تكوين شبكة VPN النشطة المزدوجة مع موقع إلى موقع من المسار إلى المستندة FDM بواسطة المدارة FTD على PBR

المحتويات

- المقدمة
- المتطلبات الأساسية
  - المتطلبات
  - المكونات المستخدمة
- معلومات أساسية
- التكوين
  - الرسم التخطيطي للشبكة
  - التكوينات على شبكة VPN
    - تكوين Site1 FTD VPN
    - تكوين Site2 FTD VPN
  - التكوينات على PBR
    - تكوين PBR الخاص بـ Site1 FTD
    - تكوين PBR الخاص بـ Site2 FTD
  - عمليات التحقق على شاشة SLA
    - تكوين مراقبة SLA لـ SITE1 FTD
    - تكوين مراقبة SLA لـ SITE2 FTD
  - التكوينات على المسار الثابت
    - تكوين المسار الثابت لـ SITE1 FTD
    - تكوين المسار الثابت لـ SITE2 FTD
- التحقق من الصحة
  - دعم لكشف الفشل بين ISP1 و ISP2
    - VPN
    - قيد
    - شاشة SLA
    - تتبع الاختبار
  - دعم لعمل نسخ احتياطي من ISP2 على ISP1 في حالة انقطاع الاتصال
    - VPN
    - قيد
    - شاشة SLA
    - تتبع الاختبار
  - دعم لعمل نسخ احتياطي من ISP1 على ISP2 في حالة انقطاع الاتصال
    - VPN
    - قيد
    - شاشة SLA
    - تتبع الاختبار
- استكشاف الأخطاء وإصلاحها

المقدمة

يوضح هذا المستند كيفية تكوين شبكة VPN النشطة المزدوجة المستندة إلى المسار من موقع إلى موقع باستخدام PBR على FTD التي تتم إدارتها بواسطة FDM.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الفهم الأساسي للشبكة الخاصة الظاهرية (VPN)
- الفهم الأساسي للتوجيه القائم على السياسة (PBR)
- الفهم الأساسي لاتفاقية مستوى خدمة بروتوكول الإنترنت (IP SLA)
- تجربة إدارة fdm

المكونات المستخدمة

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

- Cisco FTDv، الإصدار 7.4.2
- Cisco FDM، الإصدار 7.4.2

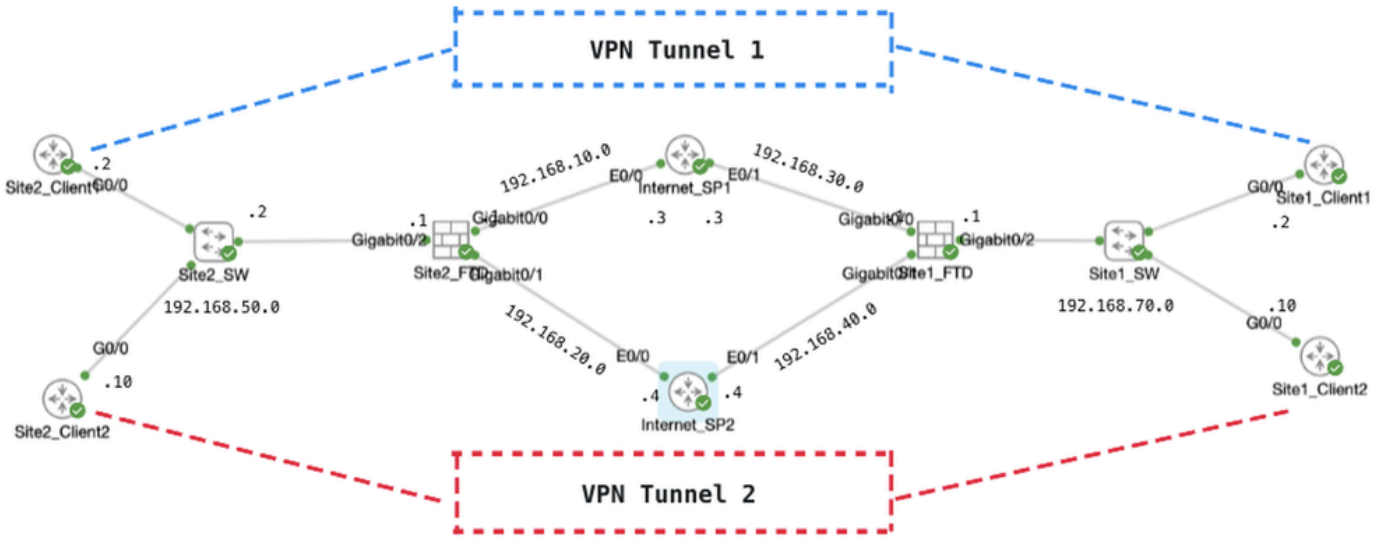
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يشرح هذا المستند كيفية تكوين شبكة VPN نشطة مزدوجة مستندة إلى مسار من موقع إلى موقع على FTD. في هذا المثال، تتضمن FTDs في كل من الموقع 1 والموقع 2 إتصالات ISP مزدوجة لإنشاء شبكة خاصة ظاهرية (VPN) من موقع إلى موقع مع كل من موزعي خدمة الإنترنت (ISPs) في آن واحد. بشكل افتراضي، تعبر حركة مرور VPN النفق 1 عبر ISP1 (الخط الأزرق). بالنسبة للمضيفين المحددين، تمر حركة المرور عبر النفق 2 عبر ISP2 (الخط الأحمر). إذا عانى ISP1 من مقاطعة، فسيقوم بتبديل حركة مرور البيانات إلى ISP2 كنسخ إحتياطي. وعلى العكس من ذلك، إذا واجه ISP2 مقاطعة، فعليك نقل البيانات إلى ISP1 كعملية نسخ إحتياطي. يتم إستخدام التوجيه المستند إلى السياسة (PBR) واتفاقية مستوى خدمة بروتوكول الإنترنت (IP SLA) في هذا المثال للوفاء بهذه المتطلبات.

التكوين

الرسم التخطيطي للشبكة



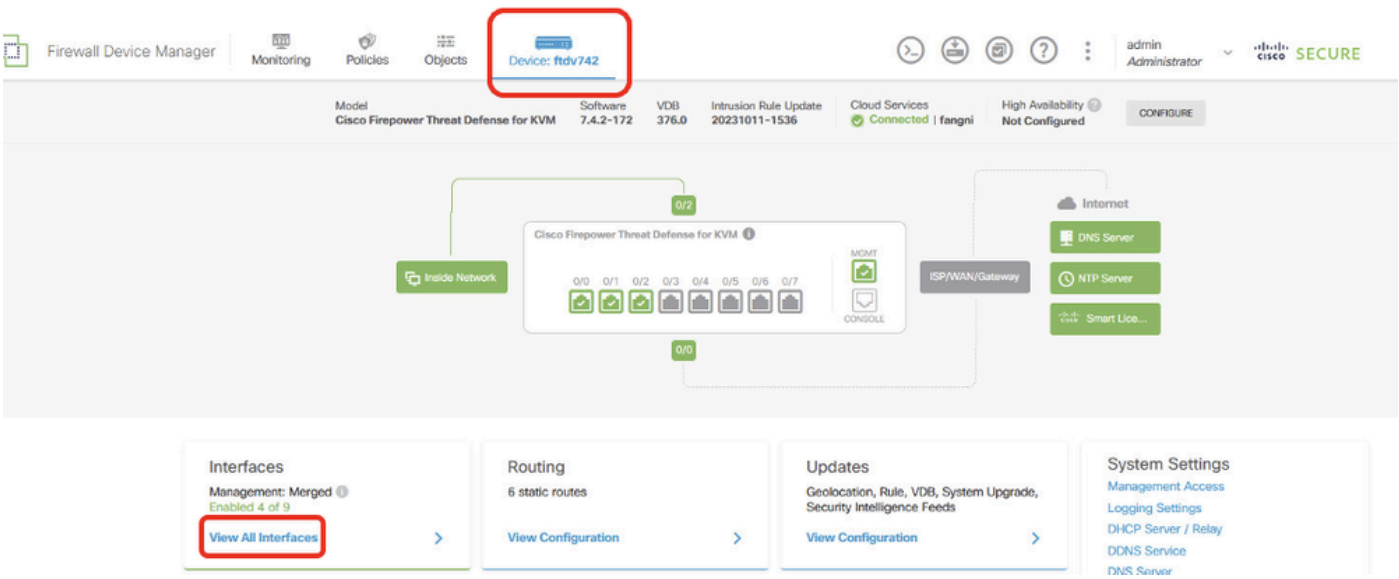
الطوبولوجيا

التكوينات على شبكة VPN

من الضروري التأكد من اكتمال التكوين الأولي لاتصال IP البيني بين العقد بشكل صحيح. يكون العملاء في كل من Site1 و Site2 مع عنوان IP الموجود في "برنامج الإرسال فائق السرعة (FTD)" كبوابة.

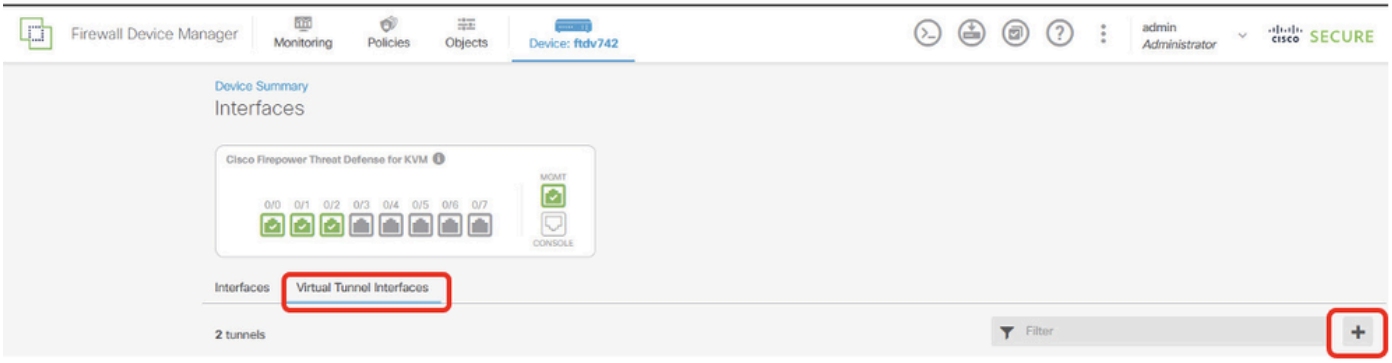
تكوين Site1 FTD VPN

الخطوة 1. قم بإنشاء واجهات النفق الظاهرية لـ ISP1 و ISP2. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) لـ FDM لـ Site1 FTD. انتقل إلى الجهاز > الواجهات. انقر فوق عرض جميع الواجهات.



Site1FTD_VIEW_ALL_Interfaces

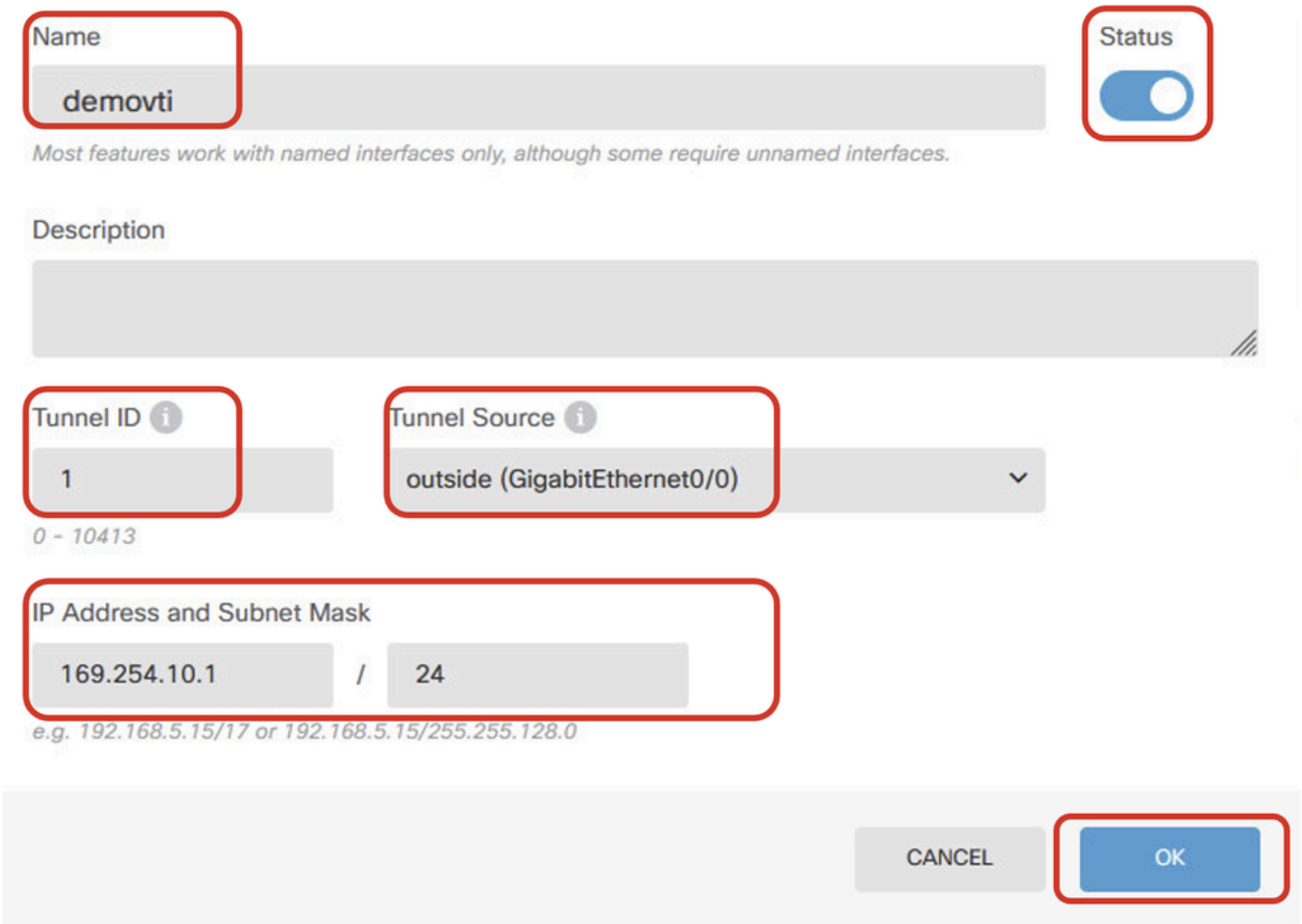
الخطوة 2. انقر فوق علامة التبويب واجهات النفق الظاهري ثم فوق الزر +.



Site1FTD_Create_VTI

الخطوة 3. قم بتوفير المعلومات الضرورية حول تفاصيل VTI. طقطقت ok زر.

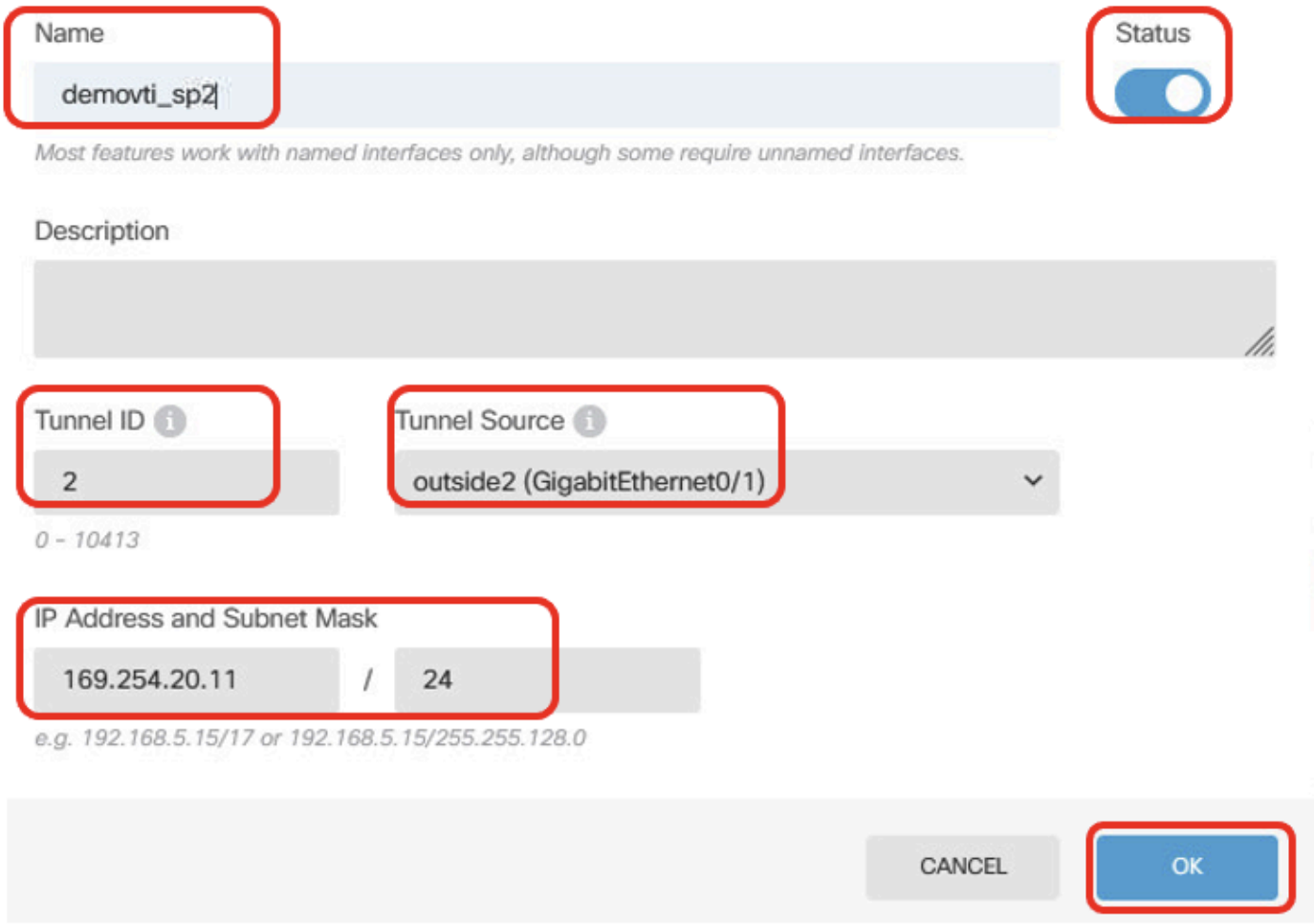
- الاسم: ديموفتي
- معرف النفق: 1
- مصدر النفق: خارج (GigabitEthernet0/0)
- عنوان IP وقناع الشبكة الفرعية: 169.254.10.1/24
- الحالة: انقر المنزلق على الموضع المتاح



site1FTD_VTI_Details_Tunnel1_ISP1

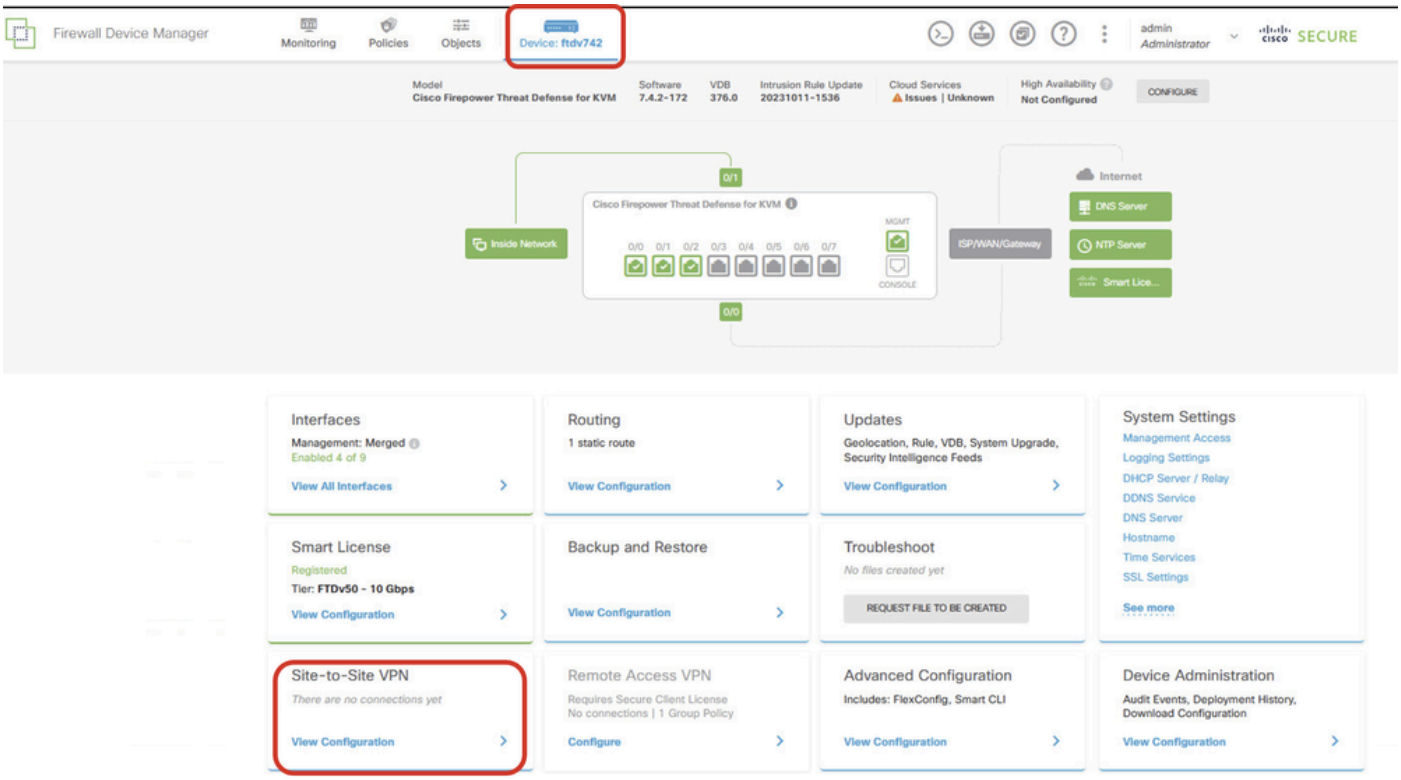
- الاسم: demovti_sp2
- معرف النفق: 2

- مصدر النفق: خارج2 (GigabitEthernet0/1)
- عنوان IP وقناع الشبكة الفرعية: 169.254.20.11/24
- الحالة: انقر المنزلق على الموضع المتاح



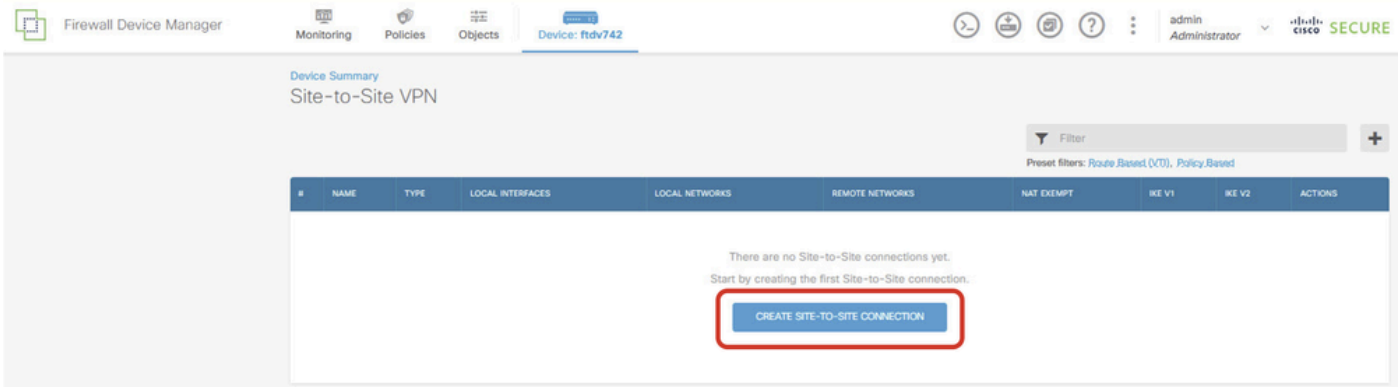
site1FTD_VTI_Details_Tunnel2_ISP2

الخطوة 4. انتقل إلى جهاز > شبكة VPN من موقع إلى موقع. طقطقة عرض تشكيل زر.



Site1FTD_VIEW_SITE2Site_VPN

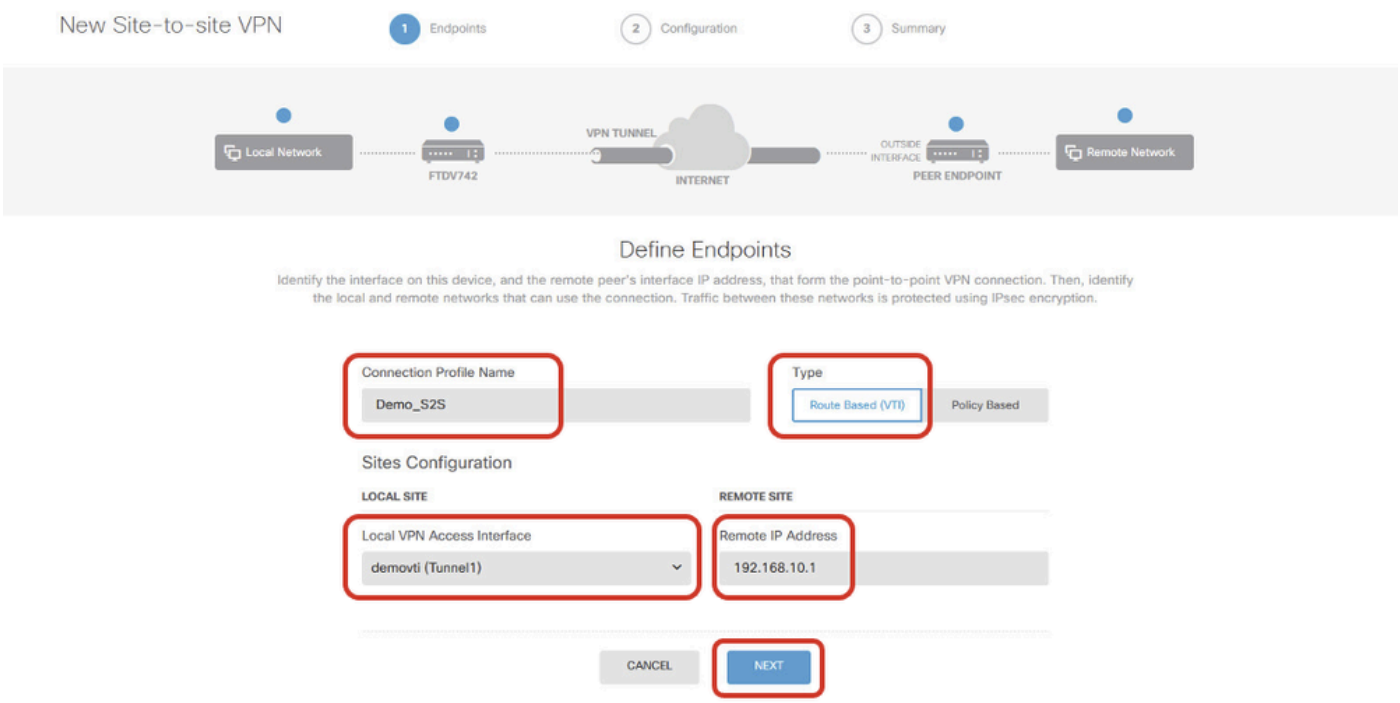
الخطوة 5. ابدأ في إنشاء شبكة VPN جديدة من موقع إلى موقع من خلال ISP1. انقر فوق إنشاء اتصال من موقع إلى موقع، أو انقر فوق الزر +.



Site1FTD_Create_site-to-site_Connection

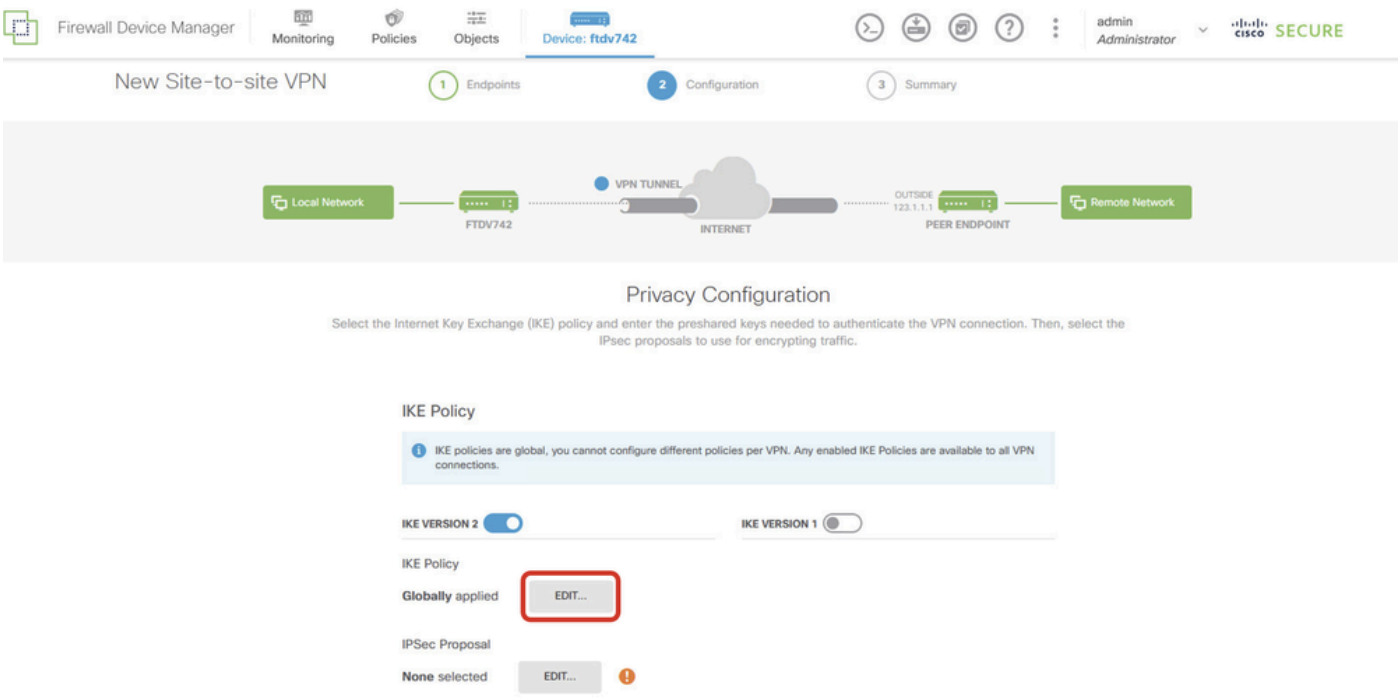
الخطوة 5-1 - توفير المعلومات اللازمة عن نقاط النهاية. طقطقت بعد ذلك زر.

