تكوين نفق IKEv2 IPv6 من موقع إلى موقع بين ASA و FTD

المحتويات

المقدمة

يقدم هذا المستند مثال للتكوين لإعداد نفق موقع IPv6 إلى موقع بين بروتوكول ASA باستخدام Firepower) وبروتوكول FTD (الدفاع ضد تهديد) (جهاز الأمان القابل للتكيف) بروتوكول تبادل مفتاح الإنترنت الإصدار 2 (IKEv2). ويتضمن الإعداد اتصال شبكة IPv6 الطرفي باستخدام ASA و FTD كأجهزة إنهاء VPN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين ASA CLI
- معرفة أساسية ببروتوكولات IKEv2 و IPSec
- فهم عنونة IPv6 والتوجيه
- الفهم الأساسي لتكوين FTD عبر FMC

المكونات المستخدمة

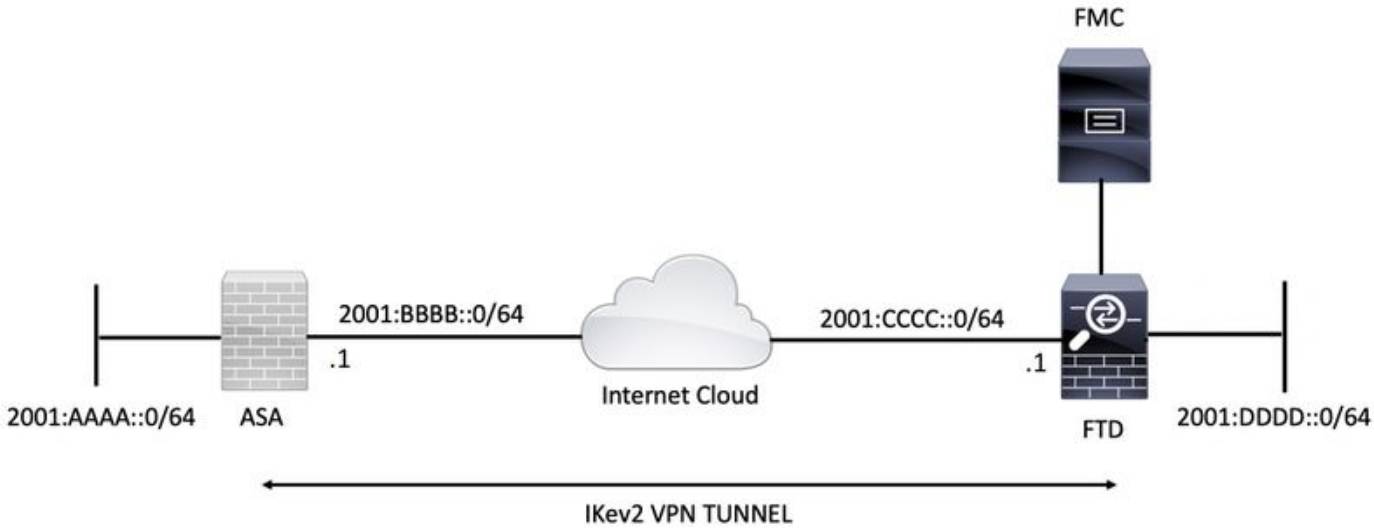
تستند المعلومات الواردة في هذا المستند إلى بيئة افتراضية، تم إنشاؤها من الأجهزة المذكورة في إعداد معملي محدد. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد الإنتاج، فتأكد من فهمك للتأثير المحتمل لأي أمر.

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

- Cisco ASAv جار 9.6(4)12
- تشغيل Cisco FTDv 6.5.0
- تشغيل Cisco FMCv، الإصدار 6.6.0

التكوين

الرسم التخطيطي للشبكة



تكوين ASA

يصف هذا القسم التكوين المطلوب على ASA.

الخطوة 1. تكوين واجهات ASA.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable

interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

الخطوة 2. تعيين المسار الافتراضي لـ IPv6.

```
ipv6 route outside ::/0 2001:bbbb::2
```

الخطوة 3. قم بتكوين نهج IKEv2 وتمكين IKEv2 على الواجهة الخارجية.

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

crypto ikev2 enable outside
```

الخطوة 4. قم بتكوين مجموعة الأنفاق.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

الخطوة 5. قم بإنشاء الكائنات وقائمة التحكم في الوصول (ACL) لمطابقة حركة المرور المفيدة.

```
object-group network local-network
network-object 2001:aaaa::/64

object-group network remote-network
network-object 2001:dddd::/64

access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

الخطوة 6. شكل تلك الهوية شبكة عنوان ترجمة (NAT) قاعدة لحركة مرور مثيرا للاهتمام.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

الخطوة 7. تكوين مقترح IKEv2 IPSec.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

الخطوة 8. قم بتعيين خريطة التشفير وتطبيقها على الواجهة الخارجية.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route

