تكوين الشبكة الخاصة الظاهرية (VPN) من الموقع إلى الموقع على FTD تتم إدارته بواسطة FMC

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين موقع إلى شبكة VPN الخاصة بالموقع على "الدفاع عن تهديد FirePOWER (FTD)" الذي تتم إدارته بواسطة FMC.

المتطلبات الأساسية

المتطلبات

لزام يكون عندك معرفة بالمواضيع التالية:

- الفهم الأساسي للشبكة الخاصة الظاهرية (VPN)
- تجربة مع مركز إدارة FirePOWER
- التجربة مع سطر أوامر ASA

المكونات المستخدمة

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

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

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.

التكوين

ابدأ بالتكوين على FTD باستخدام مركز إدارة FirePOWER.

الخطوة 1. تحديد مخطط الشبكة الخاصة الظاهرية (VPN).

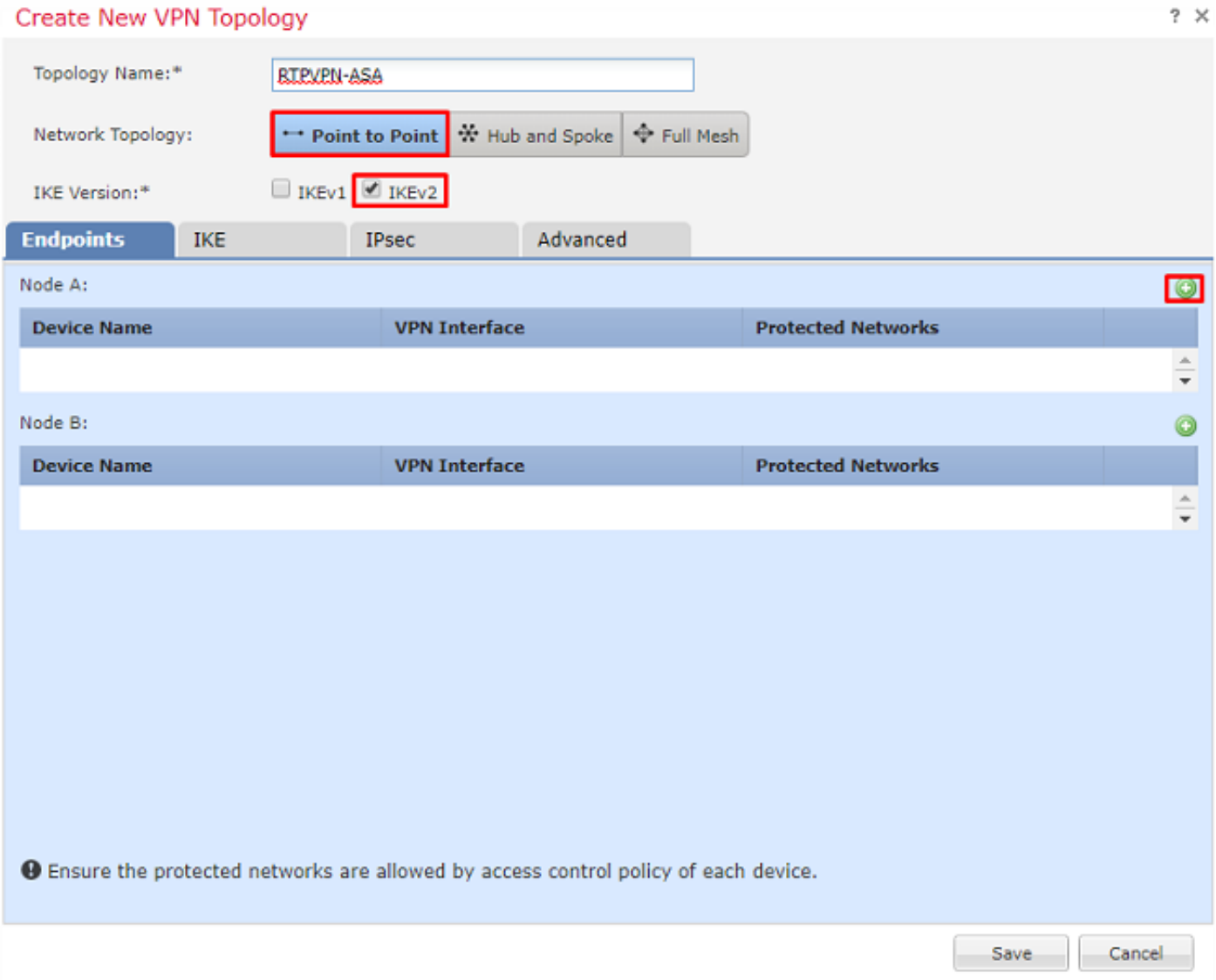
1. انتقل إلى الأجهزة > VPN > موقع إلى موقع. تحت إضافة VPN، انقر فوق جهاز الدفاع ضد تهديد FirePOWER، كما هو موضح في هذه الصورة.

2. يظهر مربع إنشاء مخطط VPN جديد. امنح شبكة VPN اسما يمكن التعرف عليه بسهولة.

مخطط الشبكة: نقطة إلى نقطة

إصدار IKE: IKEv2

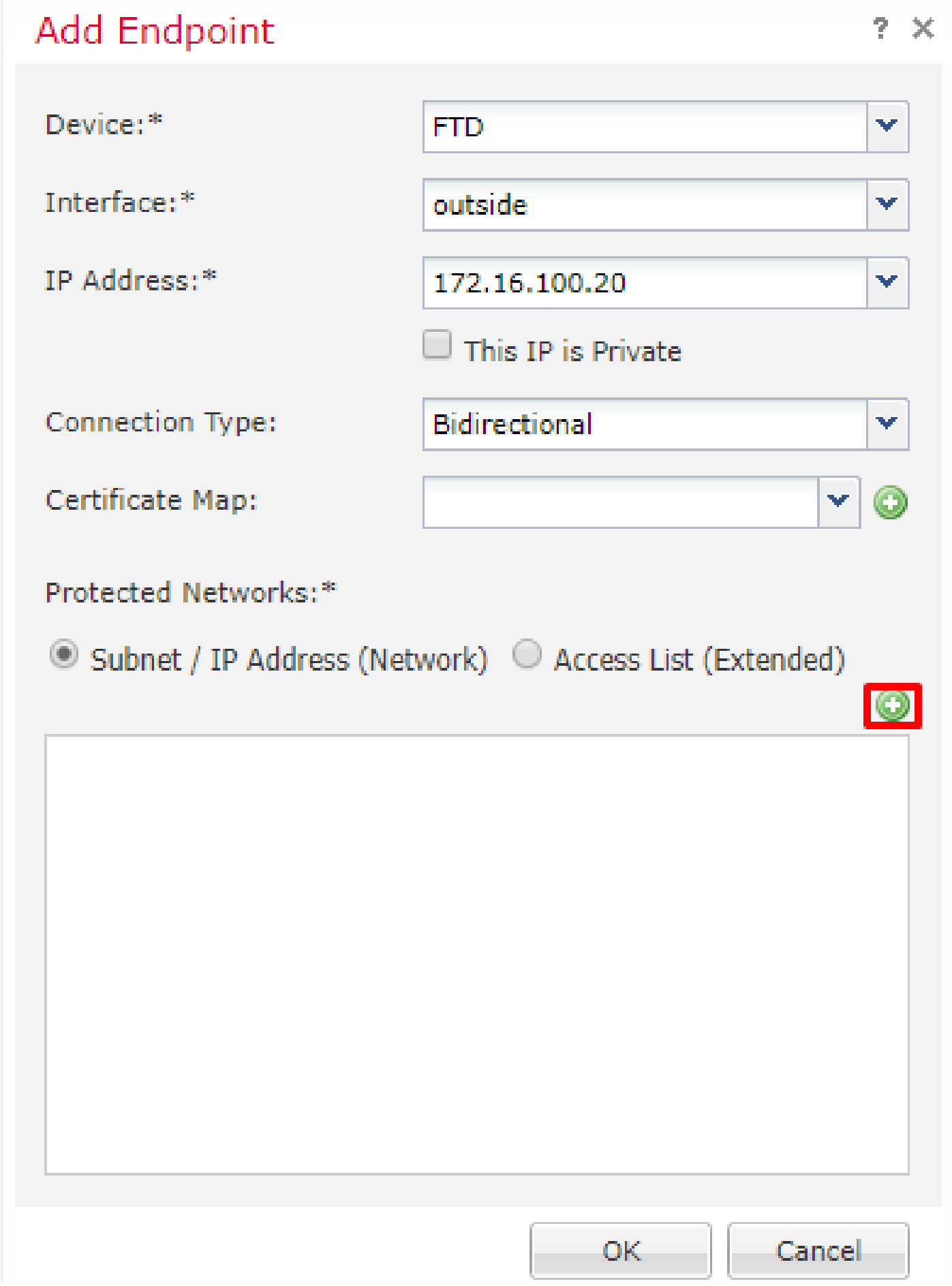
في هذا المثال، عند تحديد نقاط النهاية، تكون العقدة A هي FTD، بينما تكون العقدة B هي ASA. انقر فوق الزر الأخضر زائد لإضافة أجهزة إلى المخطط، كما هو موضح في هذه الصورة.



3. أضف "برنامج الإرسال فائق السرعة (FTD)" كنقطة النهاية الأولى.

أختر الواجهة التي يتم وضع خريطة تشفير عليها. يجب أن تتم تعبئة عنوان IP تلقائيا من تكوين الجهاز.

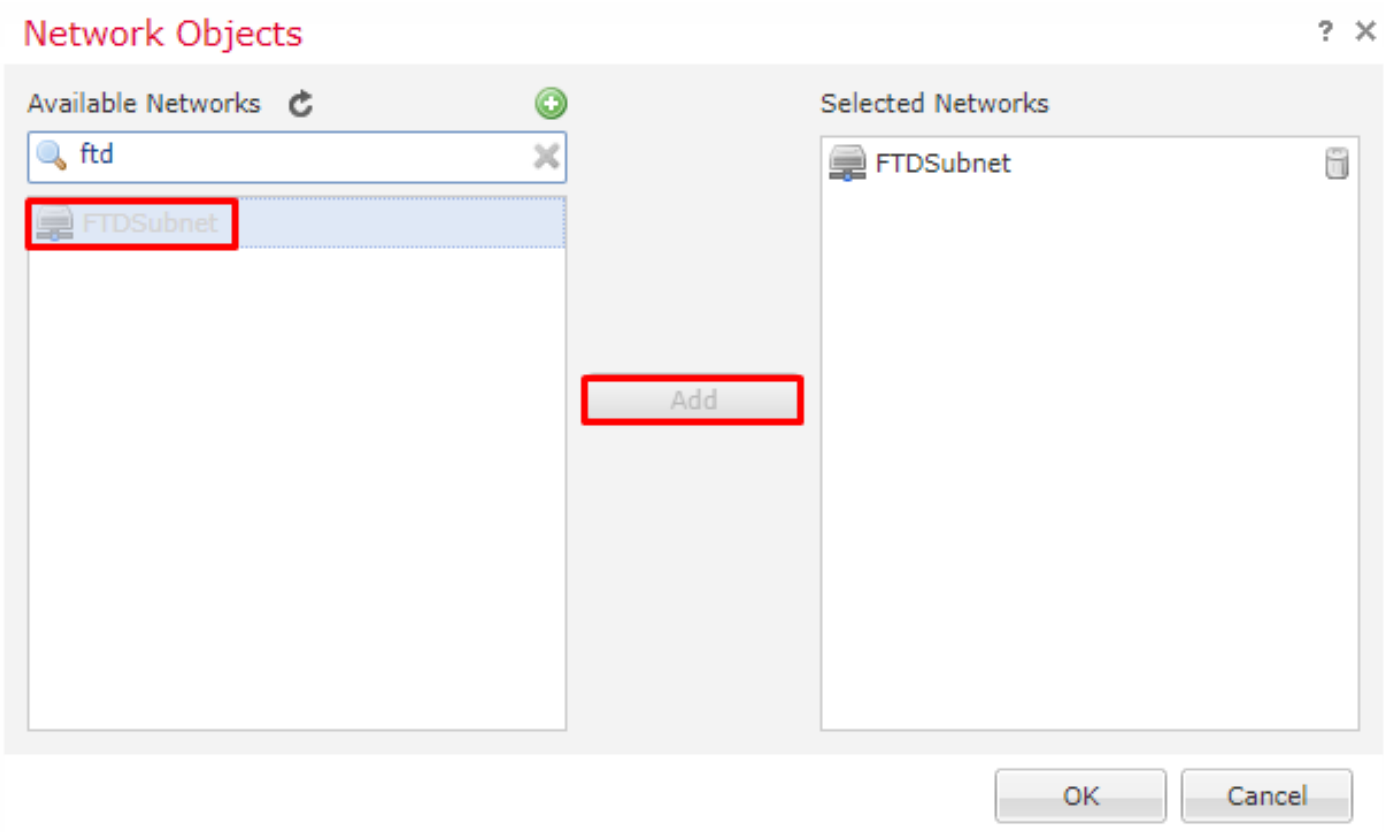
انقر فوق الشبكة الخضراء الإضافية الموجودة ضمن الشبكات المحمية، كما هو موضح في هذه الصورة، لتحديد الشبكات الفرعية التي يجب تشفيرها في شبكة VPN هذه.



