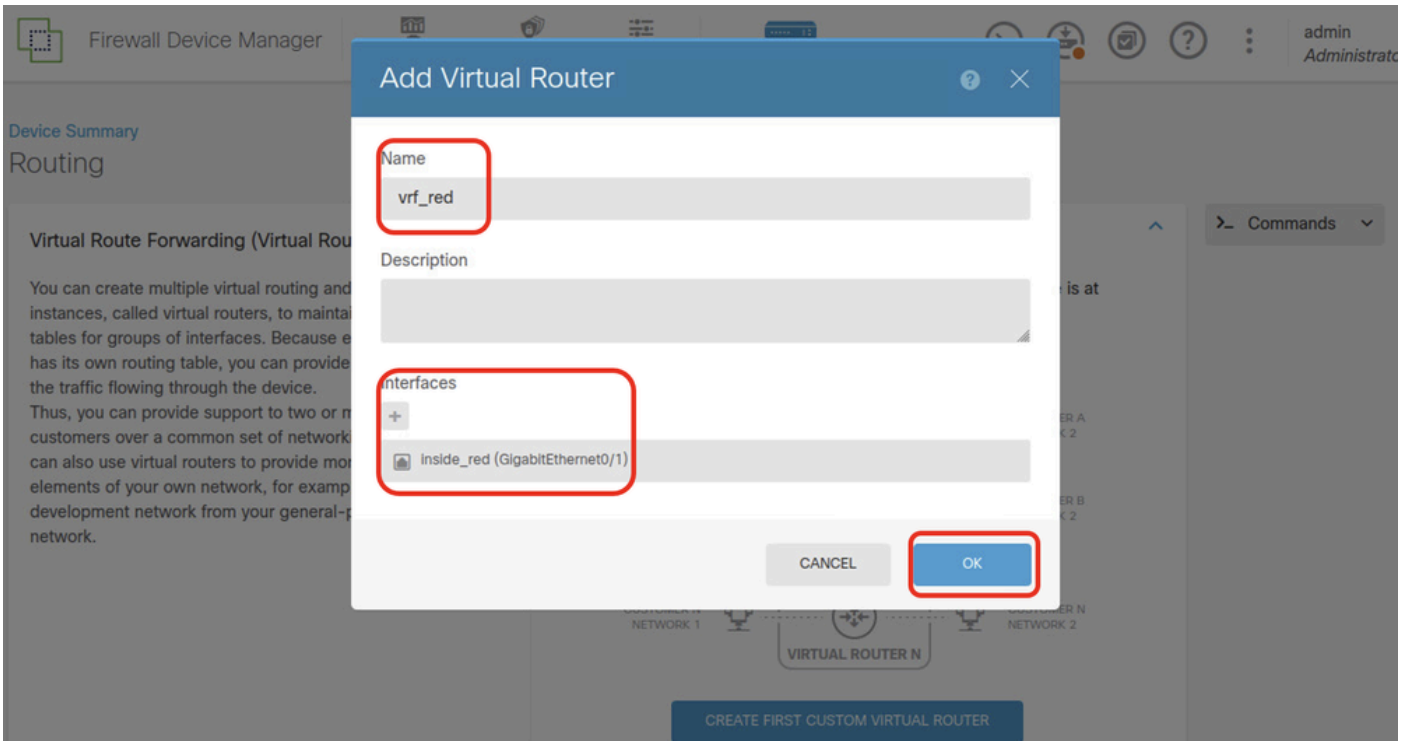
الخطوة 4.5. انقر فوق إنشاء الموجه الظاهري المخصص الأول .



FTD_ADD_FIRST_VIRTUAL_ROUTER2

الخطوة 4.6. توفير المعلومات اللازمة للموجه الظاهري الأول. طقطقة ok زر. بعد إنشاء الموجه الظاهري الأول، سيتم عرض اسم عام ل VRF تلقائيا.

- الاسم: vrf_red
- الواجهات: inside_red (GigabitEthernet0/1)



