تكوين الموقع المستند إلى المسار إلى نفق VPN للموقع على FTD الذي تتم إدارته بواسطة FMC

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين موقع ثابت مستند إلى مسار إلى نفق VPN للموقع على دفاع ضد تهديد FirePOWER تتم إدارته بواسطة مركز إدارة FirePOWER.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- فهم أساسي لكيفية عمل نفق الشبكة الخاصة الظاهرية (VPN).
- تعرف على كيفية التنقل عبر وحدة التحكم في إدارة اللوحة الأساسية (FMC).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- مركز إدارة Cisco Firepower (FMC)، الإصدار 6.7.0
- Cisco Firepower Threat Defense (FTD)، الإصدار 6.7.0

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

تسمح الشبكة الخاصة الظاهرية (VPN) المستندة إلى المسار بتشفير حركة مرور البيانات المميزة أو إرسالها عبر نفق VPN، واستخدام توجيه حركة مرور البيانات بدلا من توجيه السياسة/الوصول إلى قائمة التحكم كما هو الحال في شبكة VPN المستندة إلى السياسة أو التشفير. تم تعيين مجال التشفير للسماح بأي حركة مرور تدخل نفق IPsec. تم تعيين محددات حركة مرور البيانات المحلية والبعيدة ل IPsec على 0.0.0.0/0.0.0.0. وهذا يعني أن أي حركة مرور يتم توجيهها إلى نفق IPsec يتم تشفيرها بغض النظر عن الشبكة الفرعية للمصدر/الوجهة.

يركز هذا المستند على تكوين واجهة النفق الظاهرية الثابتة (SVTI). للحصول على تكوين واجهة النفق الظاهرية الديناميكية (DVTI) على جدار الحماية الآمن، الرجاء إعادة الرد على هذا المستند.

القيود والحدود

هذه قيود وقيود معروفة للأنفاق المستندة إلى المسار على FTD:

- يدعم IPsec فقط. GRE غير مدعوم.
- يدعم واجهات IPv4 فقط، بالإضافة إلى IPv4 أو الشبكات المحمية أو حمولة الشبكة الخاصة الظاهرية (لا يوجد دعم ل IPv6).
- يتم دعم التوجيه الثابت وبروتوكول التوجيه الديناميكي لبروتوكول BGP فقط لواجهات VTI التي تصنف حركة مرور البيانات لشبكة VPN (لا يوجد دعم للبروتوكولات الأخرى مثل OSPF و RIP وما إلى ذلك).
- فقط 100 VTIs ساندت لكل قارن.
- لا يتم دعم VTI على مجموعة FTD.
- VTI غير مدعوم في هذه السياسات:
  - جودة الخدمة
  - NAT
  - إعدادات النظام الأساسي

لم تعد هذه الخوارزميات مدعومة على الإصدار 6. 7.0 من FMC/FTD لأنفاق الشبكة الخاصة الظاهرية (VPN) الجديدة (تدعم FMC جميع التشفير الذي تمت إزالته لإدارة بروتوكول FTD < 6. 7):

- تشفير 3DES و DES و NULL غير مدعوم في نهج IKE.

- مجموعات DH 1 و 2 و 24 غير مدعومة في نهج IKE واقتراح IPsec.
- تكامل MD5 غير مدعوم في نهج IKE.
- PRF MD5 غير مدعوم في نهج IKE.
- خوارزميات التشفير DES و 3DES و AES-GMAC و AES-GMAC-192 و AES-GMAC-256 غير مدعومة في اقتراح IPsec.

ملاحظة: ينطبق هذا على كل من الموقع إلى مسار الموقع استنادا إلى أنفاق الشبكة المستندة إلى السياسة. لترقية FTD أقدم إلى 6.7 من FMC، فإنه يقوم بتشغيل فحص ما قبل التحقق من الصحة يحذر المستخدم من التغييرات التي تمت إزالتها والتي تمنع الترقية. المتعلقة بالشفرات

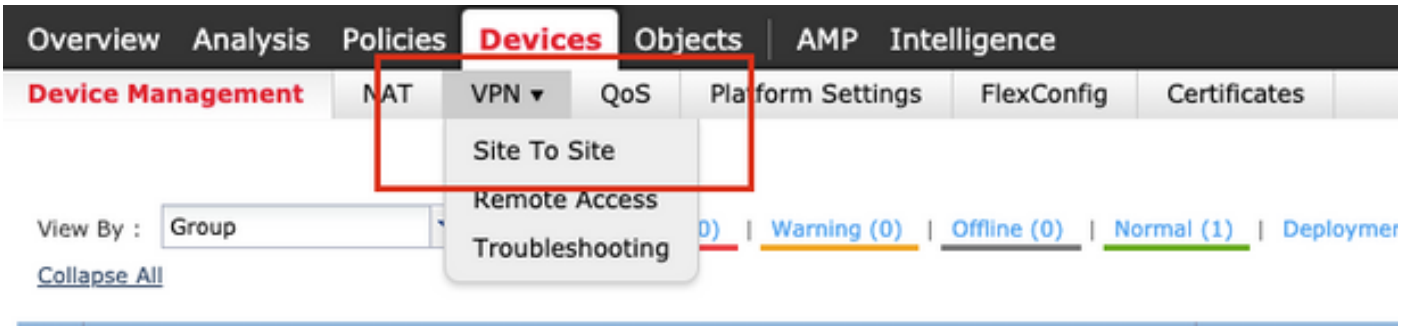
موقع إلى نفق VPN للموقع	التكوين متوفر	تتم إدارة برنامج FTD 6.7 من خلال وحدة التحكم FMC 6.7
تتوفر شفرات ضعيفة ولكن ال يمكن إستخدامها لتكوين جهاز FTD 6.7.	تتوفر شفرات ضعيفة ولكن ال يمكن إستخدامها لتكوين جهاز FTD 6.7.	تثبيت جديد
بعد ترقية FTD، وافترض أن النظير لم يغير إعداداته، ثم يتم إنهاء النفق.	الترقية من واجهة مستخدم FMC 6.7، يعرض فحص التحقق من الصحة المسبقة خطأ. تم حظر الترقية حتى إعادة التكوين.	الترقية: تم تكوين FTD فقط باستخدام شفرات ضعيفة
بعد ترقية "برنامج الإرسال السريع (FTD)"، وافترض أن النظير لديه شفرات قوية، ثم يعيد إنشاء النفق.	الترقية من واجهة مستخدم FMC 6.7، يعرض فحص التحقق من الصحة المسبقة خطأ. تم حظر الترقية حتى إعادة التكوين.	الترقية: تم تكوين FTD فقط باستخدام بعض الشفرات الضعيفة وبعض الشفرات القوية
يسمح ب DES	يسمح ب DES	الترقية: بلد الفئة C (ليس لديه ترخيص تشفير قوي)

.

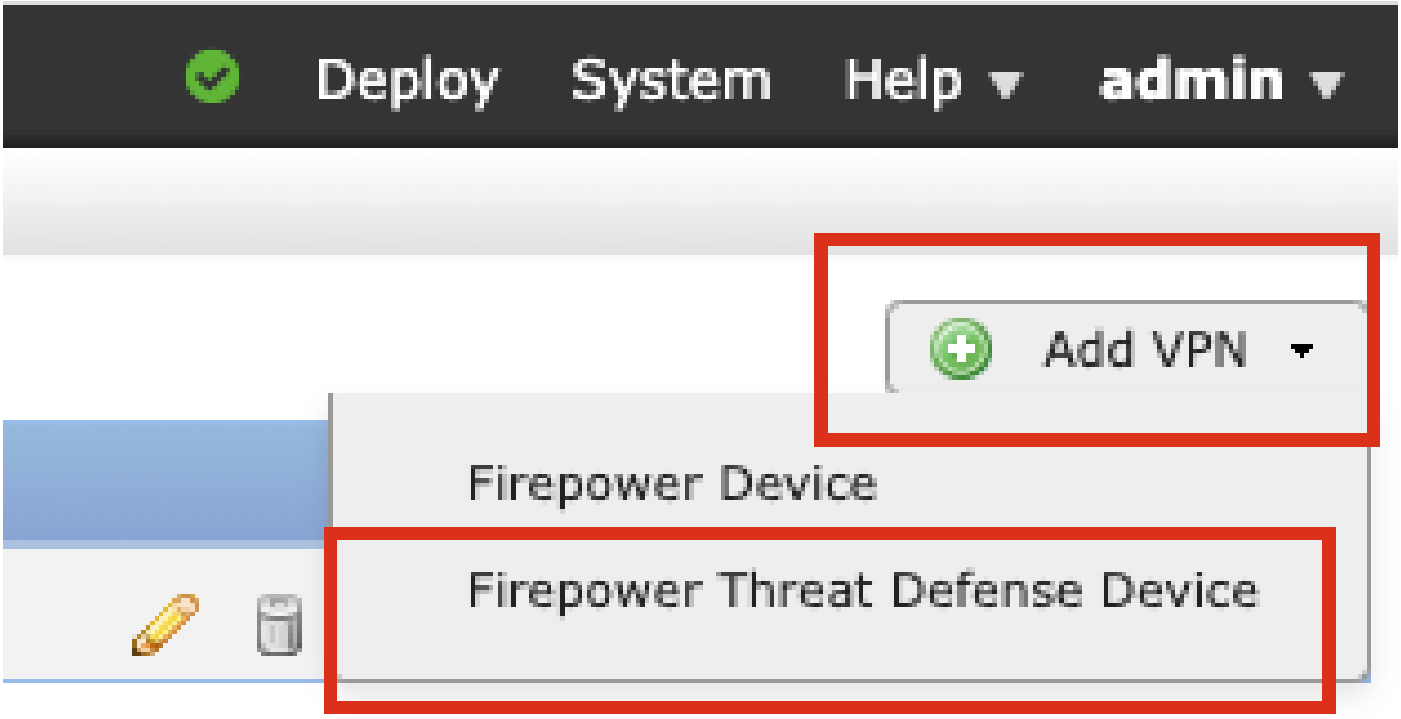
ملاحظة: ال يلزم منح ترخيص إضافي، ويمكن تكوين شبكة VPN المستندة إلى المسار في أوضاع الترخيص وكذلك التقييم. من دون التوافق مع التشفير (تمكين المميزات التي يتم التحكم فيها بالتصدير)، يمكن إستخدام DES فقط خوارزمية تشفير.