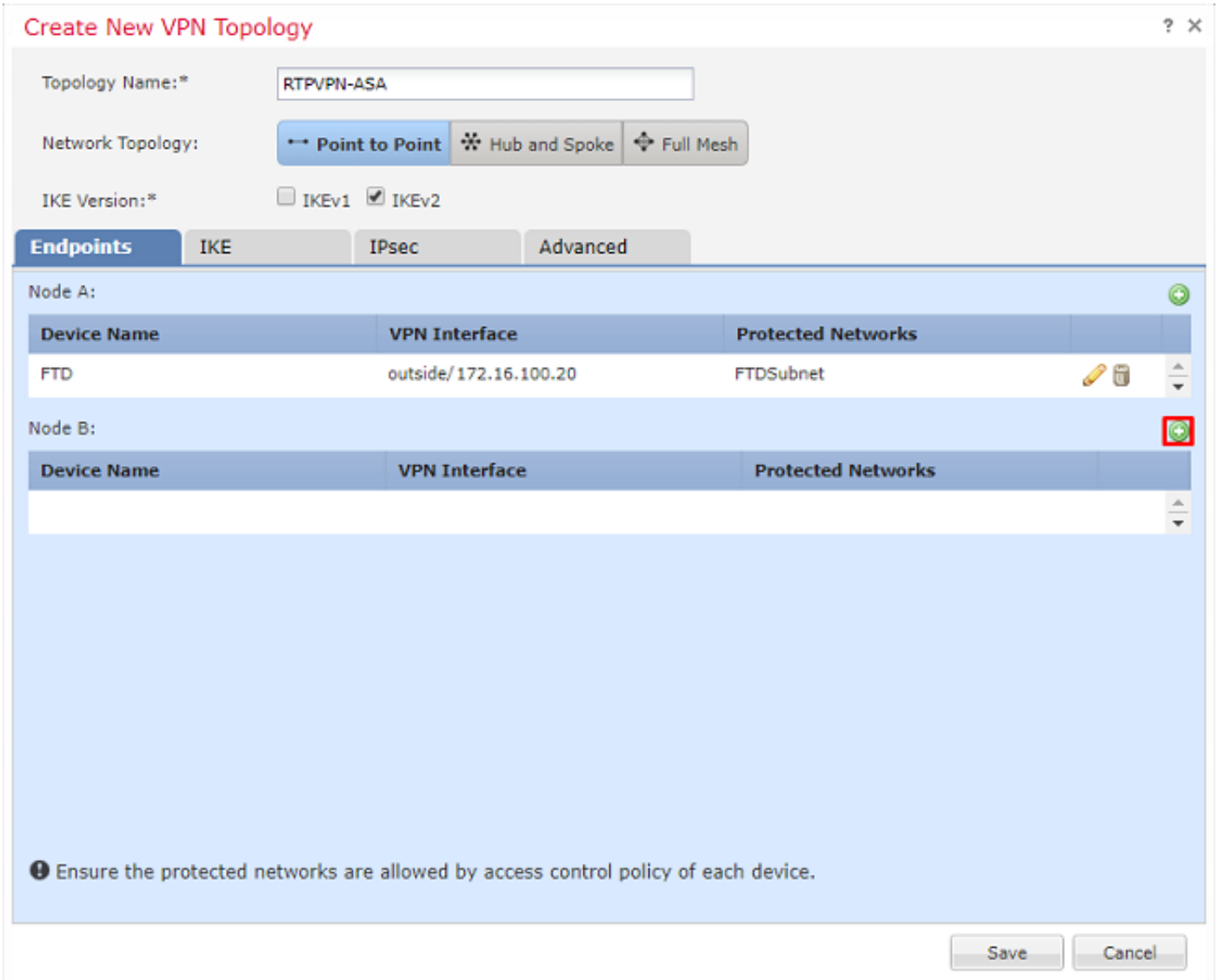
4. انقر على Green Plus وسيتم إنشاء كائن شبكة هنا.

5. أضف جميع الشبكات الفرعية المحلية إلى FTD التي يلزم تشفيرها. انقر على إضافة لنقلهم إلى الشبكات المحددة. انقر الآن على موافق، كما هو موضح في هذه الصورة.

FTDSubnet = 10.10.113.0/24

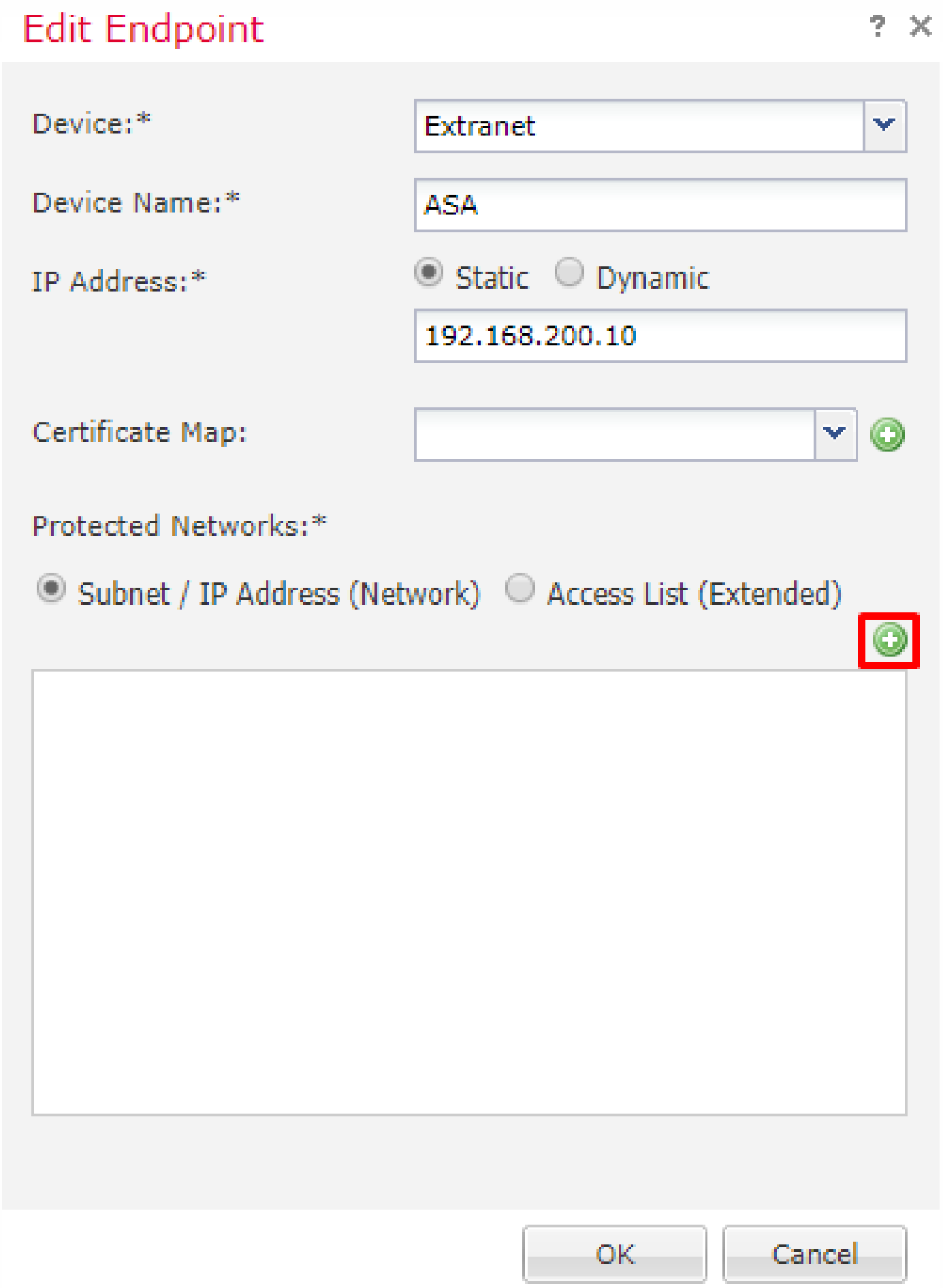


نقطة نهاية العقدة A: (FTD) مكتملة. انقر الأخضر الزائد للعقدة ب، كما هو موضح في الصورة.



العقدة B هي ASA. وتعتبر الأجهزة التي لا تتم إدارتها بواسطة FMC extranet.

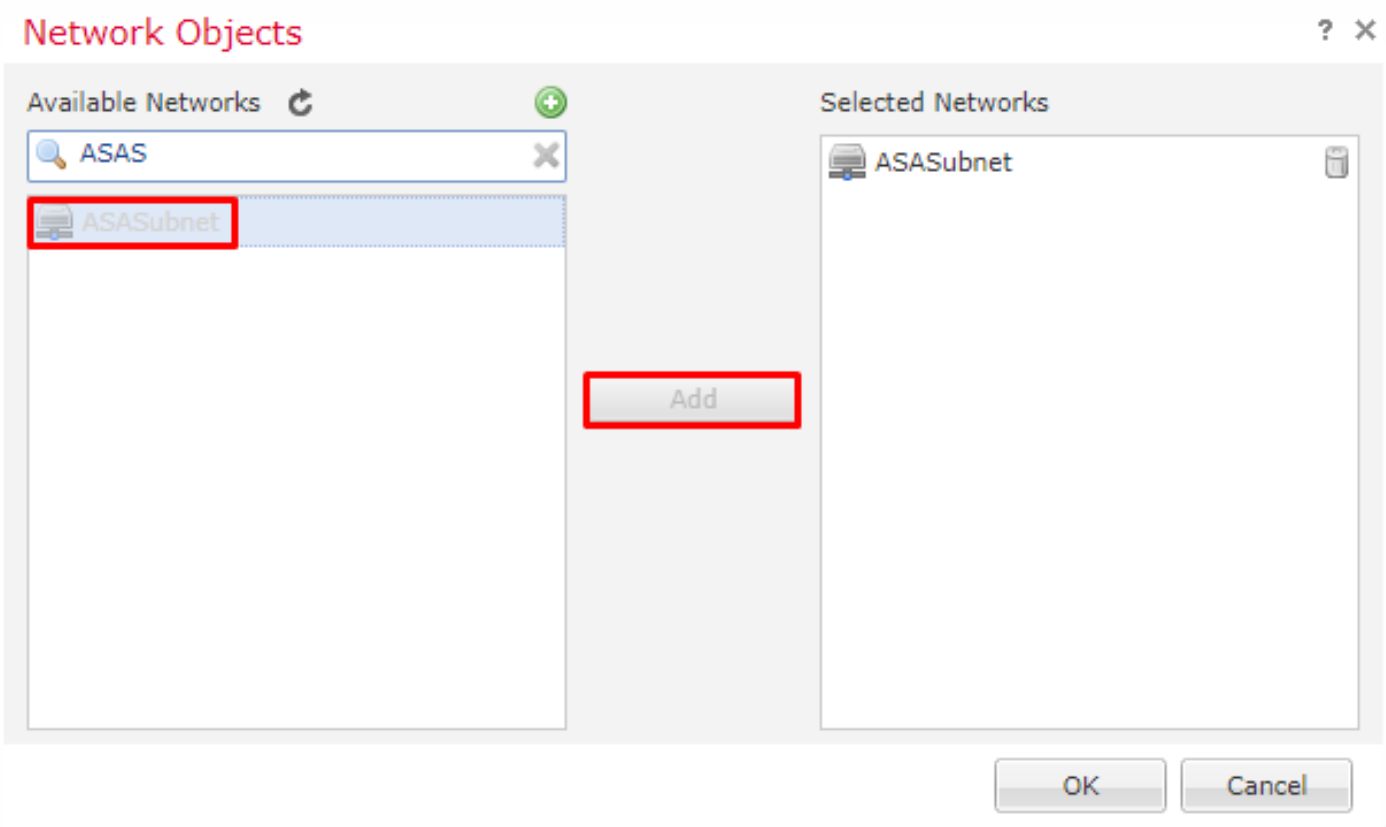
6. أضف اسم جهاز وعنوان IP. انقر فوق الأخضر الإضافي لإضافة شبكات محمية، كما هو موضح في الصورة.