FTD_ADD_FIRST_VIRTUAL_ROUTER3

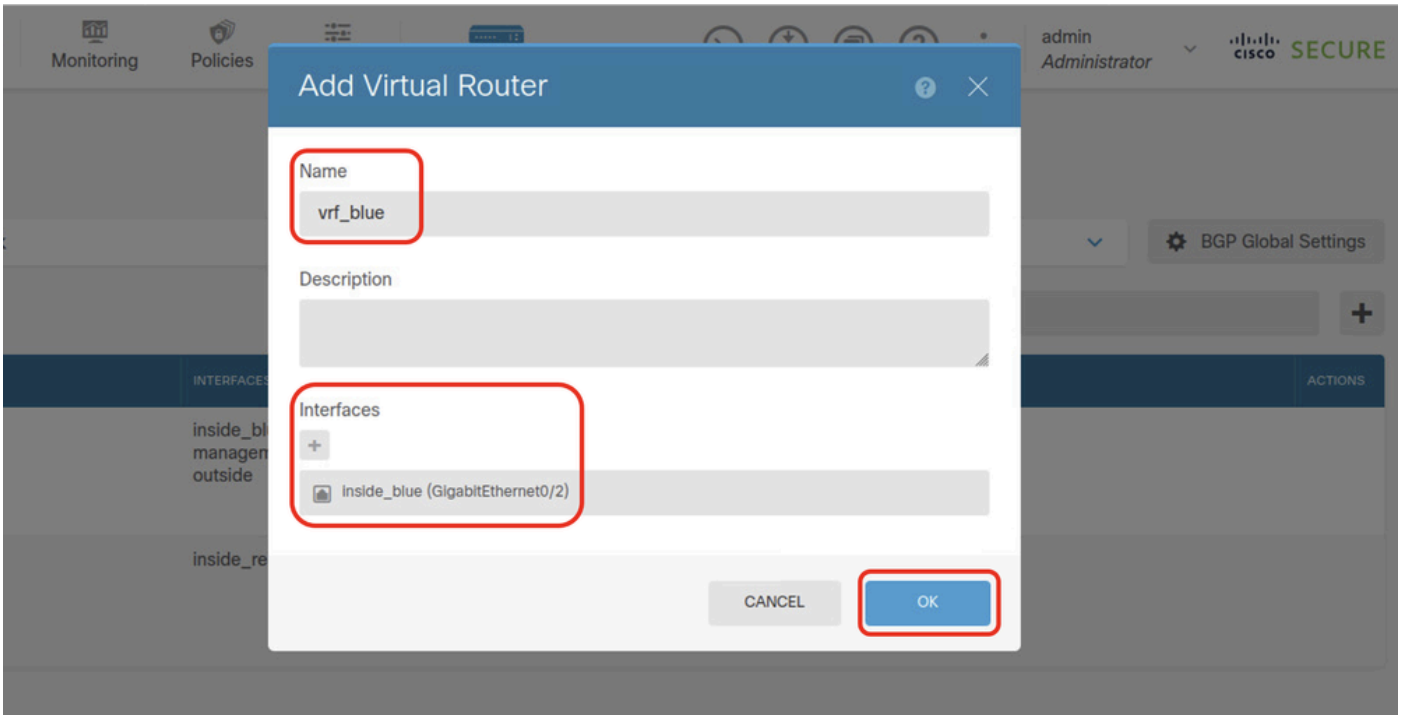
الخطوة 4.7. قم بإنشاء موجه ظاهري ثان. انتقل إلى الجهاز > التوجيه . طقطقة عرض تشكيل

. انقر فوق + زر.

الموجه FTD_Add_Second_Virtual_Router

الخطوة 4.8. قم بتوفير المعلومات اللازمة للموجه الظاهري الثاني. انقر فوق موافق

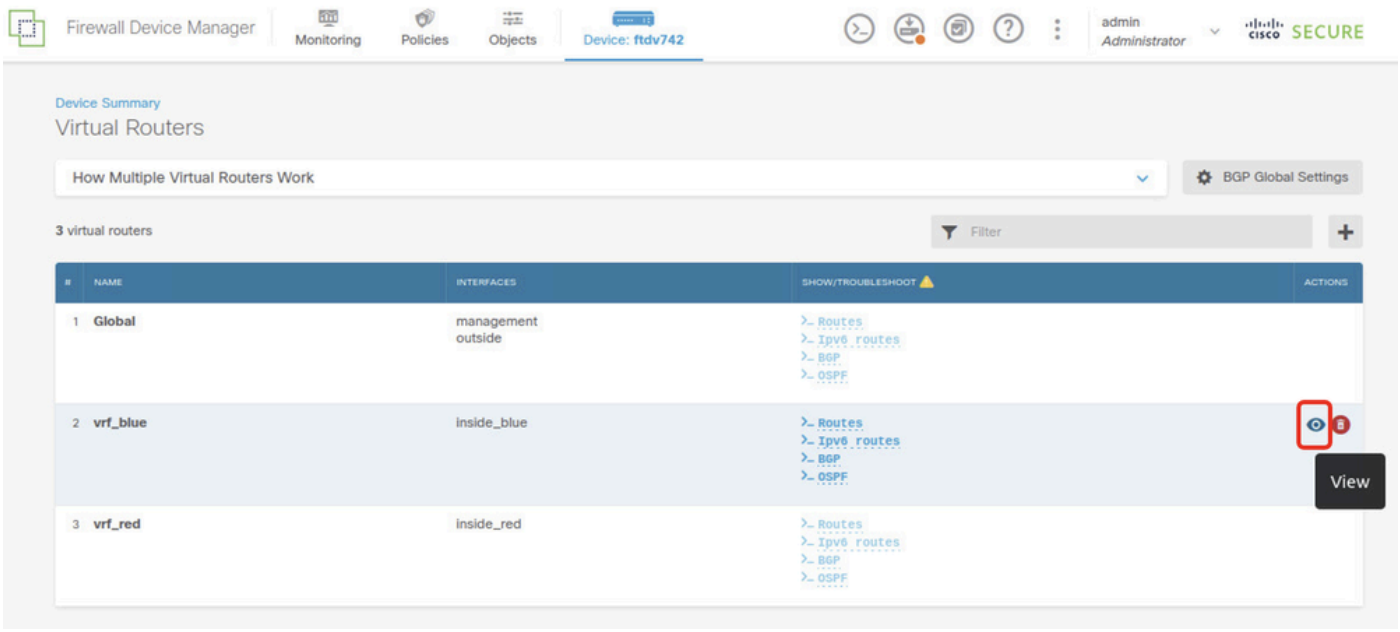
- الاسم: vrf_blue
- الواجهات: inside_blue (GigabitEthernet0/2)



