تكوين شبكة VPN من موقع إلى موقع على FTD المدارة بواسطة FDM

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين شبكة VPN من موقع إلى موقع على "الدفاع عن تهديد FirePOWER (FTD)" المدار بواسطة مدير أجهزة FirePOWER (FDM).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- المفهوم الأساسي للشبكة الخاصة الظاهرية (VPN)
- تجربة مع FDN
- تجربة مع سطر أوامر أجهزة الأمان المعدلة (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.

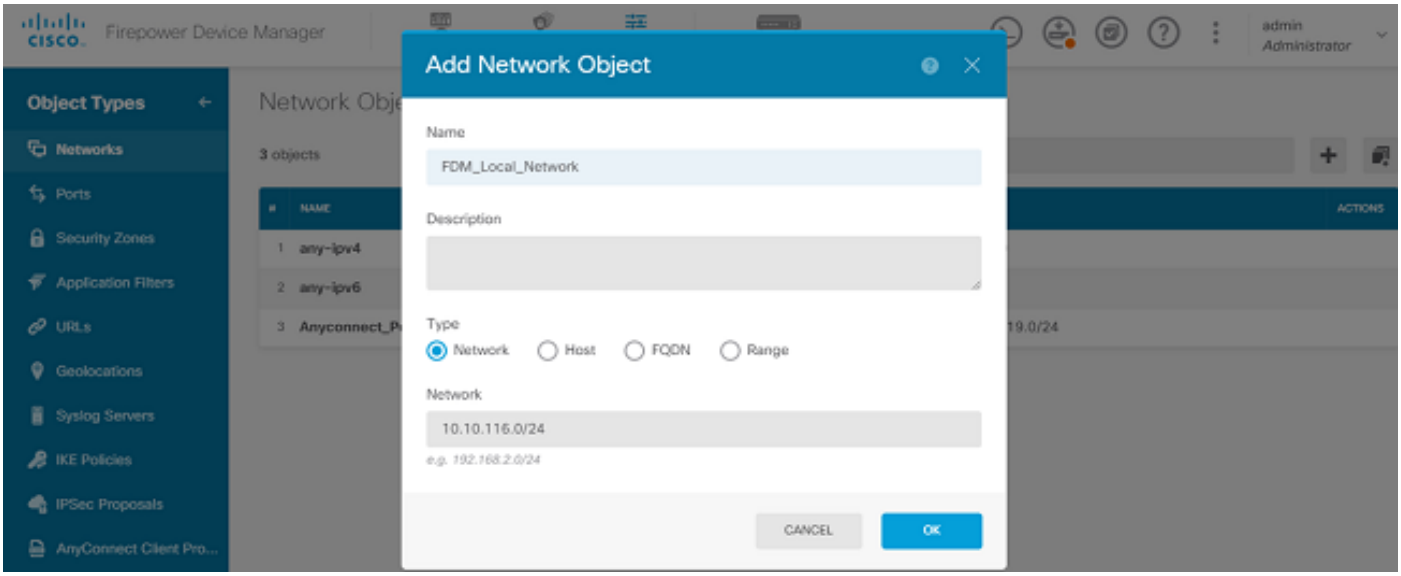
التكوين

ابدأ بالتكوين على FTD باستخدام FDM.

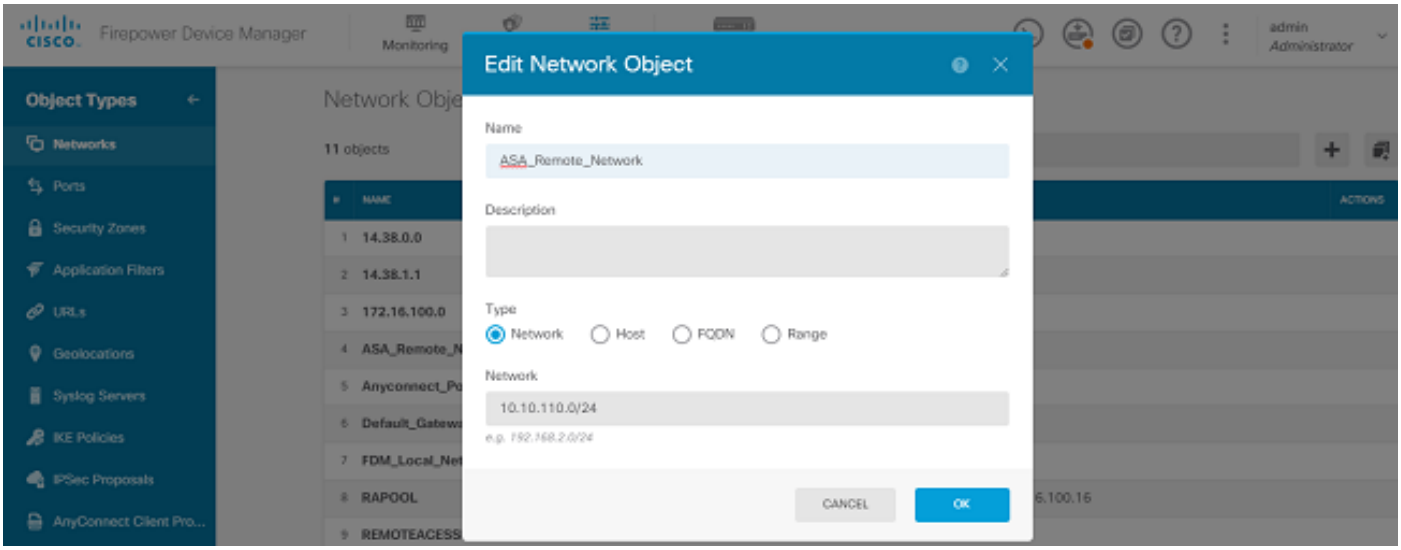
تعريف الشبكات المحمية

انتقل إلى كائنات > شبكات > إضافة شبكة جديدة..