crypto map VPN interface outside
```

تكوين FTD

يوفر هذا القسم إرشادات لتكوين FTD باستخدام FMC.

تحديد مخطط الشبكة الخاصة الظاهرية (VPN)

الخطوة 1. انتقل إلى **الأجهزة > VPN > موقع إلى موقع**.

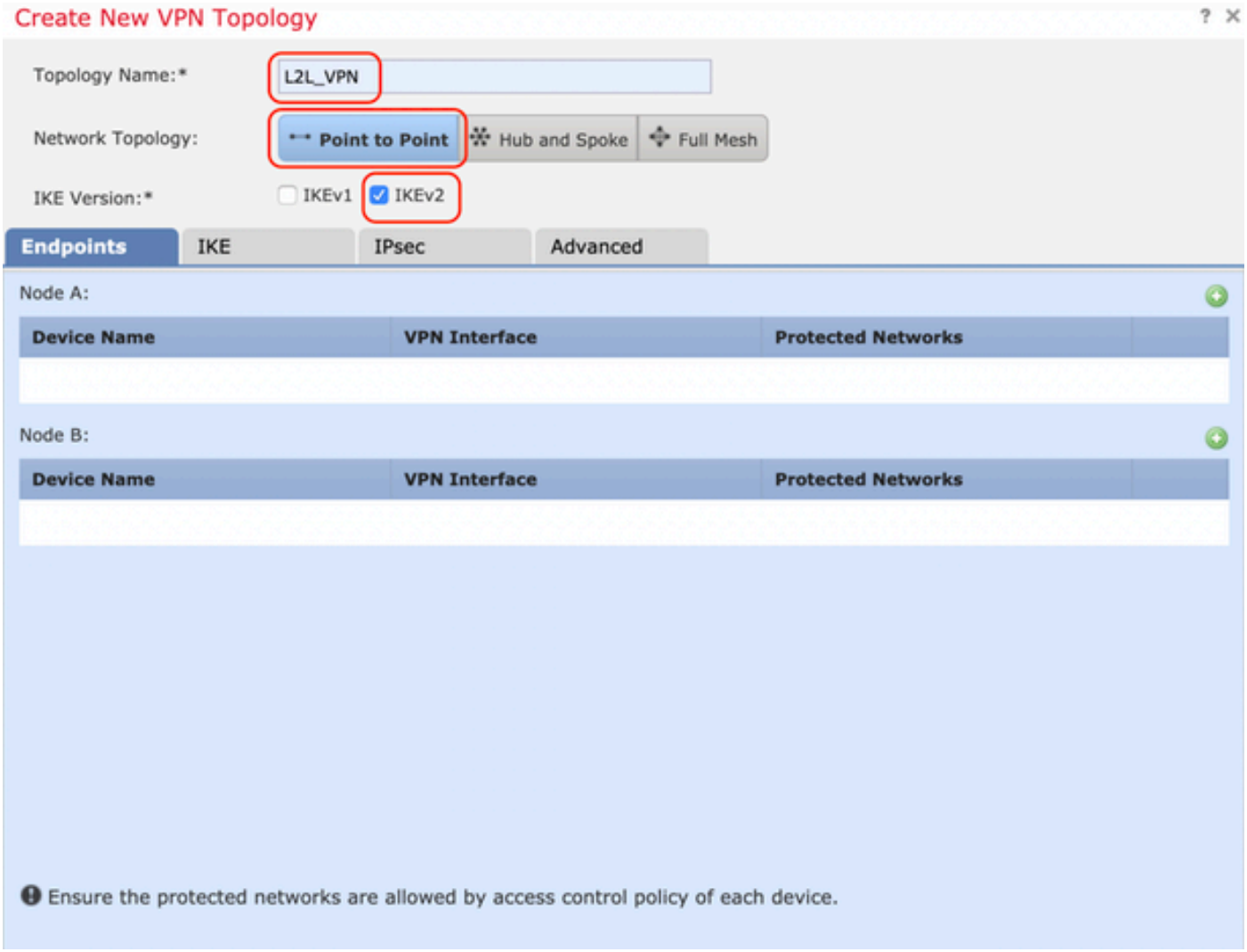
تحديد 'add VPN' واختر 'جهاز الدفاع ضد تهديد FirePOWER'، كما هو موضح في هذه الصورة.

الخطوة 2. يظهر مربع "إنشاء مخطط VPN جديد". امنح الشبكة الخاصة الظاهرية (VPN) اسما يمكن التعرف عليه بسهولة.

مخطط الشبكة: نقطة إلى نقطة

إصدار IKE: IKEv2

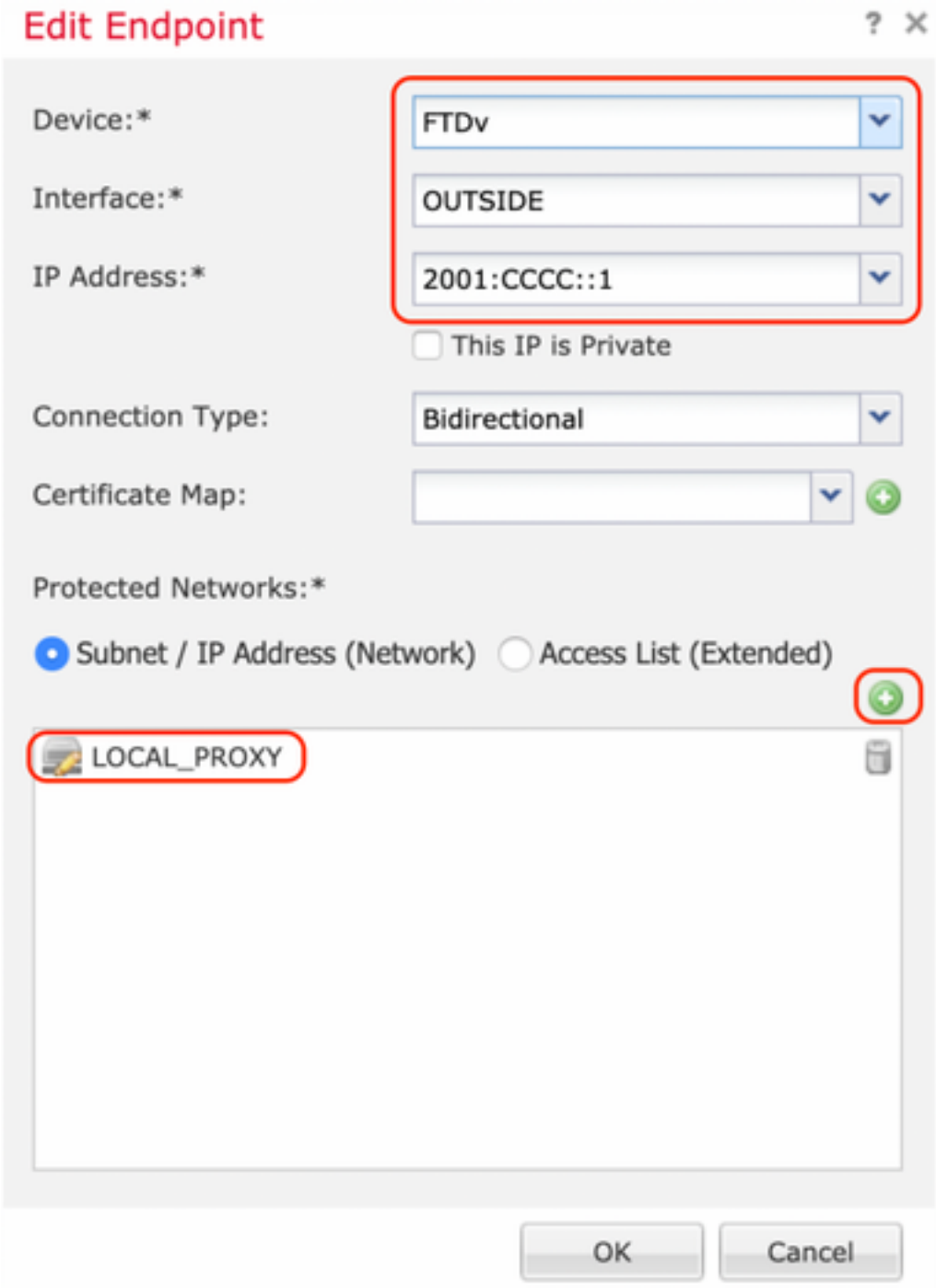
في هذا المثال، عند تحديد نقطة النهاية العقدة A، يتم استخدام FTD. العقدة B هي ASA. انقر فوق الزر "أخضر زائد" لإضافة أجهزة إلى المخطط.

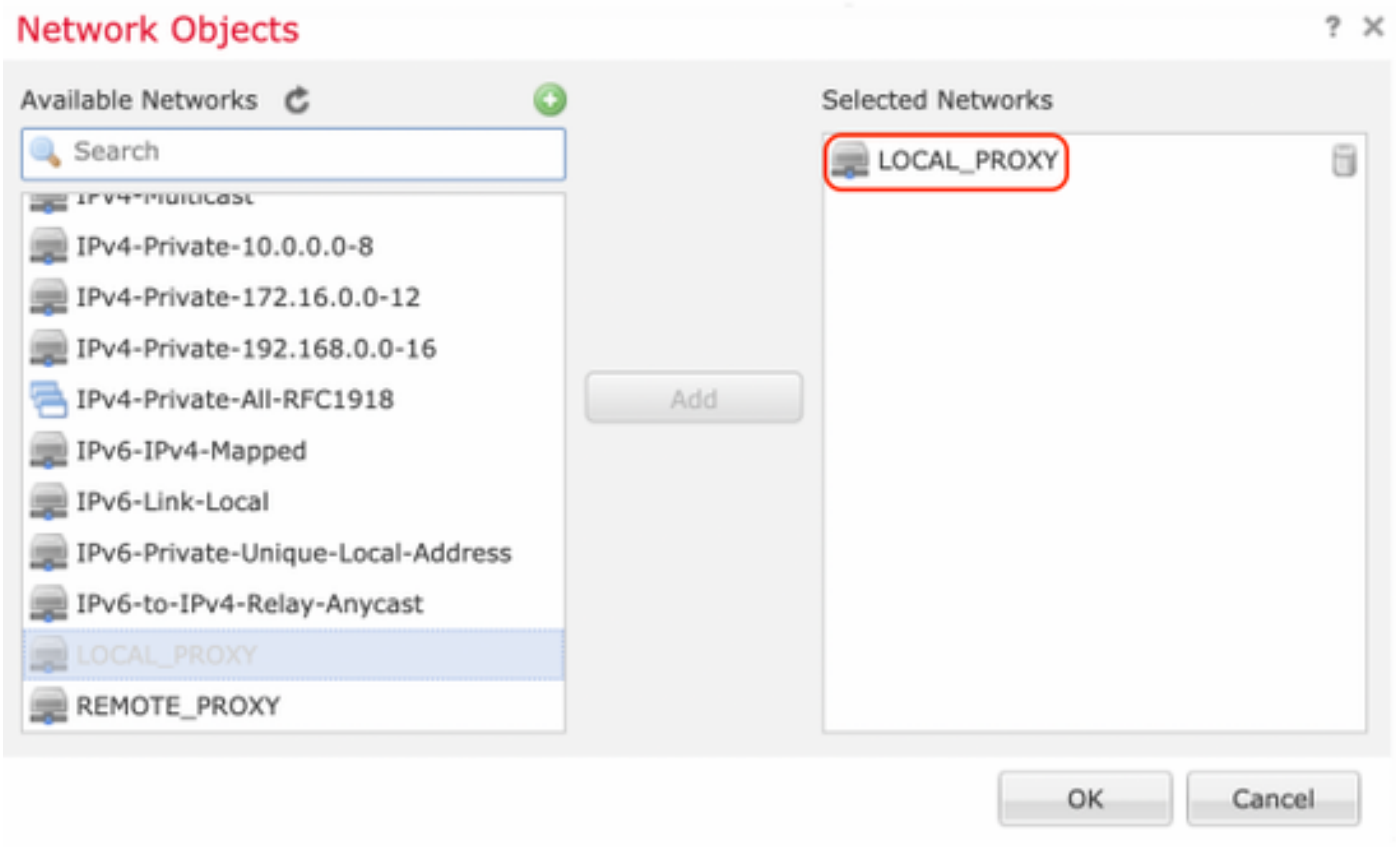


الخطوة 3. إضافة FTD كنقطة نهاية أولى.

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

انقر فوق رمز Green Plus ضمن الشبكات المحمية لتحديد الشبكات الفرعية التي يتم تشفيرها عبر نفق VPN هذا. في هذا المثال، يتكون كائن شبكة "الوكيل المحلي" على FMC من الشبكة الفرعية ل IPv6 '2001:DDDD::/64'.

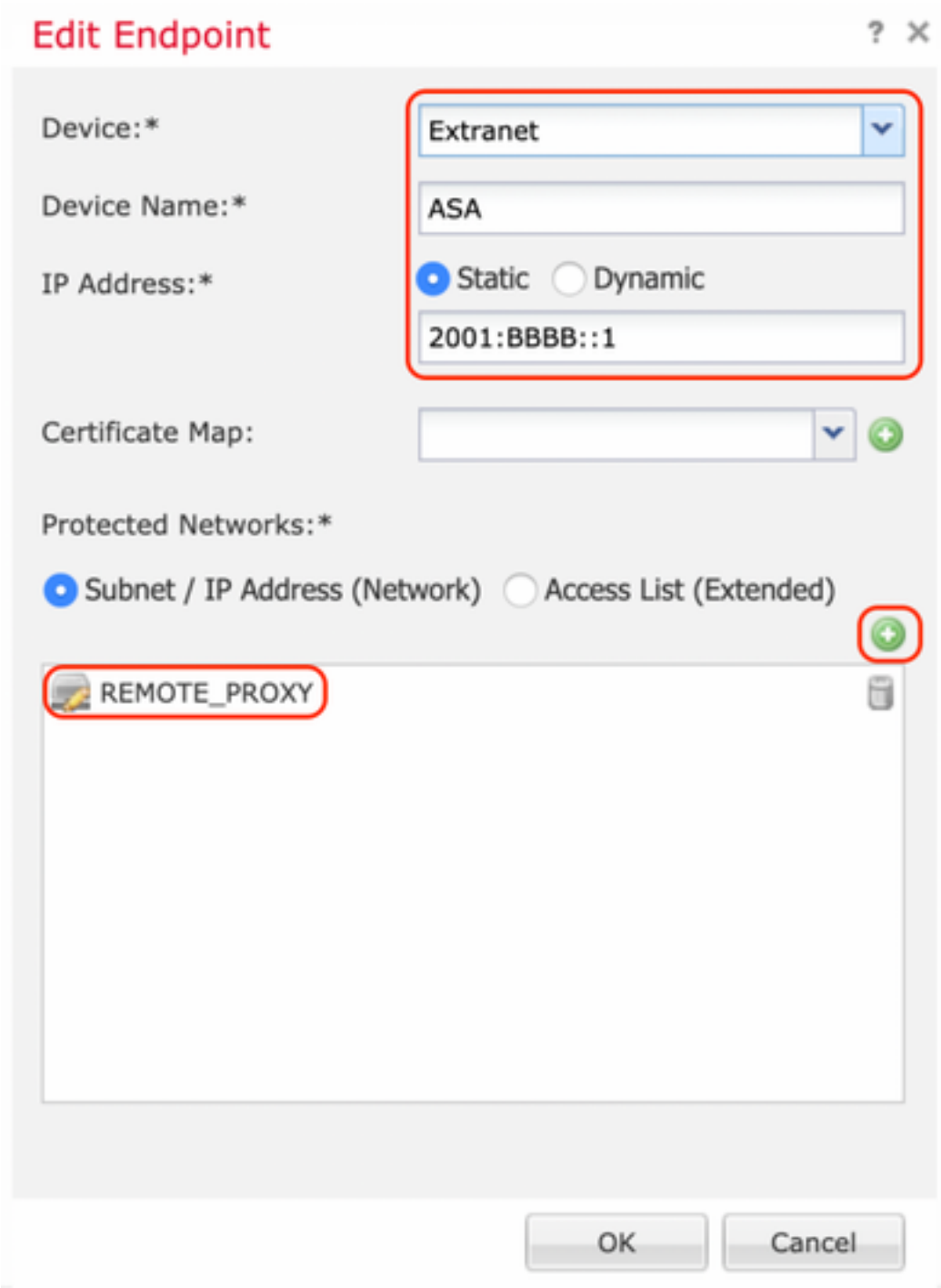

Edit Endpoint
Device:*
FTDv
Interface:*
OUTSIDE
IP Address:*
2001:CCCC::1
This IP is Private
Connection Type:
Bidirectional
Certificate Map:
Protected Networks:*
Subnet / IP Address (Network)
Access List (Extended)
LOCAL_PROXY
