تكوين شبكة VPN المستندة إلى المسار باستخدام المسار الثابت على FTD المدار بواسطة FDM

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين موقع ثابت مستند إلى مسار إلى نفق VPN للموقع على FTD تتم إدارته بواسطة FDM.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- فهم أساسي لكيفية عمل نفق الشبكة الخاصة الظاهرية (VPN).
- معرفة مسبقة بالتنقل عبر مدير أجهزة FirePOWER (FDM).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

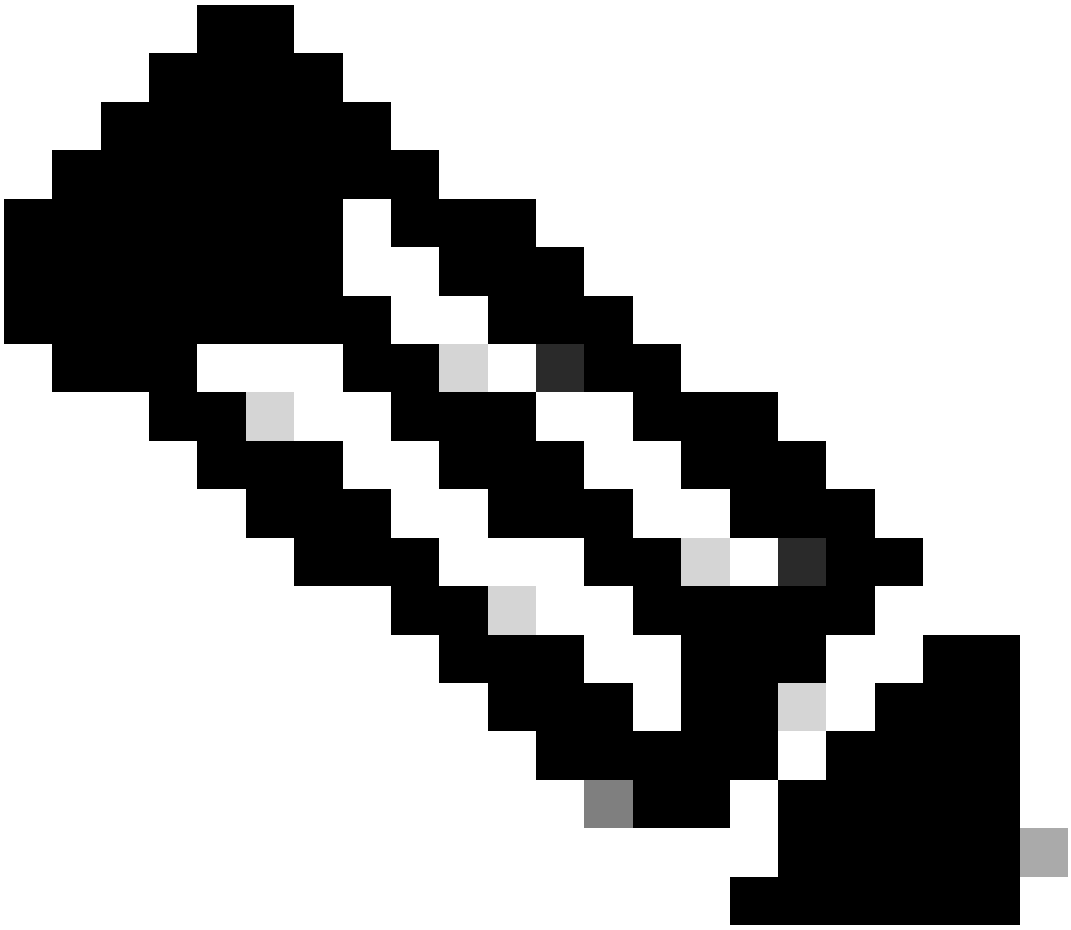
- برنامج الدفاع ضد تهديد FirePOWER (FTD) من Cisco الإصدار 7.0 المدار من قبل FirePOWER Device Manager (FDM).

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. تم 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 المثيرة للاهتمام وأ إرسالها عبر نفق VPN، واستخدام توجيه حركة المرور بدلا من قائمة الوصول/النهج كما هو الحال في شبكة VPN المستندة إلى السياسة وأ التشفير. تم تعيين محددات حركة مرور IPsec لتشفير للسماح بأي حركة مرور تدخل نفق IPsec. وهذا يعني أن أي حركة مرور يتم توجيهها إلى البعيدة على 0.0.0.0/0.0.0.0. المحلية IPsec مرور نفق IPsec يتم تشفيرها بغض النظر عن الشبكة الفرعية للمصدر/الوجهة.

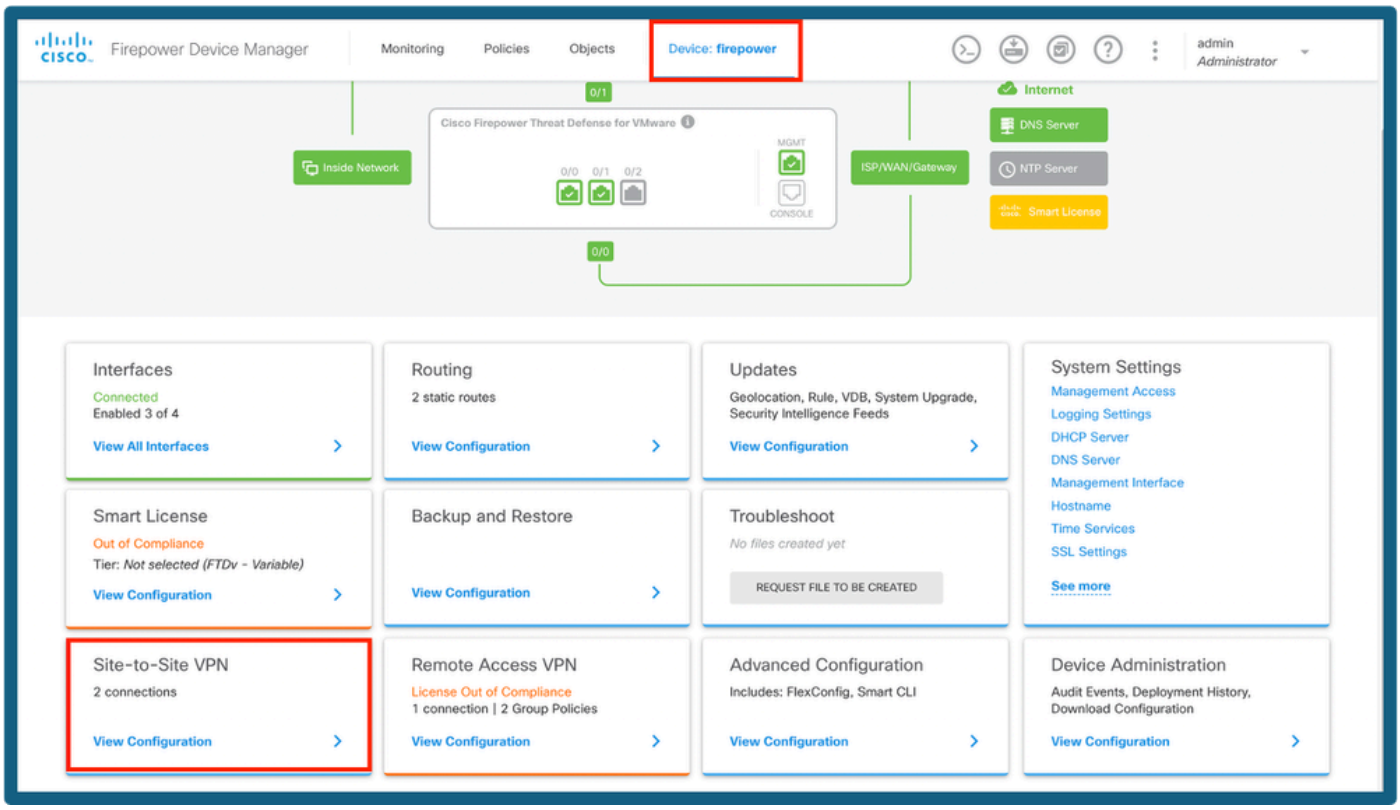
يركز هذا المستند على تكوين واجهة النفق الظاهرية الثابتة (SVTI).



ملاحظة: لا توجد حاجة إلى ترخيص إضافي، ويمكن تكوين شبكة VPN المستندة إلى المسار في أوضاع الترخيص وكذلك التقييم. بدون التوافق مع التشفير (تمكين ميزات التي يتم التحكم بها للتصدير)، يمكن إستخدام DES فقط خوارزمية تشفير.

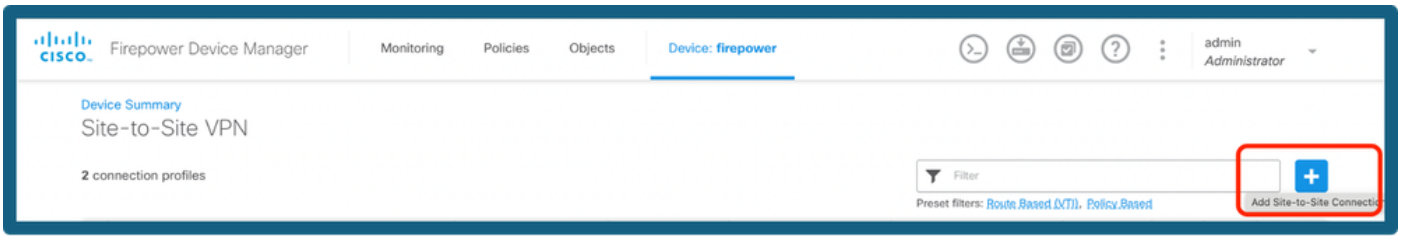
خطوات التكوين على FDM

الخطوة 1. انتقل إلى جهاز > موقع إلى موقع.