7. كما هو موضح في هذه الصورة، حدد شبكات ASA الفرعية التي يلزم تشفيرها وإضافتها

إلى الشبكات المحددة.

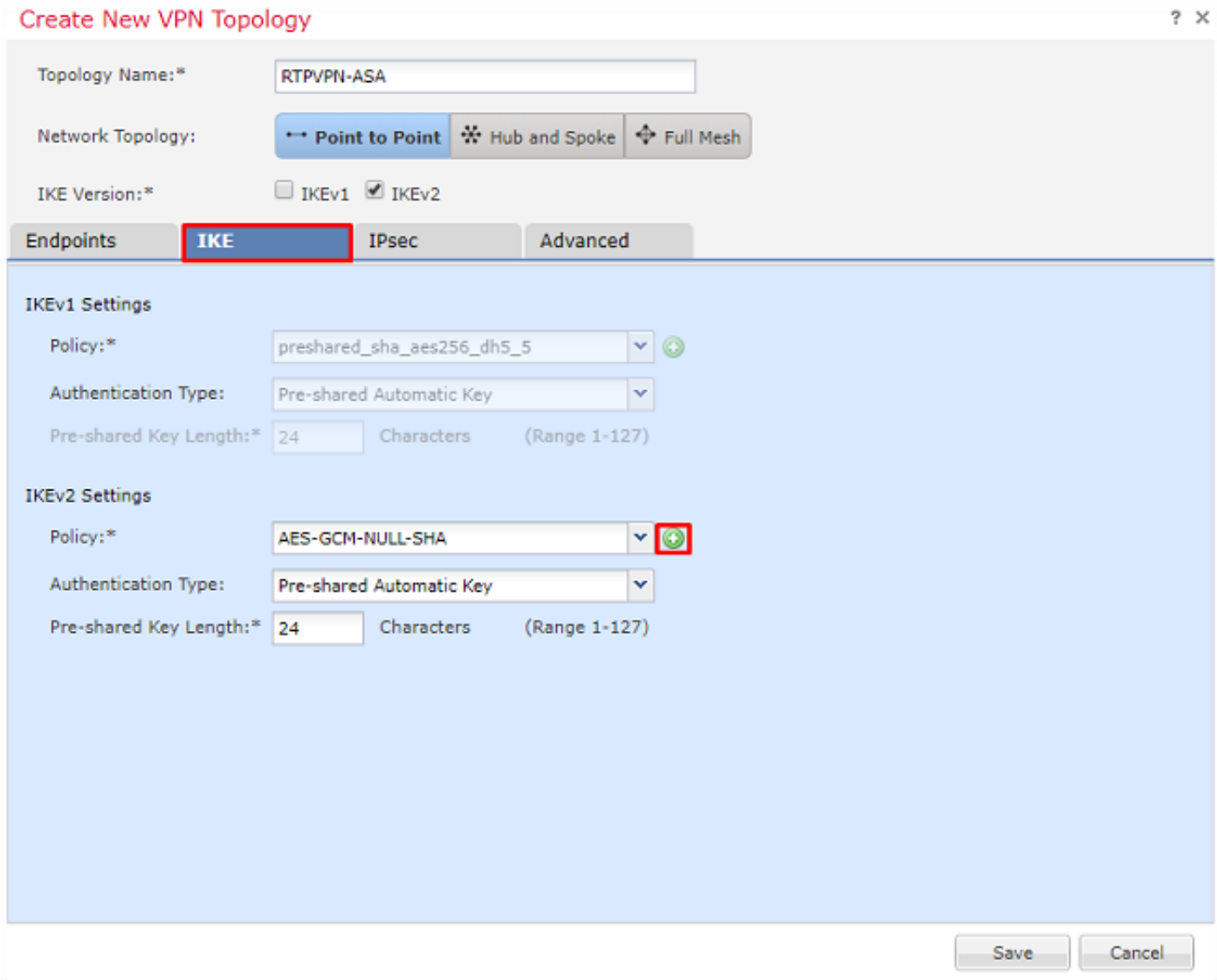
ASASubnet = 10.10.110.0/24



الخطوة 2. تكوين معلمات IKE.

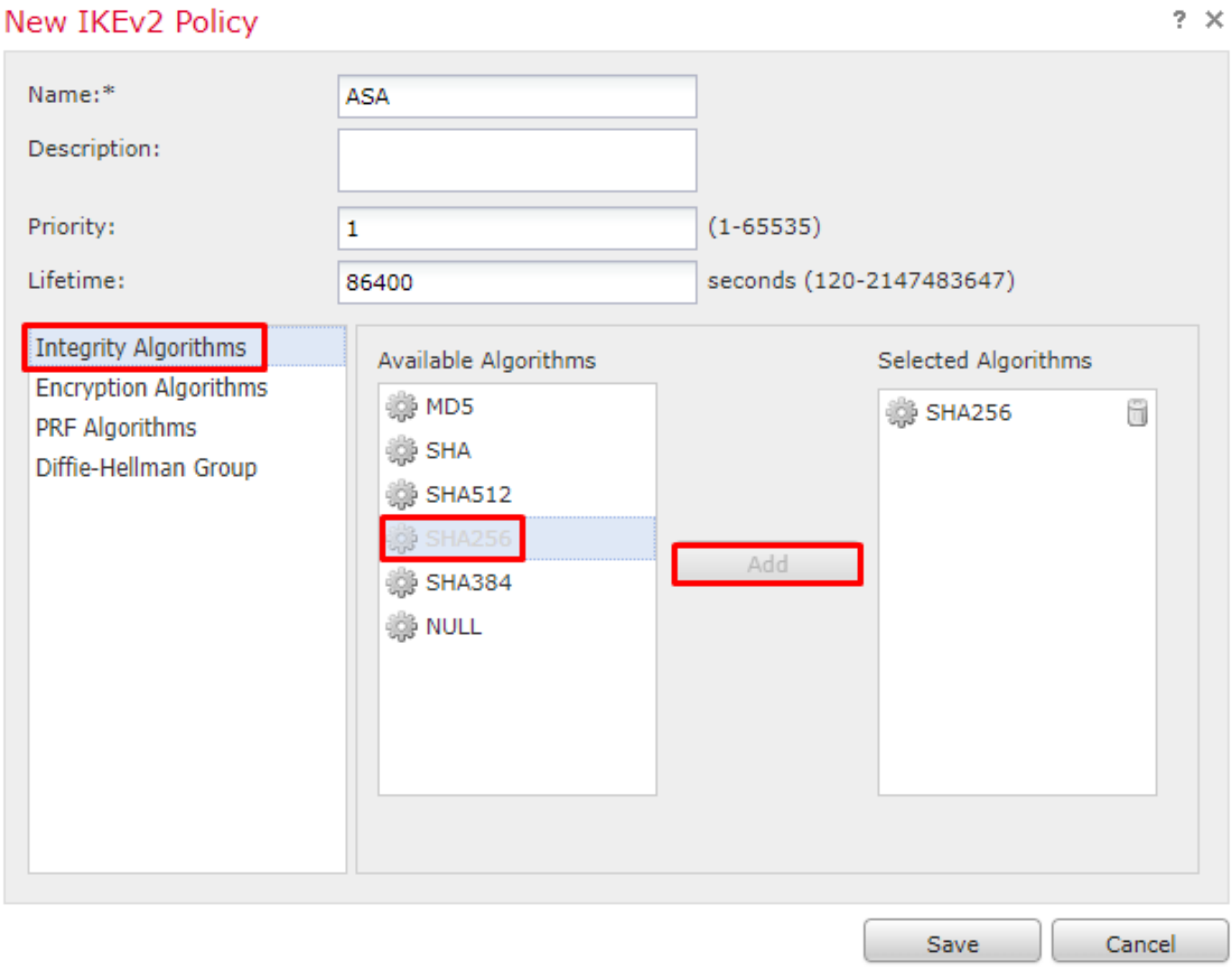
الآن كلتا نقطتي النهاية في موضعهما وتمر عبر تكوين IKE/IPSec.

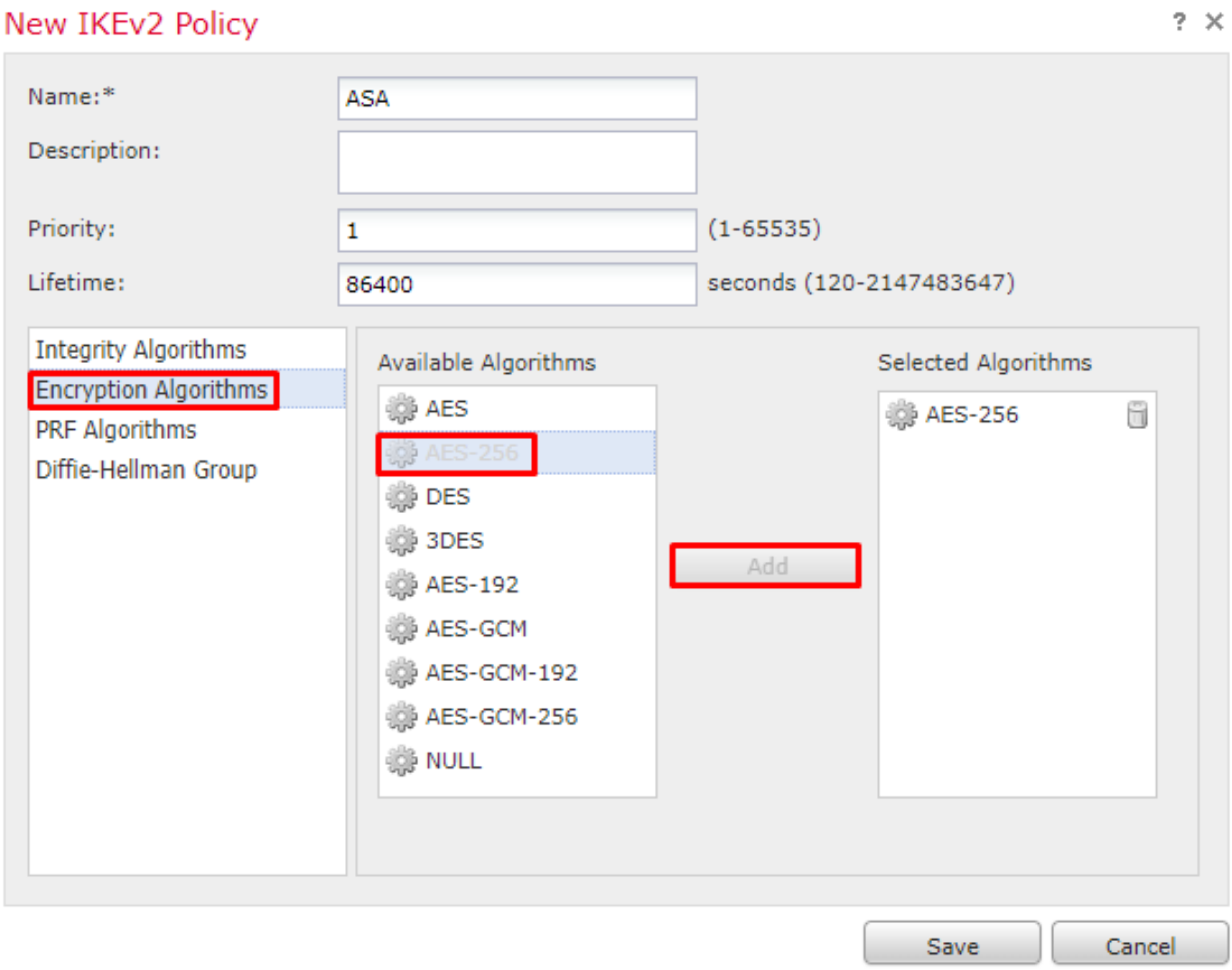
1. تحت علامة التبويب IKE، حدد المعلمات المستخدمة للتبادل الأولي ل IKEv2. انقر فوق علامة الجمع الخضراء لإنشاء سياسة IKE جديدة، كما هو موضح في الصورة.