OK
Cancel



مع الخطوة الواردة أعلاه، اكتمل تكوين نقطة نهاية FTD.

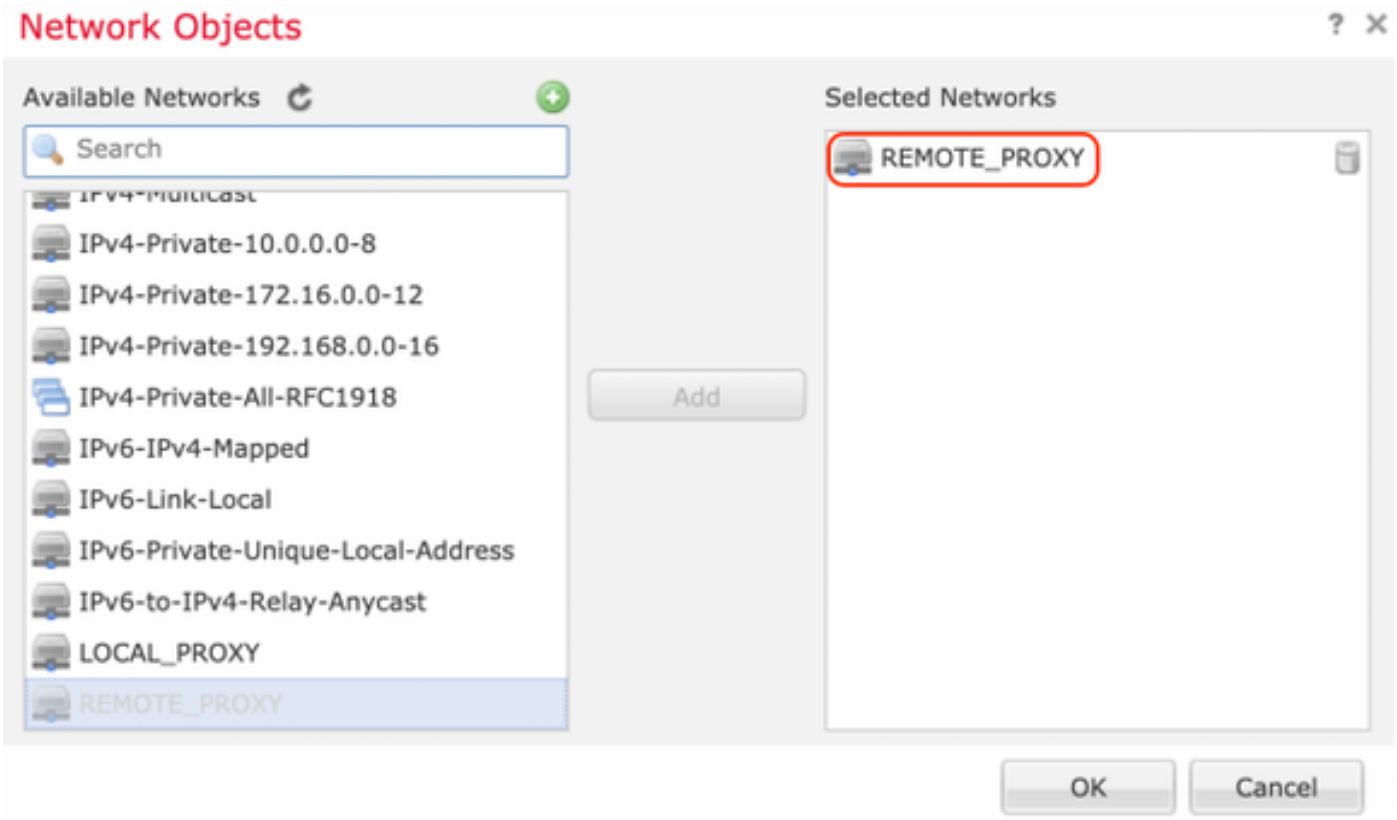
الخطوة 4. طقطقت الـ green plus رمز لـ عقدة بـ أي يكون ASA في التشكيل مثال. وتعتبر الأجهزة التي لا تتم إدارتها بواسطة FMC extranet. إضافة اسم جهاز وعنوان IP.

الخطوة 5. حدد أيقونة علامة الجمع الخضراء لإضافة شبكات محمية.



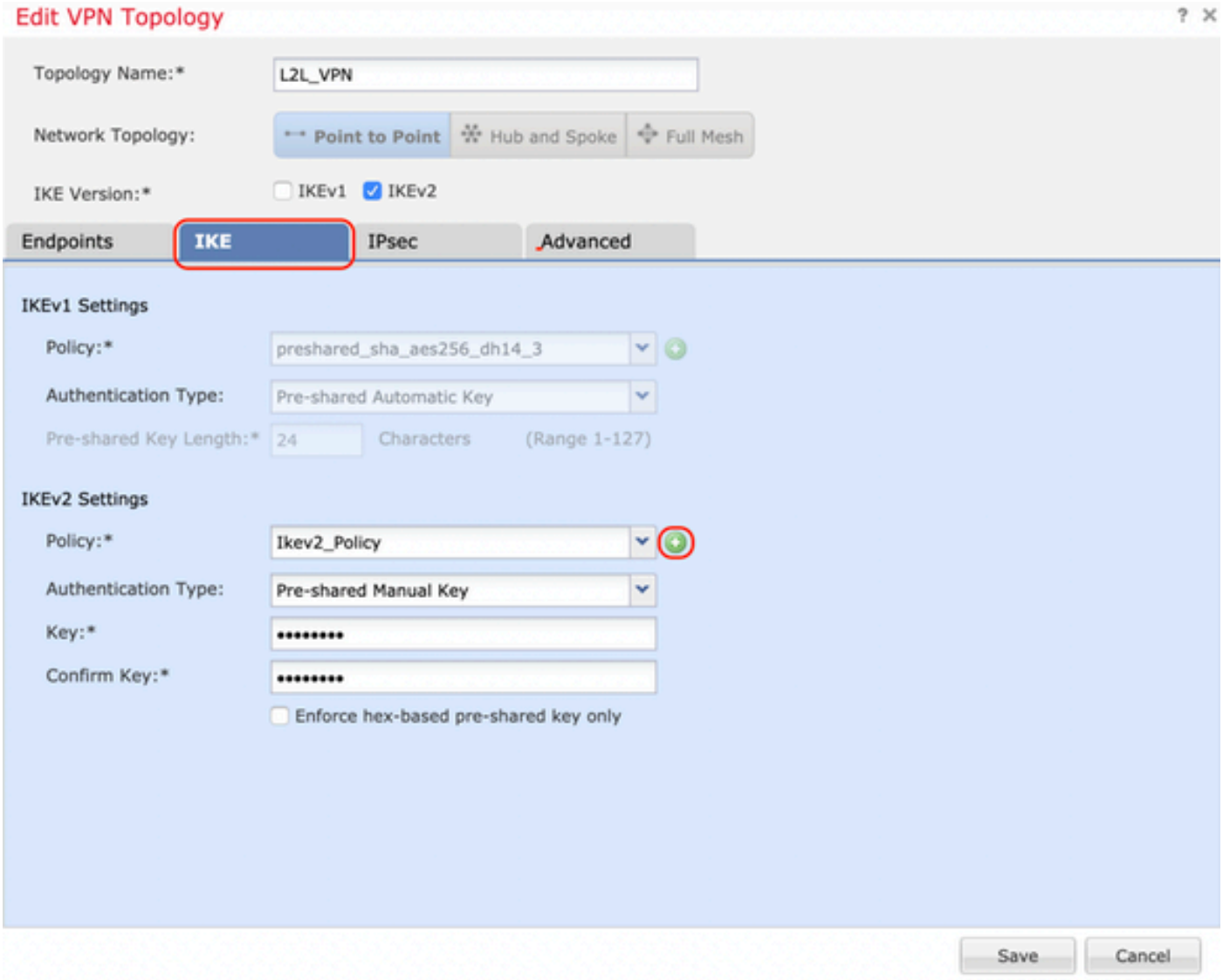
الخطوة 6. حدد شبكات ASA الفرعية التي يلزم تشفيرها وإضافتها إلى الشبكات المحددة.

في هذا المثال، شبكة ASA الفرعية '2001:AAA:/64' هي 'Remote Proxy'.



تكوين معلمات IKE

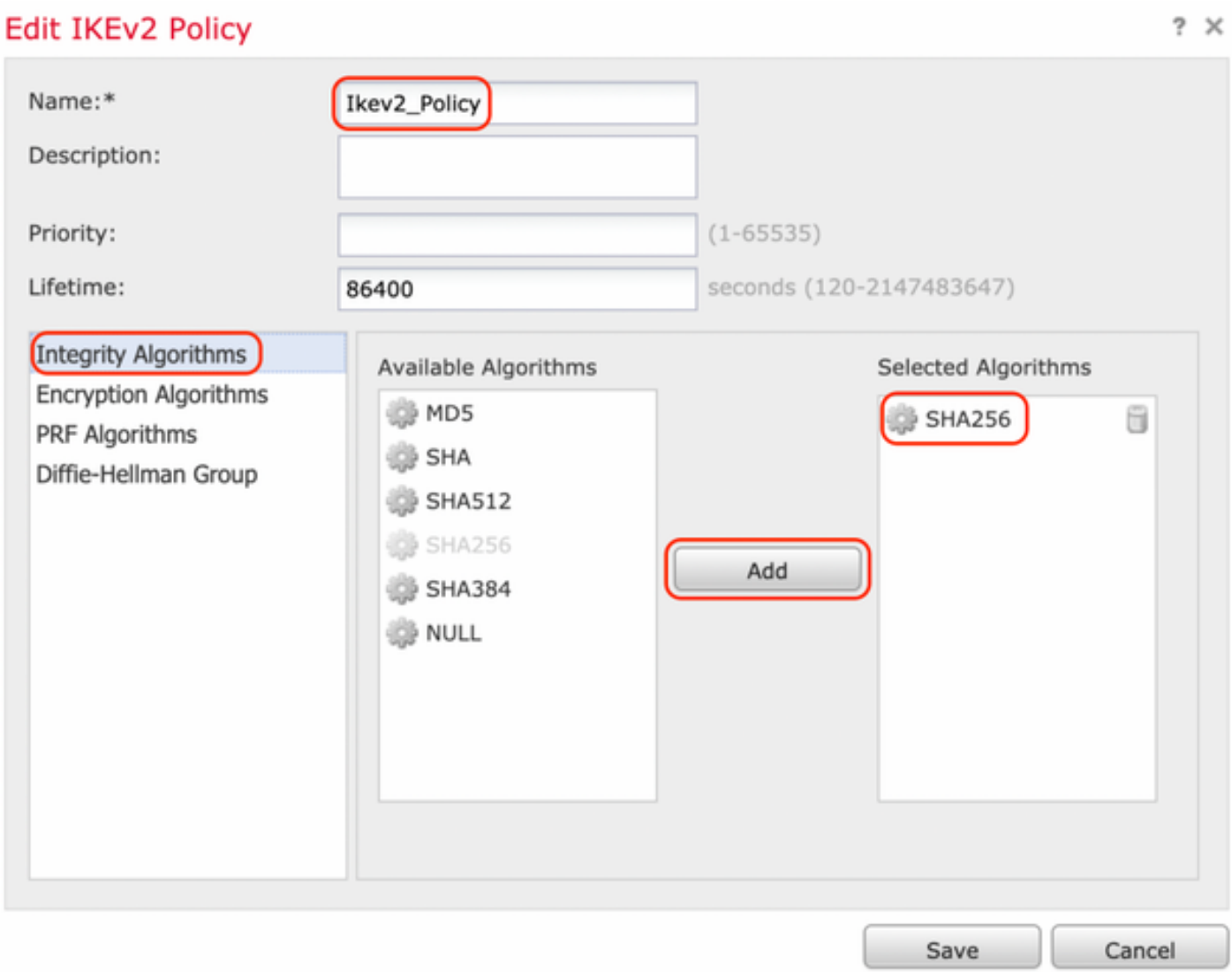
الخطوة 1. تحت علامة التبويب IKE، حدد المعلمات التي سيتم إستخدامها للتبادل الأولي IKEv2. انقر فوق رمز علامة الإضافة الخضراء لإنشاء نهج IKE جديد.

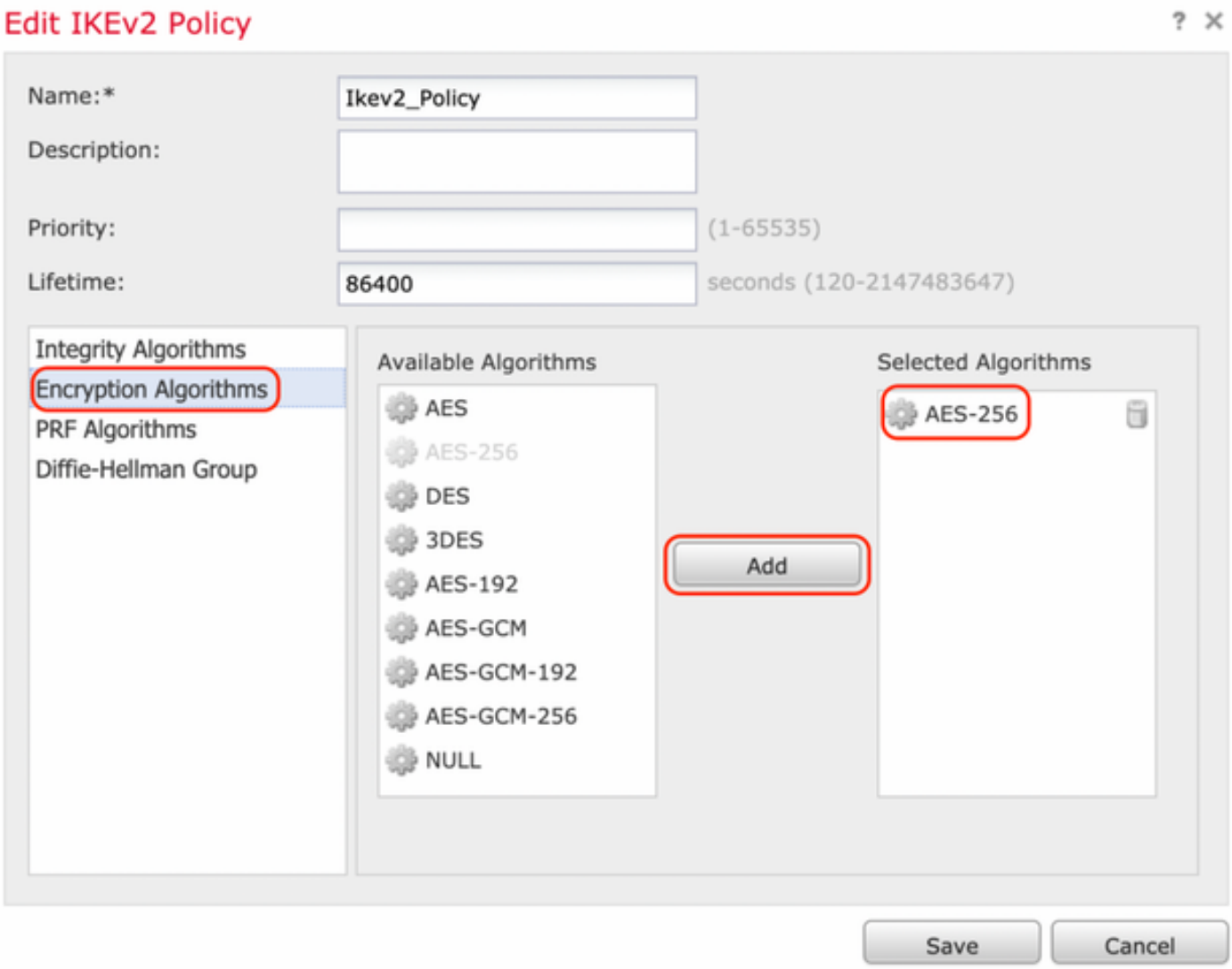


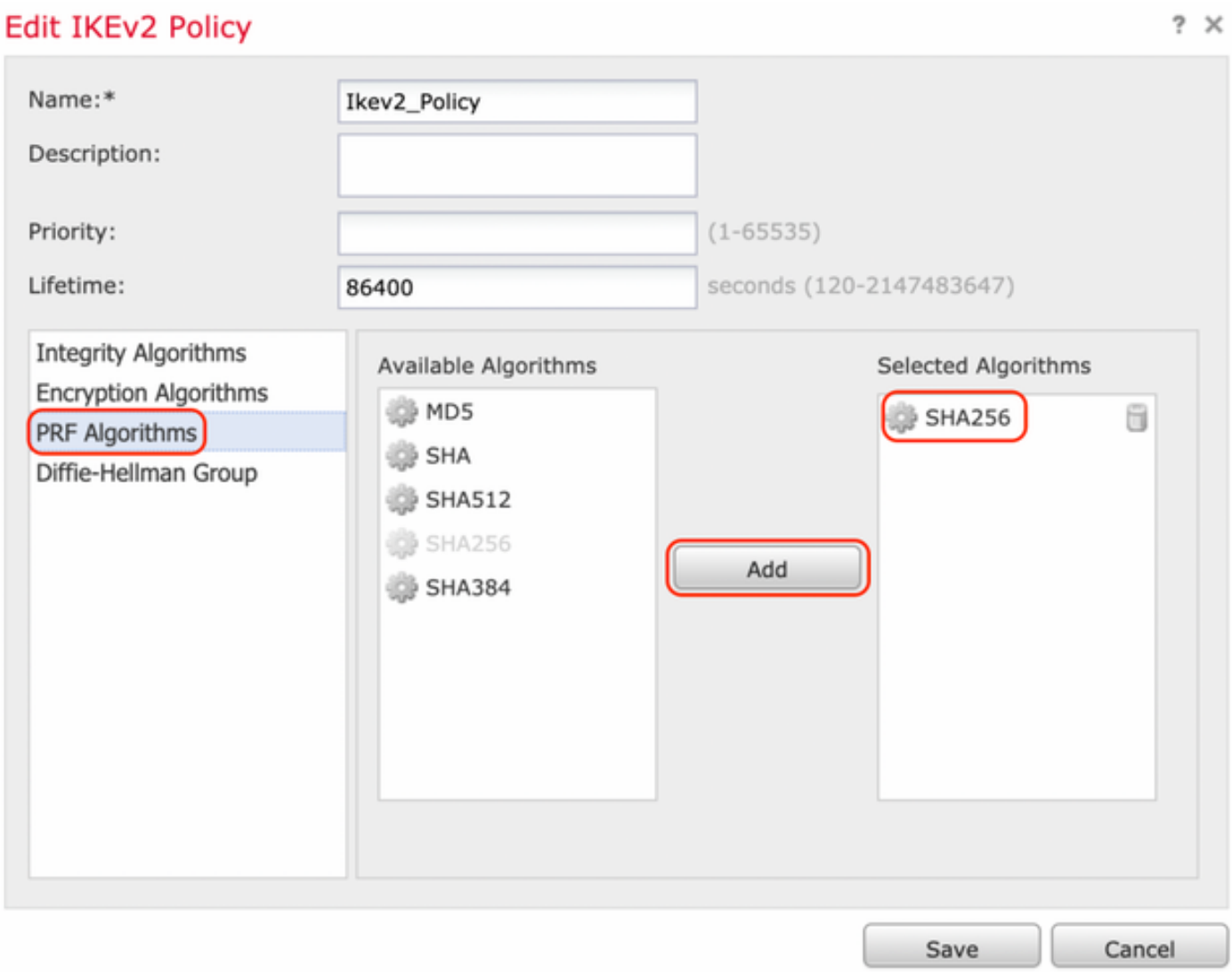
الخطوة 2. في سياسة IKE الجديدة، حدد رقم أولوية بالإضافة إلى فترة صلاحية المرحلة 1 من الاتصال. يستخدم هذا الدليل هذه المعلمات للتبادل الأولي:
التكامل (SHA256)،
التشفير (AES-256)،
PRF (SHA256)، و
مجموعة Diffie-Hellman (المجموعة 14).

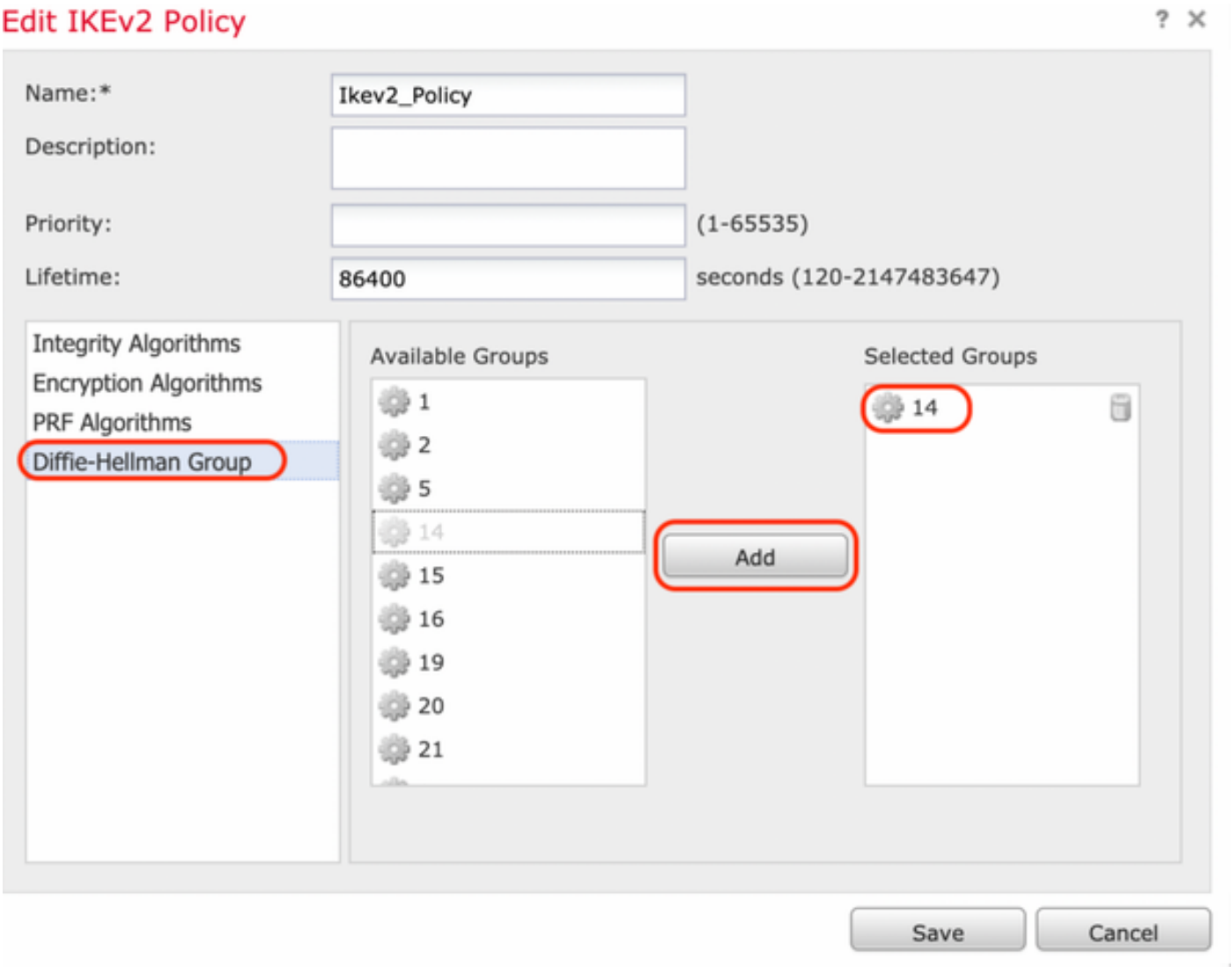
سيتم إرسال كافة نهج IKE على الجهاز إلى النظير البعيد بغض النظر عما هو موجود في قسم النهج المحدد. سيتم تحديد أول تطابق للنظير البعيد لاتصال VPN.