لوحة معلومات FDM

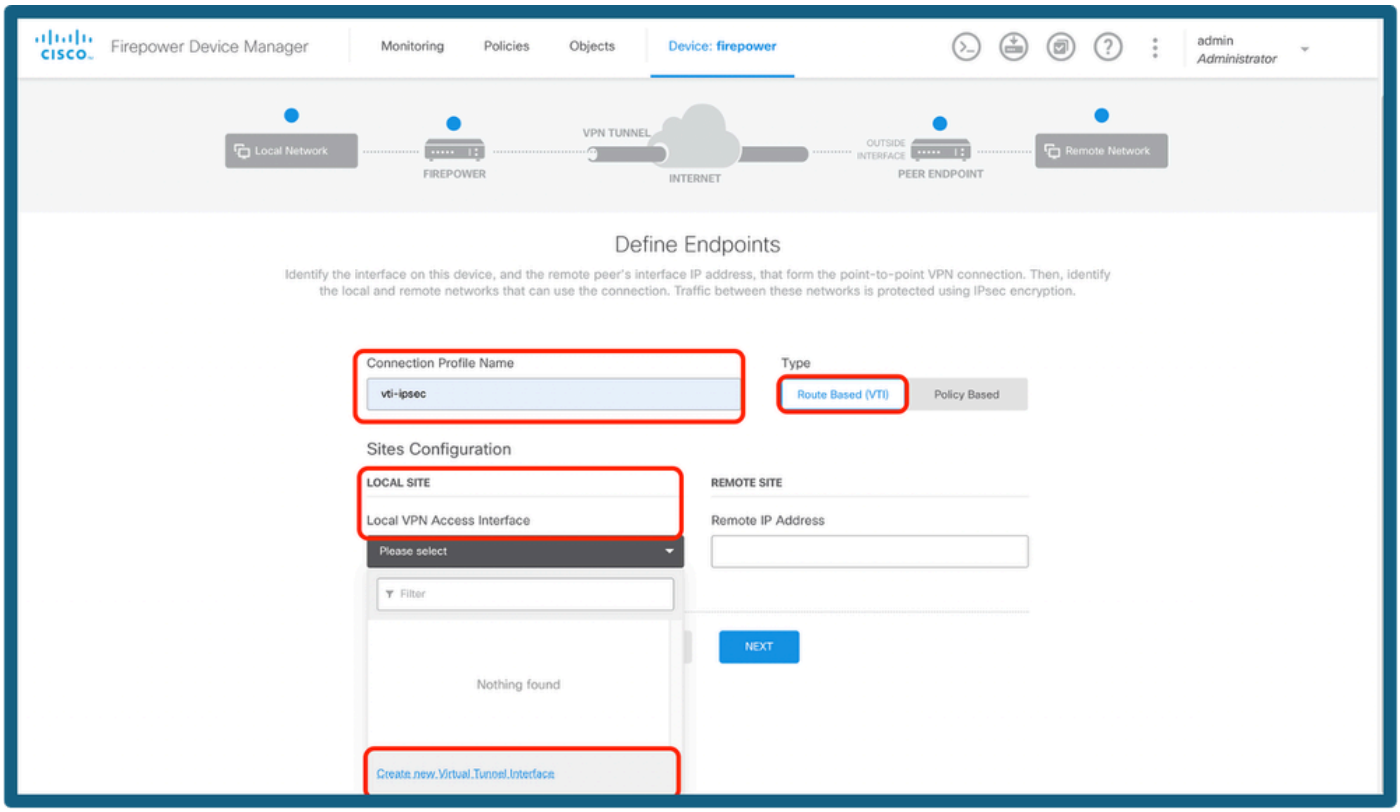
الخطوة 2. انقر فوق رمز + لإضافة موقع جديد إلى اتصال الموقع.



إضافة اتصال S2S

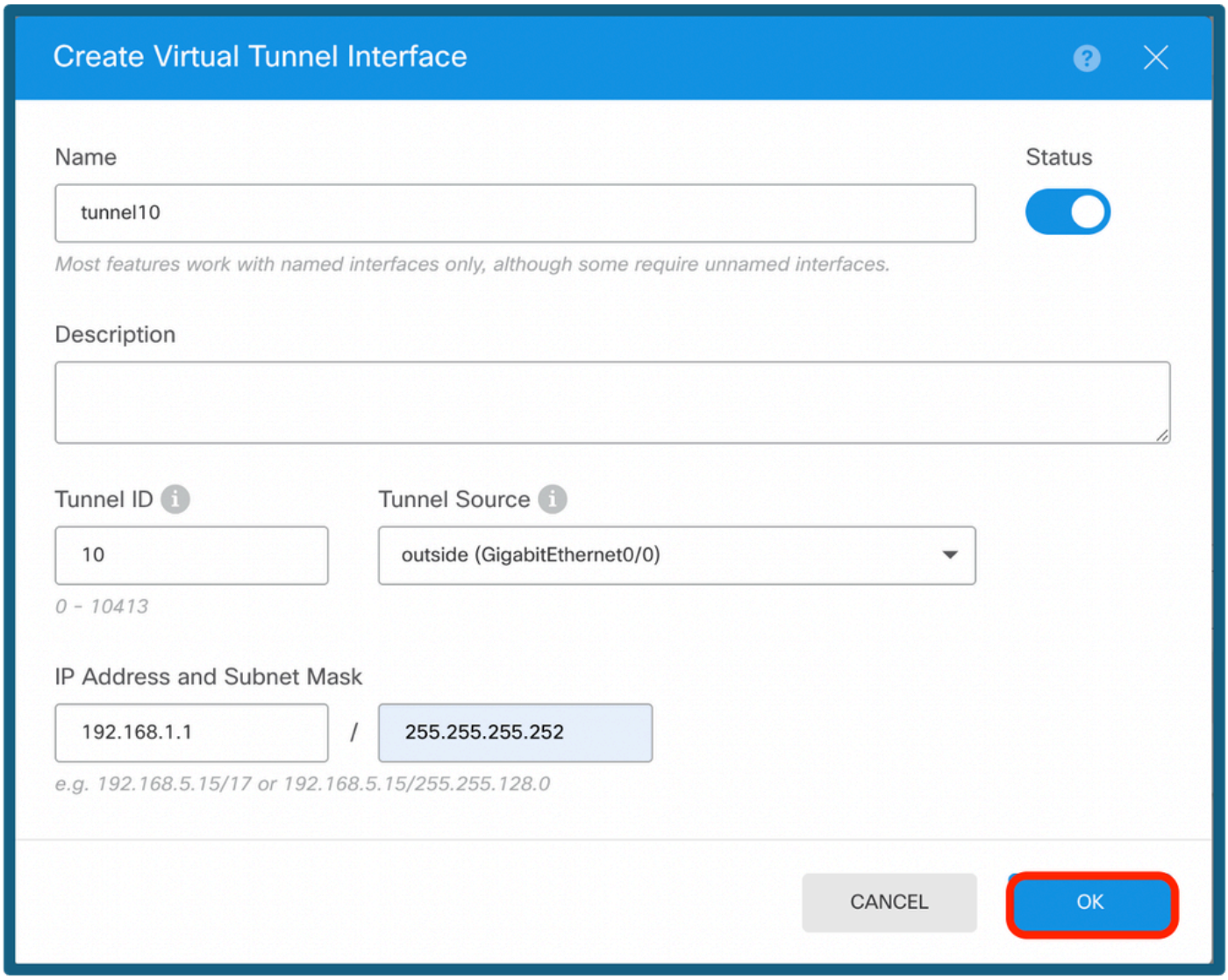
الخطوة 3. أدخل اسم مخطط وحدد نوع VPN على أنه مستند إلى المسار (VTI).

انقر فوق واجهة الوصول إلى VPN المحلية، ثم انقر فوق إنشاء واجهة نفق ظاهري جديدة أو حدد واجهة من القائمة الموجودة.



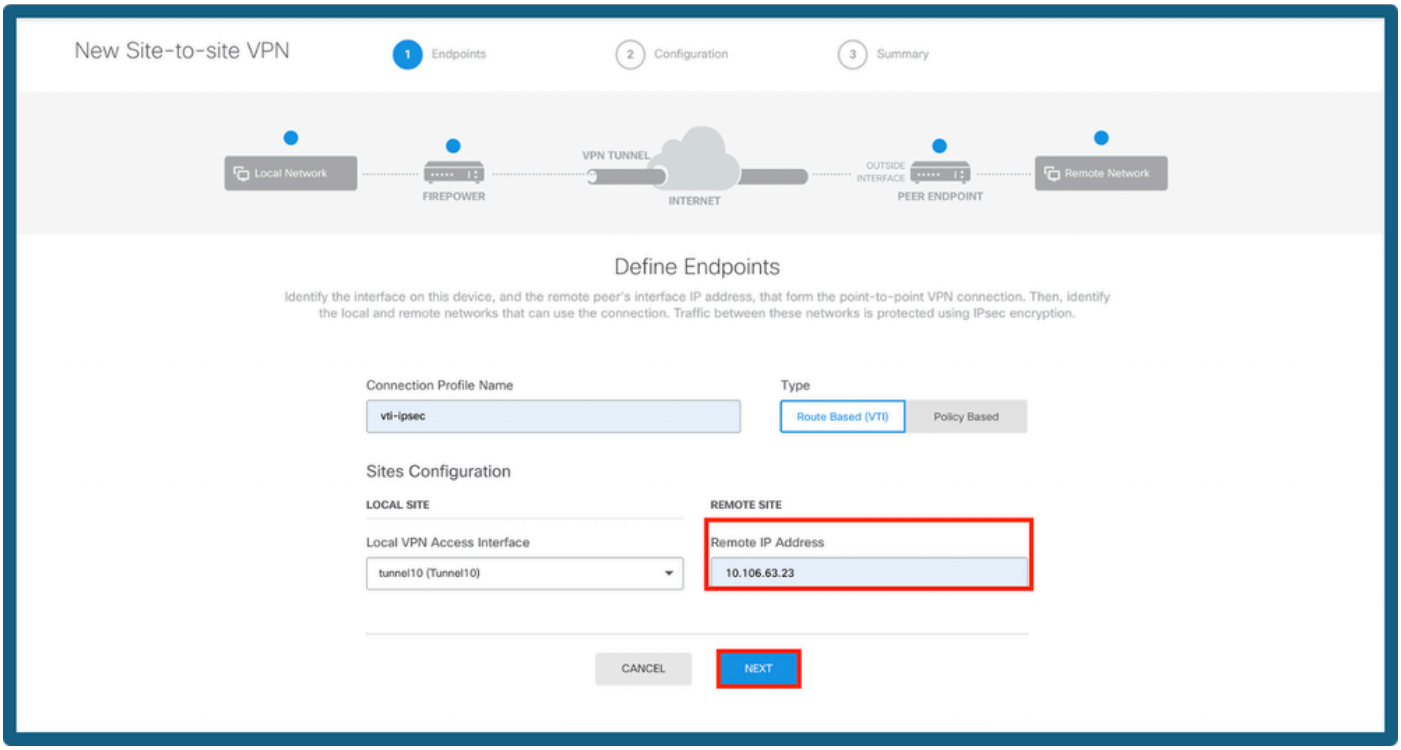
إضافة واجهة نفق

الخطوة 4. حدد معلمات واجهة النفق الظاهري الجديدة. وانقر فوق OK.