خطوات التكوين على FMC

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



الخطوة 2. انقر فوق إضافة شبكة VPN، واختر جهاز الدفاع ضد تهديد FirePOWER، كما هو موضح في الصورة.

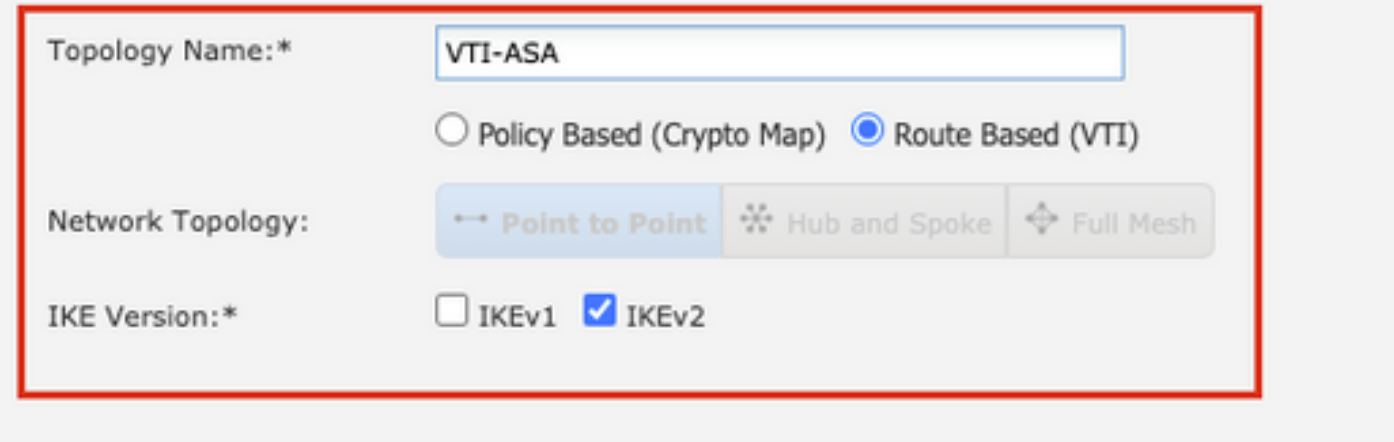


الخطوة 3. توفر اسم مخطط وحدد نوع شبكة VPN المستندة إلى المسار (VTI). أختر إصدار IKE.

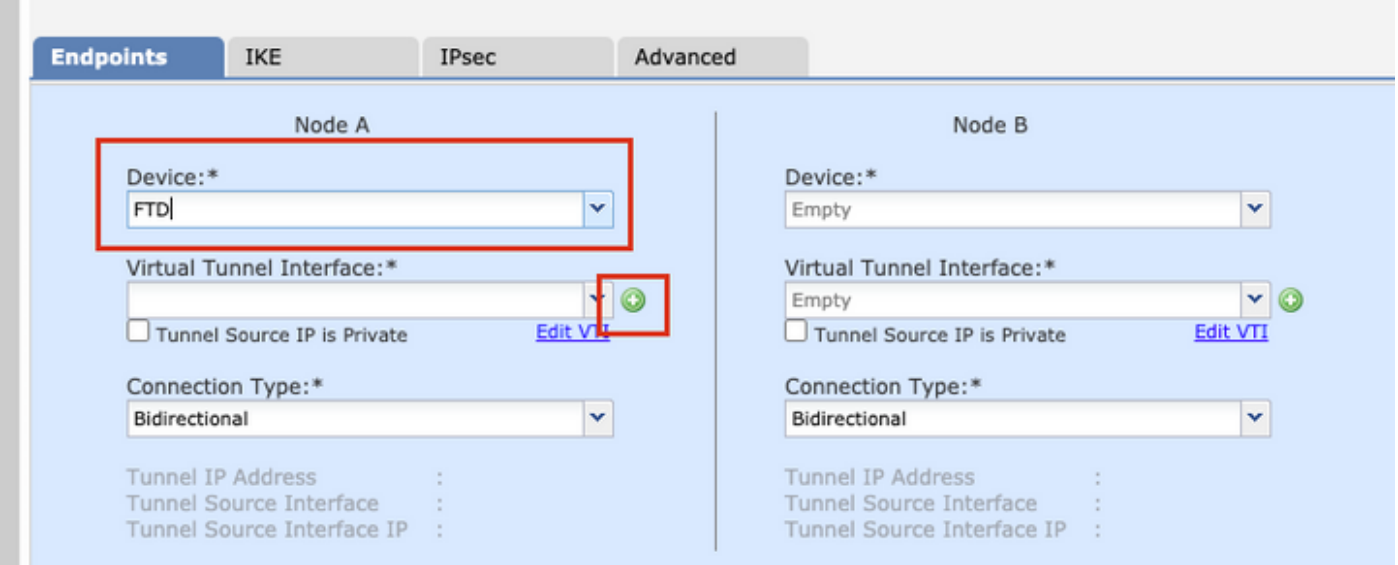
وألأغراض هذه المظاهرة:

اسم الطوبولوجيا: VTI-ASA

إصدار IKE: IKEv2



الخطوة 4. أختر الجهاز الذي يجب تكوين النفق عليه، أو يمكنك إختيار إضافة واجهة قالب ظاهري (انقر فوق + أيقونة)، أو حدد واحدا من القائمة الموجودة.



الخطوة 5. تحديد معلمات واجهة النفق الظاهري الجديدة. وانقر فوق OK.

ولأغراض هذه المظاهرة:

الاسم: VTI-ASA

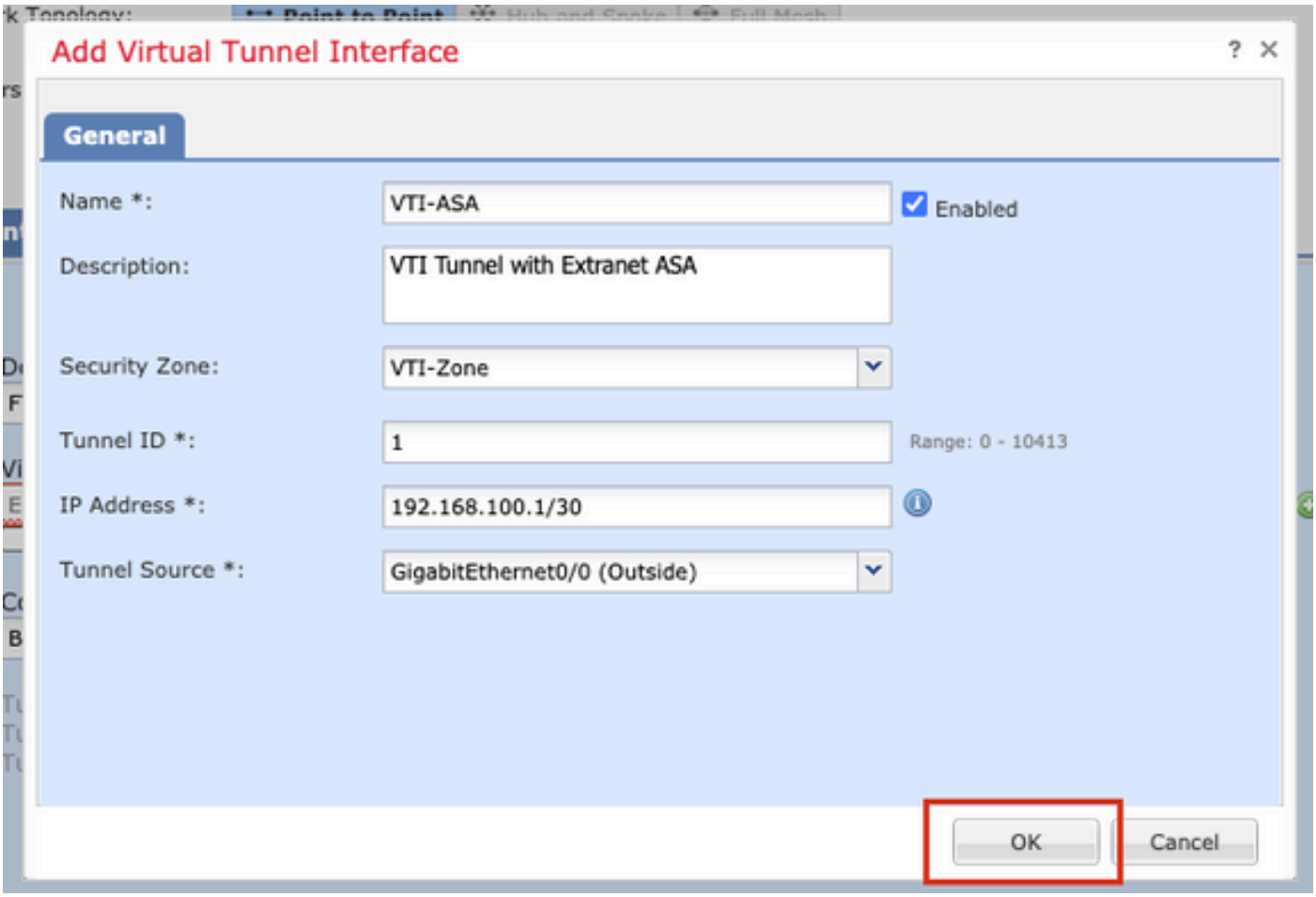
الوصف (إختياري): نفق VTI مع Extranet ASA

