تكوين الوصول الآمن باستخدام FTD و ASA مع NAT الآمن للوصول الخاص باستخدام

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مجموعة نفق شبكة الوصول الآمن باستخدام ترجمة عنوان الشبكة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة جدار الحماية من Cisco
- الدفاع ضد تهديد جدار الحماية الآمن من Cisco
- Cisco Secure Access

- Cisco من فيكتلل ةلباقلا نامألا زهجأ
- ةكبشلا نواعنا ةمجرت
- ةساسألا ىلع مئاقلا هيجوتلا
- ةيامحلا رادج ىلع ةمزحلا طاقتلا

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى:

- Cisco من 7.10 ةرادإ زكرم رادج ةيامحلا
- Cisco من 7.10 نآلما ةيامحلا رادج هدهت ضد عافدلا جمانرب
- Cisco Secure Access
- Cisco من 9.22 فيكتلل لباقلا نامألا زاهج
- Cisco هاجوم

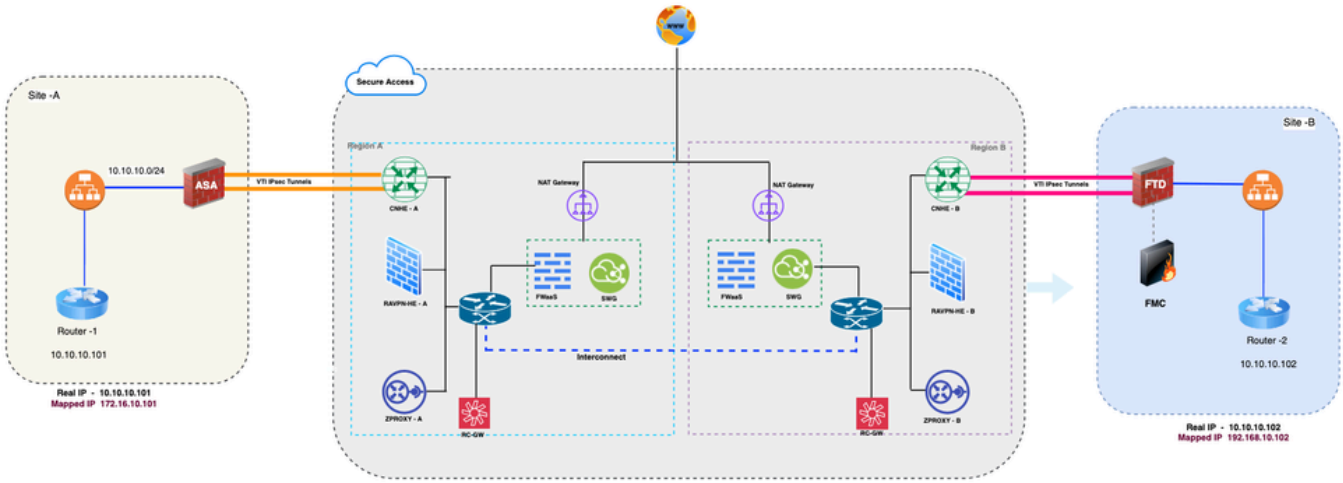
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يوفر الوصول الآمن من Cisco إمكانات طرف الخدمة الآمنة الأصلية عبر السحابة بما في ذلك الوصول الآمن إلى الإنترنت (SIA) والوصول الآمن الخاص (SPA). بالنسبة للمؤسسات التي تقوم بتوسيع الوصول إلى التطبيقات الخاصة إلى المستخدمين البعيدين دون نقل حركة مرور البيانات بشكل عكسي من خلال مركز بيانات، يستخدم الوصول الآمن مجموعات أنفاق مشفرة بين أجهزة الشبكة الداخلية - مثل Cisco Secure Access cloud و Adaptive Security Appliance (ASA) و Firewall Threat Defense (FTD) و Points-of-Presence (PoPs).

يوضح هذه المستند كيفية إنشاء نفق IPsec مستند إلى المسار باستخدام IKEv2 بين Cisco Secure Access، مما يتيح ترجمة عنوان الشبكة (NAT) على الوصول ASA و Cisco FTD، وتوجيه حركة مرور البيانات على FTD و ASA لتوجيه المستند إلى السياسة (PBR) والتوجيه المستند إلى الآمن والوصول الخاص فقط إلى النفق المرتبطة بالوصول.

الرسم التخطيطي للشبكة



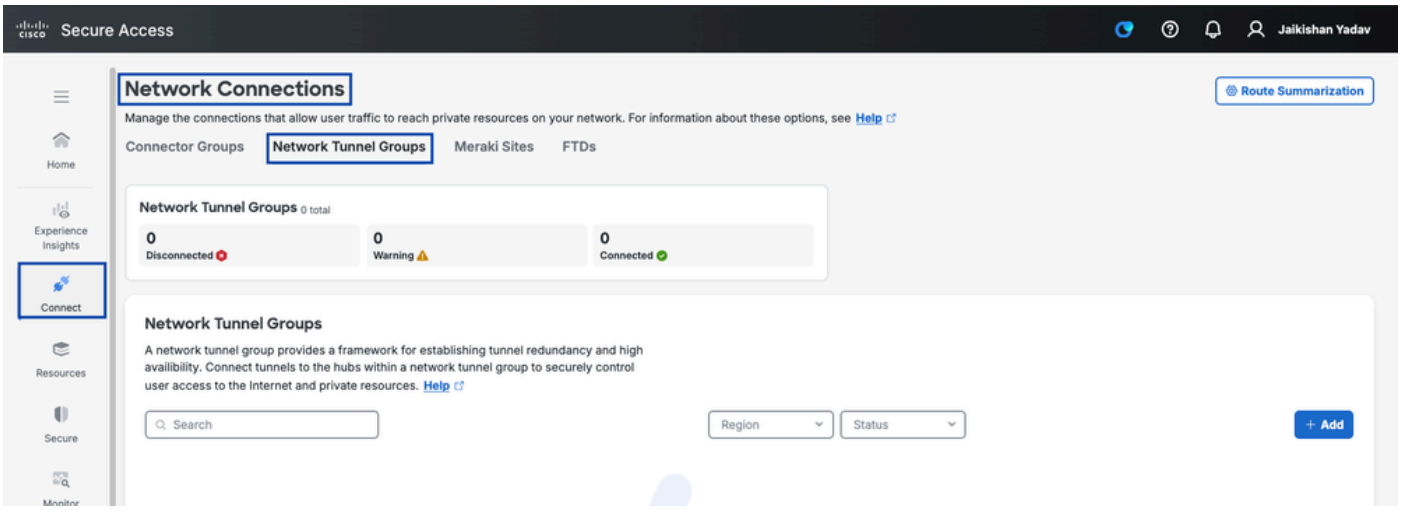
طوبولوجيا الشبكة

التكوين

الوصول الآمن والدفاع الآمن عن مؤشر ترابط جدار الحماية - الشبكة الخاصة الظاهرية (VPN) الديناميكية (BGP) القائمة على التوجيه مع PBR

تكوين مجموعة نفق الشبكة على الوصول الآمن

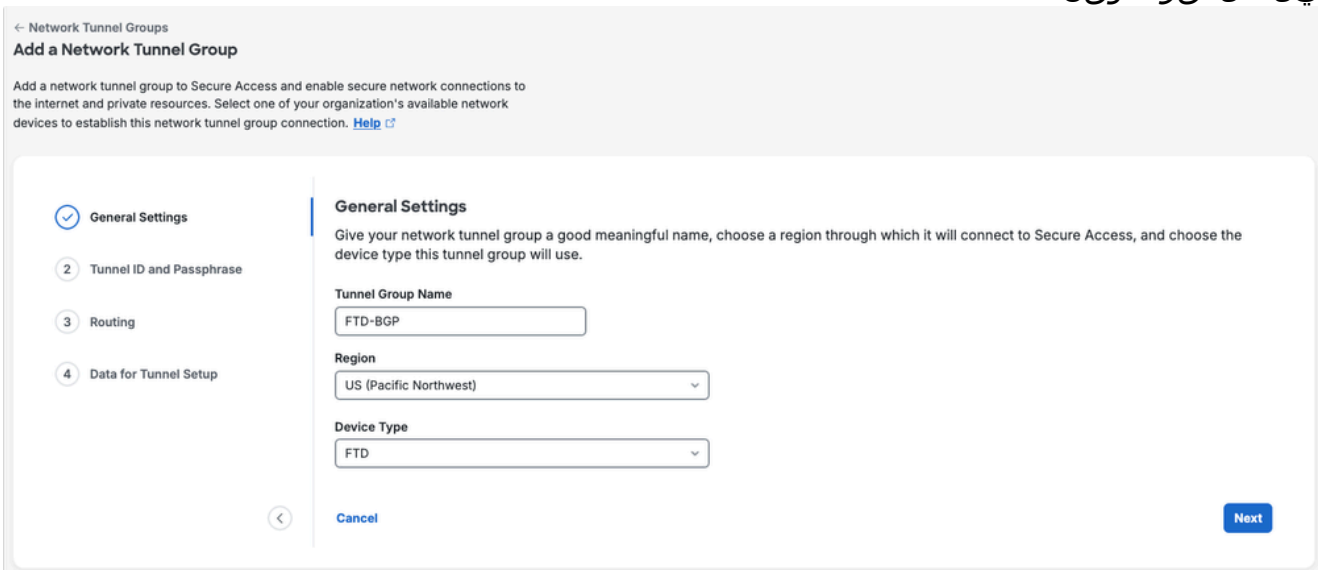
1. تسجيل الدخول إلى لوحة معلومات الوصول الآمن [الوصول الآمن](#)
2. انتقل إلى الاتصال > إتصالات الشبكة > مجموعات نفق الشبكة وانقر فوق +إضافة لتكوين مجموعة نفق الشبكة



الوصول الآمن - مجموعات نفق الشبكة

3. تكوين مجموعة نفق الشبكة - الإعدادات العامة

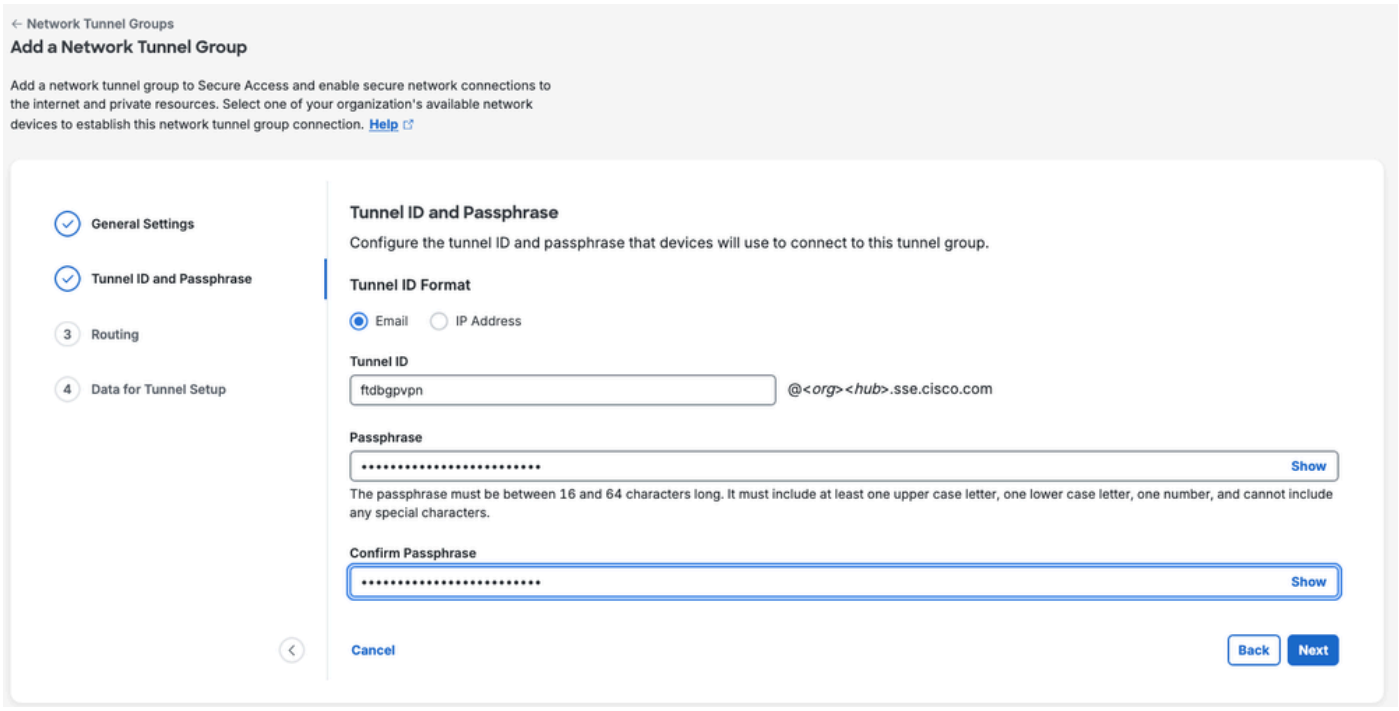
- تكوين اسم مجموعة النفق والمنطقة ونوع الجهاز
- انقر فوق التالي



الوصول الآمن - الإعدادات العامة لمجموعات النفق للشبكة

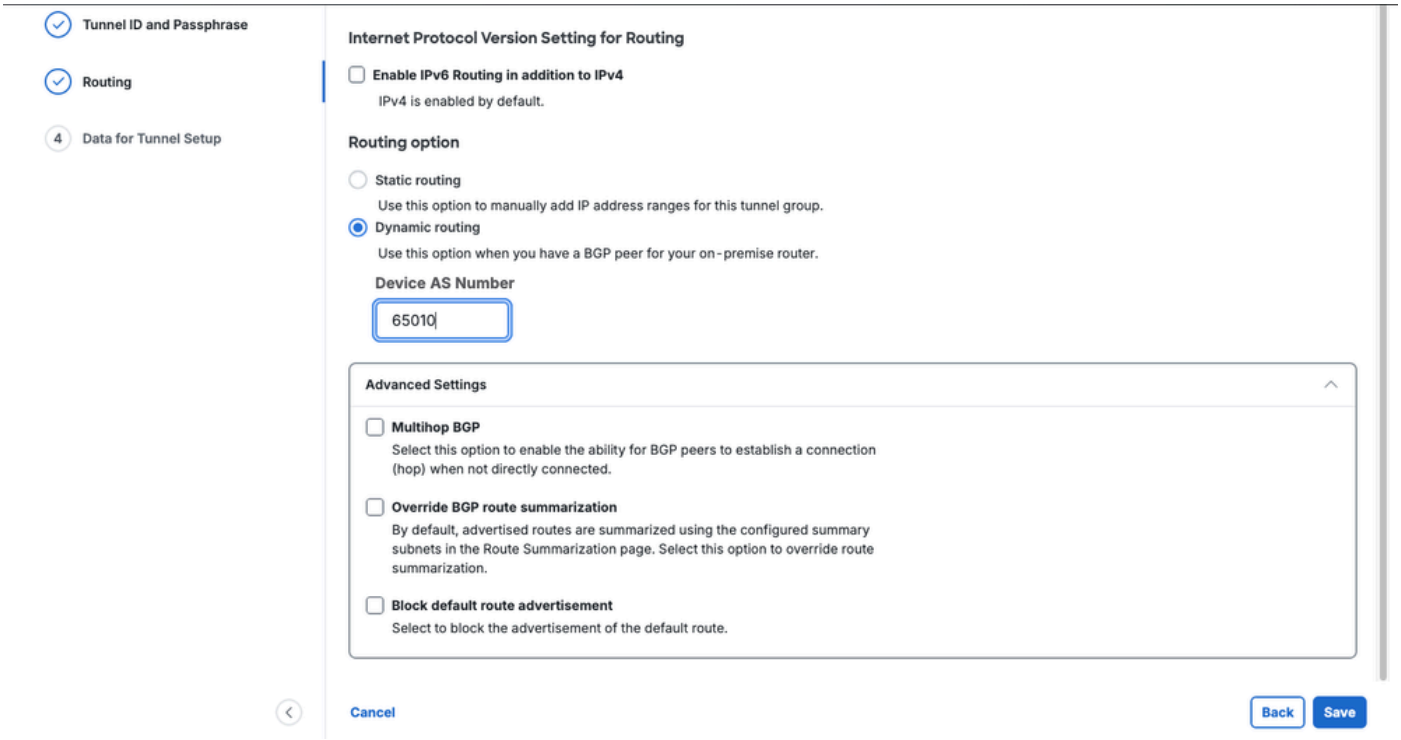
4. قم بتكوين معرف النفق وعبارة المرور.

