قم بتكوين AnyConnect to Access Server عبر نفق IPSec.

المحتويات

المقدمة:

يصف هذا المستند إجراءات نشر إعداد RAPN على FTD الذي تتم إدارته بواسطة FMC ونفق من موقع إلى موقع بين FTDs.

المتطلبات الأساسية:

المتطلبات الأساسية

- ومن المفيد التوصل إلى فهم أساسي للشبكات الخاصة الظاهرية (VPN) والشبكة الخاصة الظاهرية (RAVPN) من موقع إلى موقع.
- من الضروري فهم الأسس اللازمة لتكوين نفق يستند إلى سياسة IKEv2 على منصة Cisco Firepower.

الغرض من هذا الإجراء هو نشر إعداد RAPN على FTD الذي تتم إدارته بواسطة FMC ونفق من موقع إلى موقع بين FTDs حيث يمكن لمستخدم AnyConnect الوصول إلى الخادم خلف النظير الآخر ل FTD.

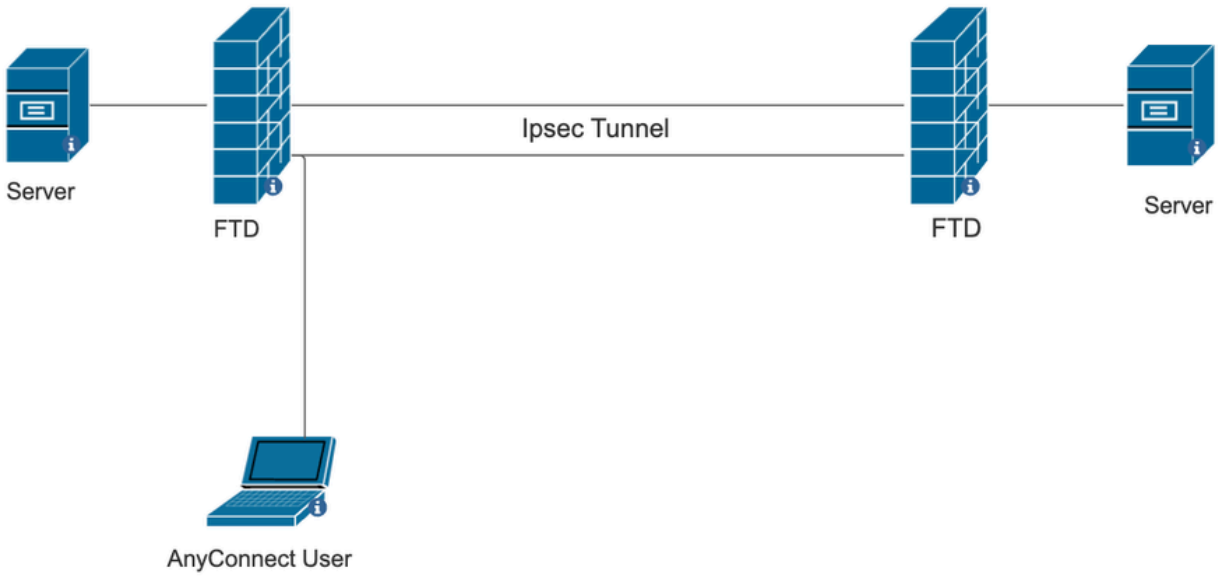
المكونات المستخدمة

- برنامج الدفاع ضد تهديد FirePOWER ل VMware من Cisco: الإصدار 7.0.0
- مركز إدارة Firepower: الإصدار 7.2.4 (بنية 169)

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر..

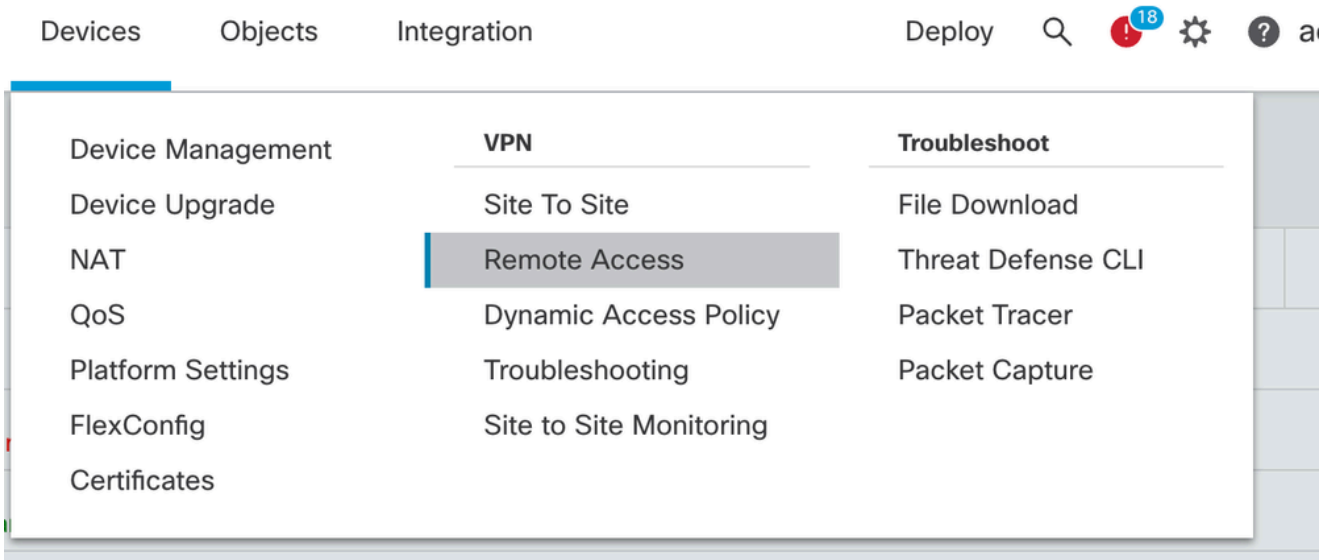
الرسم التخطيطي للشبكة



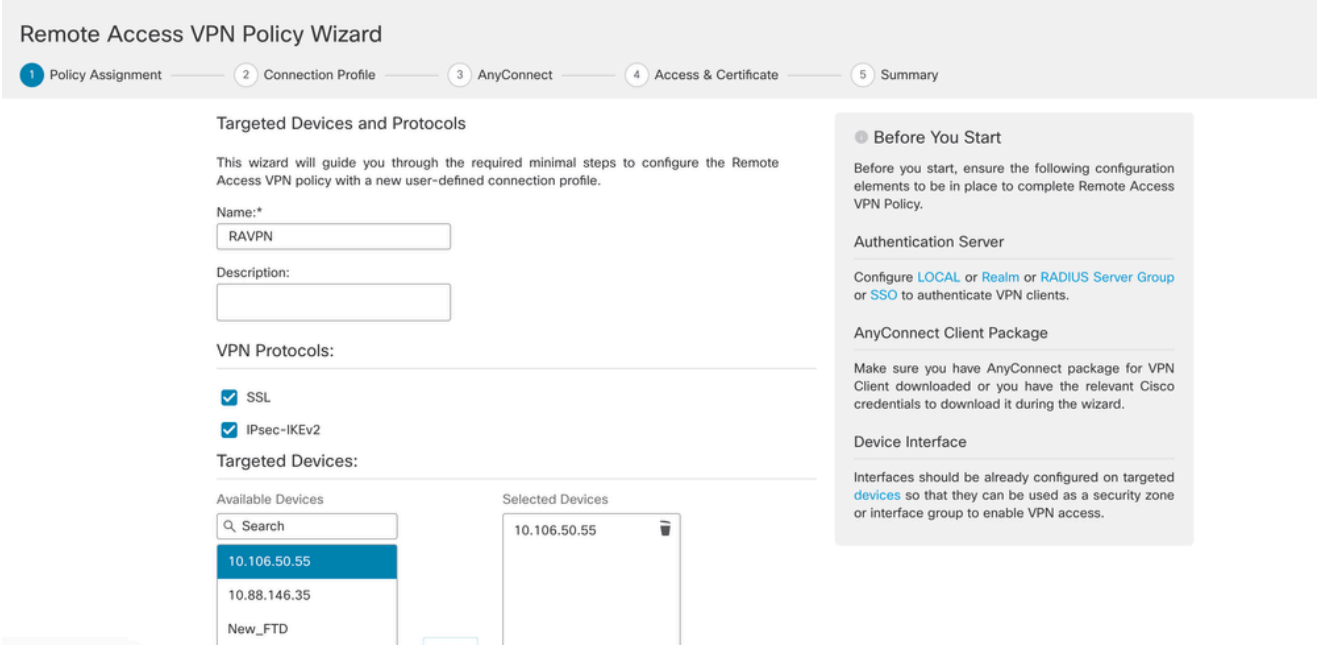
التكوينات على FMC

تكوين RAVPN على FTD الذي تتم إدارته بواسطة FMC.