المنطقة الأمنية: منطقة vTI-Zone

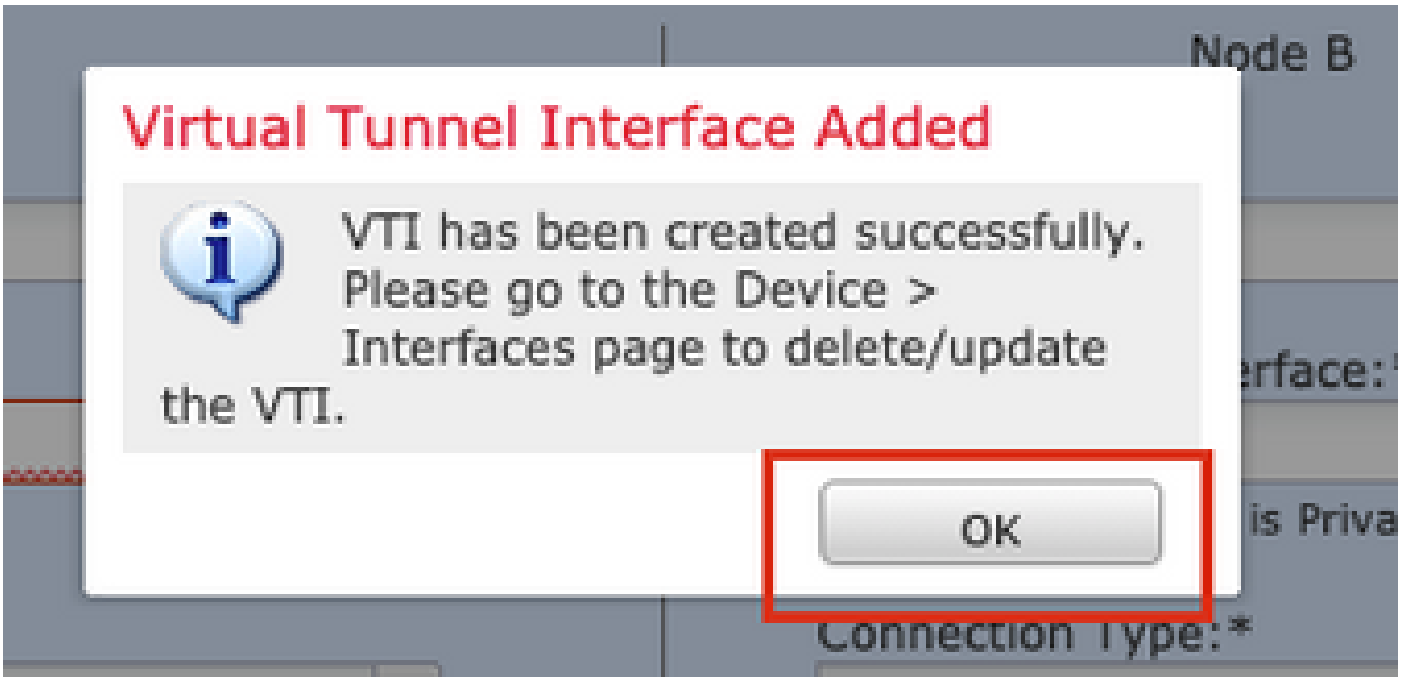
معرف النفق: 1

عنوان IP: 192.168.100.1/30

مصدر النفق: GigabitEthernet0/0 (خارجي)



الخطوة 6. طقطقت ok على المنبثق يذكر أن ال VTI جديد خلقت.



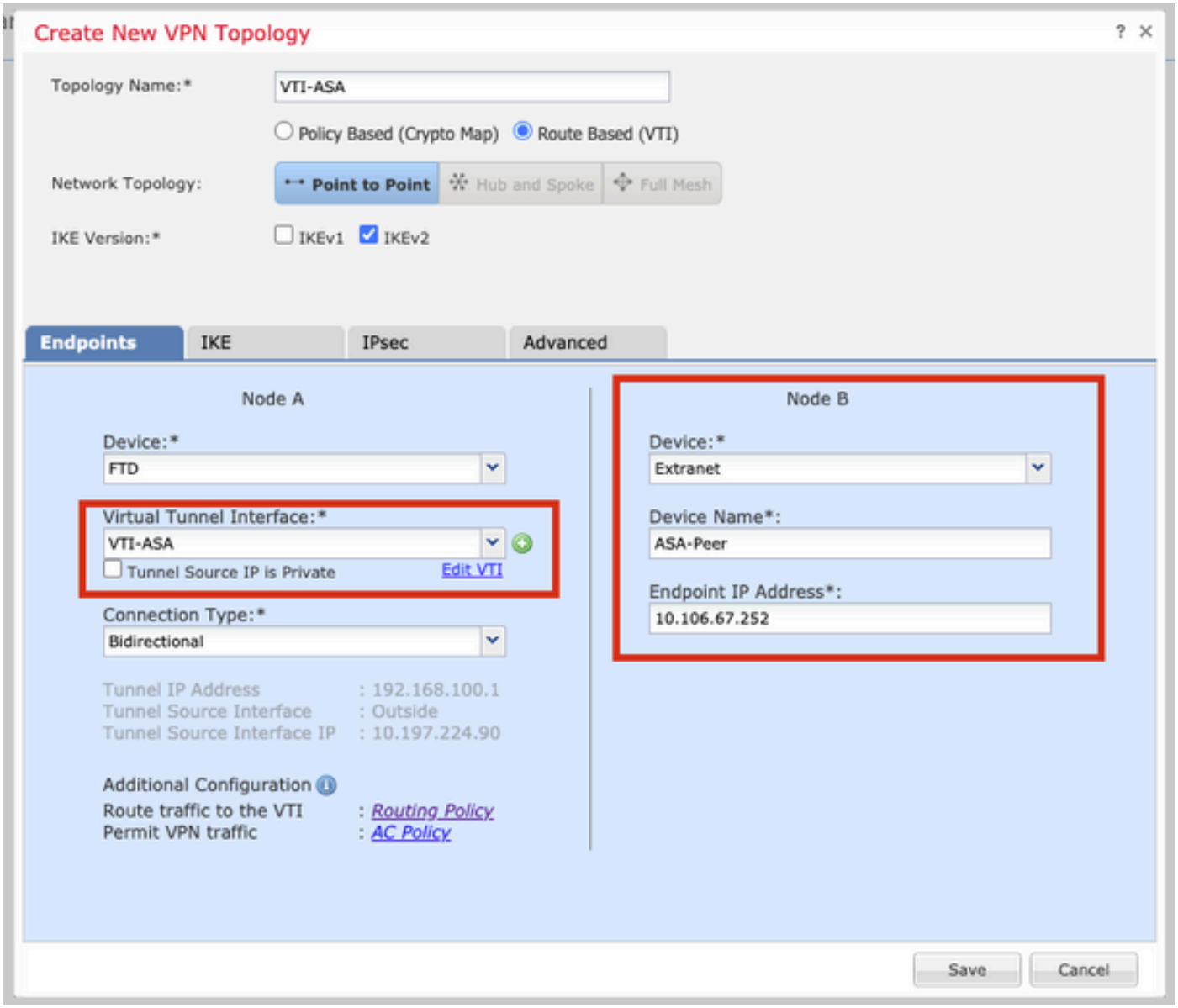
الخطوة 7. أخترت ال VTI newly created أو VTI أن يتواجد تحت الفعلي نفق قارن. قم بتوفير المعلومات للعقدة ب (والتي هي جهاز النظير).