FTD_ADD_SECOND_VIRTUAL_ROUTER2

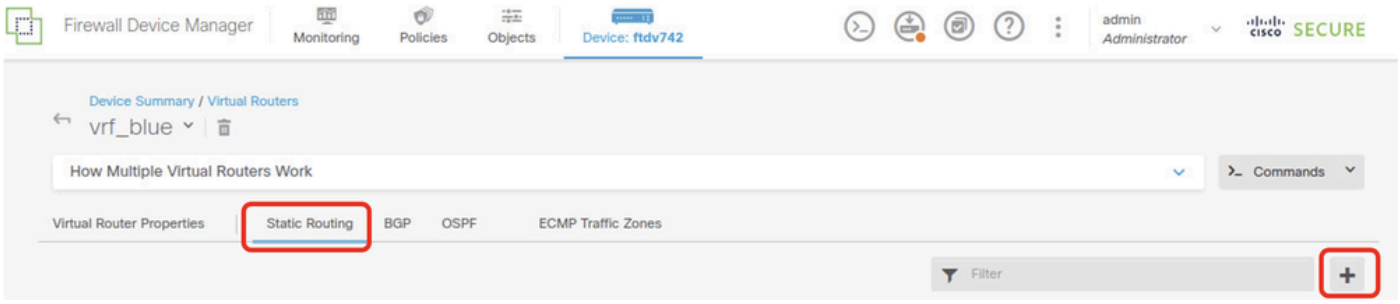
الخطوة 5. أنشئ تسريب المسار من VRF_Blue إلى Global. يتيح هذا المسار لنقاط النهاية على الشبكة 192.168.20.0/24 بدء الاتصالات التي من شأنها إجتياز نفق VPN من موقع إلى موقع. على سبيل المثال، تقوم نقطة النهاية البعيدة بحماية شبكة 192.168.50.0/24.

انتقل إلى الجهاز > التوجيه . انقر فوق عرض التكوين . انقر فوق رمز العرض في خلية الإجراء للموجه الظاهري vrf_blue.



FTD_VIEW_VRF_BLUE

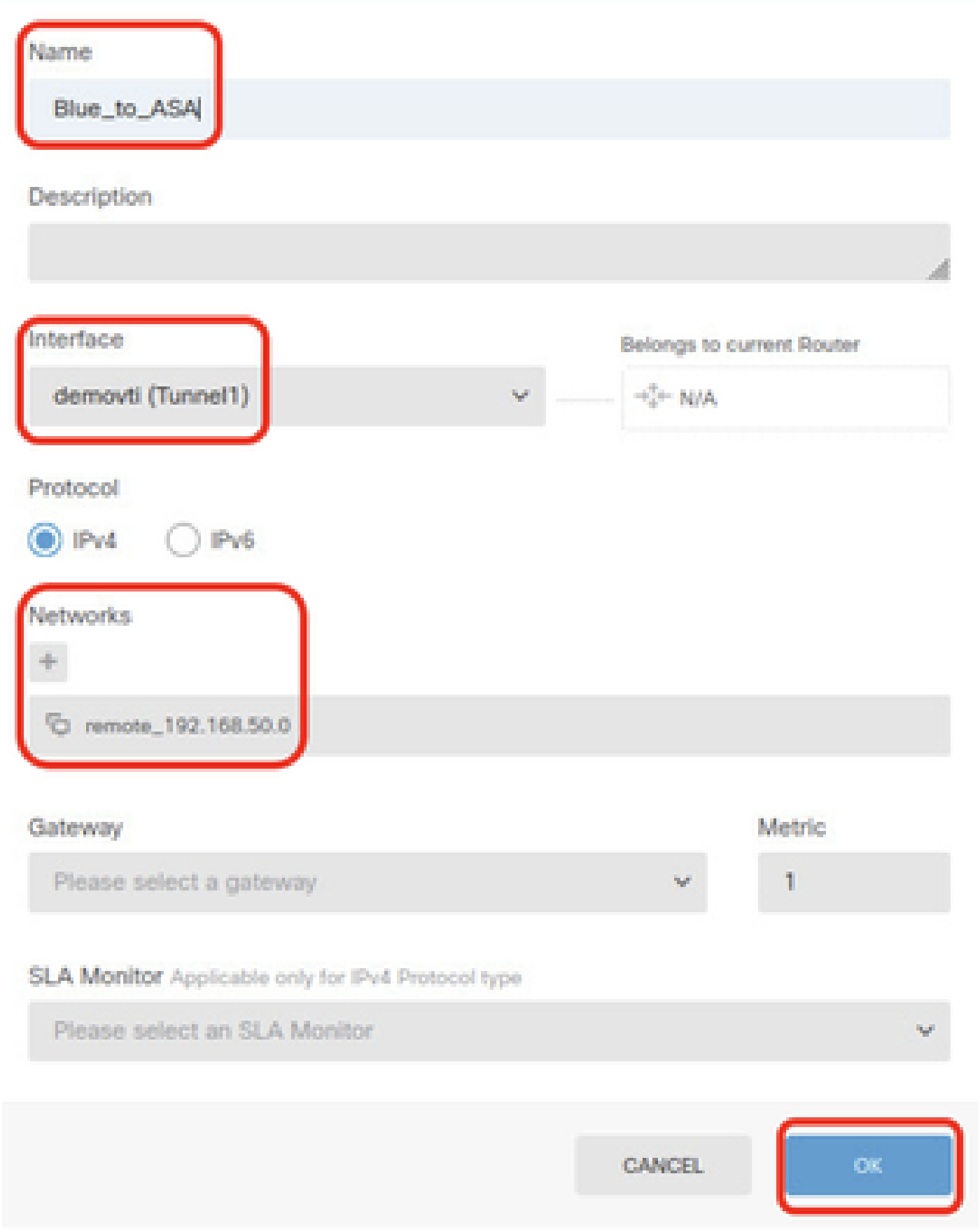
الخطوة 5.1. انقر فوق علامة التبويب توجيه ثابت. انقر فوق + زر.