- قم بتكوين معرف النفق عبارة المرور.
- انقر فوق التالي

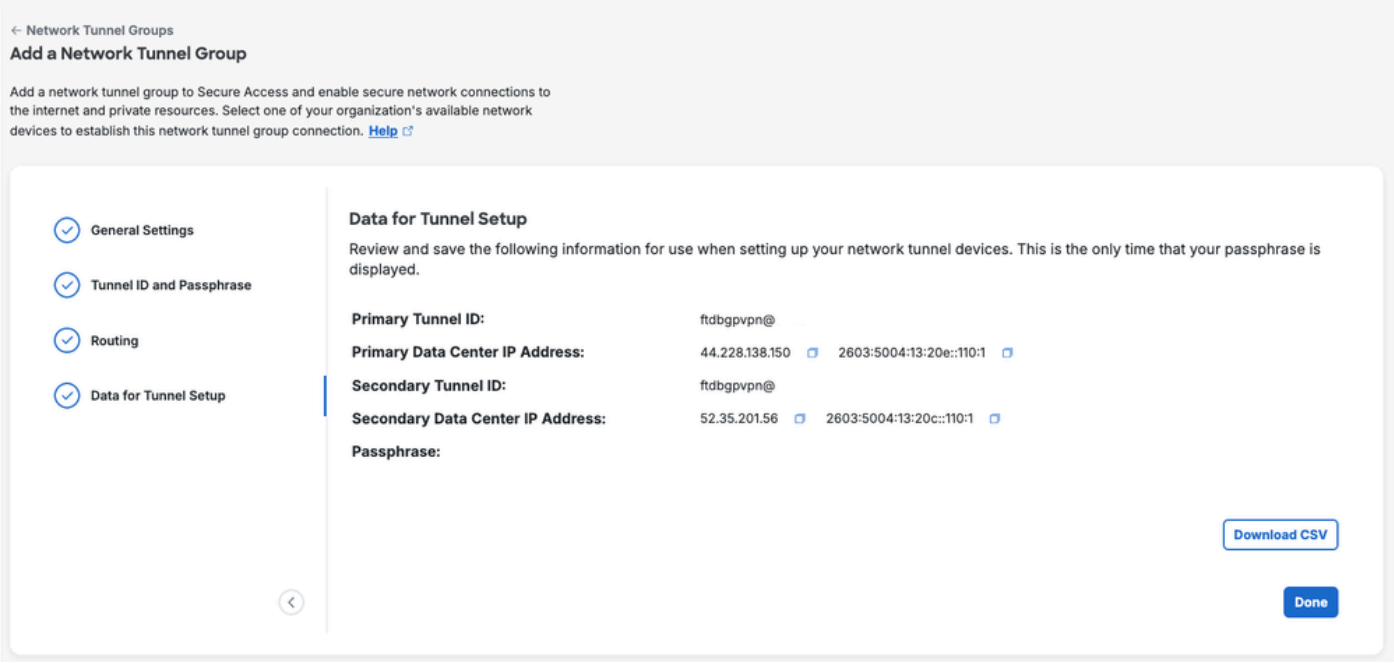


5. تكوين التوجيه

- تكوين الجهاز كرقم
- انقر فوق حفظ



6. حفظ تكوين مجموعة أنفاق الشبكة



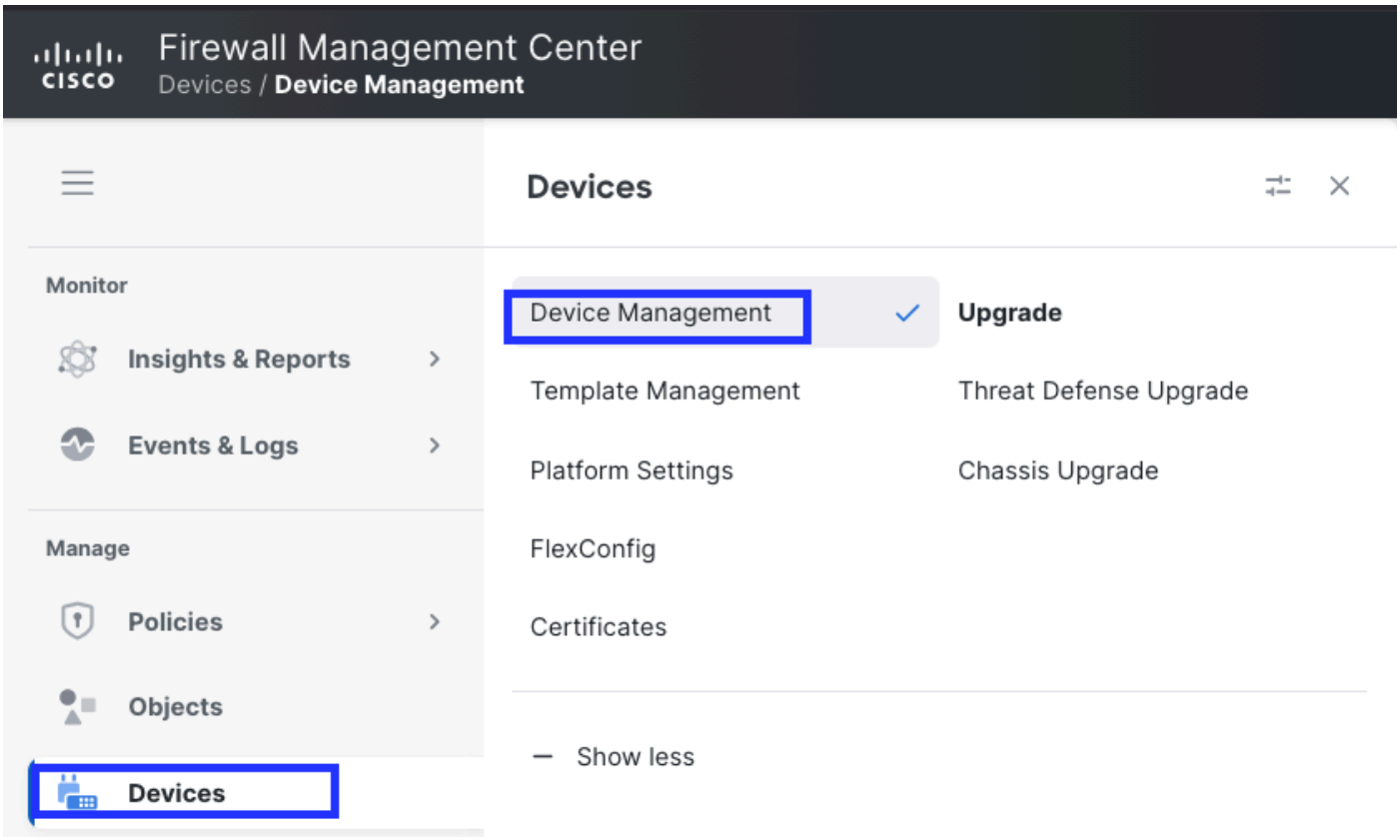
الوصول الآمن - مجموعات نفق الشبكة

تكوين VPN الديناميكي القائم على المسار ل IPsec على الدفاع الآمن عن تهديد جدار الحماية (FTD) باستخدام PBR

1. تسجيل الدخول إلى مركز إدارة جدران الحماية (FMC)

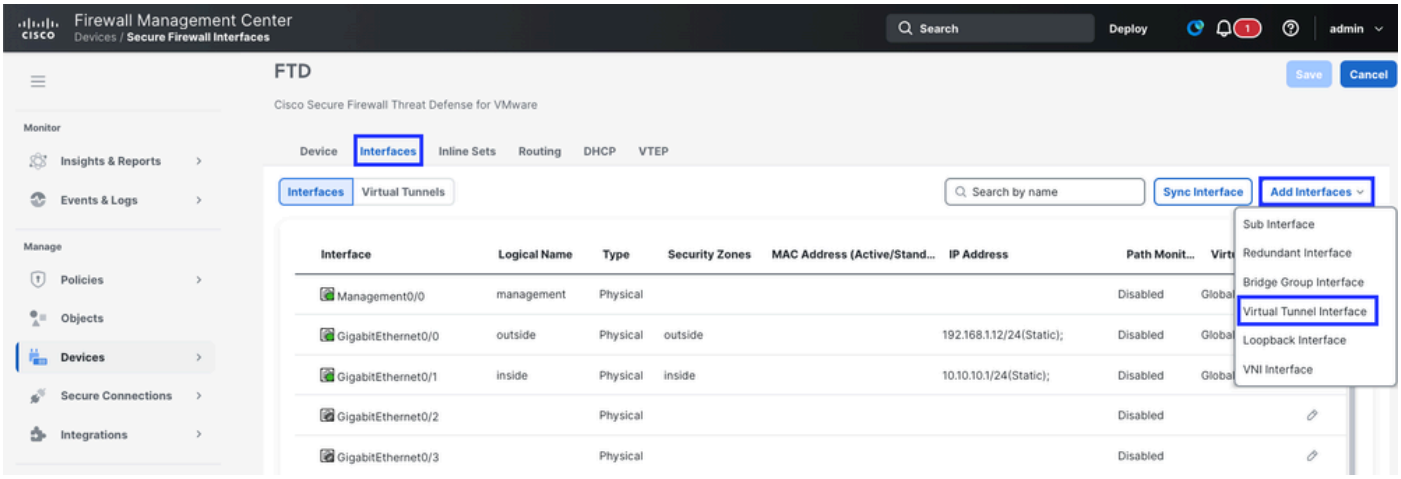
2. تكوين واجهة النفق الظاهرية VTI

- انتقل إلى الأجهزة > إدارة الأجهزة



إدارة جدار الحماية الآمنة - لوحة المعلومات

- انقر على أيقونة القلم الرصاص بجوار الجهاز وتصفح إلى قسم الواجهة
- انقر فوق إضافة الواجهات وحدد واجهة النفق الظاهري



الإدارة الآمنة لجدار الحماية - تكوين FTD VTI

- تكوين VTI

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

VTI-1

[x] Enabled

Description:

Virtual Tunnel interface for Primary VTI VPN

Security Zone:

vti

Priority:

0 *(0 - 65535)*

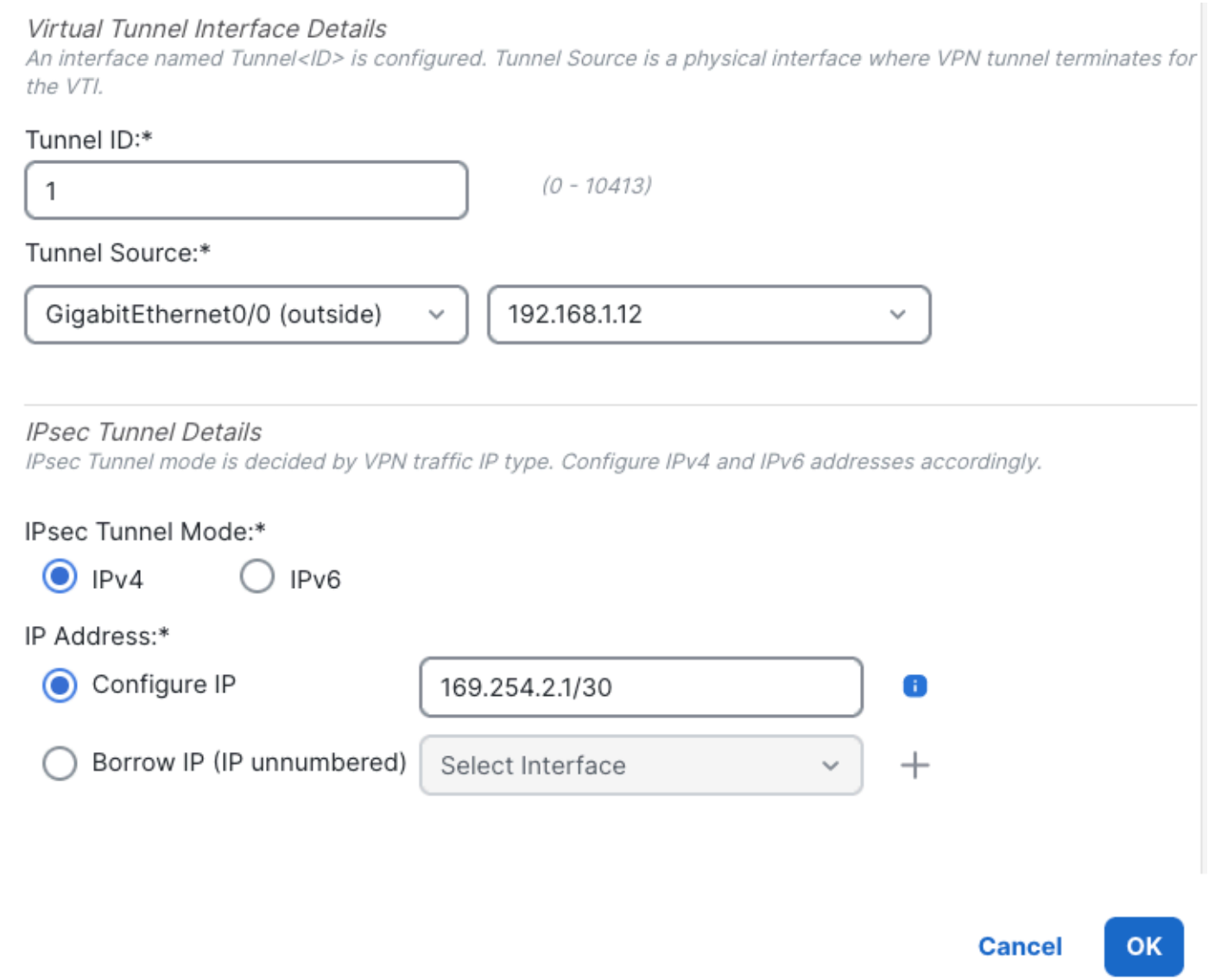
Propagate Security Group Tag: [x]