ولأغراض هذه المظاهرة:

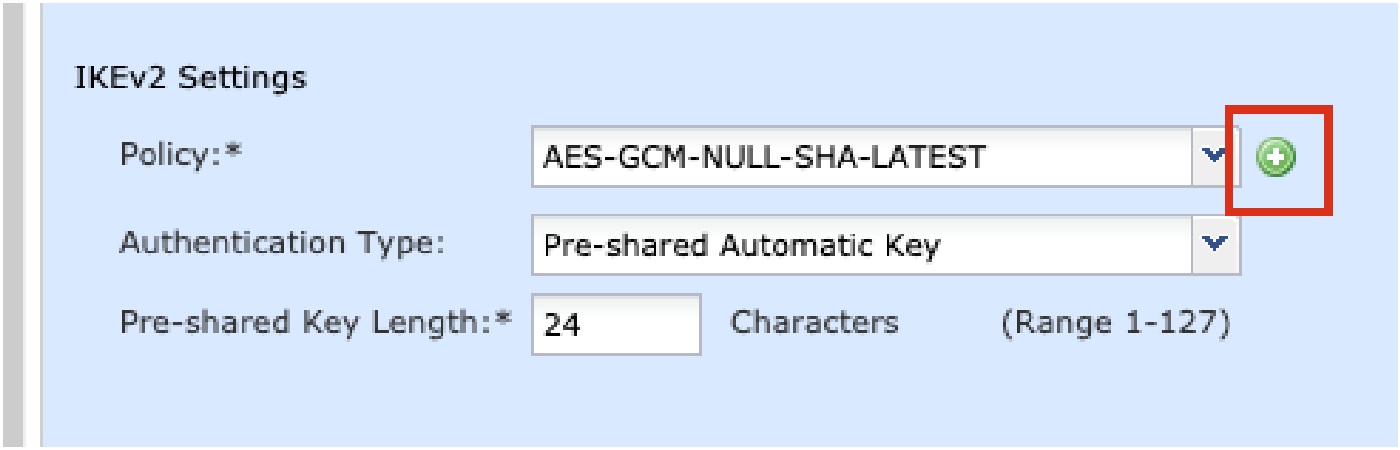
الجهاز: إكسترانت

اسم الجهاز: ASA-Peer

عنوان IP لنقطة النهاية: 10.106.67.252



الخطوة 8. انتقل إلى علامة التبويب IKE. يمكنك إختيار إستخدام نهج محدد مسبقا أو النقر فوق الزر + الموجود بجوار علامة التبويب نهج وإنشاء علامة تبويب جديدة.



الخطوة 9. (إختياري، إذا قمت بإنشاء سياسة IKEv2 جديدة.) قم بتوفير اسم للنهج وحدد الخوارزميات التي سيتم إستخدامها في النهج. انقر فوق حفظ.

ولأغراض هذه المظاهرة:

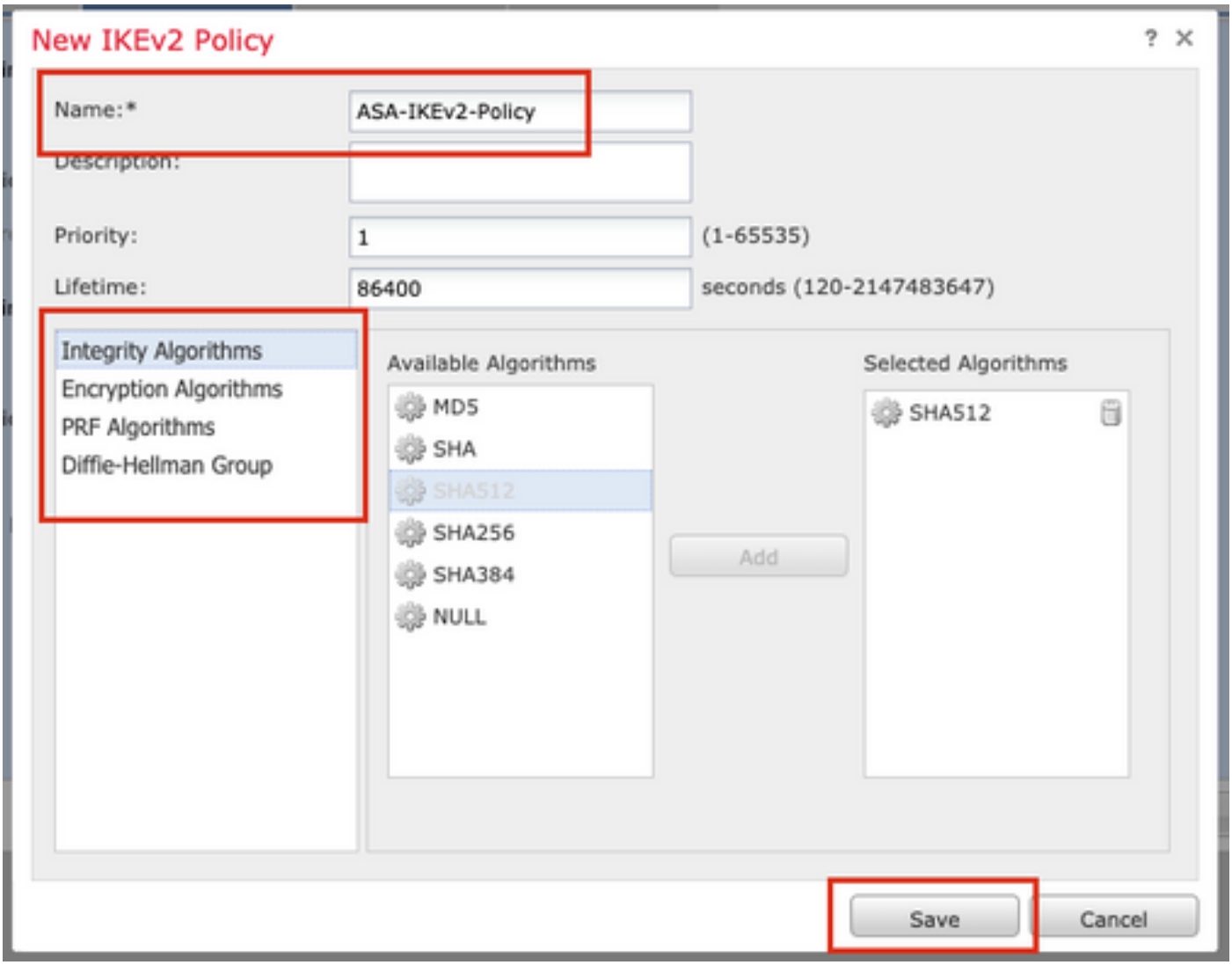
الاسم: ASA-IKEv2-Policy

خوارزميات التكامل: SHA-512

خوارزميات التشفير: AES-256

خوارزميات PRF: SHA-512

مجموعة Diffie-Hellman: 21



الخطوة 10. أختر النهج الموجود أو الذي تم إنشاؤه حديثا. حدد نوع المصادقة. إذا تم إستخدام مفتاح يدوي مشترك مسبقا، فقم بتوفير المفتاح في مربعي المفتاح وتأكيد المفتاح.

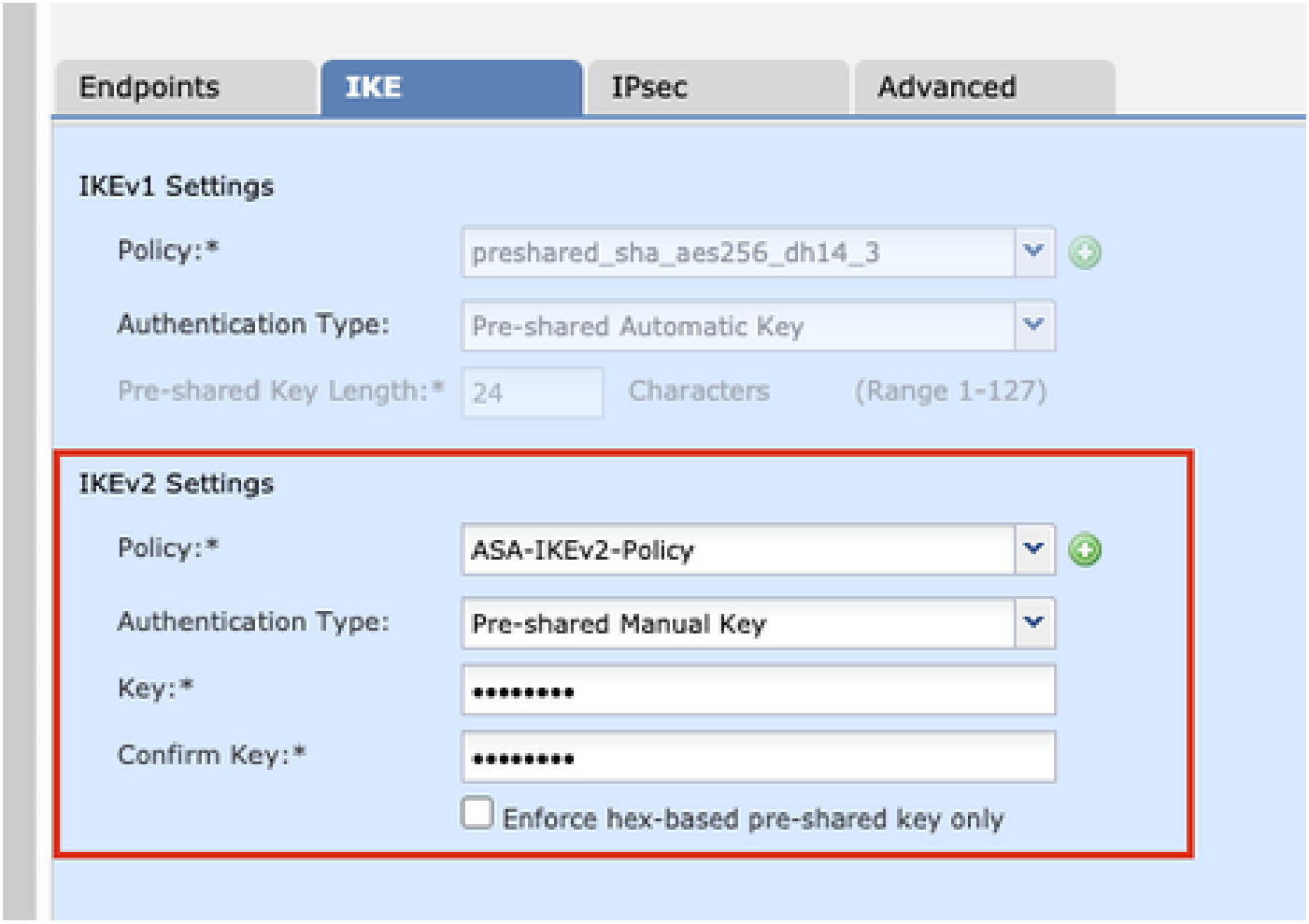
وألأغراض هذه المظاهرة:

النهج: ASA-IKEv2-Policy

نوع المصادقة: مفتاح يدوي مشترك مسبقا

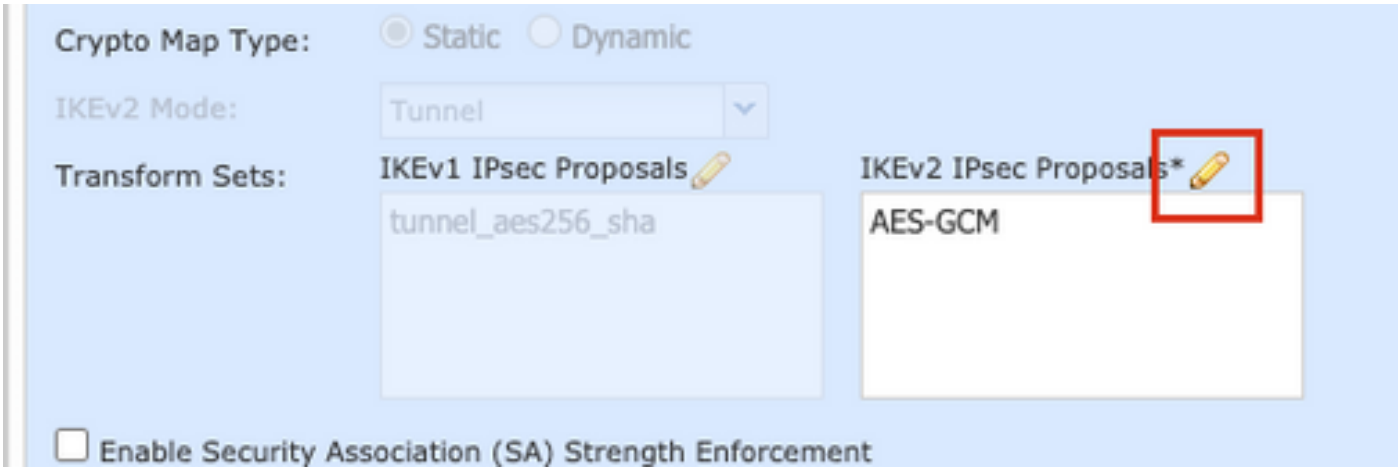
المفتاح: Cisco123

تأكيد المفتاح: Cisco123



ملاحظة: إذا تم تسجيل كل نقطتي النهاية على وحدة التحكم في الإدارة الأساسية (FMC) نفسها، يمكن إستخدام خيار المفتاح التلقائي المشترك مسبقا.

الخطوة 11. انتقل إلى علامة التبويب IPsec. يمكنك إختيار إستخدام مقترح IPsec المعرف مسبقا أو إنشاء مقترح جديد. انقر فوق الزر Editbutton المجاور لعلامة التبويب اقتراح IKEv2 IPsec.



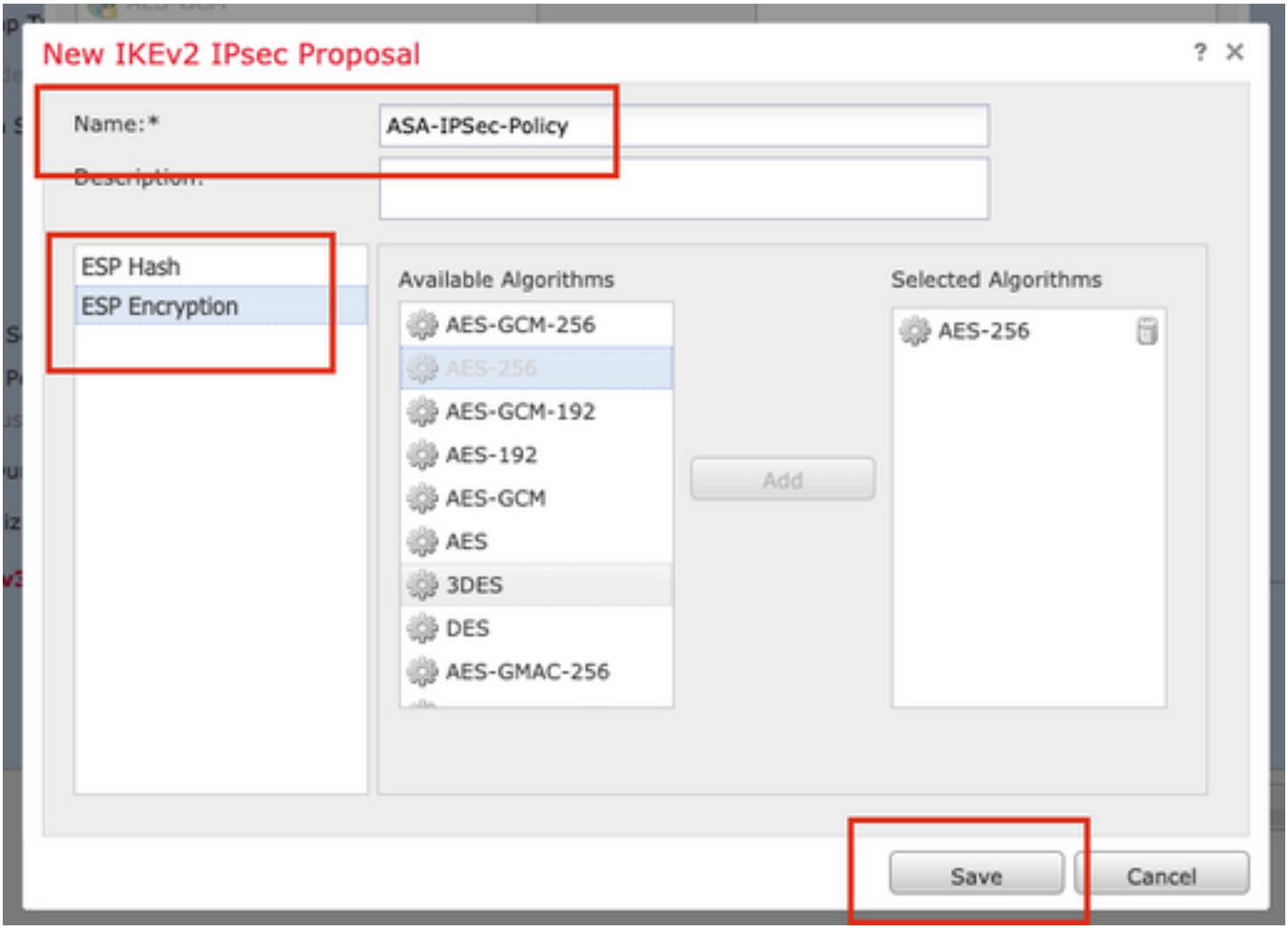
الخطوة 12. (إختياري، إذا قمت بإنشاء مقترح IKEv2 IPsec جديد.) قم بتوفير اسم للعرض وحدد الخوارزميات التي سيتم إستخدامها في العرض. انقر فوق حفظ.