1. انتقل إلى الأجهزة > الوصول عن بعد.

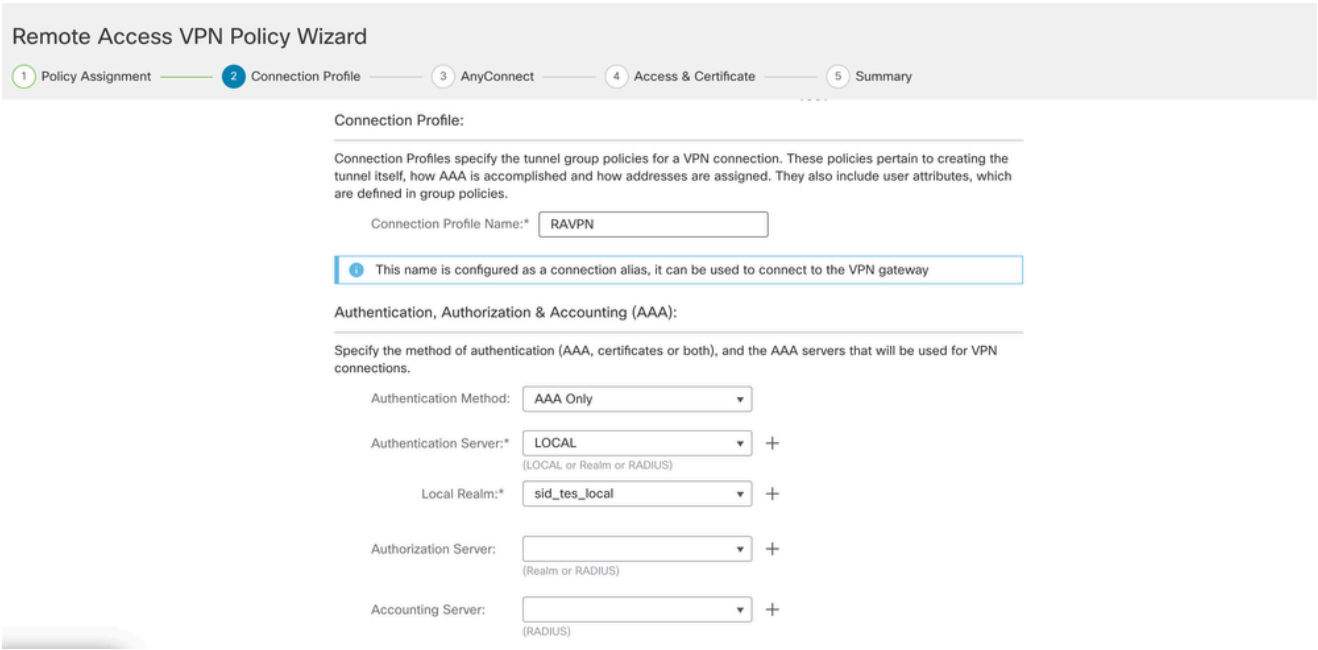


2. انقر فوق إضافة (Add).
3. قم بتكوين اسم وحدد FTD من الأجهزة المتاحة وانقر فوق التالي.

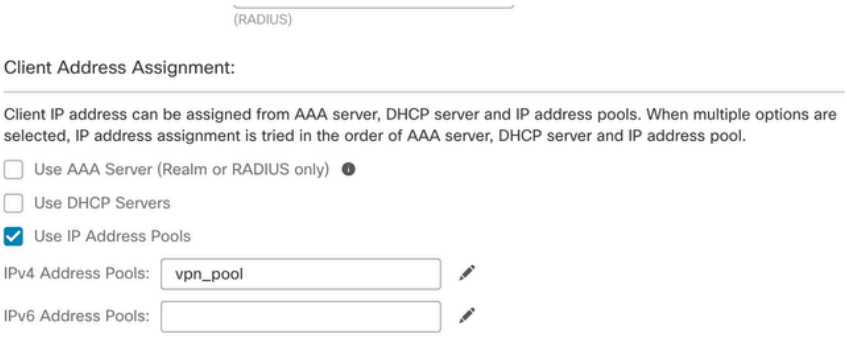


4. قم بتكوين اسم توصيف توصيل واختر أسلوب المصادقة.

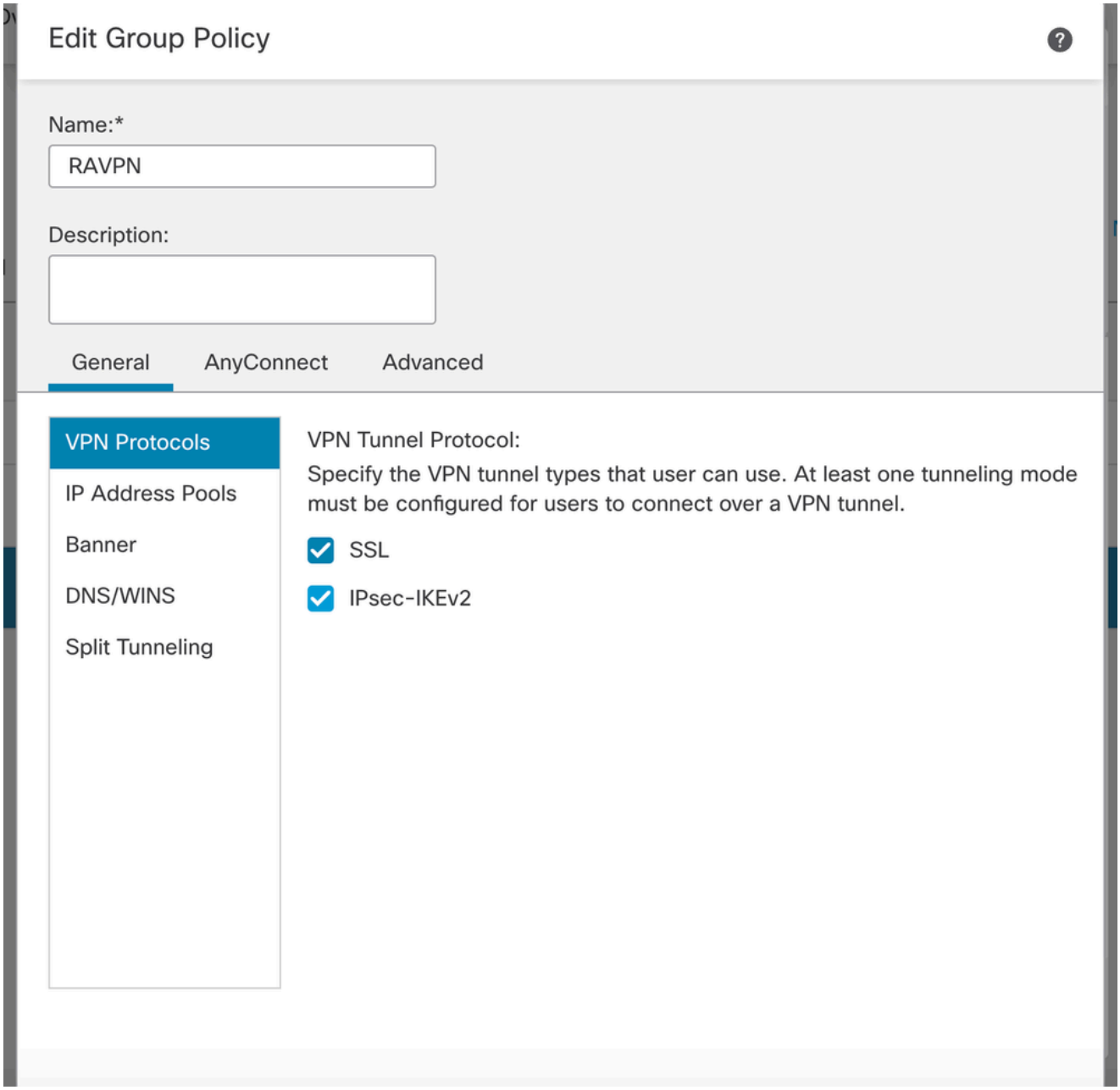
ملاحظة: بالنسبة لعينة التكوين هذه، نستخدم المصادقة والتفويض والمحاسبة (AAA) فقط والمصادقة المحلية. ومع ذلك، قم بالتكوين استنادا إلى متطلباتك.



