تكوين شبكة VPN من موقع إلى موقع على موجهات سلسلة RV34x

الهدف

الهدف من هذا المستند هو إنشاء شبكة VPN من موقع إلى موقع على موجهات سلسلة RV34x.

المقدمة

تعد الشبكة الخاصة الظاهرية (VPN) طريقة رائعة لربط العاملين عن بعد بشبكة آمنة. تسمح الشبكة الخاصة الظاهرية (VPN) للمضيف البعيد بالعمل كما لو كان متصلا بالشبكة الآمنة في الموقع. في شبكة VPN من موقع إلى موقع، يتصل الموجه المحلي في موقع واحد بموجه بعيد من خلال نفق شبكة VPN. يقوم هذا النفق بتضمين البيانات بشكل آمن باستخدام تقنيات التشفير والمصادقة المتوافقة مع معايير الصناعة لتأمين البيانات التي يتم إرسالها.

يتضمن تكوين شبكة VPN من موقع إلى موقع إعداد ملف تعريف IPsec وتكوين شبكة VPN من موقع إلى موقع على الموجهين. تم تكوين ملف تعريف IPsec بالفعل لتسهيل إعداد شبكة VPN من موقع إلى موقع، حتى مع جهة خارجية (مثل AWS أو Azure). يحتوي ملف تعريف IPsec على جميع التشفير اللازم للنفق. يقصد ب VPN من موقع إلى موقع التكوين حتى يعرف الموجه أي موقع آخر يتصل به. إذا أخترت عدم إستخدام ملف تعريف IPsec الذي تم تكوينه مسبقا، فلديك الخيار لإنشاء ملف تعريف مختلف.

عندما تقوم بتكوين شبكة VPN من موقع إلى موقع، لا يمكن أن تكون الشبكات الفرعية لشبكة المنطقة المحلية (LAN) على أي من جانبي النفق على الشبكة نفسها. على سبيل المثال، إذا كانت الشبكة المحلية (LAN) في الموقع A تستخدم الشبكة الفرعية ***1***.x/24.192.168، فلن يتمكن الموقع B من إستخدام الشبكة الفرعية نفسها. يجب أن يستخدم الموقع B شبكة فرعية مختلفة، مثل ***2***.x/24.192.168.

لتكوين نفق بشكل صحيح، أدخل الإعدادات المقابلة (عكس المحلي والبعيد) عند تكوين الموجهين. افترض أن هذا الموجه معرف على أنه الموجه A. أدخل إعداداته في قسم إعداد المجموعة المحلية أثناء إدخال إعدادات الموجه الآخر (الموجه B) في قسم إعداد المجموعة البعيدة. عند تكوين الموجه الآخر (B)، أدخل إعداداته في قسم "إعداد المجموعة المحلية"، وأدخل إعدادات الموجه A في "إعداد المجموعة البعيدة".

فيما يلي جدول لتكوين كل من الموجه A والموجه B. يتم التركيز بالخط الغامق على معلمات هي عكس الموجه المعاكس. تم تكوين كافة المعلمات الأخرى بنفس الطريقة. في هذا المستند، سنقوم بتكوين الموجه المحلي، الموجه A.

الحقل	**الموجه المحلي (الموجه A)** عنوان IP لشبكة WAN: 140.x.x.x عنوان بروتوكول الإنترنت الخاص (محلي): 24/192.168.2.0	**الموجه عن بعد (الموجه B)** عنوان IP لشبكة WAN: 145.x.x.x عنوان IP الخاص (محلي): 24/10.1.1.0
اسم الاتصال	VPNTest	VPNTestRemote
ملف تعريف IPsec	ملف تعريف الاختبار	ملف تعريف الاختبار
الواجهة	WAN1	WAN1
نقطة النهاية البعيدة	IP الثابت	IP الثابت
عنوان IP لنقطة	**x.x.x.145**	**x.x.x.140**

النهاية البعيدة		
مفتاح مشترك مسبقا	Cisco Test123!	Cisco Test123!
نوع المعرف المحلي	WAN IP المحلي	WAN IP المحلي
المعرف المحلي	**x.x.x.140**	**x.x.x.145**
نوع IP المحلي	شبكة فرعية	شبكة فرعية
عنوان IP المحلي	**192.168.2.0**	**10.1.1.0**
قناع الشبكة الفرعية المحلي	255.255.255.0	255.255.255.0
نوع المعرف البعيد	WAN IP عن بعد	WAN IP عن بعد
المعرف البعيد	**x.x.x.145**	**x.x.x.140**
نوع IP البعيد	شبكة فرعية	شبكة فرعية
عنوان IP البعيد	**10.1.1.0**	**192.168.2.0**
قناع الشبكة الفرعية البعيدة	255.255.255.0	255.255.255.0