FTD_Create_STATIC_ROUTE_VRF_BLUE

الخطوة 5.2. قم بتوفير المعلومات اللازمة. طقطقة ok زر.

- الاسم: Blue_to_ASA
- الواجهة: Demovti (النفق 1)
- الشبكات: remote_192.168.50.0
- البوابة: أترك هذا العنصر فارغا.

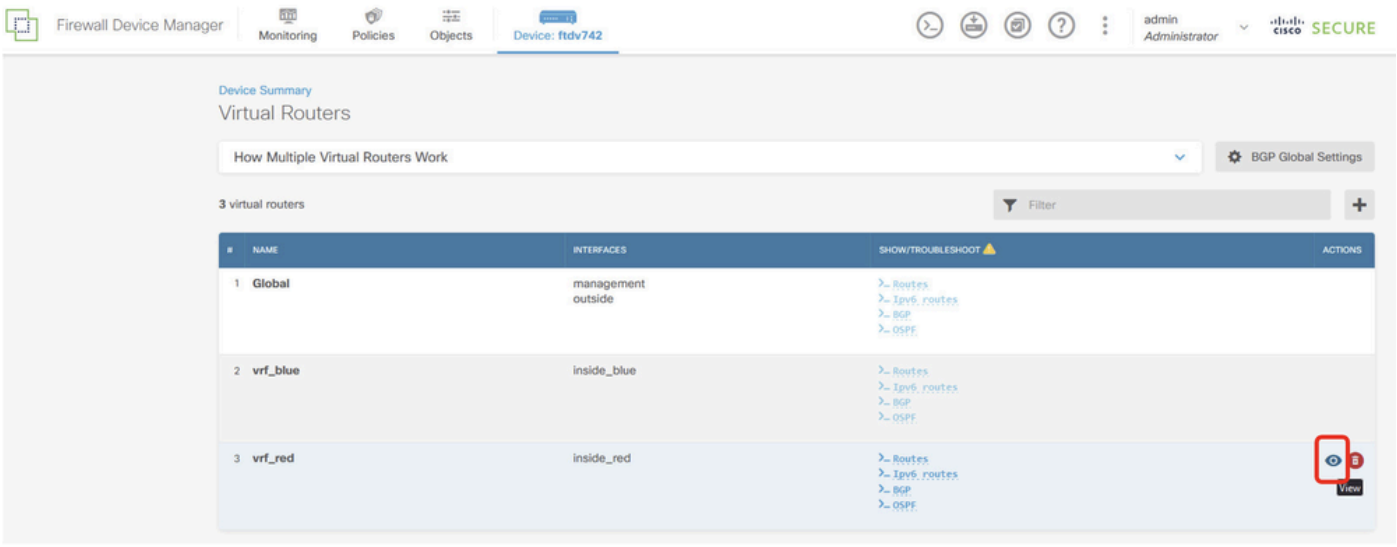


تفاصيل FTD_Create_STATIC_ROUTE_VRF_BLUE_Details

الخطوة 6. أنشئ تسريب المسار من VRF_RED إلى Global. يتيح هذا المسار لنقاط النهاية عبر الاتصالات التي من شأنها إجتياز نفق VPN من موقع إلى 192.168.10.0/24 على الشبكة