[إختياري] أختر النهج الذي يتم إرساله أولا باستخدام حقل الأولوية. يتم إرسال الأولوية 1 أولا.


Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(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

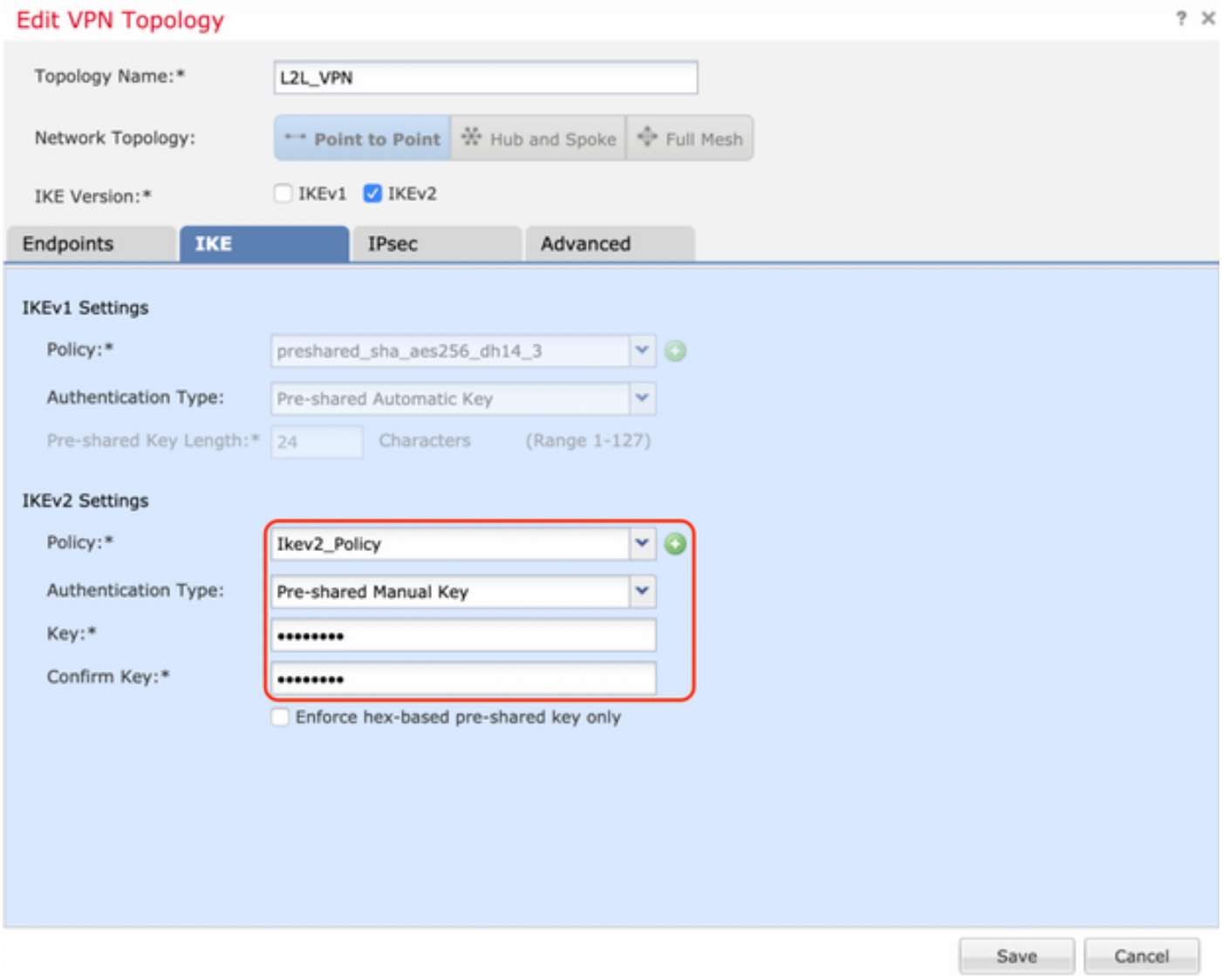

Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms
AES-256
Save
Cancel


Edit IKEv2 Policy
Name:*
Ikev2_Policy
Description:
Priority:
(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



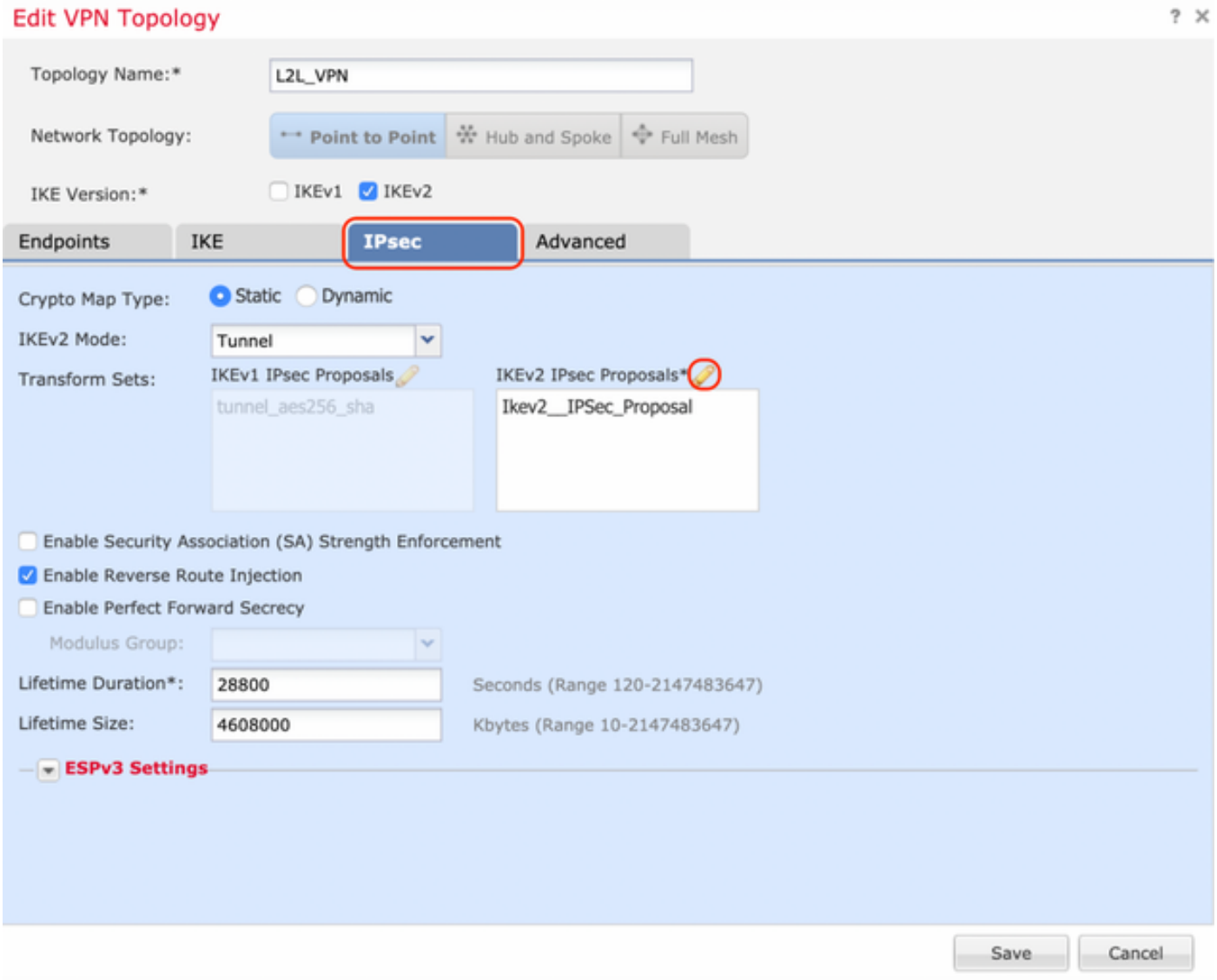
الخطوة 3. بمجرد إضافة المعلمات، حدد السياسة التي تم تكوينها أعلاه واختر نوع المصادقة.

حدد خيار المفتاح اليدوي المشترك مسبقا. ل هذا مرشد، استعملت المفتاح مشترك مسبقا **cisco123**'.



تكوين معلمات IPsec

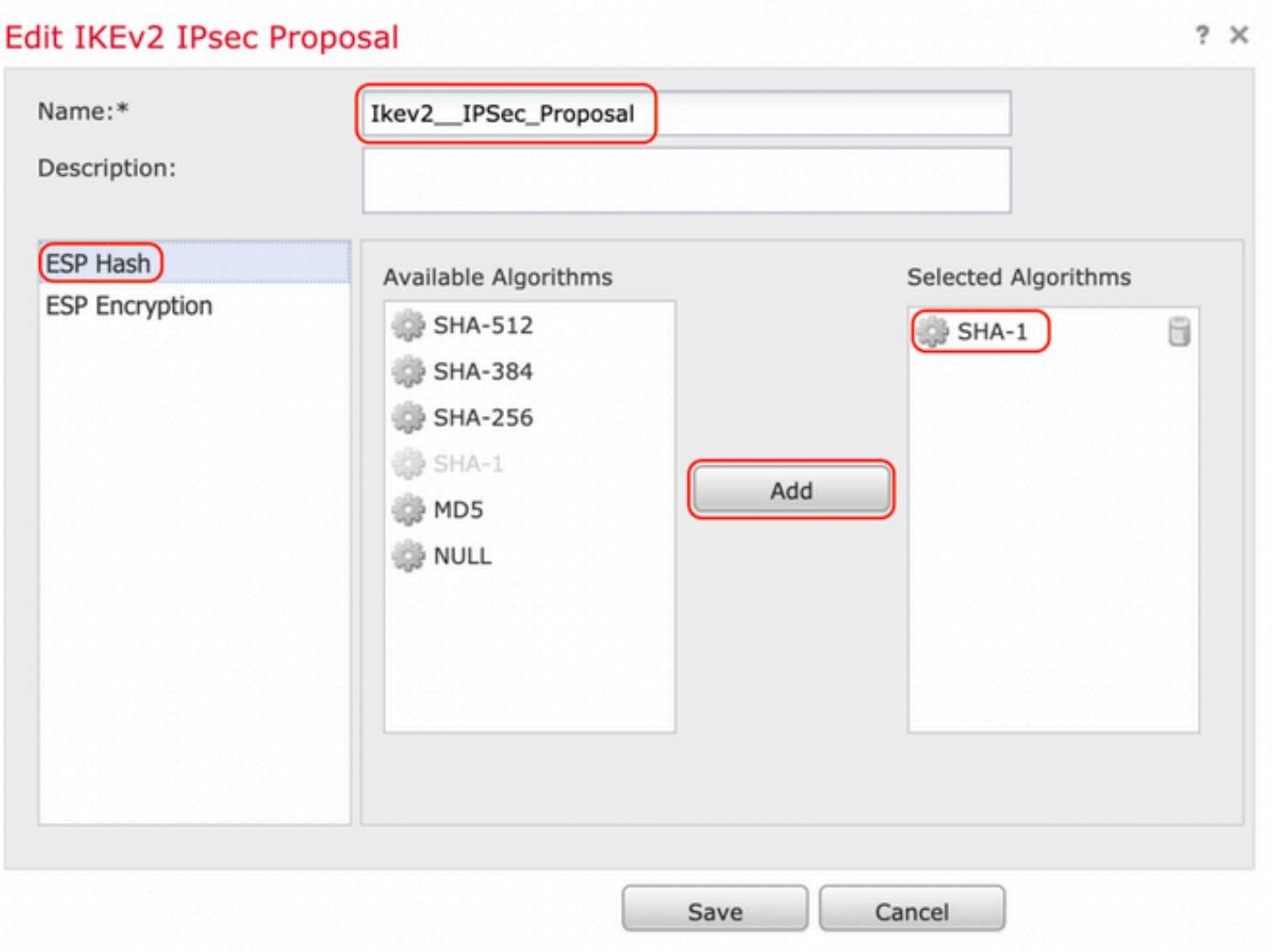
الخطوة 1. انتقل إلى علامة التبويب IPsec وقم بإنشاء "مقترح IPsec" جديد عن طريق النقر فوق رمز القلم الرصاص لتحرير مجموعة التحويل.

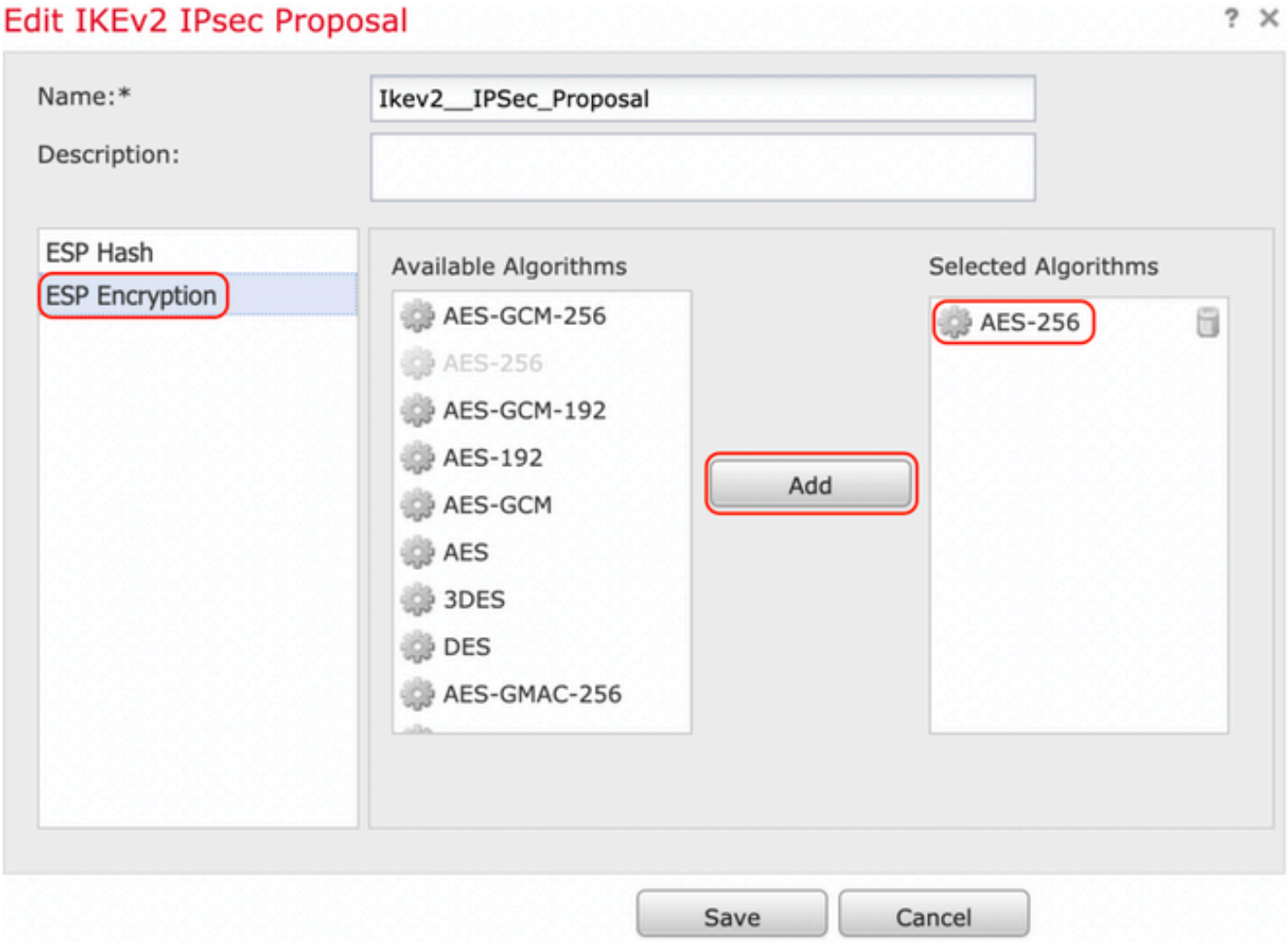


الخطوة 2. إنشاء مقترح IKEv2 IPsec جديد من خلال تحديد أيقونة Green Plus وإدخال معلمات المرحلة 2 كما هو موضح أدناه:

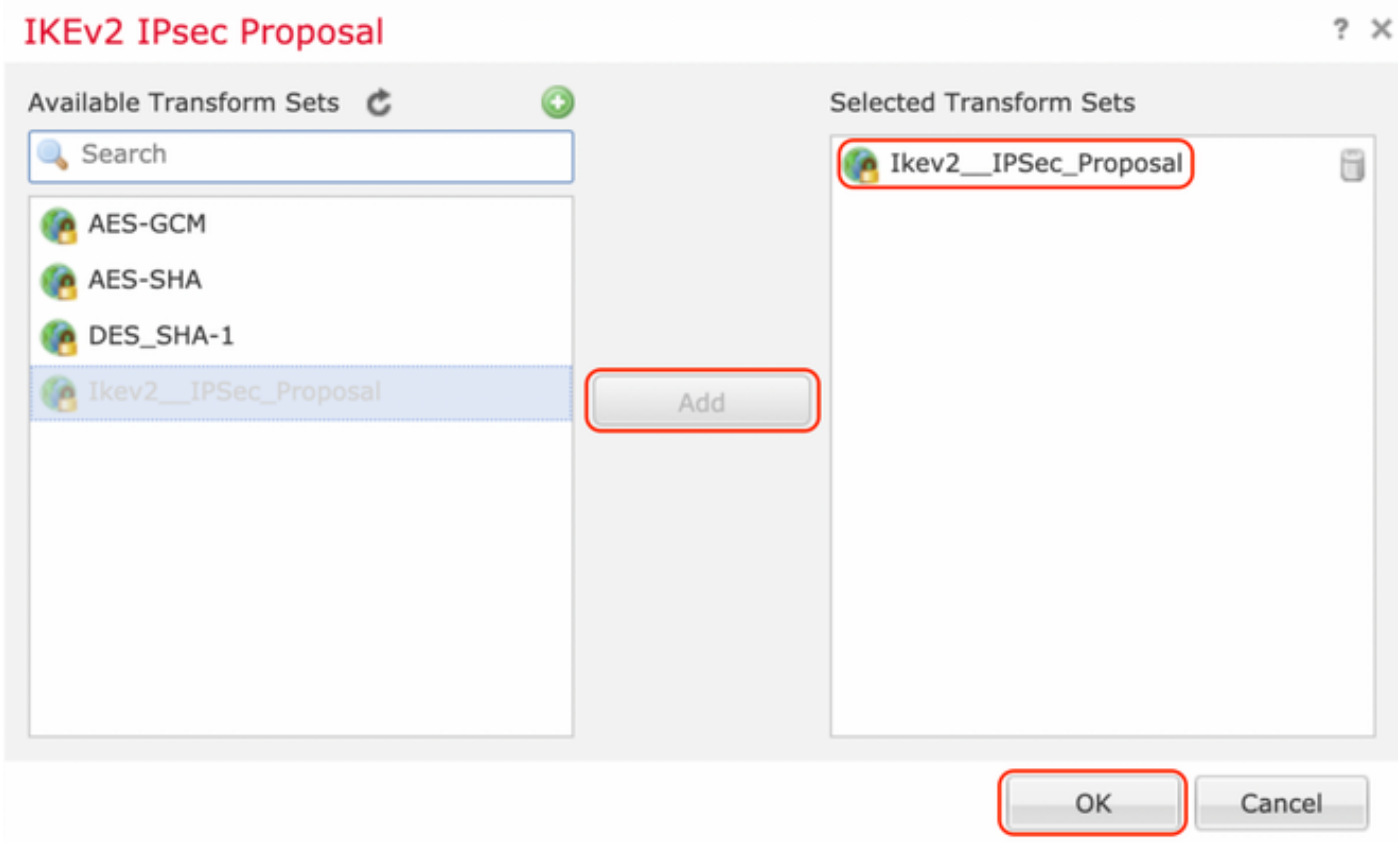
تجزئة ESP: SHA-1

تشفير ESP : AES-256


Edit IKEv2 IPsec Proposal
Name:*
Ikev2__IPSec_Proposal
Description:
ESP Hash
ESP Encryption
Available Algorithms
SHA-512
SHA-384
SHA-256
SHA-1
MD5
NULL
Add
Selected Algorithms