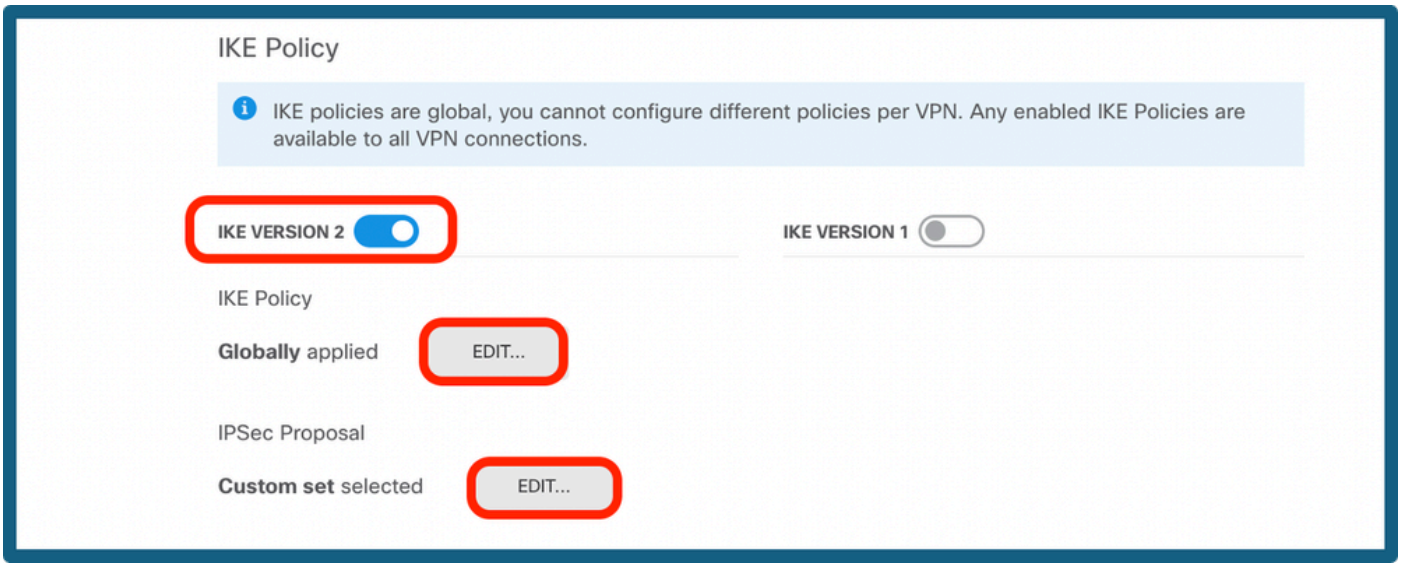
تكوين VTI

أخترت خطوة 5. ال VTI newly created أو VTI أن يتواجد تحت الفعلي نفق قارن.يزود العنوان بعيد.



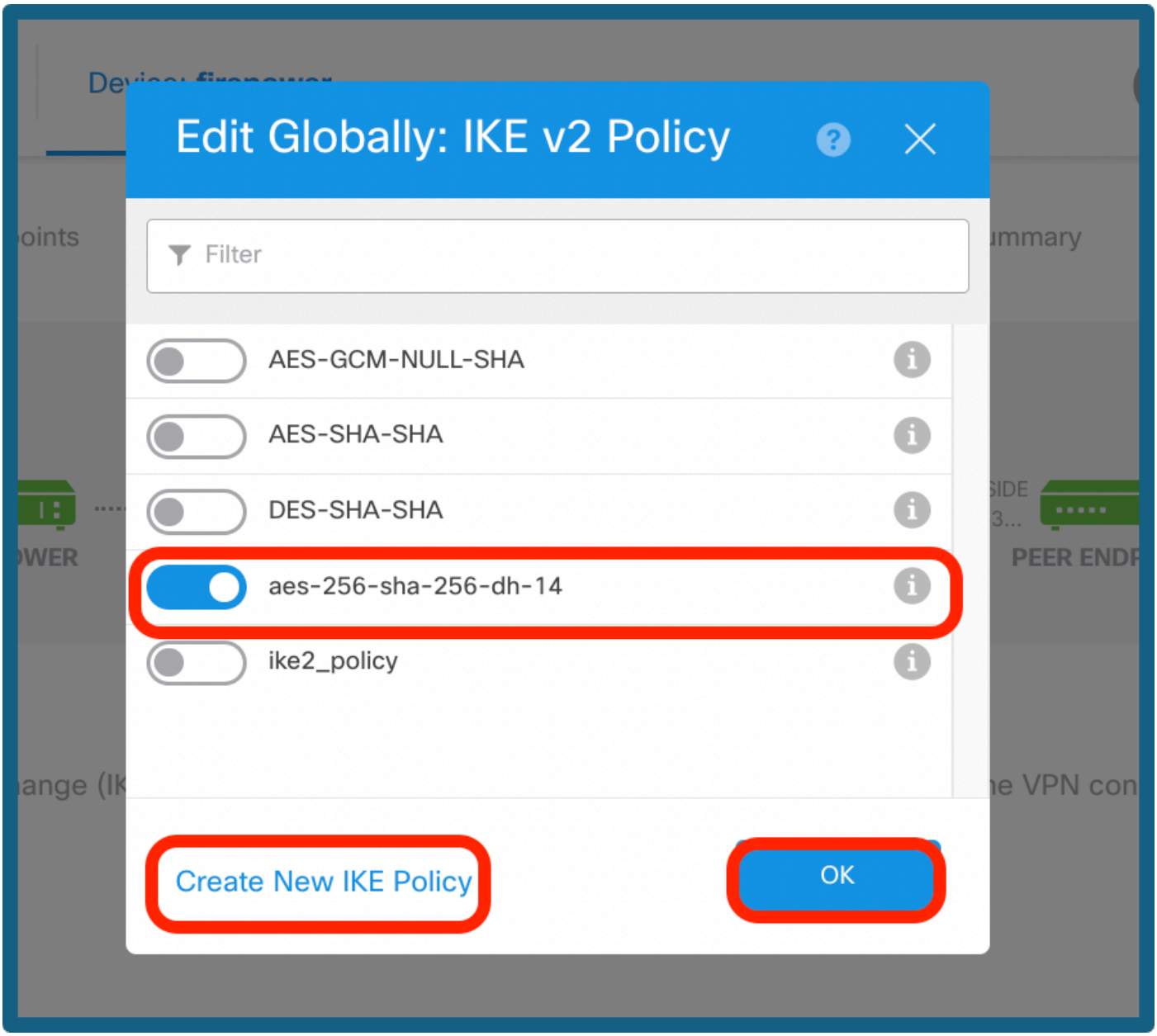
إضافة IP النظير

الخطوة 6. أختر إصدار IKE واختر الزر تحرير لتعيين معلمات IKE و IPsec كما هو موضح في الصورة.

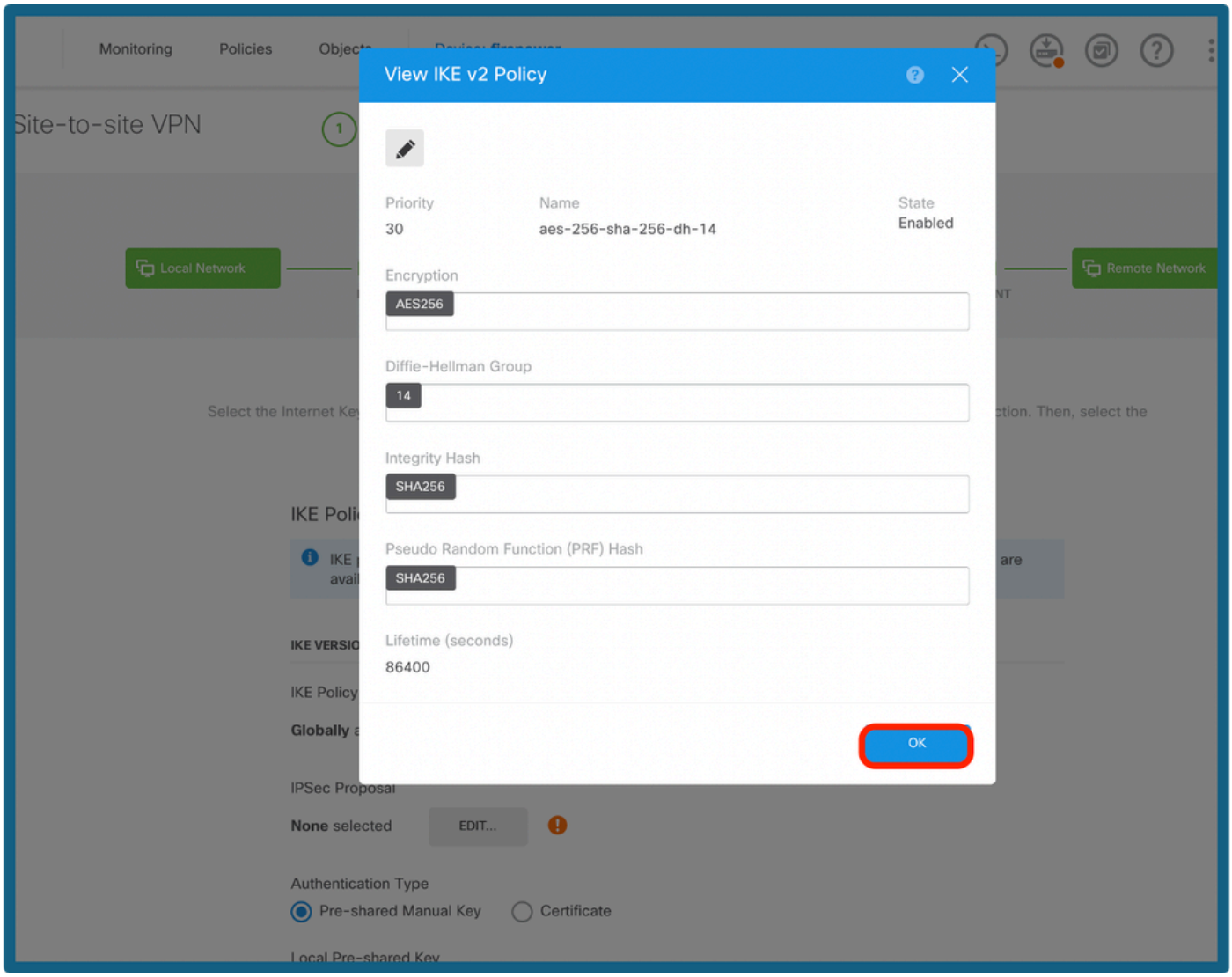


تكوين إصدار IKE

الخطوة 7 أ. أختر زر نهج IKE كما هو موضح في الصورة وانقر على زر موافق أو إنشاء نهج IKE جديد، إذا كنت ترغب في إنشاء نهج جديد.

