ASDM 6.4: قفن VPN من موقع إلى موقع مع IKEv2 نيوكت لاثم

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نفق VPN من موقع إلى موقع بين جهازي الأمان القابل للتكيف (ASAs) من Cisco باستخدام الإصدار 2 من تبادل مفتاح الإنترنت (IKE). وهو يصف الخطوات المستخدمة لتكوين نفق VPN باستخدام معالج واجهة المستخدم الرسومية (GUI) لإدارة أجهزة الأمان المعدلة (ASDM).

المتطلبات الأساسية

المتطلبات

تأكدت أن ال cisco ASA يتلقى يكون شكلت مع العملية إعداد أساسي.

المكونات المستخدمة

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

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances التي تشغل الإصدار 8.4 والإصدارات الأحدث
- برنامج Cisco ASDM، الإصدار 6.4 والإصدارات الأحدث

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

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

IKEv2، هو تحسين لبروتوكول IKEv1 الحالي الذي يتضمن هذه الفوائد:

- تقليل تبادل الرسائل بين أقران IKE
- طرق المصادقة أحادي الإتجاه
- دعم مدمج لاكتشاف النظير الميت (DPD) وتجريب NAT
- إستخدام بروتوكول المصادقة المتوسع (EAP) للمصادقة
- تقليل مخاطر الهجمات البسيطة على رفض الخدمة (DoS) باستخدام ملفات تعريف الارتباط المضادة للسحب

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

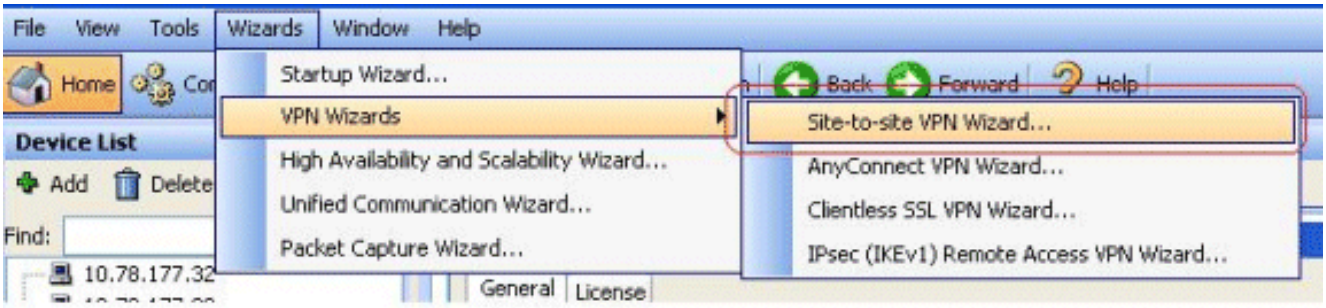
يوضح هذا المستند تكوين نفق VPN من موقع إلى موقع على HQ-ASA. ويمكن اتباع نفس الشيء كمرآة على "قاعدة بيانات آسا".