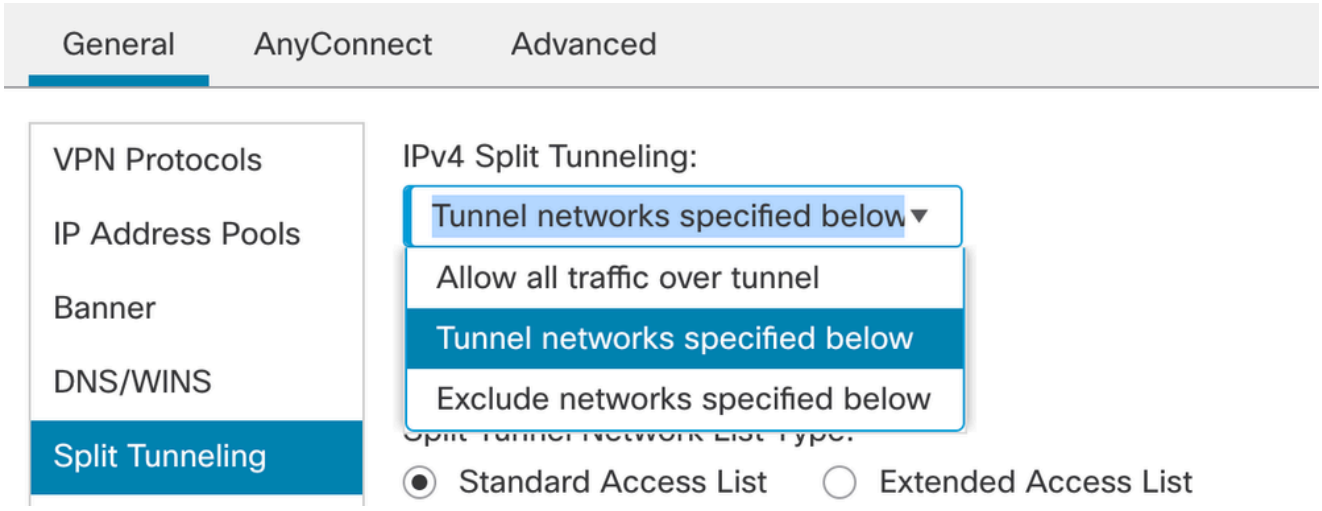
5. قم بتكوين تجمع VPN الذي يتم إستخدامه لتعيين عنوان IP ل AnyConnect.



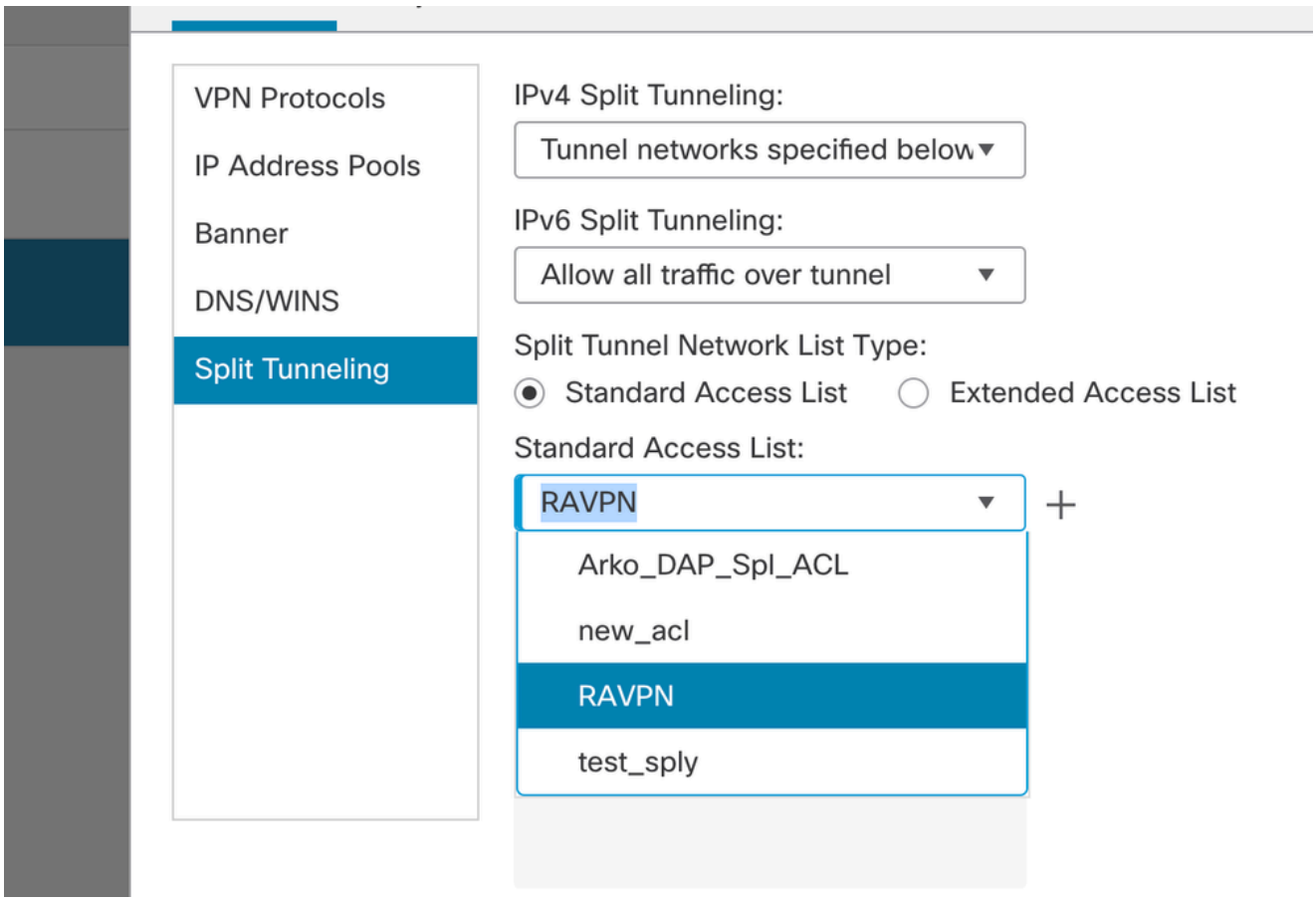
6. إنشاء نهج المجموعة. انقر فوق + لإنشاء نهج مجموعة. إضافة اسم نهج المجموعة.