قم بتكوين الكائنات لشبكات LAN من واجهة المستخدم الرسومية (GUI) لـ FDM. قم بإنشاء كائن للشبكة المحلية خلف جهاز FDM كما هو موضح في الصورة.



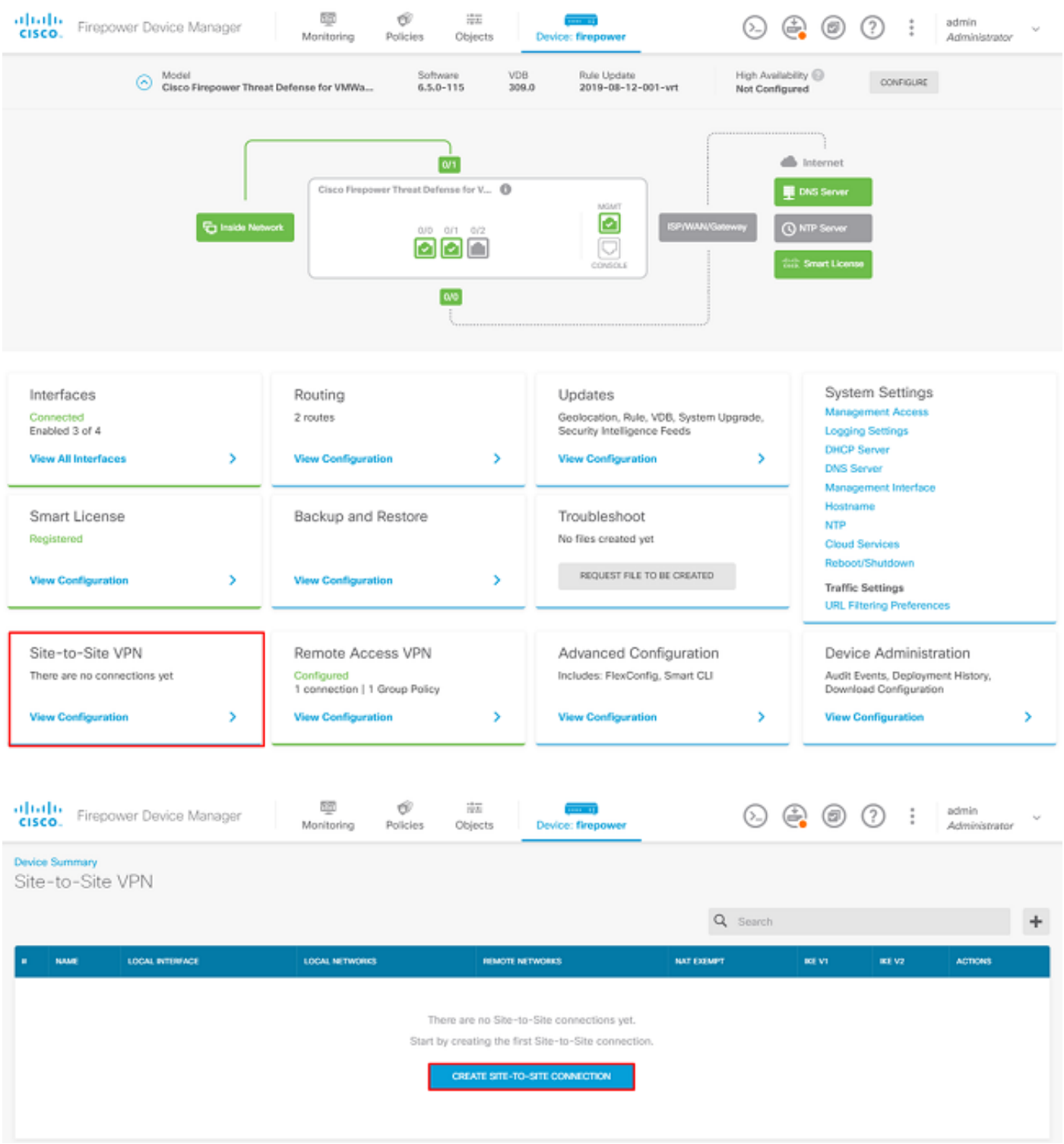
قم بإنشاء كائن للشبكة البعيدة خلف جهاز ASA كما هو موضح في الصورة.



تكوين شبكة VPN من موقع إلى موقع

انتقل إلى شبكة VPN من موقع إلى موقع > إنشاء اتصال من موقع إلى موقع.