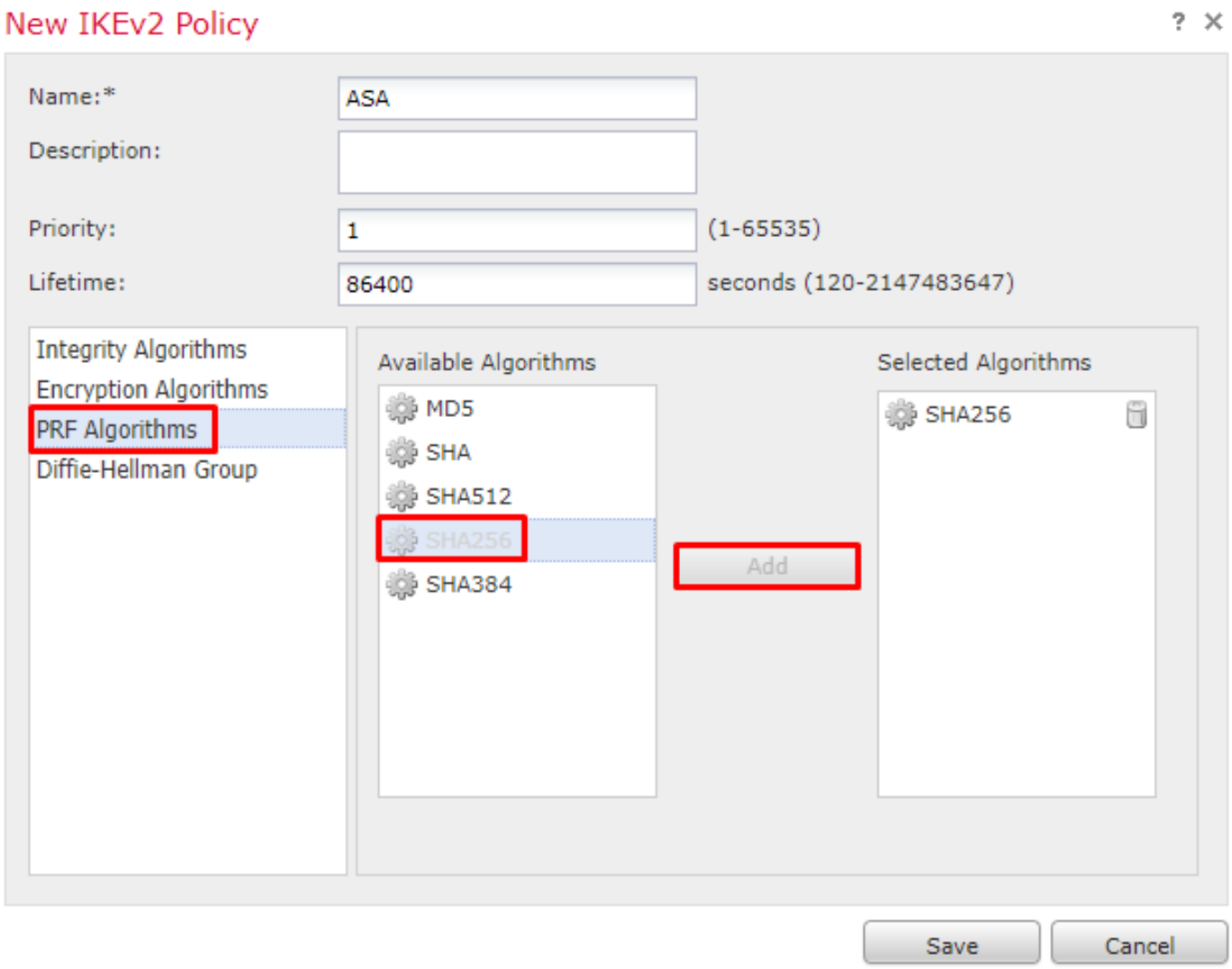


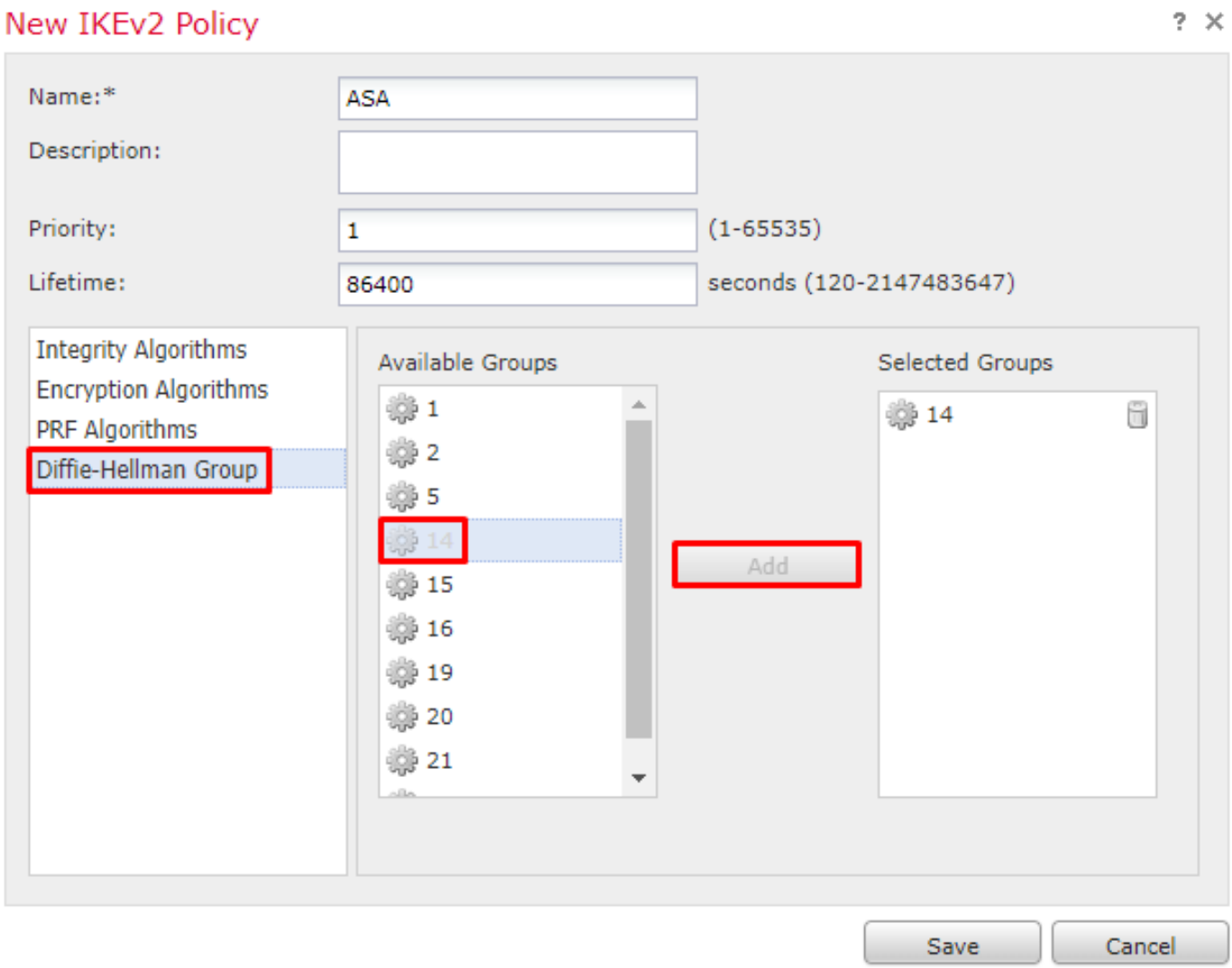
2. في سياسة IKE الجديدة، حدد رقم الأولوية وكذلك عمر المرحلة 1 من الاتصال. يستخدم هذا المستند هذه المعلمات للتبادل الأولي: Integrity (SHA256) والتشفير (AES-256) و PRF (SHA256) ومجموعة Diffie-Hellman (المجموعة 14)

ملاحظة: يتم إرسال جميع سياسات IKE على الجهاز إلى النظير البعيد بغض النظر عما هو موجود في قسم النهج المحدد. سيتم تحديد أول نهج IKE المتطابق مع النظير البعيد لاتصال VPN. أختر النهج الذي يتم إرساله أولا باستخدام حقل الأولوية. سيتم إرسال الأولوية 1 أولا.


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
NULL
Add
Selected Algorithms
SHA256
Save
Cancel