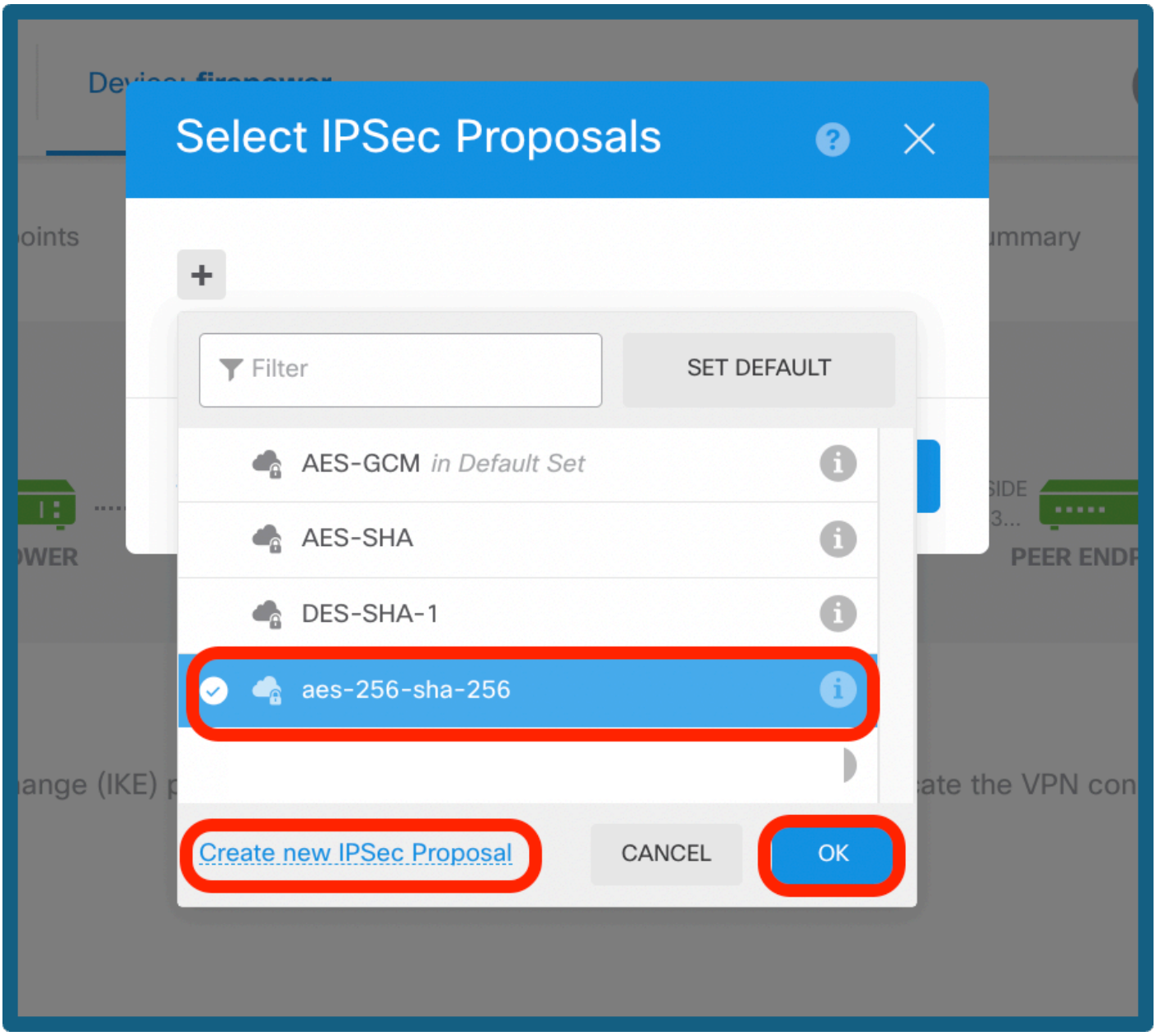


اختيار نهج IKE

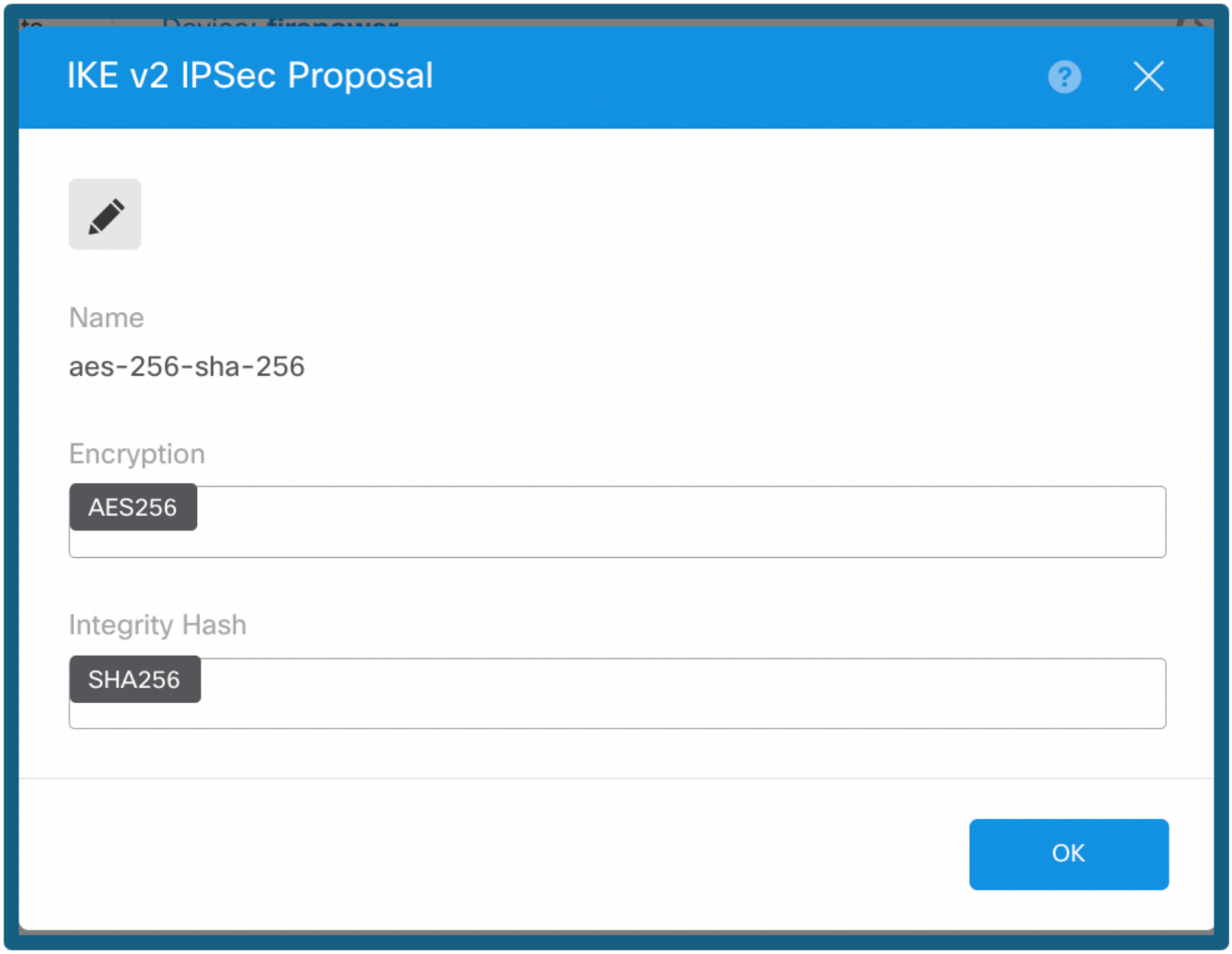


تكوين سياسة IKE

الخطوة 7 ب. أختر الزر نهج IPSec كما هو موضح في الصورة وانقر فوق الزر موافق أو إنشاء مقترح IPsec جديد، إذا كنت ترغب في إنشاء مقترح جديد.