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

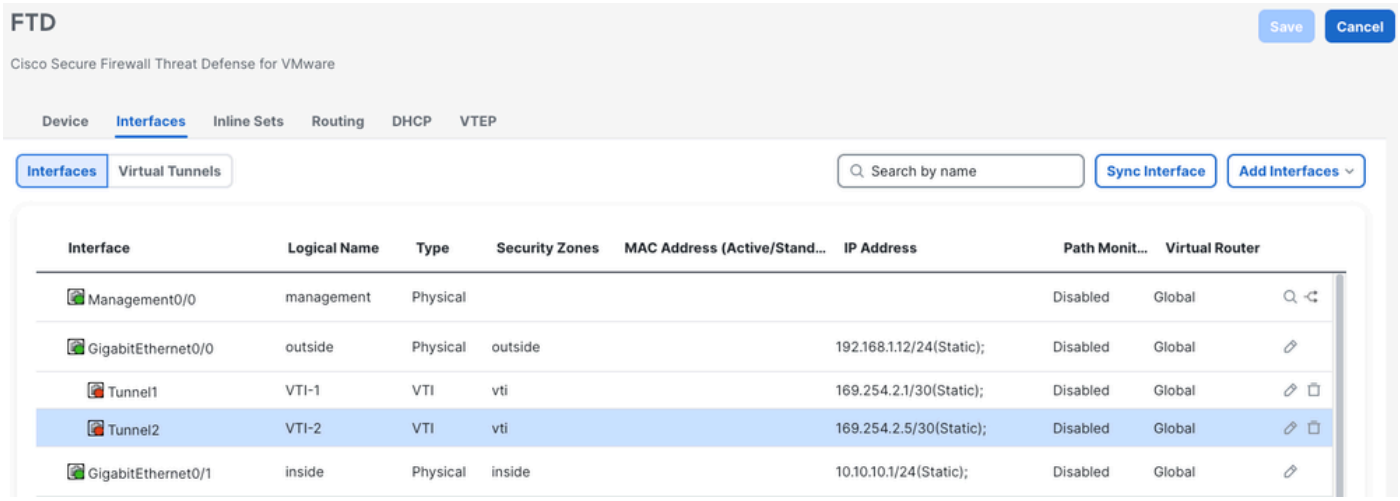
Tunnel ID:*

1 *(0 - 10413)*

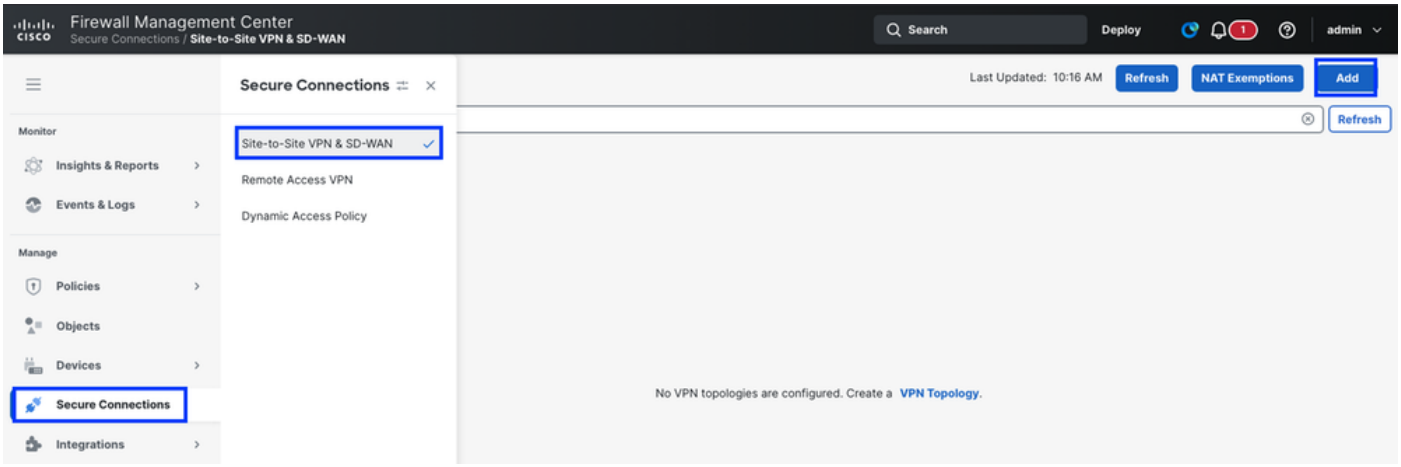


الإدارة الآمنة لجدار الحماية - تكوين FTD VTI

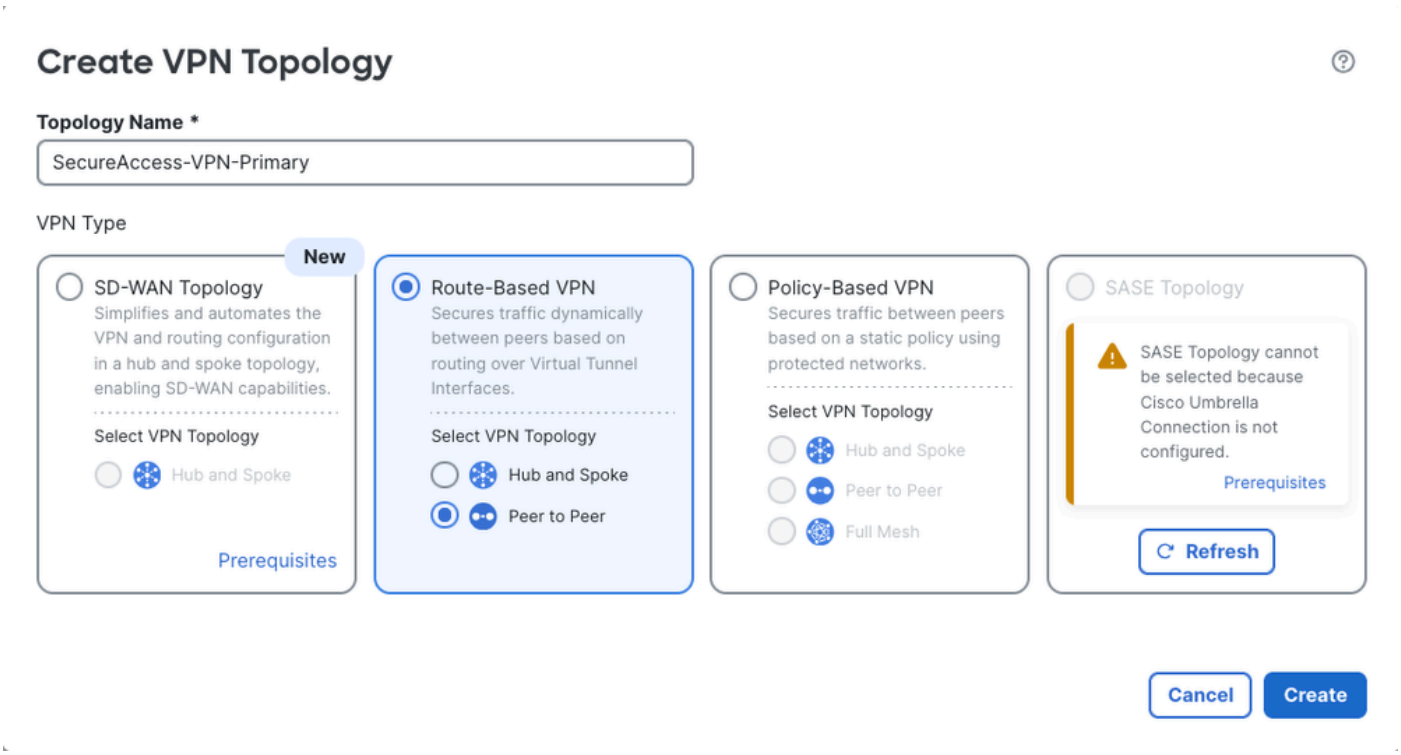
- تكوين VTI-2 بالإضافة إلى شبكات VPN الثانوية ل IPsec مع الوصول الآمن



3. انتقل إلى الاتصالات الآمنة > VPN من موقع إلى موقع و SD-WAN وانقر فوق Add لتكوين شبكة VPN



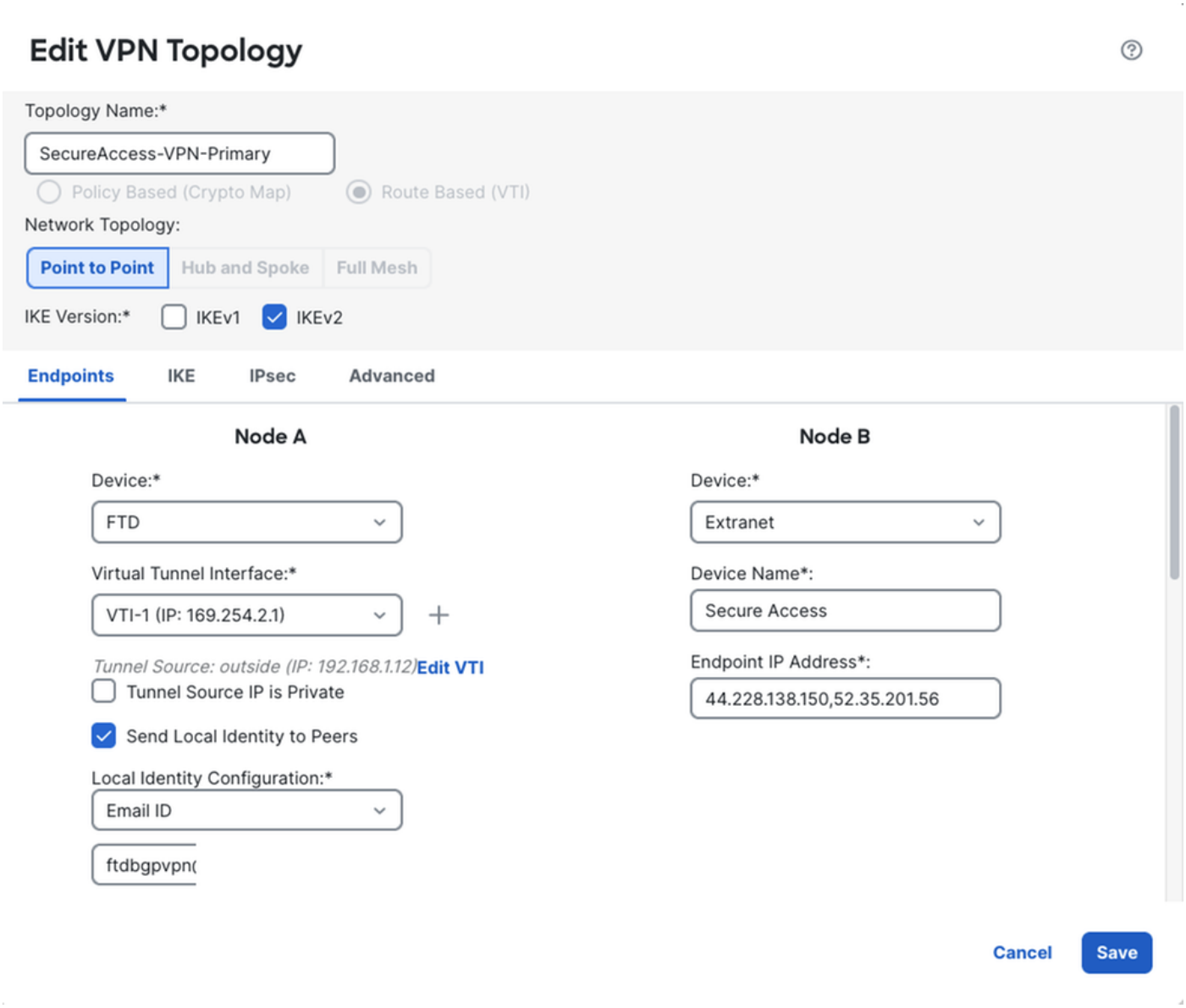
- إنشاء مخطط VPN



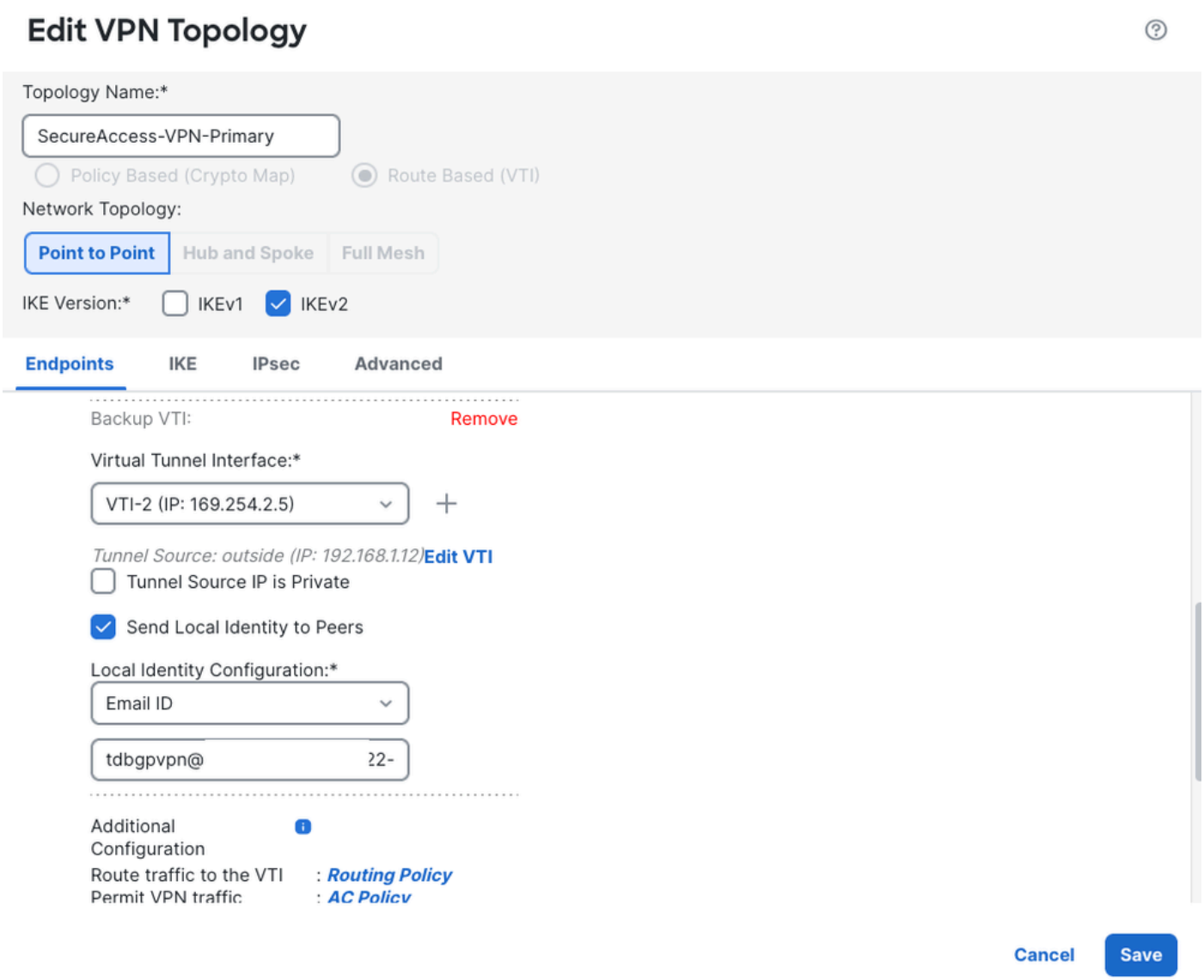
- من الخطوة 6 من تكوين مجموعة نفق الشبكة على الوصول الآمن ، احصل على معرفات

.النفق وعناوين IP لمراكز البيانات الأساسية والثانوية

- انقر فوق نقاط النهاية
- تحت العقدة A، انقر فوق الجهاز وحدد جهاز FTD الخاص بك
- انقر على واجهة النفق الظاهرية وحدد واجهة VTI الأولى التي تم إنشاؤها في الخطوة السابقة
- انقر على خيار إرسال الهوية المحلية إلى الأقران وحدد معرف البريد الإلكتروني، وأدخل معرف النفق الأساسي (من "حفظ تكوين مجموعة نفق الشبكة" ضمن تكوين مجموعة نفق الشبكة على الوصول الآمن)
- تحت العقدة B، انقر فوق الجهاز وحدد إكستارانت
- انقر على اسم الجهاز وأعطه اسما
- انقر فوق عناوين IP لنقطة النهاية وأدخل عناوين IP الأساسية والثانوية للوصول الآمن التي يتم فصلها بفاصلة (من "حفظ تكوين مجموعة نفق الشبكة" ضمن تكوين مجموعة نفق الشبكة على الوصول الآمن)
- انقر فوق إضافة VTI للنسخ الاحتياطي
- انقر فوق واجهة النفق الظاهرية وحدد واجهة VTI الثانية التي تم إنشاؤها في الخطوة السابقة
- انقر على خيار إرسال الهوية المحلية إلى الأقران وحدد معرف البريد الإلكتروني، وأدخل معرف النفق الثانوي (من "حفظ تكوين مجموعة نفق الشبكة" ضمن تكوين مجموعة نفق الشبكة على الوصول الآمن)
- انقر على حفظ