- اسم ملف تعريف الاتصال: العرض التوضيحي_S2S
- النوع: مستند إلى المسار (VTI)
- واجهة الوصول إلى شبكة VPN المحلية: demovti (تم إنشاؤها في الخطوة 3.)
- عنوان IP البعيد: 192.168.10.1 (هذا هو عنوان IP ل Site2 FTD ISP1)



site1FTD_ISP1_site-to-site_VPN_Define_Endpoints

الخطوة 5.2. انتقل إلى سياسة IKE. طقطقة يحرر زر.

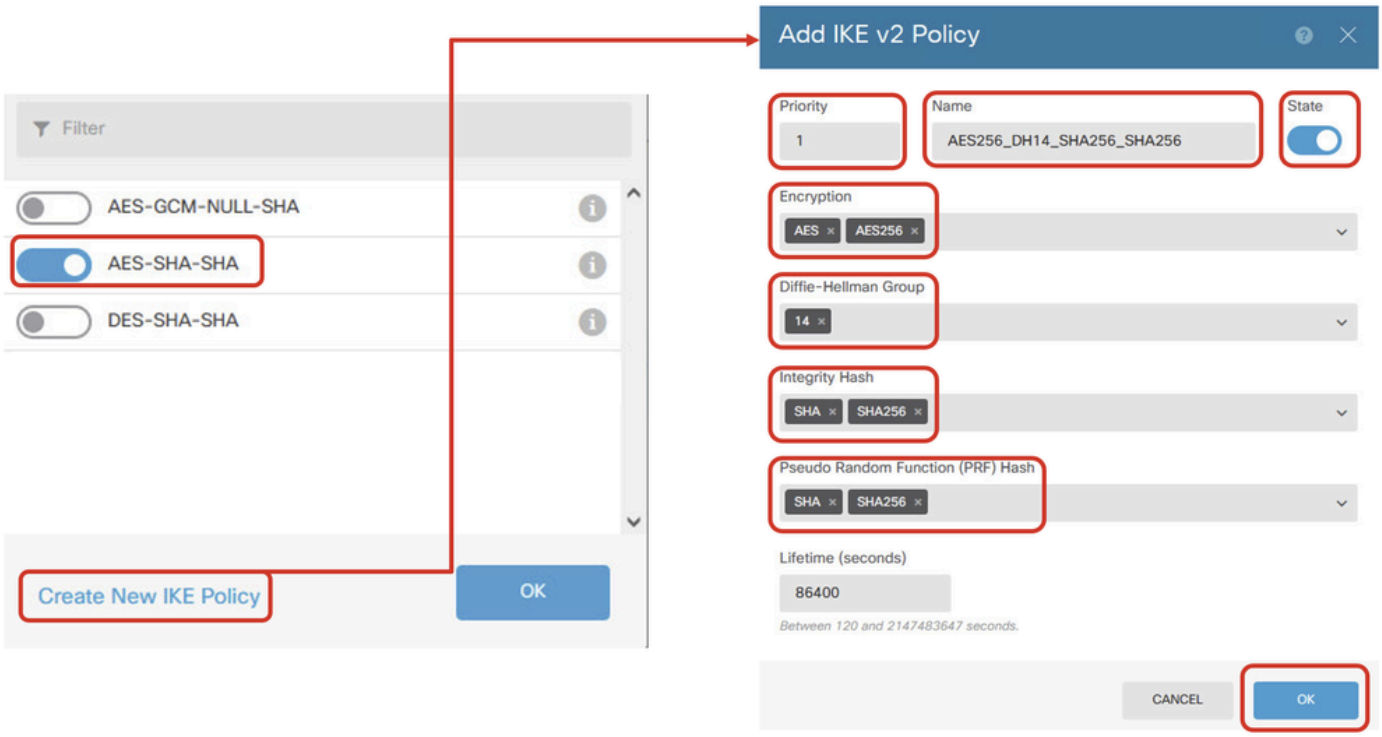


Site1FTD_Edit_IKE_Policy

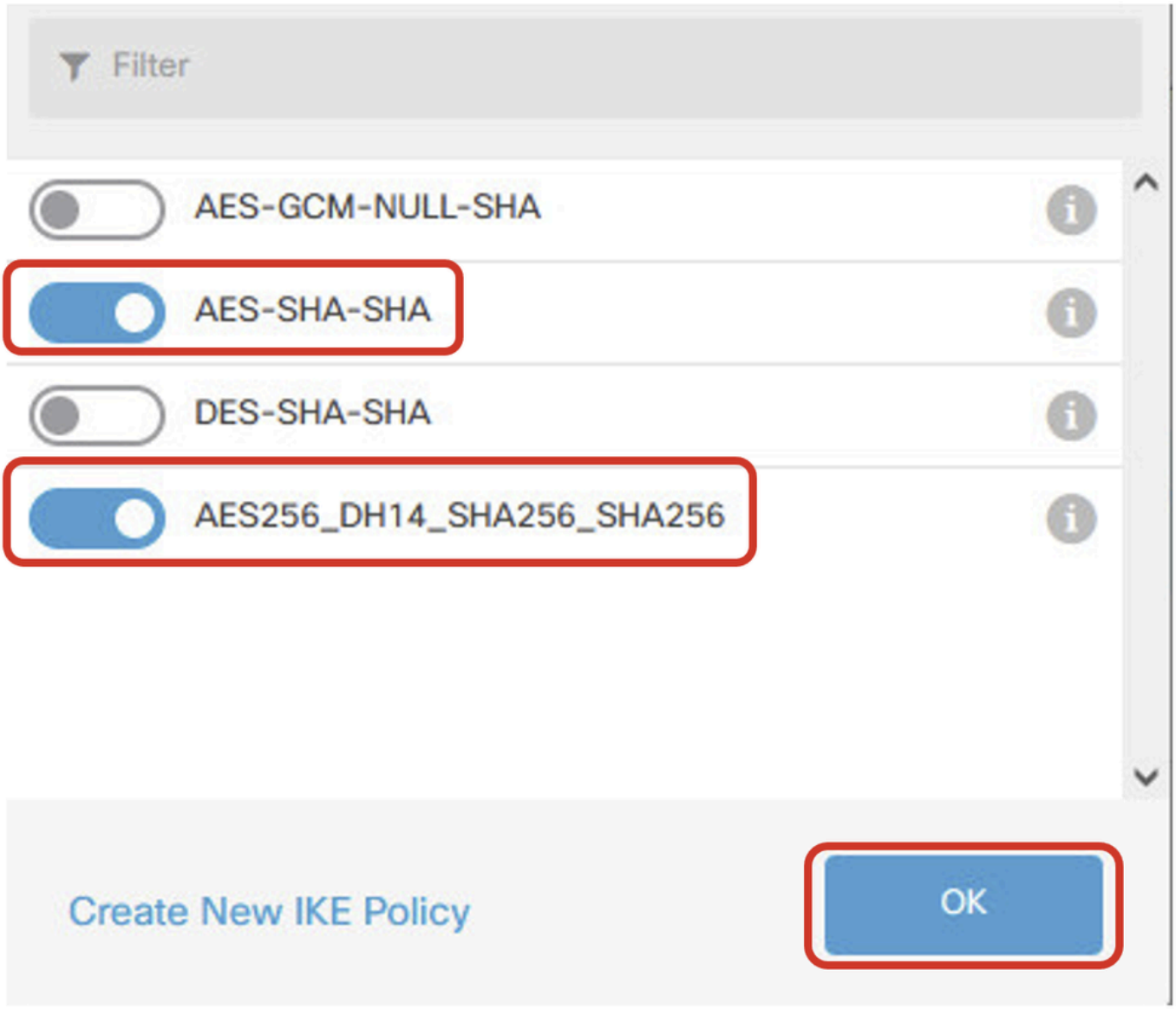
الخطوة 5.3. لنهج IKE، يمكنك إستخدام معرف مسبقا أو يمكنك إنشاء نهج جديد بالنقر فوق إنشاء نهج IKE جديد.

في هذا المثال، قم بالتبديل بين سياسة IKE الحالية AES-SHA وقم أيضا بإنشاء سياسة جديدة بغرض العرض التوضيحي. طقطقة ok زر in order to أنفذت.

- الاسم: AES256_DH14_SHA256_SHA256
- التشفير: معيار التشفير المتطور، معيار AES256
- مجموعة DH: 14
- تجزئة التكامل: أ.م. 256
- تجزئة PRF: أ.م. 256
- العمر: 86400 (الافتراضي)

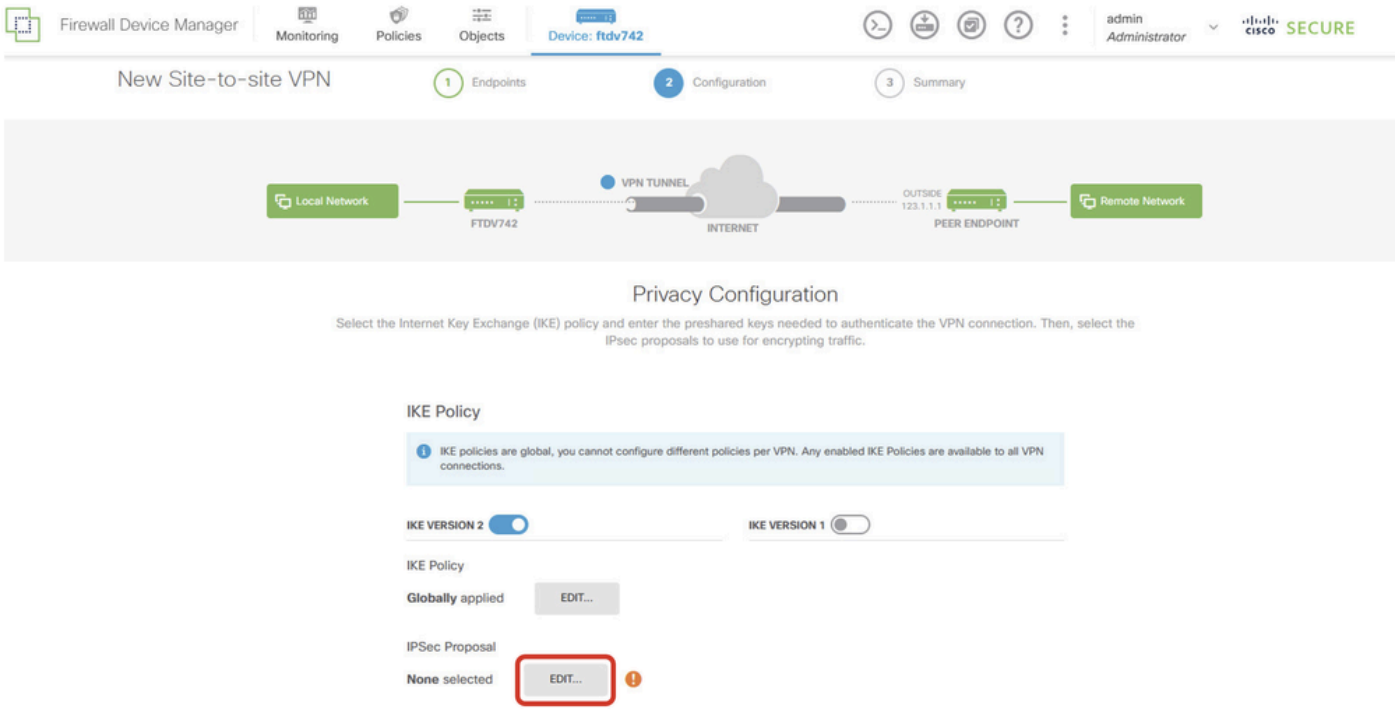


Site1FTD_Add_New_IKE_Policy



site1FTD_ENABLE_NEW_IKE_POLICY

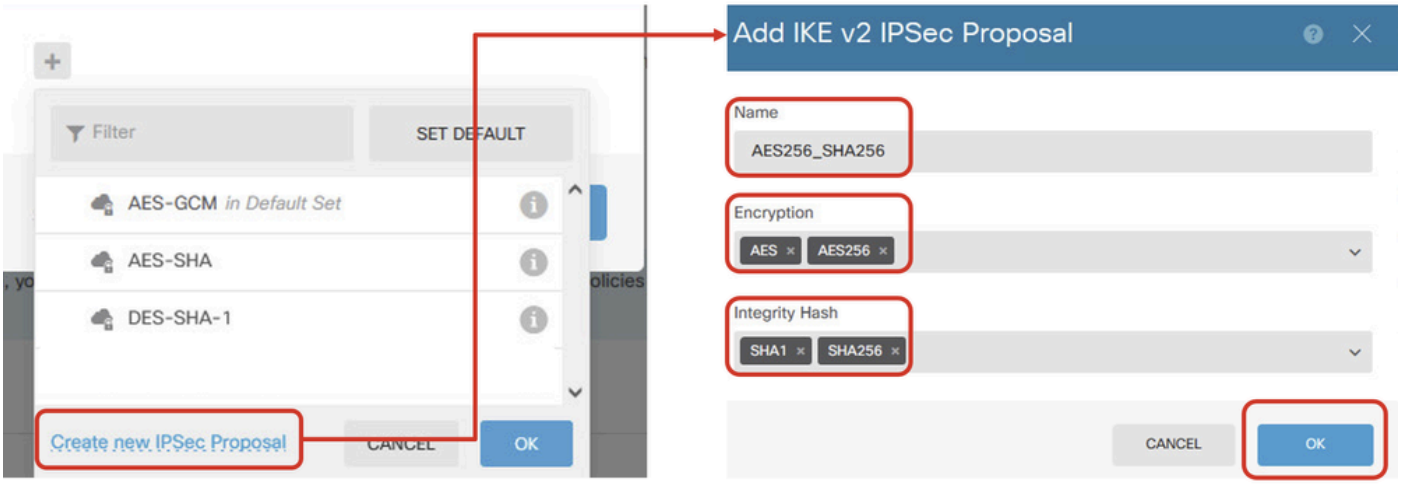
الخطوة 5.4. انتقل إلى اقتراح IPSec. طقطقة يحرر زر.



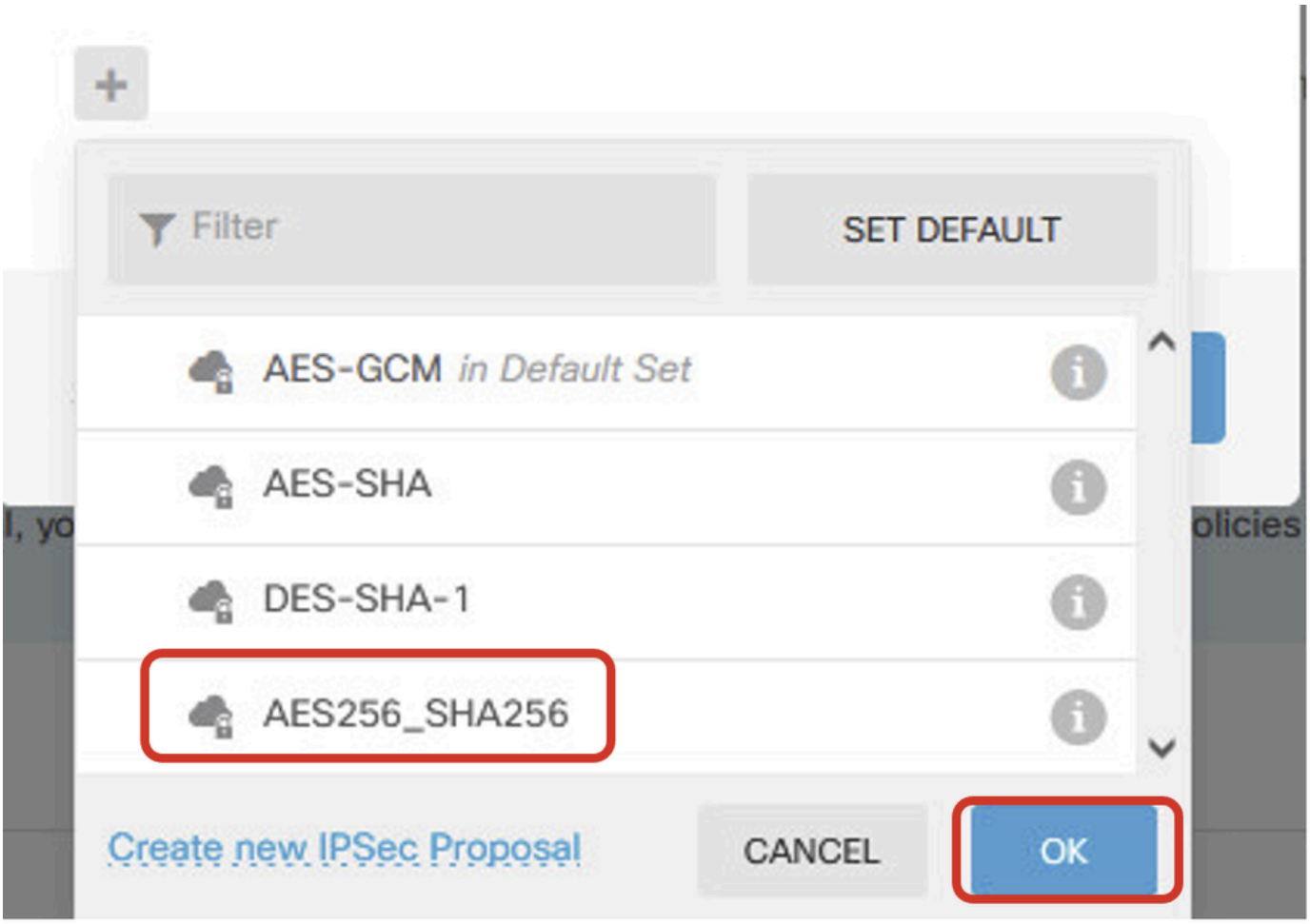
Site1FTD_Edit_IKE_Proposal

الخطوة 5.5. بالنسبة لاقتراح IPSec، يمكنك إستخدام معرف مسبقا أو يمكنك إنشاء اقتراح جديد من خلال النقر فوق إنشاء مقترح IPSec جديد. في هذا المثال، قم بإنشاء مثال جديد لغرض العرض التوضيحي. طقطقة ok زر in order to أنقذت.

- الاسم: AES256_SHA256
- التشفير: معيار التشفير المتطور، معيار AES256
- تجزئة التكامل: SHA1، SHA256



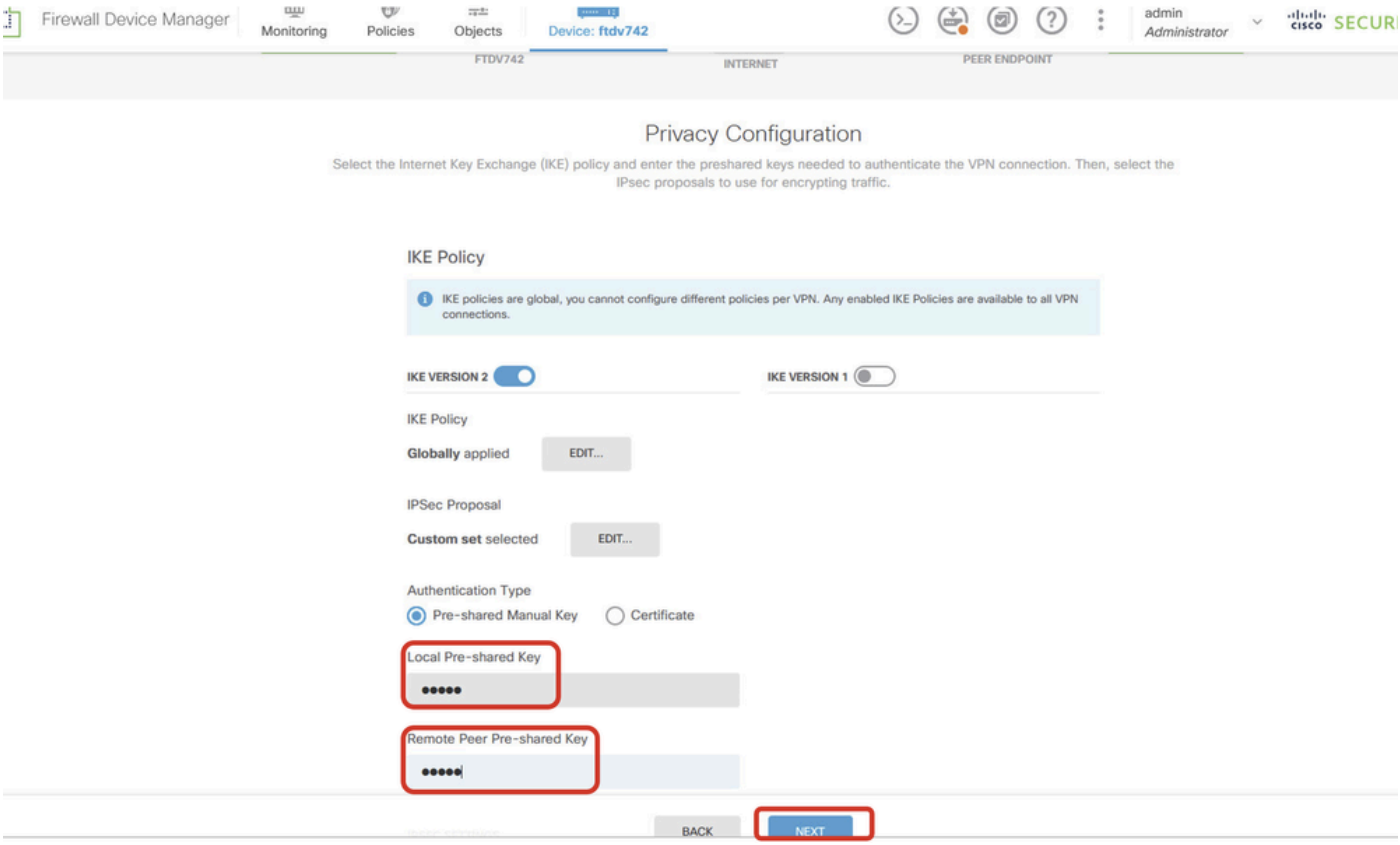
Site1FTD_Add_New_IKE_Proposal



Site1FTD_ENABLE_NEW_IKE_Proposal

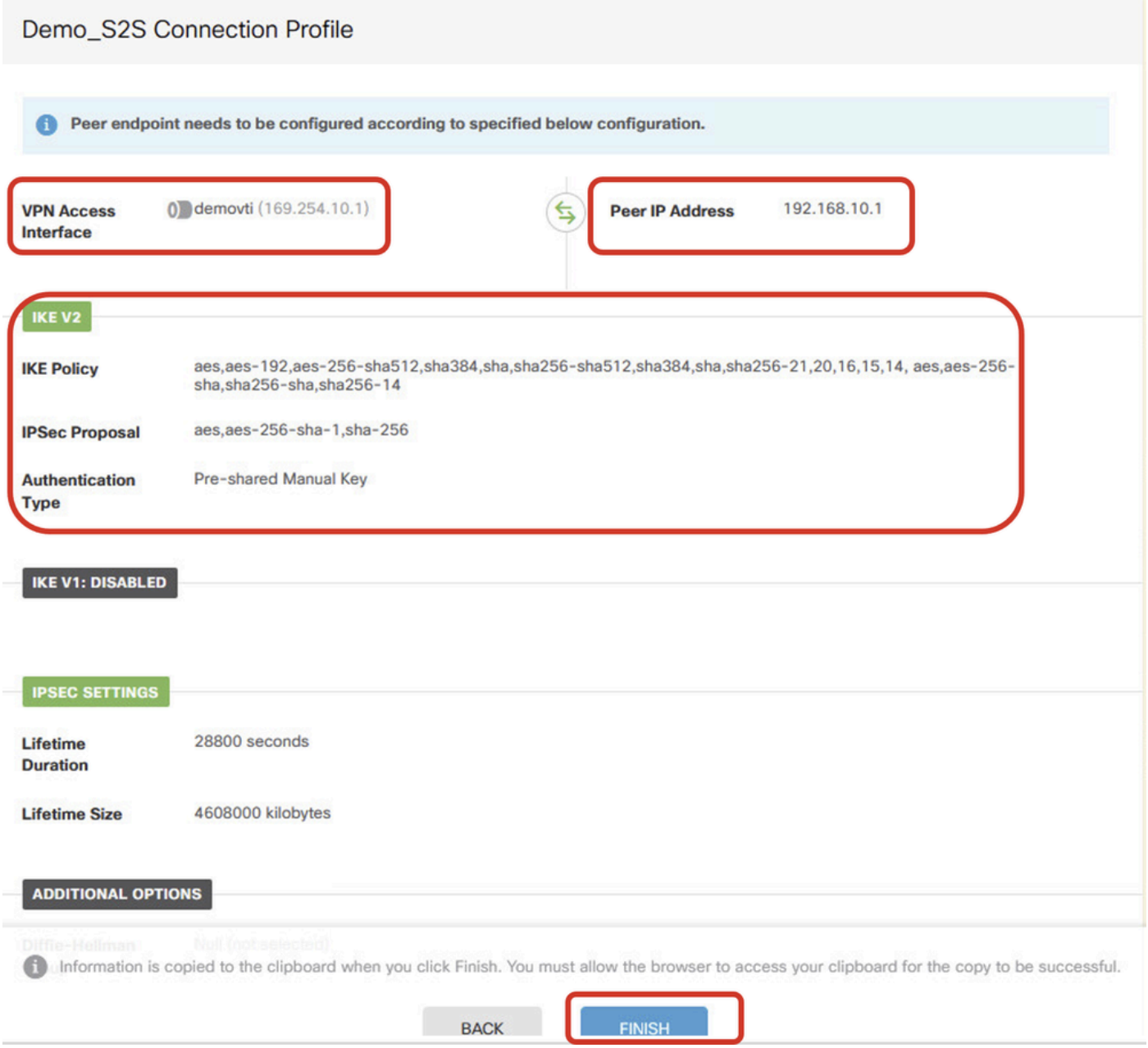
الخطوة 5.6. انزلق إلى الصفحة وقم بتكوين المفتاح المشترك مسبقا. انقر فوق الزر التالي.

لاحظ هذا المفتاح المشترك مسبقا وقم بتكوينه على Site2 FTD لاحقا.



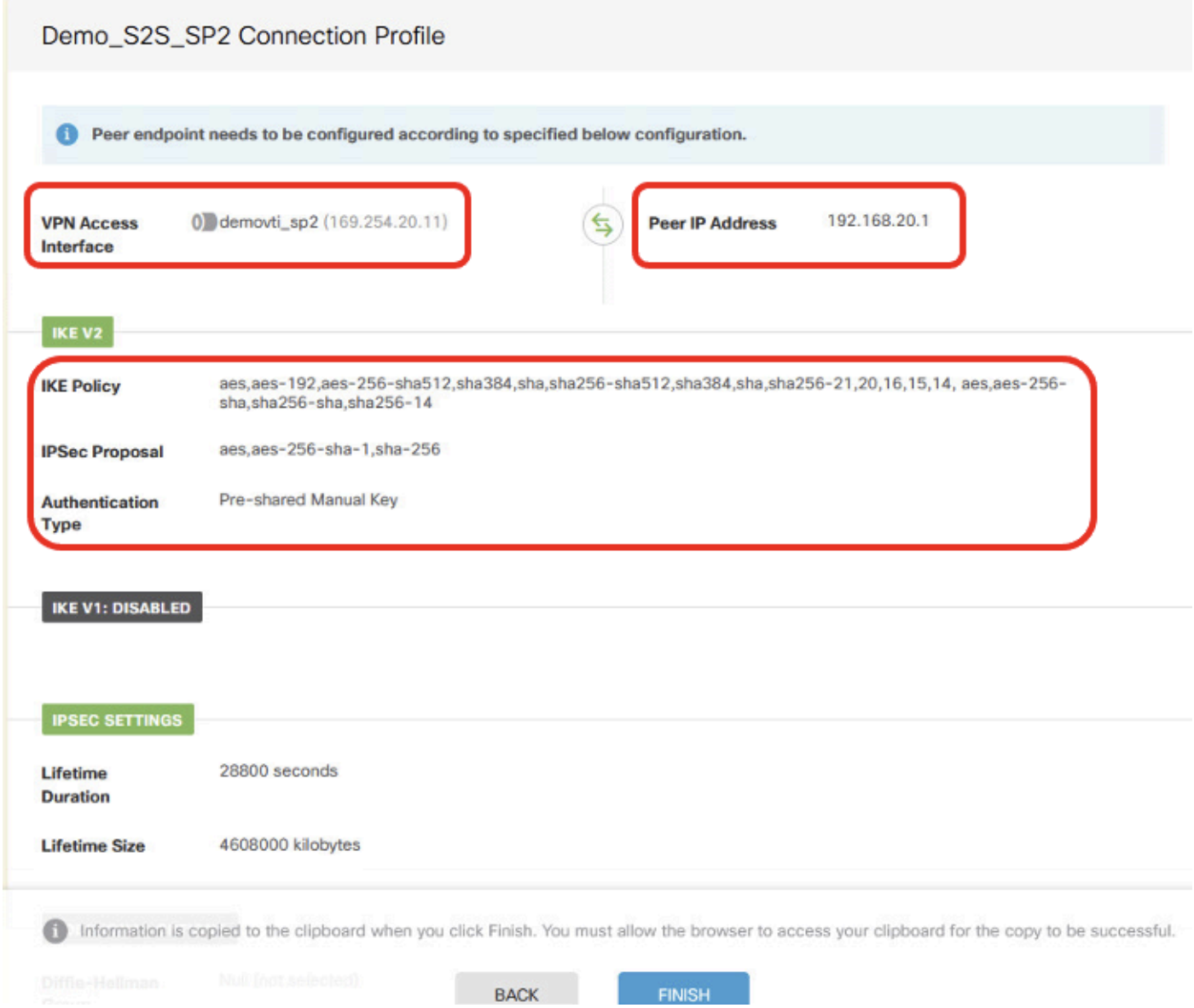
Site1FTD_CONFIGURE_PRE_SHARED_Key

الخطوة 5.7. راجع تكوين شبكة VPN. إذا كان هناك أي شيء يحتاج للتعديل، انقر فوق زر الخلف. إذا كان كل شيء جيدا، انقر فوق الزر إنهاء".