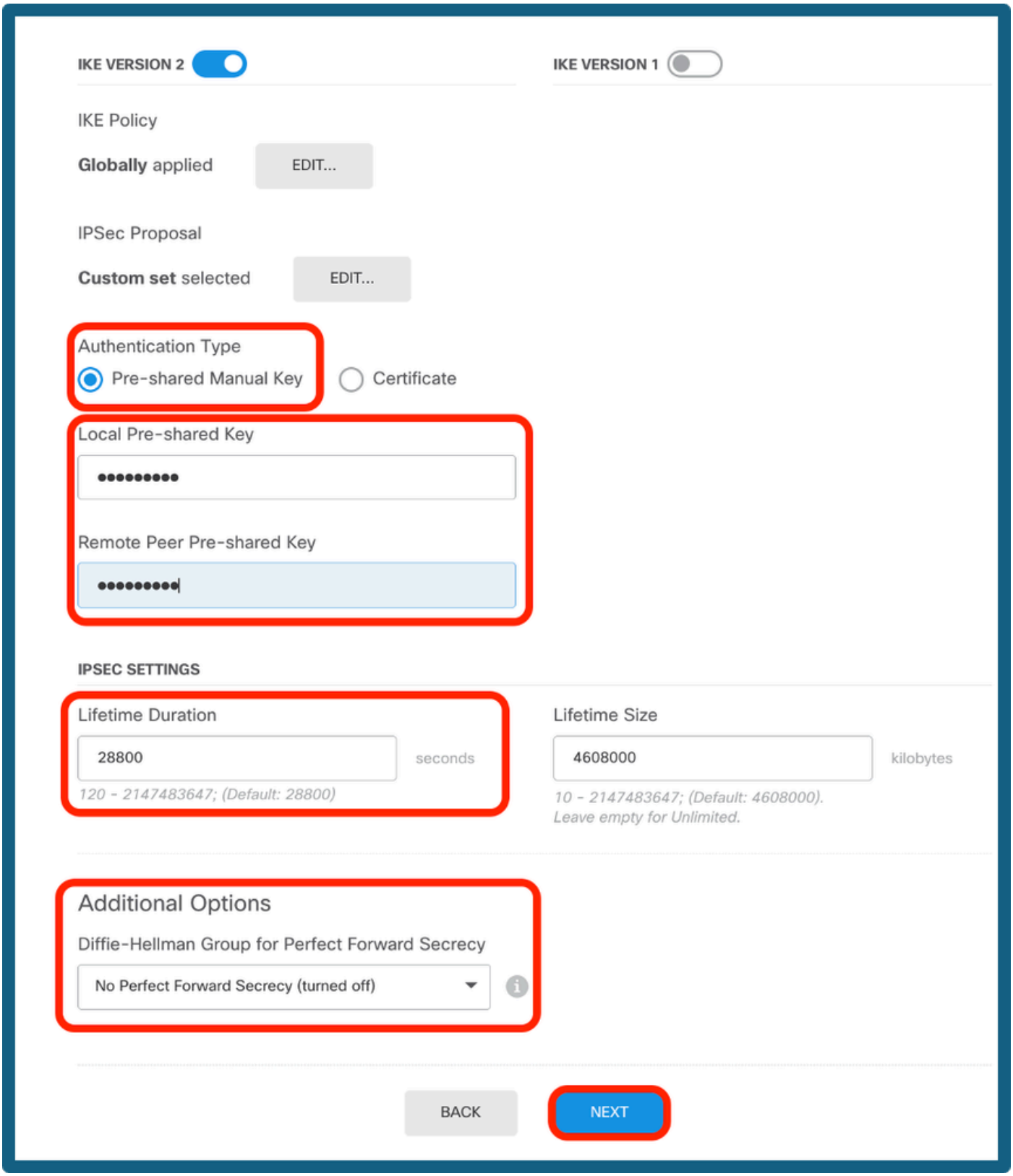
تحديد مقترح IPsec



تكوين مقترح IPsec

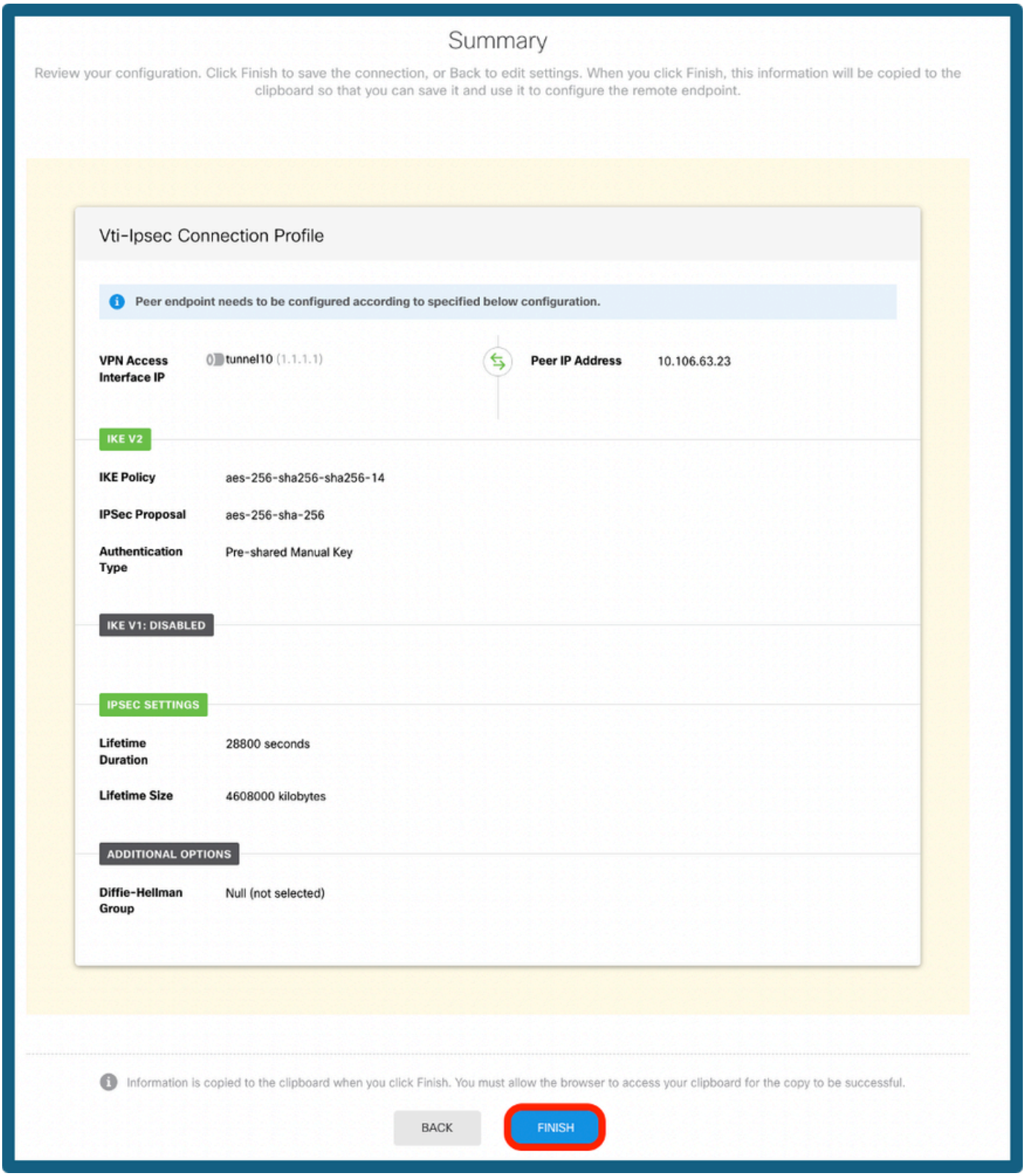
الخطوة 8 أ. حدد نوع المصادقة. إذا تم إستخدام المفتاح اليدوي المشترك مسبقا، فقم بتوفير المفتاح المحلي والمفتاح الذي تمت مشاركته مسبقا عن بعد.

الخطوة 8 ب. (إختياري) أختر إعدادات سرية إعادة التوجيه المثالية. قم بتكوين مدة العمر الافتراضي لبروتوكول IPsec وحجم العمر الافتراضي، ثم انقر فوق التالي.



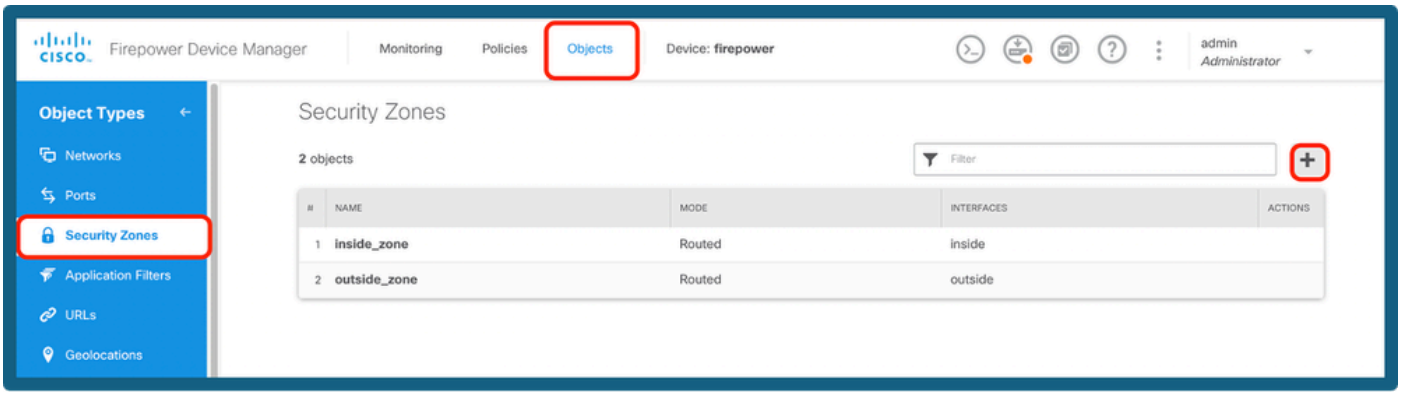
تكوين PSK و Life

الخطوة 9. راجع التكوين وانقر فوق إنهاء.



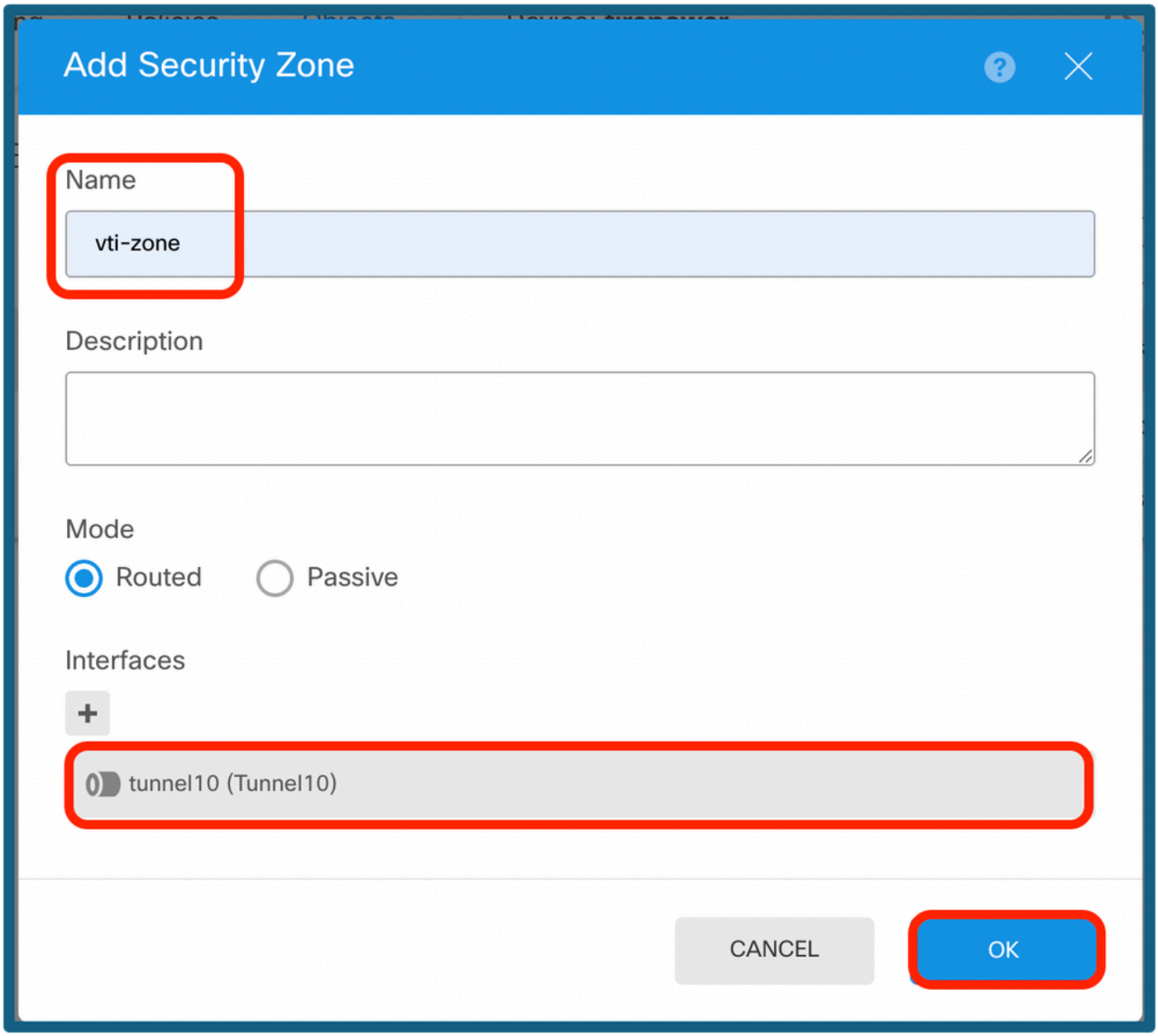
ملخص التكوين

الخطوة 10a. انتقل إلى كائنات > مناطق أمان ثم انقر على + أيقونة.



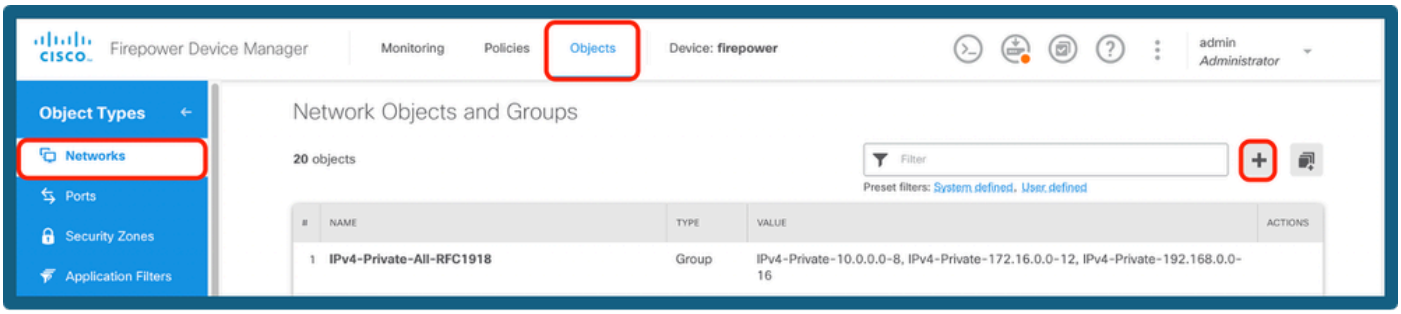
إضافة منطقة أمان

الخطوة 10b. قم بإنشاء منطقة، ثم حدد واجهة VTI كما هو موضح أدناه.