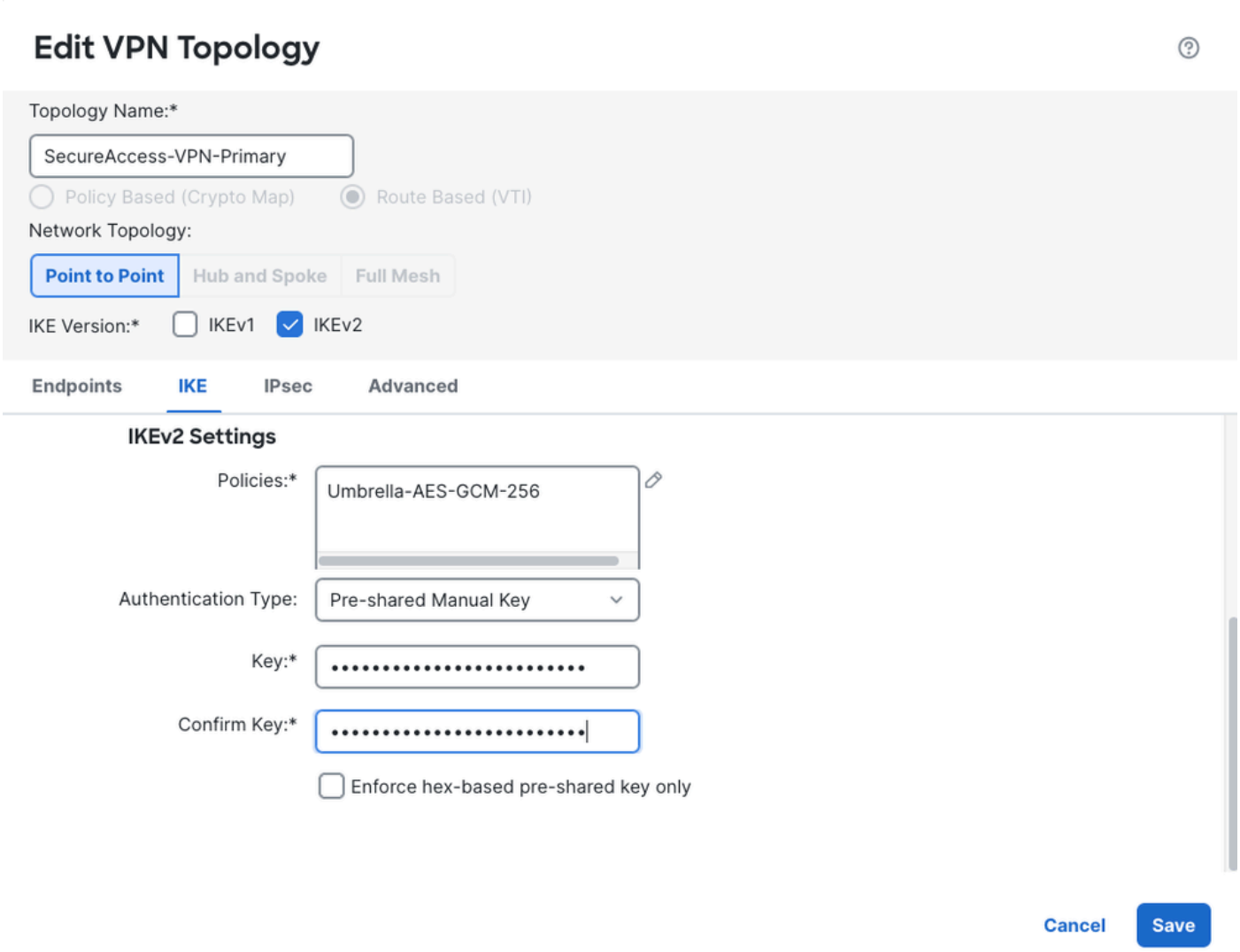


تكوين نقطة نهاية FTD الآمن - VPN



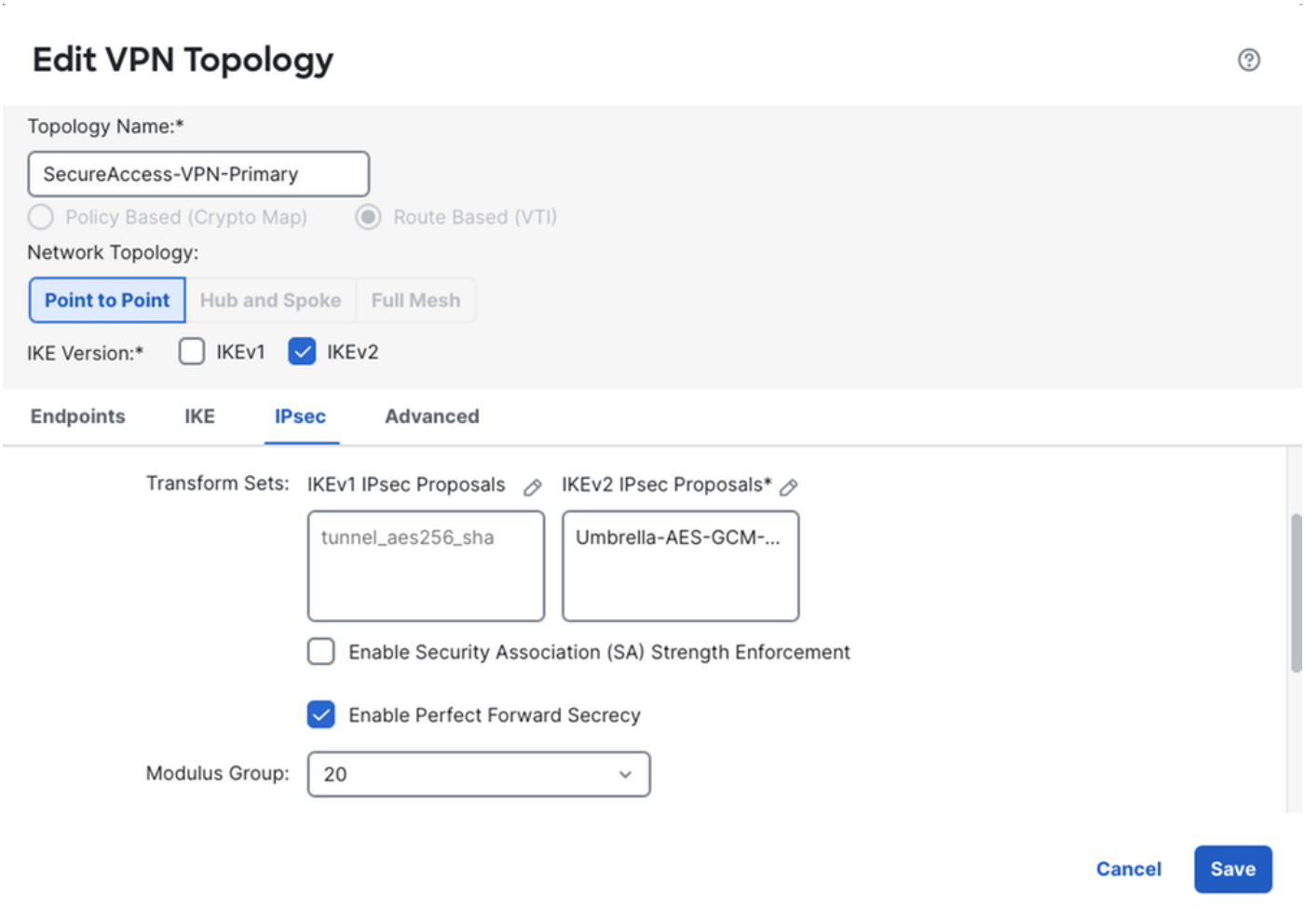
تكوين نقطة نهاية FTD الآمن - VPN

- تكوين إعدادات IKEv2 وفقا لمعلمات IPsec المدعومة
- حدد السياسات على أنها Umbrella-AES-GCM-256
- حدد نوع المصادقة كمفتاح يدوي مشترك مسبقا



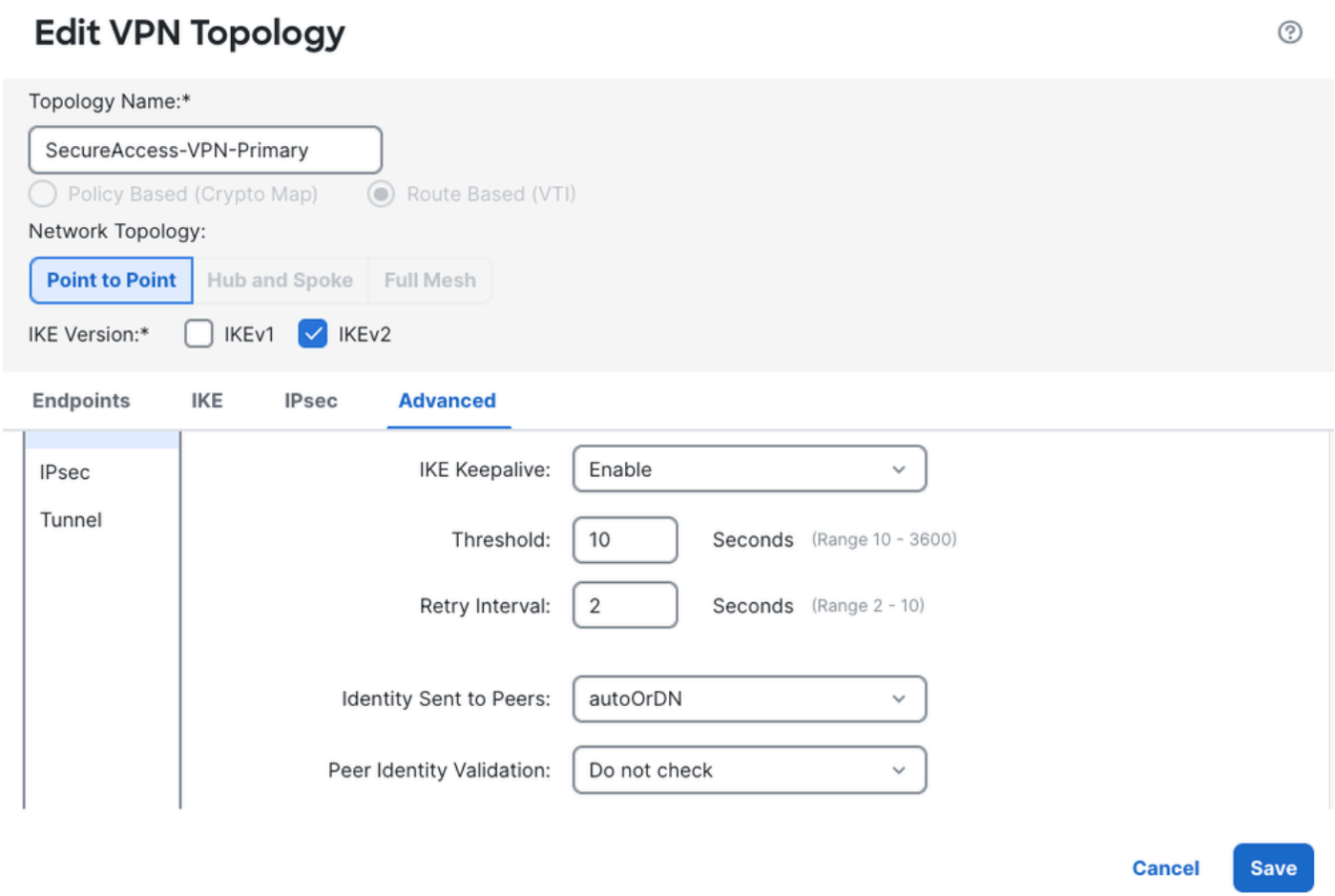
إعدادات IKE لـ FTD الآمن - VPN

- تكوين إعدادات IPsec
  - حدد مقترحات IKEv2 IPsec على أنها Umbrella-AES-GCM-256
  - تمكين PFS على هيئة تحديد مجموعة وحدات على هيئة 20



إعدادات IPsec الخاصة ب FTD الآمن - VPN

- إعدادات متقدمة
- انقر فوق حفظ



إعدادات متقدمة ل FTD الآمن - VPN

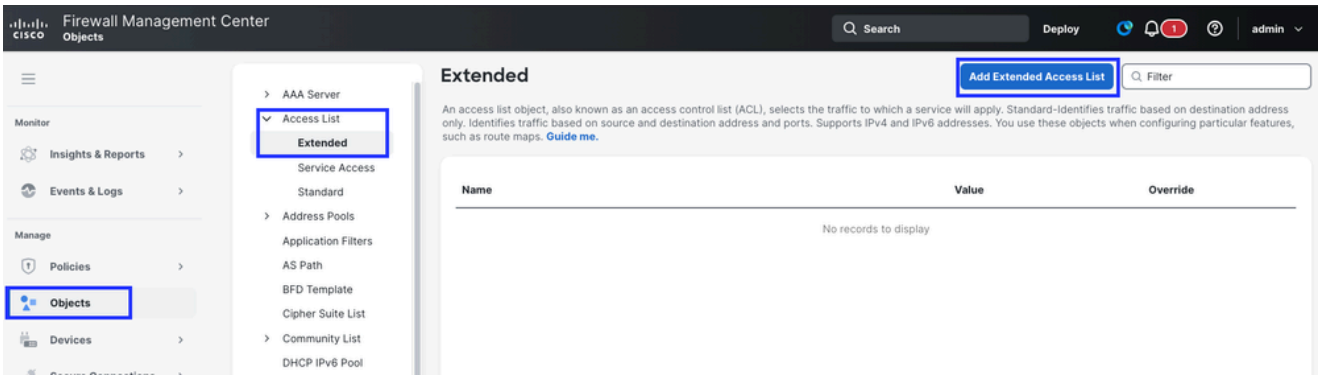
التوجيه القائم على سياسة FTD

في التوجيه التقليدي، يتم توجيه الحزم بناء على عنوان IP للوجهة. من الصعب تغيير توجيه حركة مرور معينة في نظام التوجيه القائم على الوجهة. يعمل التوجيه المستند إلى السياسة (PBR) على توسيع الآليات التي توفرها بروتوكولات التوجيه وإكمالها، مما يمنحك المزيد من التحكم في التوجيه.