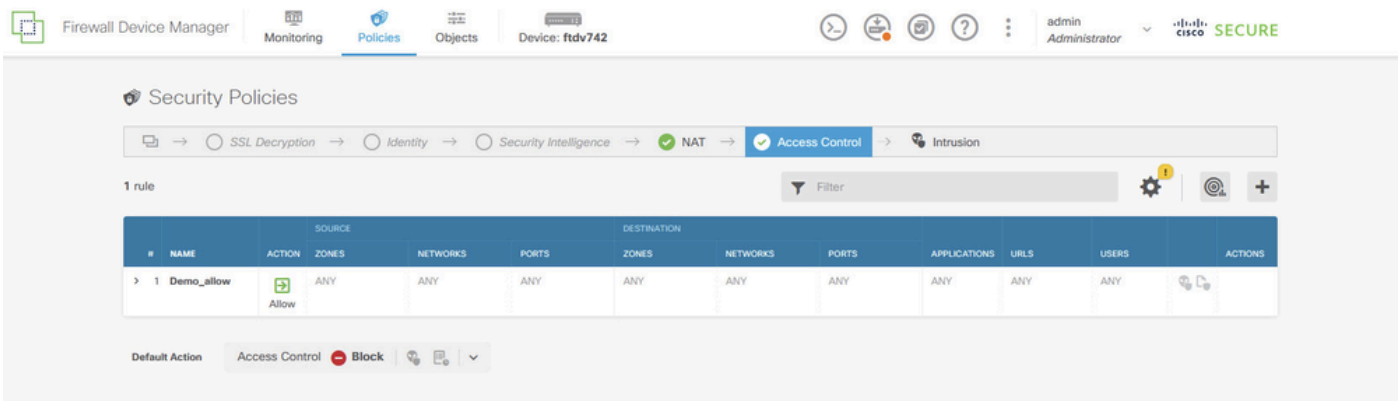
site1FTD_ISP1_REVIEW_VPN_Config_Summary

الخطوة 6. كرر الخطوة 5. من أجل إنشاء شبكة VPN جديدة من موقع إلى موقع من خلال ISP2.



site1FTD_ISP2_REVIEW_VPN_Config_Summary

الخطوة 7. قم بإنشاء قاعدة التحكم في الوصول للسماح لحركة المرور عبر FTD. في هذا المثال، قم بالسماح للجميع بهدف العرض التوضيحي. قم بتعديل النهج الخاص بك استنادا إلى إحتياجاتك الفعلية.



Site1FTD_ALLOW_ACCESS_CONTROL_RULE_EXAMPLE

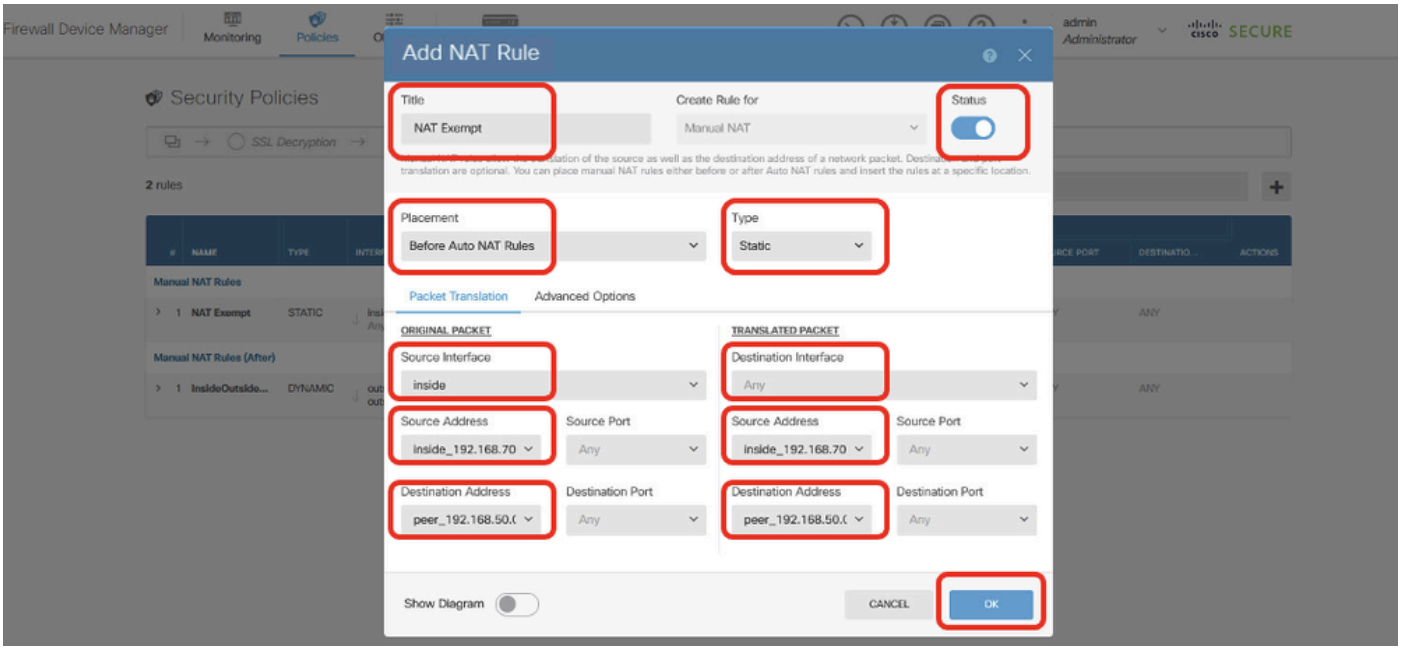
الخطوة 8. (إختياري) قم بتكوين قاعدة إستثناء NAT لحركة مرور العميل على FTD إذا كان

هناك NAT ديناميكي تم تكوينه للعميل من أجل الوصول إلى الإنترنت.

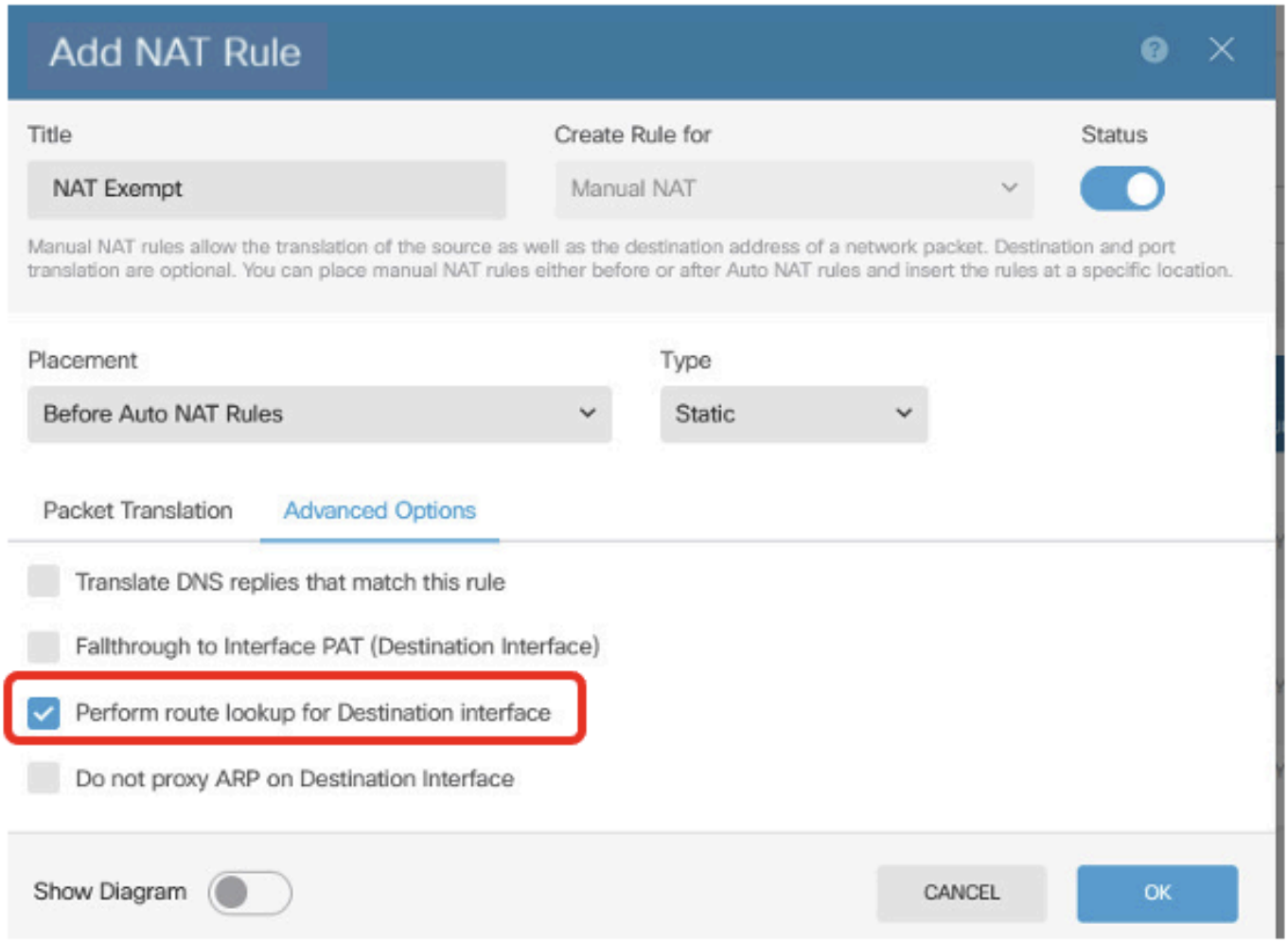
لهدف العرض التوضيحي، يتم تكوين NAT الديناميكي للعملاء من أجل الوصول إلى الإنترنت في هذا المثال. لذلك يلزم وجود قاعدة إستثناء NAT.

انتقل إلى السياسات > NAT. انقر فوق + زر. قم بتوفير التفاصيل وانقر فوق موافق.

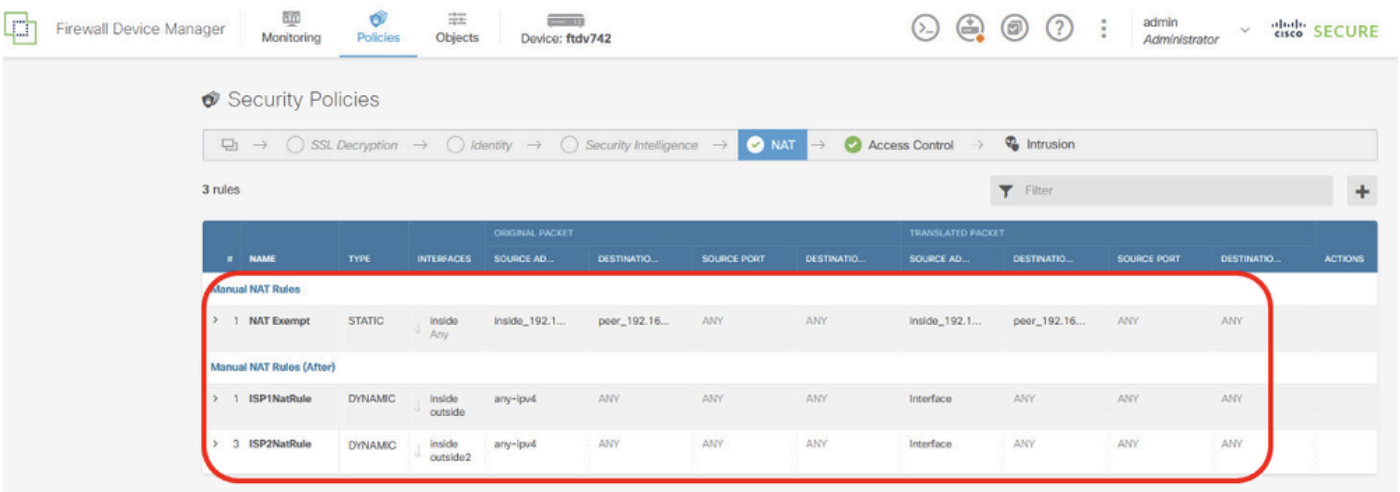
- العنوان: إعفاء NAT
- الوضع: قبل قواعد NAT التلقائية
- النوع: ثابت
- واجهة المصدر: داخل
- الوجهة: أي
- عنوان المصدر الأصلي: 192.168.70.0/24
- عنوان المصدر المترجم: 192.168.70.0/24
- عنوان الوجهة الأصلية: 192.168.50.0/24
- ترجمة غاية عنوان: 192.168.50.0/24
- مع تمكين البحث عن المسار



Site1FTD_NAT_EXEMPT_RULE



site1FTD_nat_EXEMPT_RULE_2



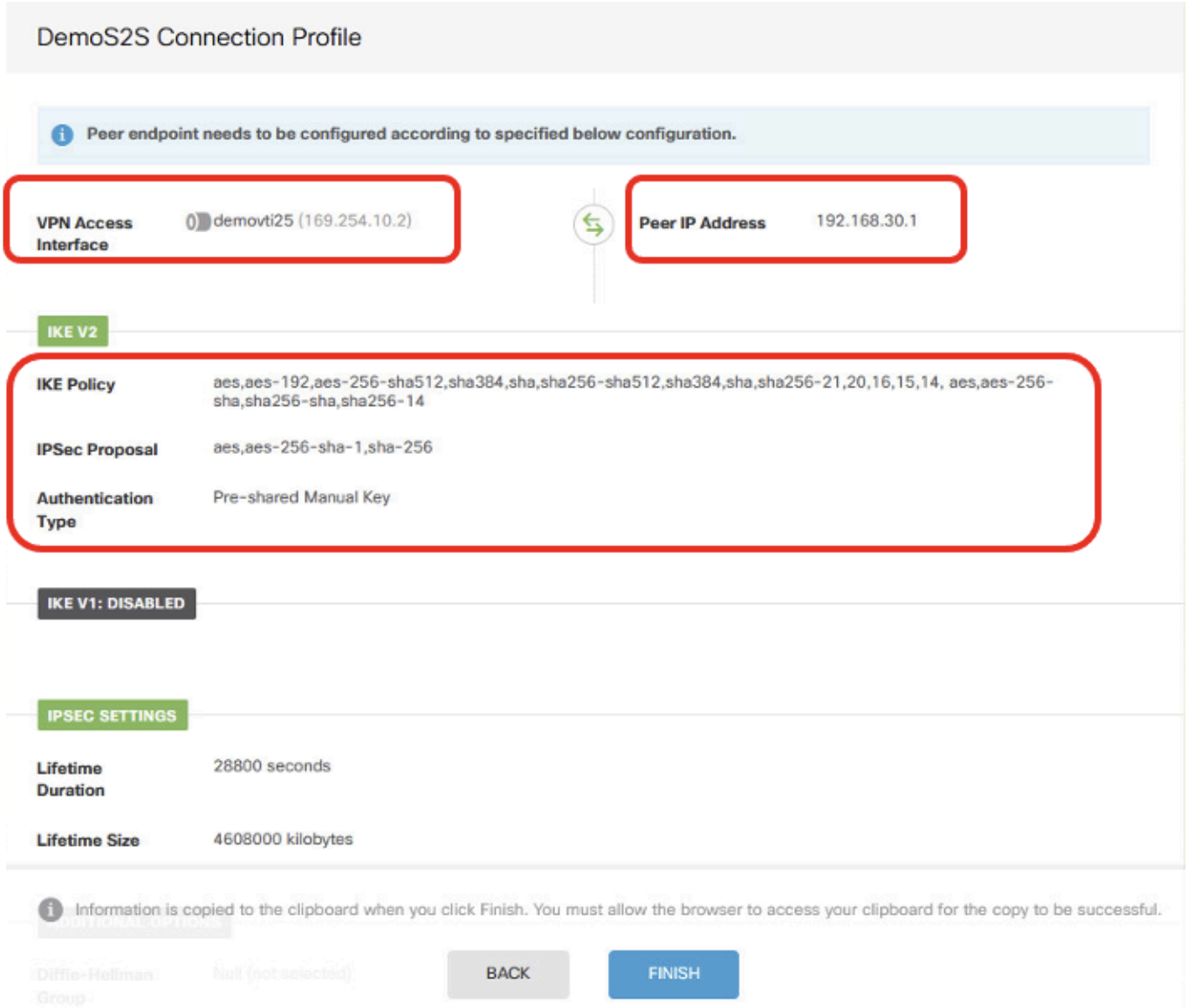
Site1FTD_NAT_RULE_OVERVIEW

الخطوة 9. نشر تغييرات التكوين.

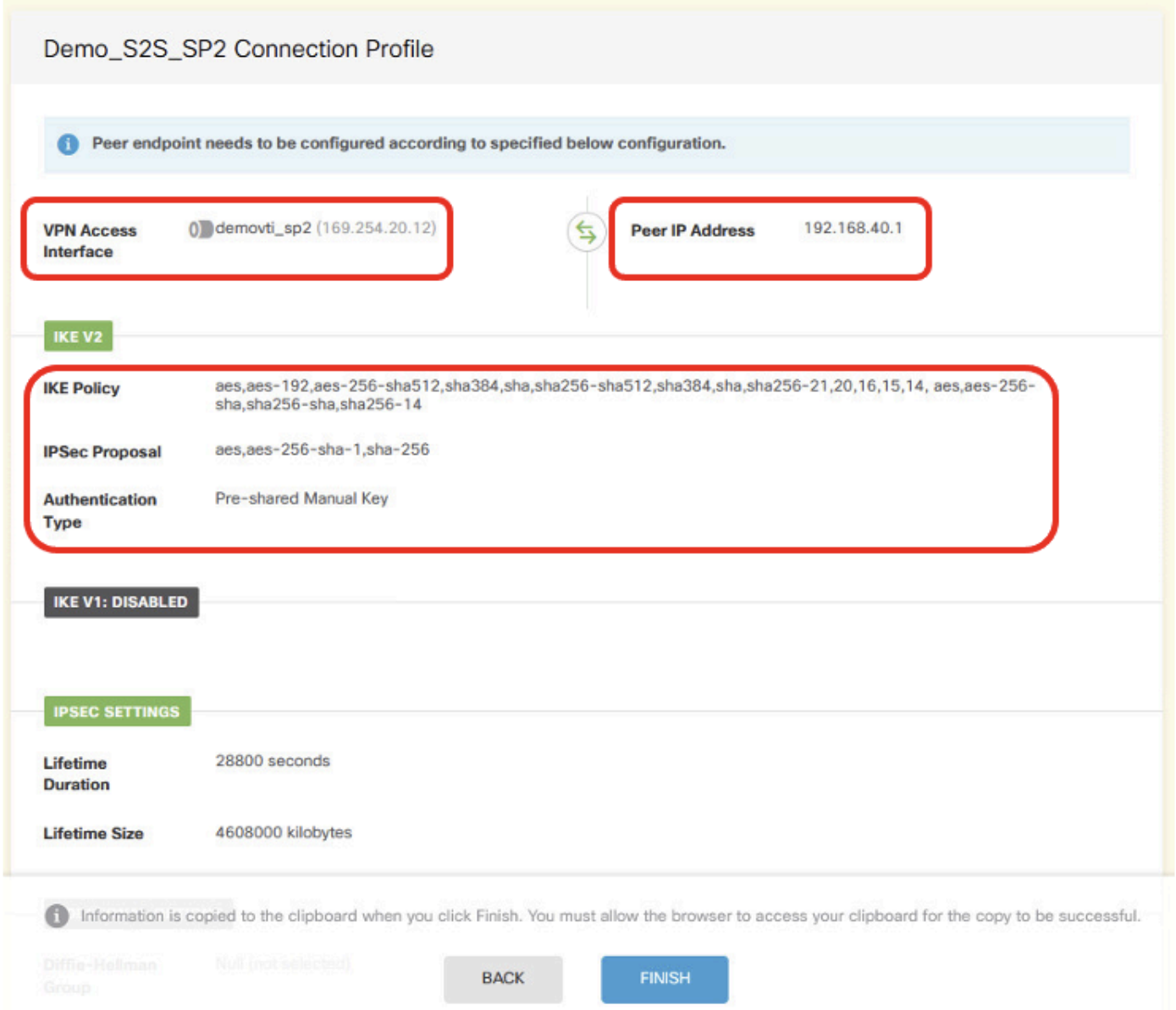
site1FTD_DEPLOYMENT_CHANGES

تكوين Site2 FTD VPN

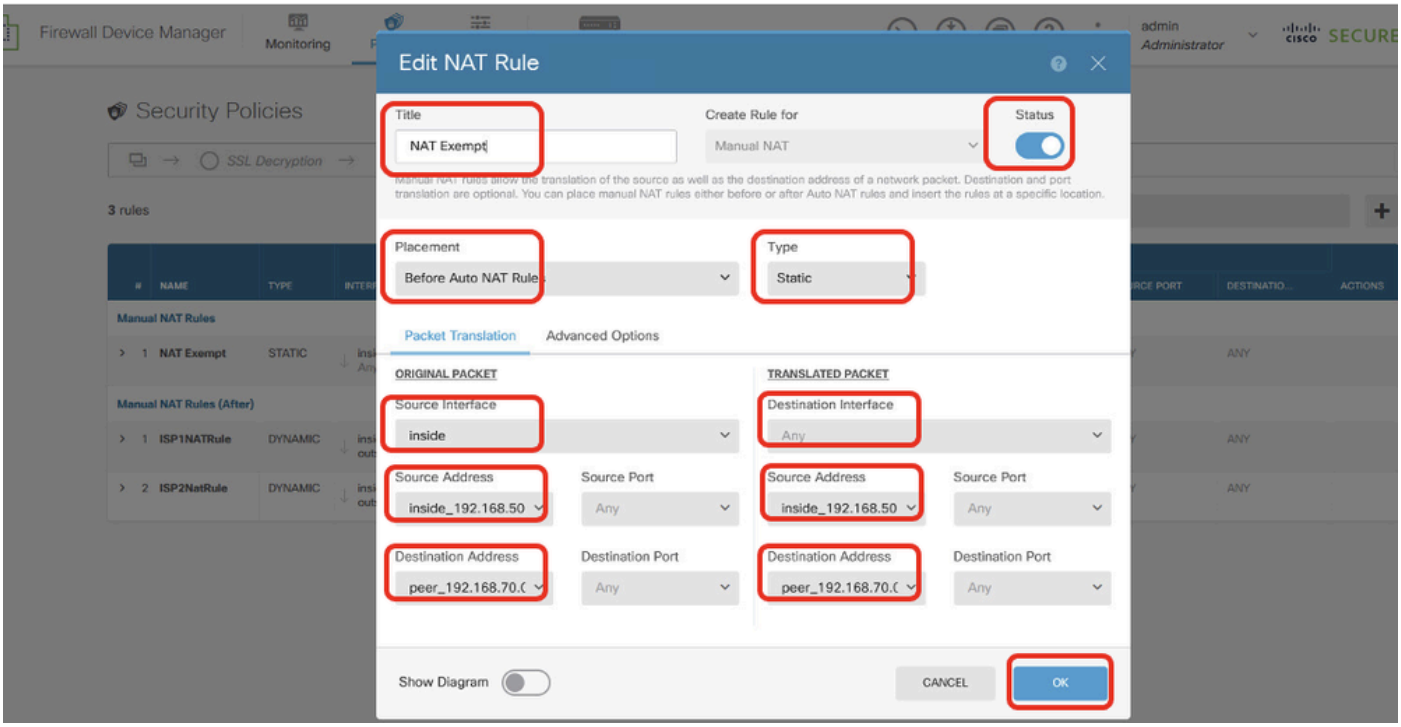
الخطوة 10. كرر الخطوة 1 إلى الخطوة 9 باستخدام المعلمات المقابلة ل Site2 FTD.



site2FTD_ISP1_review_vpn_config_summary



site2FTD_ISP2_review_vpn_config_summary

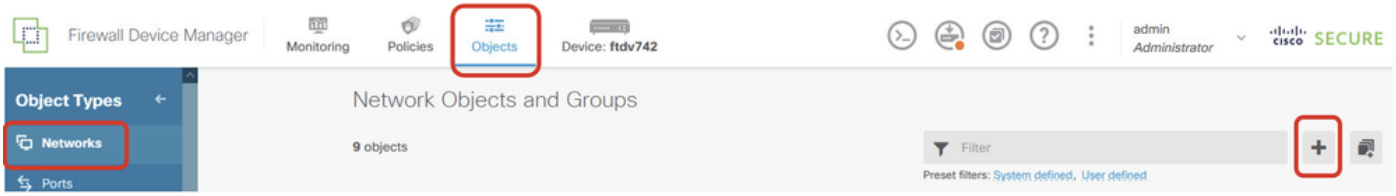


Site2FTD_nat_EXEMPT_RULE

التكوينات على PBR

تكوين PBR الخاص ب Site1 FTD

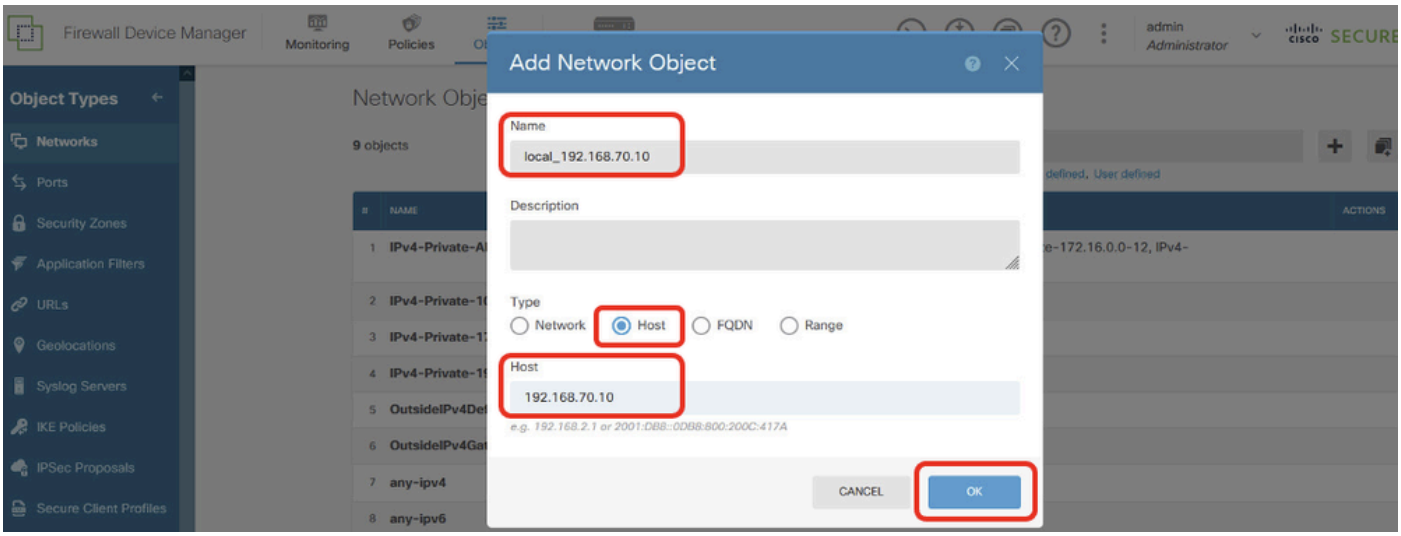
الخطوة 11. قم بإنشاء كائنات شبكة جديدة ليتم إستخدامها من قبل قائمة الوصول ل PBR للموقع 1 FTD. انتقل إلى الكائنات > الشبكات وانقر + زر.



site1FTD_CREATE_NETWORK_OBJECT

الخطوة 11.1. قم بإنشاء كائن لعنوان IP الخاص ب Site1 Client2. قم بتوفير المعلومات الضرورية. انقر فوق الزر موافق.