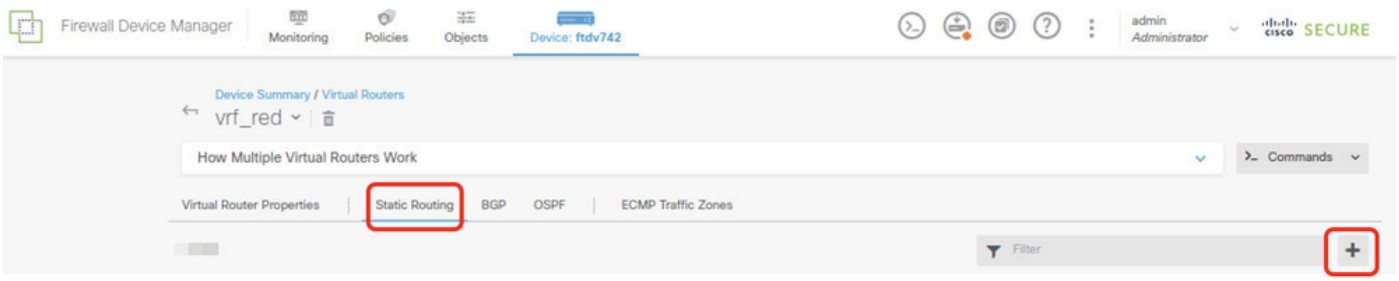
موقع. على سبيل المثال، توقوم نقطة النهاية البعيدة بحماية شبكة 192.168.50.0/24.

انتقل إلى الجهاز > التوجيه . انقر فوق عرض التكوين . انقر فوق رمز العرض في خلية الإجراءات للموجه الظاهري vrf_red.



FTD_VIEW_VRF_RED

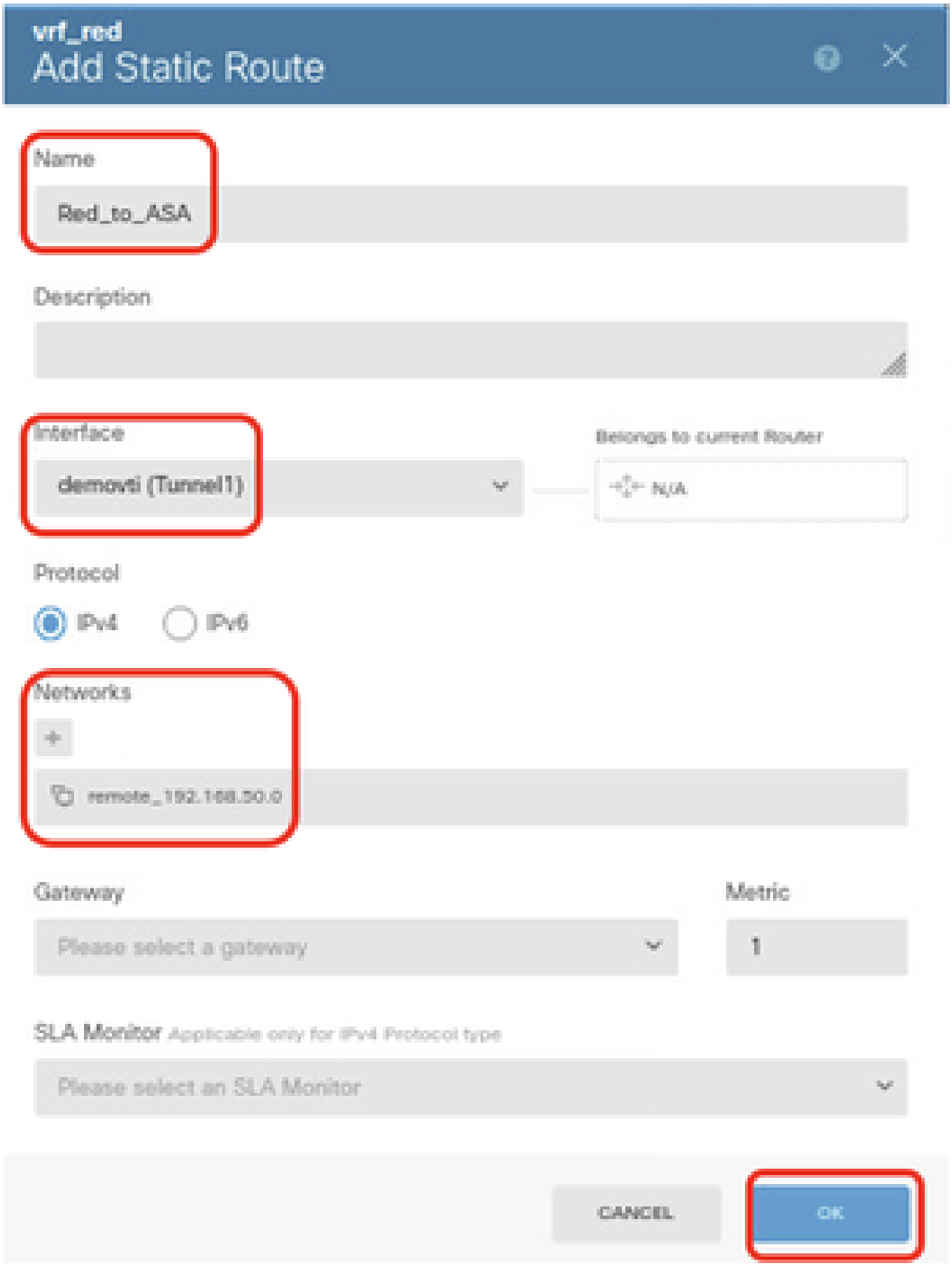
الخطوة 6.1. انقر فوق علامة التبويب توجيه ثابت. انقر فوق + زر.