SHA-1
Save
Cancel

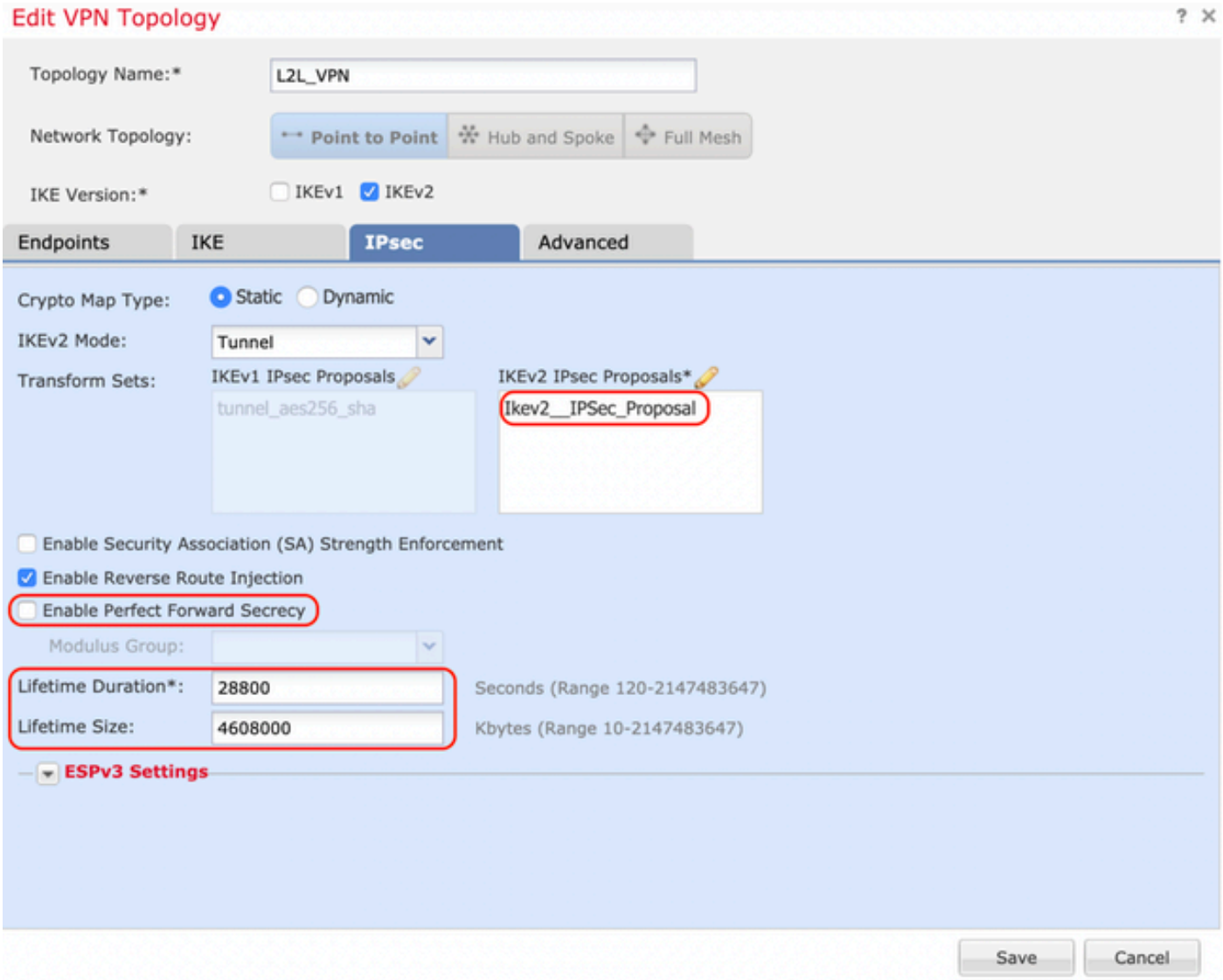


الخطوة 3. بمجرد إنشاء مقترح IPsec الجديد، قم بإضافته إلى مجموعات التحويل المحددة.



الخطوة 4. تم إدراج مقترح IPsec المحدد حديثا الآن ضمن مقترحات IKEv2 IPsec.

إن تطلب الأمر، يمكن تحرير عمر المرحلة 2 ومطابقات PFS هنا. لهذا المثال، يتم ضبط العمر الافتراضي على أنه افتراضي و PFS معطل.



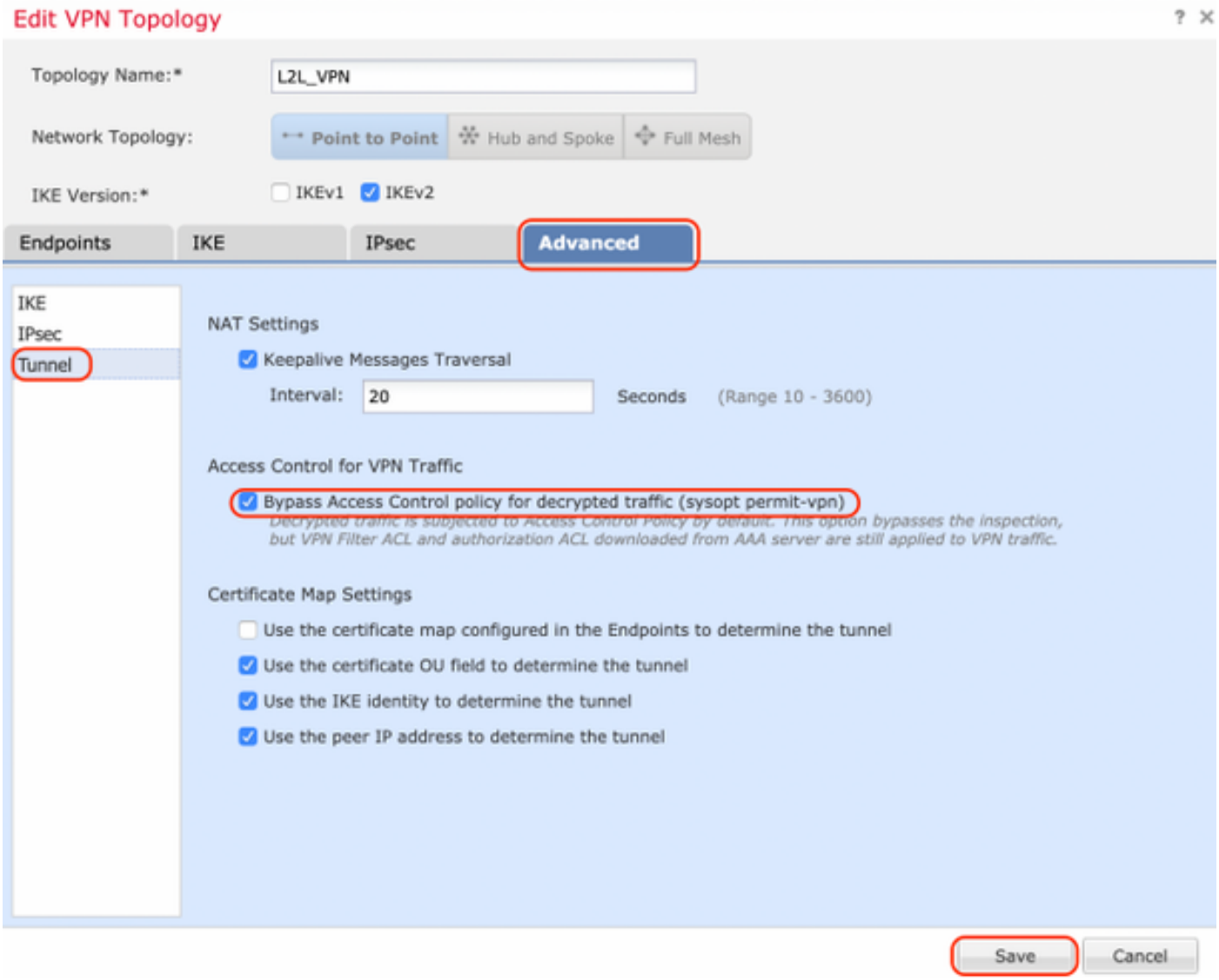
يجب عليك تكوين الخطوات التالية لتجاوز التحكم في الوصول وأ إنشاء قواعد سياسة التحكم في الوصول للسماح بالشبكات الفرعية للشبكات الخاصة الظاهرية (VPN) من خلال FTD.

التحكم بالوصول الجانبي

إذا لم يتم تمكين *sysopt allowed-vpn* بعد ذلك يجب إنشاء سياسة التحكم في الوصول للسماح بحركة مرور VPN من خلال جهاز FTD. إذا تم تمكين sysopt allowed-vpn تخطي إنشاء سياسة التحكم في الوصول. يستخدم مثال التكوين هذا خيار "التحكم في الوصول الالتفافي".

يمكن تمكين الميزة *sysopt allowed-vpn* ضمن Advanced > Tunnel.

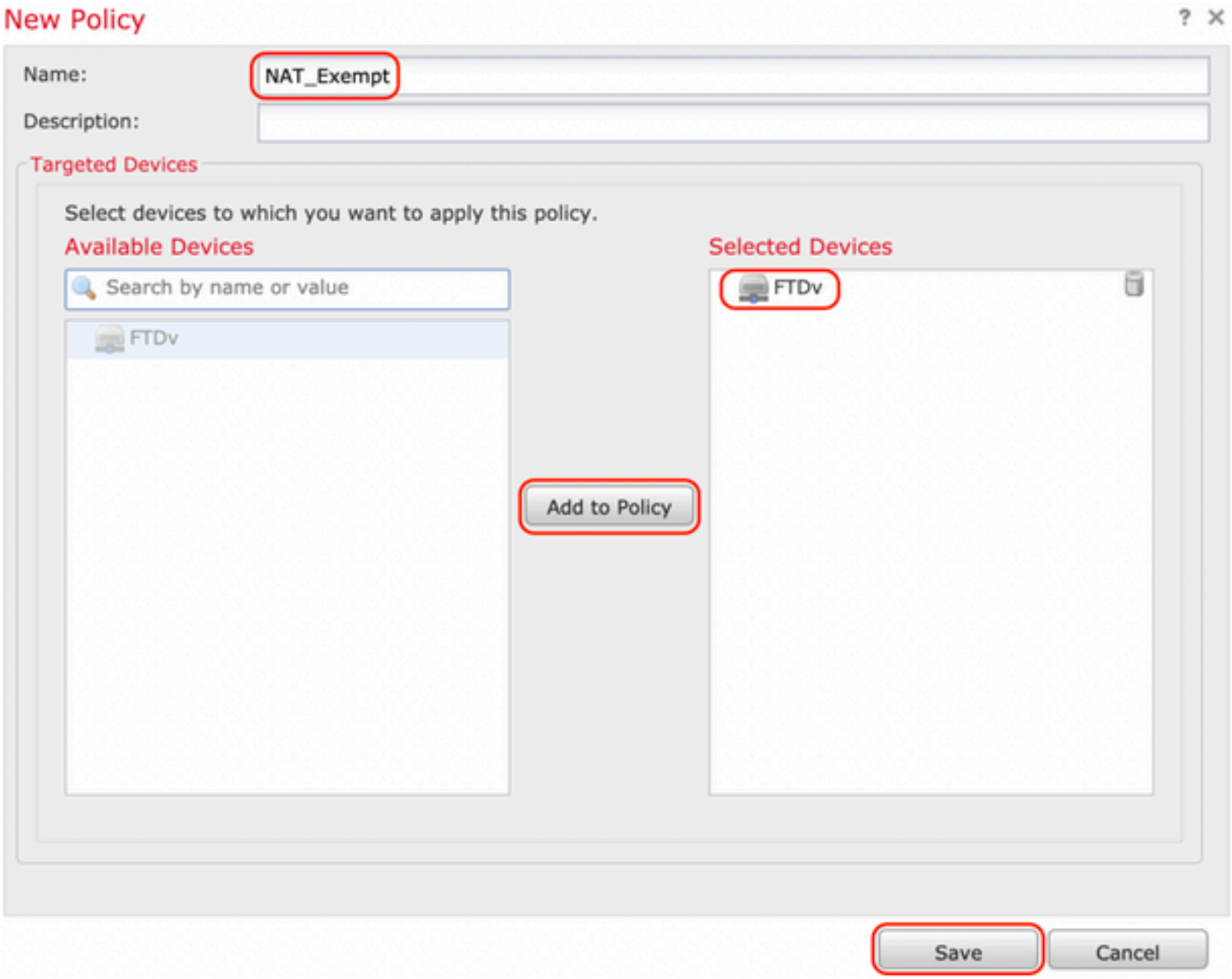
> **تحذير**: يزيل هذا الخيار إمكانية إستخدام سياسة التحكم في الوصول لفحص حركة المرور القادمة من المستخدمين. لا يزال يمكن إستخدام عوامل تصفية VPN أو قوائم التحكم في الوصول (ACL) القابلة للتنزيل لتصفية حركة مرور المستخدم. هذا أمر عام ينطبق على جميع شبكات VPN إذا تم تمكين خانة الاختيار هذه.



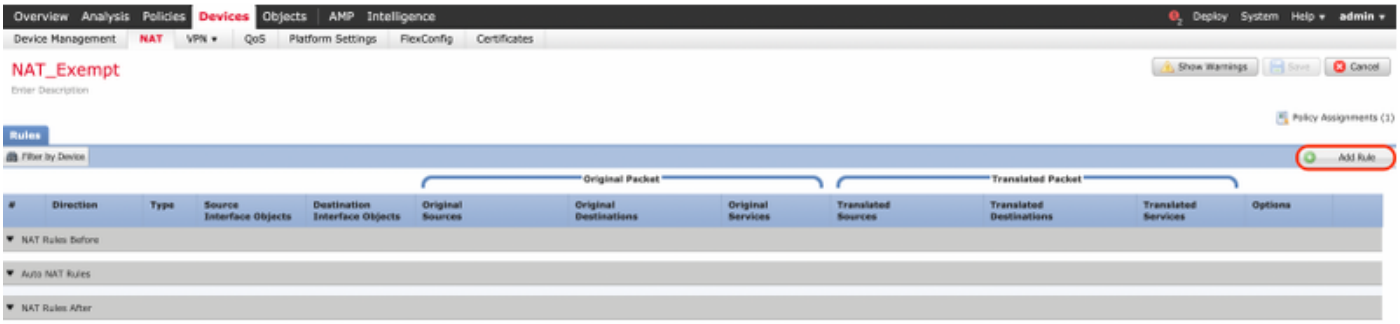