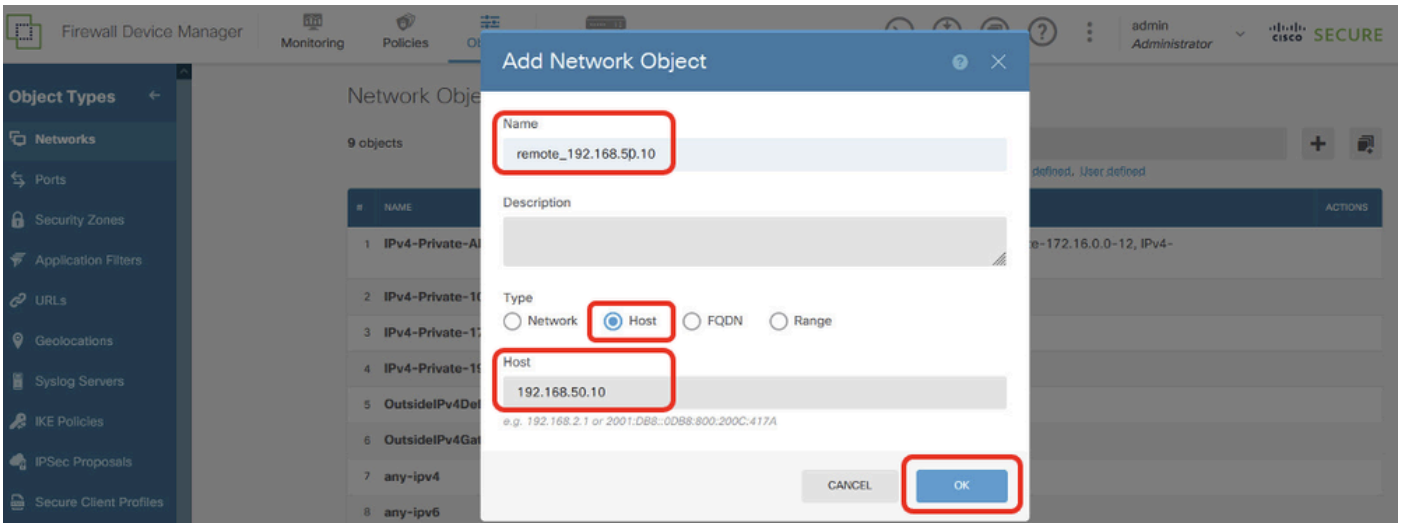
- الاسم: local_192.168.70.10
- النوع: مضيف
- المضيف: 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

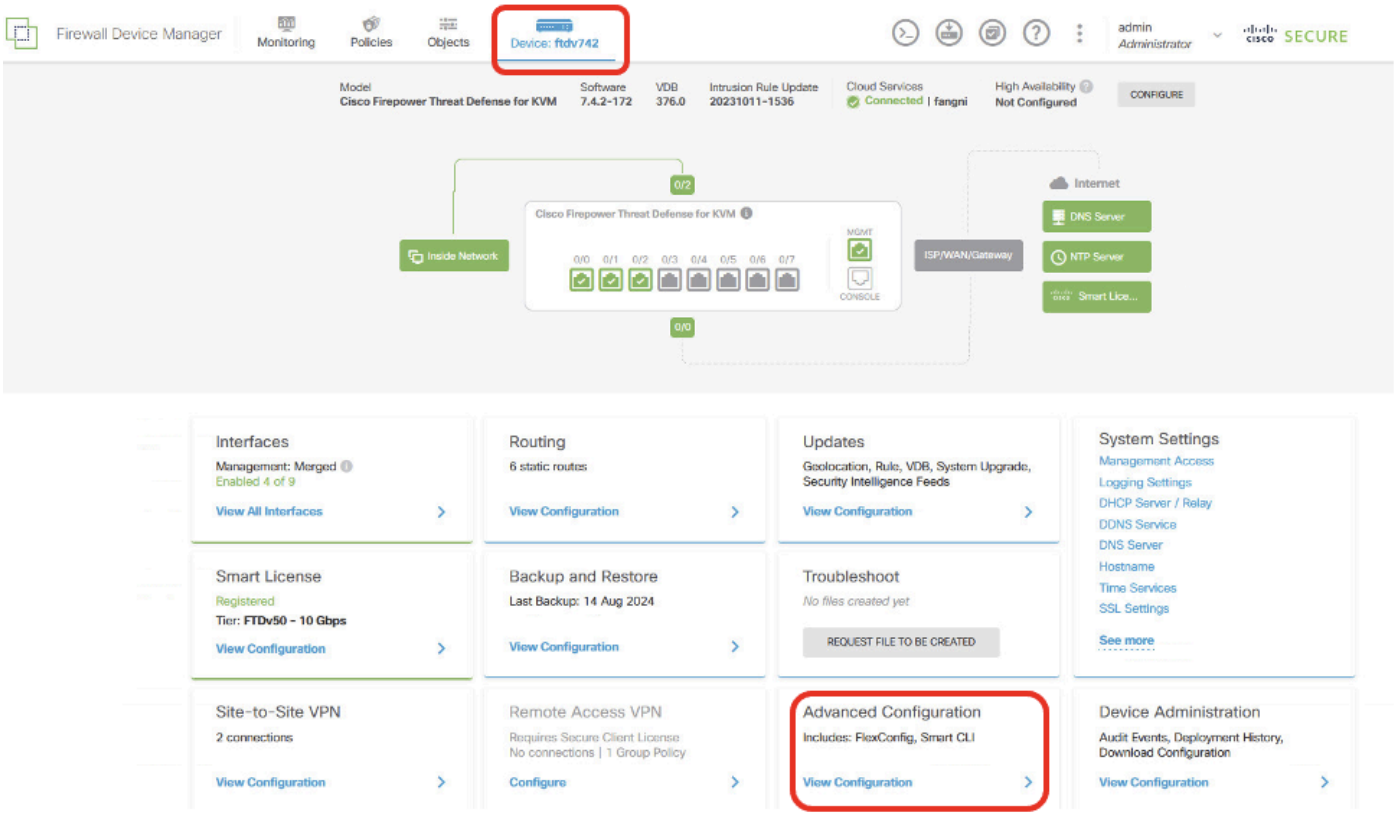
الخطوة 11.2. إنشاء كائن لعنوان IP الخاص ب Site2 Client2. توفير المعلومات اللازمة. طقطقت ok زر.

- الاسم: remote_192.168.50.10
- النوع: مضيف
- المضيف: 192.168.50.10



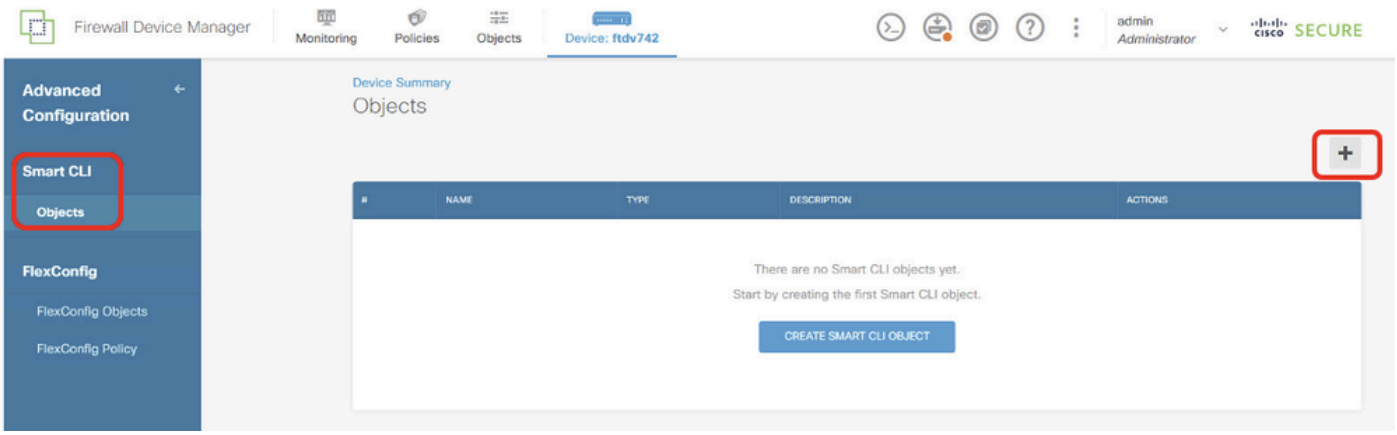
Site1FTD_PBR_RemoteObject

الخطوة 12. إنشاء قائمة وصول موسعة ل PBR. انتقل إلى الجهاز > التكوين المتقدم. طقطقة عرض تشكيل.



site1FTD_VIEW_ADVANCED_CONFIGURATION

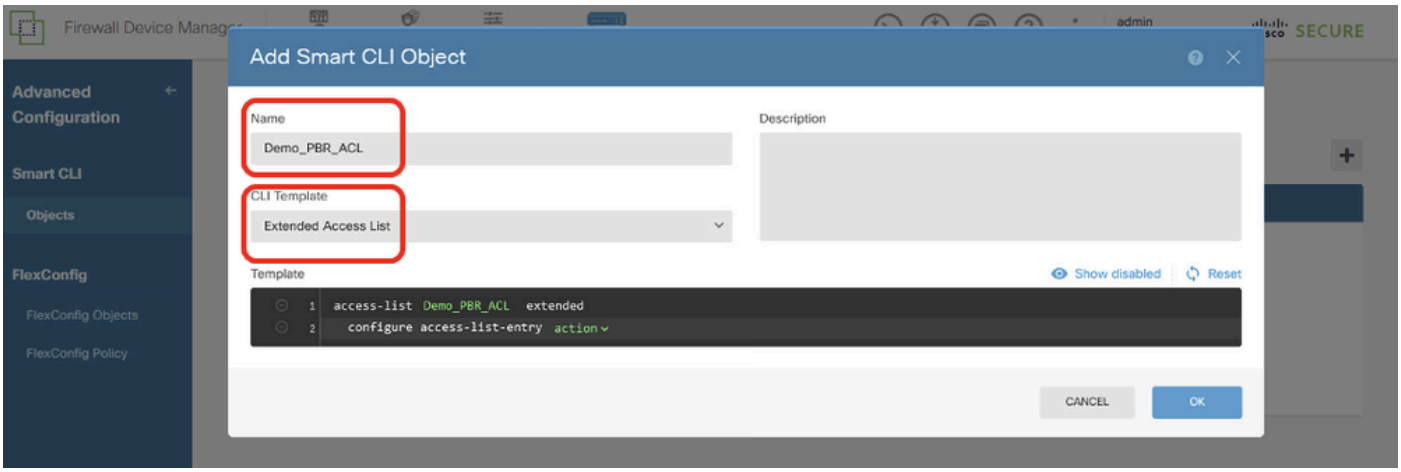
الخطوة 12.1. انتقل إلى CLI (واجهة سطر الأوامر) الذكية > الكائنات. انقر فوق + زر.



Site1FTD_Add_SmartCLI_Object

الخطوة 12.2. أدخل اسما للكائن واختر قالب واجهة سطر الأوامر.

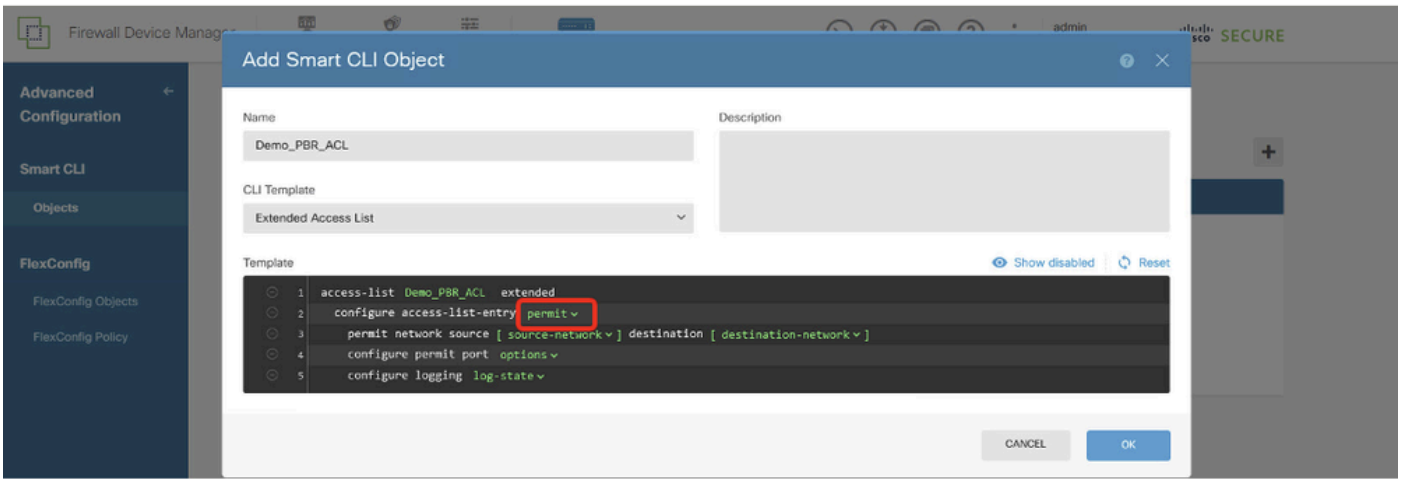
- الاسم: العرض التوضيحي_PBR_ACL
- قالب واجهة سطر الأوامر: قائمة الوصول الموسعة



Site1FTD_Create_PBR_ACL_1

الخطوة 12.3. انتقل إلى القالب والتكوين. طقطقت ال ok زر in order to أنقذت.

السطر 2، انقر فوق إجراء. أختر سماح.

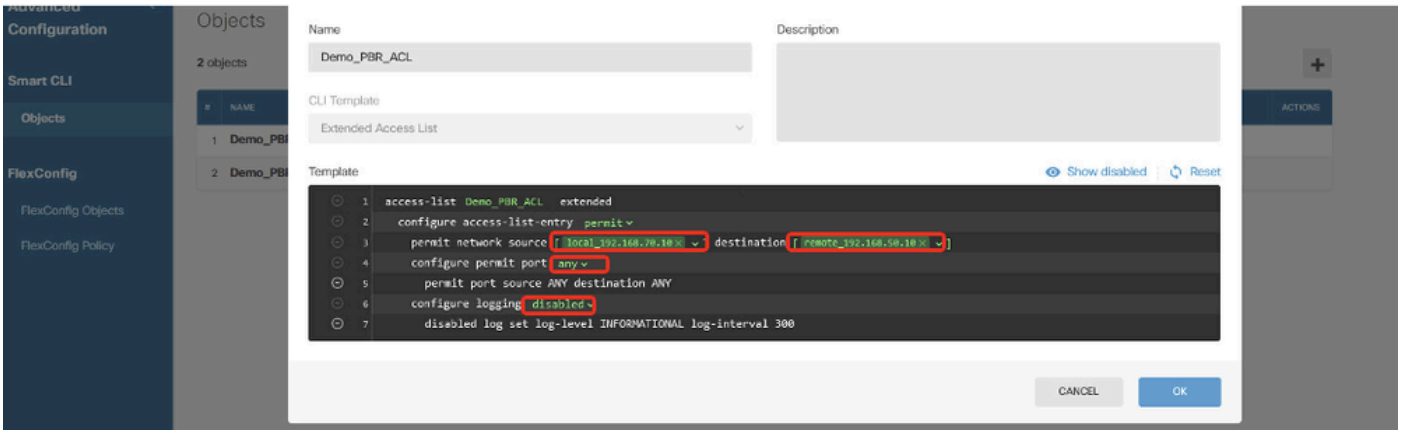


Site1FTD_Create_PBR_ACL_2

السطر 3، انقر فوق شبكة المصدر. أخترت محلي_192.168.70.10. طقطقت غايةة-شبكة. أختر remote_192.168.50.10.

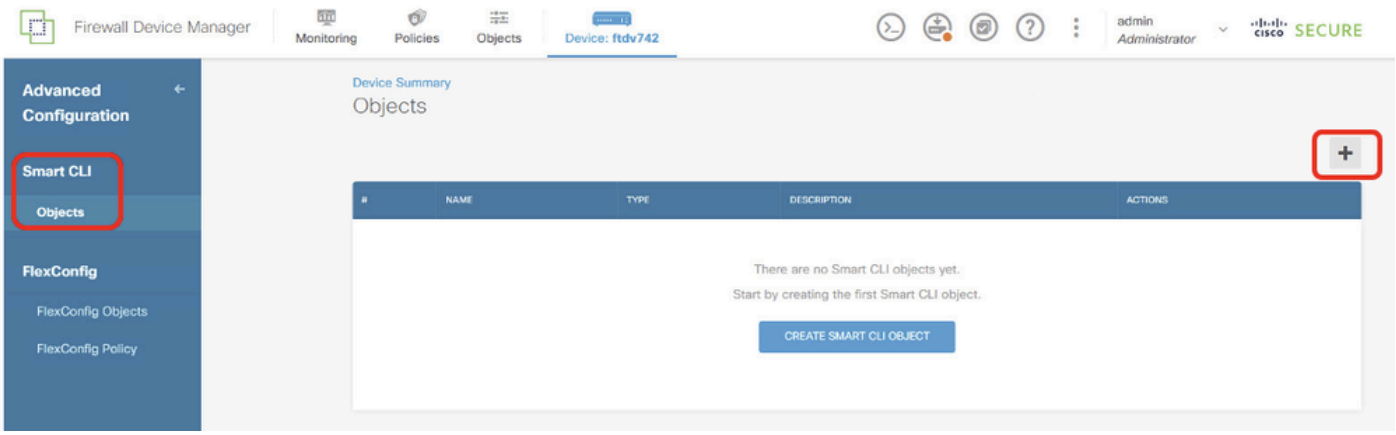
السطر 4، انقر الخيارات واختر أي.

السطر 6، انقر فوق حالة السجل واختر معطل.



Site1FTD_Create_PBR_ACL_3

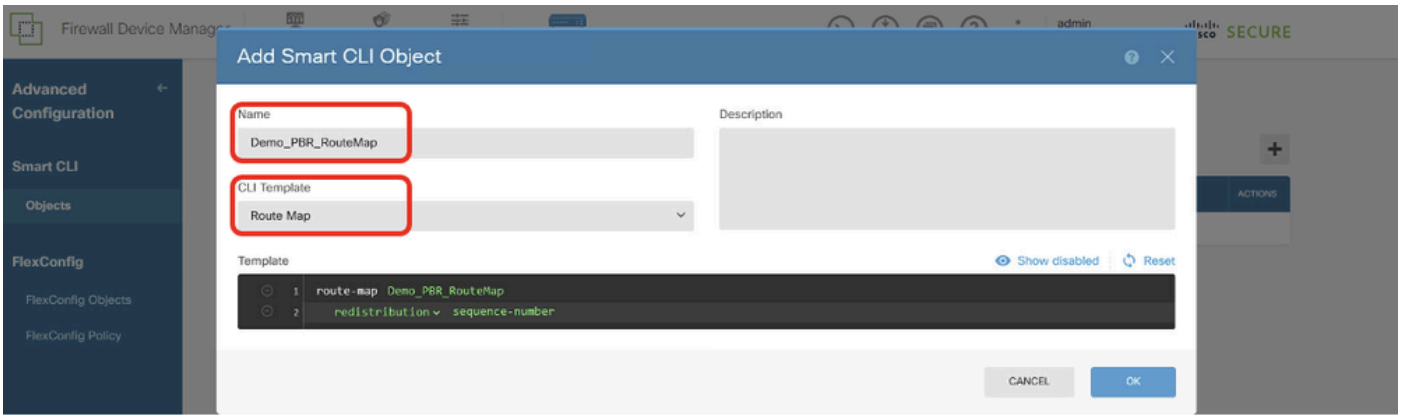
الخطوة 13. إنشاء خريطة مسار ل PBR. انتقل إلى الجهاز > تكوين متقدم > CLI الذكي > الكائنات. انقر فوق + زر.



Site1FTD_Add_SmartCLI_Object

الخطوة 13.1. أدخل اسما للكائن واختر قالب واجهة سطر الأوامر.

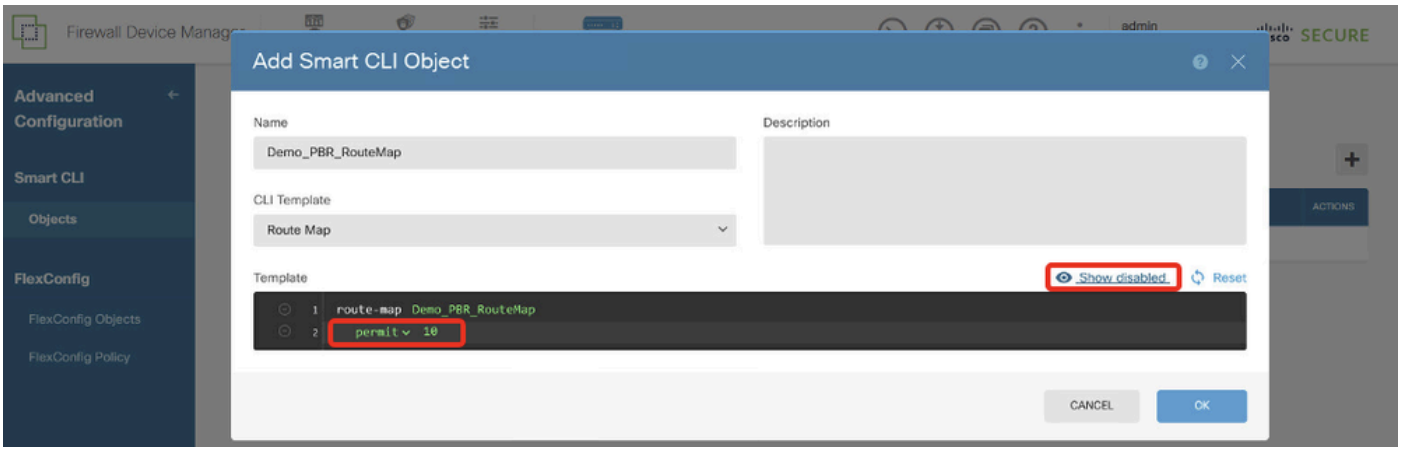
- الاسم: العرض التوضيحي_PBR_RouteMap
- قالب واجهة سطر الأوامر: خريطة المسار



Site1FTD_Create_PBR_RouteMap_1

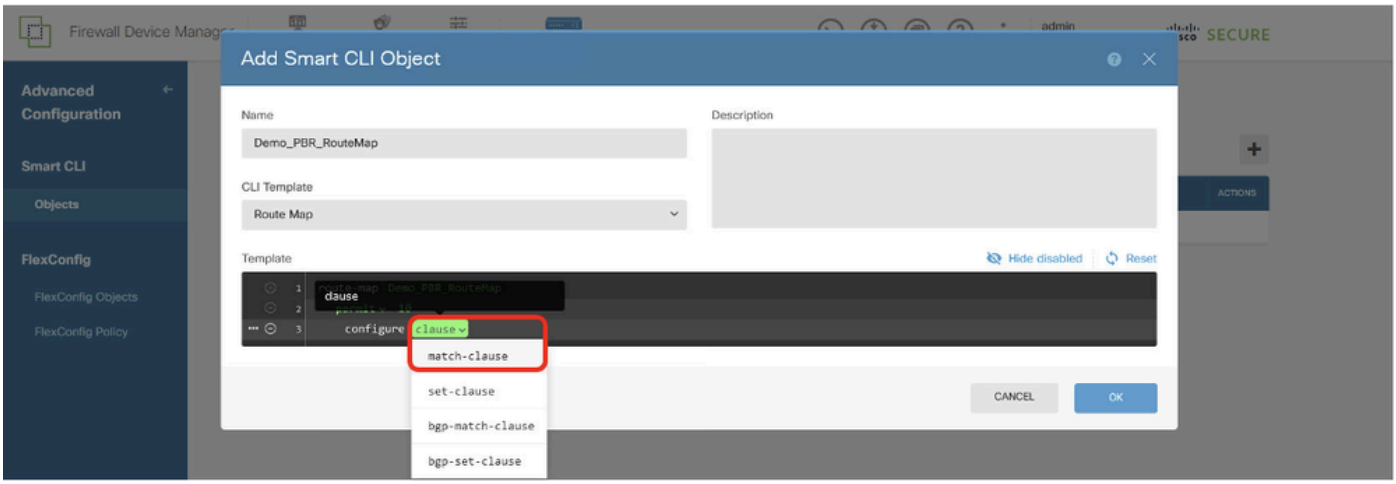
الخطوة 13.2. انتقل إلى القالب والتكوين. انقر فوق الزر موافق" للحفظ.

السطر 2، انقر إعادة توزيع. أختر سماح. انقر فوق sequence-number، الإدخال اليدوي 10. انقر فوق إظهار المعطل.



Site1FTD_Create_PBR_RouteMap_2

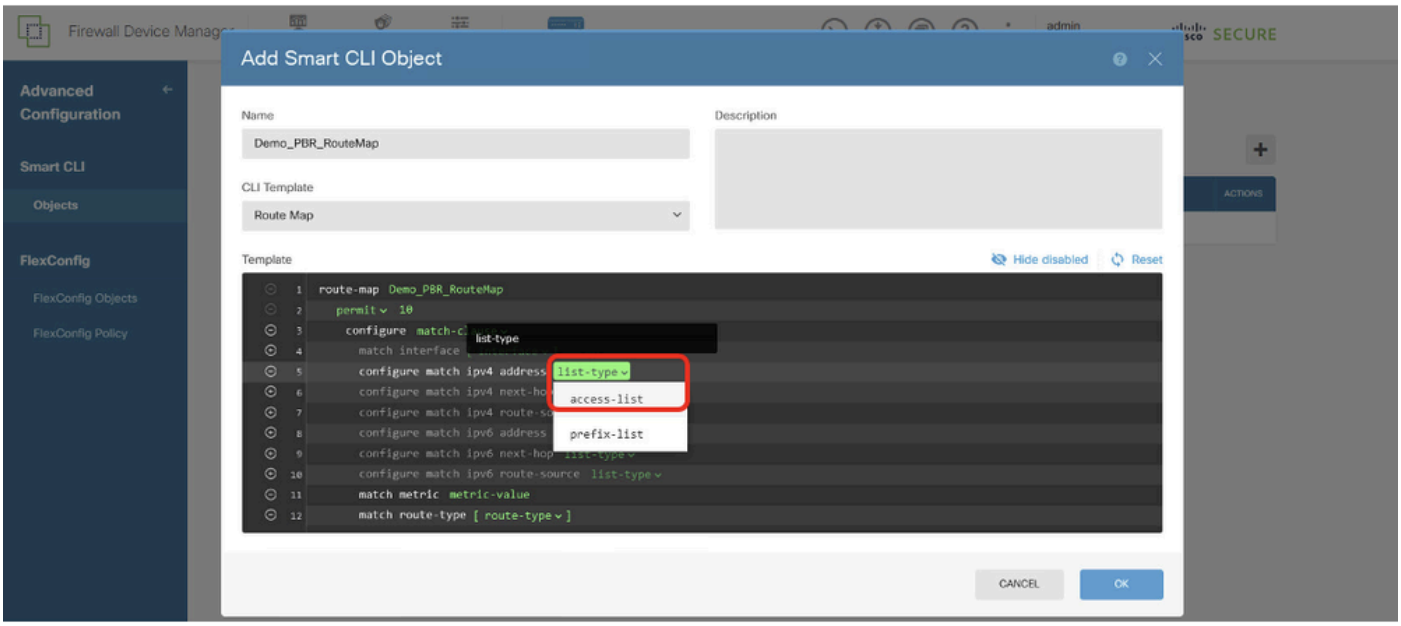
السطر 3، انقر فوق + لتمكين السطر. طقطقة عبارة. أختر عبارة المطابقة.



Site1FTD_Create_PBR_RouteMap_3

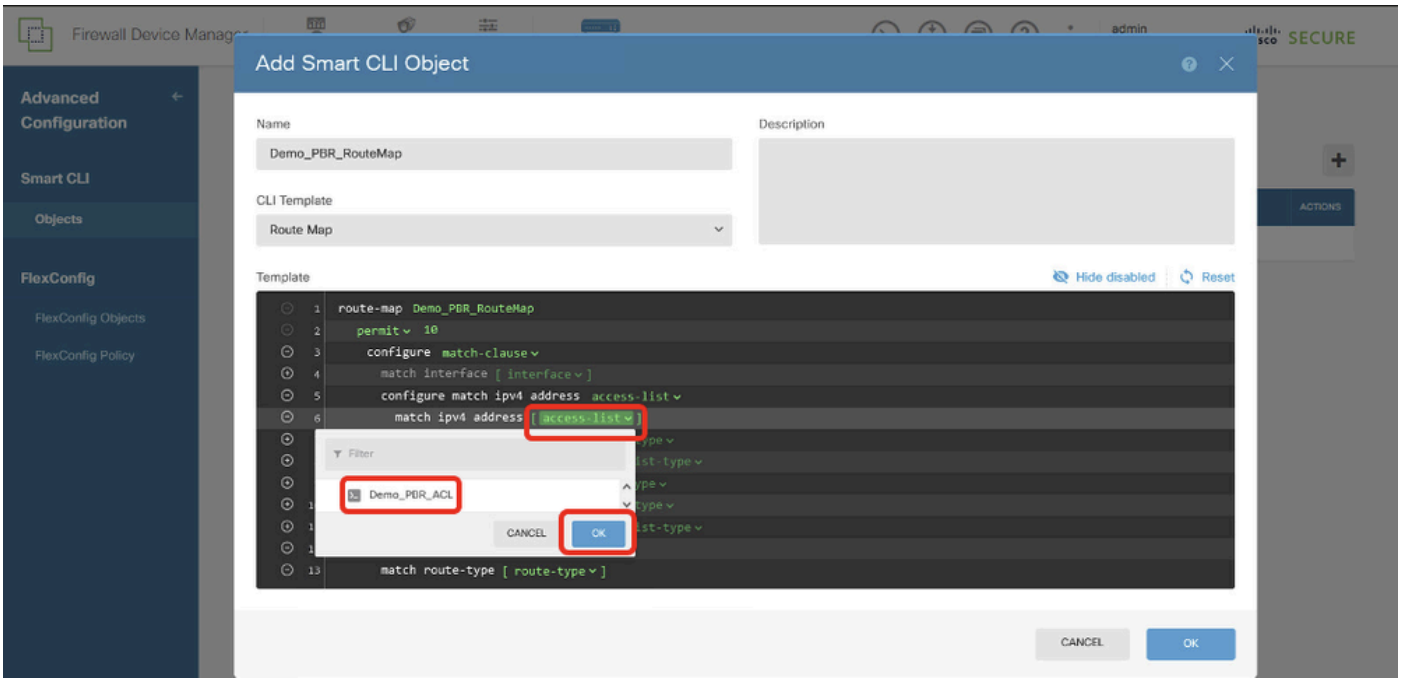
السطر 4، انقر - لتعطيل الخط.