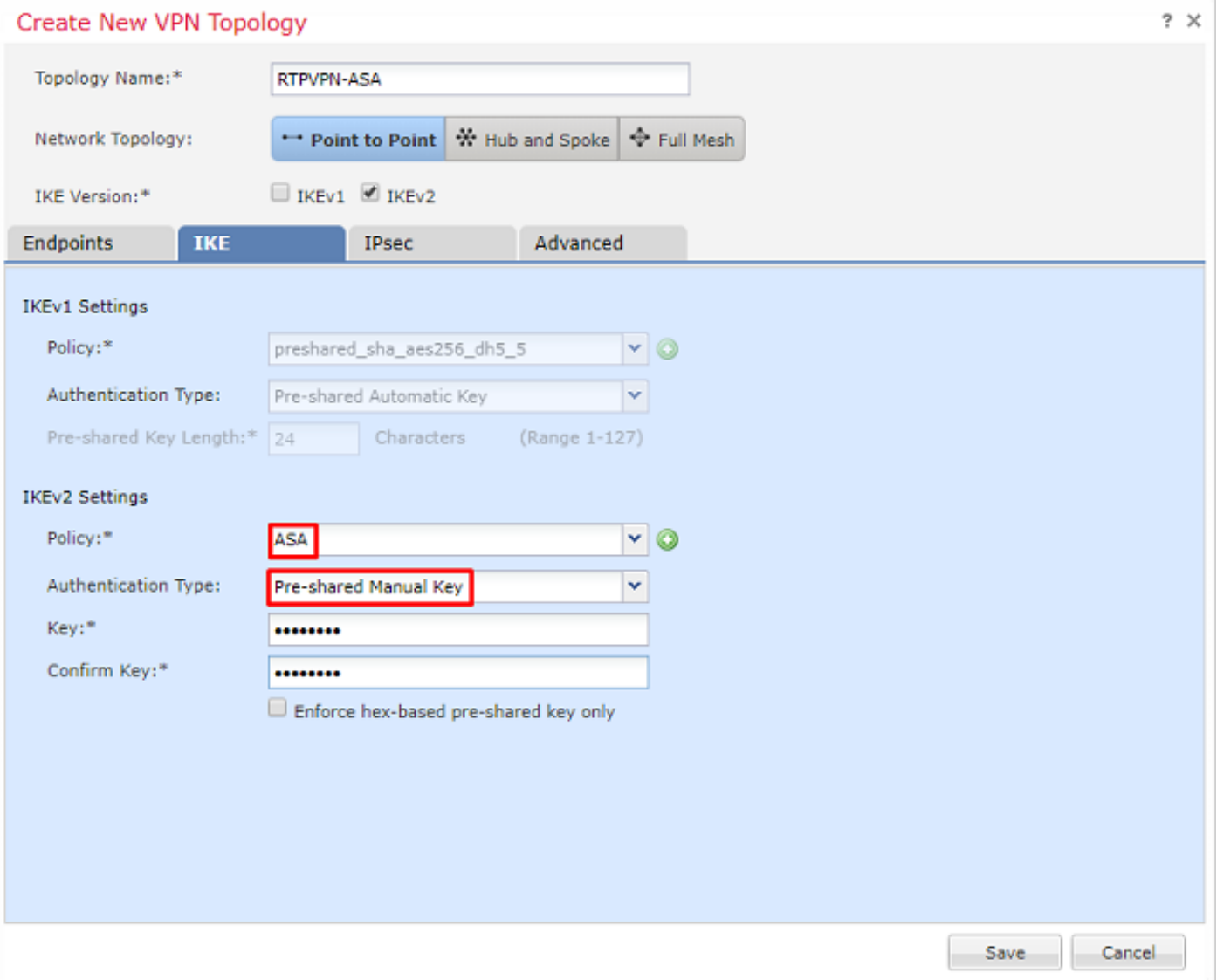

New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms
AES-256
Save
Cancel


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
Add
Selected Algorithms
SHA256
Save
Cancel



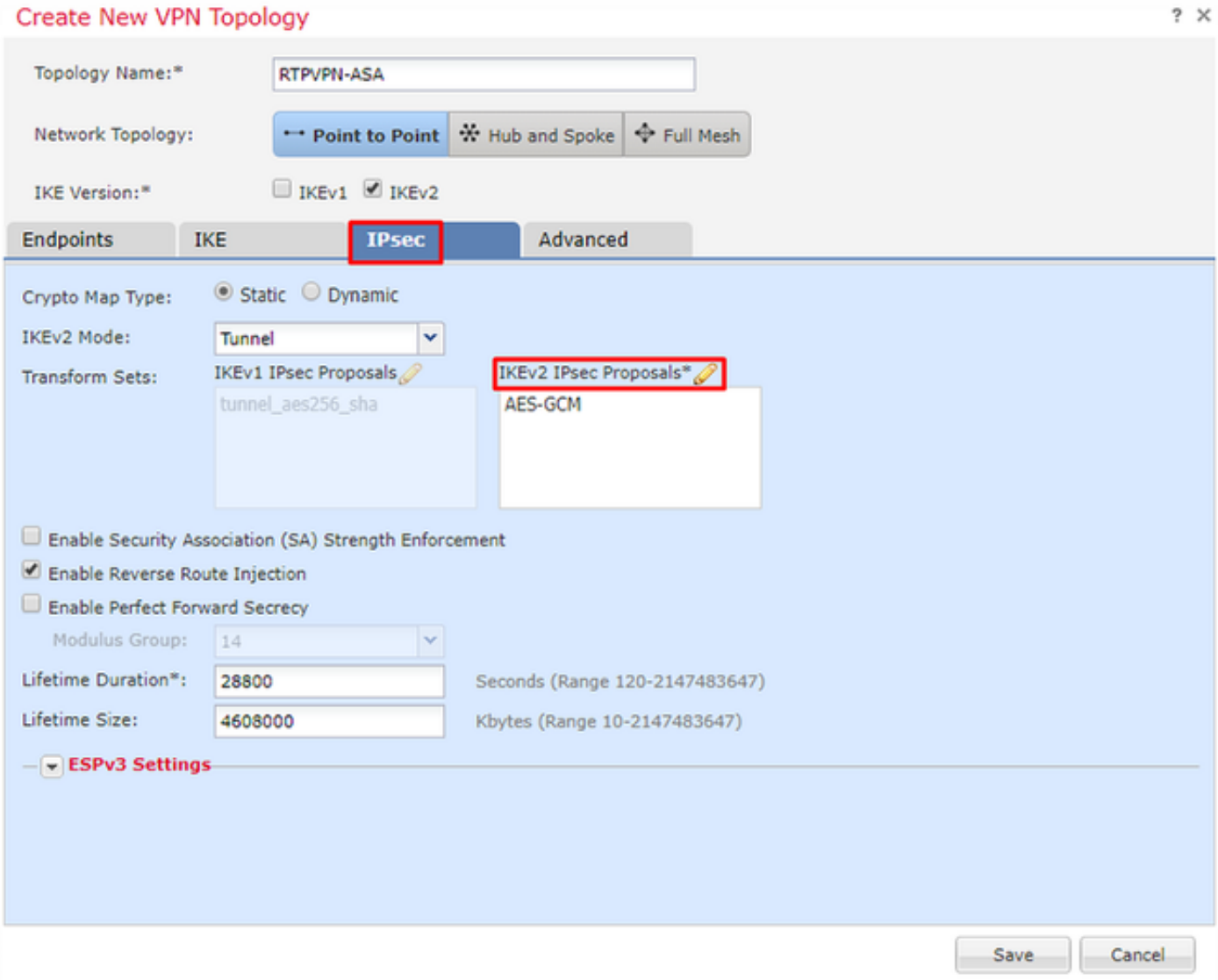
3. بمجرد إضافة المعلمات، حدد هذا النهج واختر نوع المصادقة.

4. أختر دليل المفاتح المشترك مسبقا. ل هذا وثيقة، ال PSK Cisco123 استعملت.



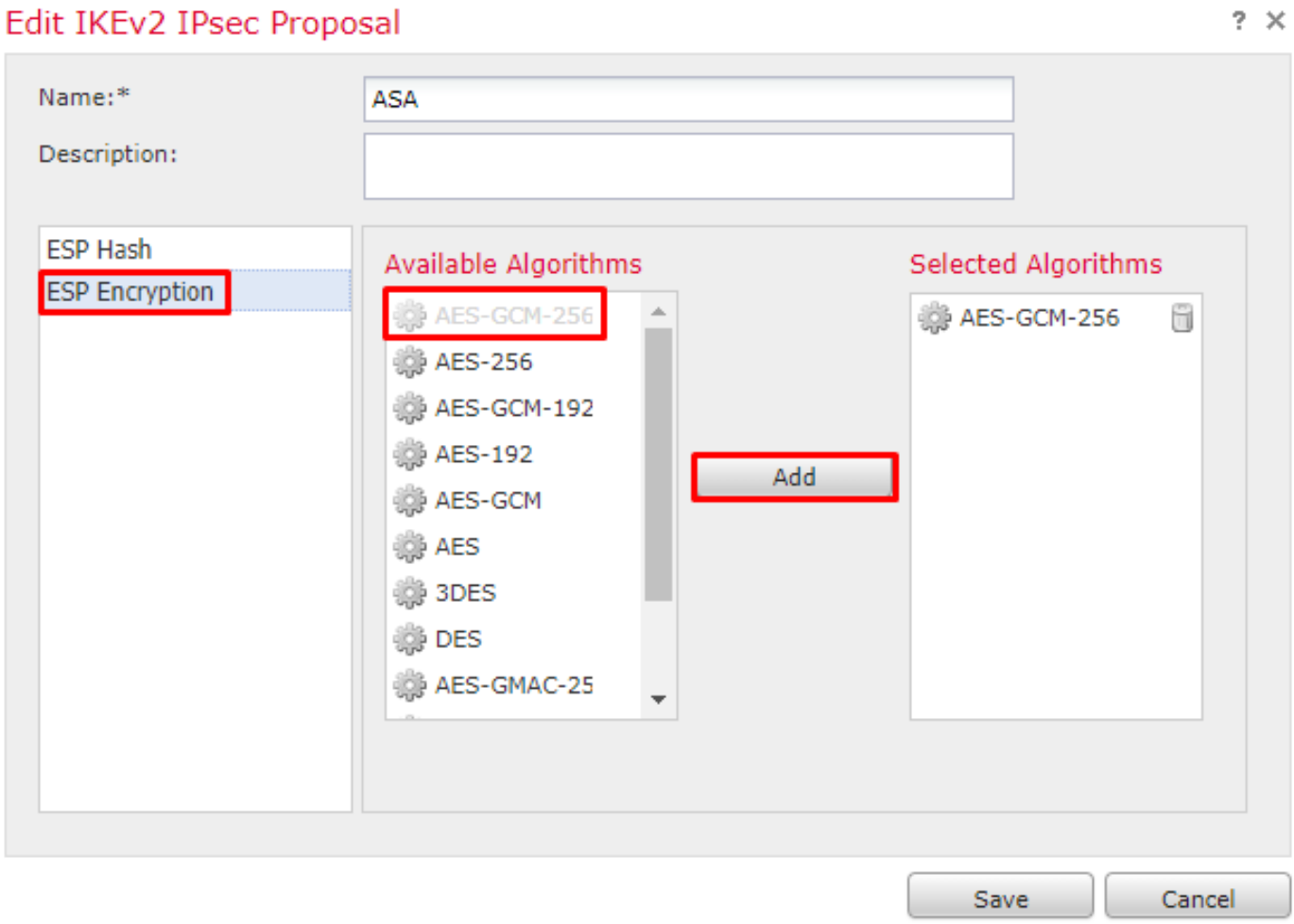
الخطوة 3. تكوين معلمات IPsec.

1. تحت IPsec، انقر فوق القلم الرصاص لتحرير مجموعة التحويل وإنشاء مقترح IPsec جديد، كما هو موضح في هذه الصورة.