FTD_Create_STATIC_ROUTE_VRF_RED

الخطوة 6-2. توفير المعلومات اللازمة. طقطقة ok زر.

- الاسم: Red_to_ASA
- الواجهة: Demovti (النفق 1)
- الشبكات: remote_192.168.50.0
- البوابة: أترك هذا العنصر فارغا.

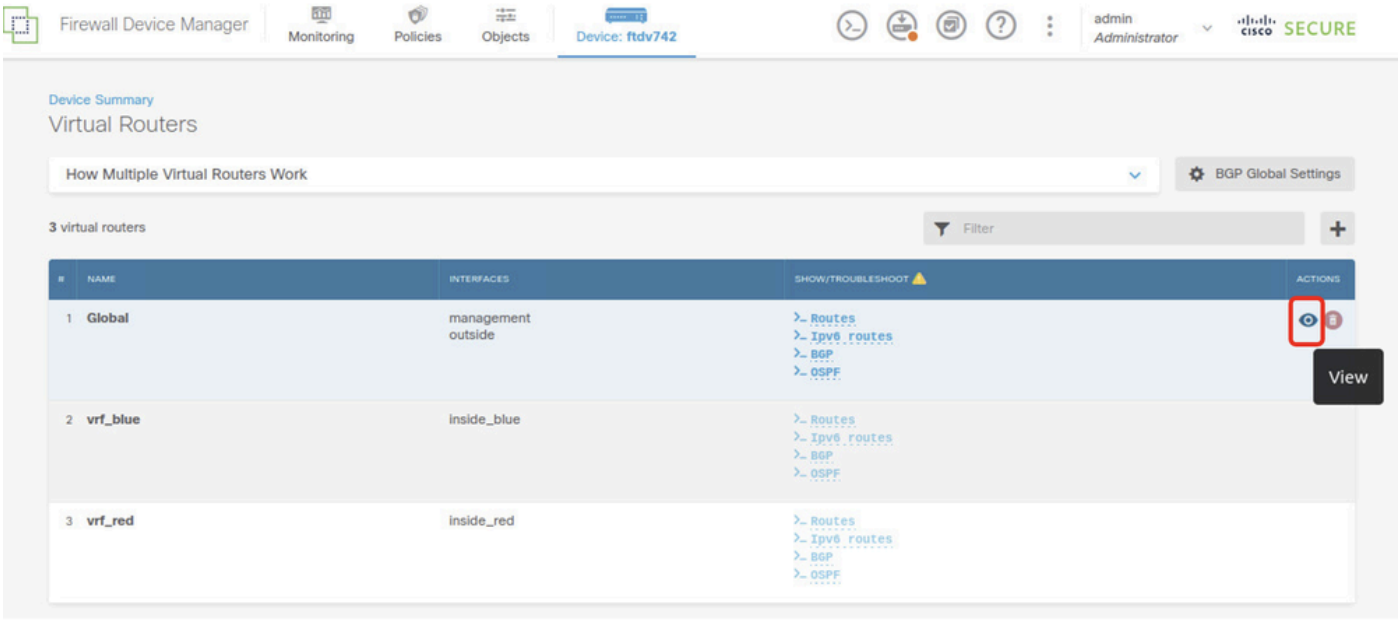


تفاصيل FTD_Create_STATIC_ROUTE_VRF_RED_Details

الخطوة 7. إنشاء تسريب المسار من الموجهات العالمية إلى الافتراضية. وتسمح المسارات لنقاط النهاية المحمية بواسطة الطرف البعيد من شبكة VPN من الموقع إلى الموقع

بالوصول إلى شبكة 192.168.10.0/24 في الموجه الظاهري VRF_RED وشبكة 192.168.20.0/24 في الموجه الظاهري VRF_BLUE.

انتقل إلى الجهاز > التوجيه . انقر فوق عرض التكوين . انقر فوق رمز العرض في خلية الإجراءات للموجه الظاهري العام.