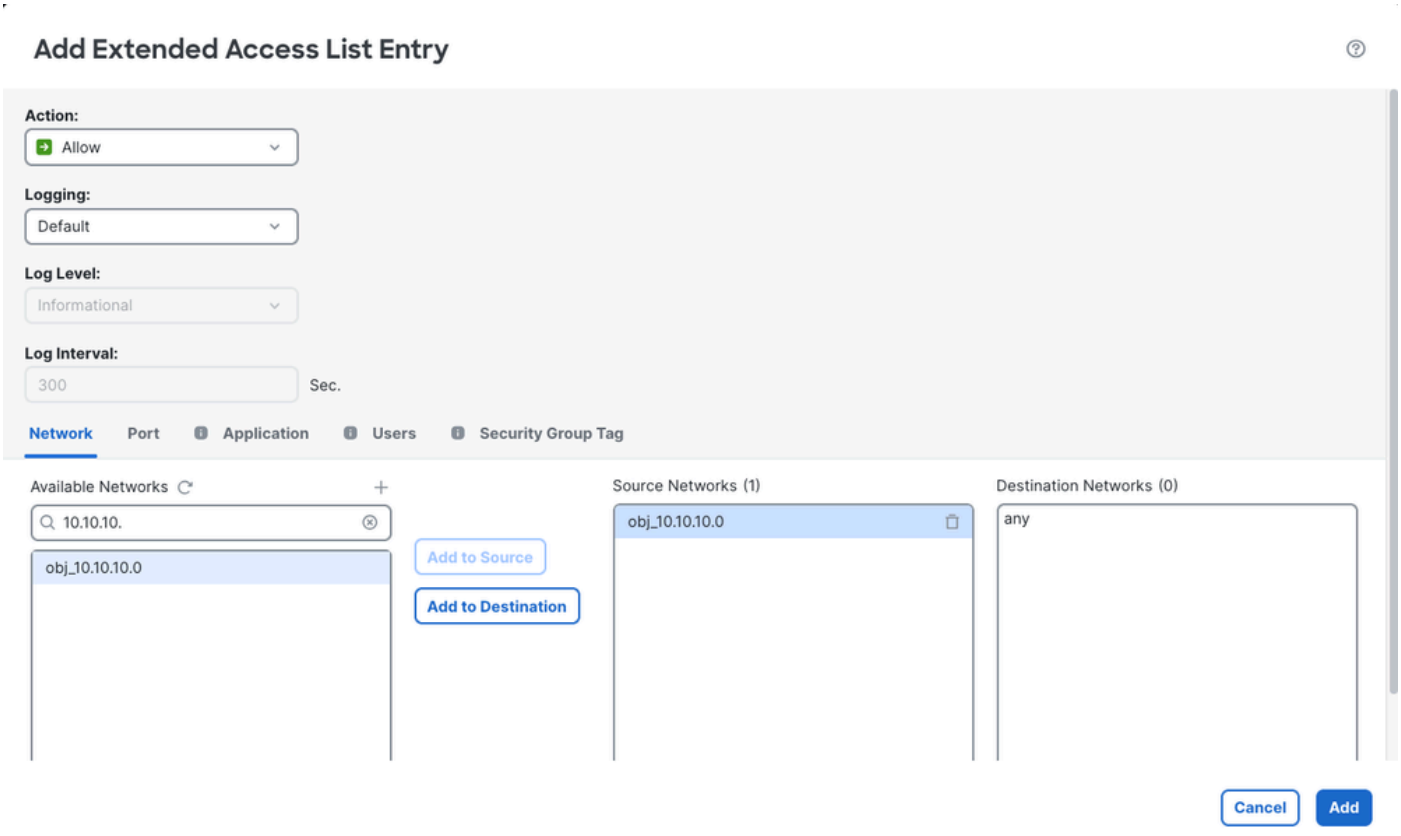
يسمح لك PBR بتعيين أسبقية IP. كما أنها تسمح لك بتعيين مسار لحركة مرور معينة، مثل حركة مرور الأولوية عبر ارتباط عالي التكلفة. مع PBR، يمكنك تحديد التوجيه الذي يستند إلى معايير أخرى غير شبكة الوجهة مثل منفذ المصدر أو عنوان الوجهة أو منفذ الوجهة أو البروتوكول أو التطبيقات أو مجموعة من هذه الكائنات. للحصول على مزيد من المعلومات، ارجع إلى التوجيه المستند إلى السياسة

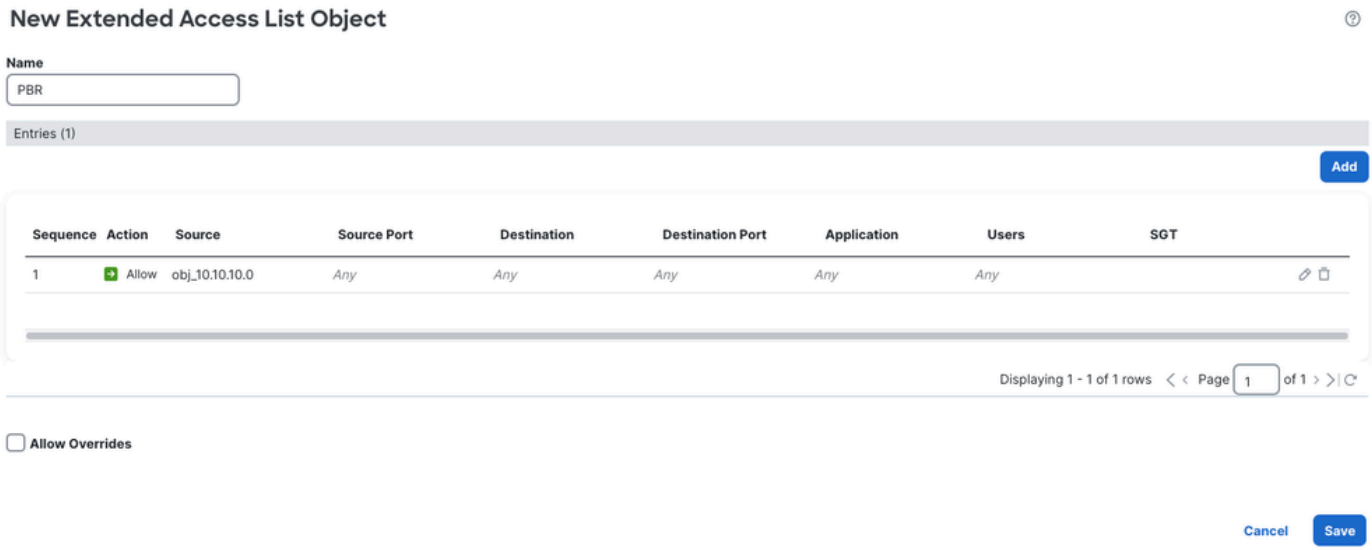
1. تكوين قائمة الوصول

- انتقل إلى كائنات > قائمة الوصول > موسع
- انقر على إضافة قائمة الوصول الموسعة



- إعطاء اسم قائمة الوصول
- تحديد الإجراء
  - سماح. - سيتم إرسال حركة المرور المعرفة إلى نفق IPsec
  - الحظر - سيتم تجاوز حركة المرور من نفق IPsec
  - ستتم مطابقة القاعدة استنادا إلى الرقم التسلسلي (أقل إلى أعلى)
  - انقر على إضافة
  - انقر فوق حفظ

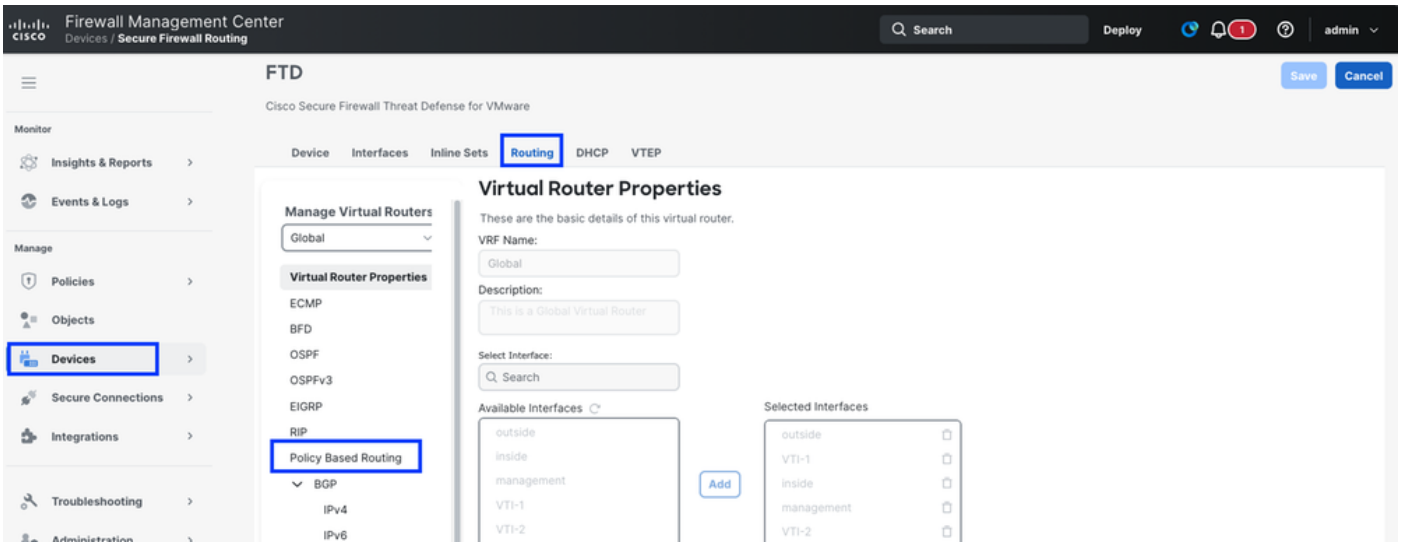




برووتوكول FTD الآمن - قائمة الوصول الموسعة

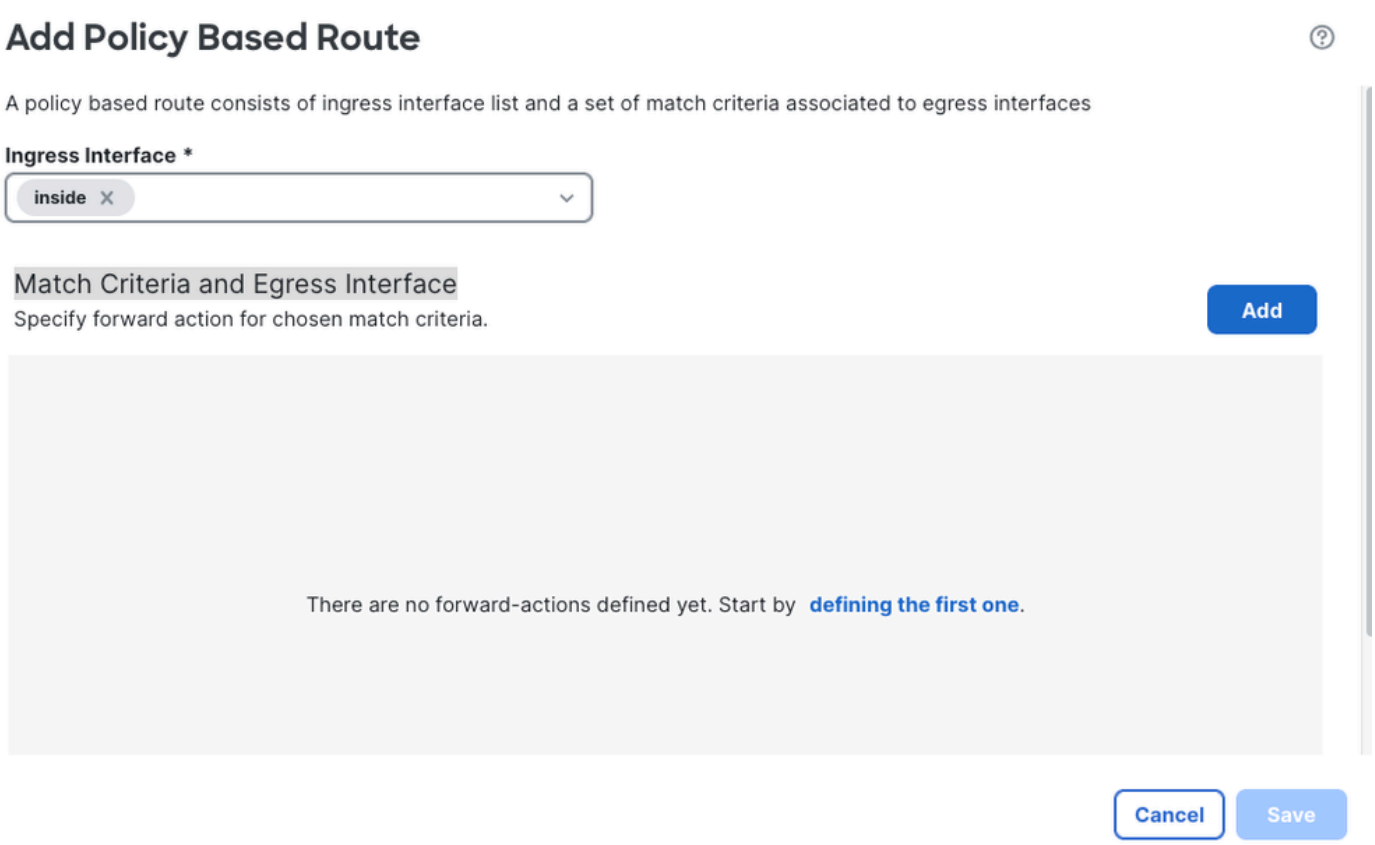
2. تكوين التوجيه المستند إلى السياسة

- انتقل إلى الأجهزة > إدارة الأجهزة > FTD > التوجيه

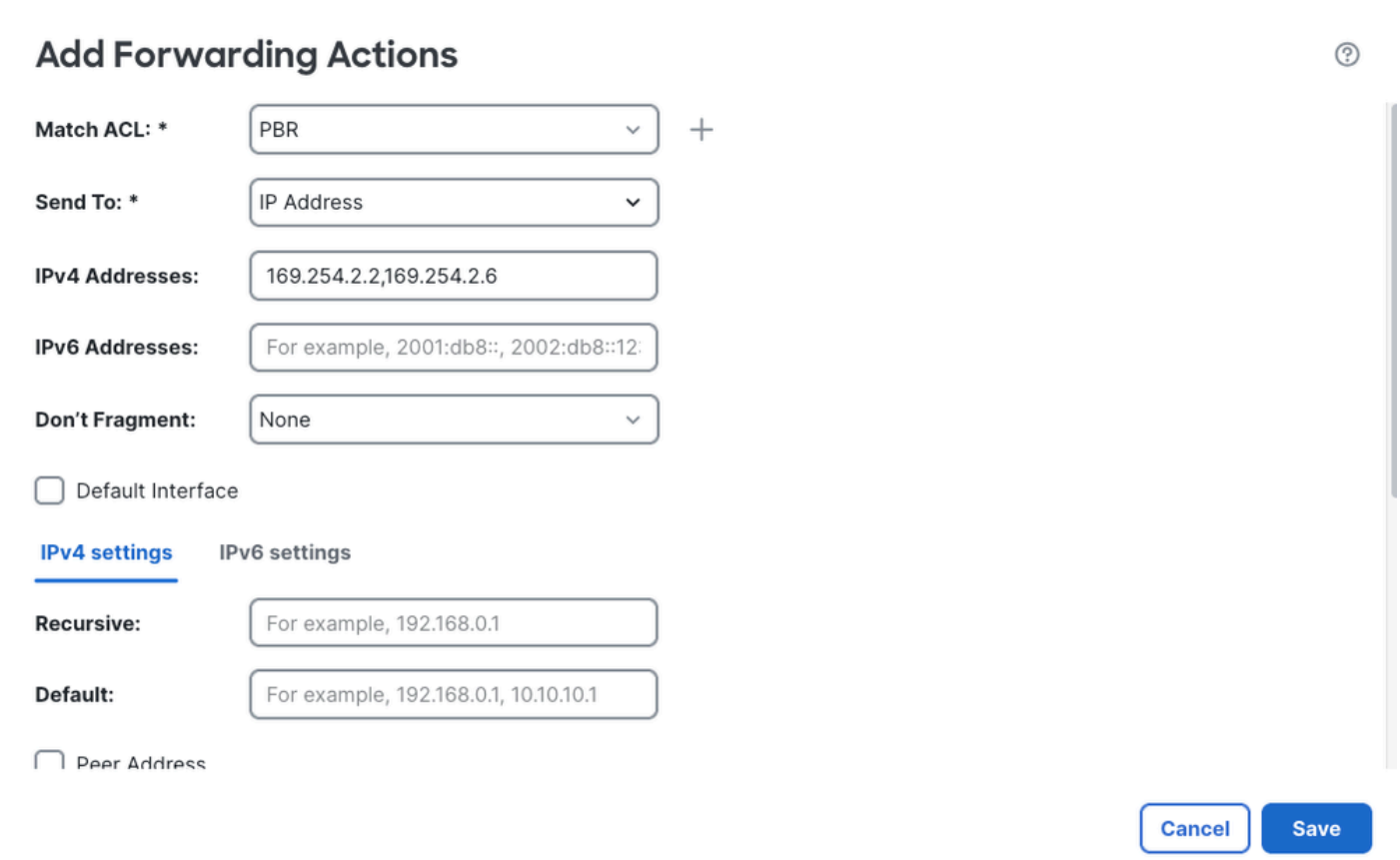


برنامج FTD الآمن - التوجيه المستند إلى السياسة

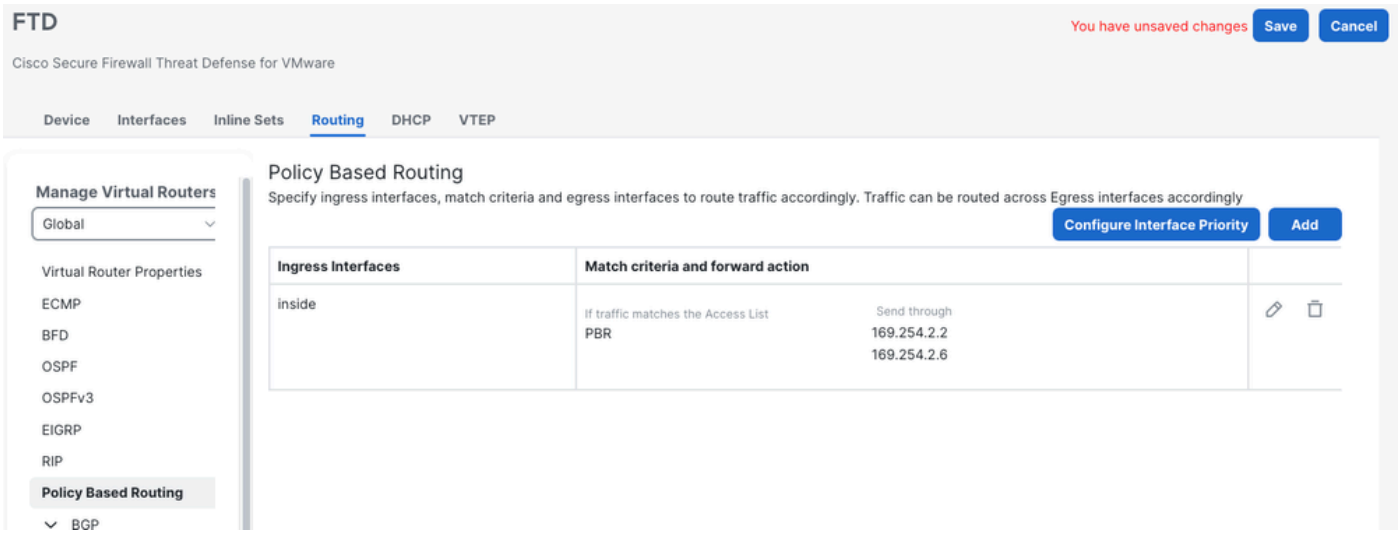
- انقر فوق إضافة
- حدد واجهة الدخول - واجهة الدخول للشبكة الفرعية التي قمنا بتعريفها في قائمة الوصول