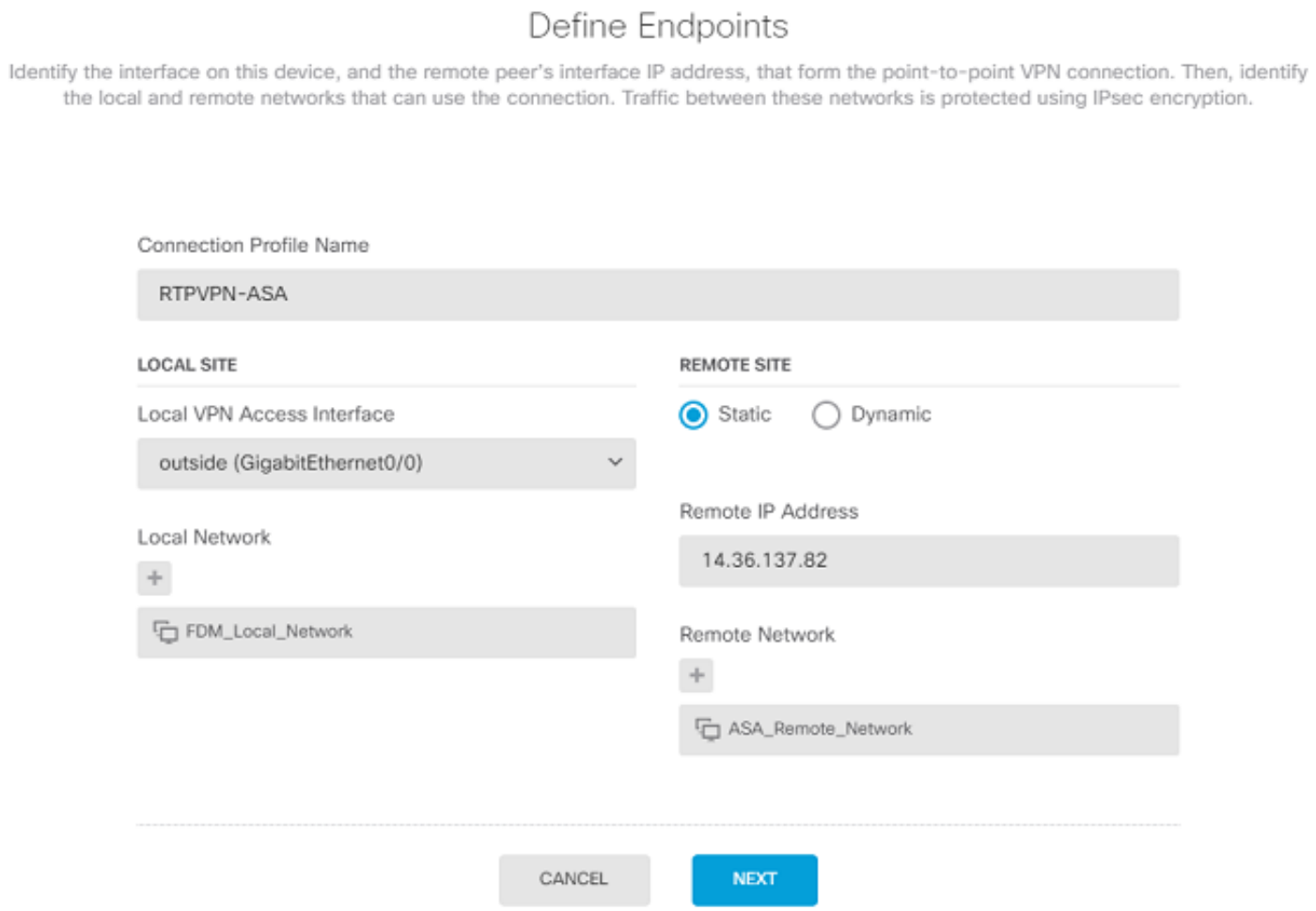
انتقل عبر معالج "من موقع إلى موقع" على FDM كما هو موضح في الصورة.



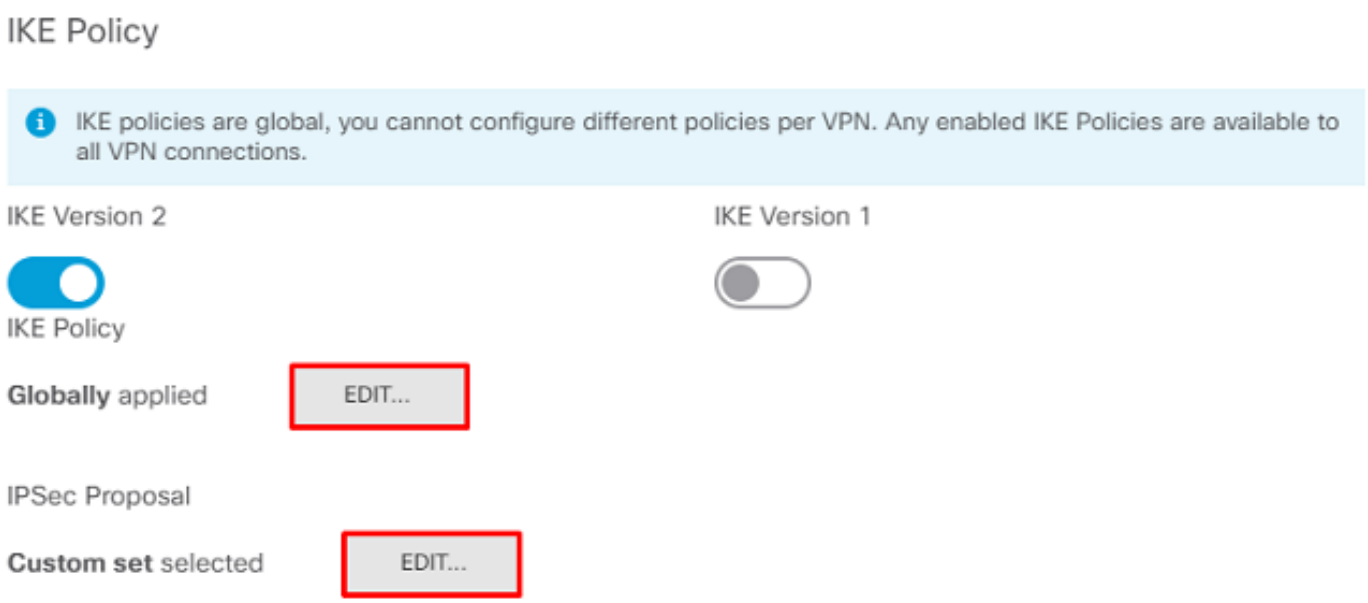
امنح الاتصال من موقع إلى موقع اسم ملف تعريف اتصال يسهل التعرف عليه.