الأجهزة القابلة للتطبيق

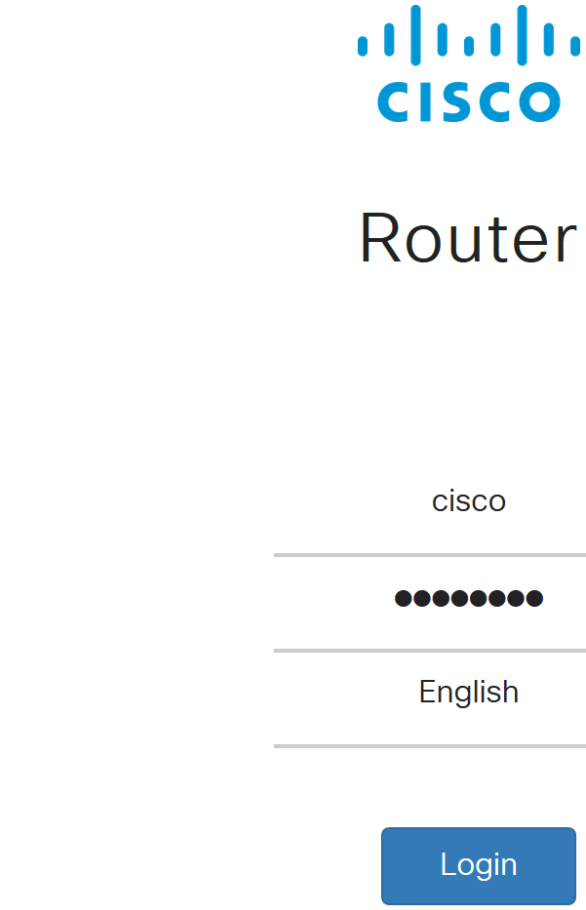
- RV34x

إصدار البرامج

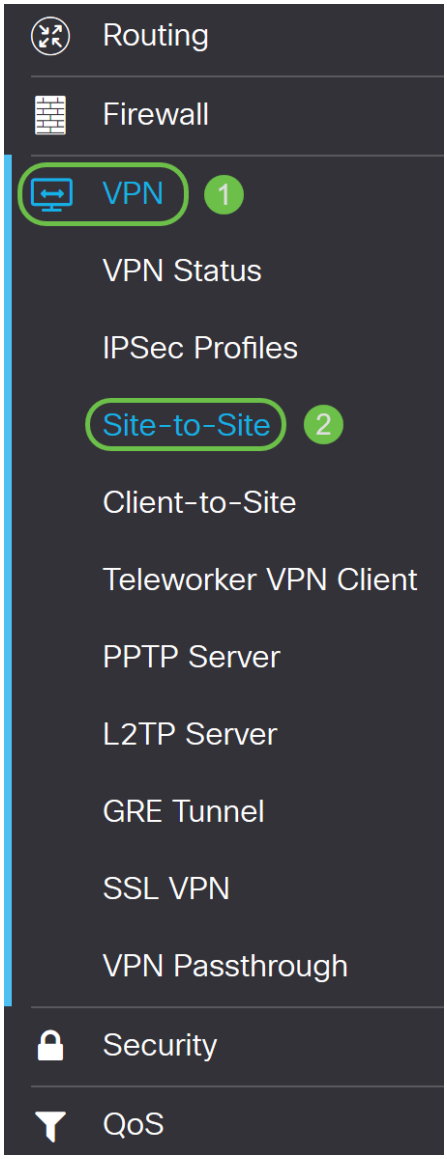
- 1.0.02.16

تكوين اتصال VPN من موقع إلى موقع

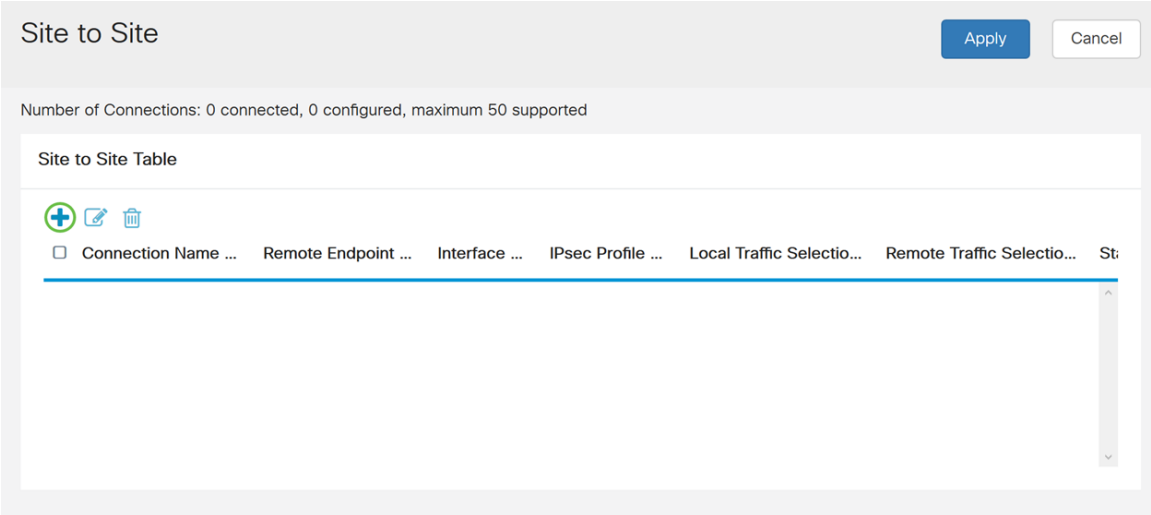
الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب الخاصة بالموجه لديك.



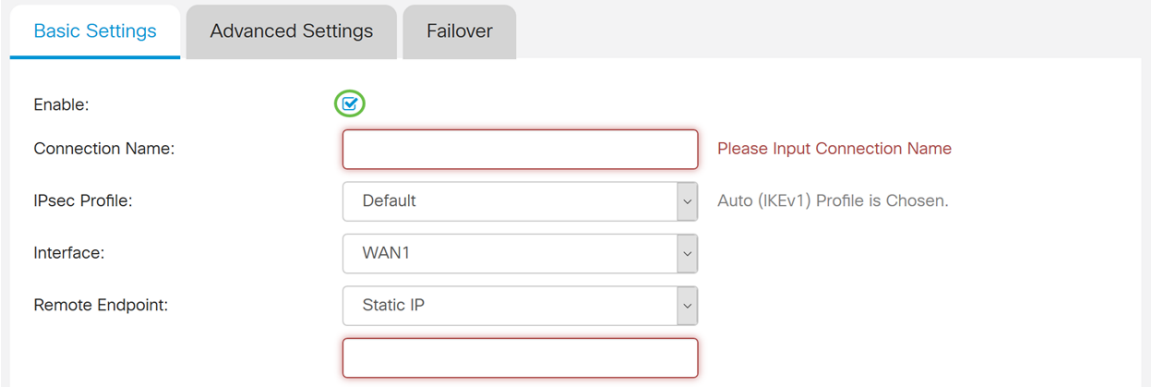
الخطوة 2. انتقل إلى **VPN > من موقع إلى موقع**.



الخطوة 3. انقر فوق الزر **إضافة** لإضافة اتصال VPN جديد من موقع إلى موقع.