- تحديد معايير المطابقة وواجهة الخروج
  - انقر على إضافة
  - تحديد قائمة التحكم في الوصول (ACL) المطابقة
  - حدد إرسال إلى كعنوان IP
  - إضافة عنوان IP للخطوة التالية. - عناوين IP الخاصة بواجهة VTIs. 169.254.2.130 وهو VTI-2 و VTI -1 ل. ذلك، سيكون عنوان IP الخطوة التالية 169.254.2.5/30. و 169.254.2.6 على التوالي. و 169.254.2.2
  - انقر على حفظ



برنامج FTD الآمن - التوجيه المستند إلى السياسة

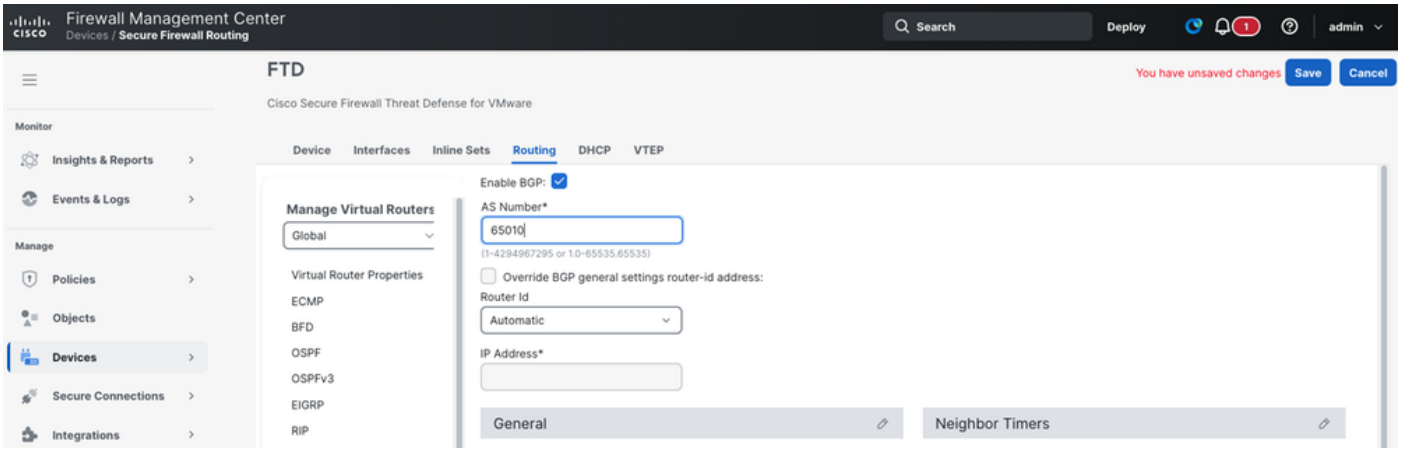


برنامج FTD الآمن - التوجيه المستند إلى السياسة

تكوين BGP على FTD

1. تمكين BGP

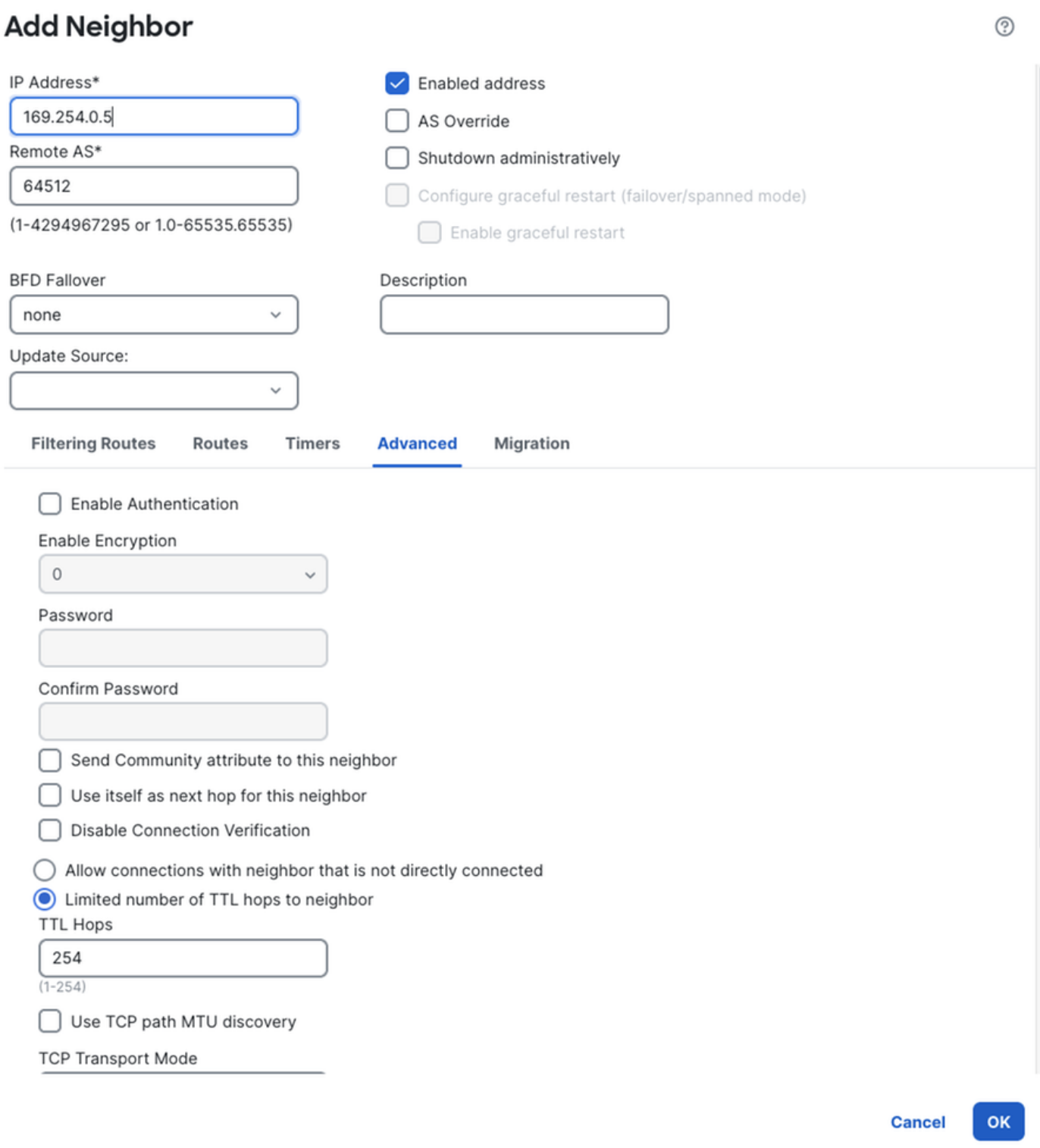
- انتقل إلى الأجهزة > إدارة الأجهزة > FTD > التوجيه > الإعدادات العامة > BGP
- تمكين BGP وإضافة رقم AS (رقم FTD المحلي AS)
- انقر فوق حفظ

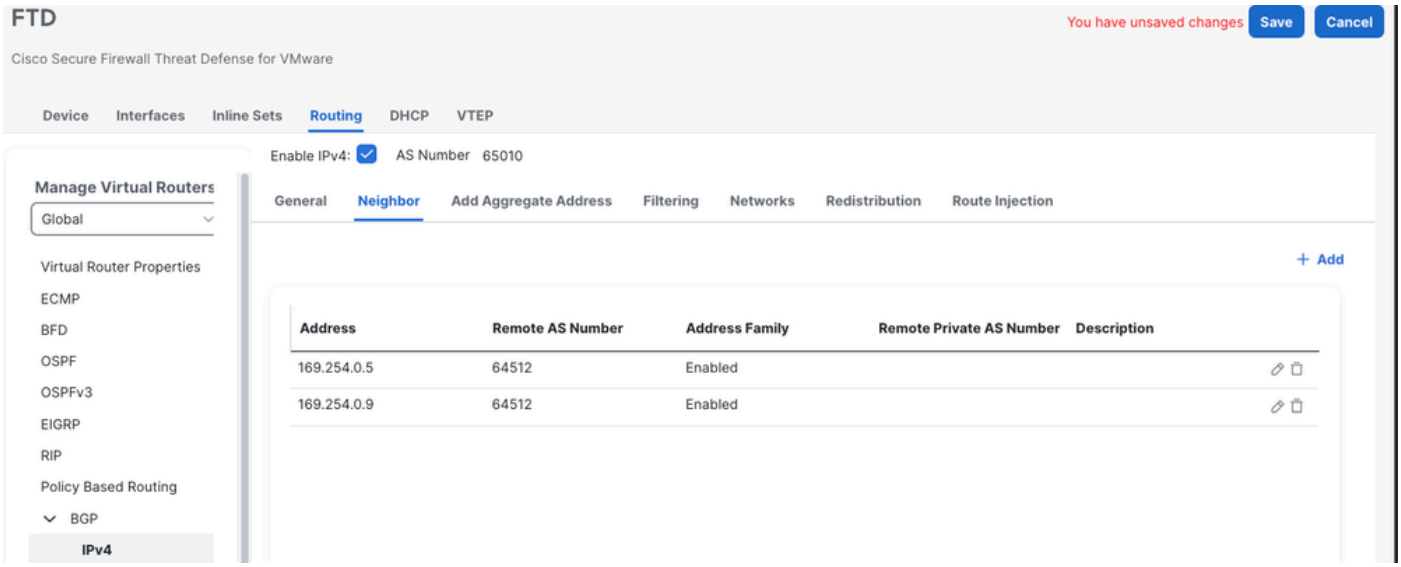


برووتوكول FTD الآمن - توجيه BGP

- انتقل إلى BGP > IPv4

2. إضافة جار BGP - نظير BGP للوصول الآمن هو 169.254.0.5 و. 169.254.0.9

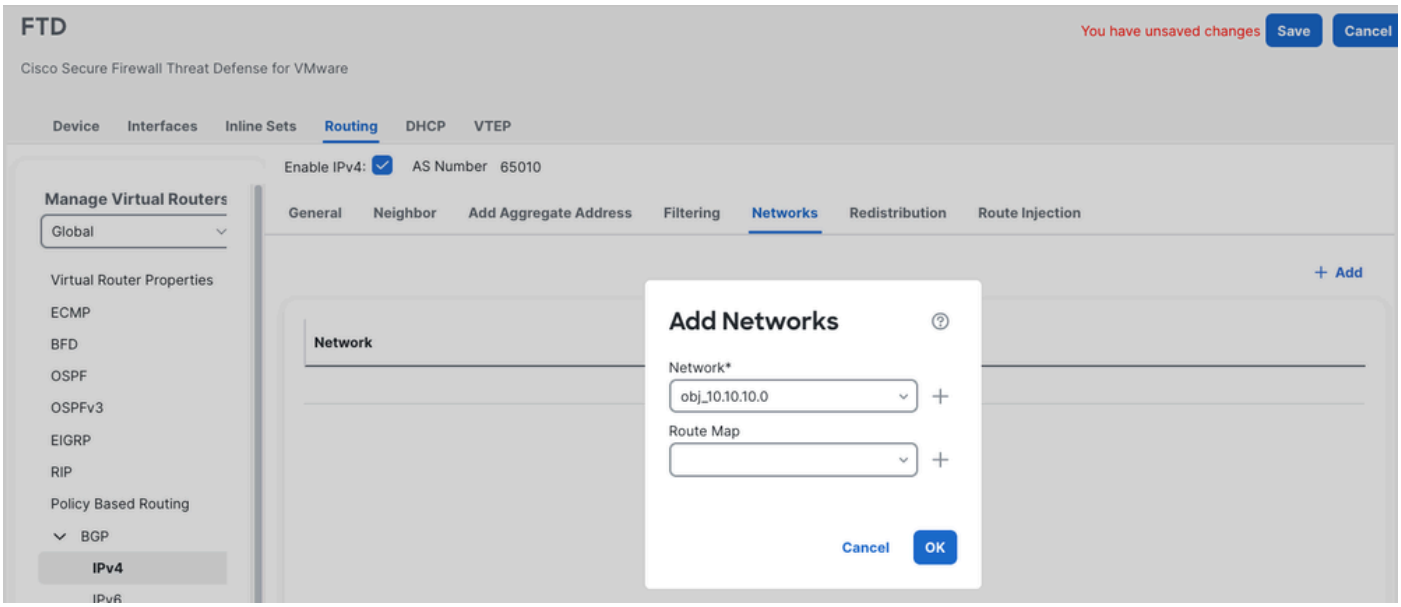

Add Neighbor
IP Address*
169.254.0.5
Remote AS*
64512
(1-4294967295 or 1.0-65535.65535)
Enabled address
AS Override
Shutdown administratively
Configure graceful restart (failover/spanned mode)
Enable graceful restart
BFD Fallover
none
Description
Update Source:
Filtering Routes
Routes
Timers
Advanced
Migration
Enable Authentication
Enable Encryption
0
Password
Confirm Password
Send Community attribute to this neighbor
Use itself as next hop for this neighbor
Disable Connection Verification
Allow connections with neighbor that is not directly connected
Limited number of TTL hops to neighbor
TTL Hops
254
(1-254)
Use TCP path MTU discovery
TCP Transport Mode
Cancel
OK