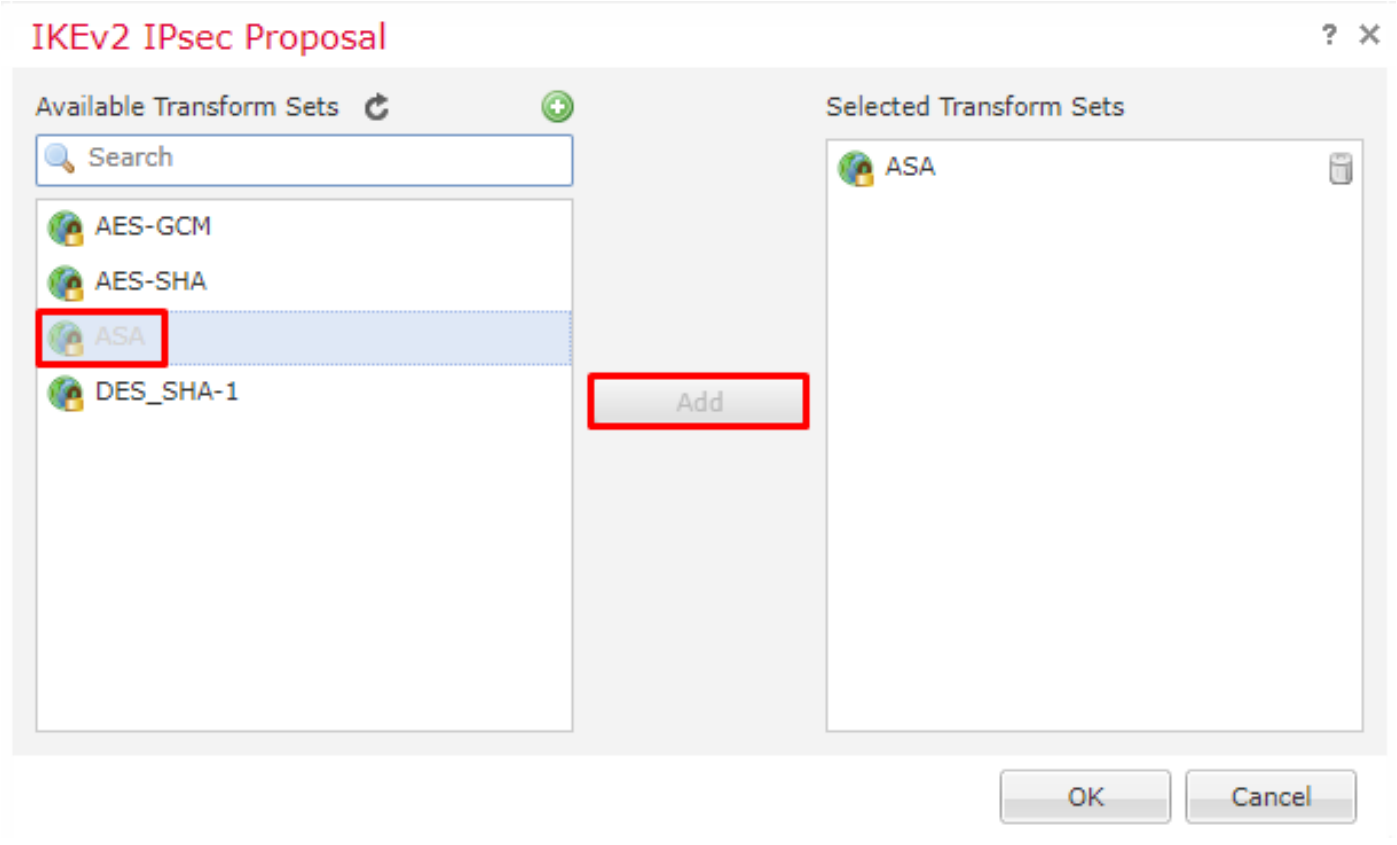


2. من أجل إنشاء مقترح IKEv2 IPsec جديد، انقر فوق علامة Green Plus وقم بإدخال معلمات المرحلة 2.

حدد تشفير ESP > AES-GCM-256. عند إستخدام خوارزمية GCM للتشفير، لا تكون هناك حاجة إلى خوارزمية التجزئة. باستخدام GCM تكون دالة التجزئة مضمنة.

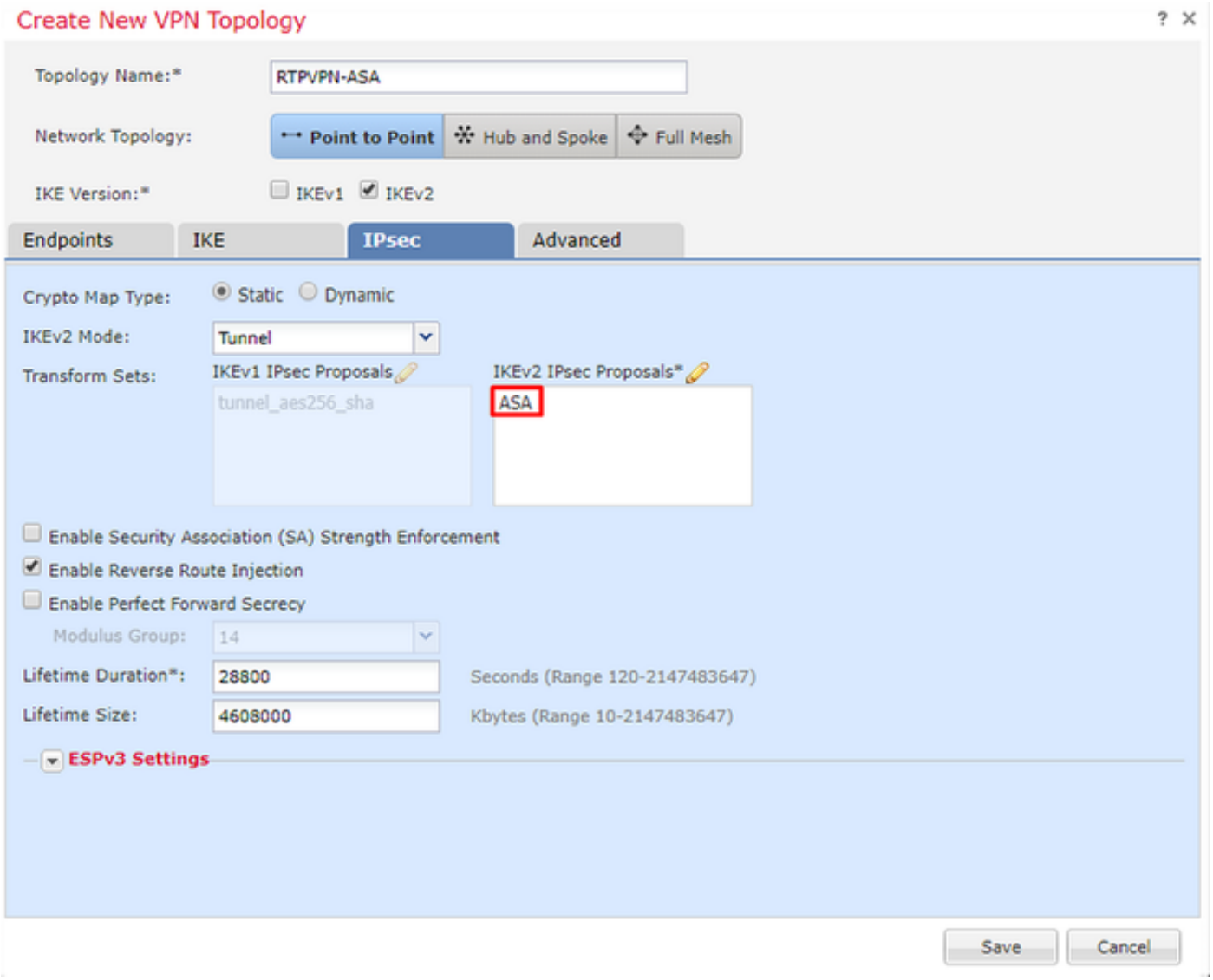


3. بمجرد إنشاء مقترح IPsec الجديد، أضفه إلى مجموعات التحويل المحددة.



تم إدراج مقترح IPsec المحدد حديثا الآن ضمن مقترحات IKEv2 IPsec.

إن تطلب الأمر، يمكن تحرير عمر المرحلة 2 وملفات PFS هنا. على سبيل المثال، سيتم ضبط العمر الافتراضي على أنه افتراضي و PFS معطل.

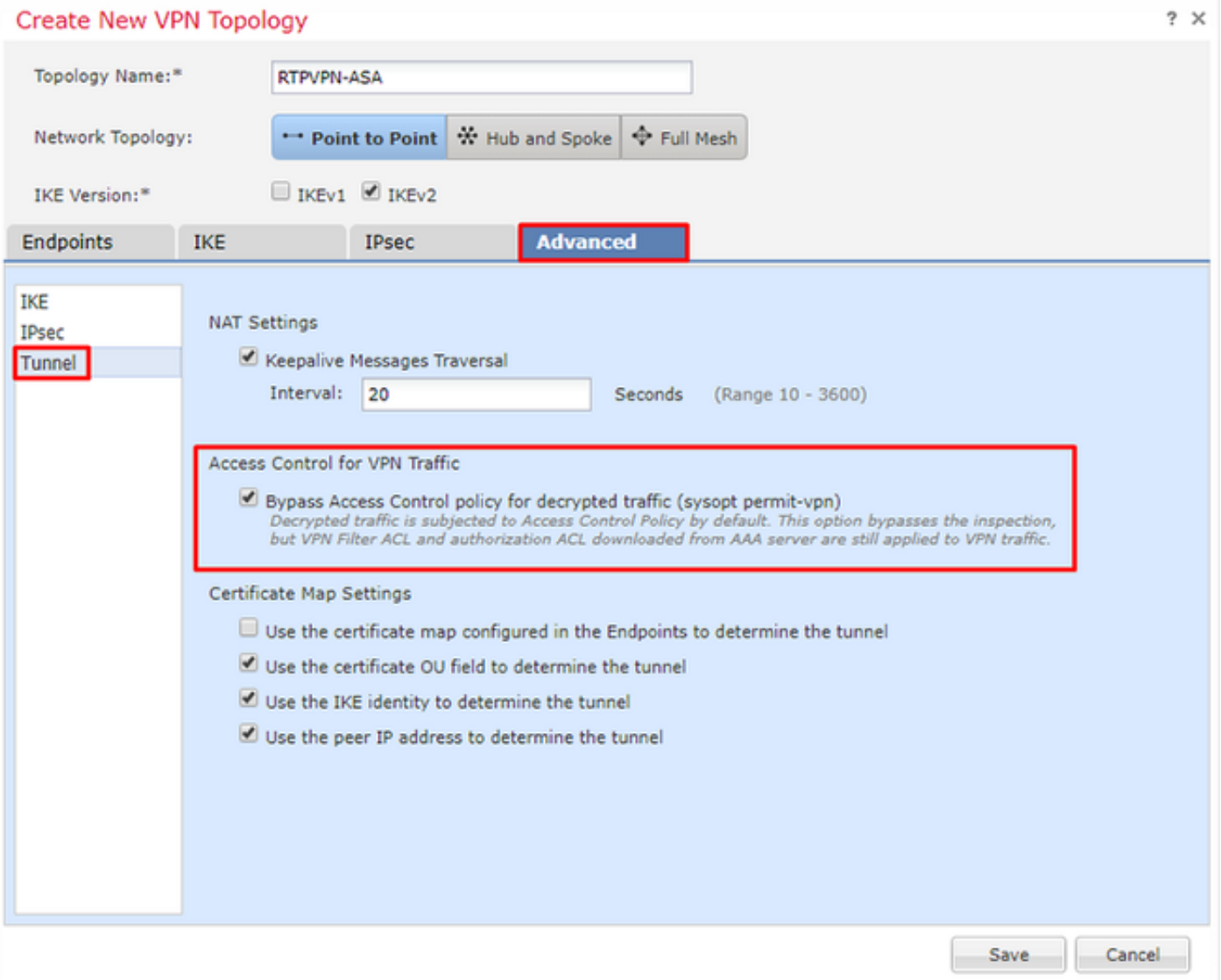


إختياري- يجب عليك إما إكمال الخيار لتجاوز التحكم في الوصول أو إنشاء سياسة التحكم في الوصول.

الخطوة 4. تجاوز التحكم في الوصول.

إختياري، يمكن تمكين sysopt allowed-vpn ضمن المتقدم > نفق.

يؤدي هذا إلى إزالة إمكانية إستخدام نهج التحكم في الوصول لفحص حركة المرور القادمة من المستخدمين. لا يزال يمكن إستخدام عوامل تصفية VPN أو قوائم التحكم في الوصول (ACL) القابلة للتنزيل لتصفية حركة مرور المستخدم. هذا أمر عام وسيتم تطبيقه على كل VPNs إذا تم تمكين خانة الاختيار هذه.