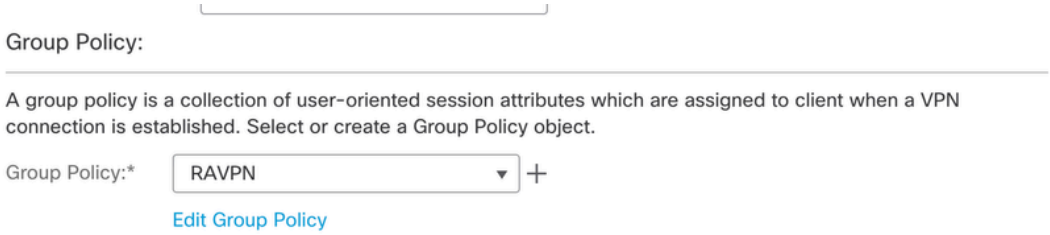
7. انتقل إلى الاتصال النفقي المنقسم. حدد شبكات النفق المحددة هنا:



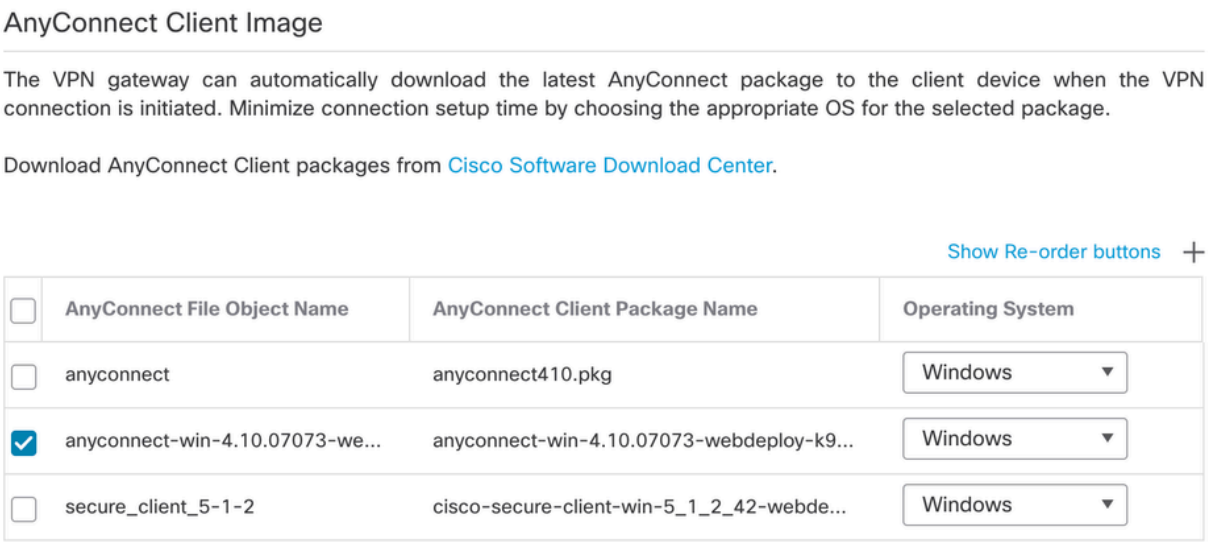
8. حدد قائمة الوصول الصحيحة من القائمة المنسدلة. إذا لم يتم تكوين قائمة تحكم في الوصول (ACL) بالفعل: انقر فوق أيقونة + لإضافة قائمة الوصول القياسية وإنشاء قائمة وصول جديدة.
انقر فوق حفظ.



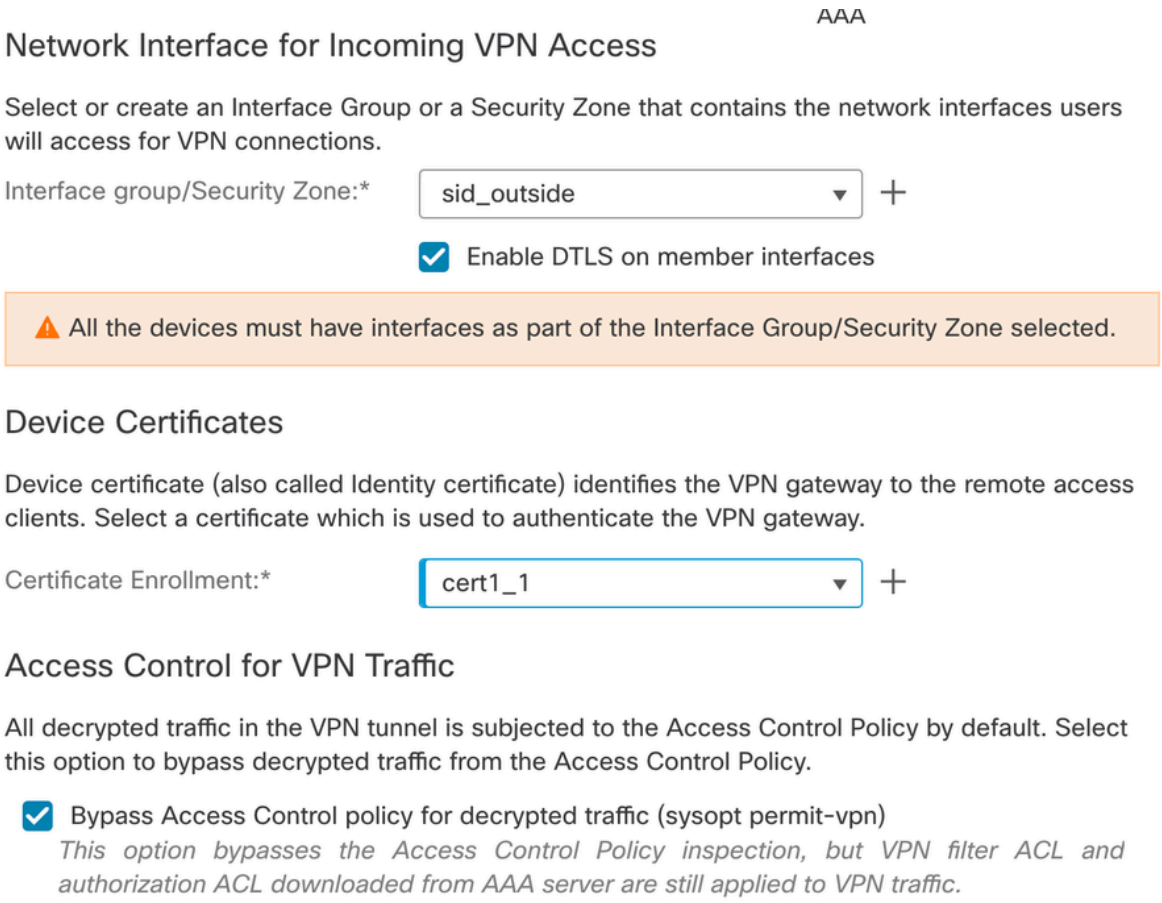
9. حدد نهج المجموعة الذي تمت إضافته وانقر فوق التالي.



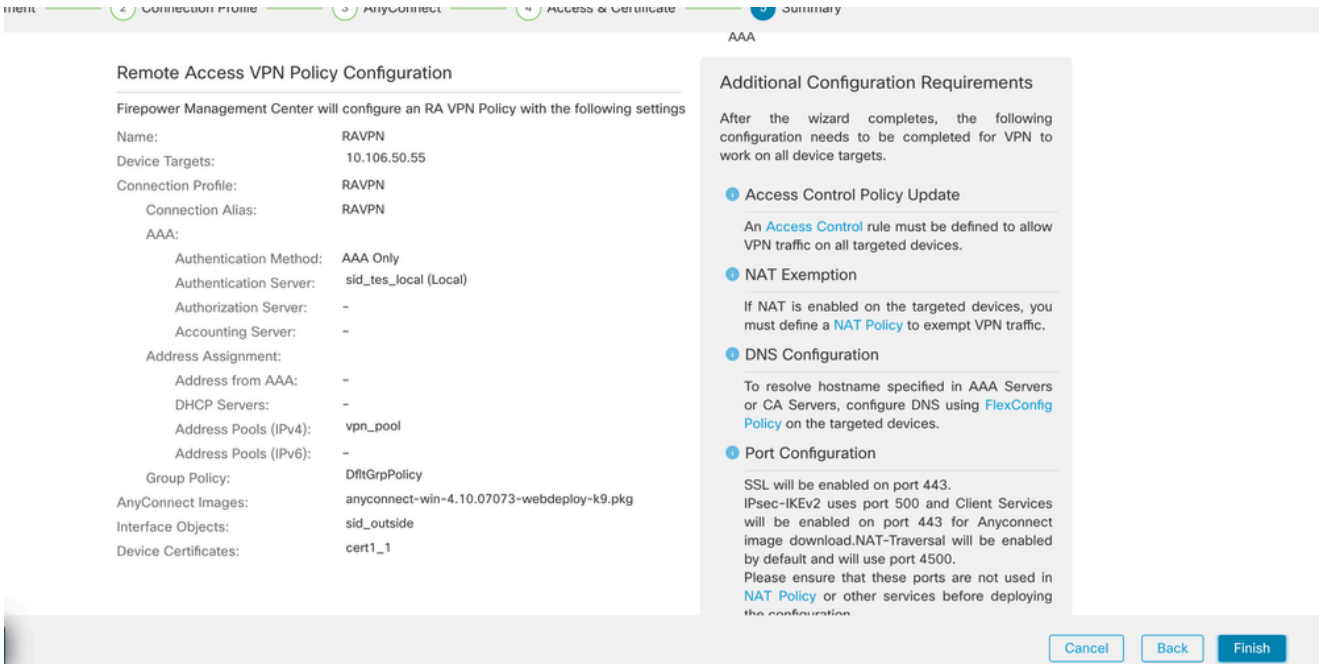
10. حدد صورة AnyConnect.