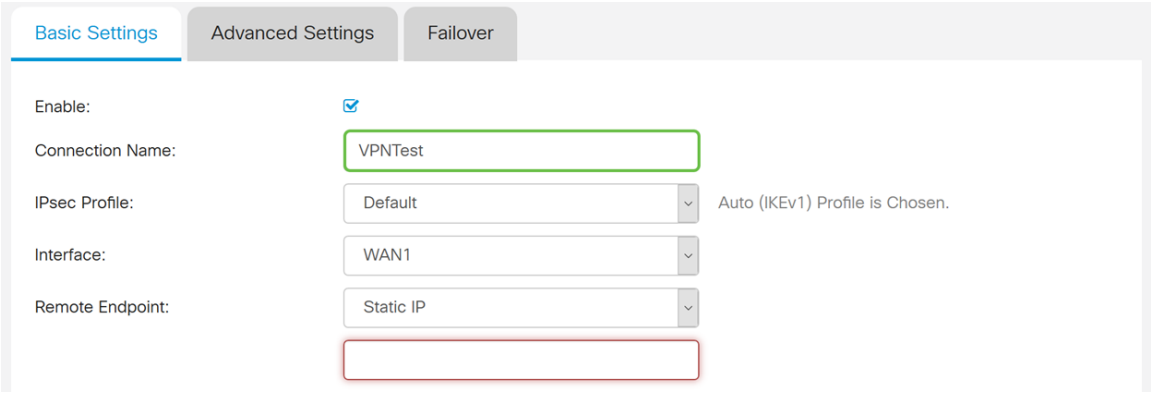


الخطوة 4. تدقيق **يمكن** أن يمكن التشكيل. مكنت هذا افتراضيا.



الخطوة 5. أدخل اسم اتصال لنفق VPN. هذا الوصف هو لأغراض مرجعية ولا يجب أن يطابق الاسم المستخدم في الطرف الآخر من النفق.

في هذا المثال، سندخل **VPNTest** كاسم اتصال لنا.

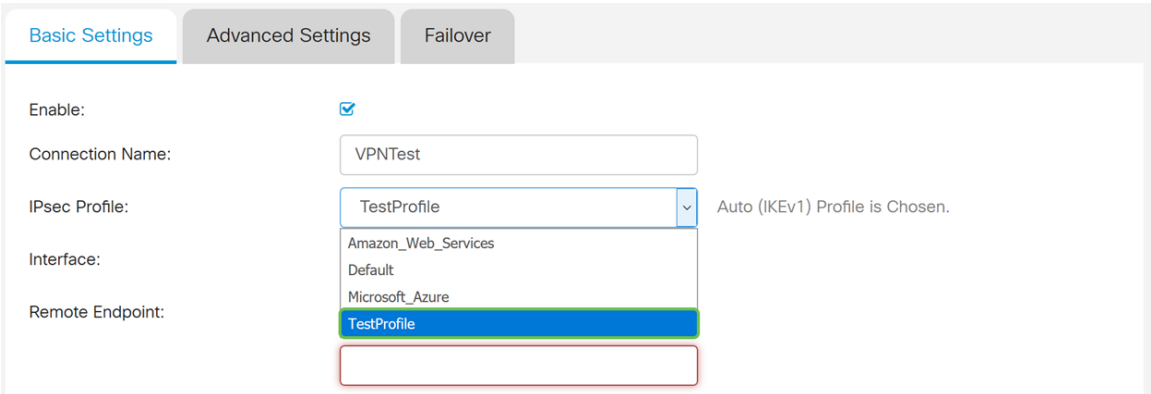


الخطوة 6. حدد ملف تعريف IPsec الذي تريد إستخدامه لشبكة VPN. يعد ملف تعريف IPsec هو التكوين المركزي في IPsec الذي يحدد الخوارزميات مثل التشفير والمصادقة ومجموعة (Diffie-Hellman (DH لمفاوضات المرحلة الأولى والمرحلة الثانية.

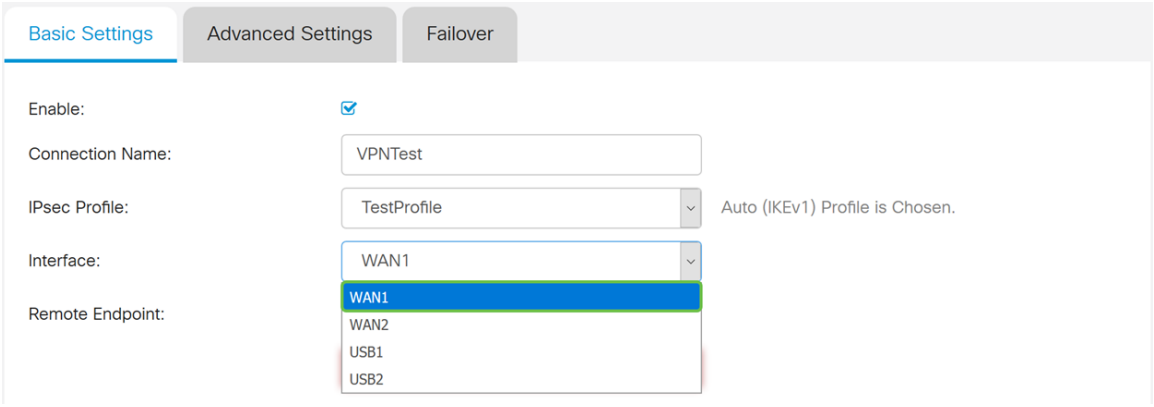
لمعرفة كيفية تكوين ملف تعريف IPsec باستخدام IKEv2، الرجاء النقر فوق الارتباط تكوين ملف تعريف IPsec باستخدام IKEv2 على RV34x.

ملاحظة: يتوفر خيار إستخدام طرف ثالث (Amazon Web Services أو Microsoft Azure) لملف تعريف IPsec. تم تكوين ملف تعريف IPsec هذا بالفعل باستخدام جميع التحديدات الضرورية التي تحتاج إلى التكوين ل Amazon Web Services أو Microsoft Azure حتى لا تضطر إلى تكوينه. إذا كنت تحاول تكوين شبكة VPN من موقع إلى موقع بين AWS أو Azure إلى موقعك، فستحتاج عندئذ إلى إستخدام المعلومات التي يمنحها لك AWS أو Azure من جانبها واستخدام ملف تعريف IPsec الذي تم تكوينه مسبقا عند تكوين شبكة VPN من موقع إلى موقع على هذا الجانب.