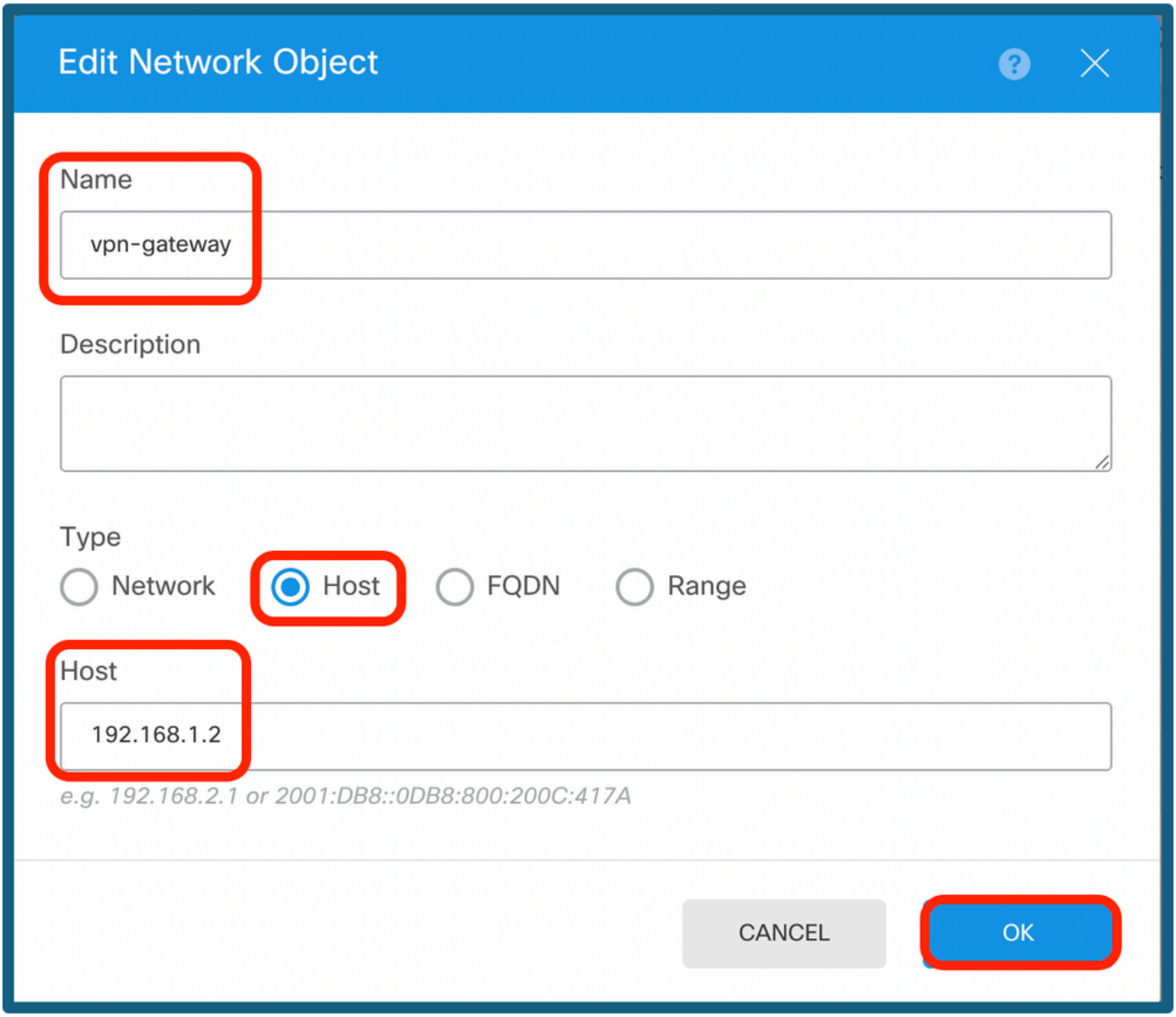
تكوين المنطقة الأمنية

الخطوة 11a. انتقل إلى كائنات > شبكات، انقر على + أيقونة.



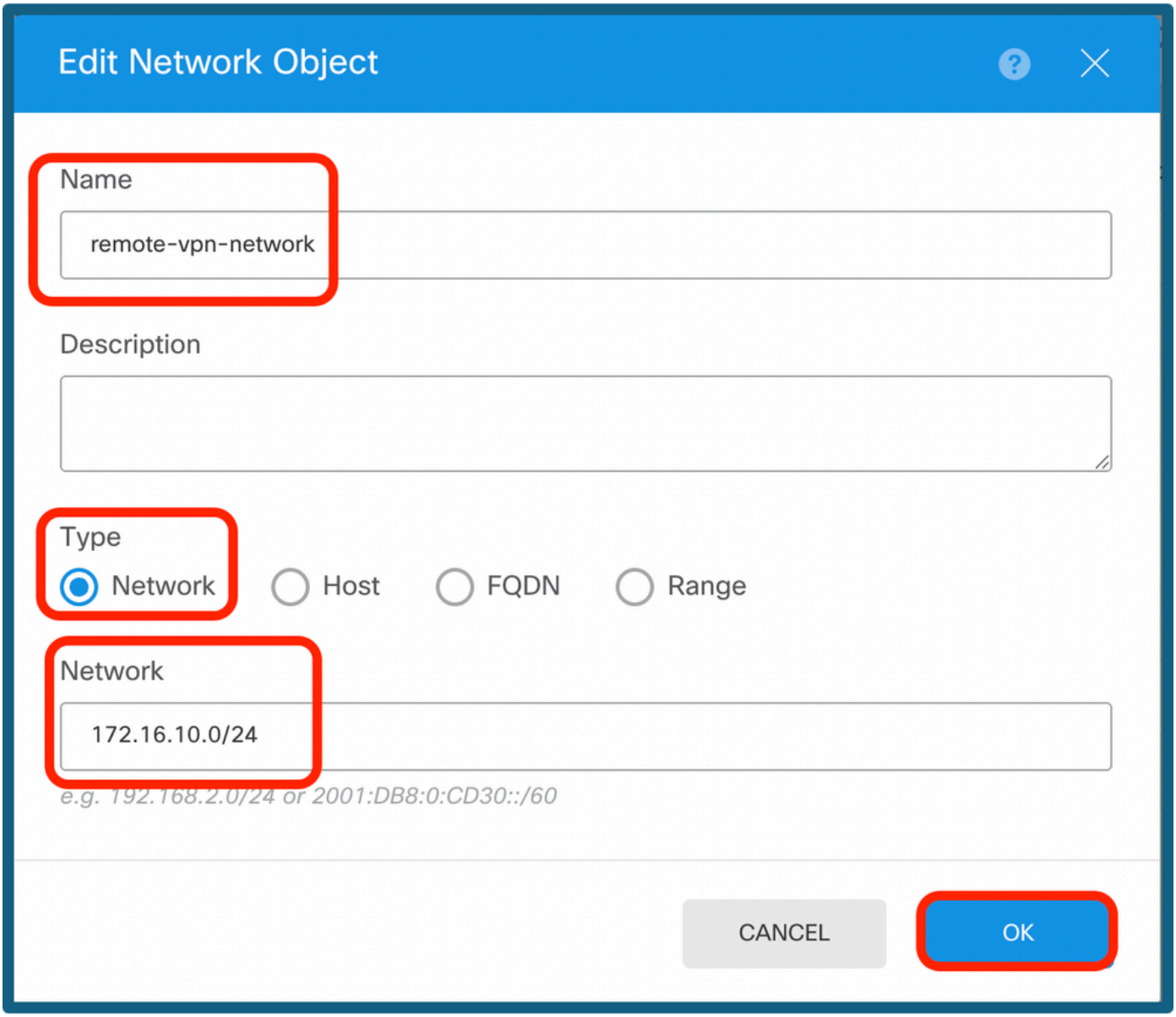
إضافة كائنات شبكة

الخطوة 11b. إضافة كائن مضيف، وإنشاء بوابة باستخدام عنوان IP للنفق الخاص بنقطة نهاية النظير.

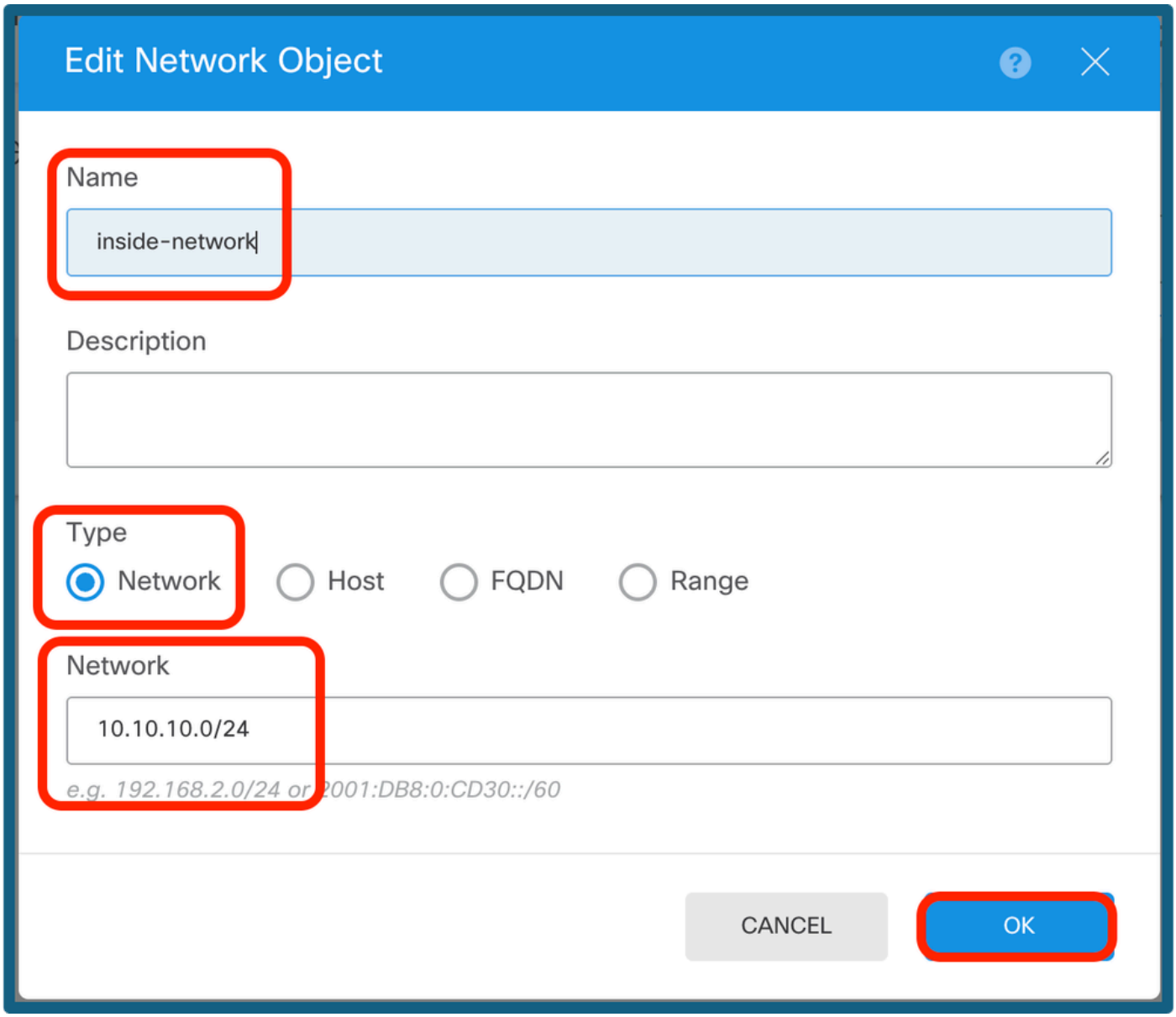


تكوين بوابة VPN

الخطوة 11c. إضافة الشبكة الفرعية البعيدة والشبكة الفرعية المحلية.