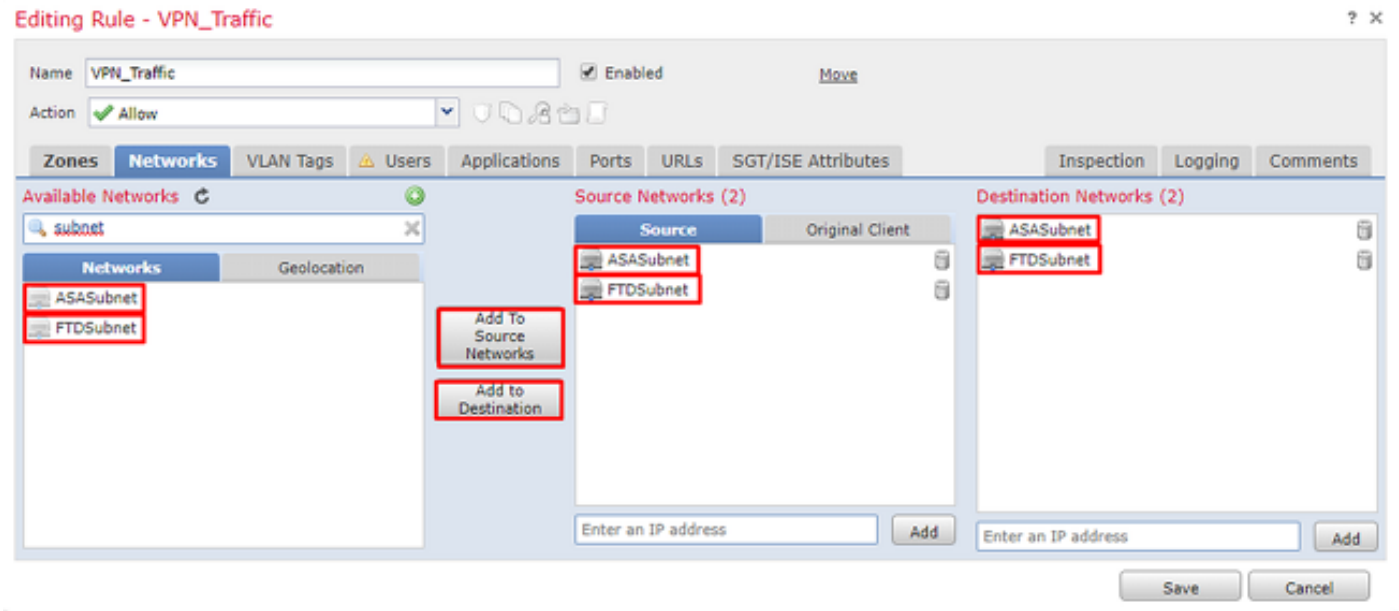


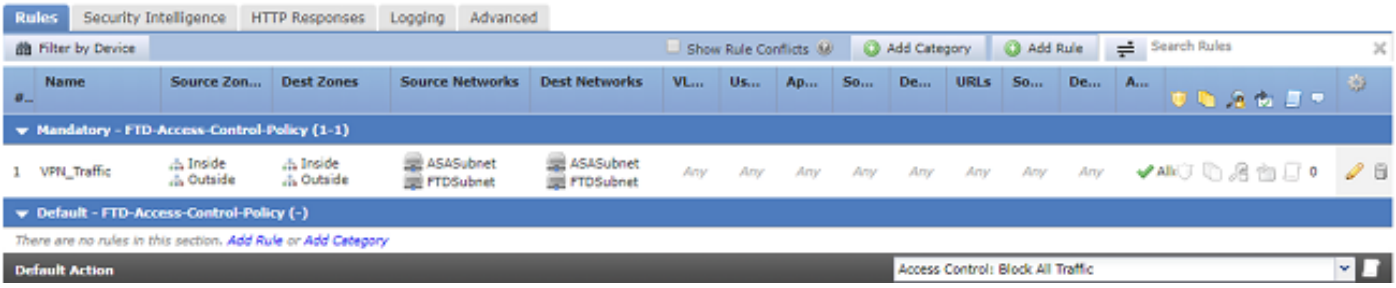
إذا لم يتم تمكين sysopt allowed-vpn بعد ذلك يجب إنشاء سياسة التحكم في الوصول للسماح بحركة مرور VPN من خلال جهاز FTD. في حالة تمكين sysopt allowed-vpn، يتم تخطي إنشاء سياسة التحكم في الوصول.

الخطوة 5. إنشاء سياسة للتحكم في الوصول.

تحت سياسات التحكم في الوصول، انتقل إلى السياسات > التحكم في الوصول > التحكم في الوصول وحدد السياسة التي تستهدف جهاز FTD. لإضافة قاعدة، انقر فوق إضافة قاعدة، كما هو موضح في الصورة هنا.

يجب السماح بحركة المرور من الشبكة الداخلية إلى الشبكة الخارجية ومن الشبكة الخارجية إلى الشبكة الداخلية. قم بإنشاء قاعدة واحدة للقيام بكل القاعدتين أو قم بإنشاء قاعدتين لإبقائهما منفصلين. في هذا المثال، يتم إنشاء قاعدة واحدة للقيام بالأمرين معا.

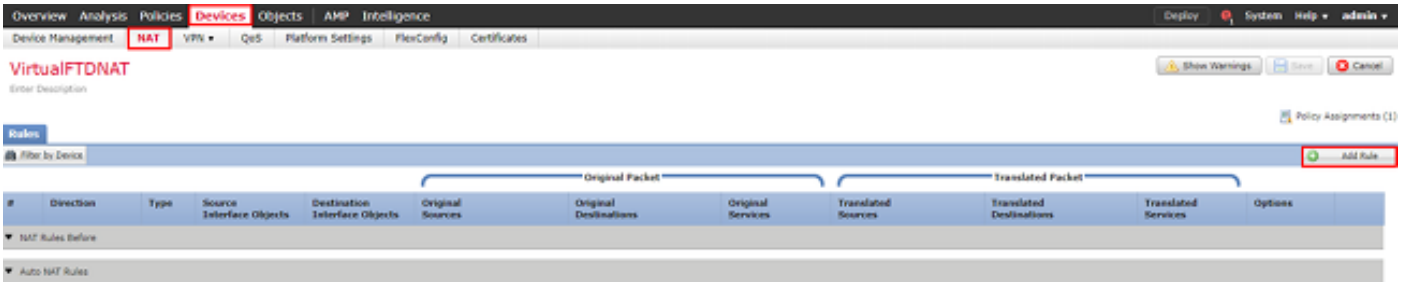




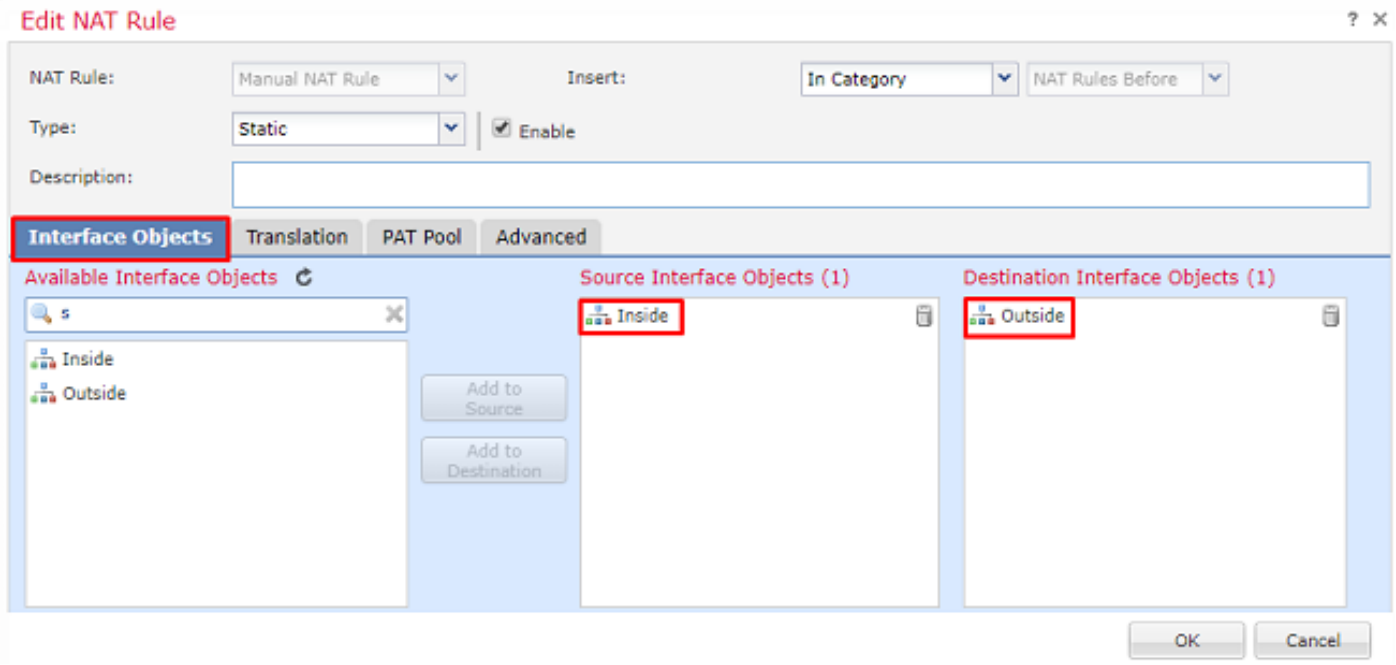
الخطوة 6. تكوين إستثناء NAT.

شكلت NAT إعفاء بيان ل ال VPN حركة مرور. يجب أن يكون إستثناء NAT في مكانه لمنع حركة مرور VPN من الوصول إلى بيان NAT آخر وترجمة حركة مرور VPN بشكل غير صحيح.

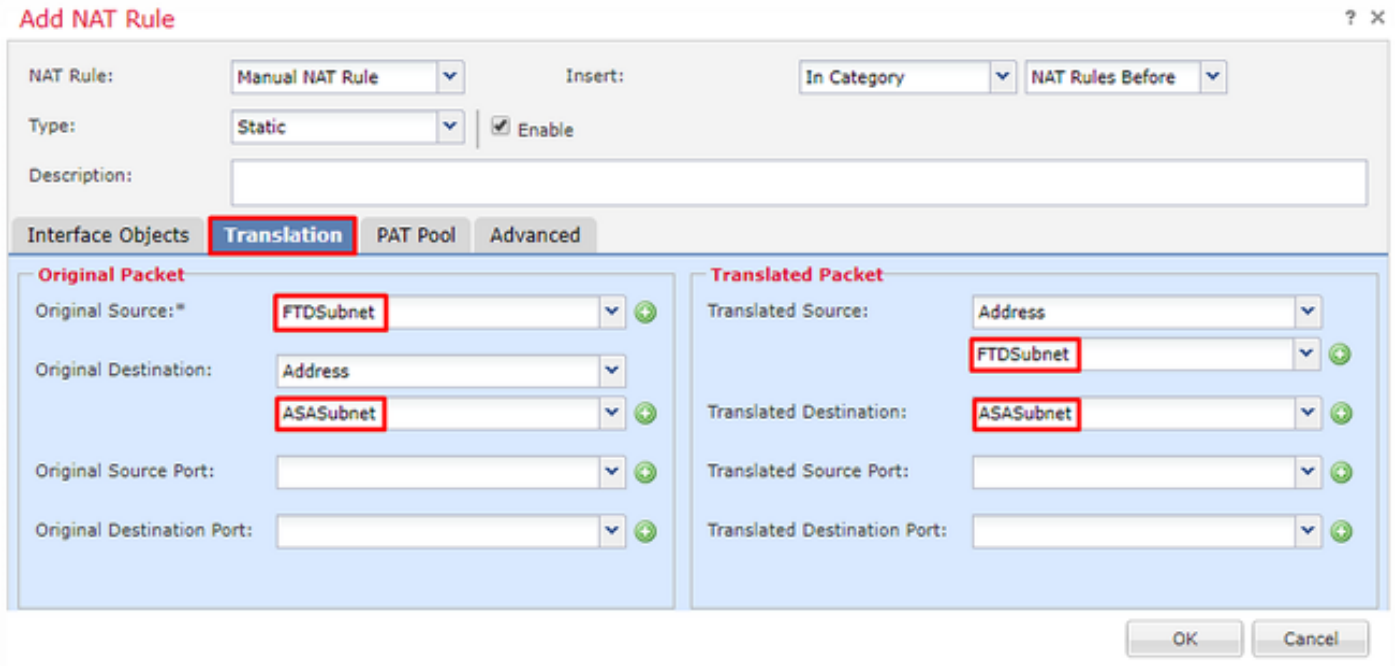
1. انتقل إلى الأجهزة > NAT، وحدد سياسة NAT التي تستهدف FTD. قم بإنشاء قاعدة جديدة أثناء النقر فوق الزر إضافة قاعدة.