السطر 5، انقر + لتمكين السطر. انقر فوق نوع القائمة. أختر قائمة الوصول.



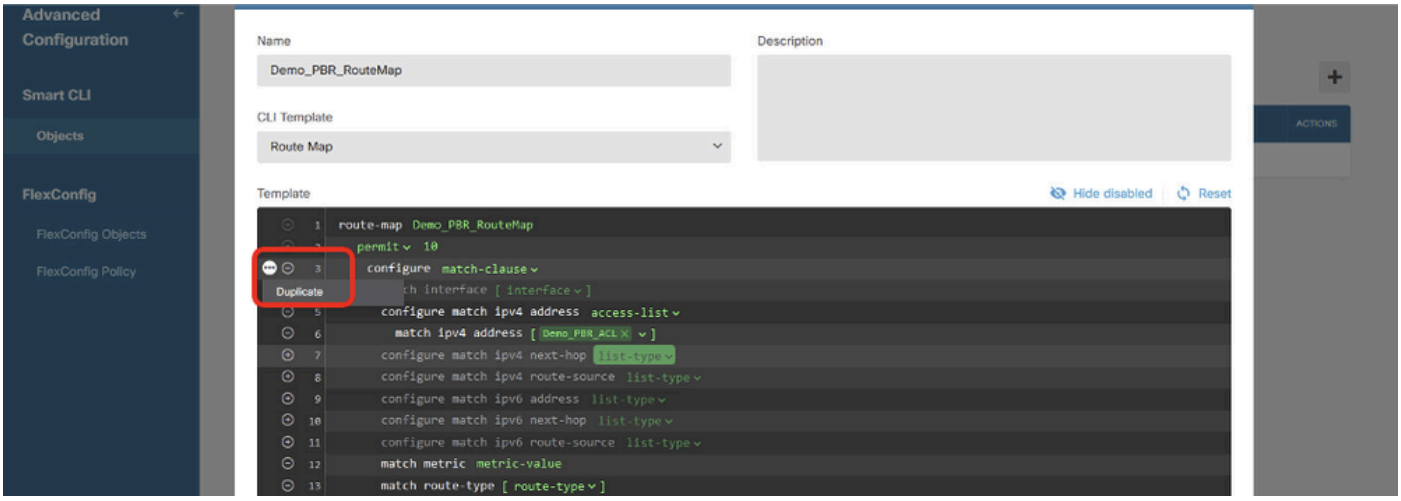
Site1FTD_Create_PBR_RouteMap_4

السطر 6، انقر فوق قائمة الوصول. أختر اسم قائمة التحكم في الوصول (ACL) الذي تم إنشاؤه في الخطوة 12. في هذا المثال، ستكون demo_pbr_acl.



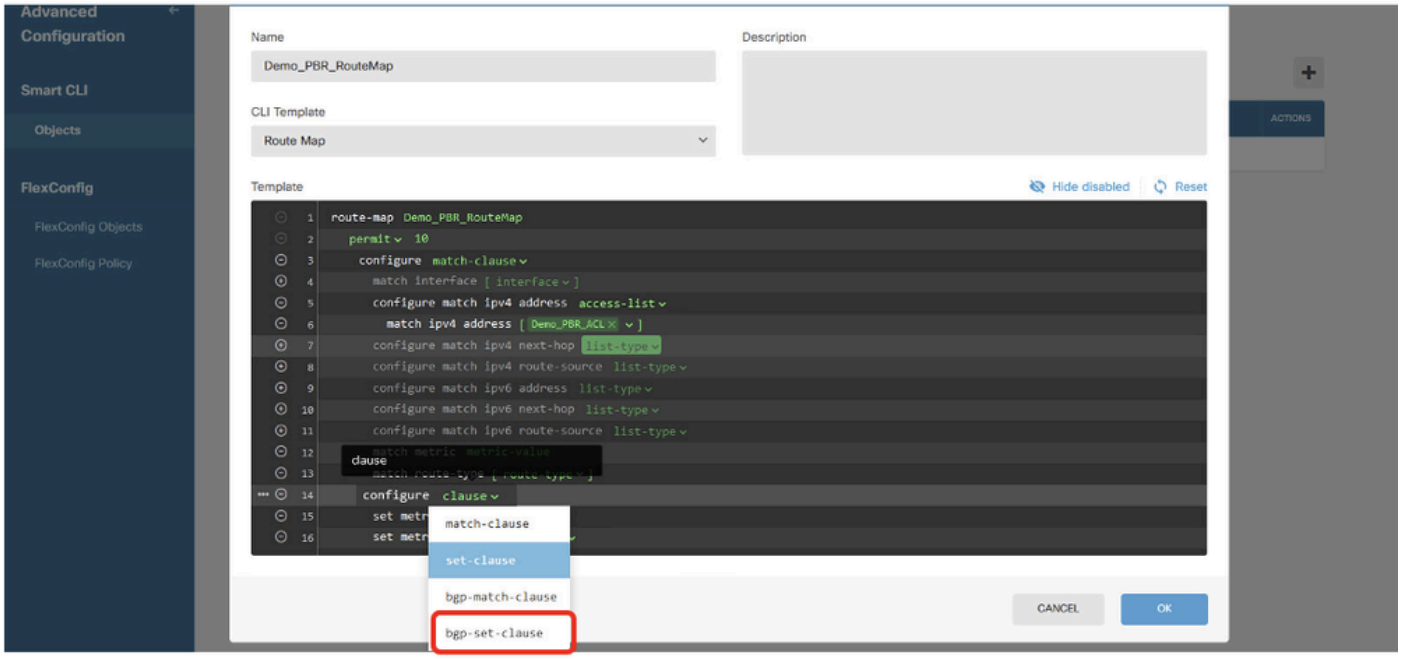
Site1FTD_Create_PBR_RouteMap_5

انقل إلى السطر 3. انقر فوق الخيارات ... أختر مضاعفة.



Site1FTD_Create_PBR_RouteMap_6

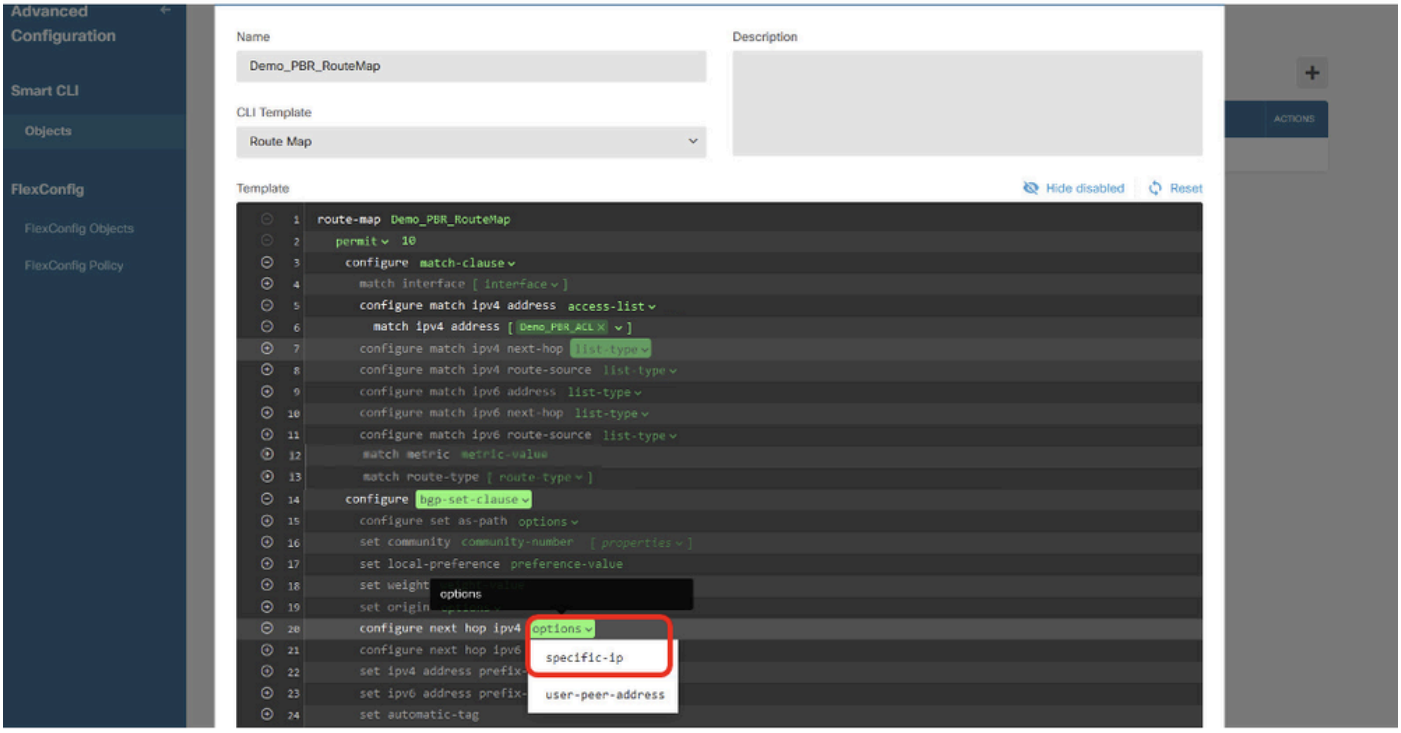
سطر 14، انقر فوق عبارة واختر bgp-set-clause.



Site1FTD_Create_PBR_RouteMap_7

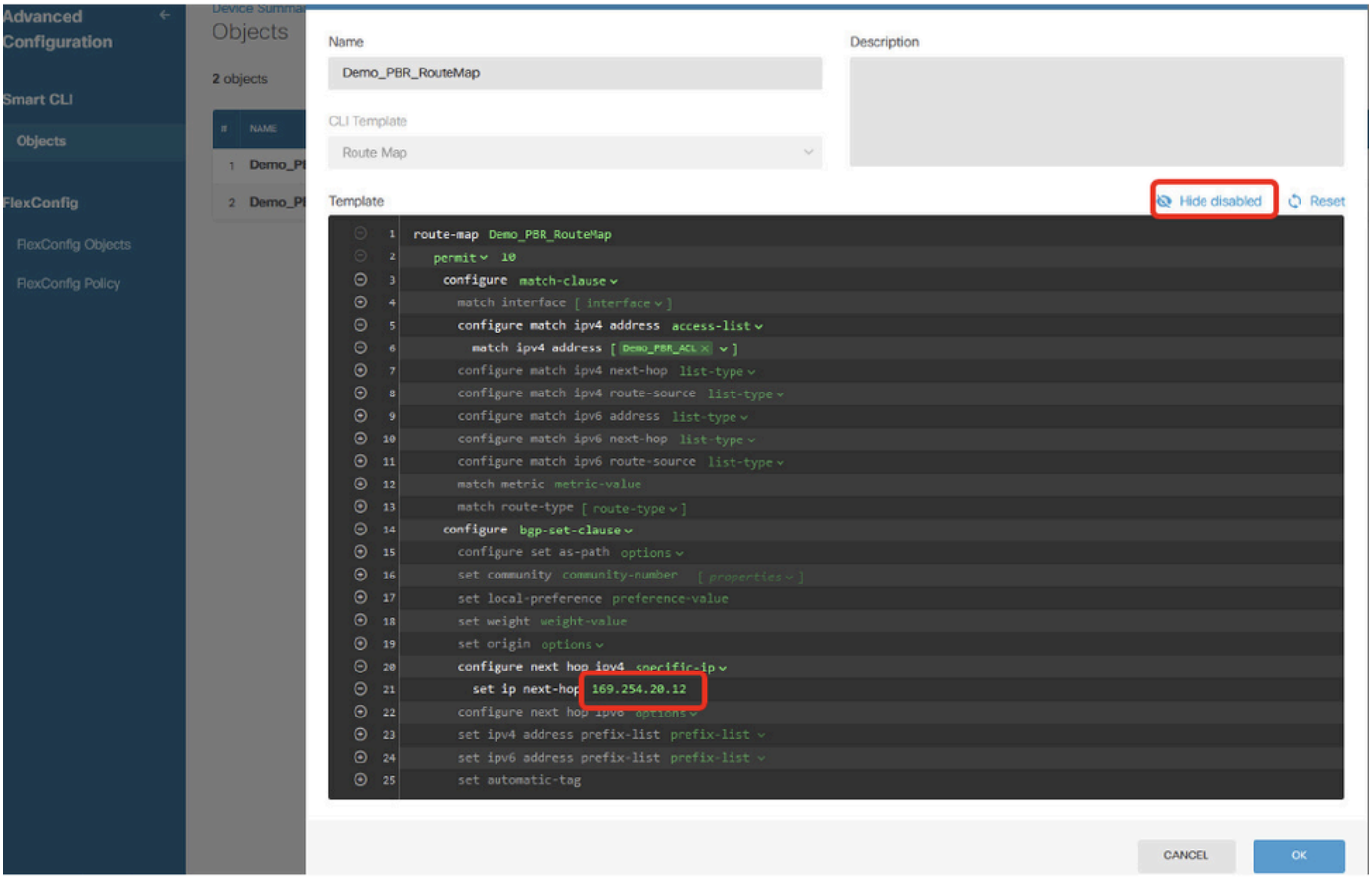
في الأسطر 12 و 13 و 15 و 16 و 17 و 18 و 19 و 21 و 22 و 23 و 24، انقر فوق - زر من أجل التعطيل.

السطر 20، انقر فوق خيارات واختر ip خاص.



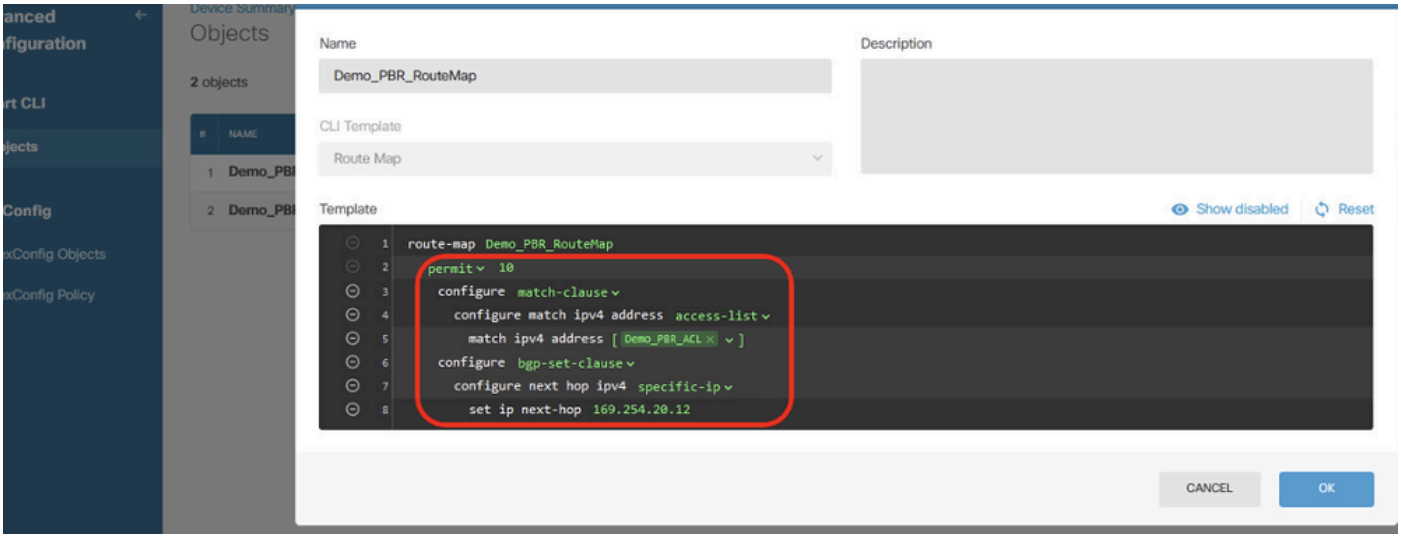
Site1FTD_Create_PBR_RouteMap_8

السطر 21، انقر فوق عنوان IP. عنوان IP للإدخال اليدوي في الخطوة التالية. في هذا المثال، يكون عنوان IP الخاص بموقع النظير 2 نفق VTI ل FTD 2 (169.254.20.12). انقر على إخفاء معطل.



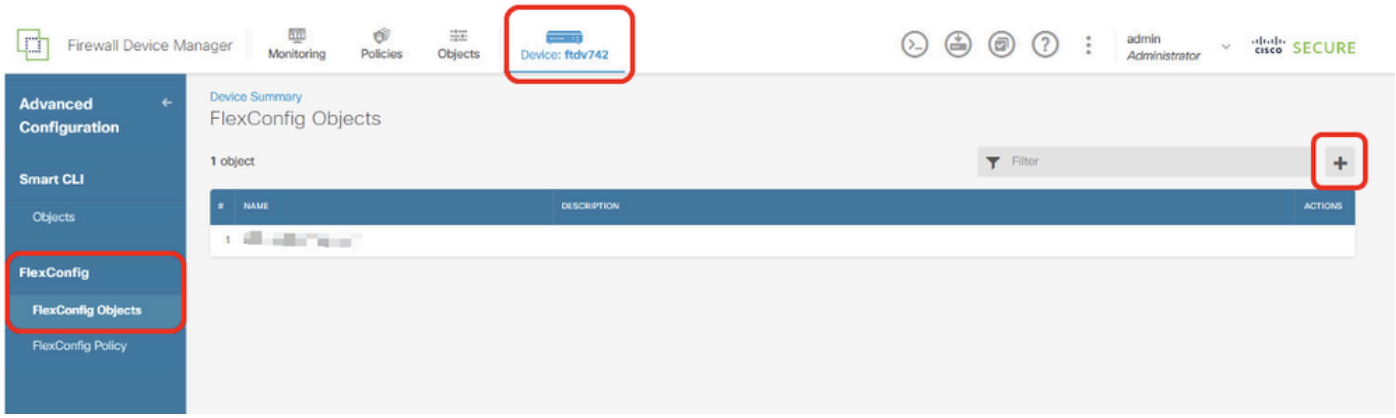
Site1FTD_Create_PBR_RouteMap_9

راجع تكوين خريطة المسار.



Site1FTD_Create_PBR_RouteMap_10

الخطوة 14. قم بإنشاء كائن FlexConfig لـ PBR. انتقل إلى الجهاز > التكوين المتقدم > كائنات FlexConfig وانقر + زر.



Site1FTD_Create_PBR_FlexObj_1

الخطوة 14.1. أدخل اسم للكائن. في هذا المثال، Demo_PBR_FlexObj. في Template وNegative Template Editor، أدخل أسطر الأوامر.

- القالب:

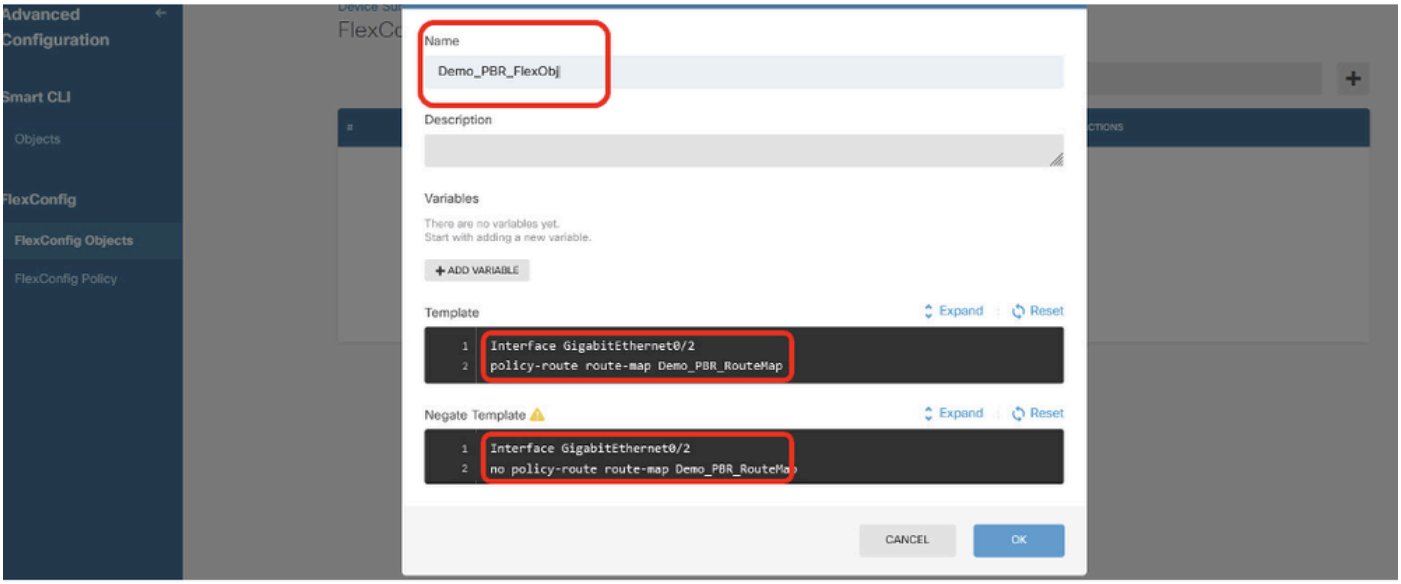
interface GigabitEthernet0/2

policy-route-route-map demo_pbr_routeMap_site2

- قالب غير صالح:

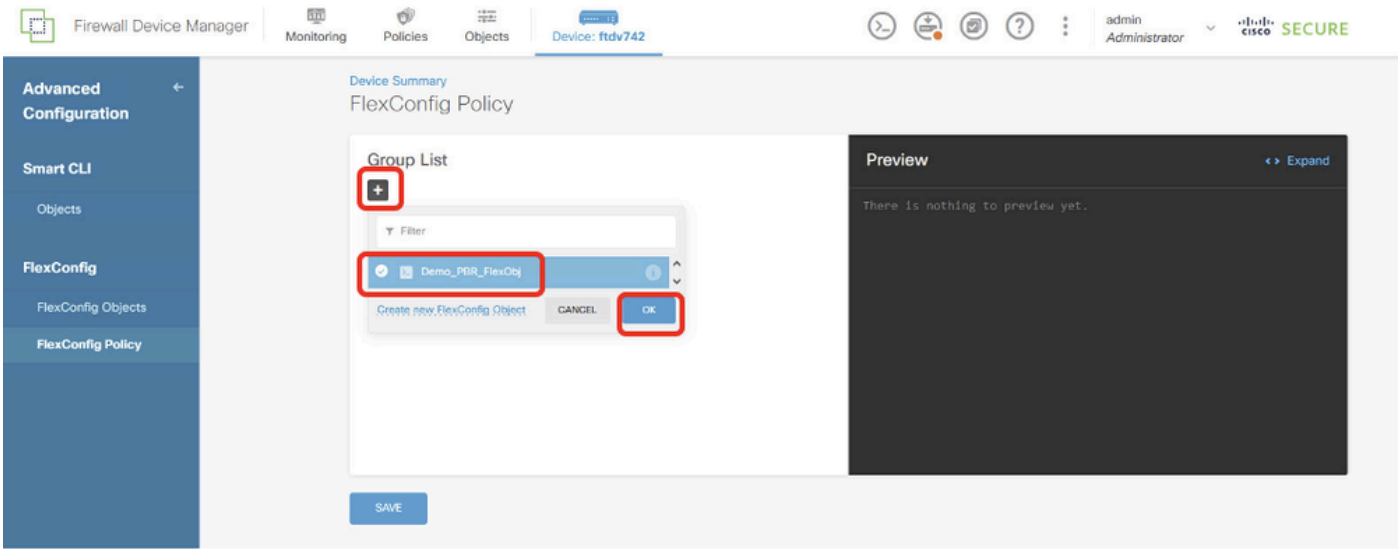
interface GigabitEthernet0/2

ال يوجد Policy-route-map demo_PBR_RouteMap_Site2



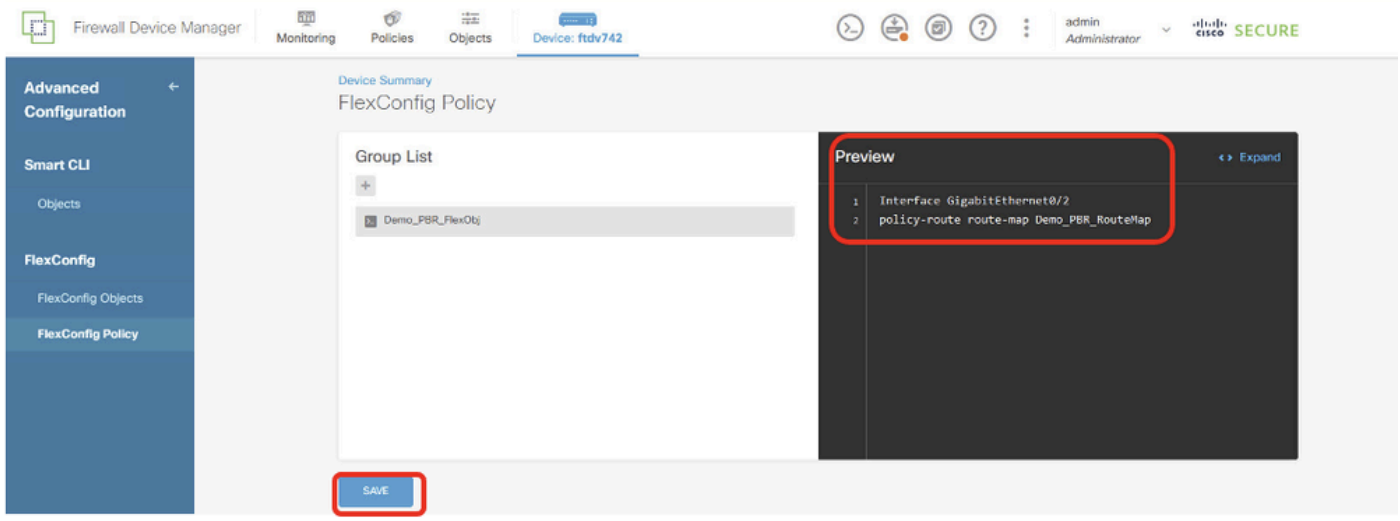
Site1FTD_Create_PBR_FlexObj_2

الخطوة 15. قم بإنشاء سياسة FlexConfig ل PBR. انتقل إلى جهاز > تكوين متقدم > سياسة FlexConfig. انقر فوق + زر. أختر اسم كائن FlexConfig الذي تم إنشاؤه في الخطوة 14. انقر فوق الزر موافق.



Site1FTD_Create_PBR_FlexPolicy_1

الخطوة 15.1. تحقق من الأمر في نافذة المعاينة. إذا كان جيدا، انقر فوق حفظ.



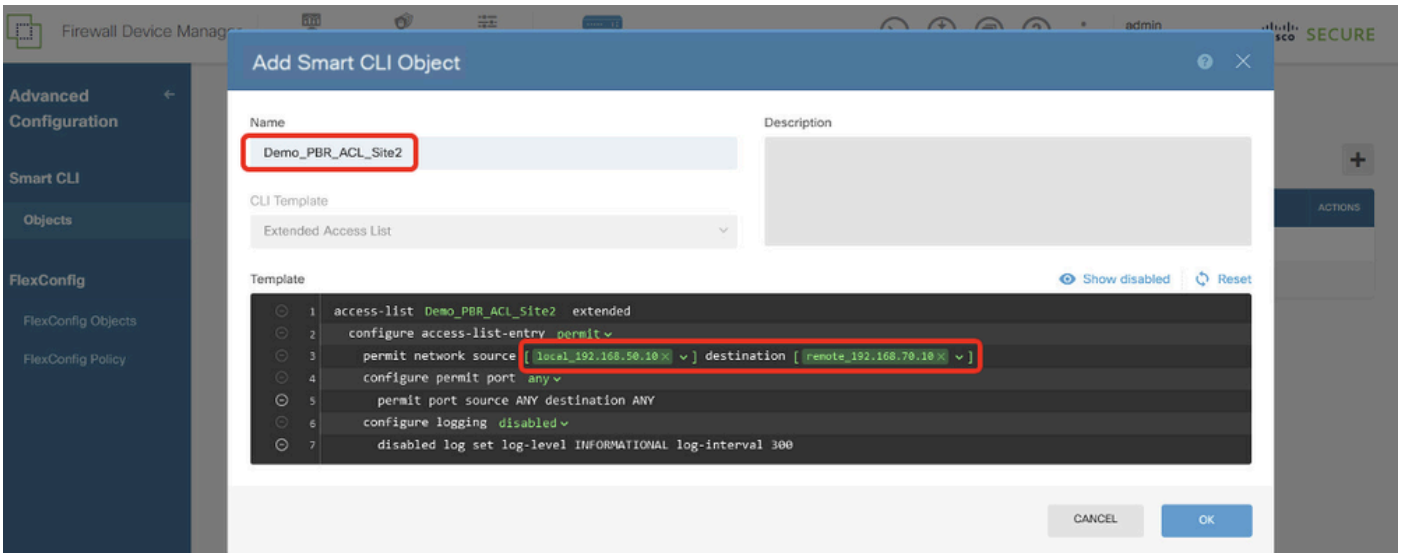
Site1FTD_Create_PBR_FlexPolicy_2

الخطوة 16. نشر تغييرات التكوين.