ولأغراض هذه المظاهرة:

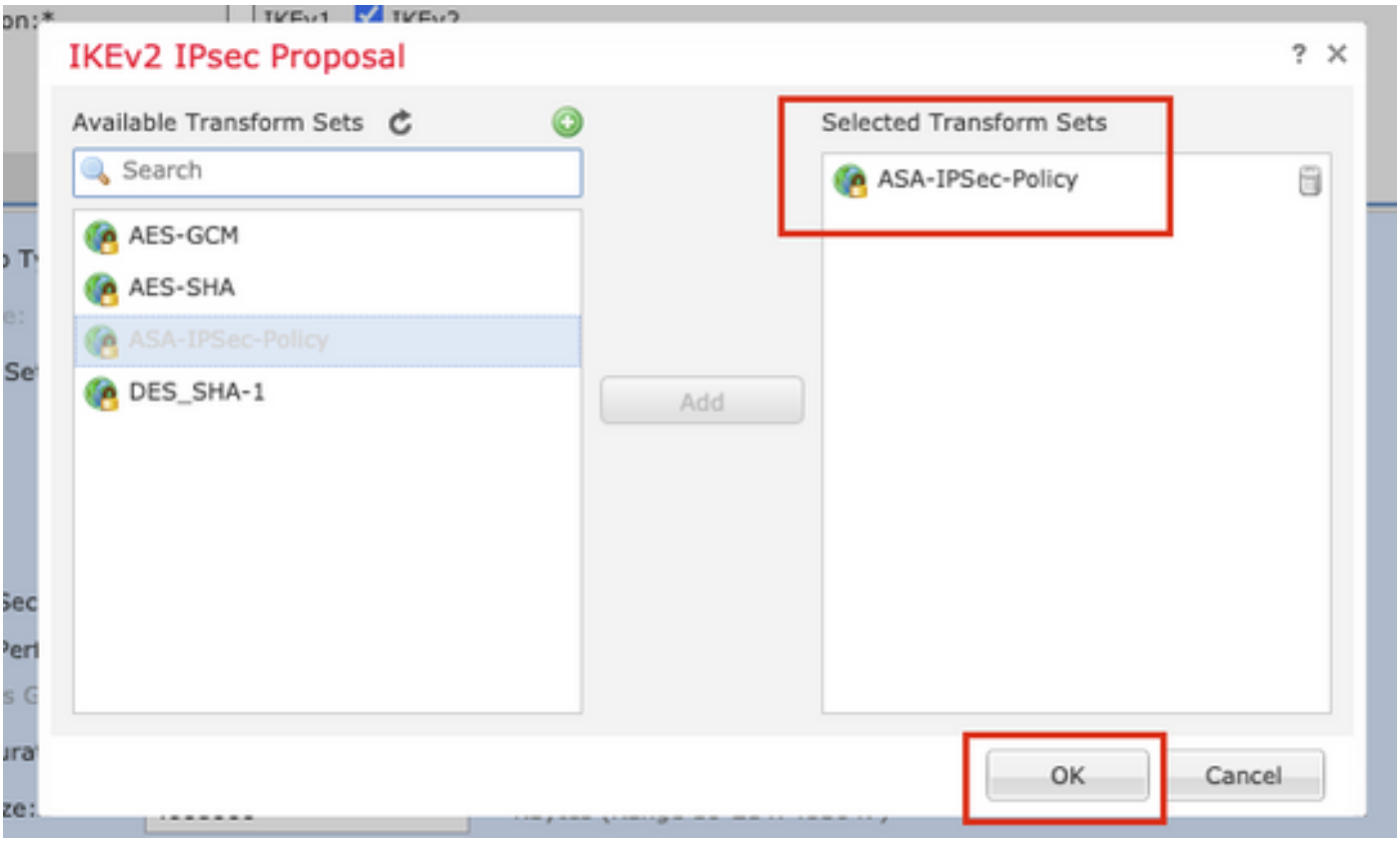
الاسم: ASA-IPSec-Policy

تجزئة ESP: SHA-512

تشفير ESP: AES-256



الخطوة 13. أختر المقترح أو المقترح الذي تم إنشاؤه حديثا من قائمة الاقتراحات المتوفرة. وانقر فوق OK.



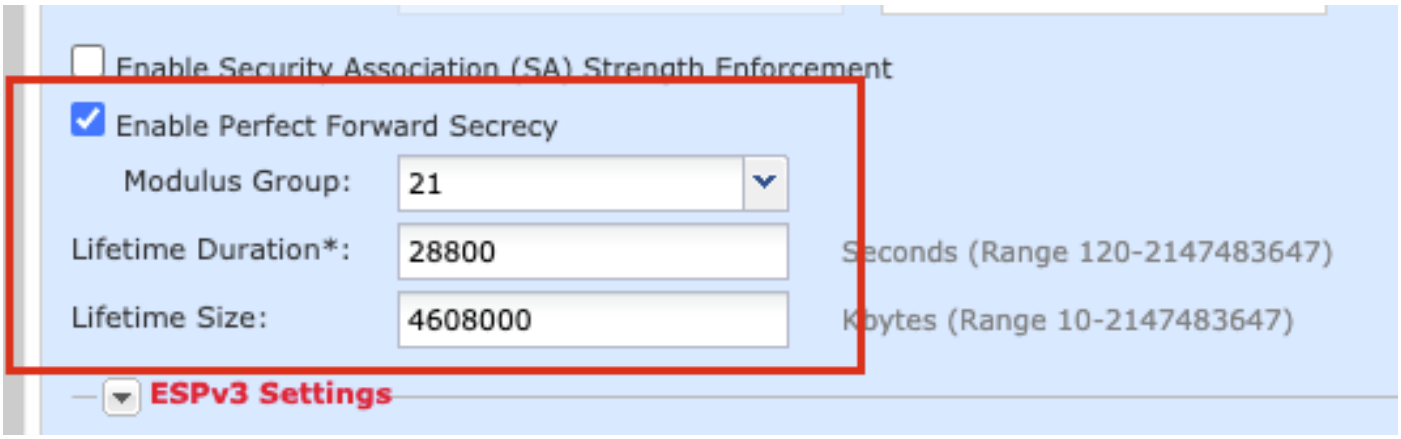
الخطوة 14. (إختياري) أخترإعدادات سرية إعادة التوجيه المثالية. تكوين مدة العمر الافتراضي لبروتوكول IPsec وحجم العمر الافتراضي له.

وألأغراض هذه المظاهرة:

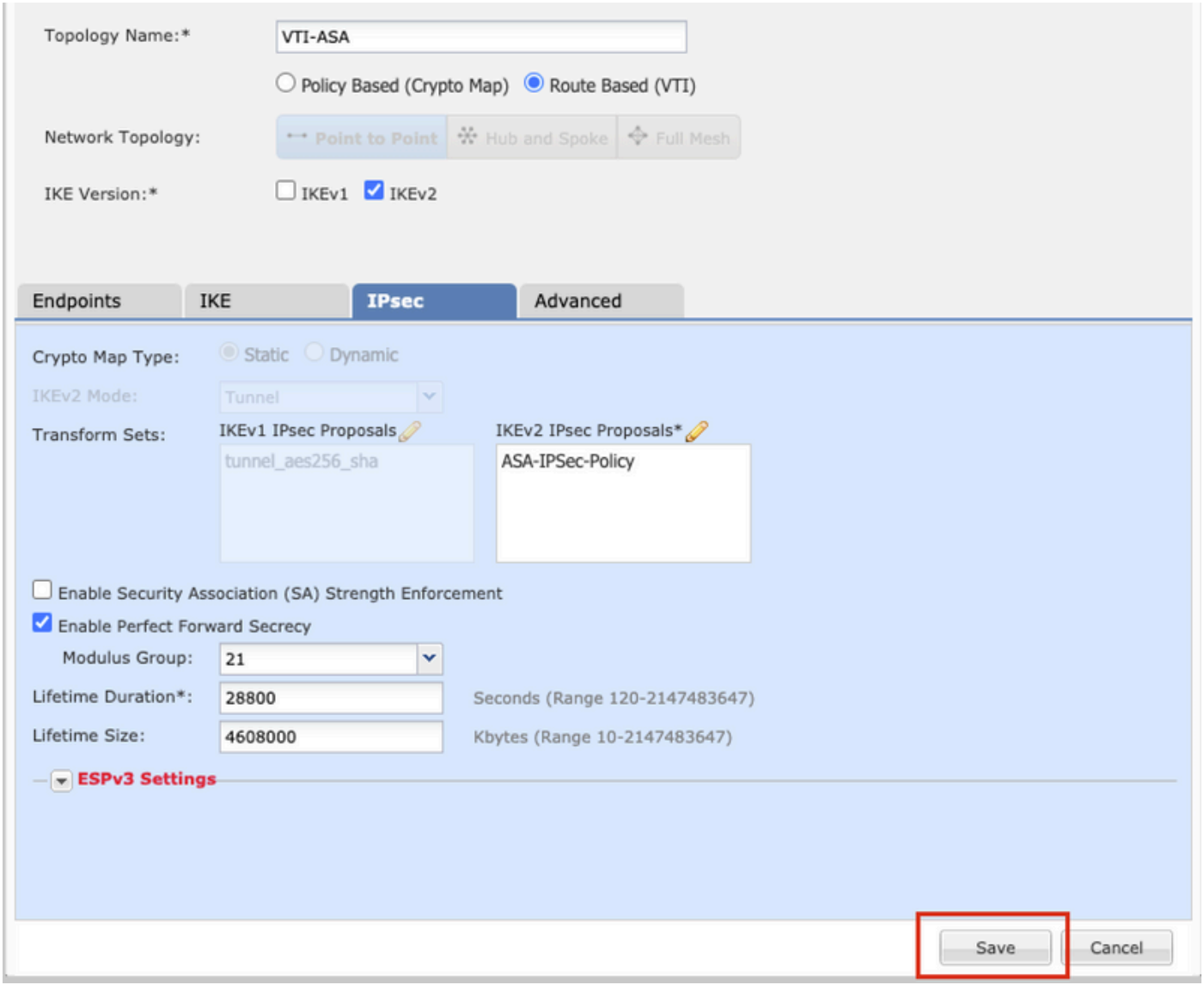
السرية التامة لإعادة التوجيه: مجموعة Modulus 21

مدة العمر: 28800 (الافتراضي)

حجم العمر الافتراضي: 4608000 (الافتراضي)



الخطوة 15. تحقق من الإعدادات التي تم تكوينها. انقر فوق حفظ ، كما هو موضح في هذه الصورة.