على سبيل المثال، سنقوم بتحديد **TestProfile** كملف تعريف IPsec الخاص بنا.

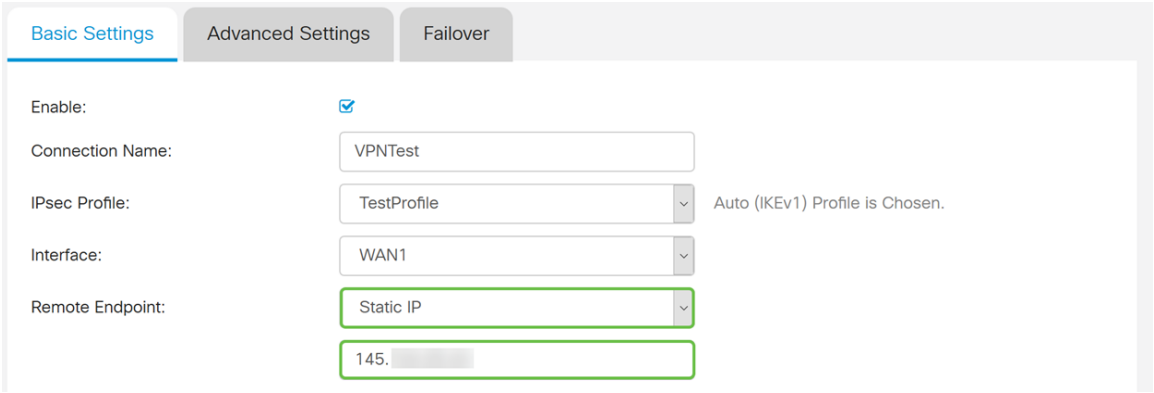


الخطوة 7. في حقل *الواجهة* ، حدد الواجهة المستخدمة للنفق. في هذا المثال، سنستخدم **WAN1** كواجهة لنا.



الخطوة 8. حدد إما **IP ثابت**، **اسم المجال المؤهل بالكامل (FQDN)**، أو **IP الديناميكي** لنقطة النهاية **البعيدة**. أدخل في عنوان IP أو FQDN لنقطة النهاية البعيدة استنادا إلى التحديد الخاص بك.

لقد حددنا **IP ثابت** ودخلنا في عنوان IP لنقطة النهاية البعيدة الخاصة بنا.



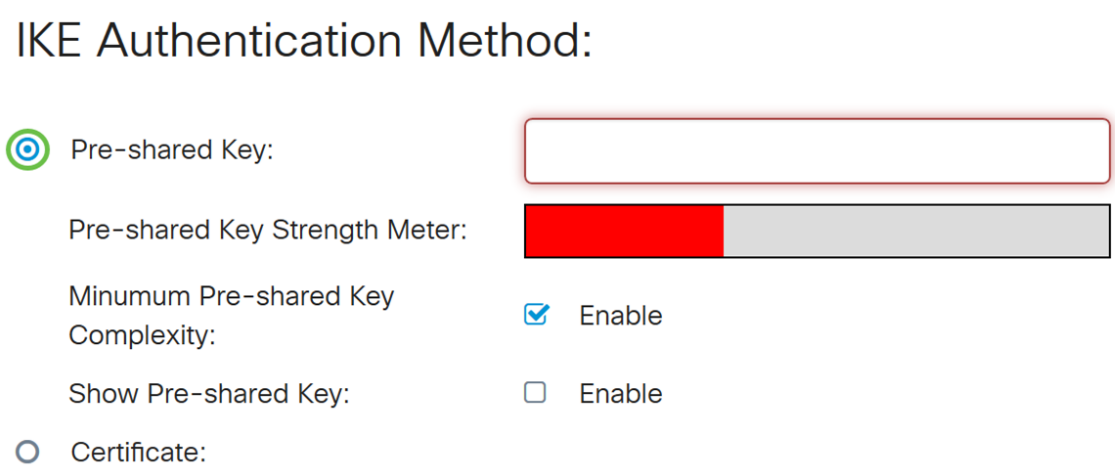
تكوين أسلوب مصادقة IKE

الخطوة 1. حدد إما **مفتاح مشترك مسبقا** أو **شهادة**.

مفتاح مشترك مسبقا: يقوم نظراء IKE بمصادقة بعضهم البعض عن طريق حساب حزمة مصنعة من البيانات تتضمن المفتاح المشترك مسبقا وإرسالها. يجب أن يشترك كلا النظيرين في نفس المفتاح السري. إذا كان النظير المتلقي قادرا على إنشاء التجزئة نفسها بشكل مستقل باستخدام المفتاح المشترك مسبقا الخاص به، فإنه يصادق النظير الآخر. لا يتم تطوير المفاتيح المشتركة مسبقا بشكل جيد لأنه يجب تكوين كل نظير IPsec باستخدام المفتاح المشترك مسبقا لكل نظير آخر يقوم بإنشاء جلسة عمل معه.