تكوين ASDM على HQ-ASA

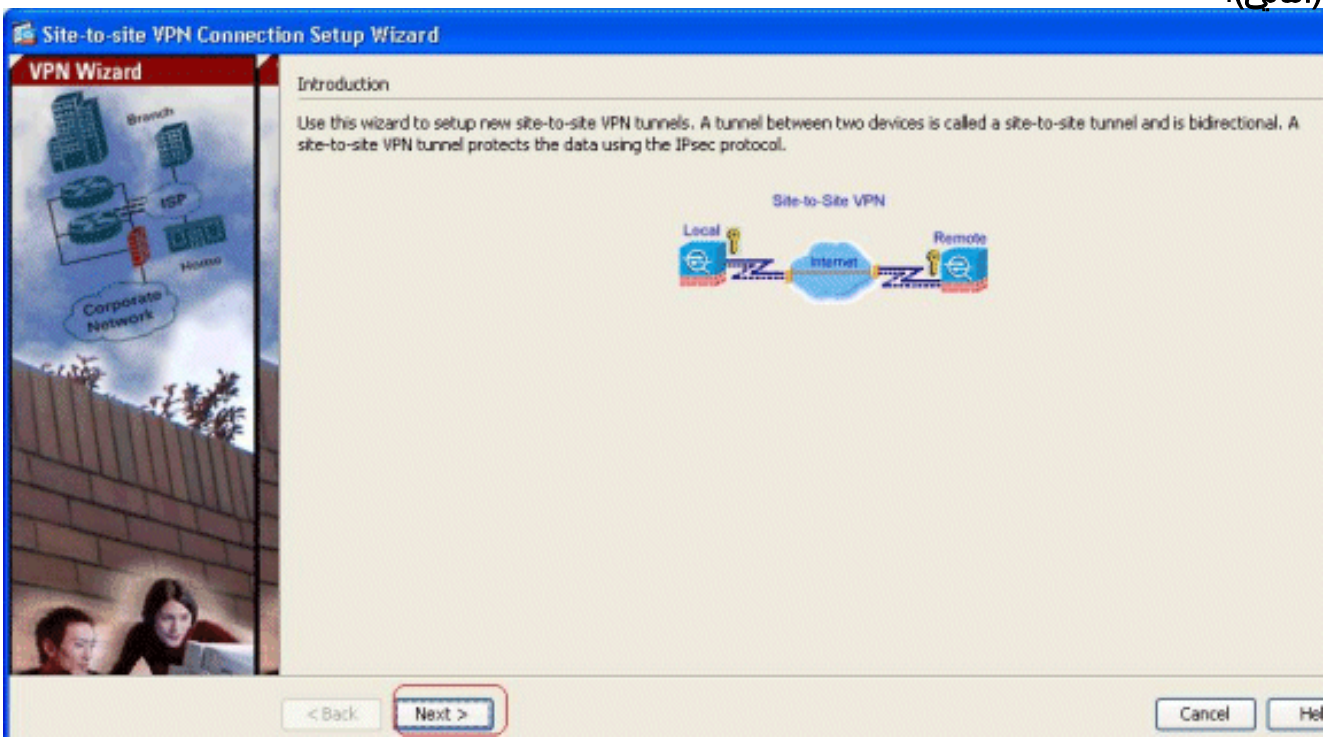
يمكن تكوين نفق VPN هذا باستخدام معالج واجهة المستخدم الرسومية (GUI) سهل الاستخدام.

أكمل الخطوات التالية:

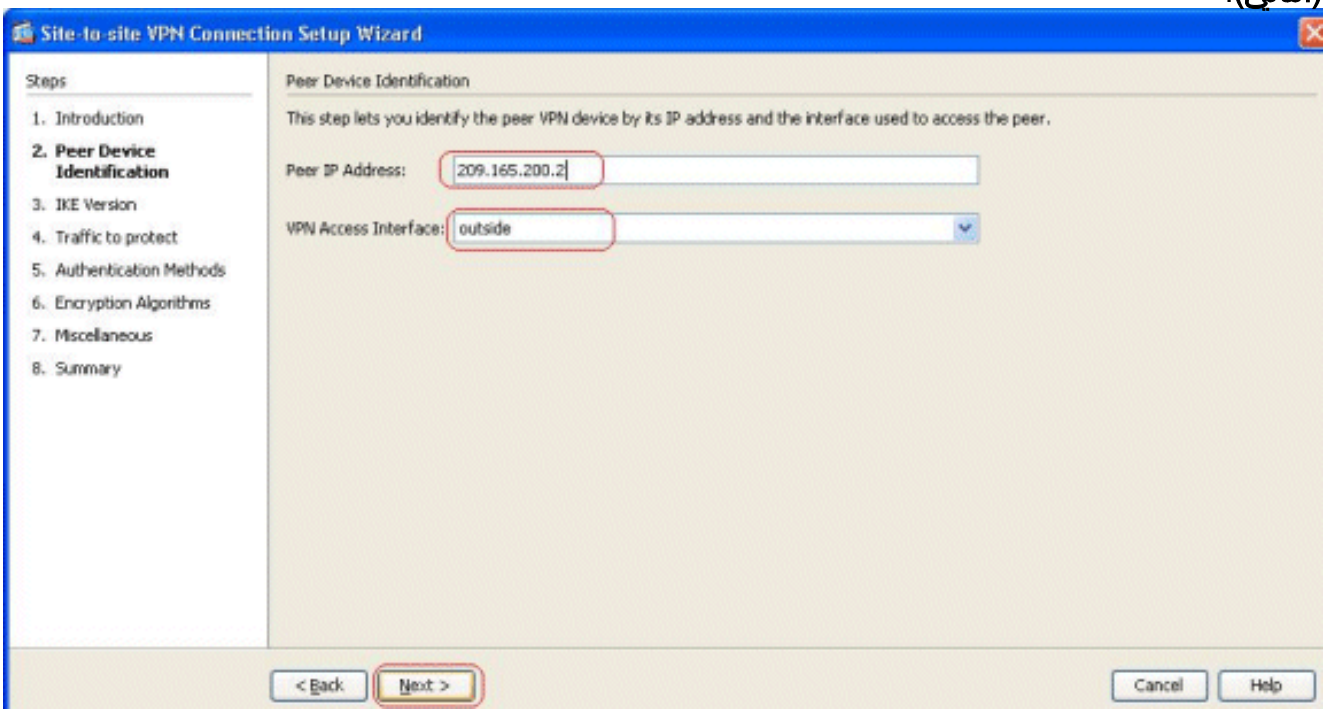
1. قم بتسجيل الدخول إلى إدارة قاعدة بيانات المحول (ASDM)، وانتقل إلى **المعالجات > معالجات VPN > معالج شبكة VPN من موقع إلى موقع**.