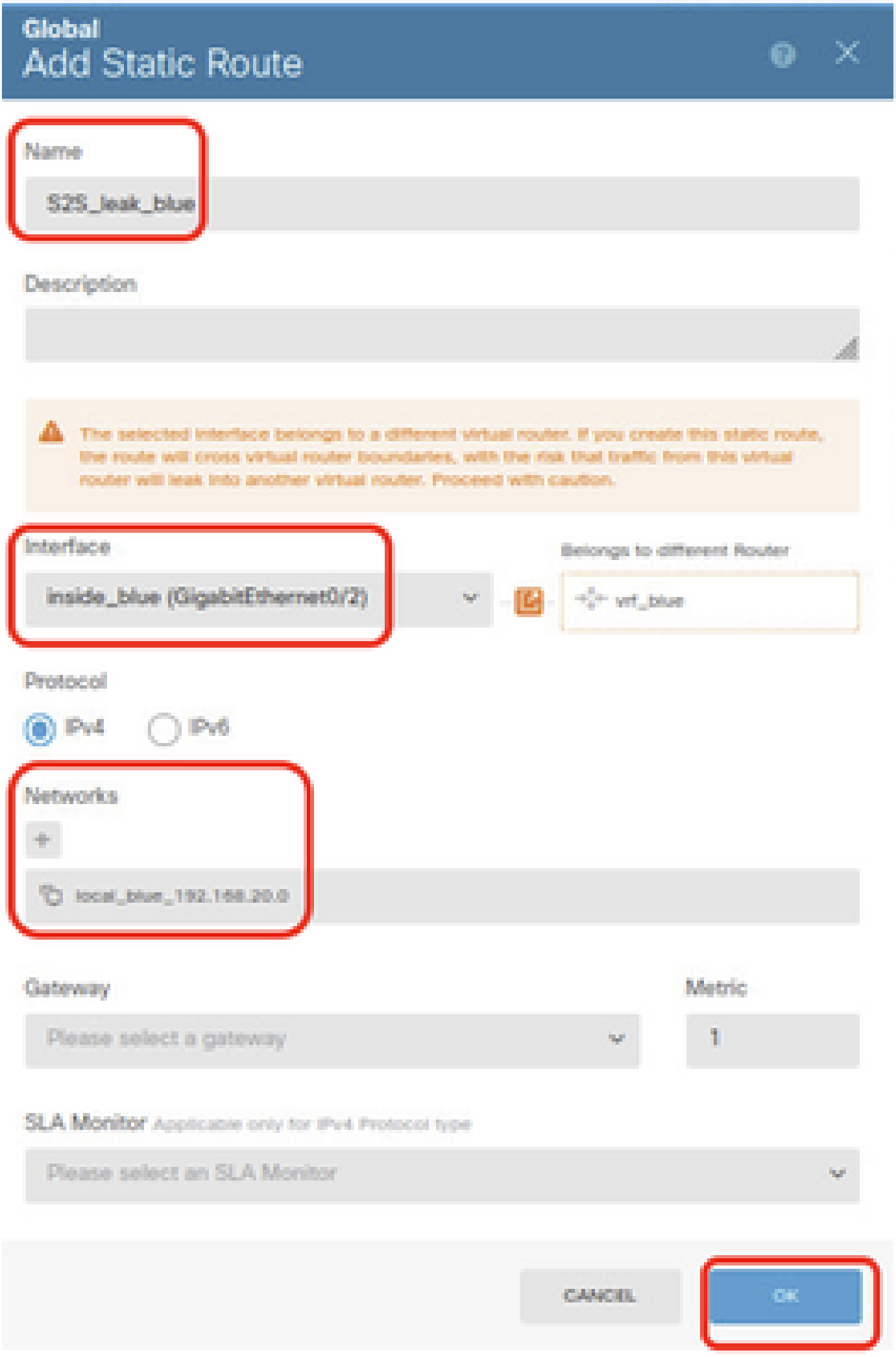
FTD_VIEW_VRF_Global

الخطوة 7.1. انقر فوق علامة التبويب توجيه ثابت. انقر فوق + زر.

FTD_Create_STATIC_ROUTE_VRF_GLOBAL

الخطوة 7-2. توفير المعلومات اللازمة. طقطقة ok زر.

- الاسم: S2S_leaks_blue
- الواجهة: inside_blue (GigabitEthernet0/2)
- الشبكات: local_blue_192.168.20.0
- البوابة: أترك هذا العنصر فارغا.


Global
Add Static Route
Name
S2S_leak_blue
Description
The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.
Interface
inside_blue (GigabitEthernet0/2)
Belongs to different Router
vrf_blue
Protocol
IPv4
IPv6
Networks
local_blue_192.168.20.0
Gateway
Please select a gateway
Metric
1
SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor
CANCEL
OK

```
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 21 20 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

الخطوة 10. قم بإنشاء مقترح IKEv2 IPsec الذي يحدد نفس المعلمات التي تم تكوينها على FTD.