بروتوكول FTD الآمن - توجيه BGP

3. إضافة الشبكات - الشبكات التي يلزم الإعلان عنها لتأمين الوصول

- ثم انقر فوق موافق

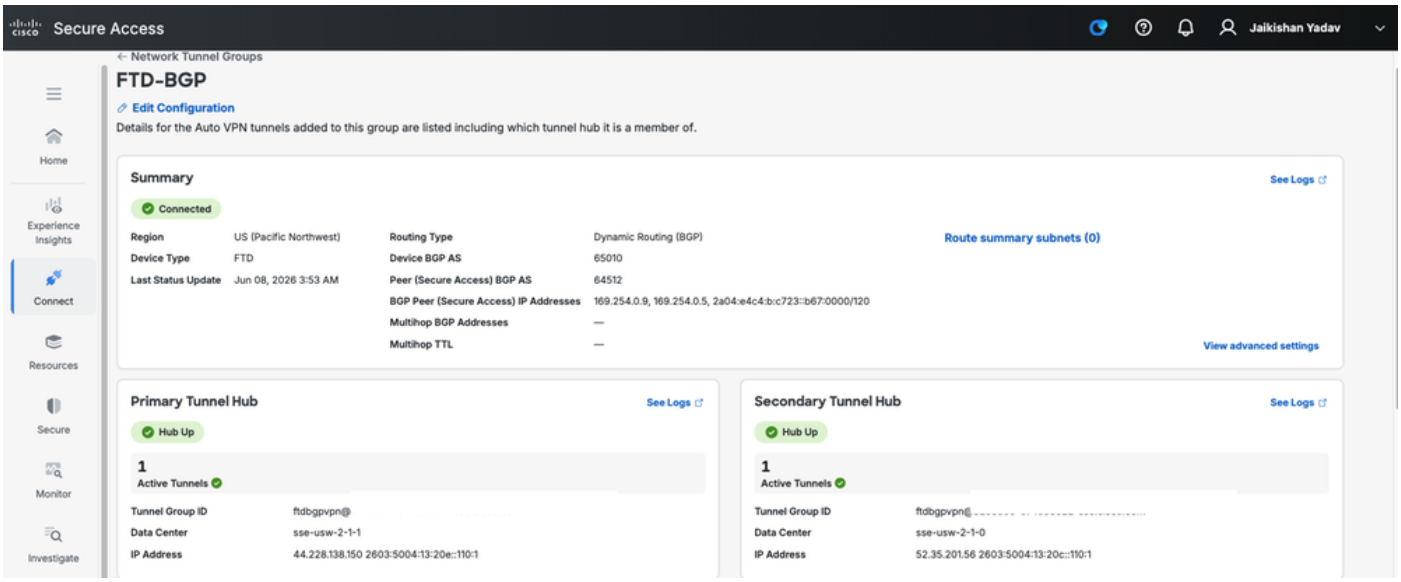


بروتوكول FTD الآمن - توجيه BGP

- حفظ التغييرات ونشرها

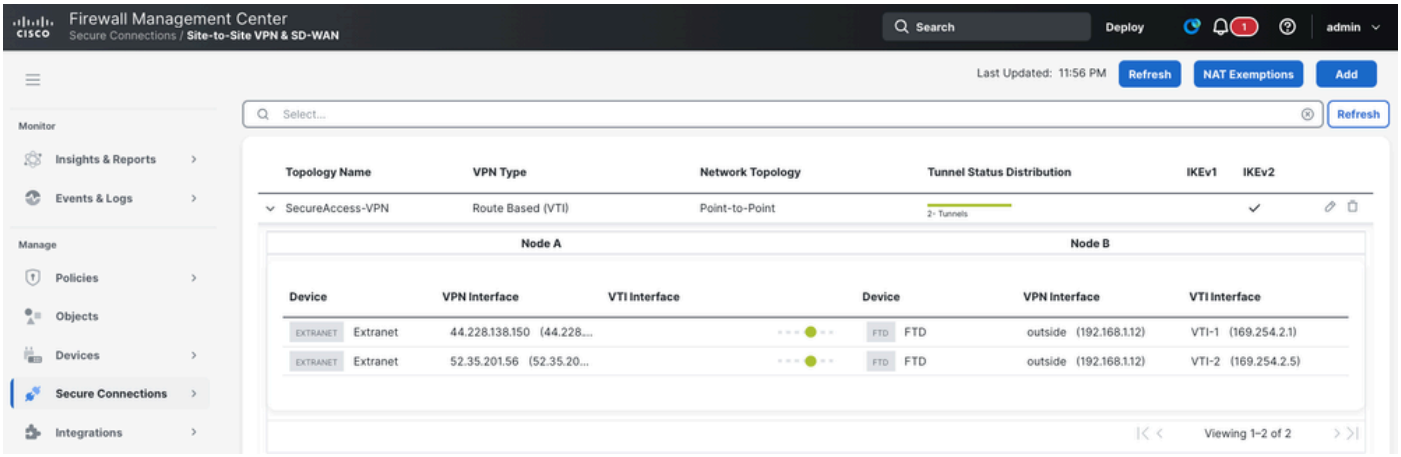
التحقق من حالة النفق

عند الوصول الآمن



حالة نفق FTD الآمن - IPsec

على FMC



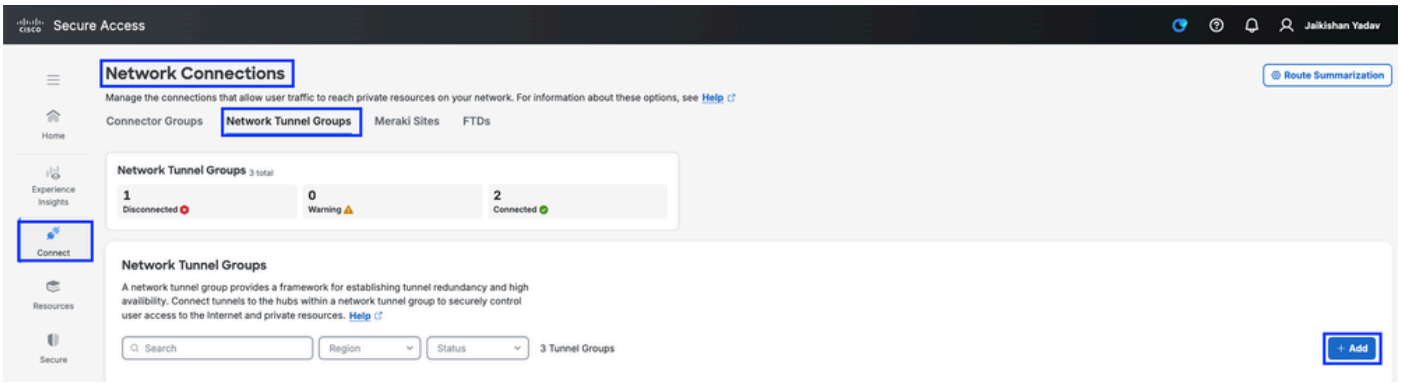
FMC الآمن - حالة نفق IPsec

تكوين شبكة VPN IPsec المستندة إلى المسار الثابتة على جهاز الأمان القابل للتكيف (ASA) باستخدام PBR

تكوين VPN على الوصول الآمن

1. تسجيل الدخول إلى لوحة معلومات الوصول الآمن [الوصول الآمن](#)
2. انتقل إلى الاتصال > إتصالات الشبكة > مجموعات نفق الشبكة وانقر فوق +إضافة

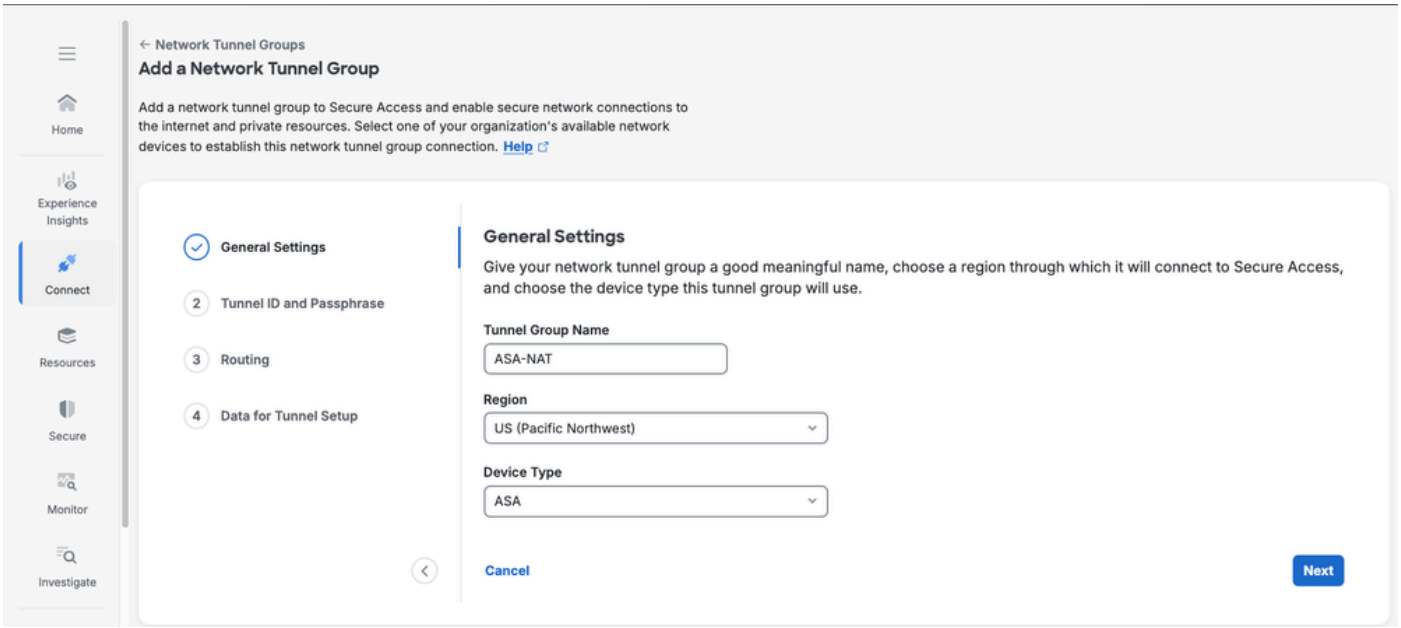
لتكوين مجموعة نفق الشبكة



الوصول الآمن - مجموعات نفق الشبكة

3. تكوين مجموعة نفق الشبكة - الإعدادات العامة

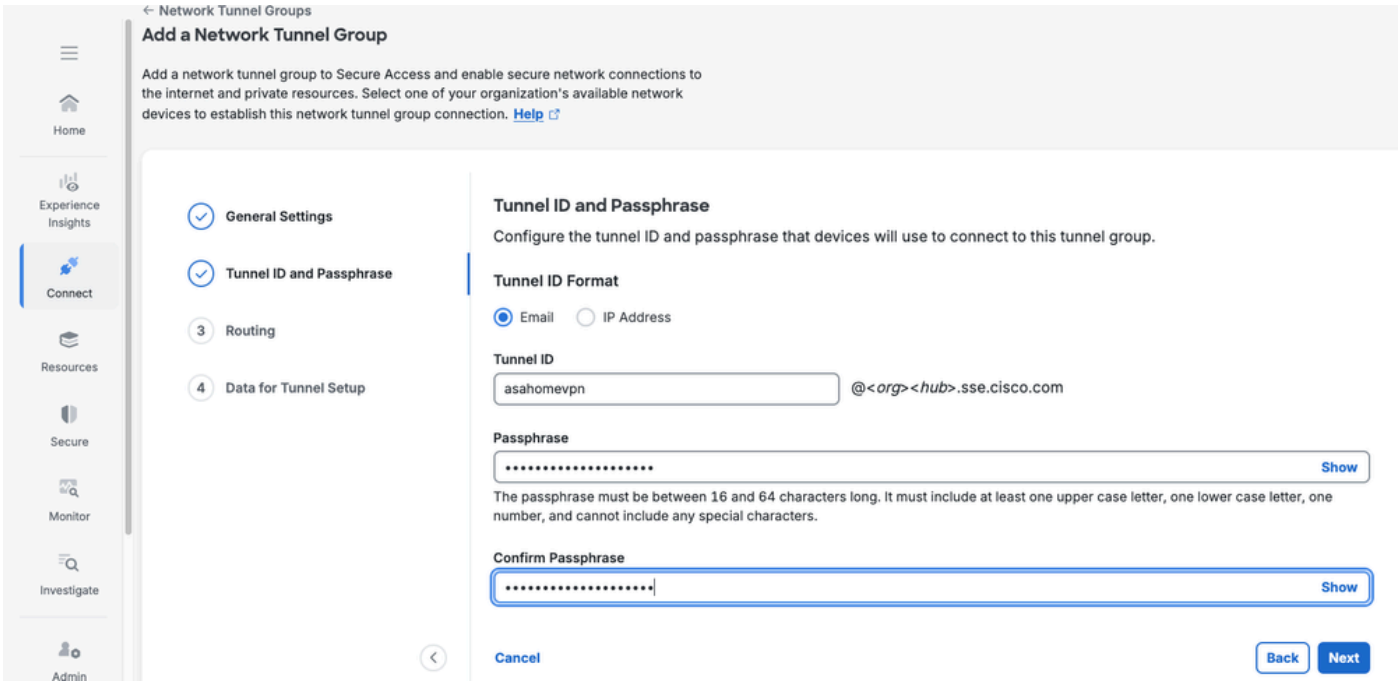
- تكوين اسم مجموعة النفق والمنطقة ونوع الجهاز
- انقر فوق التالي



الوصول الآمن - الإعدادات العامة لمجموعات النفق للشبكة

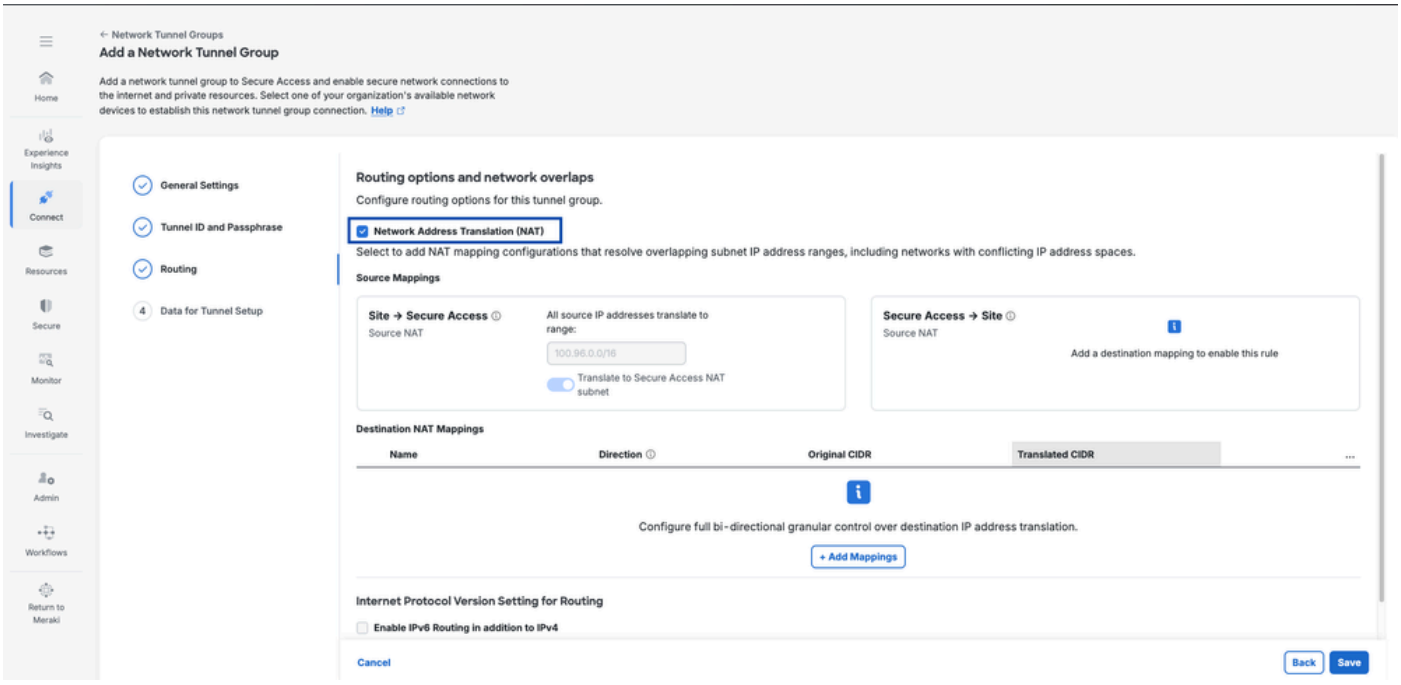
4. قم بتكوين معرف النفق وعبارة المرور.