أختر ال يصح قارن خارجي ل FTD وبعد ذلك أختر الشبكة محلي أن يحتاج أن يكون شفرت عبر الموقع إلى موقع VPN.

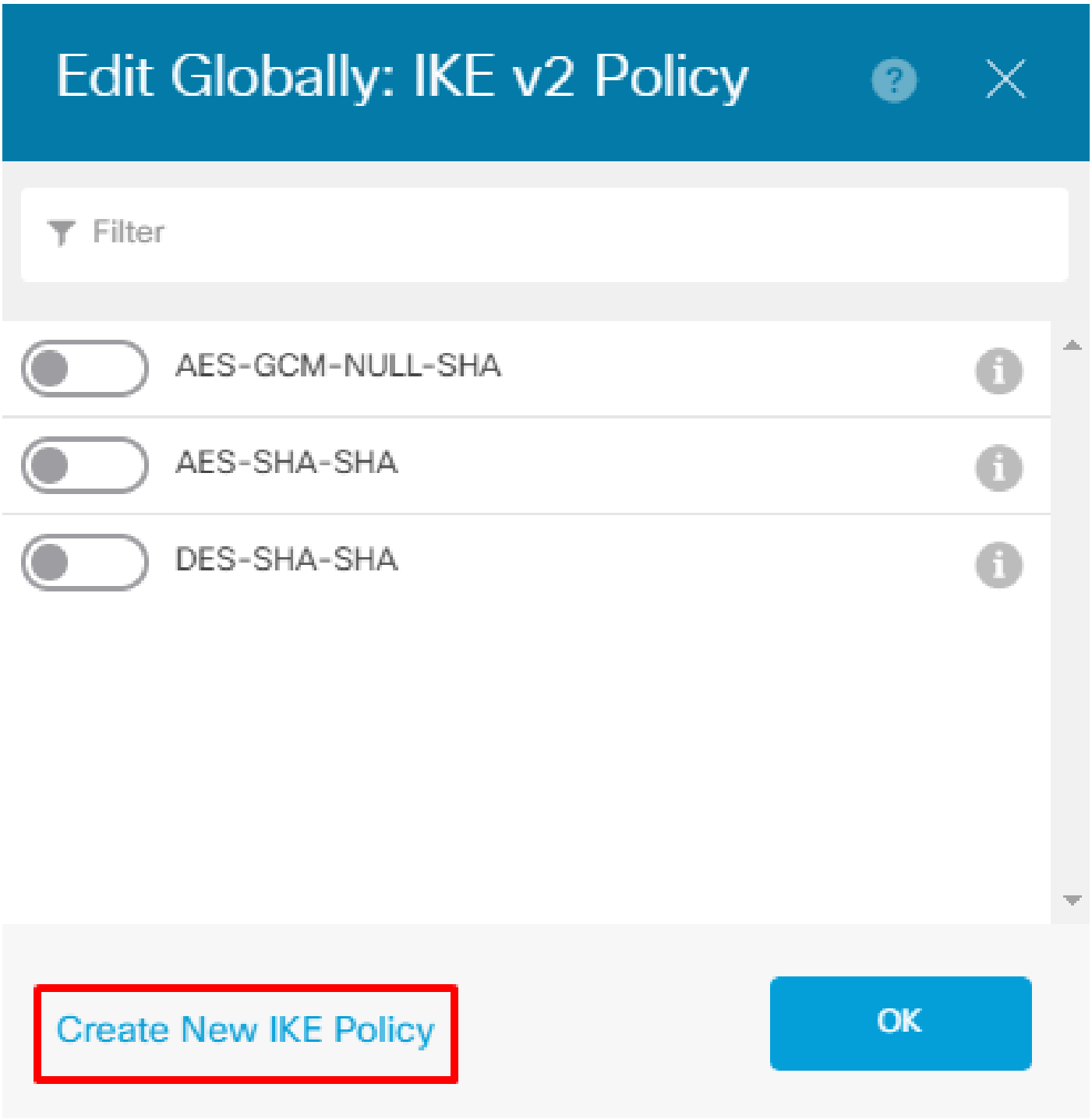
قم بتعيين الواجهة العامة للنظير البعيد. ثم أختر شبكة النظراء البعيدين التي يتم تشفيرها عبر شبكة VPN من موقع إلى موقع كما هو موضح في الصورة.



في الصفحة التالية، أختر زر تحرير لتعيين معلمات Internet Key Exchange (IKE) كما هو موضح في الصورة.