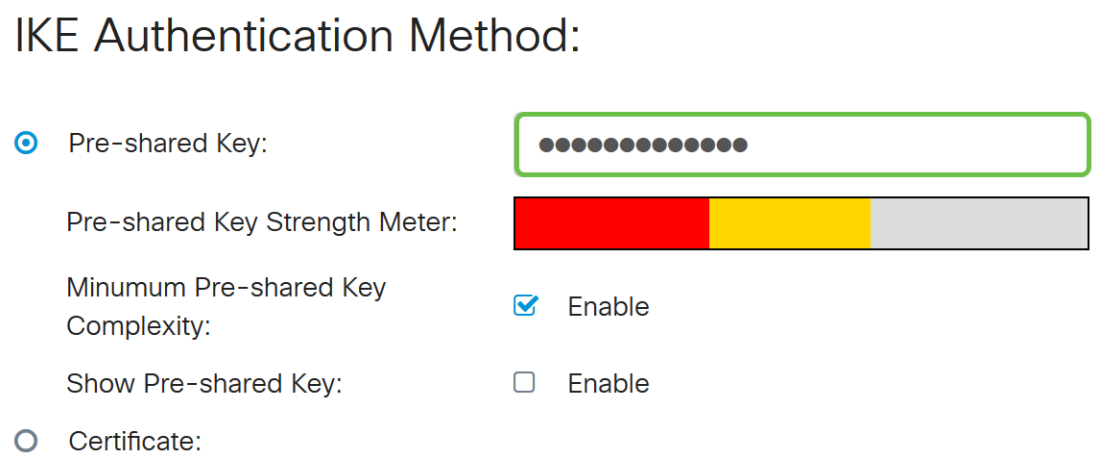
الشهادة: الشهادة الرقمية هي حزمة تحتوي على معلومات مثل هوية حامل الشهادة بما في ذلك اسم أو عنوان IP، الرقم التسلسلي للشهادة، تاريخ انتهاء صلاحية الشهادة، ونسخة من المفتاح العام لحاملها. يتم تعريف تنسيق الشهادة الرقمية القياسي في مواصفات X.509. يحدد الإصدار 3 من X.509 بنية البيانات للشهادات. إذا قمت بتحديد **شهادة**، تأكد من إستيراد شهادتك الموقعة في **الإدارة > الترخيص**. حدد الشهادة من القائمة المنسدلة لكل من المحلي والبعيد.

بالنسبة لهذا العرض التوضيحي، سنختار **المفتاح المشترك مسبقا** كطريقة مصادقة IKE.

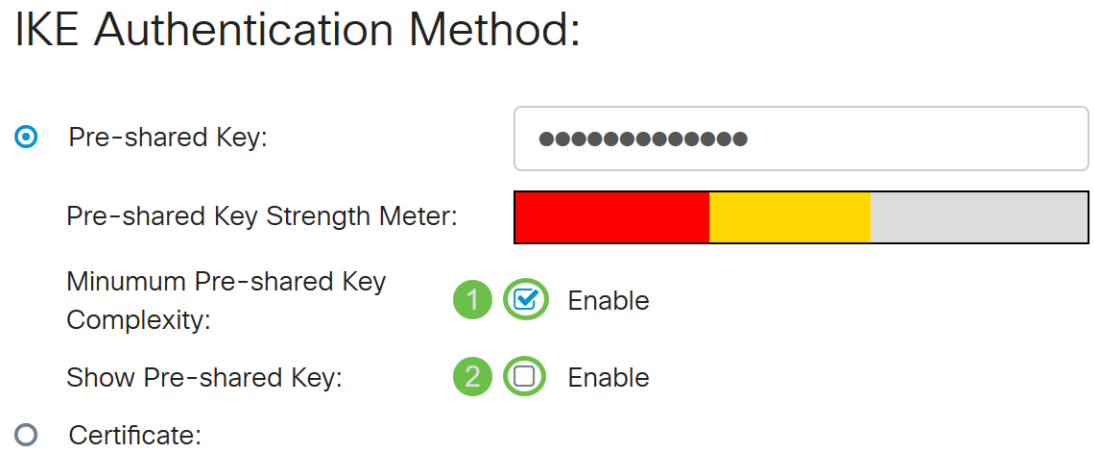


الخطوة 2. في حقل *مفتاح مشترك مسبقا*، أدخل في مفتاح مشترك مسبقا.

ملاحظة: تأكد من أن الموجه البعيد يستخدم نفس المفتاح المشترك مسبقا.

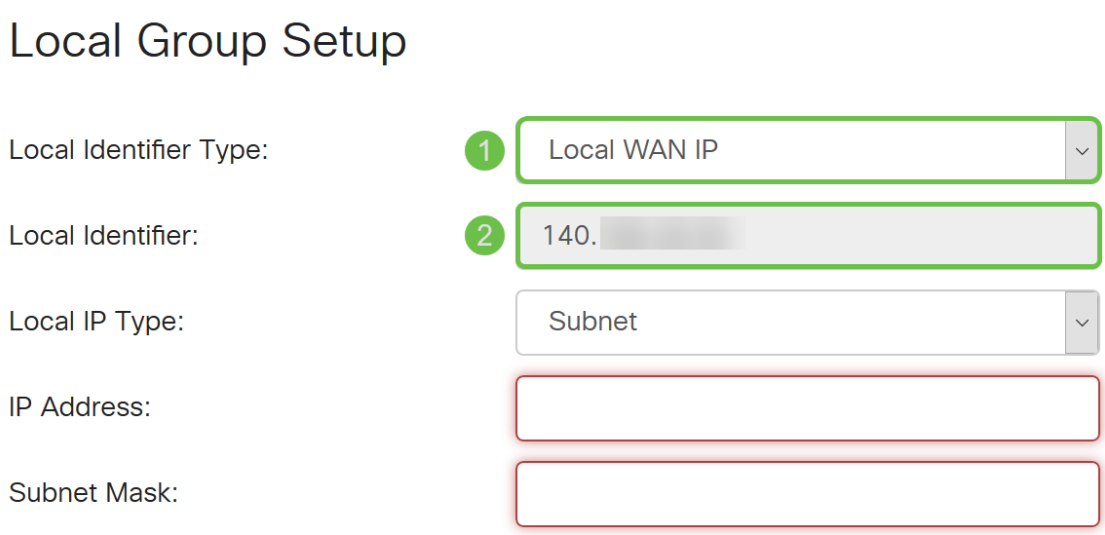


الخطوة 3. يظهر *مقياس شدة المفتاح المشترك مسبقا* قوة المفتاح المشترك مسبقا عبر الأشرطة الملونة. حدد **تمكين** لتمكين الحد الأدنى لتعقيد المفتاح المشترك مسبقا. يتم التحقق من تعقيد المفتاح المشترك مسبقا بشكل افتراضي. إذا كنت ترغب في عرض المفتاح المشترك مسبقا، فحدد خانة الاختيار **تمكين**.