- قم بتكوين معرف النفق عبارة المرور.
- انقر فوق التالي



الوصول الآمن - مجموعات نفق الشبكة

5. تمكين ترجمة عنوان الشبكة (NAT)

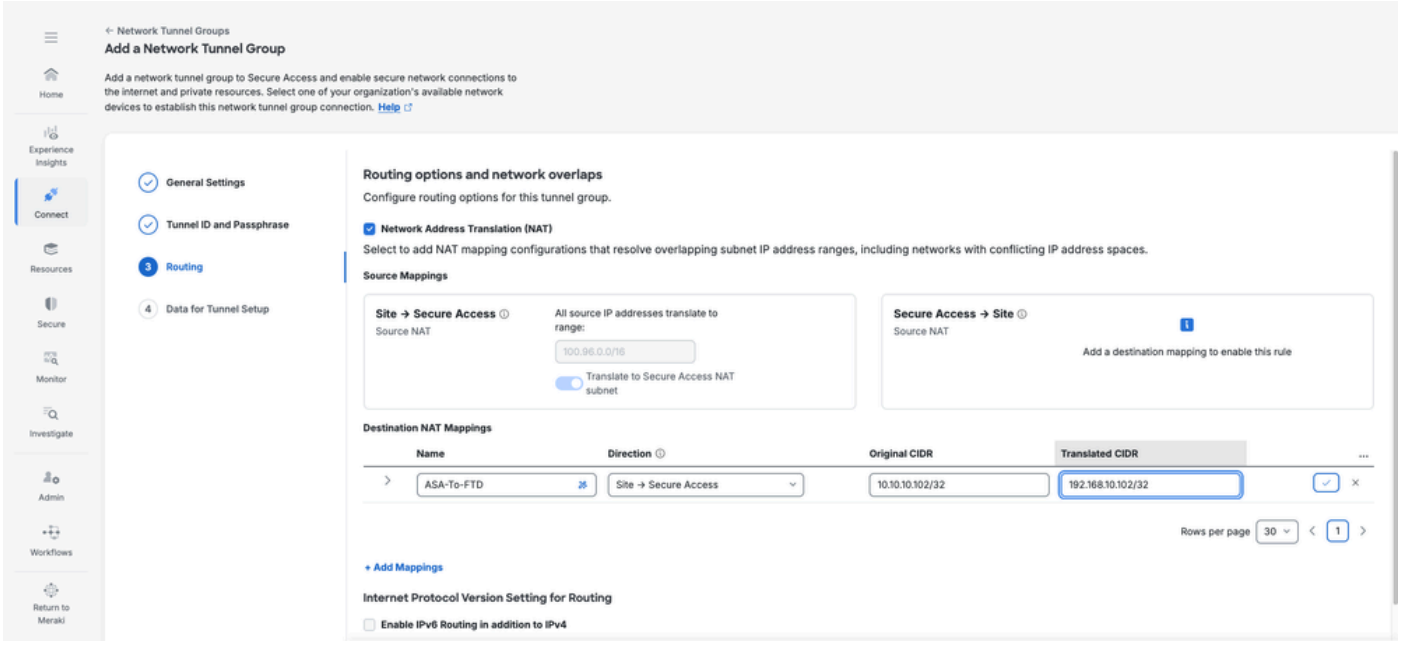


Secure Access - إعدادات NAT لمجموعات النفق للشبكة

6. إضافة تعيين NAT للوجهة

التدفق 1 - الموجه 1 إلى الموجه 2 (الموقع إلى الوصول الآمن)

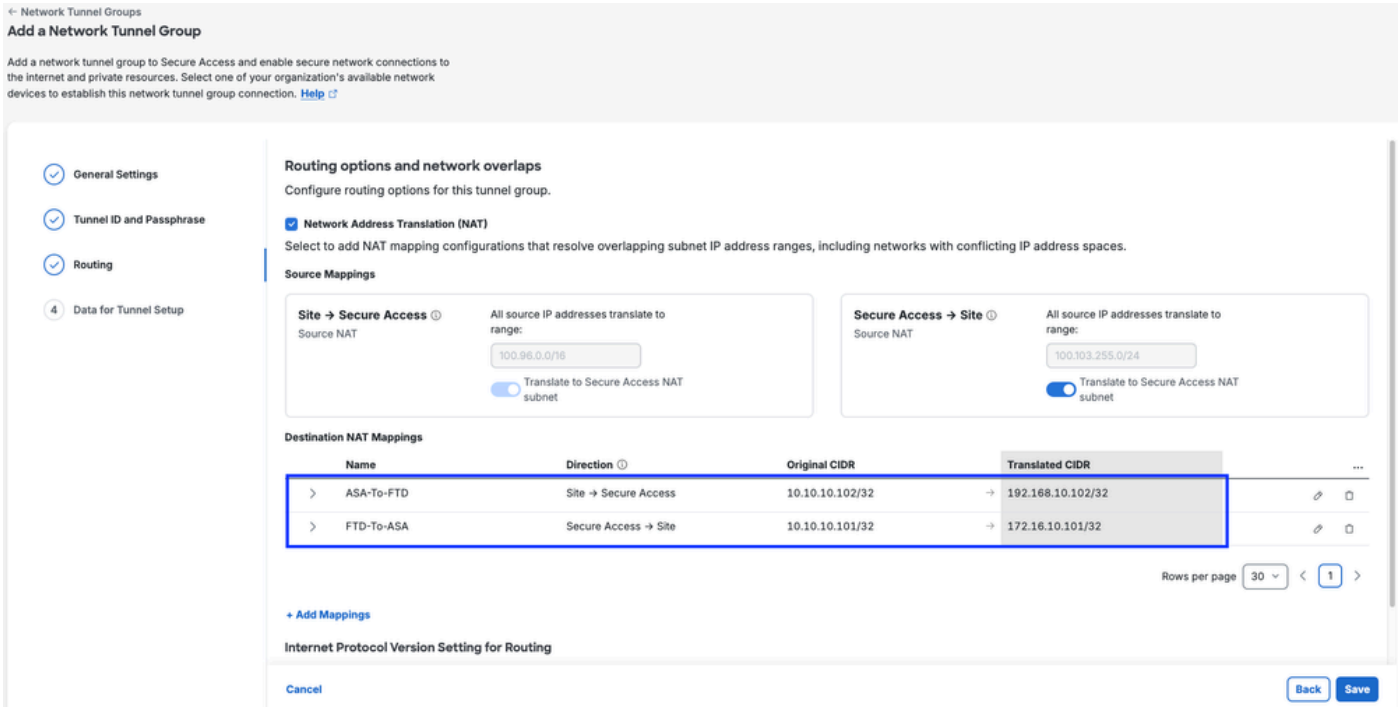
(الوصول الآمن إلى الموقع) 1 موجه 2 إلى الموجه 2 - التدفق



Secure Access - إعدادات NAT لمجموعات النفق للشبكة

تحذير: عند تمكين NAT، الا يكون BGP ممكنا . أيضا، شكلت VPN ساكن إستاتيكي
على زبون حافة أداة أيضا

تلميح: تذكر دائما إختبار اتصال IP المترجم .
يترجم IP في يترجم CIDR و حقيقي IP يذهب في الأصلي CIDR.



Secure Access - إعدادات NAT لمجموعات النفق للشبكة

انقر فوق Save

تلميح: بالنسبة لحركة المرور التي تنتقل من "الموقع أ" إلى "الموقع ب"، فإن إتجاه وجهة النظر CNHE-1 هو "Site-> SecureAccess"
بالنسبة لحركة المرور التي تنتقل من "الموقع ب" إلى "الموقع أ"، يكون إتجاه وجهة نظر CNHE-1 هو "SecureAccess -> Site"

تكوين VPN على ASA

1. سجل الدخول إلى ASA CLI، وأدخل وضع التمكين وتحقق من اتصال IP الأساسي باتجاه الإنترنت

```
ASA# sh ip
عناوين IP للنظام:
طريقة قناع شبكة IP الفرعية لعنوان اسم الواجهة
GigabitEthernet0/0 خارج دليل 192.168.1.40 255.255.255.0
GigabitEthernet0/1 داخل دليل 10.10.10.1 255.255.255.0

عناوين IP الحالية:
طريقة قناع شبكة IP الفرعية لعنوان اسم الواجهة
GigabitEthernet0/0 خارج دليل 192.168.1.40 255.255.255.0
```

255.255.255.0 10.10.10.1 لخاد دلي GigabitEthernet0/1

ASA# ping 8.8.8
.كتب تسلسل الهروب للإجهاض
:إرسال أصداء بروتوكول ICMP سعة 5 و 100 باي إلى 8.8.8.8، المهلة هي ثانيتان
!!!!!
= نسبة النجاح هي 100 بالمائة (5/5)، الحد الأدنى/المتوسط/الحد الأقصى للرحلة المستديرة 20/28/30 ملي ثانية
ASA#

2. تكوين سياسة IKEv2 وتمكين IKEv2 على الواجهة الخارجية

crypto ikev2 policy 10
aes-gcm-256 تشفير
integrity null
group 19
prf sha512
lifetime seconds 86400
crypto ikev2 enable outside

3. تكوين مقترح IPSec

crypto ipsec ikev2 ipsec-proposal ipSec-primary
protocol esp encryption aes-GCM-256

4. تكوين ملف تعريف IPsec

ipsec-proposal ipSec-primary إلى CSA-profile الأساسي للتشفير
set ikev2 IPsec الأساسي لـ IPsec IKEv2 إعداد مقترح
set ikev2 <primary tunnel-id> معرف البريد الإلكتروني للهوية المحلية

5. قم بتكوين "مجموعة النفق" وتمكين بروتوكول IKEv2 تحت السمة.

group-policy csa-policy-basic internal
group-policy csa-policy-group-policy attributes
vpn-tunnel-protocol ikev2

6. تكوين مجموعة النفق.

tunnel-group 44.228.138.150 type ipsec-l2l
tunnel-group 44.228.138.150 general-attributes

افتراضي-group-policy csa-policy-primary
سمات بروتوكول الإنترنت Tunnel-group 44.228.138.150
<pre-shared-key> اقبس مشترك مفتاح مشترك عن بعد مصادقة IKEv2
<اقبس مشترك مفتاح مشترك> مفتاح مشترك مسبق لمصادقة محلية IKEv2

7. تكوين واجهة النفق الظاهرية (VTI)

- وه كان خيارك إذا
- ASA على عكس أي واجهة أخرى يجب أن تتداخل عنوان IP المعين إلى VTIs مع
- مصدر النفق الواجهة الخارجية لجدار الحماية
- تحديد موقع النفق عنوان IP لمركز البيانات

نفق الواجهة 1
VTI-1 فيميان
عنوان IP 169.254.2.1 255.255.255.252
واجهة مصدر النفق خارج
وجهة النفق 44.228.138.150
قفل عضو النفق لبروتوكول IPv4
ملف تعريف CSA-profile الأساسي لحماية النفق

8. قم بتكوين التوجيه بطريقة يتم بها توجيه حركة المرور إلى عنوان IP المعين أو
.VTI. الرمحلة التالية تحتاج إلى ب ip ضمن مدى VTI. الشبكة الفرعية داخل واجهة VTI.

5. (للإساءة الإنترنت وأ تجمع RAPN وأ حركة مرور CGNAT القطريق VTI-1 0.0.0.0.0.0 169.254.2.2

وأ

Route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

التوجيه القائم على السياسة

1. قائمة الوصول

أي Access-list PBR IP 10.10.10.0 255.255.255.0 لـ عوسم الحامل

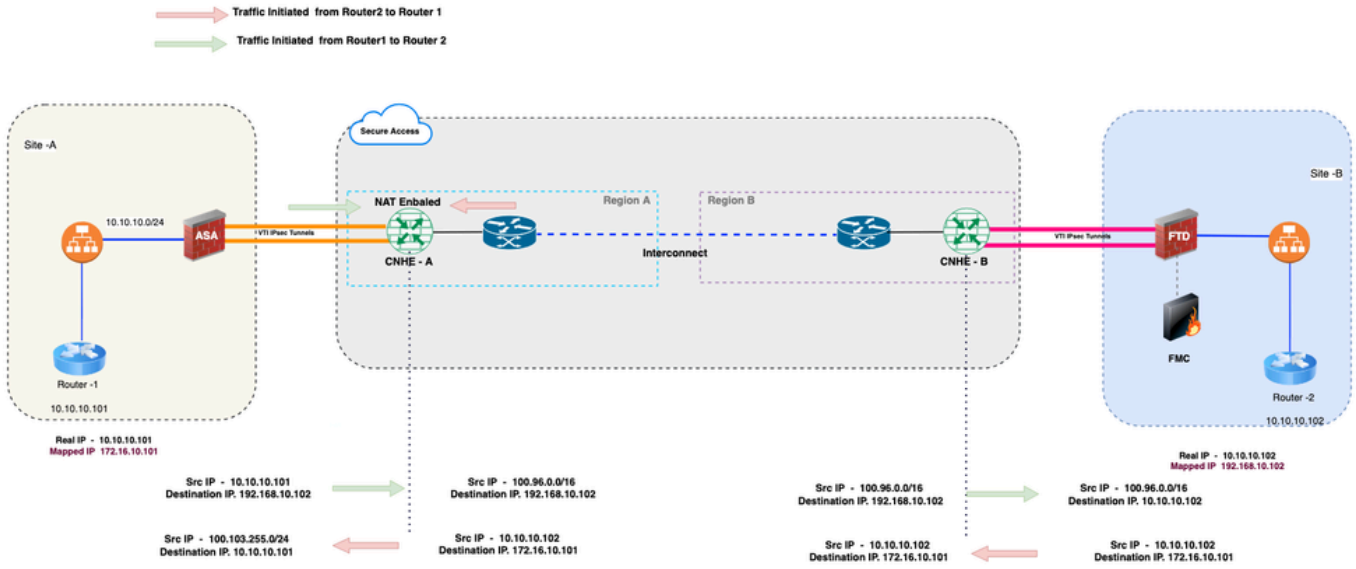
2 - خريطة القطريق

10 قطريق خريطة الخاص بـ RM-CSA تصريح
عنوان IP PBR مطابقة
169.254.2.2 169.254.2.6 التالية القوطة set ip

3. تطبيق خريطة المسار على واجهة الدخول

interface GigabitEthernet0/1
إسم داخل
100 من المستوى الأمني
ip address 10.10.10.1 255.255.255.0
policy-route-map RM-CSA

التحقق من الصحة



واجهة الموجه وحالة إمكانية الوصول إلى GW

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.101   YES NVRAM  down                  down
GigabitEthernet2       10.10.10.101    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet9       unassigned      YES unset  administratively down down
Router1#ping  10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

إختبار Ping - 1. الموجه --> الموجه 2- إختبار

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

التقاط الحزمة على ASA (FW محلي)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

   1: 10:56:45.024244       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.231143       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232470       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441856       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443122       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652477       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653423       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875397       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876450       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082301       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 10:56:45.024458       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.230914       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232516       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441795       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443153       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652432       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653454       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875351       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876480       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082240       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

التقاط الحزمة على FTD (FW عن بعد)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

10 packets captured

   1: 16:06:41.122292       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124856       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.329557       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330442       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546327       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547106       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752036       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752814       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.967891       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968501       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:06:41.123299       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124825       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.330000       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330396       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546800       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547090       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752448       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752783       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.968242       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968486       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
```

الموجه 1 <— الموجه 2 اتصال إختبار - .2 الاختبار

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.10.10.102    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

التقاط حزمة FTD (FW المحلي)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

   1: 16:11:45.622450       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823825       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825762       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045667       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046857       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252321       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253572       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453803       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454764       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664119       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:11:45.622083       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823886       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825442       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045697       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046582       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252352       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253313       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453849       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454596       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664150       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
```

التقاط حزمة ASA (FW بعيد)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

   1: 11:08:30.288391       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289123       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504566       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.504963       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710992       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711404       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917112       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917402       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128243       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128640       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 11:08:30.287964       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289322       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504505       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.505009       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710961       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711434       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917066       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917417       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128197       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128685       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```

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).