الخطوة 16. تكوين نهج التحكم في الوصول. انتقل إلى السياسات > التحكم في الوصول > التحكم في الوصول. تحرير النهج المطبق على FTD.

ملاحظة: لا يعمل بروتوكول السماح باتصال VPN مع أنفاق الشبكة الخاصة الظاهرية (VPN) المستندة إلى المسار. يجب تكوين قواعد التحكم في الوصول لكل من المناطق الداخلة أو الخارجة في المناطق.

قم بتوفير مناطق المصدر ومناطق الوجهة في علامة تبويب المناطق.

توفير شبكات المصدر، شبكات الوجهة في علامة التبويب الشبكات. انقر فوق إضافة (Add).

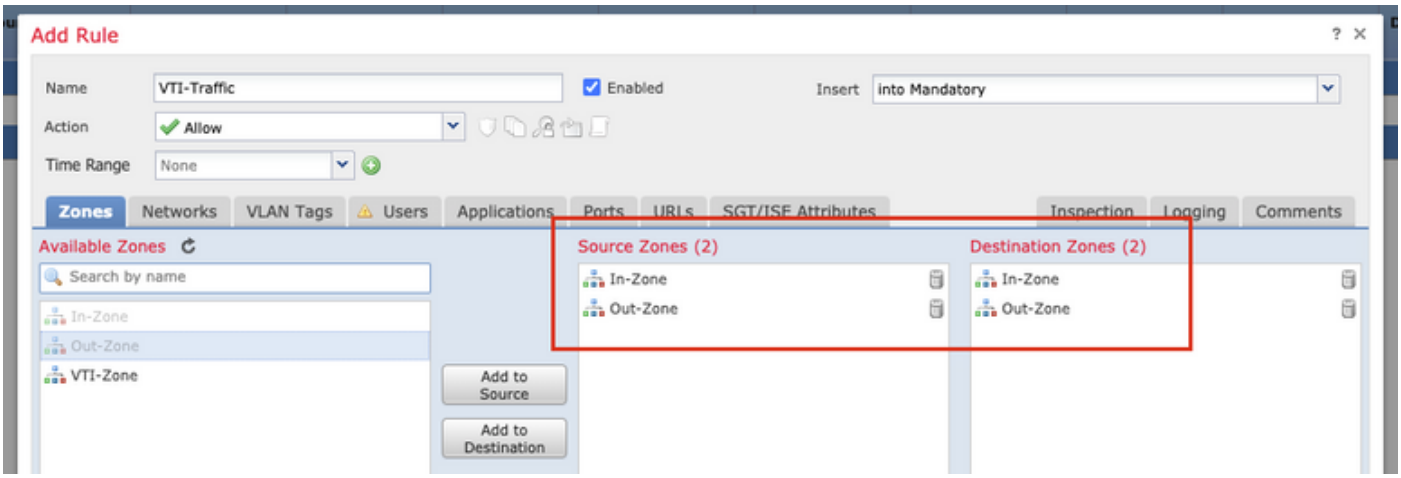
وألأغراض هذه المظاهرة:

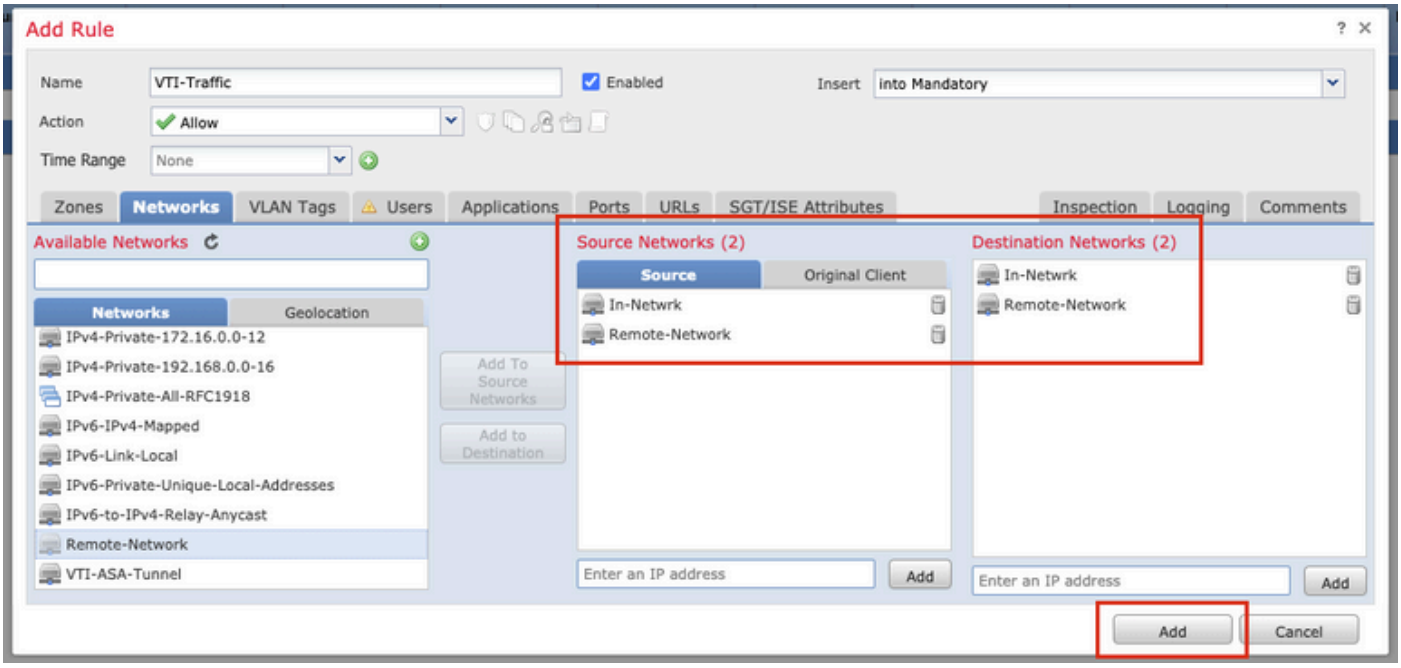
المناطق المصدر: داخل المنطقة وخارجها

المناطق المستهدفة: خارج المنطقة وداخل المنطقة

الشبكات المصدر: الشبكة الداخلية والشبكة البعيدة

الشبكات الوجهة: الشبكة البعيدة والشبكة الداخلية





الخطوة 17. قم بإضافة التوجيه عبر نفق VTI. انتقل إلى الأجهزة > إدارة الأجهزة. قم بتحرير الجهاز الذي تم تكوين نفق VTI عليه.

انتقل إلى المسار الثابت ضمن علامة التبويب التوجيه. انقر على إضافة مسار.