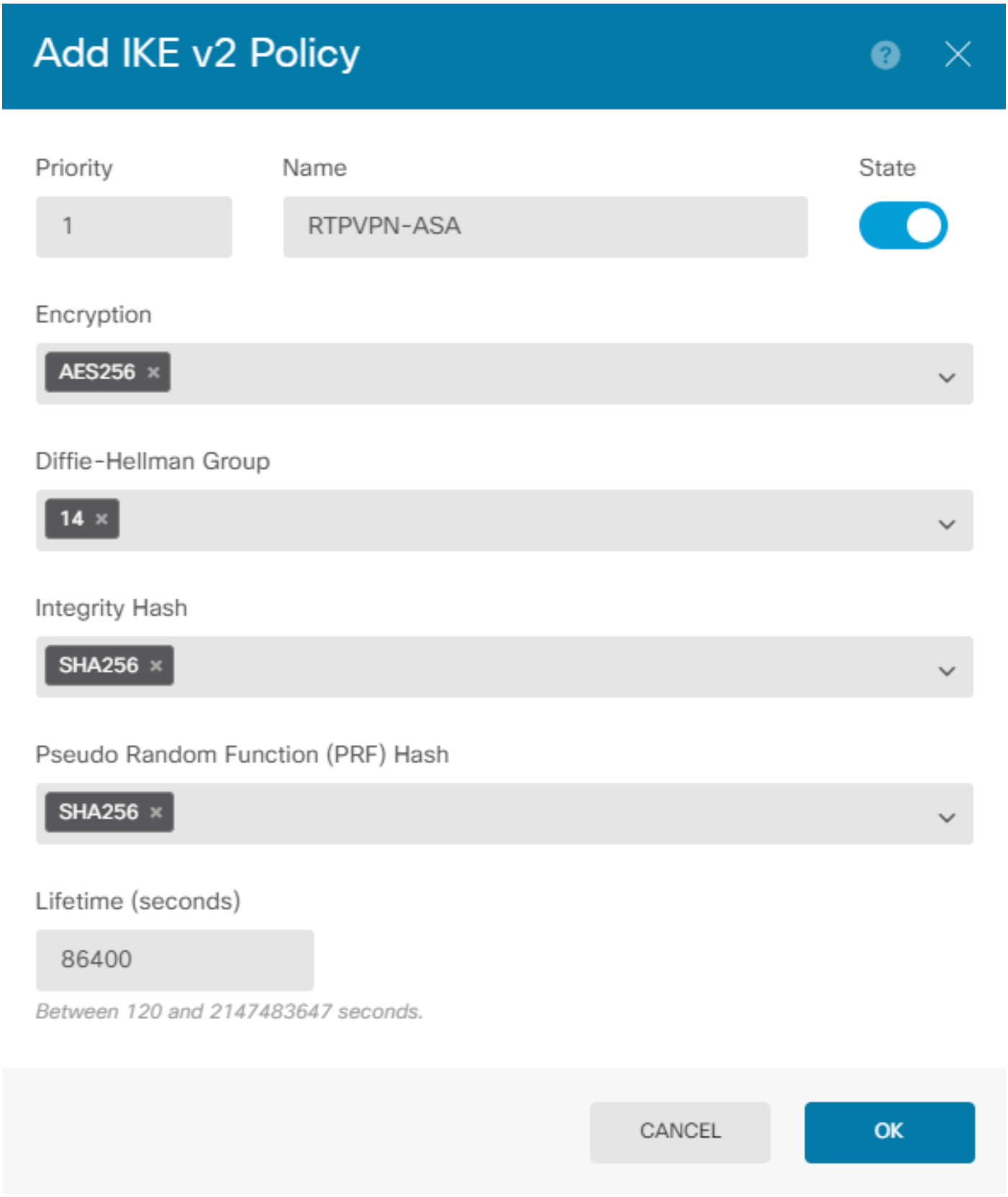


أختر زر إنشاء نهج IKE جديد كما هو موضح في الصورة.