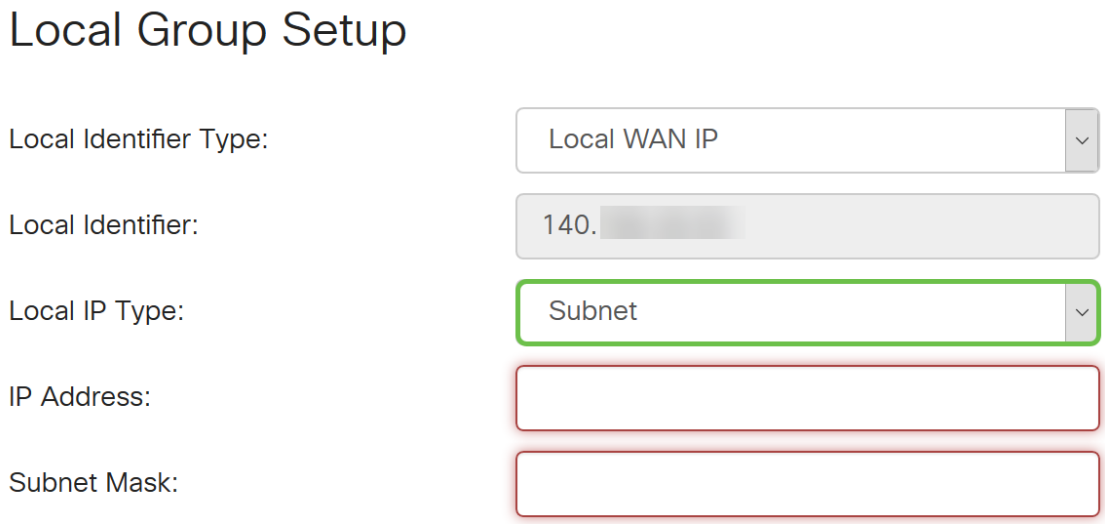
إعداد المجموعة المحلية

الخطوة 1. حدد **IP لشبكة WAN المحلية** أو **عنوان IP** أو **FQDN المحلي** أو **FQDN للمستخدم المحلي** من القائمة المنسدلة. أدخل اسم المعرف أو عنوان IP استنادا إلى التحديد الخاص بك. إذا قمت بتحديد **WAN IP المحلي**، فيجب إدخال عنوان WAN IP الخاص بالموجه لديك تلقائيا.



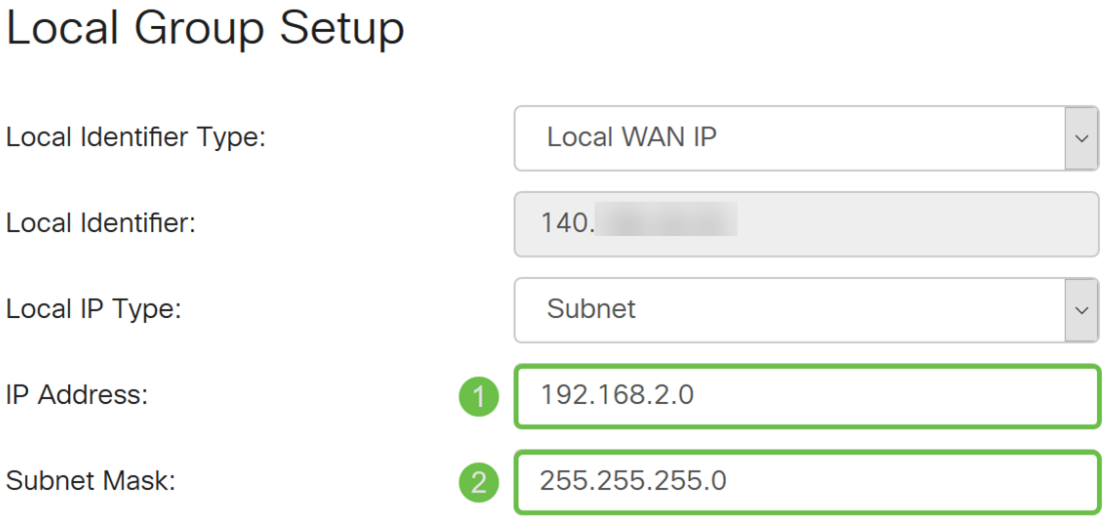
الخطوة 2. بالنسبة لنوع IP المحلي، حدد الشبكة الفرعية أوأحادي أو **أي** أو **مجموعة IP** أو واجهة GRE من القائمة المنسدلة.

في هذا المثال، تم إختيار **الشبكة الفرعية**.



الخطوة 3. دخلت العنوان من الأداة أن يستطيع استعملت هذا نفق. ثم أدخل قناع الشبكة الفرعية.

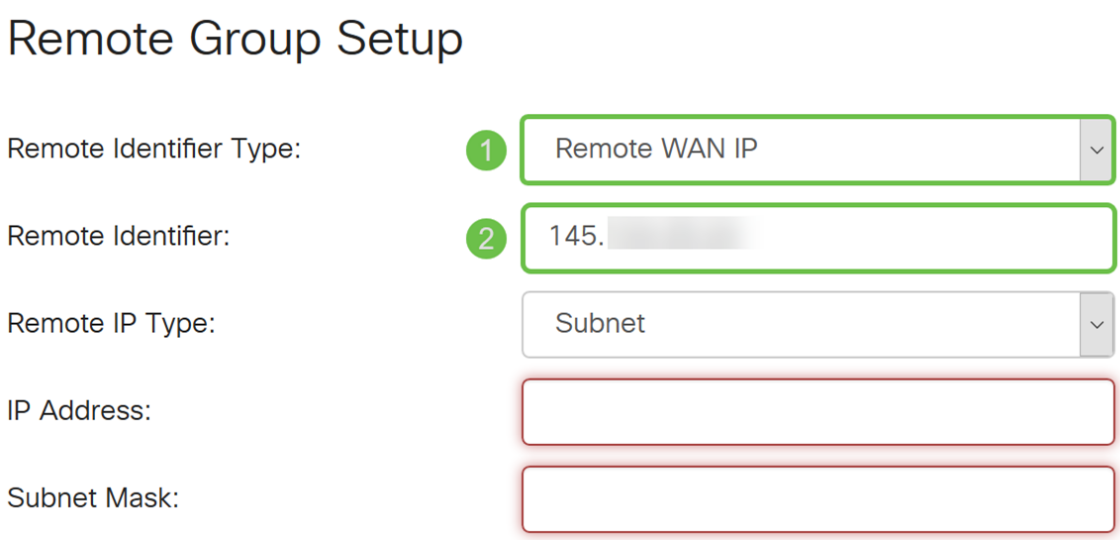
بالنسبة لهذا العرض التوضيحي، سندخل **192.168.2.0** كعنوان IP محلي لنا و**255.255.255.0** لقناع الشبكة الفرعية.