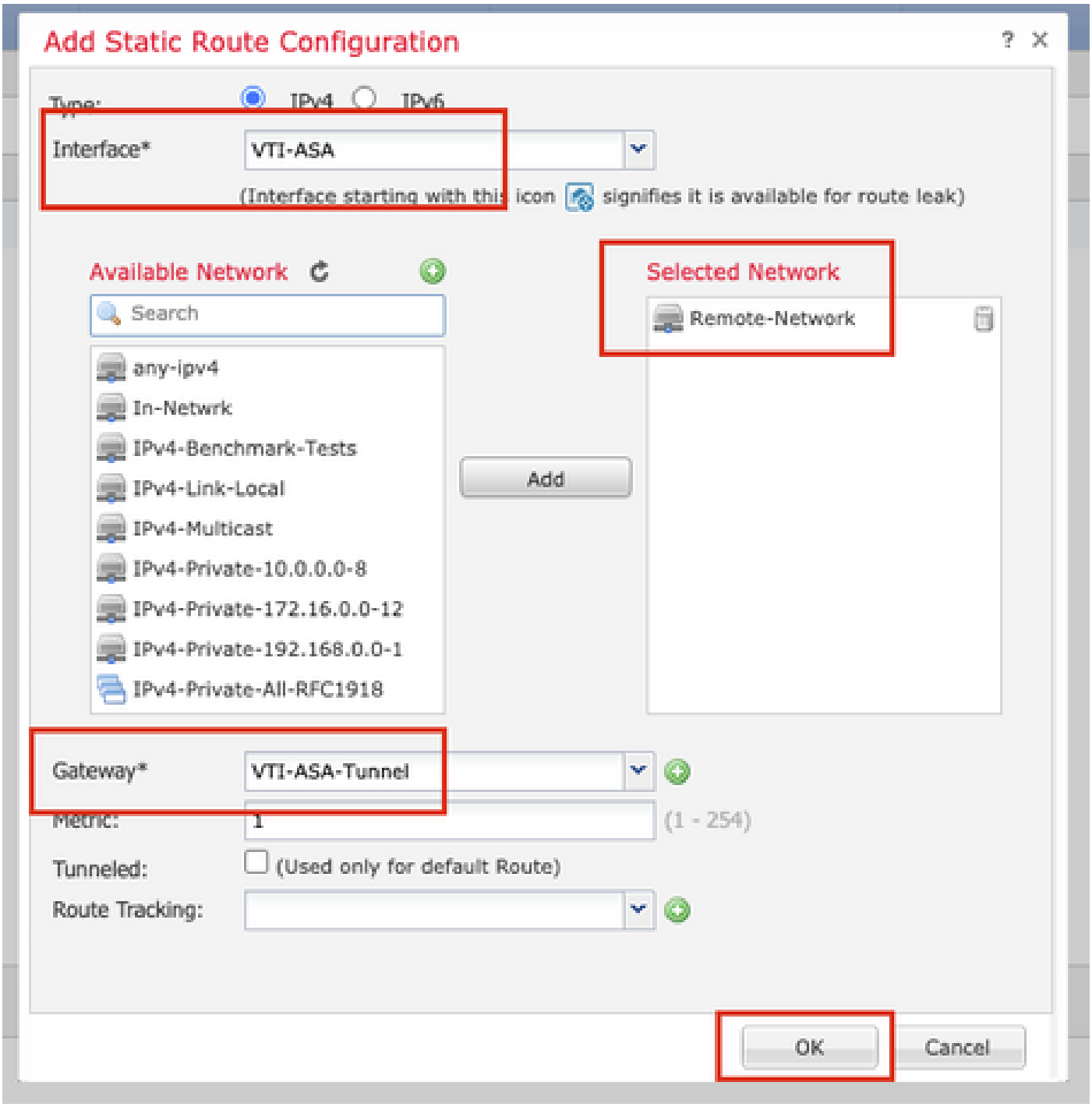
قم بتوفير الواجهة، واختر الشبكة، وتقديم البوابة. وانقر فوق OK.

وألأغراض هذه المظاهرة:

الواجهة: VTI-ASA

الشبكة: الشبكة عن بعد

البوابة: vti-asa-tunnel



الخطوة 18. انتقل إلى نشر > نشر. أختر الـ FTD الذي تحتاج أن يكون نشرت إليه أي تشكيل، وطقطقة ينشر.

تم دفع التكوين إلى واجهة سطر الأوامر (CLI) الخاصة بـ FTD بعد عملية النشر الناجحة:

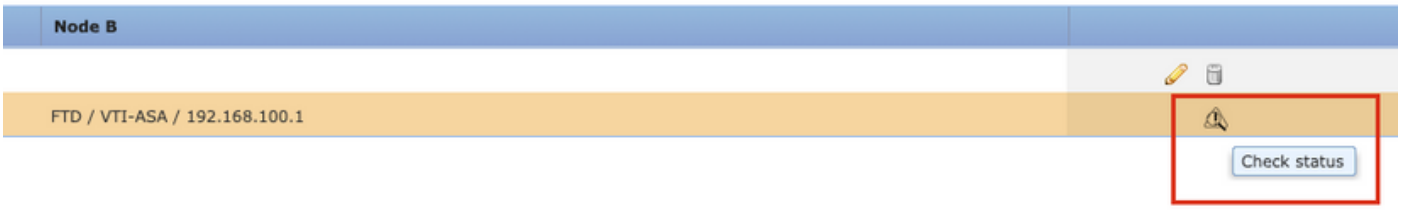
```
<#root>

crypto ikev2 policy 1


 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 86400
```

```
crypto ikev2 enable Outside


crypto ipsec ikev2 ipsec-proposal CSM_IP_1


 protocol esp encryption aes-256
 protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1


 set ikev2 ipsec-proposal CSM_IP_1
 set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****


interface Tunnel1


 description VTI Tunnel with Extranet ASA

 nameif VTI-ASA


 ip address 192.168.100.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 10.106.67.252
 tunnel mode ipsec ipv4

 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

التحقق من الصحة

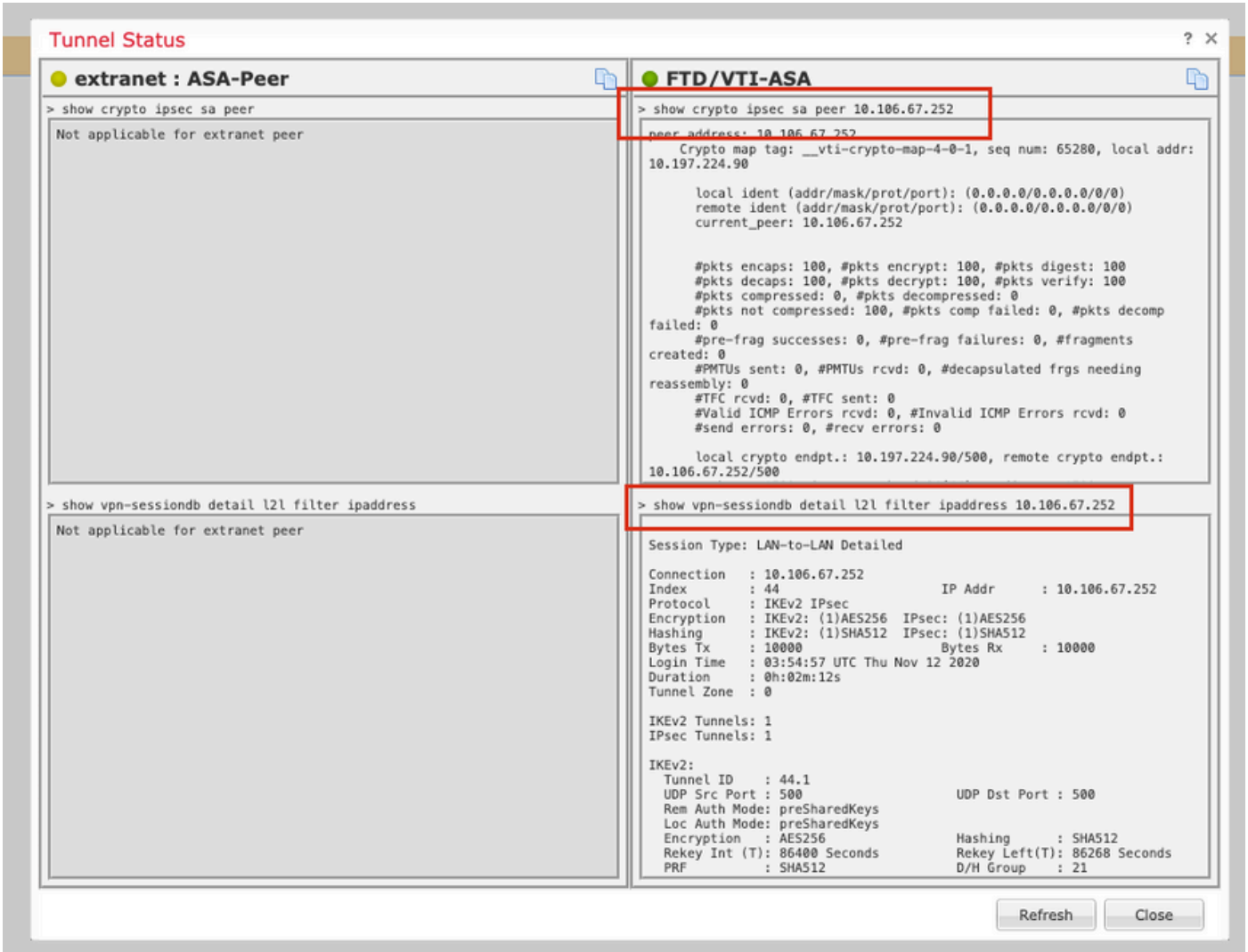
من واجهة المستخدم الرسومية الخاصة بمركز إدارة Firepower (FMC)

انقر فوق خيار التحقق من الحالة لمراقبة حالة النفق الخاصة بـ VPN من واجهة المستخدم الرسومية (GUI) نفسها



وهذا يتضمن هذه الأوامر المأخوذة من واجهة سطر الأوامر (CLI) الخاصة ب FTD:

- عرض نظير IPsec للتشفير <عنوان IP للنظير>
- show vpn-sessiondb detail l2l مرشح ipAddress <peer ip address>



من واجهة سطر أوامر FTD

يمكن إستخدام هذه الأوامر من واجهة سطر الأوامر (CLI) الخاصة ب FTD لعرض تكوين أنفاق شبكة VPN وحالتها.

```
show running-config crypto
show running-config nat
```

```
show running-config route
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail l2l
```

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).