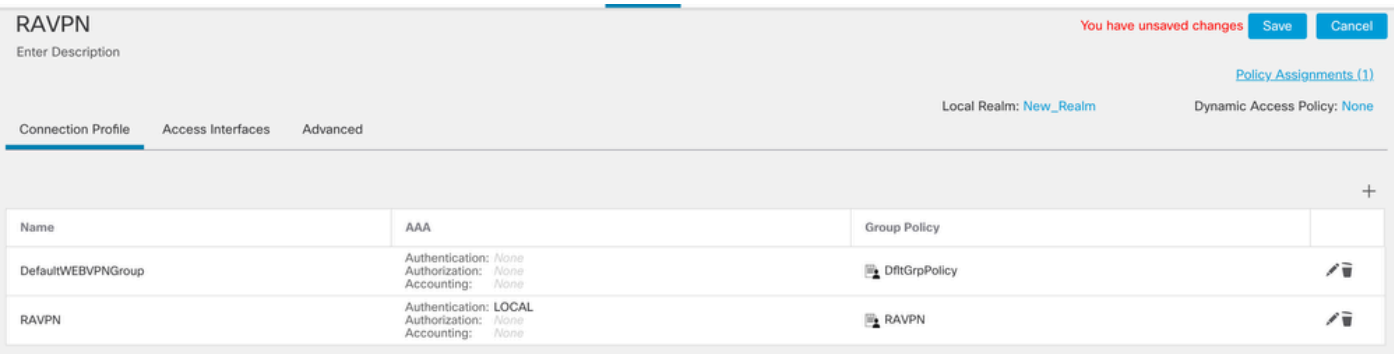
11. حدد الواجهة التي يجب تمكينها لاتصال AnyConnect، وقم بإضافة الشهادة، وحدد نهج التحكم في الوصول الالتفافي لحركة المرور التي تم فك تشفيرها، وانقر فوق التالي.



12. راجعت التشكيل وطقطقة إنجاز.

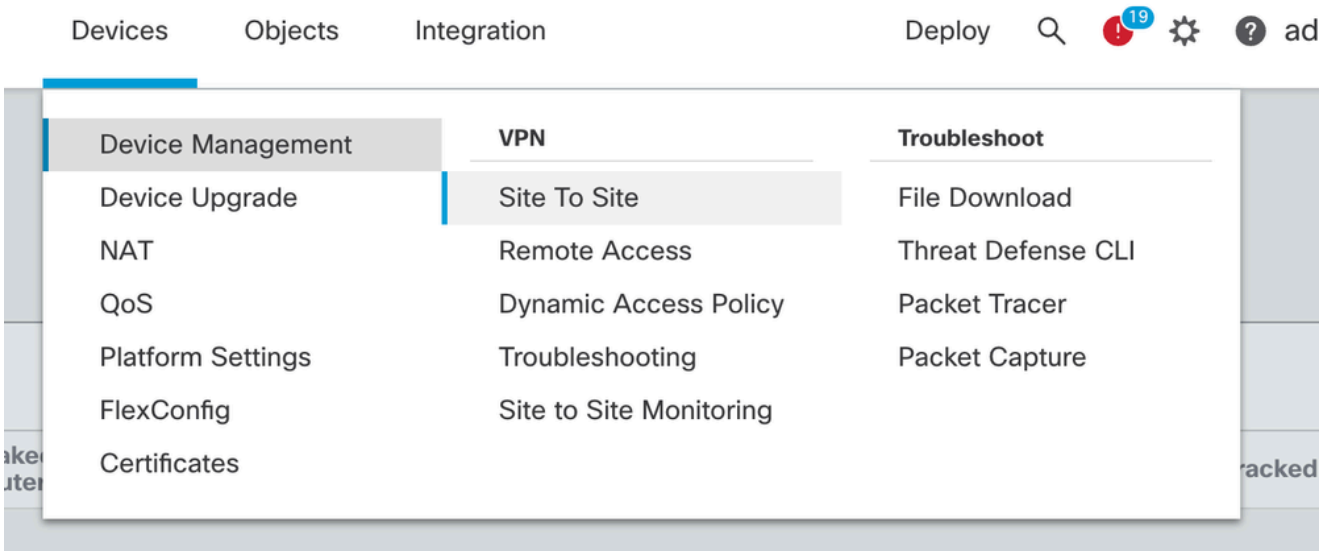


13. انقر فوق حفظ ونشر.

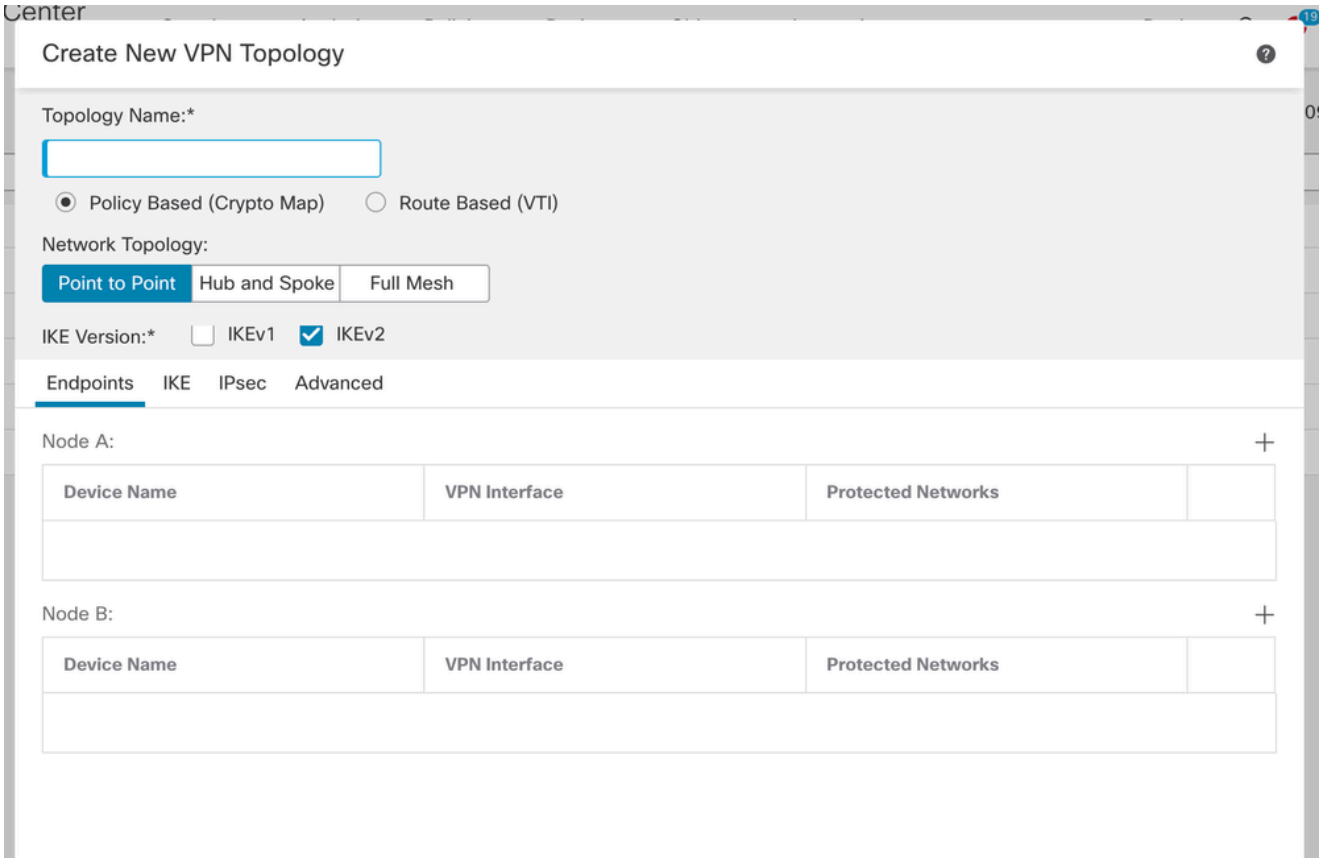


IKEv2 VPN على إدارة FTD بواسطة FMC:

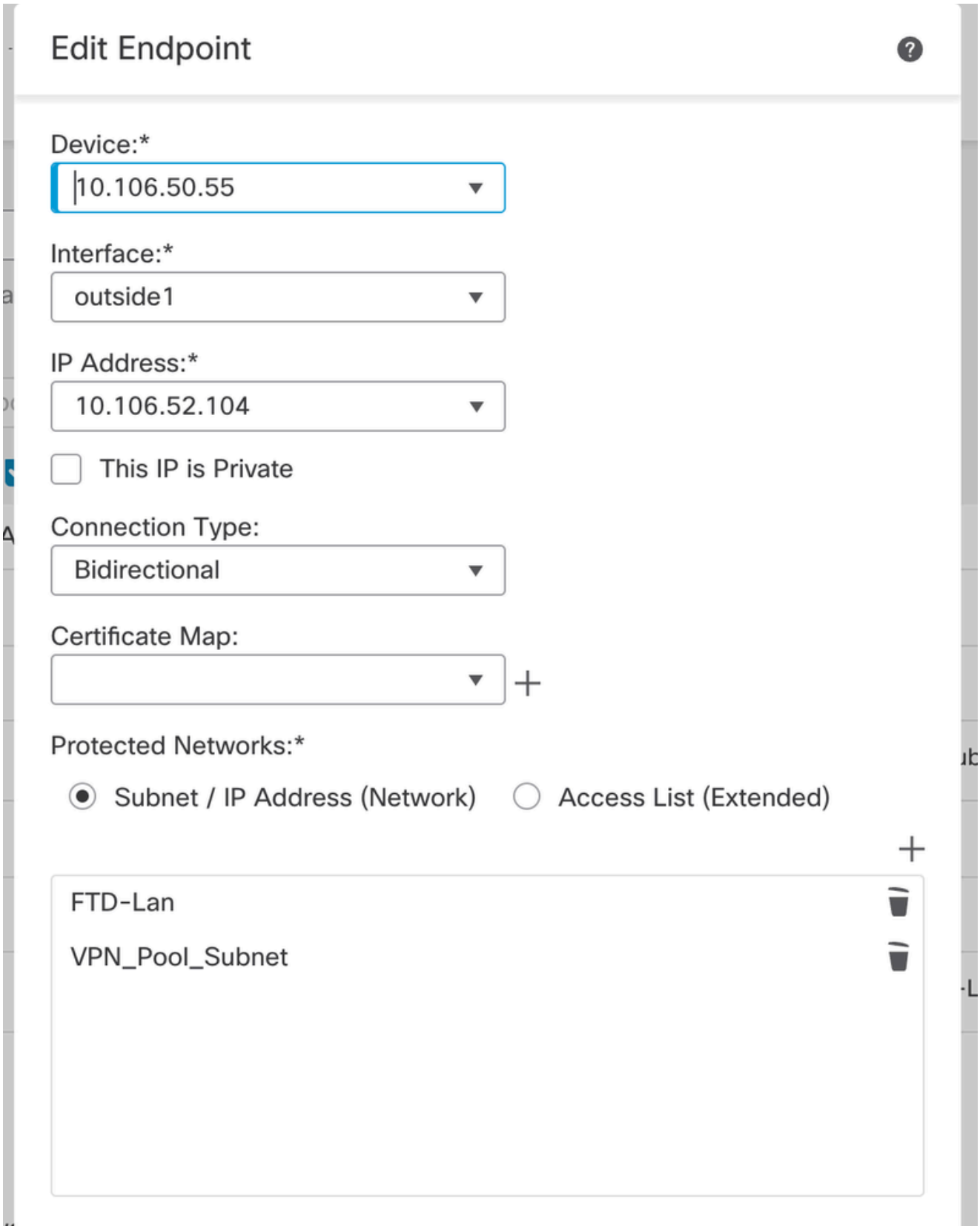
1. انتقل إلى الأجهزة > موقع إلى موقع.



2. انقر فوق إضافة (Add).
3. انقر + للعقدة A:



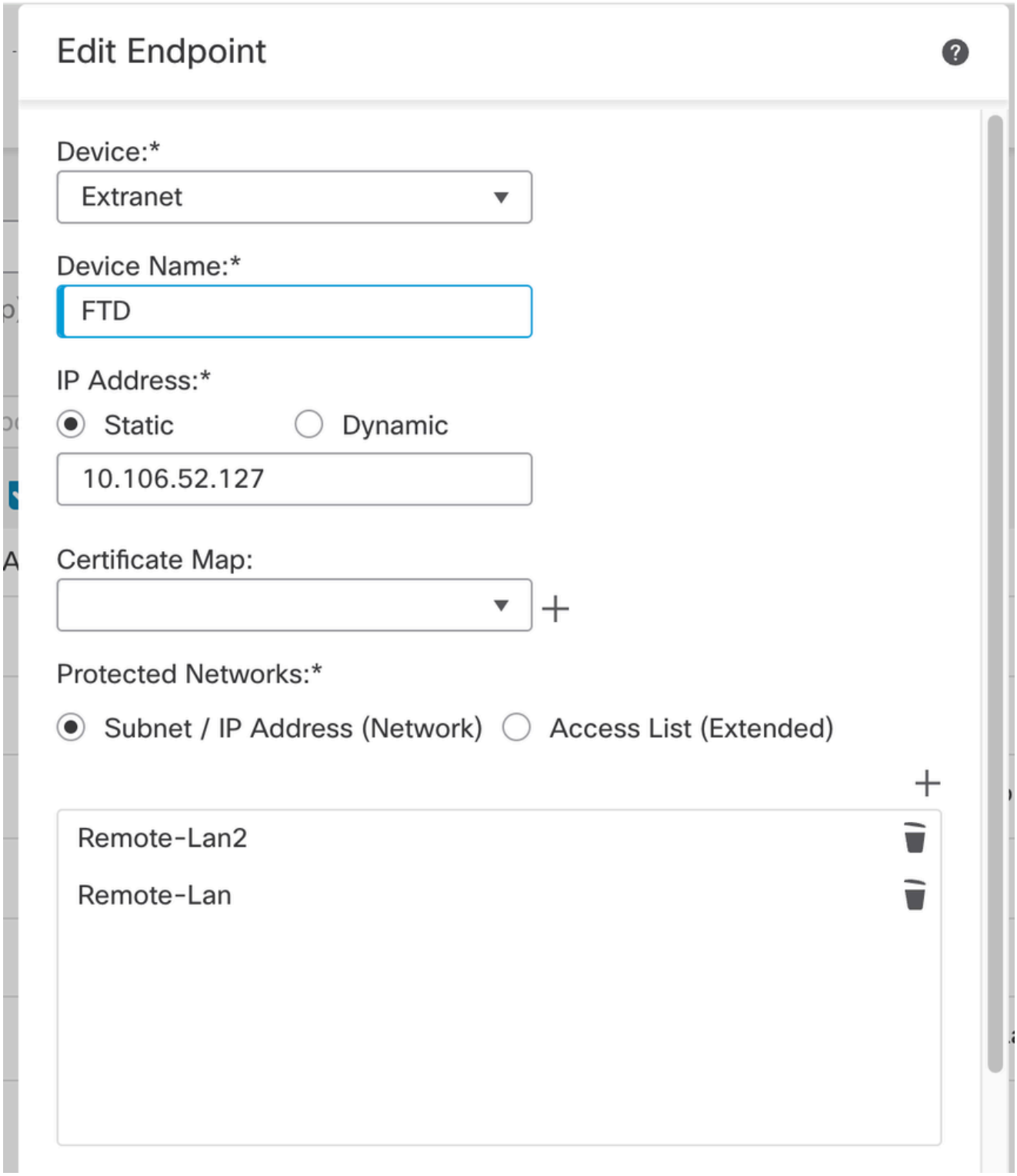
4. حدد FTD من الجهاز، وحدد الواجهة، وقم بإضافة الشبكة الفرعية المحلية التي يجب تشفيرها من خلال نفق IPSec (وفي هذه الحالة، تحتوي أيضا على عناوين تجمع VPN)، وانقر فوق موافق.