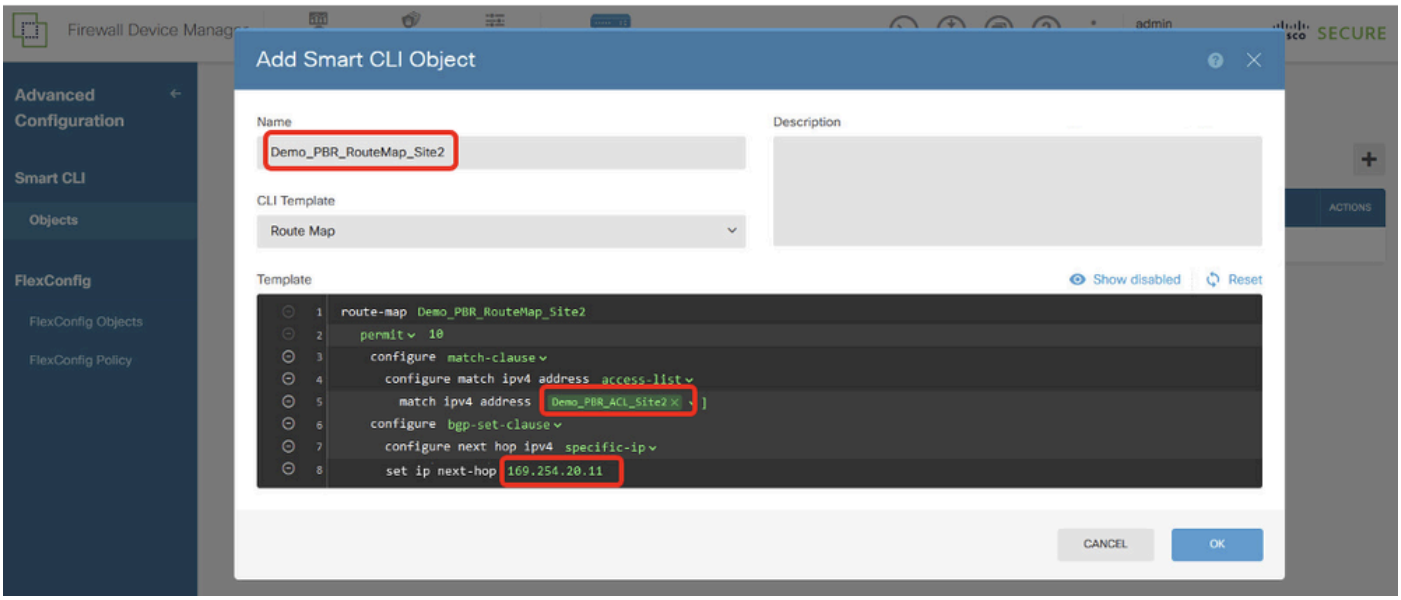
site1FTD_DEPLOYMENT_CHANGES

تكوين PBR الخاص ب Site2 FTD

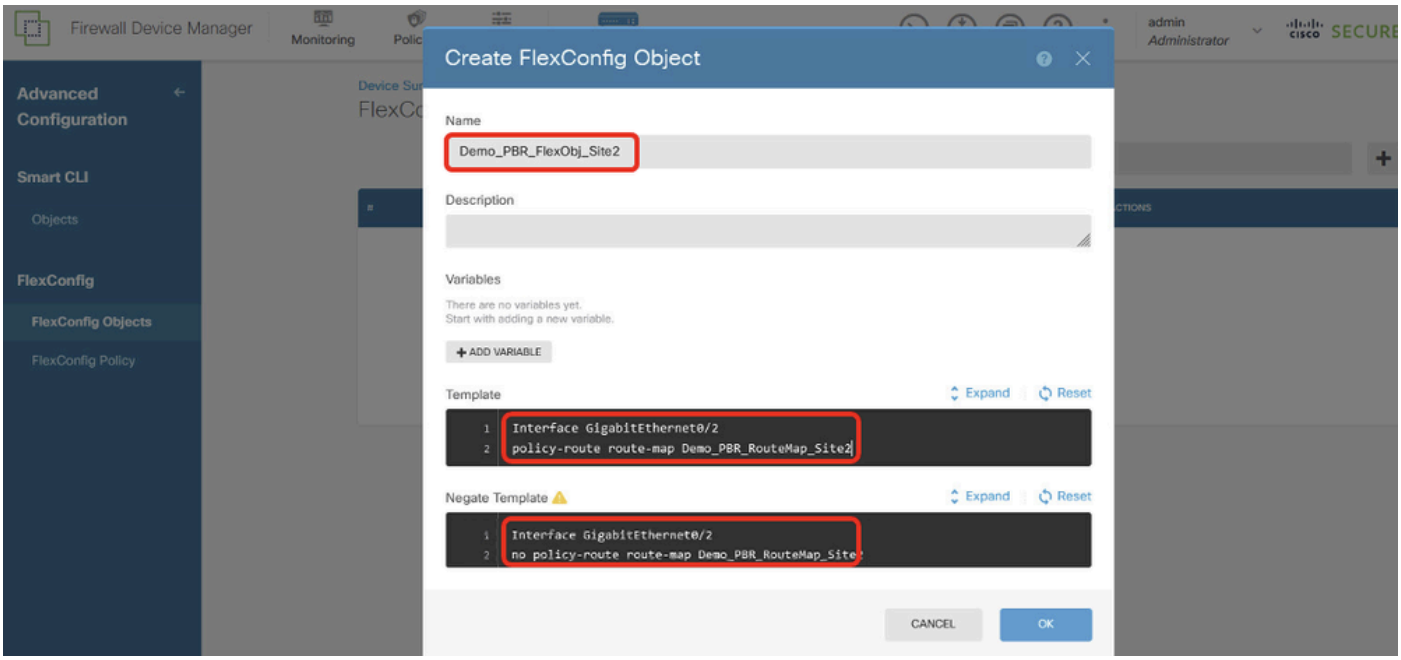
الخطوة 17. كرر الخطوة 11. إلى الخطوة 16. من أجل إنشاء PBR باستخدام المعلمات المقابلة للموقع 2 FTD.



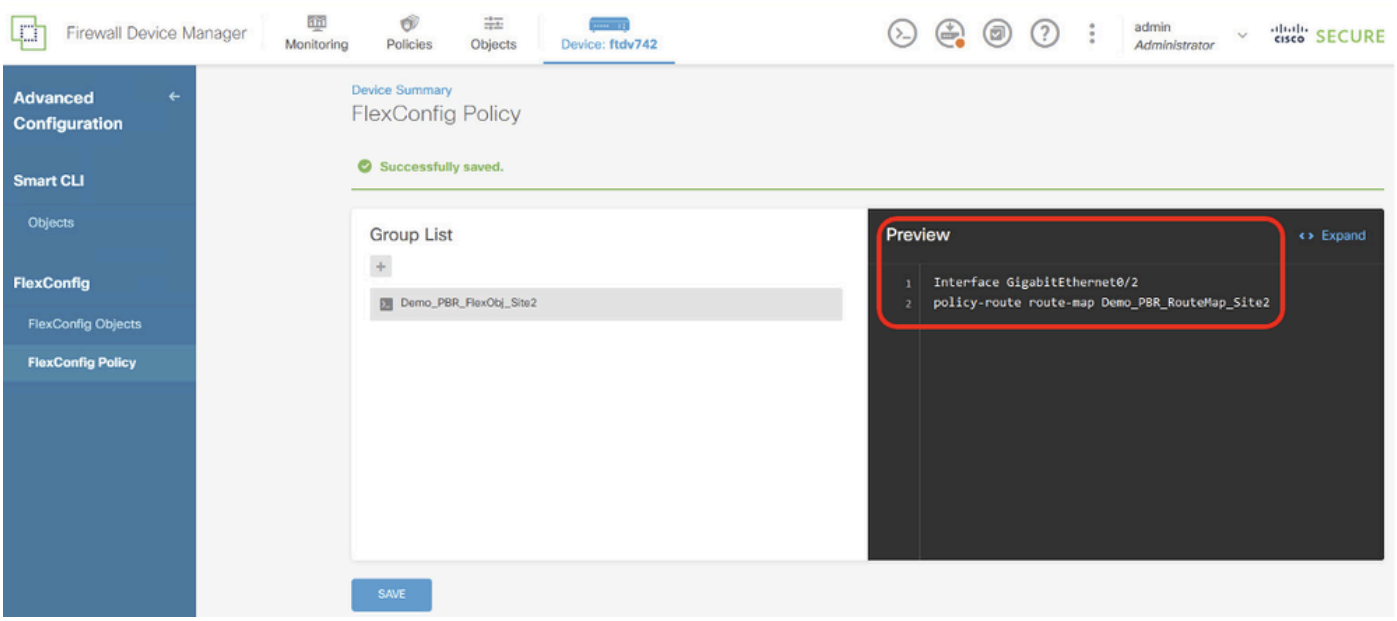
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

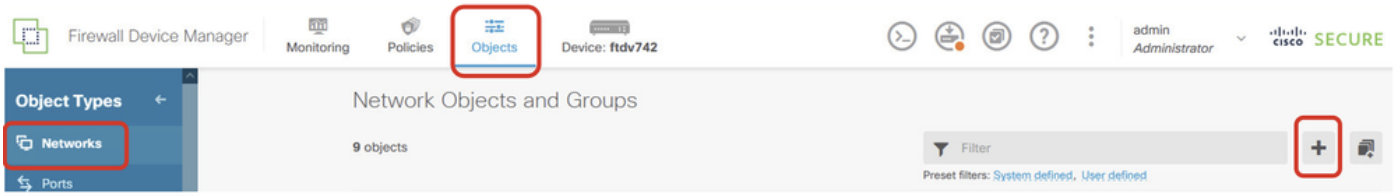


Site2FTD_Create_PBR_FlexPolicy

عمليات التهيئة على شاشة SLA

تكوين مراقبة SLA لـ SITE1 FTD

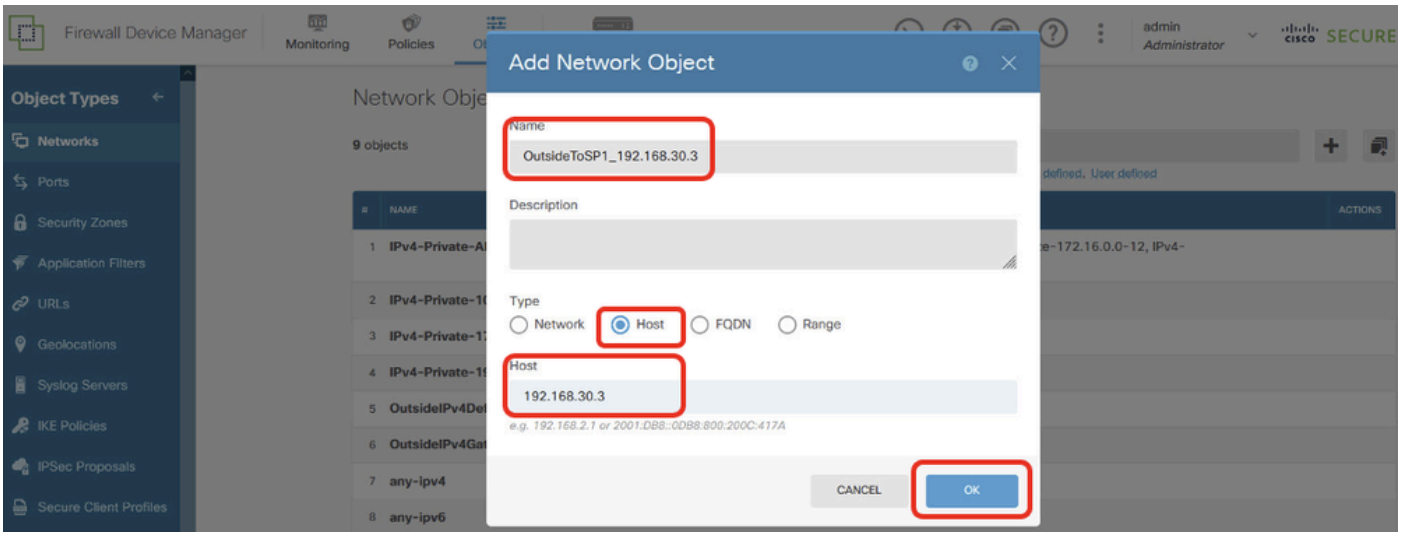
الخطوة 18. قم بإنشاء كائنات شبكة جديدة ليتم إستخدامها من قبل شاشات SLA للموقع 1 FTD. انتقل إلى كائنات > شبكات، انقر فوق + زر.



site1FTD_CREATE_NETWORK_OBJECT

الخطوة 18.1. قم بإنشاء كائن لعنوان IP لبوابة ISP1. قم بتوفير المعلومات اللازمة. طقطقت ok زر.

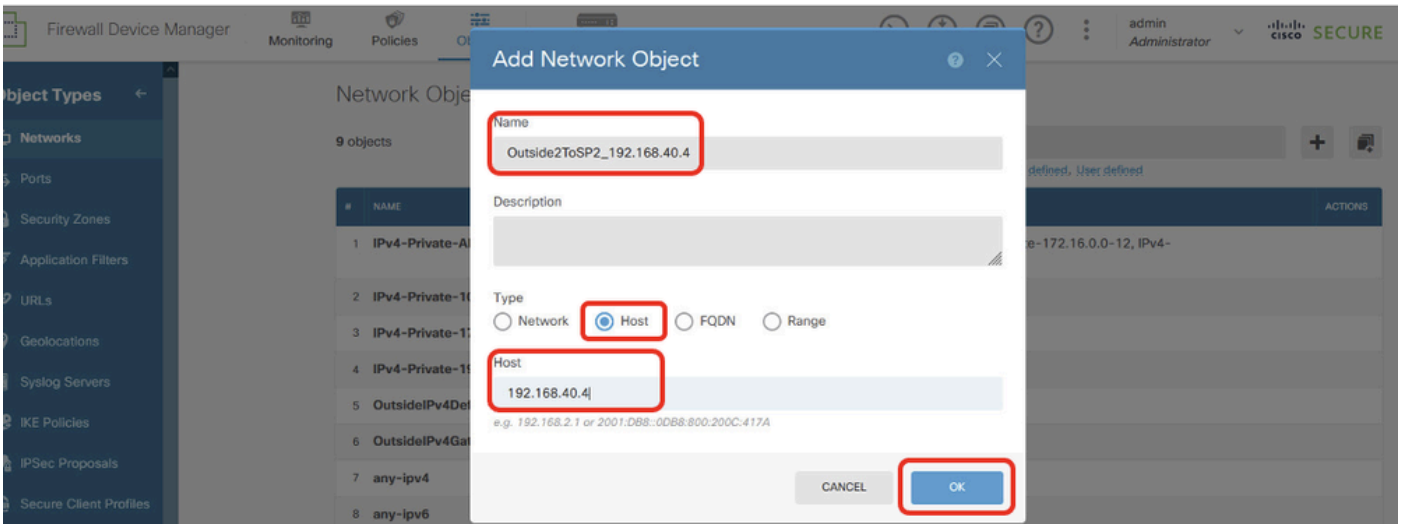
- الاسم: OutsideToSP1_192.168.30.3
- النوع: مضيف
- المضيف: 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

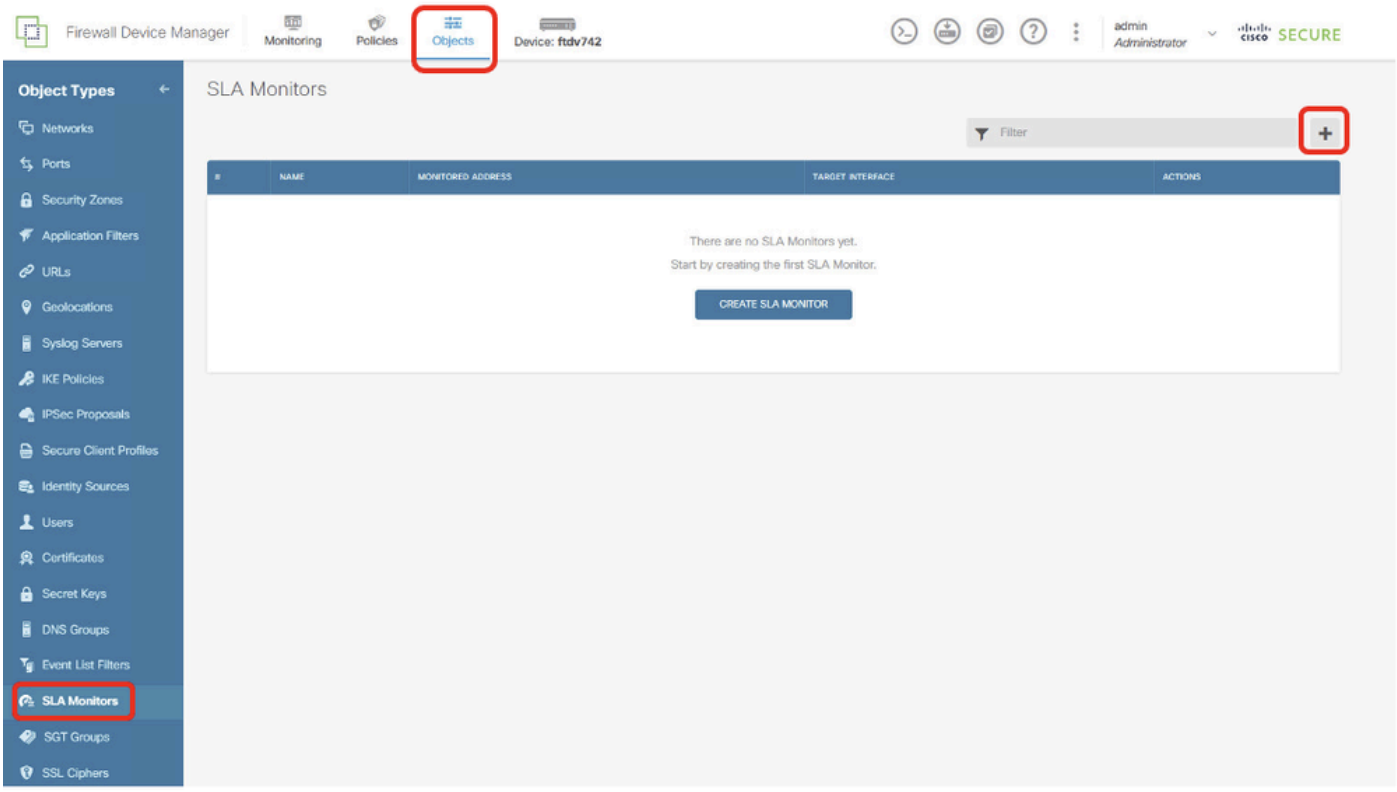
الخطوة 18.2. قم بإنشاء كائن لعنوان IP لبوابة ISP2. قم بتوفير المعلومات الضرورية. طقطقت ok زر.

- الاسم: Outside2ToSP2_192.168.40.4
- النوع: مضيف
- المضيف: 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

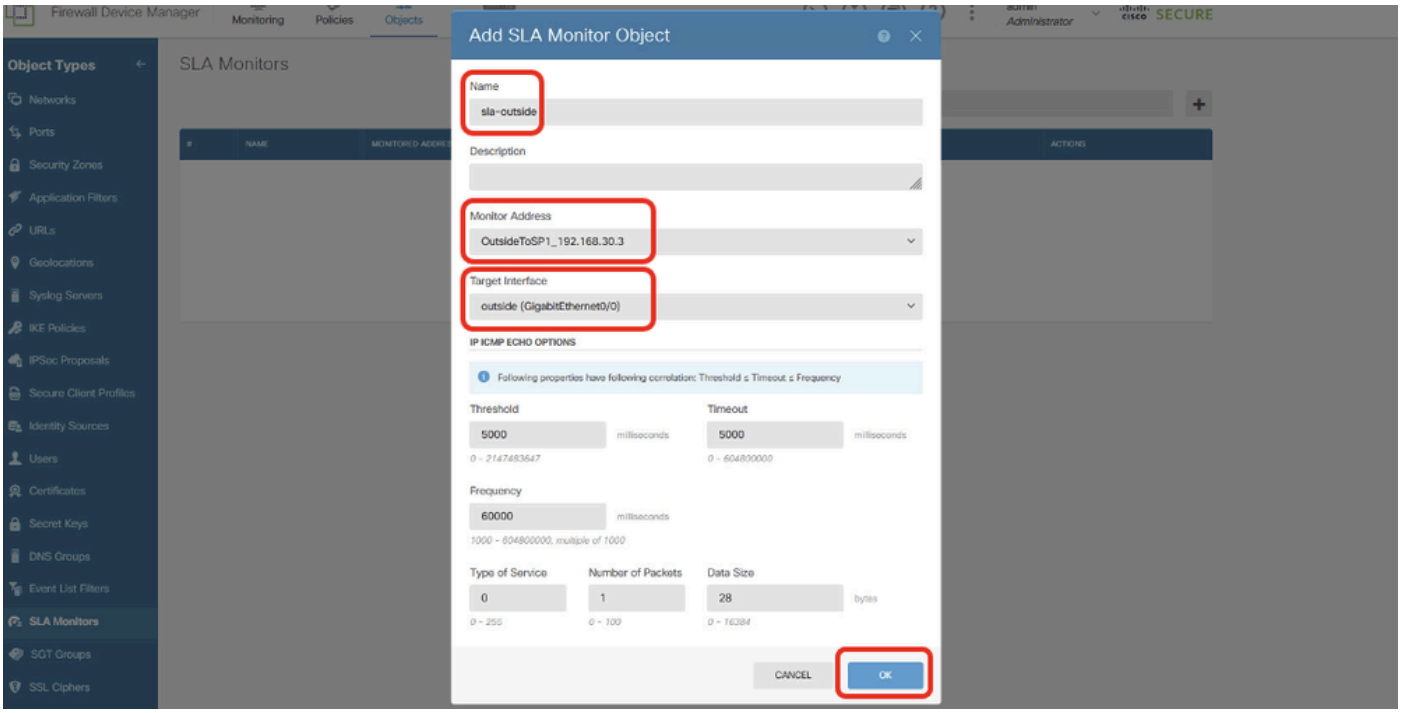
الخطوة 19. إنشاء شاشة SLA. انتقل إلى كائنات > أنواع كائن > شاشات SLA. انقر فوق + زر لإنشاء شاشة SLA جديدة.



Site1FTD_Create_SLAMonitor

الخطوة 19.1. في نافذة إضافة كائن مراقبة SLA، قم بتوفير المعلومات اللازمة لبوابة ISP1. انقر فوق الزر موافق" للحفظ.

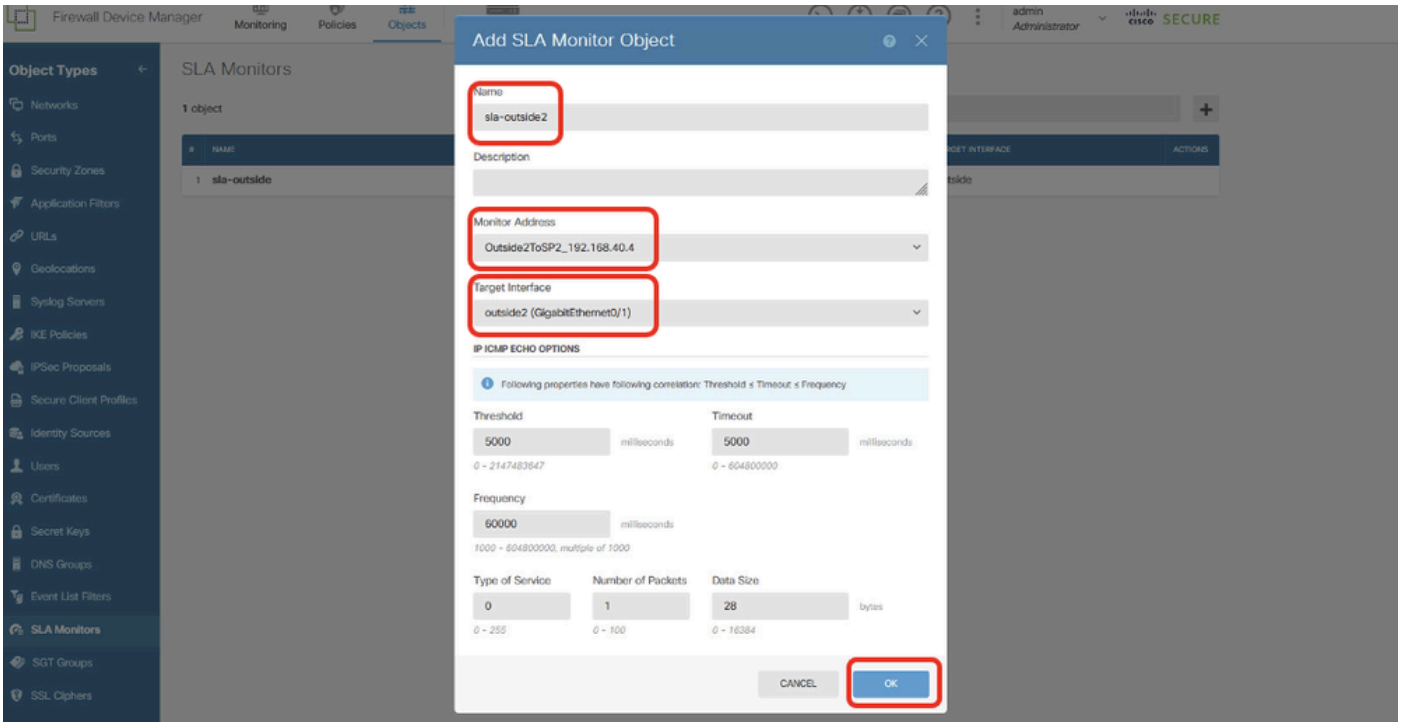
- الاسم: إتفاقية مستوى الخدمة (SLA) الخارجية
- عنوان الشاشة: OutsideToSP1_192.168.30.3
- الواجهة الهدف: خارج (GigabitEthernet0/0)
- خيارات صدى ICMP ل IP: افتراضي



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

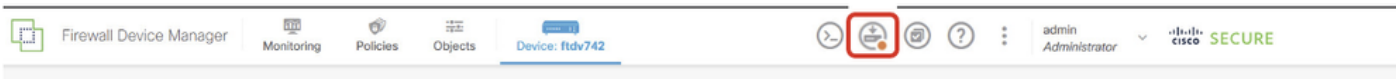
الخطوة 19.2. استمر في النقر فوق + زر لإنشاء شاشة SLA جديدة لبوابة ISP2. في نافذة إضافة كائن مراقبة SLA، قم بتوفير المعلومات الضرورية لبوابة ISP2. انقر فوق الزر موافق" للحفظ.

- الاسم: إتفاقية مستوى الخدمة (SLA) الخارجية2
- عنوان الشاشة: Outside2ToSP2_192.168.40.4
- الواجهة الهدف: خارج2(GigabitEthernet0/1)
- خيارات صدى ICMP ل IP: افتراضي



Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

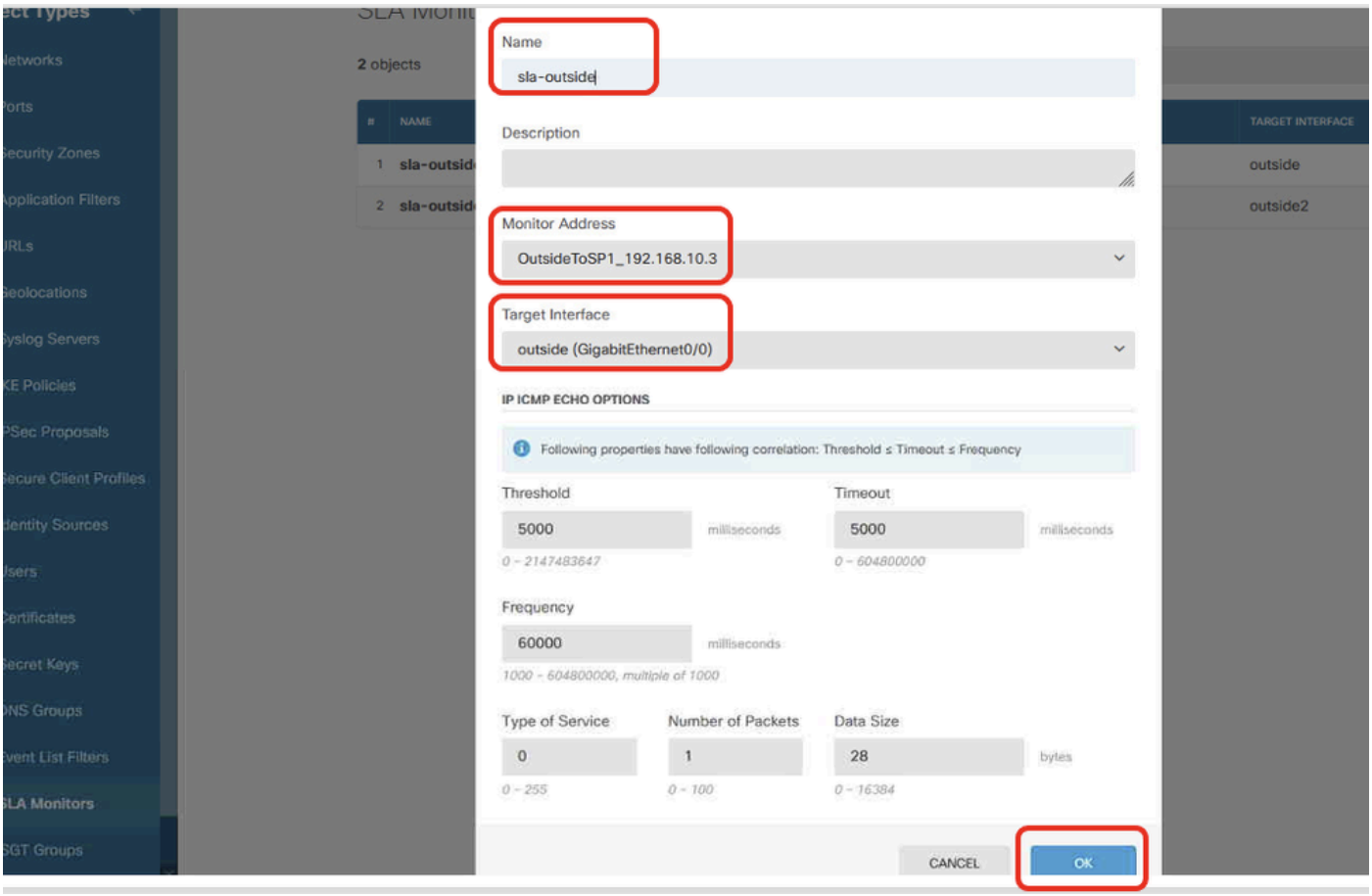
الخطوة 20. نشر تغييرات التكوين.