```
<#root>

crypto ipsec ikev2 ipsec-proposal

AES-SHA

 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

الخطوة 11. إنشاء ملف تعريف IPSec، المرجع تم إنشاء مقترح IPSec في الخطوة 10.

```
<#root>

crypto ipsec profile

demo_ipsec_profile

 set ikev2 ipsec-proposal

AES-SHA

 set security-association lifetime kilobytes 4608000
 set security-association lifetime seconds 28800
```

الخطوة 12. قم بإنشاء سياسة مجموعة تسمح ببروتوكول IKEv2.

```
<#root>

group-policy

demo_gp_192.168.30.1

 internal
group-policy demo_gp_192.168.30.1 attributes
 vpn-tunnel-protocol ikev2
```

الخطوة 13. قم بإنشاء مجموعة أنفاق لعنوان IP الخارجي للنظير FTD، للإشارة إلى سياسة

المجموعة التي تم إنشاؤها في الخطوة 12 و تكوين المفاتيح المشترك مسبقا نفسه مع FTD(الذي تم إنشاؤه في الخطوة 3.7).

<#root>

```
tunnel-group 192.168.30.1 type ipsec-l2l
tunnel-group 192.168.30.1 general-attributes
 default-group-policy
```

demo_gp_192.168.30.1

```
tunnel-group 192.168.30.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

الخطوة 14. قم بتمكين IKEv2 على الواجهة الخارجية.

```
crypto ikev2 enable outside
```

الخطوة 15. إنشاء نفق ظاهري.

<#root>

```
interface Tunnel1
 nameif demovti_asa
 ip address 169.254.10.2 255.255.255.0
 tunnel source interface outside
 tunnel destination 192.168.30.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile
```

demo_ipsec_profile

الخطوة 16. إنشاء مسار ثابت.

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الخطوة 1. انتقل إلى واجهة سطر الأوامر (CLI) الخاصة ب FTD و ASA عبر وحدة التحكم أو SSH للتحقق من حالة شبكة VPN للمرحلة 1 والمرحلة 2 من خلال الأوامر show crypto ikev2 sa وshow crypto ipSec .

برنامج FTD:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv742#
ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
 32157565 192.168.30.1/500                              192.168.40.1/500                    G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/67986 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: 0x4cf55637/0xa493cc83

ftdv742# show crypto ipsec sa
interface: demovti
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1

      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: 192.168.40.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #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.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: A493CC83
      current inbound spi : 4CF55637

    inbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16867)
```

```
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
    outbound esp sas:
      spi: 0xA493CC83 (2761149571)
        SA State: active
        transform: esp-aes-256 esp-sha-512-hmac no compression
        in use settings ={L2L, Tunnel, IKEv2, VTI, }
        slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
        sa timing: remaining key lifetime (kB/sec): (4285440/16867)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

ASA:

```
ASA9203# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
 26025779 192.168.40.1/500                                192.168.30.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/68112 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: 0xa493cc83/0x4cf55637
ASA9203#
ASA9203# show cry
ASA9203# show crypto ipsec sa
interface: demovti_asa
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1

      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: 192.168.30.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #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.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 4CF55637
```

```
      current inbound spi : A493CC83

    inbound esp sas:
      spi: 0xA493CC83 (2761149571)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4101120/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

الخطوة 2. تحقق من مسار VRF و Global على FTD.

```
ftdv742# show route

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 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
SI       192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI       192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside


ftdv742# show route vrf vrf_blue


Routing Table: vrf_blue
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 not set

C        192.168.20.0 255.255.255.0 is directly connected, inside_blue
L        192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti


ftdv742# show route vrf vrf_red


Routing Table: vrf_red
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 not set

C        192.168.10.0 255.255.255.0 is directly connected, inside_red
L        192.168.10.1 255.255.255.255 is directly connected, inside_red
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

الخطوة 3. التحقق من إختبار الاتصال.

قبل إختبار الاتصال، تحقق من عدادات show crypto ipSec sa | واجهة inc:|encap|decap على FTD.

في هذا المثال، يعرض النفق1 30 حزمة لكل من التضمين والعزل.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

عميل إختبار الاتصال Client1 3 بنجاح.

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

عميل إختبار الاتصال Client2 3 بنجاح.

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

تحقق من عدادات show crypto ipsec sa | واجهة inc:|encap|decap في FTD بعد إختبار الاتصال بنجاح.

في هذا المثال، يعرض Tunnel1 40 حزمة لكل من التضمين والعزل بعد إختبار اتصال ناجح. وبالإضافة إلى ذلك، زاد العدد بمقدار 10 حزم، مما يطابق طلبات صدى إختبار الاتصال العشرة، مما يشير إلى أن حركة مرور ping قد مرت بنجاح عبر نفق IPSec.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
      #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أنت يستطيع استعملت أن يضبط أمر أن يتحرى ال VPN قسم.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

يمكنك إستخدام أوامر تصحيح الأخطاء هذه لاستكشاف أخطاء قسم المسار وإصلاحها.

```
debug ip routing
```

المرجع

دليل تكوين مدير جهاز جدار الحماية الآمن من Cisco، الإصدار 7.4

دليل تكوين واجهة سطر الأوامر Cisco Secure Firewall ASA VPN، 9.20

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).