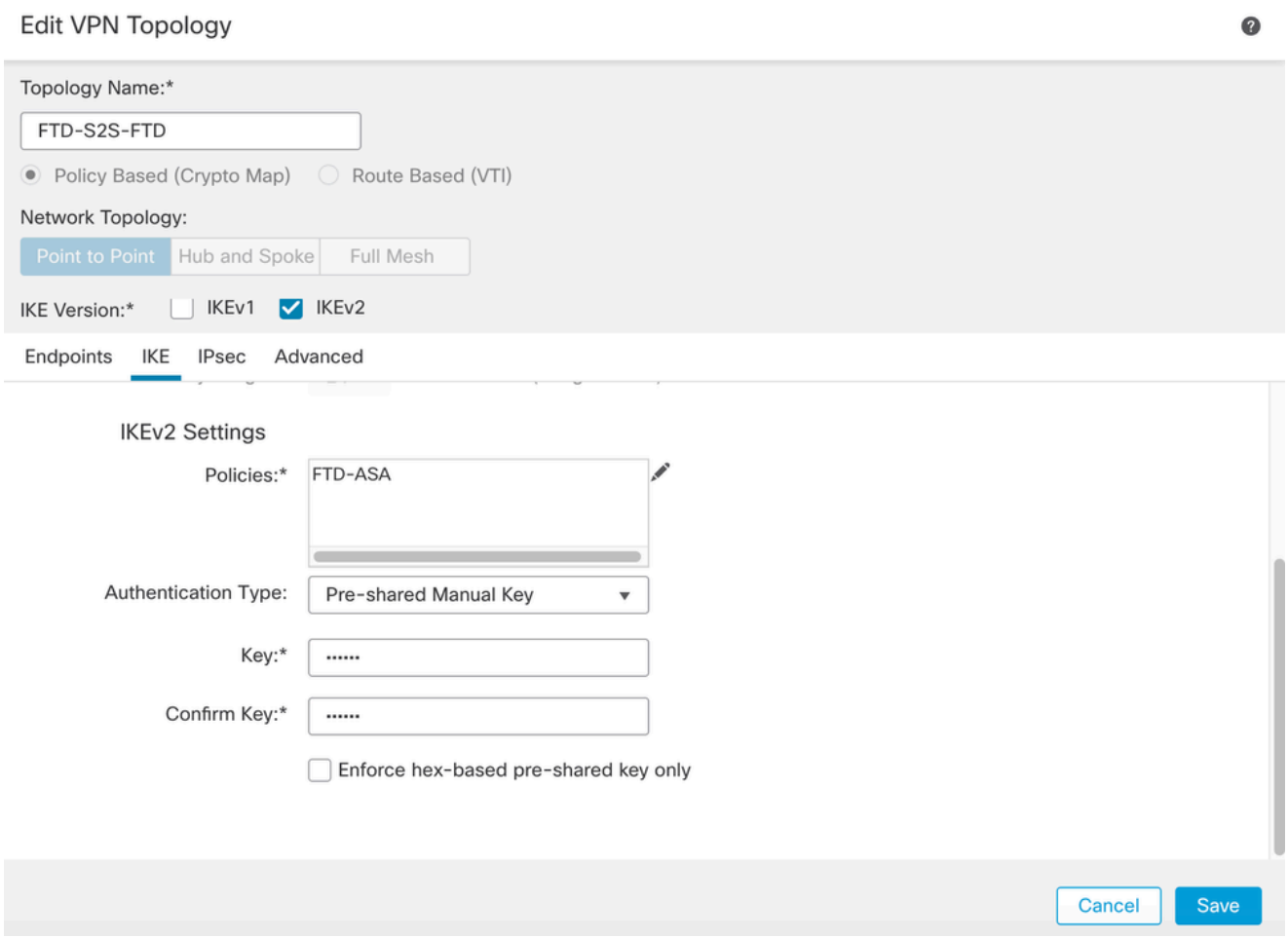
5. انقر فوق + للعقدة ب:

> حدد إكسترانت من الجهاز، وأعط اسم جهاز النظير.

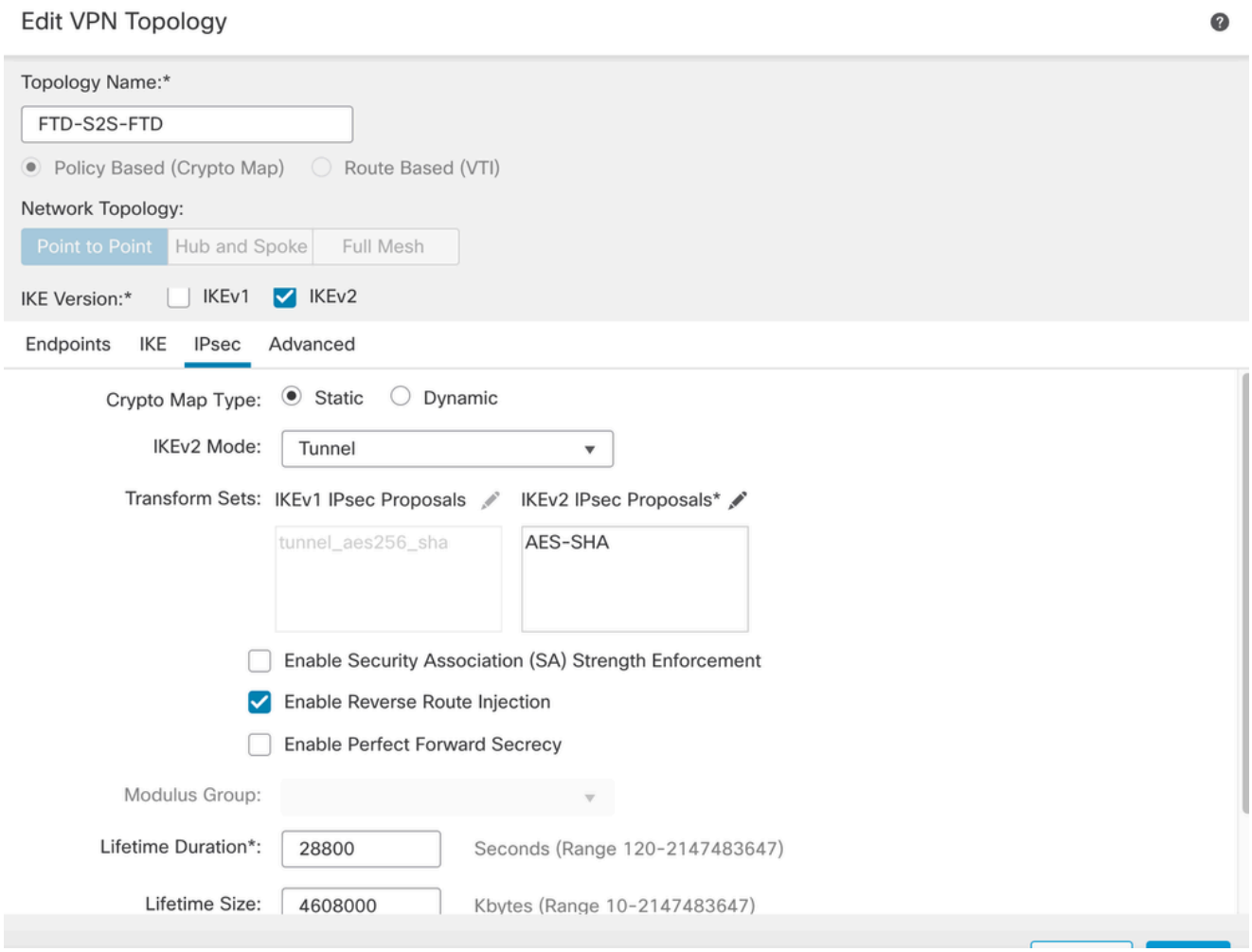
<تكوين تفاصيل النظير وإضافة الشبكة الفرعية البعيدة التي يلزم الوصول إليها عبر نفق الشبكة الخاصة الظاهرية (VPN) وانقر فوق موافق.