إعداد المجموعة البعيدة

الخطوة 1. حدد **IP لشبكة WAN البعيدة** أو **FQDN** البعيدة أو **FQDN للمستخدم البعيد** من القائمة المنسدلة. أدخل اسم المعرف أو عنوان IP استنادا إلى التحديد الخاص بك.

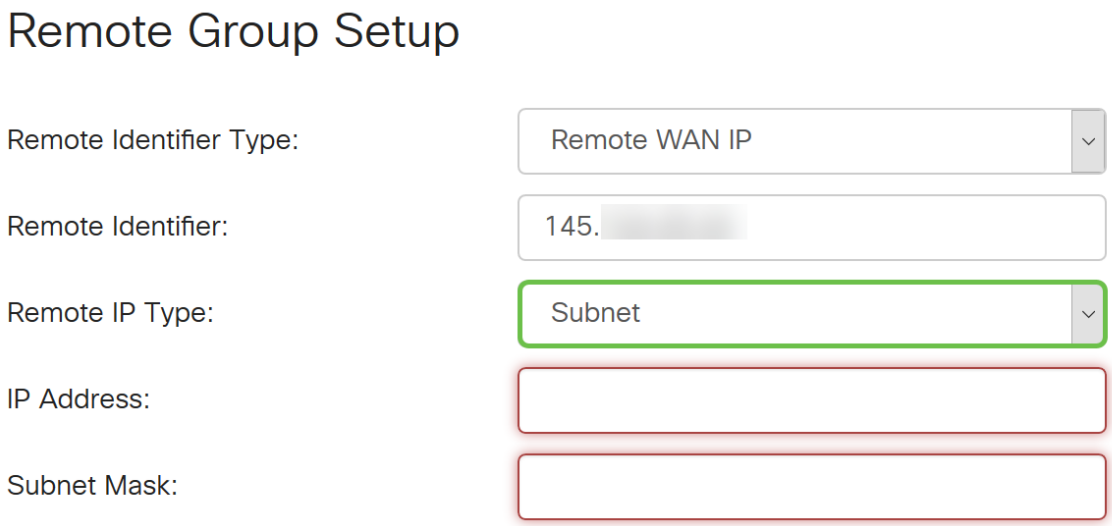
تم تحديد **IP لشبكة WAN البعيدة** كنوع *المعرف البعيد* وأدخلنا في عنوان IP الخاص بالموجه البعيد.



الخطوة 2. حدد الشبكة الفرعية، **أحادية**، **أي**، **مجموعة IP** من القائمة المنسدلة **نوع IP البعيد**.

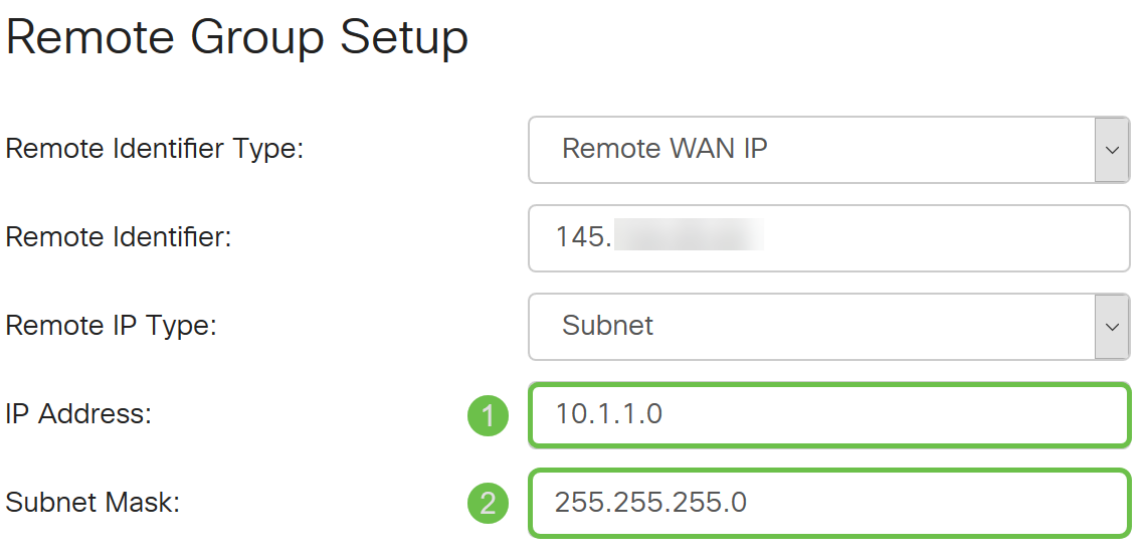
في هذا المثال، سنختار **الشبكة الفرعية**.

ملاحظة: إذا كنت قد حددت مجموعة IP كنوع IP البعيد الخاص بك، ستظهر نافذة منبثقة لإنشاء مجموعة IP جديدة.