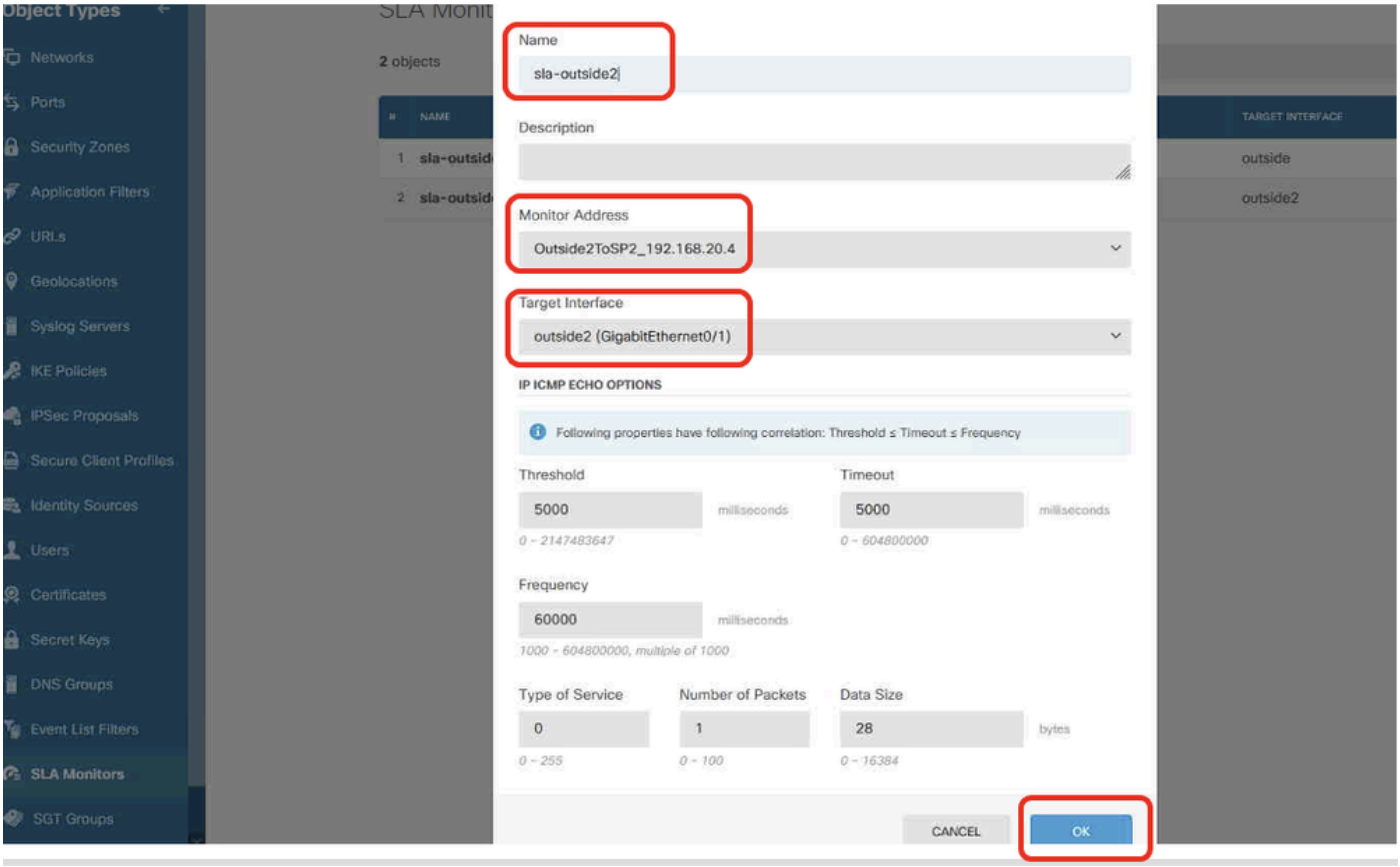
site1FTD_DEPLOYMENT_CHANGES

تكوين مراقبة SLA ل SITE2 FTD

الخطوة 21. كرر الخطوة 18. إلى الخطوة 20. قم بإنشاء مراقبة SLA مع المعلمات المقابلة على Site2 FTD.



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

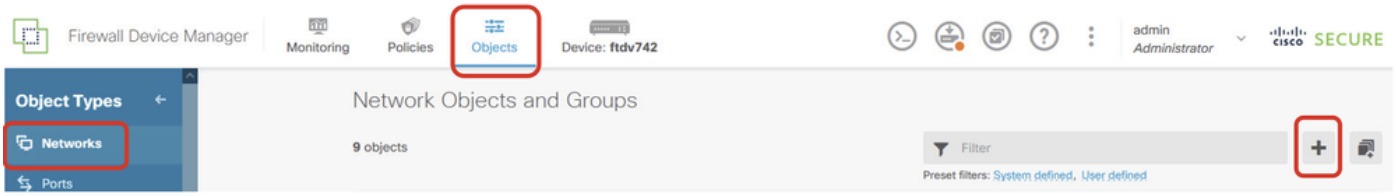


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

التكوينات على المسار الثابت

تكوين المسار الثابت لـ SITE1 FTD

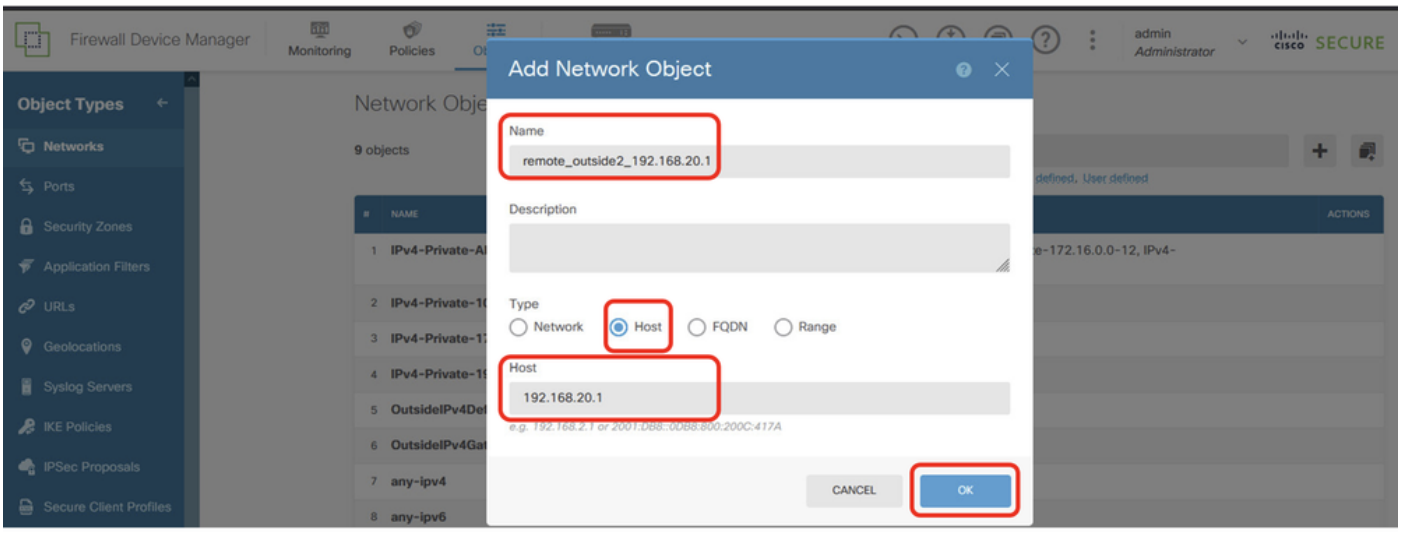
الخطوة 22. قم بإنشاء كائنات شبكة جديدة ليتم إستخدامها من قبل المسار الثابت لـ Site1 FTD. انتقل إلى الكائنات > الشبكات، انقر فوق + زر.



Site1FTD_Create_Obj

الخطوة 22.1. قم بإنشاء كائن لعنوان IP الخارجي2 لموقع النظير 2 FTD. قم بتوفير المعلومات الضرورية. طقطقت ok زر.

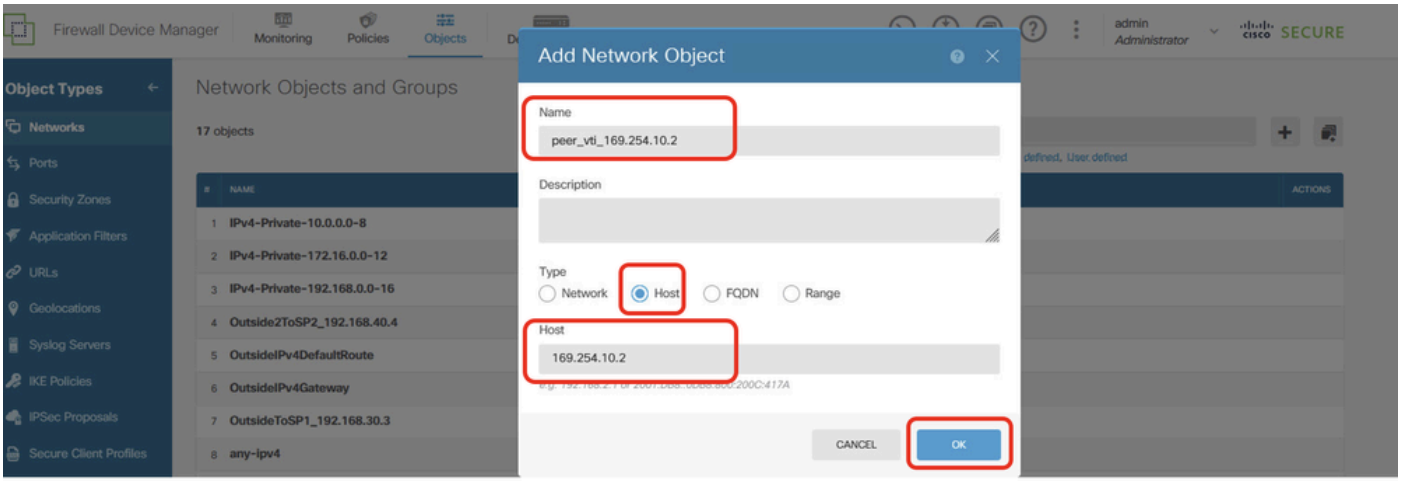
- الاسم: remote_outside2_192.168.20.1
- النوع: مضيف
- الشبكة: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

الخطوة 22.2. قم بإنشاء كائن لعنوان IP الخاص ب VTI Tunnel1 لموقع النظير 2 FTD. قم بتوفير المعلومات اللازمة. طقطقت ok زر.

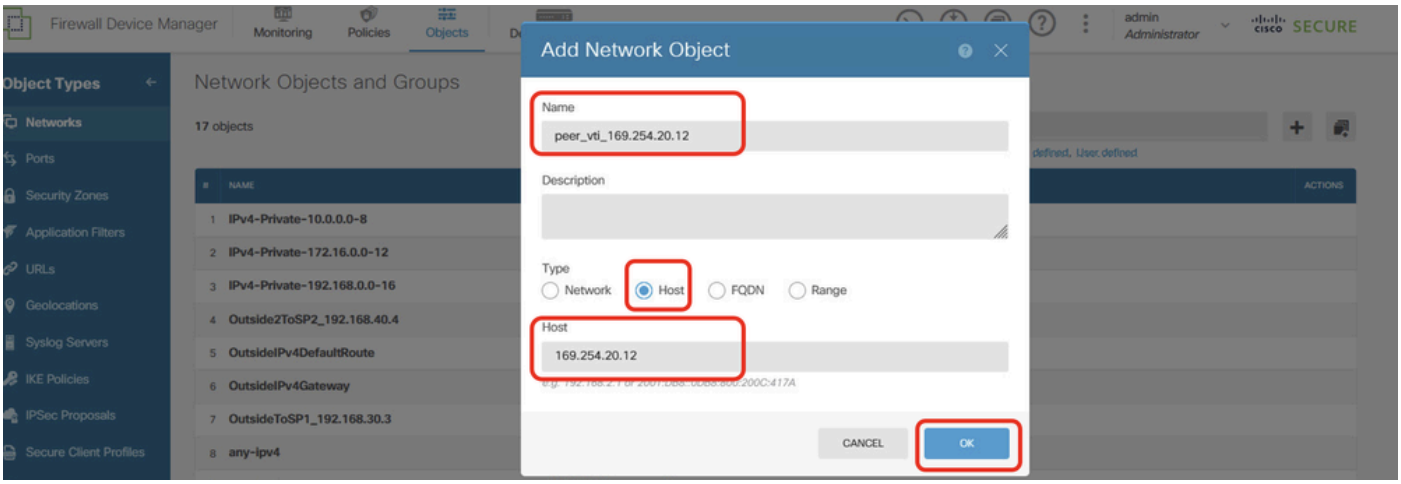
- الاسم: peer_vti_169.254.10.2
- النوع: مضيف
- الشبكة:169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

الخطوة 22.3. قم بإنشاء كائن لعنوان IP ل VTI Tunnel2 الخاص بموقع النظير 2 FTD. قم بتوفير المعلومات اللازمة. طقطقت ok زر.

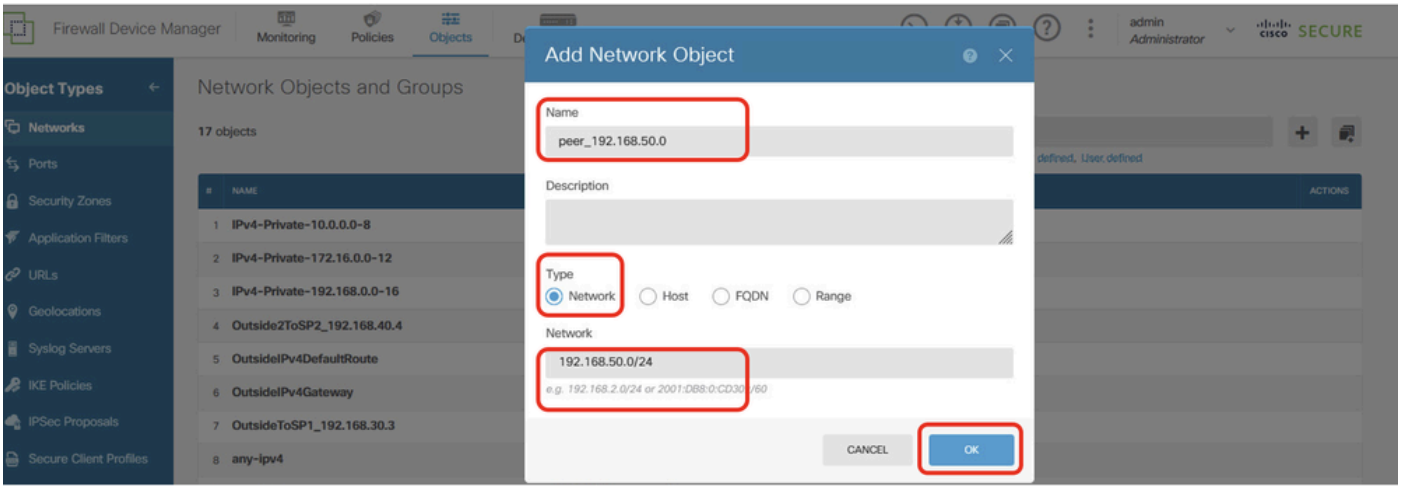
- الاسم: peer_vti_169.254.20.12
- النوع: مضيف
- الشبكة:169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

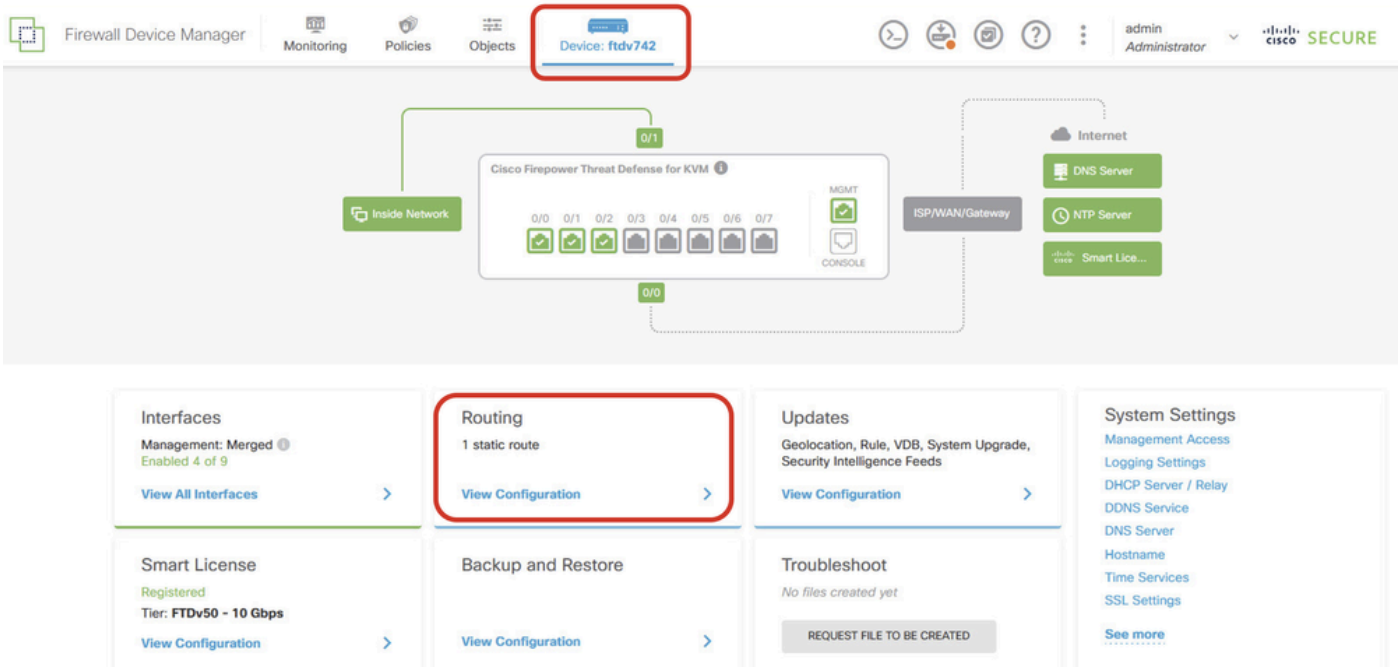
الخطوة 22.4. قم بإنشاء كائن للشبكة الداخلية ل Peer Site2 FTD. قم بتوفير المعلومات الضرورية. طقطقت ok زر.

- الاسم: peer_192.168.50.0
- النوع: الشبكة
- الشبكة:192.168.50.0/24

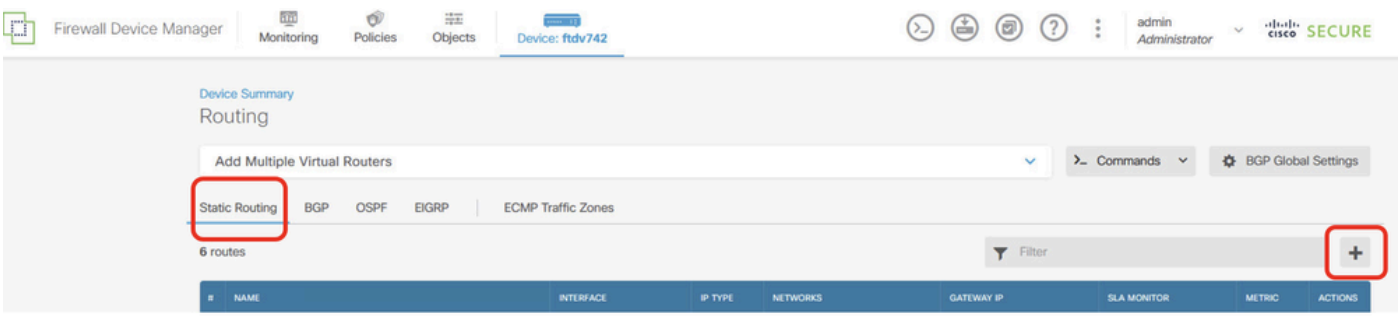


Site1FTD_Create_NetObj_StaticRoute_4

الخطوة 23. انتقل إلى جهاز > توجيه. طقطقة عرض تشكيل. انقر على علامة تبويب توجيه ساكن إستاتيكي. انقر فوق + زر لإضافة مسار ثابت جديد.



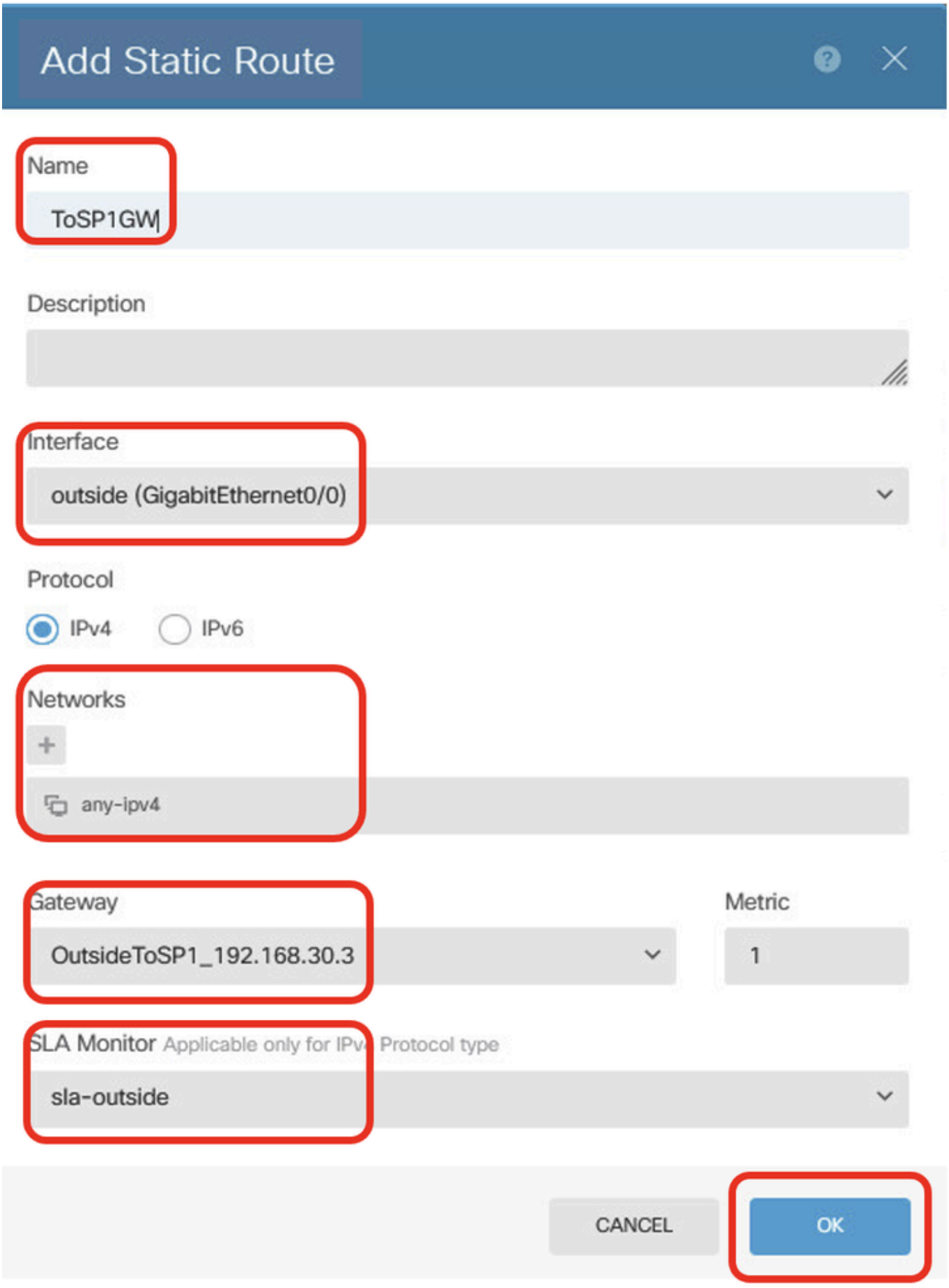
site1FTD_VIEW_ROUTE_CONFIGURATION



Site1FTD_Add_STATIC_Route

الخطوة 23.1. قم بإنشاء مسار افتراضي باستخدام بوابة ISP1 مع مراقبة SLA. إذا تعرضت بوابة ISP1 إلى مقاطعة، فستقوم محولات حركة مرور البيانات إلى المسار الافتراضي للنسخ الاحتياطي عبر ISP2. بمجرد إستئناف ISP1، ترجع حركة مرور البيانات إلى إستخدام ISP1. قم بتوفير المعلومات اللازمة. انقر فوق الزر موافق" للحفظ.

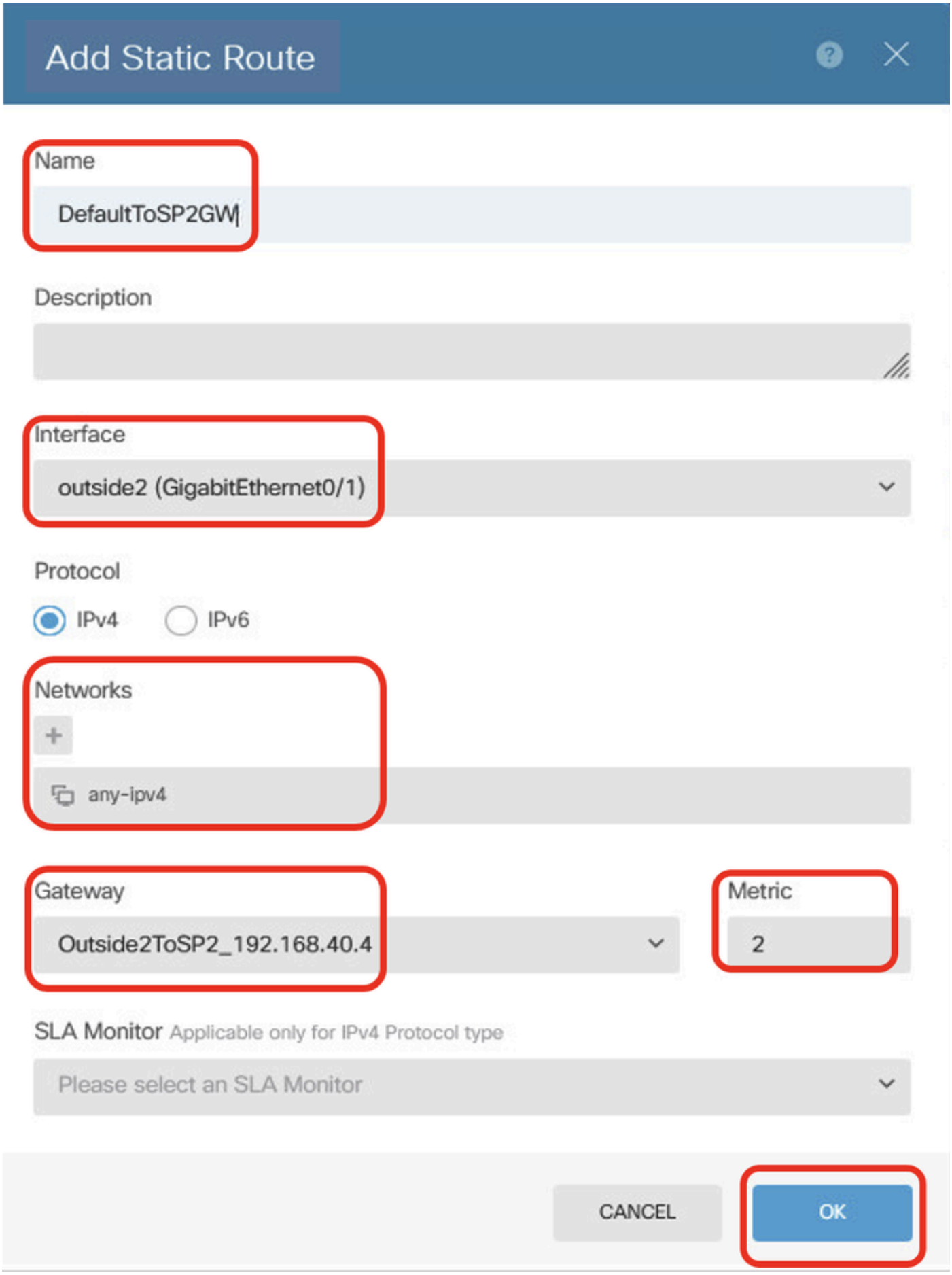
- الاسم: ToSP1GW
- الواجهة: خارج (GigabitEthernet0/0)
- البروتوكول: IPv4
- الشبكات: أي-IPv4
- البوابة: OutsideToSP1_192.168.30.3
- القياس: 1
- شاشة SLA: إتفاقية مستوى الخدمة (SLA) الخارجية



Site1FTD_Create_StaticRoute_1

الخطوة 23.2. إنشاء مسار النسخ الاحتياطي الافتراضي عبر بوابة ISP2. يجب أن يكون المقياس أعلى من 1. في هذا المثال، المقياس هو 2. قم بتوفير المعلومات الضرورية. انقر فوق الزر "موافق" للحفظ.