تكوين إستثناء NAT

شكلت NAT إعفاء بيان ل الـ VPN حركة مرور. يجب أن يكون إستثناء NAT في موضع لمنع حركة مرور VPN من مطابقة عبارة NAT أخرى وترجمة حركة مرور VPN بشكل غير صحيح.

الخطوة 1. انتقل إلى **الأجهزة > NAT** و Cأعد سياسة جديدة بالنقر فوق **سياسة جديدة > NAT للدفاع عن التهديد**.



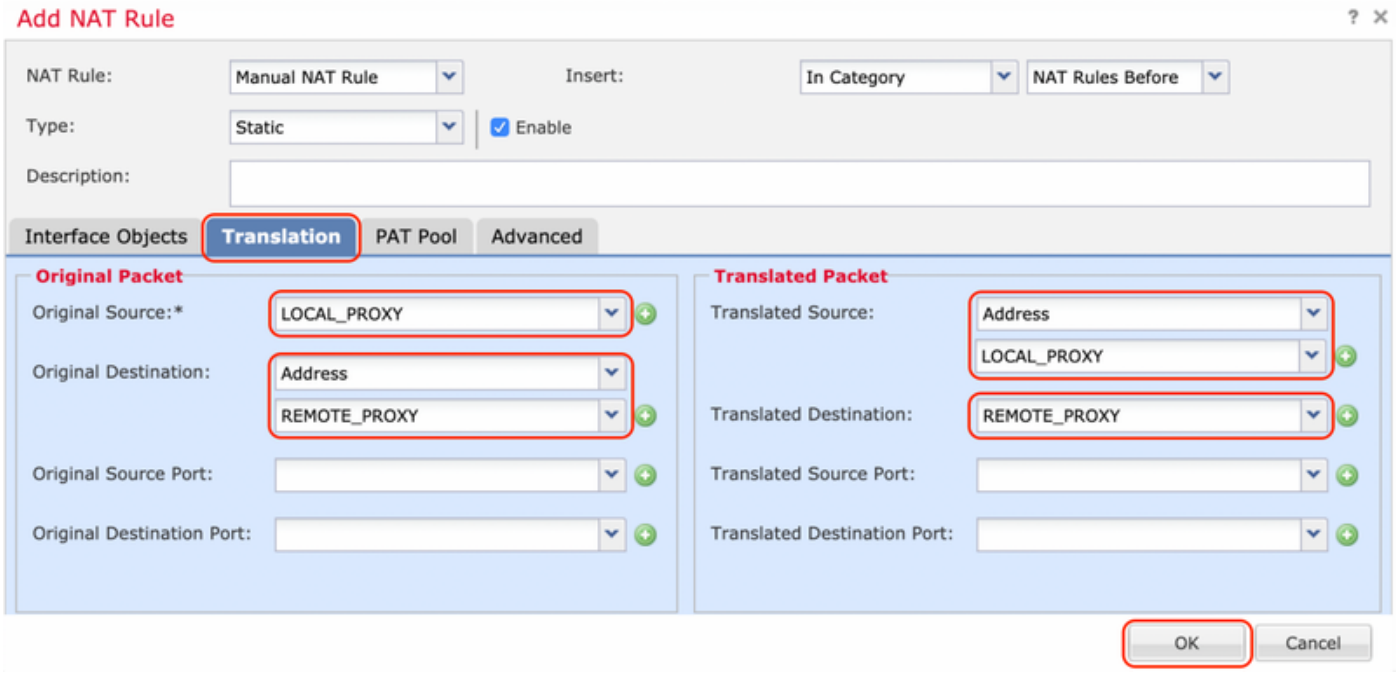
الخطوة 2. انقر فوق **إضافة قاعدة**.



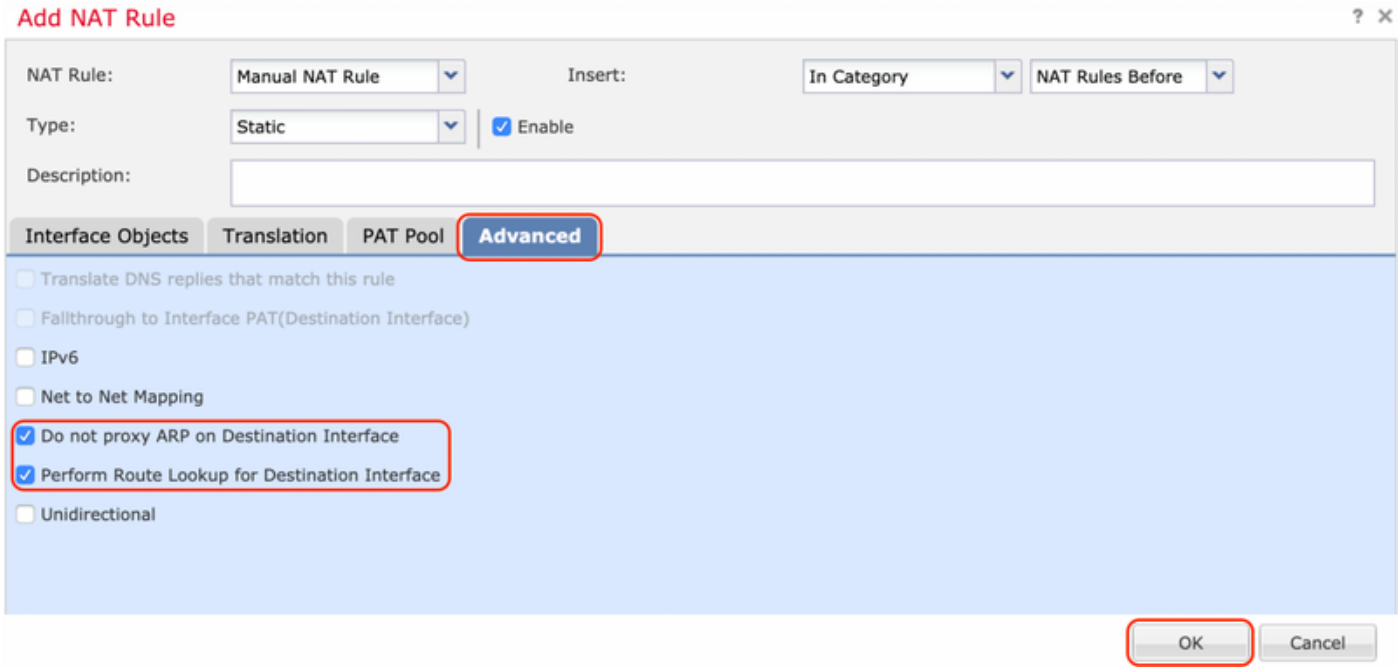
الخطوة 3. خلق جديد سائن إستاتيكي قاعدة nat.

أحلت الداخلي وقارن خارجي ل ال nat قاعدة. يؤدي تحديد الواجهات في علامة التبويب كائنات الواجهة إلى منع تأثير هذه القواعد على حركة المرور من الواجهات الأخرى.

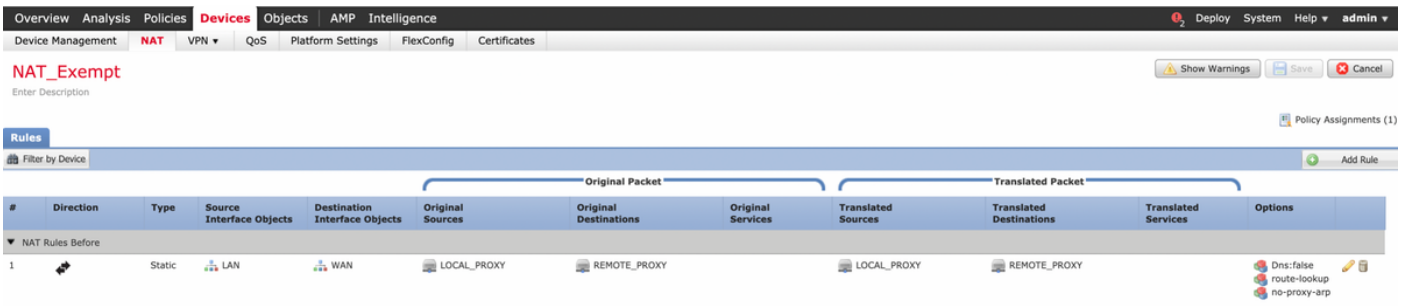
انتقل إلى علامة التبويب "ترجمة" وحدد الشبكات الفرعية المصدر والوجهة. بما أن هذا هو قاعدة إستثناء nat، ضمنت المصدر/الوجهة الأصلية والمصدر/الوجهة المترجم نفس.



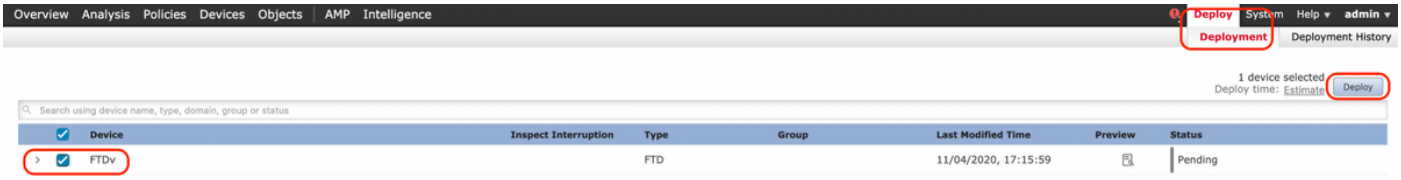
انقر فوق علامة التبويب خيارات متقدمة وقم بتمكين **no-proxy-arp** و**بحث المسار.**



أنقذت هذه القاعدة وأكدت النهاية nat جملة في ال nat القائمة.



الخطوة 4. بمجرد اكتمال التكوين، احفظ التكوين ثم قم بنشره إلى FTD.



التحقق من الصحة

ابدأ حركة مرور مثيرة للاهتمام من جهاز الشبكة المحلية أو يمكنك تشغيل الأمر أدناه packet-tracer على ASA.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

ملاحظة: يمثل النوع هنا = 128 والرمز=0 "طلب صدى" ICMPv6.

يصف القسم التالي الأوامر التي يمكنك تشغيلها على واجهة سطر الأوامر (CLI) ل ASAv أو FTD LINA للتحقق من حالة نفق IKEv2.

هذا مثال من إنتاج من ال ASA:

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
                    Status         Role
  6638313 2001:bbbb::1/500                              2001:cccc::1/500
                    READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/224 sec
Child sa: local selector  2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
          remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
          ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8


ciscoasa# show crypto ipsec sa detail
interface: outside
    Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1

      access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
      local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
      remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
      current_peer: 2001:cccc::1

      #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
      #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
      #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
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