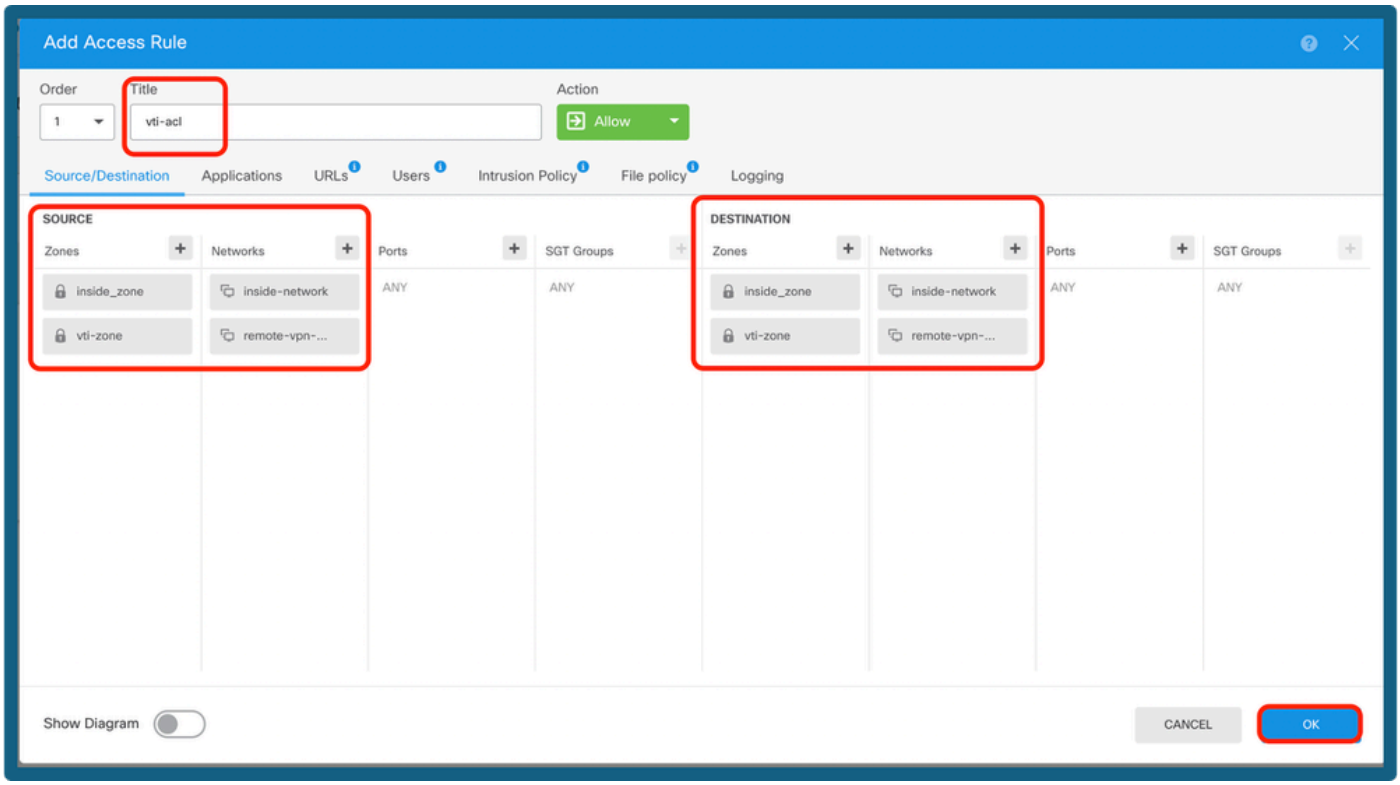


تكوين IP البعيد



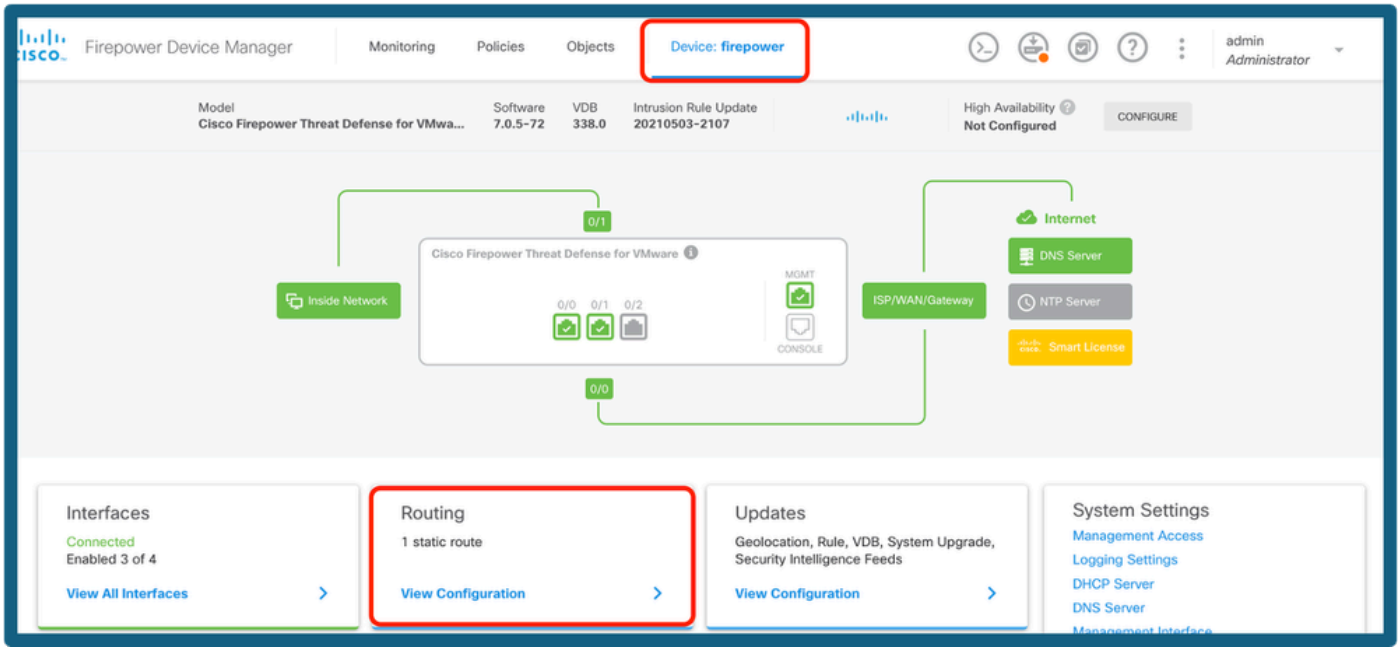
تكوين IP المحلي

الخطوة 12. انتقل إلى الجهاز > السياسات، وقم بتكوين نهج التحكم في الوصول.



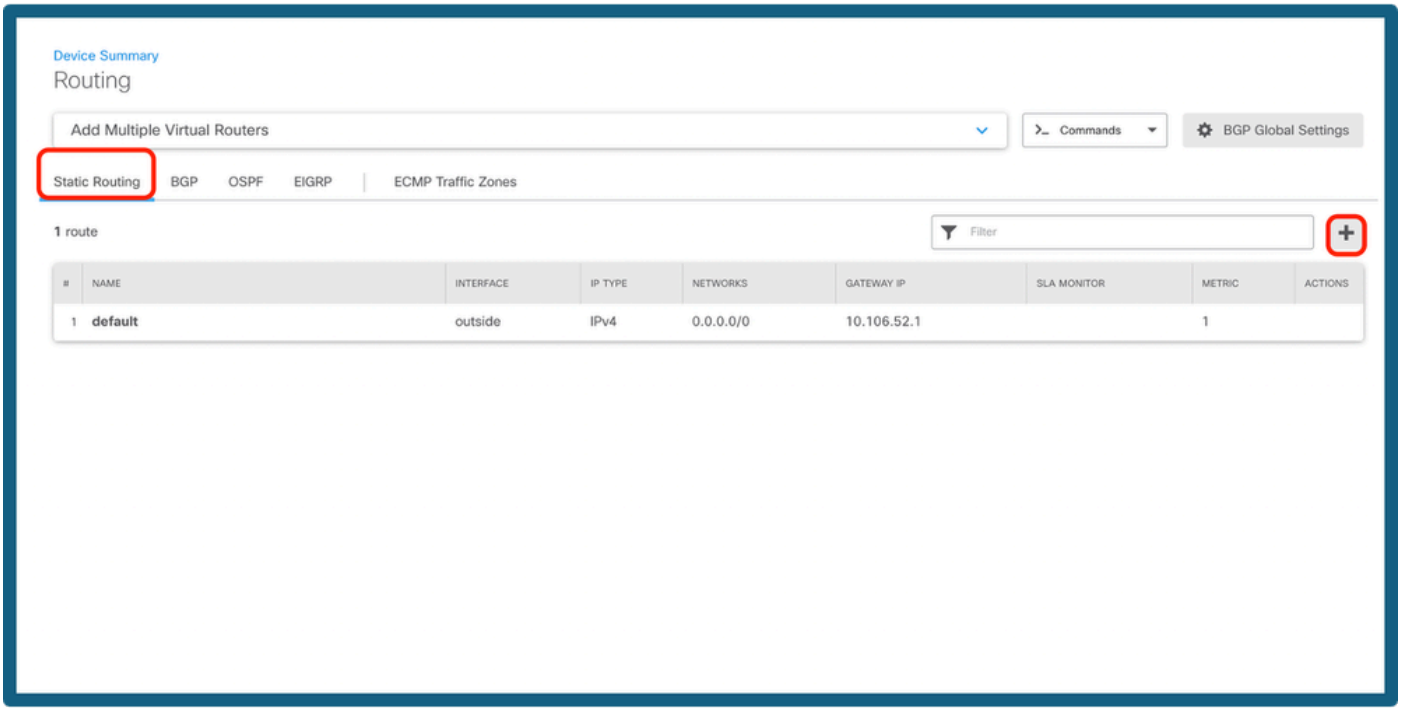
اضافة نهج التحكم بالوصول

الخطوة 13a. قم بإضافة التوجيه عبر نفق VTI. انتقل إلى الجهاز > التوجيه.