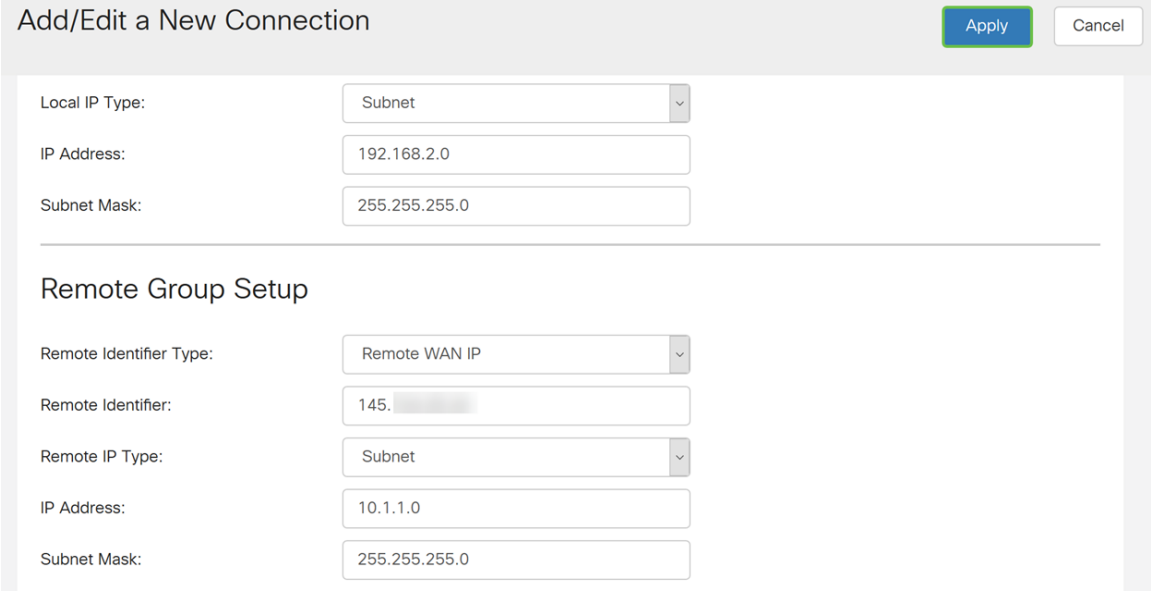


الخطوة 3. أدخل عنوان IP وقناع الشبكة الفرعية للجهاز الذي يمكن أن يستخدم هذا النفق.

لقد دخلنا **10.1.1.0** لعنوان IP المحلي البعيد الذي يمكن أن يستخدم هذا النفق وقناع الشبكة الفرعية **255.255.255.0**.



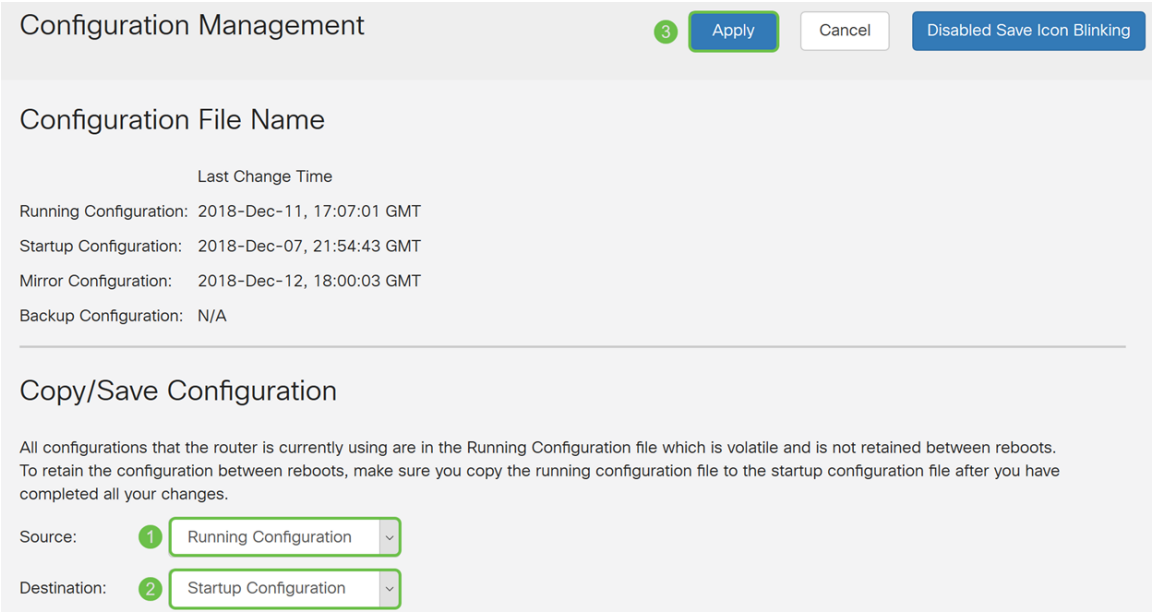
الخطوة 4. انقر فوق **تطبيق** لإنشاء اتصال VPN جديد من موقع إلى موقع.



توجد جميع التكوينات التي قمت بإدخالها على الموجه في ملف التكوين الجاري تشغيله والذي يكون متطايرا ولا يتم الاحتفاظ به بين عمليات إعادة التمهيد.

الخطوة 5. في أعلى الصفحة، انقر فوق الزر **حفظ** للتنقل إلى *إدارة التكوين* لحفظ التكوين الجاري تشغيله إلى تكوين بدء التشغيل. الغرض من ذلك هو الاحتفاظ بالتكوين بعد إعادة التمهيد.

الخطوة 6. في إدارة التكوين، تأكد من أن *المصدر* **يشغل التكوين** وأن *الوجهة* هي تكوين بدء التشغيل. ثم اضغط على **تطبيق** لحفظ التكوين الجاري تشغيله إلى تكوين بدء التشغيل. سيحتفظ ملف تكوين بدء التشغيل الآن بجميع التكوينات بعد إعادة التمهيد.



القرار

يجب عليك الآن إضافة اتصال VPN جديد من موقع إلى موقع للموجه المحلي لديك بنجاح. ستحتاج إلى تكوين الموجه عن بعد (الموجه B) باستخدام المعلومات العكسية.

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).