```
      #pkts invalid pad (rcv): 0,
      #pkts invalid ip version (rcv): 0,
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
      path mtu 1500, ipsec overhead 94(64), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D95ECDB8
      current inbound spi : A0FD3FE6

    inbound esp sas:
      spi: 0xA0FD3FE6 (2700951526)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 1937408, crypto-map: VP
         sa timing: remaining key lifetime (kB/sec): (4055040/28535)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0xD95ECDB8 (3646868920)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 1937408, crypto-map: VPN
         sa timing: remaining key lifetime (kB/sec): (4193280/28535)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001


ciscoasa# show vpn-sessiondb detail l2l filter name 2001:cccc::1

Session Type: LAN-to-LAN Detailed

Connection   : 2001:cccc::1
Index        : 473                    IP Addr      : 2001:cccc::1
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA256  IPsec: (1)SHA1
Bytes Tx     : 352                    Bytes Rx     : 352
Login Time   : 12:27:36 UTC Sun Apr 12 2020
Duration     : 0h:06m:40s

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 473.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                 Hashing      : SHA256
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86000 Seconds
  PRF          : SHA256                 D/H Group    : 14
  Filter Name  :

IPsec:
  Tunnel ID    : 473.2
```

```
  Local Addr    : 2001:aaaa::/64/0/0
  Remote Addr   : 2001:dddd::/64/0/0
  Encryption    : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28400 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 23 Minutes
  Bytes Tx      : 352                   Bytes Rx     : 352
  Pkts Tx       : 11                    Pkts Rx      : 11
```

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء إنشاء نفق IKEv2 وإصلاحها على ASA و FTD، قم بتشغيل أوامر تصحيح الأخطاء التالية:

نظير شرط تصحيح الأخطاء للتشفير <peer IP>
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255

فيما يلي عينة عمل تصحيح أخطاء IKEv2 للرجوع إليها:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

المراجع

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html
https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html

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).