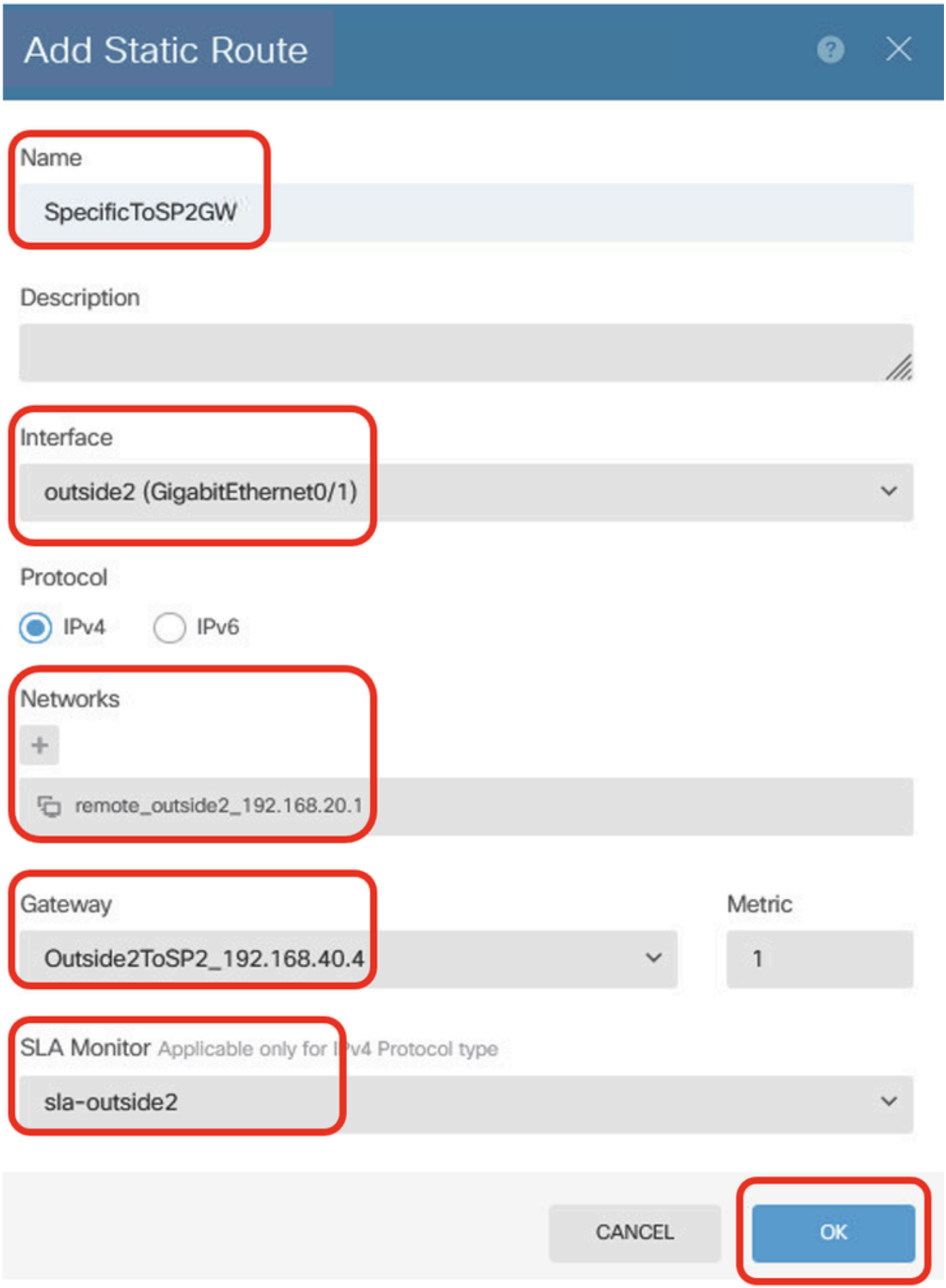
- الاسم: DefaultToSP2GW
- الواجهة: خارج2(GigabitEthernet0/1)
- البروتوكول: IPv4
- الشبكات: أي-IPv4
- البوابة: Outside2ToSP2_192.168.40.4
- القياس: 2



Site1FTD_Create_StaticRoute_2

الخطوة 23.3. قم بإنشاء مسار ثابت لحركة مرور الوجهة إلى خارج 2 عنوان IP الخاص بموقع الظير 2 FTD عبر بوابة ISP2، مع مراقبة SLA، المستخدمة لإنشاء VPN مع خارج 2 من Site2 FTD. قم بتوفير المعلومات الضرورية. انقر فوق الزر موافق" للحفظ.

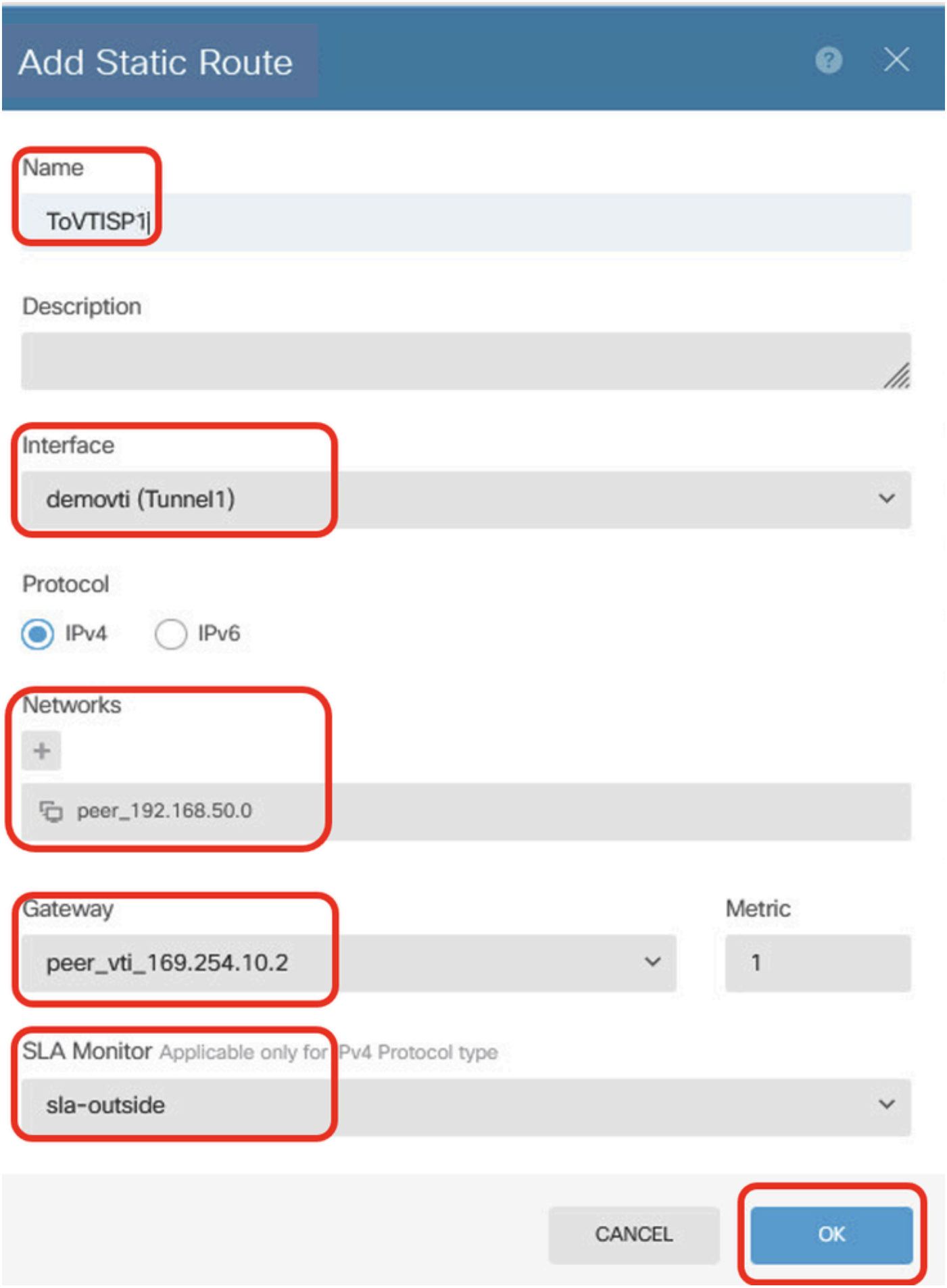
- الاسم: SpecificToSP2GW
- الواجهة: خارج2(GigabitEthernet0/1)
- البروتوكول: IPv4
- الشبكات: remote_outside2_192.168.20.1
- البوابة: Outside2ToSP2_192.168.40.4
- القياس: 1
- شاشة SLA: إتفاقية مستوى الخدمة (SLA) الخارجية2



Site1FTD_Create_StaticRoute_3

الخطوة 23.4. قم بإنشاء مسار ثابت لحركة مرور الوجهة إلى الشبكة الداخلية لموقع النظير 2 FTD عبر النفق النظير VTI 1 من SITE2 FTD كبوابة، مع مراقبة SLA لتشفير حركة مرور VPN إلى العميل عبر النفق 1. إذا واجهت بوابة ISP1 مقاطعة، فستواجه حركة مرور البيانات إلى نفق VTI 1 من ISP1. قم بترجع حركة مرور البيانات إلى ISP1، بمجرد إستدادا ISP2. من 2 قم بتوفير المعلومات اللازمة. انقر فوق الزر موافق" للحفظ.

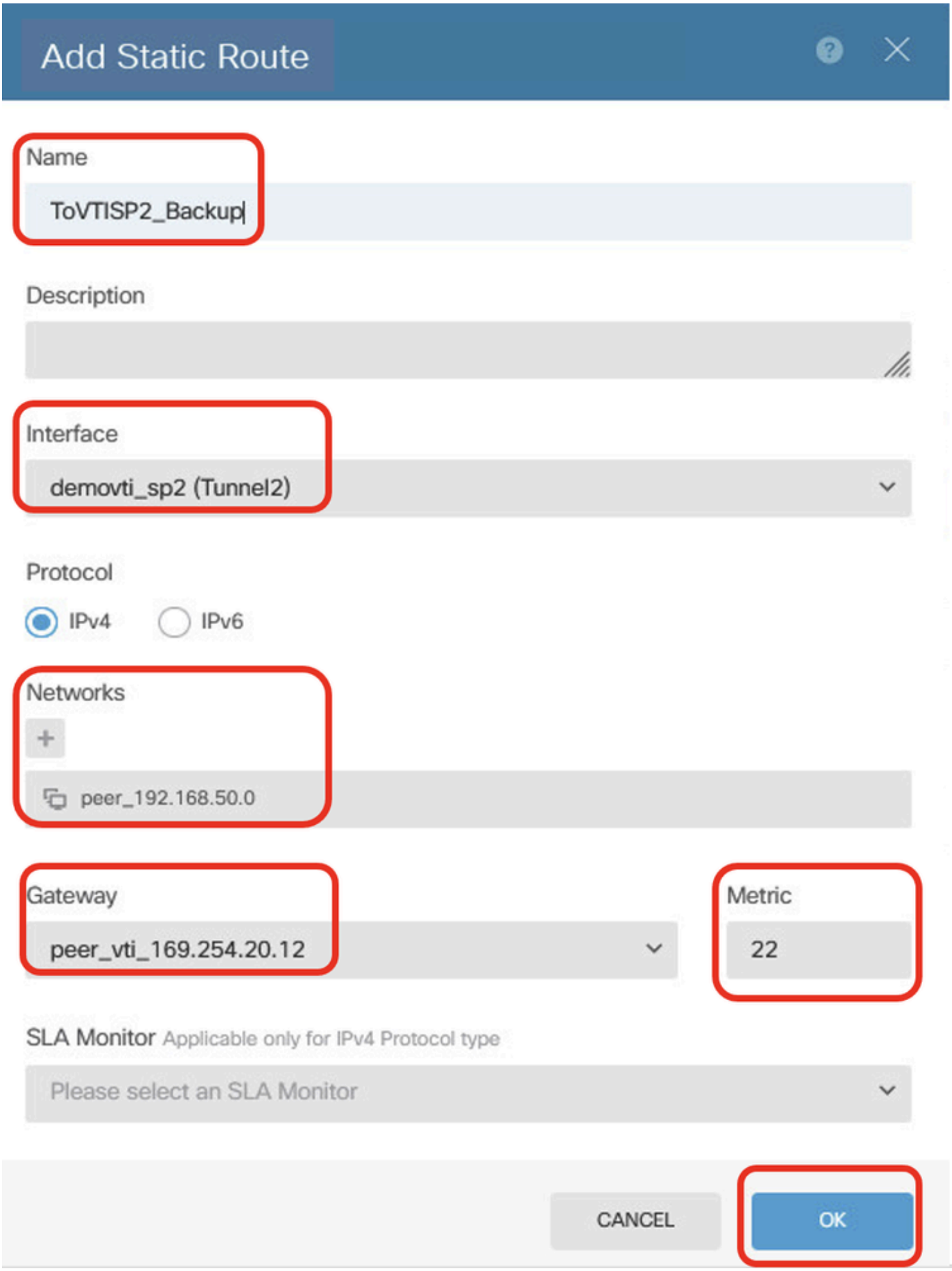
- الاسم: ToVTISP1
- الواجهة: demovti(Tunnel1)
- البروتوكول: IPv4
- الشبكات: peer_192.168.50.0
- البوابة: peer_vti_169.254.10.2
- القياس: 1
- شاشة SLA: إتفاقية مستوى الخدمة (SLA) الخارجية



Site1FTD_Create_StaticRoute_4

الخطوة 23.5. قم بإنشاء مسار ثابت للنسخ الاحتياطي لحركة مرور الوجهة إلى الشبكة الداخلية لموقع النظير 2 FTD عبر نفق VTI النظير 2 للموقع 2 FTD كبوابة، تستخدم في الخطوة 1 من أعلى قيمة أعلى لتشفير حركة مرور العميل عبر النفق 2. قم بتعيين المقياس إلى قيمة أعلى من 22 وهو المقياس الذي تريد استخدامه لهذا المسار الثابت. انقر فوق الزر موافق" للحفظ.

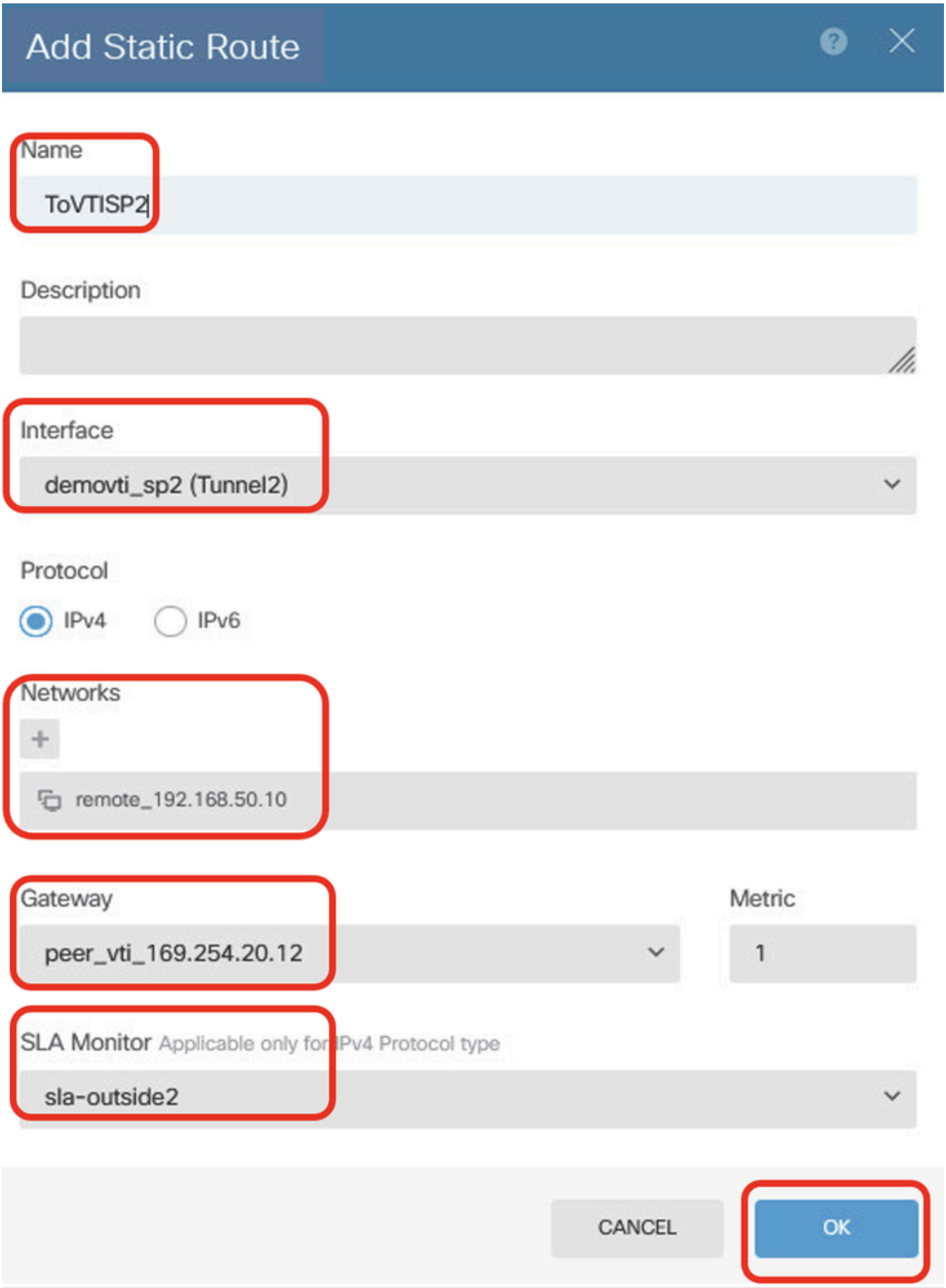
- الاسم: ToVTISP2_Backup
- الواجهة: demovti_sp2(Tunnel2)
- البروتوكول: IPv4
- الشبكات: peer_192.168.50.0
- البوابة: peer_vti_169.254.20.12
- القياس: 22



Site1FTD_Create_StaticRoute_5

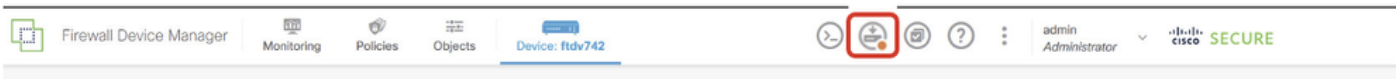
الخطوة 23.6. قم بإنشاء مسار ثابت لحركة مرور PBR. حركة مرور الوجهة إلى Site2 Client2 عبر Peer VTI Tunnel 2 لـ Site2 FTD كبوابة، مع مراقبة SLA. توفير المعلومات الضرورية. انقر فوق الزر موافق" للحفظ.

- الاسم: ToVTISP2
- الواجهة: demovti_sp2(Tunnel2)
- البروتوكول: IPv4
- الشبكات: remote_192.168.50.10
- البوابة: peer_vti_169.254.20.12
- القياس: 1
- شاشة SLA: إتفاقية مستوى الخدمة (SLA) الخارجية2



Site1FTD_Create_StaticRoute_6

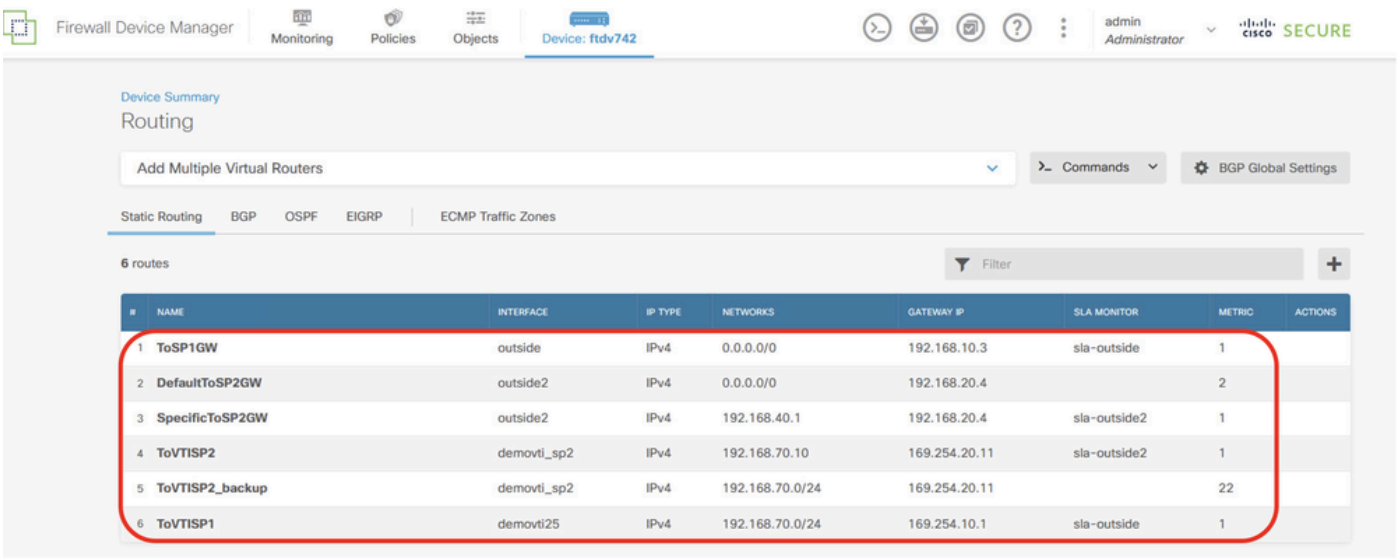
الخطوة 24. قم بنشر تغييرات التكوين.



site1FTD_DEPLOYMENT_CHANGES

تكوين المسار الثابت ل SITE2 FTD

الخطوة 25. كرر الخطوات من 22 إلى 24 من أجل إنشاء مسار ثابت باستخدام المعلمات المقابلة ل Site2 FTD.



Site2FTD_Create_StaticRoute

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح. انتقل إلى واجهة سطر الأوامر (CLI) الخاصة ب Site1 FTD و Site2 FTD عبر وحدة التحكم أو SSH.

كل من ISP1 و ISP2 يعمل بشكل جيد

VPN

```
//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
1072332533 192.168.30.1/500                              192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44895 sec
```

```
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
1045734377 192.168.40.1/500                                192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77860 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
499259237 192.168.10.1/500                                192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44985 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
477599833 192.168.20.1/500                                192.168.40.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77950 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x82e8781d/0x47bfa607
```

طريق

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

ةشاش SLA

```
// Site1 FTD:
```

```
ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:


ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

```
Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

// Site2 FTD:

```
ftdv742#  show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
```

```
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100

Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

إختبار بينغ

السيناريو 1. Site1 Client1 ping Site2 Client1.

قبل إختبار الاتصال، تحقق من عدادات show crypto ipSec | واجهة inc:|encap|decap على Site1 FTD.

في هذا المثال، يعرض النفق1497 حزمة لعملية التضمين و 1498 حزمة لعزل الكبسلة.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
      #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
```

```
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 بنجاح.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

تحقق من عدادات show crypto ipSec sa | واجهة inc:|encap|decap على Site1 FTD بعد إختبار الاتصال بنجاح.

في هذا المثال، يبدي نفق 1502 ربط العملية كبسلة و 1503 ربط القطع كبسلة، مع الكل هوجيه توت إلى أنه تم إزيل العملية 5 لل مثالي، ربط 5 ب زيد قارن. وهذا يشير إلى أن حدى ط بلب. تظهر النفق 2 أي زيادة في إختبارات اتصال Site1 Client1 إلى Site2 Client1 عبر نفق ISP1. ال عدادات التضمين وأ زالة الكبسلة، مم إستخدام حركة المرور هذه.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
      #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

السيناريو 2. Site1 Client2 ping Site2 Client2.

قبل إختبار الاتصال، تحقق من عدادات show crypto ipSec | واجهة inc:|encap|decap على Site1 FTD.

في هذا المثال، يعرض النفق2 21 حزمة العملية التضمين و 20 حزمة لإزالة الكبسلة.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
```

```
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2 Ping Site2 Client2 بنجاح.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/39/87 ms
```

تحقق من عدادات show crypto ipSec sa | واجهة inc:|encap|decap على Site1 FTD بعد إختبار الاتصال بنجاح.

في هذا المثال، يبدي نفق 2 26 رطب لعملية كبسلة و 25 رطب لعزل، مع الك اق ن يزي د ب 5 لا 5 عملية أزيز صدى طلب. وهذا يشير إلى أن إختبارات اتصال Site1 Client2 إلى Site2 Client2 يتم توجيهها عبر نفق ISP2 2. الظهر النفق 1 أية زيادة في عدادات التضمين أو إزالة الكبسلة، مما يؤدي أن هذه الحركة المرور إستخدمه حتى ال.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

جديد نحو على ISP2 لمعل عانأث عطاقم ISP1 جاوي

في هذا المثال، قم بإيقاف التشغيل اليدوي للواجهة E0/1 على ISP1 لمحاكاة ISP1 الذي يواجه مقاطعة.

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
```

```
Internet_SP1(config)#
```

VPN

1. يكون Tunnel2 فقط نشط مع IKEv2 SA. قبل النفق لزن

```
// Site1 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.1, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.30.1
    Destination IP address: 192.168.10.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d


ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
1045734377 192.168.40.1/500                                      192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80266 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x47bfa607/0x82e8781d



// Site2 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.2, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.10.1
    Destination IP address: 192.168.30.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
477599833 192.168.20.1/500                                      192.168.40.1/500
```

```
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80382 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x82e8781d/0x47bfa607
```

طريق

في جدول التوجيه، يتم تفعيل مسارات النسخ الاحتياطي.

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.40.4 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside
```

```
// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
```

```
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

شاشة SLA

في Site1 FTD، تظهر شاشة SLA مهلة الإدخال 855903900 (العنوان الهدف هو 192.168.30.3) لـ ISP1.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000

Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

ftdv742# show track
Track 1
```

```
  Response Time Reporter 855903900 reachability
  Reachability is Down
  7 changes, last change 00:11:03
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Up
  4 changes, last change 13:15:11
  Latest operation return code: OK
  Latest RTT (millisecs) 140
  Tracked by:
    STATIC-IP-ROUTING 0
```

إختبار بينغ

قبل إختبار الاتصال، تحقق من عدادات show crypto ipSec | واجهة inc:|encap|decap على Site1 FTD.

في هذا المثال، يعرض Tunnel2 36 حزمة لعملية التضمين و 35 حزمة لإزالة الكبسلة.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
      #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 بنجاح.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

Site1 Client2 Ping Site2 Client2 بنجاح.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/56/87 ms
```

تحقق نم تادادع show crypto ipSec sa | ةهجاو inc:|encap|decap ىلع Site1 FTD دعب رابتخإ الاتصال حاجنب.

في اذه الاثم، يدبي 2 قفن 46 رطب ةيلمعل ةلسبك و 45 رطب كفل الكبسلة، عم الك نراق رابتخإ مزح هيجوت ىلإ ريشي اذهو .بلط ىدص زيزأ ةيلمع 10 لا لثامي ،رطب 10 ب ديزي الاتصال ربع قفن ISP2 2.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
      #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

هجاوي ISP2 ةعطاقم أثناء لمع ISP1 بشكل جيد

في اذه الاثمل، مق فاقيإب التشغيل اليدوي للةهجاو E0/1 ىلع ISP2 ةاكاحمل ISP2 الذي يجاوه ةعطاقم.

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

لزن النفق 2. نوكي Tunnel1 طشن اقفق عم IKEV2 SA.

```
// Site1 FTD:

ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.40.1
    Destination IP address: 192.168.20.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:
```

```
Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1375077093 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/349 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x40f407b4/0x26598bcc



// Site2 FTD:

ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.12, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.20.1
    Destination IP address: 192.168.40.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1025640731 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/379 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x26598bcc/0x40f407b4
```

طريق

في جدول المسارات، يختفي المسار المرتبط ب ISP2 لحركة مرور PBR.

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0
```

```
S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside
```

```
// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

شاشة SLA

في Site1 FTD، يظهر دمر بـ SLA معلمة الإدخال 188426425 (العنوان الهدف هو 192.168.40.4) ل ISP2.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
```

```
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100


ftdv742#  show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Up
  8 changes, last change 00:14:37
  Latest operation return code: OK
  Latest RTT (millisecs) 60
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Down
  5 changes, last change 00:09:30
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

إختبار بينغ

قبل إختبار الاتصال، تحقق من عدادات show crypto ipSec | واجهة inc:|encap|decap على Site1 FTD.

في هذا المثال، يجب أن تكون هناك 1 74 رطب لعملية كبسلة و 73 رطب لفك الكبسلة.

```
// Site1 FTD:
```

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
      #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 بنجاح.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

Site1 Client2 Ping Site2 Client2 بنجاح.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/58/143 ms
```

تحقق من عدادات show crypto ipSec sa | واجهة inc:|encap|decap على Site1 FTD بعد إختبار الاتصال بنجاح.

في هذا المثال، يدي نفق 1 84 رطب لعملية كبسلة و 83 رطب لعزل، مع الكل قارن يزيد ب 10 رطب، يماثل ال 10 عملية أزيز صدى طلب. وهذا يشير إلى توجيه حزم إختبار الاتصال عبر نفق ISP1 1.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
      #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أنت يستطيع استعملت هذا يضبط أمر in order to تحريت ال VPN قسم.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

أنت يستطيع استعملت هذه يضبط أمر أن يتحرى ال PBR قسم.

```
debug policy-route
```

أنت يستطيع استعملت هذه يضبط أمر أن يتحرى ال SLA مدرب قسم.

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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).