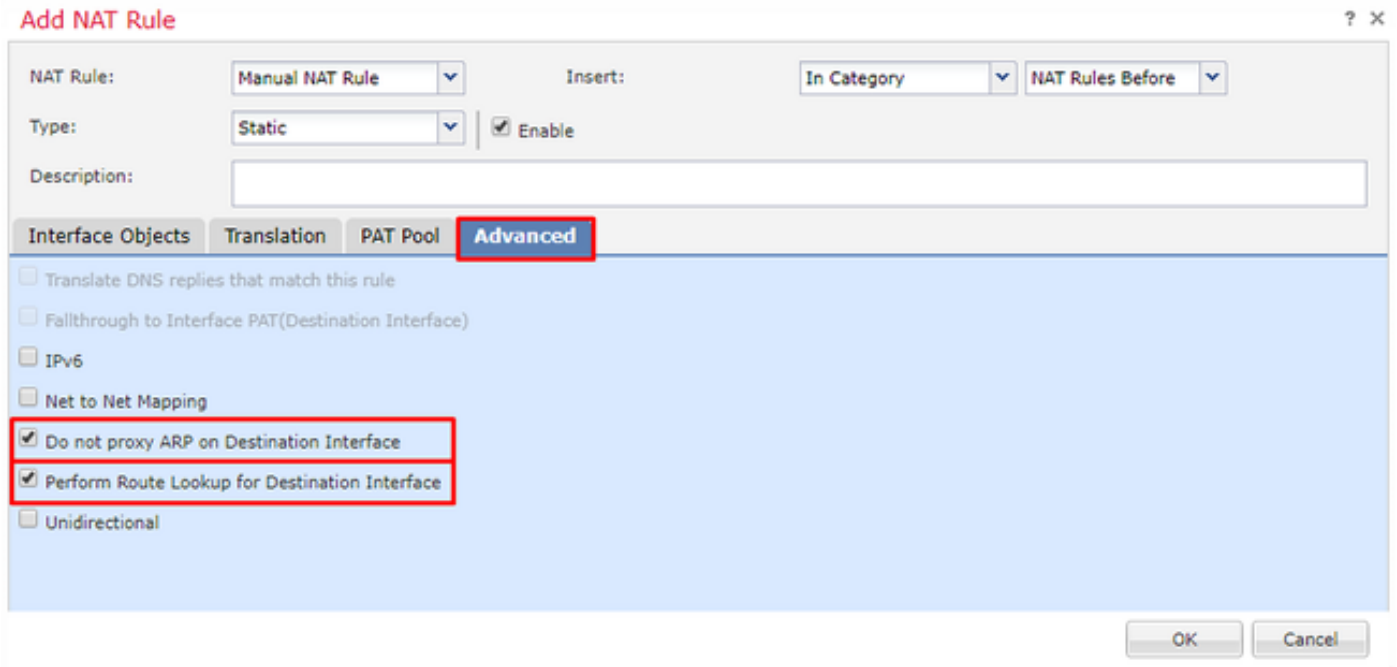
2. قم بإنشاء قاعدة ثابتة جديدة ل NAT في الدليل. الإشارة إلى الواجهات الداخلية والخارجية.



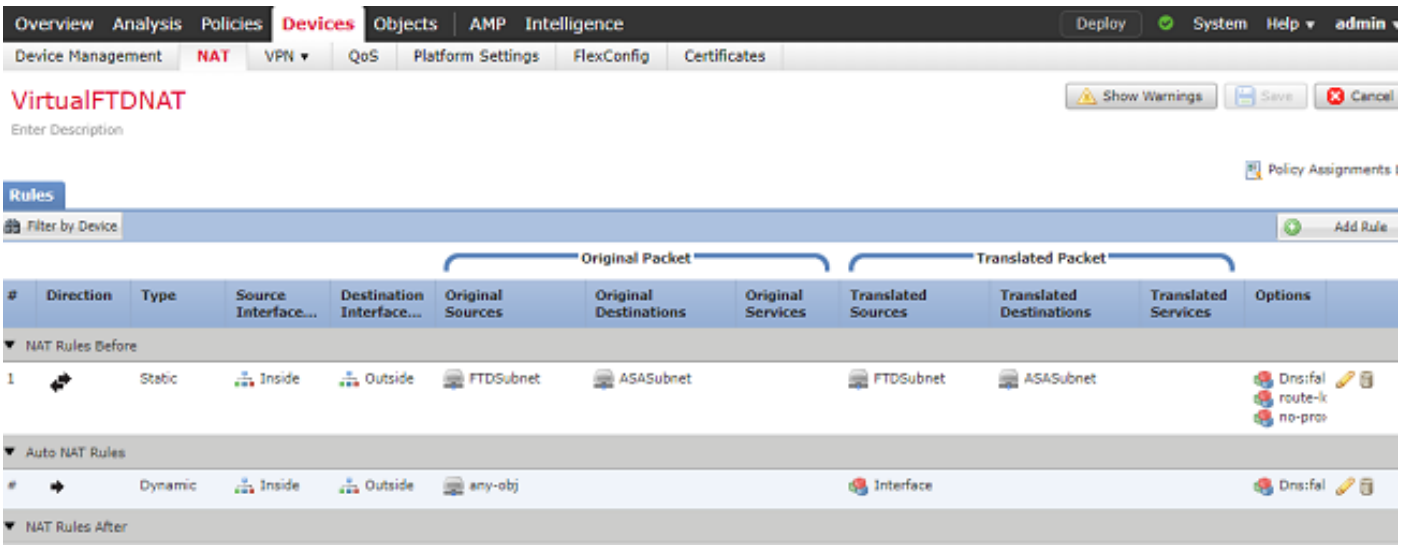
3. تحت علامة التبويب ترجمة وحدد الشبكات الفرعية المصدر والوجهة. بما أن هذه قاعدة إستثناء NAT، أجعل المصدر/الوجهة الأصلية والمصدر/الوجهة المترجمة متشابهين، كما هو موضح في هذه الصورة:



4. أخيرا، انتقل إلى علامة التبويب خيارات متقدمة وتمكين no-proxy-arp و route-lookup.



5. احفظ هذه القاعدة وانظر إلى النتائج النهائية في قائمة nat.



6. بمجرد اكتمال التكوين، قم بحفظ التكوين ونشره إلى FTD.

الخطوة 7. قم بتكوين ASA.

1. مكنت IKEv2 على القارن خارجي من ال ASA:

```
Crypto ikev2 enable outside
```

2. قم بإنشاء نهج IKEv2 الذي يحدد نفس المعلمات التي تم تكوينها على FTD:

```
Crypto ikev2 policy 1
```

```
 Encryption aes-256
 Integrity sha256
 Group 14
 Prf sha256
 Lifetime seconds 86400
```

3. إنشاء سياسة مجموعة تسمح ببروتوكول iKEV2:

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
 Vpn-tunnel-protocol ikev2
```

4. قم بإنشاء مجموعة أنفاق لعنوان IP العام لـ FTD النظير. راجع نهج المجموعة وحدد المفاتيح المشترك مسبقا:

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco123
 ikev2 remote-authentication pre-shared-key cisco123
```

5. قم بإنشاء قائمة وصول تحدد حركة المرور التي سيتم تشفيرها: (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSubnet
 Subnet 10.10.113.0 255.255.255.0
Object network ASASubnet
 Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. إنشاء مقترح ikev2 ipSec يشير إلى الخوارزميات المحددة في FTD:

```
Crypto ipsec ikev2 ipsec-proposal FTD
 Protocol esp encryption aes-gcm-256
```

7. قم بإنشاء إدخال خريطة تشفير ربط التكوين مع:

```
Crypto map outside_map 10 set peer 172.16.100.20
```

```
Crypto map outside_map 10 match address ASAtoFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. قم بإنشاء بيان إستثناء NAT الذي سيمنع حركة مرور VPN من أن تحدث بواسطة جدار الحماية:

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet no-
```

التحقق من الصحة

ملاحظة: في هذا الوقت، لا توجد طريقة لمراجعة حالة نفق VPN من وحدة التحكم في الوصول الخاصة (FMC). هناك طلب تعزيز لهذه القدرة CSCvh77603.

محاولة بدء حركة مرور البيانات من خلال نفق VPN. مع الوصول إلى سطر الأوامر من ASA أو FTD، يمكن القيام بذلك باستخدام أمر حزم tracer. عند إستخدام الأمر packet-tracer لعرض نفق VPN، يجب تشغيله مرتين للتحقق من ظهور النفق. أول مرة يتم إصدار الأمر فيها، يكون نفق VPN معطل، وبالتالي سيفشل الأمر packet-tracer مع تشفير VPN Drop. ال يستعمل العنوان داخلي من جدار الحماية بما أن المصدر عنوان في الربط-tracer بما أن هذا سوف يفشل دائما.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10

Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-
Additional Information:
```

```
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483 ifc ou
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
object-group network FMC_INLINE_src_rule_268436483
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
object-group network FMC_INLINE_dst_rule_268436483
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-
Additional Information:
Static translate 10.10.113.10/0 to 10.10.113.10/0

Phase: 10
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Result:
input-interface: Inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

in order to راقبت النفق وضع انتقل إلى ال CLI من ال FTD أو ASA.

من واجهة سطر الأوامر (CLI) الخاصة ب FTD تحقق من المرحلة 1 والمرحلة 2 باستخدام هذا الأمر:

show crypto ikev2 sa

<#root>

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:

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

Tunnel-id Local                                                 Remote
  9528731 172.16.100.20/500                                      192.168.200.10/500

 READY

   INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/118 sec
Child sa: local selector

10.10.113.0/0 - 10.10.113.255/65535


          remote selector

10.10.110.0/0 - 10.10.110.255/65535


          ESP spi in/out:

0x66be357d/0xb74c8753
```

أستكشاف الأخطاء وإصلاحها وتصحيح الأخطاء

مشكلات الاتصال الأولية

عند بناء شبكة خاصة ظاهرية، هناك جانبان يتفاوضان حول النفق. لذلك، من الأفضل الحصول على كلا جانبي المحادثة عند أستكشاف أي نوع من أنواع فشل النفق وإصلاحها. يمكن العثور على دليل تفصيلي حول كيفية تصحيح أخطاء أنفاق IKEv2 هنا: [كيفية تصحيح أخطاء شبكات IKEv2 VPNs]

أكثر سبب شائع لفشل النفق هو مشكلة توصيل. أفضل طريقة لتحديد هذا الإجراء هي التقاط حزم على الجهاز. أستخدم هذا الأمر لالتقاط حزم على الجهاز:

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

ما إن الإعتقالفي مكان، حاولت أن يرسل حركة مرور عبر ال VPN وفحصت ل ثنائي إتجاه حركة مرور في الربط التقاط.

راجع التقاط الحزمة باستخدام هذا الأمر:

إظهار كابتن

```
firepower# show cap capout

4 packets captured
```

```
1: 11:51:12.059628       172.16.100.20.500 > 192.168.200.10.500:  udp 690
2: 11:51:12.065243       192.168.200.10.500 > 172.16.100.20.500:  udp 619
3: 11:51:12.066692       172.16.100.20.500 > 192.168.200.10.500:  udp 288
4: 11:51:12.069835       192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

المشاكل الخاصة بحركة المرور

المشاكل الشائعة لحركة المرور التي تواجهها هي:

- مشاكل التوجيه خلف FTD — الشبكة الداخلية غير قادرة على توجيه الحزم مرة أخرى إلى عناوين IP المخصصة وعملاء VPN.
- قوائم التحكم في الوصول التي تمنع حركة المرور.
- لا يتم تجاوز ترجمة عنوان الشبكة لحركة مرور VPN.

لمزيد من المعلومات حول شبكات VPN على FTD الذي تتم إدارته بواسطة FMC، يمكنك العثور على دليل التكوين الكامل هنا: [دليل تكوين FMC الذي تتم إدارته بواسطة FTD]

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).