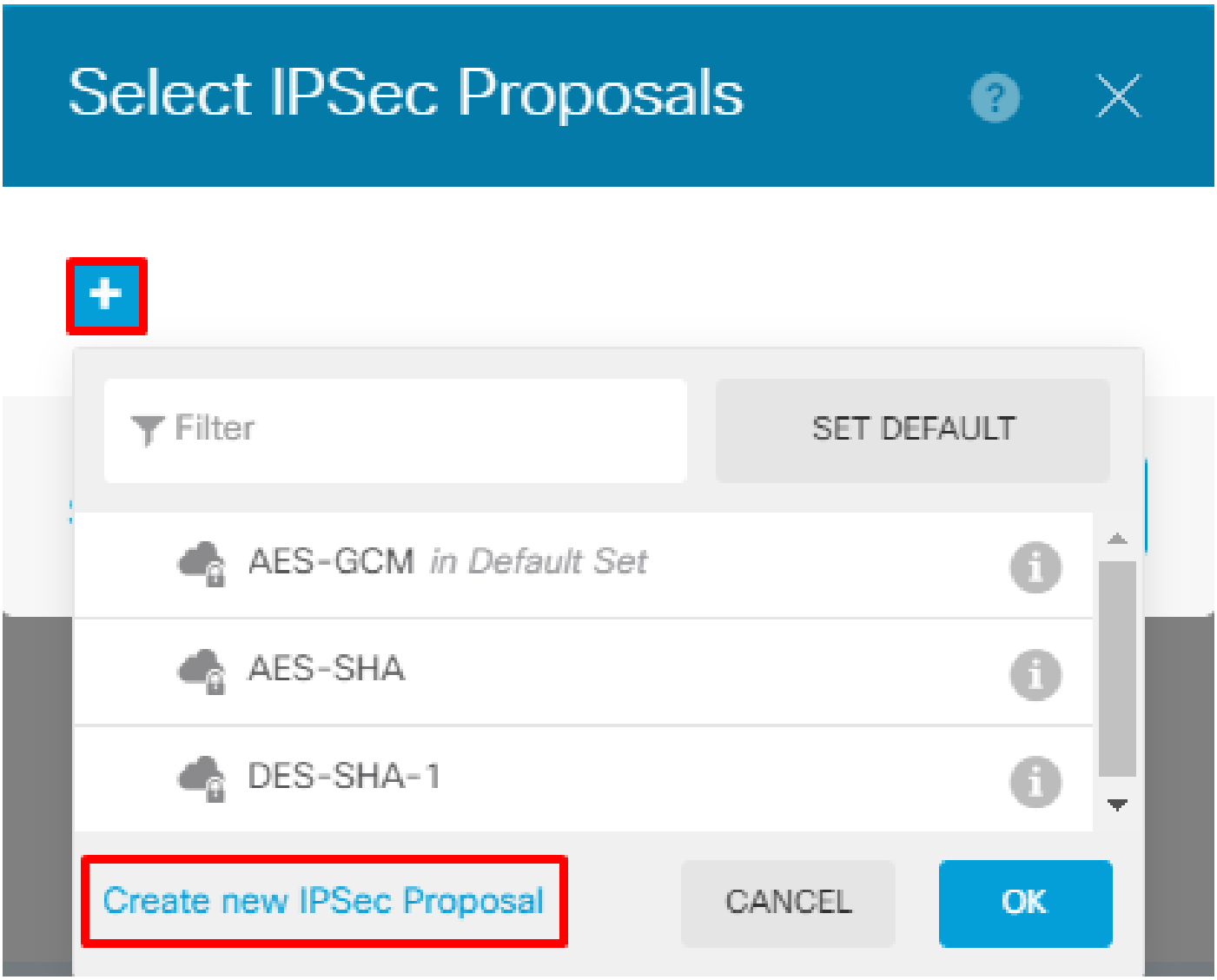


يستخدم هذا الدليل هذه المعلمات للتبادل الأولي لـ IKEv2:

التشفير AES-256
التكامل SHA256
DH المجموعة 14
PRF SHA256



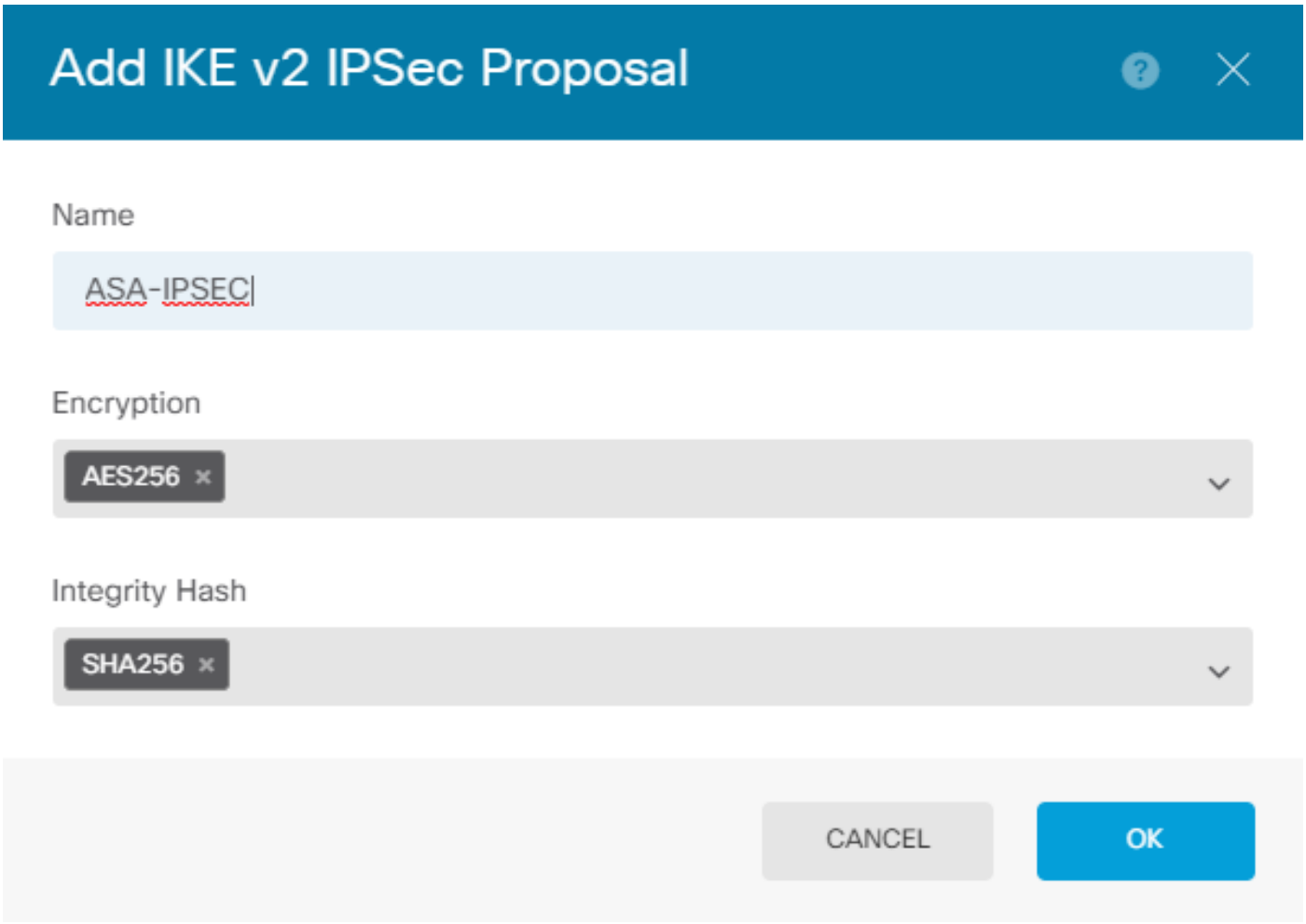
أختر مرة أخرى على الصفحة الرئيسية زر تحرير لمقترح IPSec. قم بإنشاء مقترح IPSec جديد كما هو موضح في الصورة.