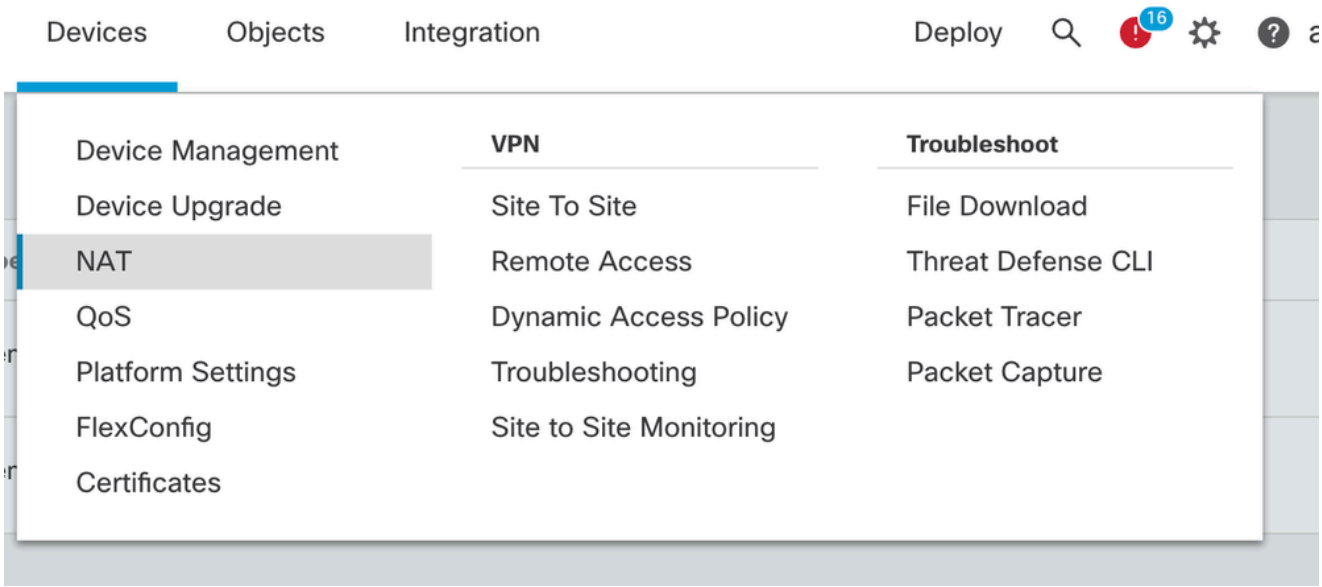
6. انقر فوق علامة التبويب IKE: قم بتكوين إعدادات IKEv2 وفقا لمتطلباتك



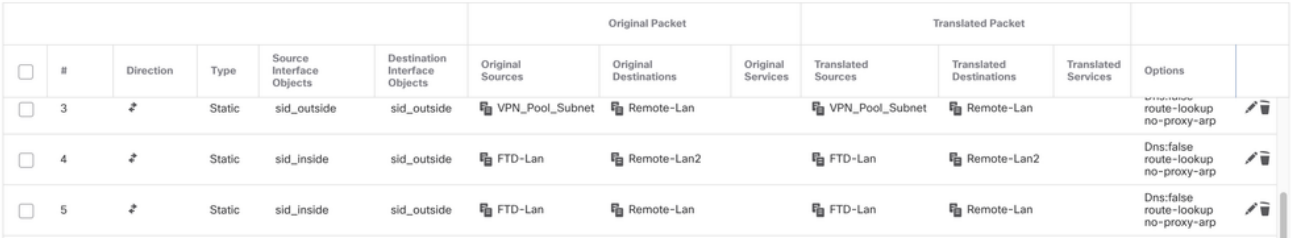
7. انقر فوق علامة التبويب IPsec: قم بتكوين إعدادات IPSec وفقا لمتطلباتك.



8. تكوين NAT-Exempt لحركة المرور المثيرة للاهتمام (إختياري)
انقر على الأجهزة > NAT



9. يسمح NAT الذي تم تكوينه هنا ل RAVPN والمستخدمين الداخليين بالوصول إلى الخوادم من خلال نفق S2S IPSec.



	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet: Original Sources	Original Packet: Original Destinations	Original Packet: Original Services	Translated Packet: Translated Sources	Translated Packet: Translated Destinations	Translated Packet: Translated Services	Options
☐	3	⇄	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		route-lookup no-proxy-arp
☐	4	⇄	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan2		FTD-Lan	Remote-Lan2		Dns:false route-lookup no-proxy-arp
☐	5	⇄	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan		FTD-Lan	Remote-Lan		Dns:false route-lookup no-proxy-arp

10. وبالمثل، قم بالتكوين على الطرف الآخر للنظير الخاص بنفق S2S الذي سيتم إنشاؤه.

    ملاحظة: يجب أن تكون قوائم التحكم في الوصول (ACL) للتشفير أو الشبكات الفرعية لحركة المرور المثيرة للاهتمام نسخا مطابقة لبعضها البعض على كل النظامين.

التحقق من الصحة

1. للتحقق من اتصال RAVPN:

<#root>

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : test

 Index : 5869

Assigned IP : 2.2.2.1 Public IP : 10.106.50.179

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

Bytes Tx : 15470 Bytes Rx : 2147

Group Policy : RAVPN Tunnel Group : RAVPN

Login Time : 03:04:27 UTC Fri Jun 28 2024

Duration : 0h:14m:08s

Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a3468016ed000667e283b
```

Security Grp : none Tunnel Zone : 0

2. للتحقق من اتصال IKEv2:

<#root>

firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:2443, Status:UP-ACTIVE

, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555

10.106.52.104/500 10.106.52.127/500 READY INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/259 sec

Child sa: local selector 2.2.2.0/0 - 2.2.2.255/65535

remote selector 10.106.54.0/0 - 10.106.54.255/65535

ESP spi in/out: 0x4588dc5b/0x284a685

3. للتحقق من اتصال IPSec:

<#root>

firepower# show crypto ipsec sa peer 10.106.52.127
peer address: 10.106.52.127

Crypto map tag: CSM_outside1_map

,

seq num: 2, local addr: 10.106.52.104

access-list CSM_IPSEC_ACL_1 extended permit ip 2.2.2.0 255.255.255.0 10.106.54.0 255.255.255.0

local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.106.54.0/255.255.255.0/0/0)

current_peer: 10.106.52.127

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 3, #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.: 10.106.52.104/500, remote crypto endpt.: 10.106.52.127/500
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: 0284A685
current inbound spi : 4588DC5B

i

nbound esp sas:

spi: 0x4588DC5B (1166597211)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map
sa timing: remaining key lifetime (kB/sec): (3962879/28734)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000000F

outbound esp sas:

spi: 0x0284A685 (42247813)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

```
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map
sa timing: remaining key lifetime (kB/sec): (4285439/28734)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

استكشاف الأخطاء وإصلاحها

1. لاستكشاف أخطاء اتصال AnyConnect وإصلاحها، قم بجمع حزمة البيانات أو تمكين تصحيح أخطاء AnyConnect.
2. لاستكشاف أخطاء نفق IKEv2 وإصلاحها، أستخدم عمليات تصحيح الأخطاء التالية:

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. أستكشاف أخطاء حركة المرور وإصلاحها علي FTD، قم بأخذ التقاط الحزمة والتحقق من التكوين.

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).