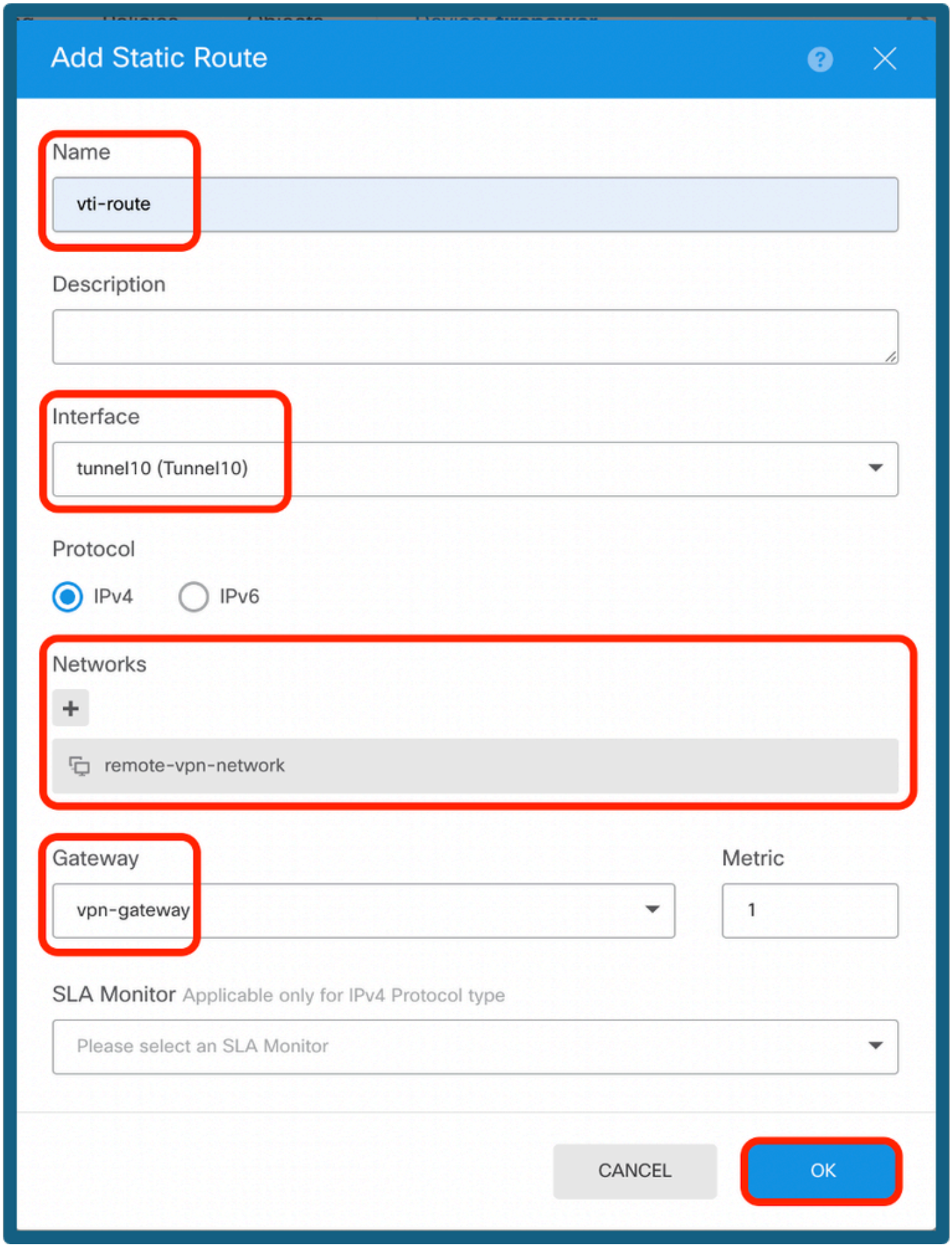
تحديد توجيه

الخطوة 13 ب. انتقل إلى المسار الثابت ضمن علامة التبويب التوجيه. انقر فوق + الأيقونة.



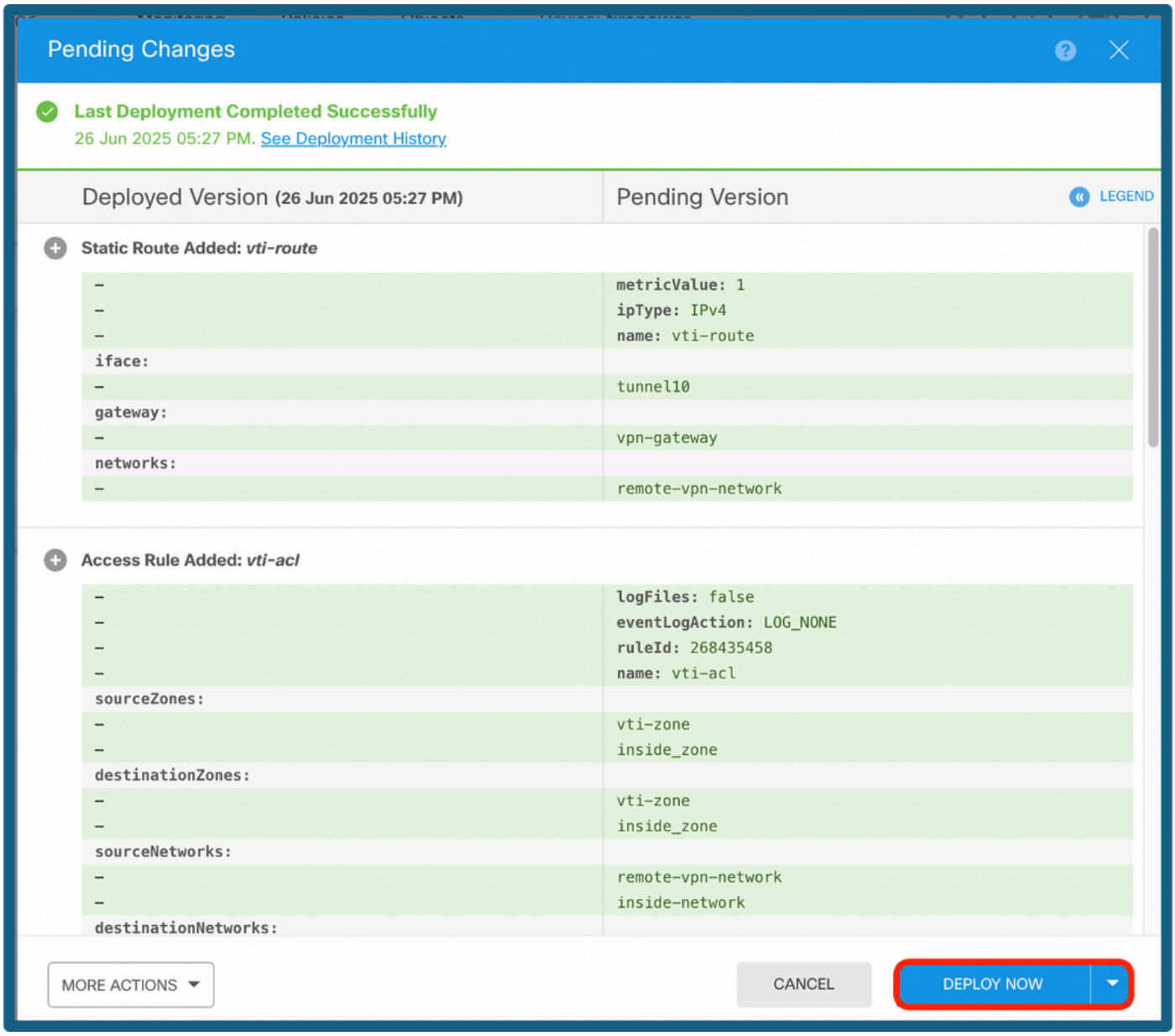
اضافة مسار

الخطوة 13c. قم بتوفير الواجهة، واختر الشبكة، وتقديم البوابة. وانقر فوق OK.



تكوين المسار الثابت

الخطوة 14. انتقل إلى النشر. راجع التغييرات ثم انقر فوق النشر الآن.

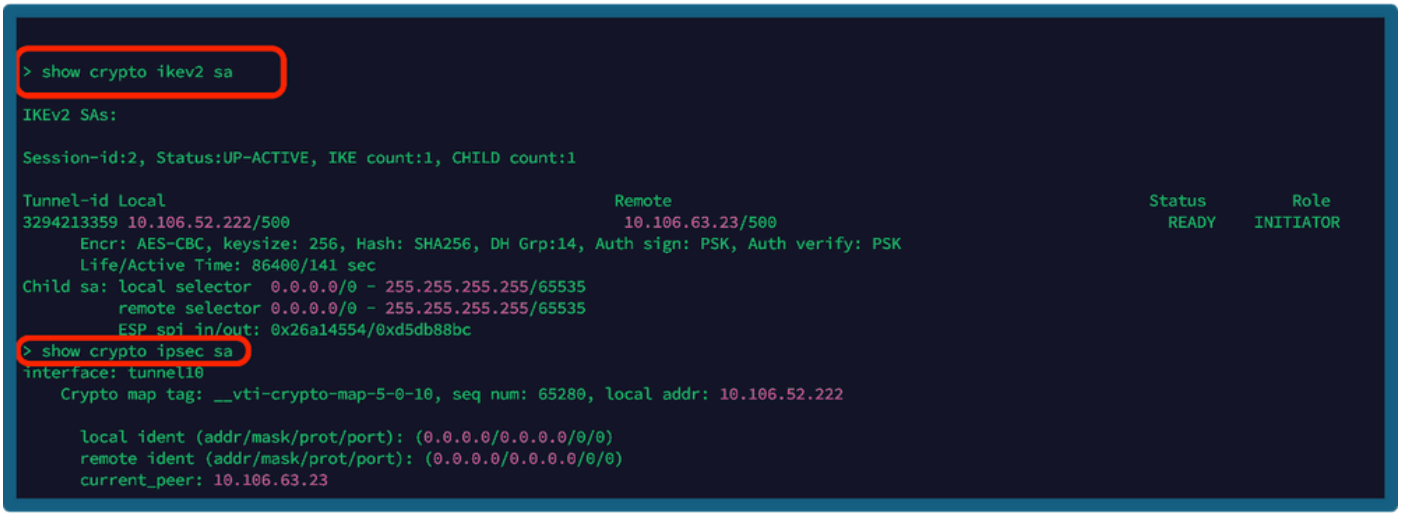


نشر التكوين

التحقق من الصحة

بمجرد اكتمال النشر، يمكنك التحقق من حالة النفق على CLI باستخدام الأوامر:

1. show crypto ikev2 sa
2. show crypto ipSec sa <peer-ip>



إظهار الأوامر

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:

[دليل تكوين FTD المدار من قبل 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).