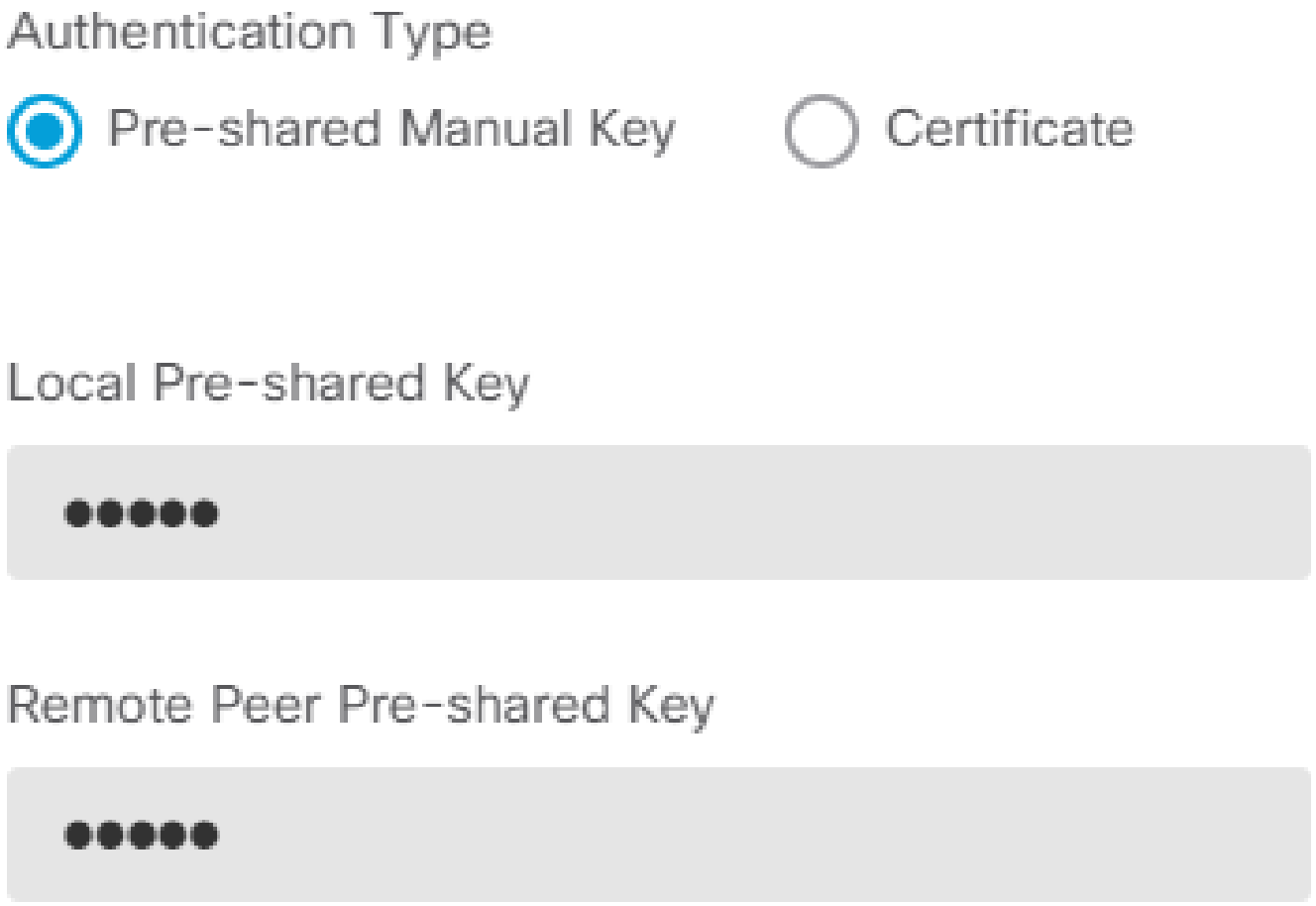
يستخدم هذا الدليل المعلمات التالية ل IPSec:

التشفير AES-256

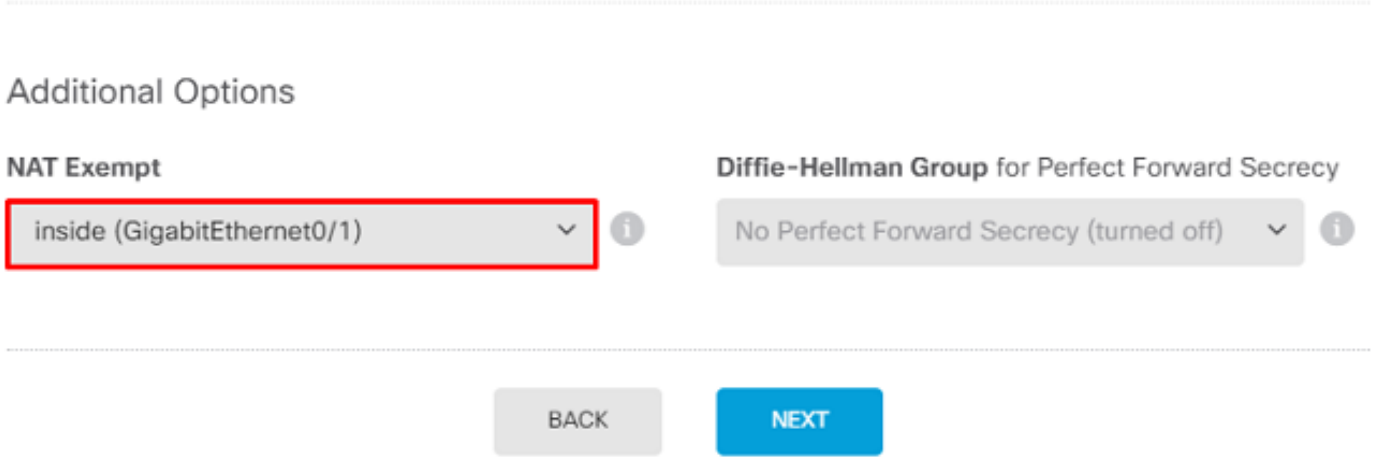
التكامل SHA256



قم بتعيين المصادقة على مفتاح مشترك مسبقا وأدخل المفتاح المشترك مسبقا (PSK) الذي يتم إستخدامه على كلا النهايتين. في هذا الدليل، يتم إستخدام PSK من Cisco كما هو موضح في الصورة.



ثبتت الداخلي nat يعفي قارن. إن هناك يتعدد داخل قارن أن يكون استعملت، nat يعفي قاعدة يدويا تحت السياسات > nat.



في الصفحة الأخيرة، يتم عرض ملخص للاتصال من موقع إلى موقع. تأكد من تحديد عناوين IP الصحيحة، ومن استخدام معلمات التشفير المناسبة، ثم اضغط زر إنهاء. قم بنشر

شبكة VPN الجديدة من موقع إلى موقع.

يتم إكمال تكوين ASA باستخدام واجهة سطر الأوامر.

تكوين 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. قم بإنشاء نهج مجموعة يسمح ببروتوكول IKEv2:

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

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

```
Tunnel-group 172.16.100.10 type ipsec-l2l
Tunnel-group 172.16.100.10 general-attributes
 Default-group-policy FDM_GP
Tunnel-group 172.16.100.10 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco
 ikev2 remote-authentication pre-shared-key cisco
```

5. قم بإنشاء قائمة وصول تحدد حركة المرور التي سيتم تشفيرها: (FTDSubnet

10.10.116.0/24) (ASASubnet 10.10.110.0/24):

```
Object network FDMSubnet
 Subnet 10.10.116.0 255.255.255.0
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 FDM
 Protocol esp encryption aes-256
 Protocol esp integrity sha-256
```

7. قم بإنشاء إدخال خريطة تشفير يربط التكوين معا:

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

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

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FDMSubnet FDMSubnet
no-proxy-arp route-lookup
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

عم الوصول إلى سطر الأوامر من ASA أو FTD، يمكن القيام بذلك باستخدام أمر حزم tracer. عندما يستعمل أن الربط-tracer أمر قبل وضع الإرسال من البيانات مرور حركة بدء ولالة VPN. مرة أول يظهر. in order to تحقق إذا ما النفق، هو يغبني كرتضت مرتين VPN قفن، ال يجلب VPN مع تشفير packet-tracer أمر لشفي حتى الطعم VPN قفن يكون، الأمر إصدار يتم ما بالربط-tracer في عنوان المصدر أن ما ية جدار الحماية من خلال عنوان الداخلي يستعمل ال Drop.

أن هذا يفشل دائما.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.116.10 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 |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4
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 NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0

Phase: 9
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 الأمر show crypto ikev2 sa.

```
> show crypto ikev2 sa

IKEv2 SAs:

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

Tunnel-id Local                                          Remote
  3821043 172.16.100.10/500                               192.168.200.10/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1150 sec
Child sa: local selector  10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

مشكلات الاتصال الأولية

عندما تبني شبكة خاصة ظاهرية، هناك جانبان يتفاوضان حول النفق. لذلك، من الأفضل الحصول على الجانبي 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 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 172.16.100.10 host 192.168.200.10
```

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

راجع التقاط الحزمة باستخدام الأمر show cap capout.

```
firepower# show cap capout

4 packets captured

   1: 01:21:06.763983       172.16.100.10.500 > 192.168.200.10.500:  udp 574
   2: 01:21:06.769415       192.168.200.10.500 > 172.16.100.10.500:  udp 619
   3: 01:21:06.770666       172.16.100.10.500 > 192.168.200.10.500:  udp 288
   4: 01:21:06.773748       192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

المشاكل الخاصة بحركة المرور

المشاكل الشائعة لحركة المرور التي يواجهها المستخدمون 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.
- ال يتم تجاوز ترجمة عنوان الشبكة (NAT) لحركة مرور VPN.

معلومات ذات صلة

لمزيد من المعلومات حول شبكات VPN من موقع إلى موقع على FTD الذي تتم إدارته بواسطة FDM، يمكنك العثور على دليل التكوين الكامل هنا.

- تتم إدارة FTD بواسطة دليل تكوين FDM.

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).