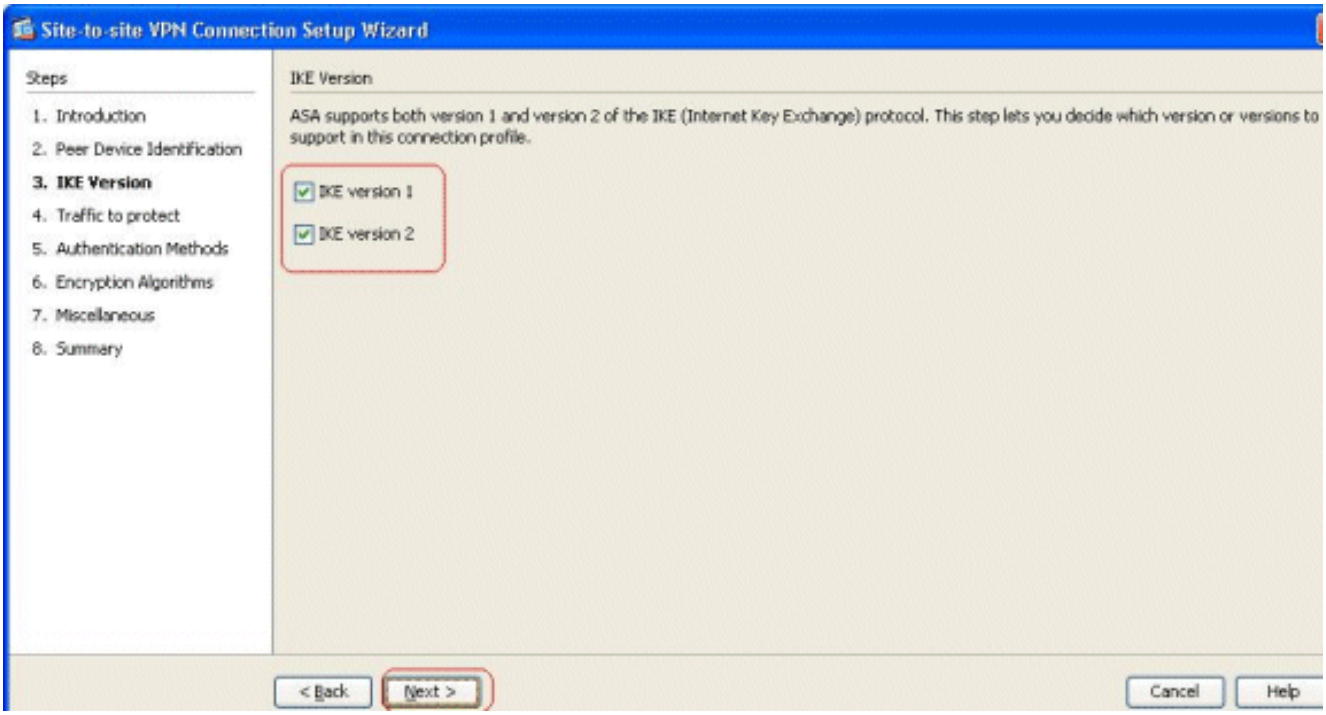
2. تظهر نافذة إعداد اتصال VPN من موقع إلى موقع. انقر فوق **Next (التالي)**.



3. حدد واجهة الوصول إلى VPN وعنوان IP للنظير. انقر فوق **Next (التالي)**.

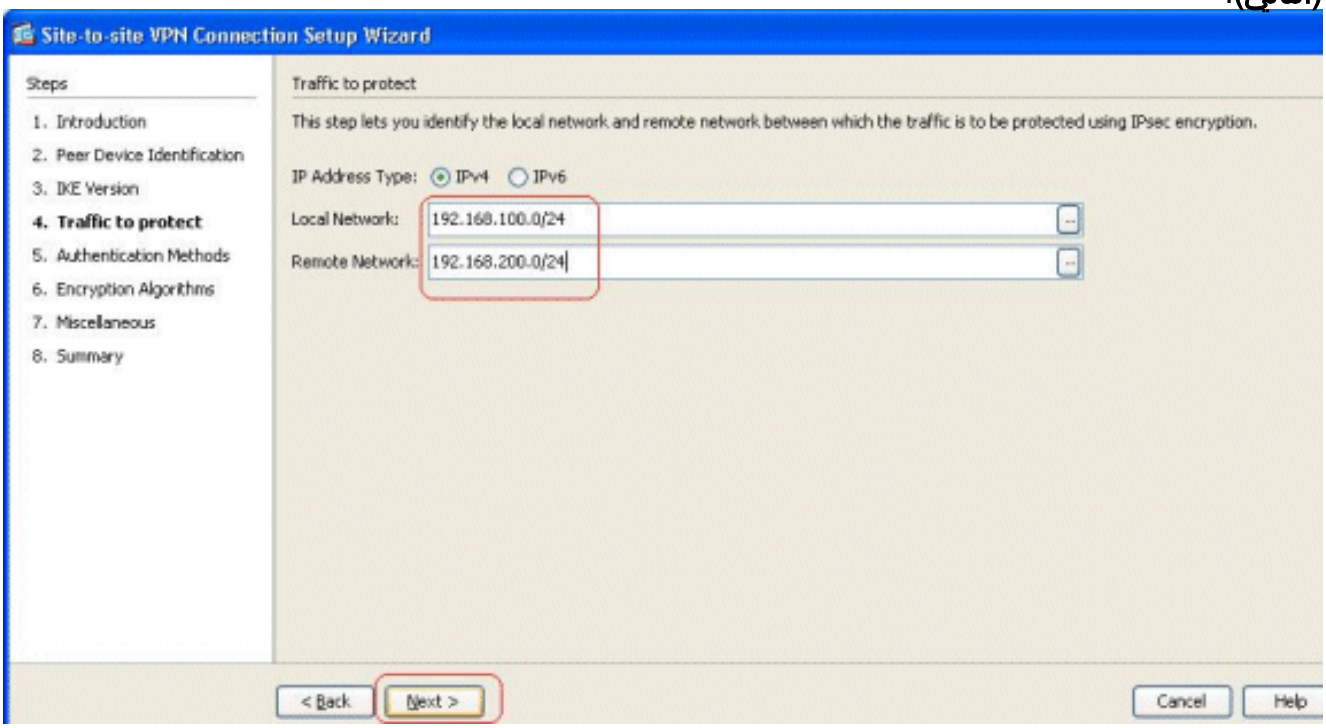


4. حدد كلا من إصداري IKE، وانقر فوق **التالي**.

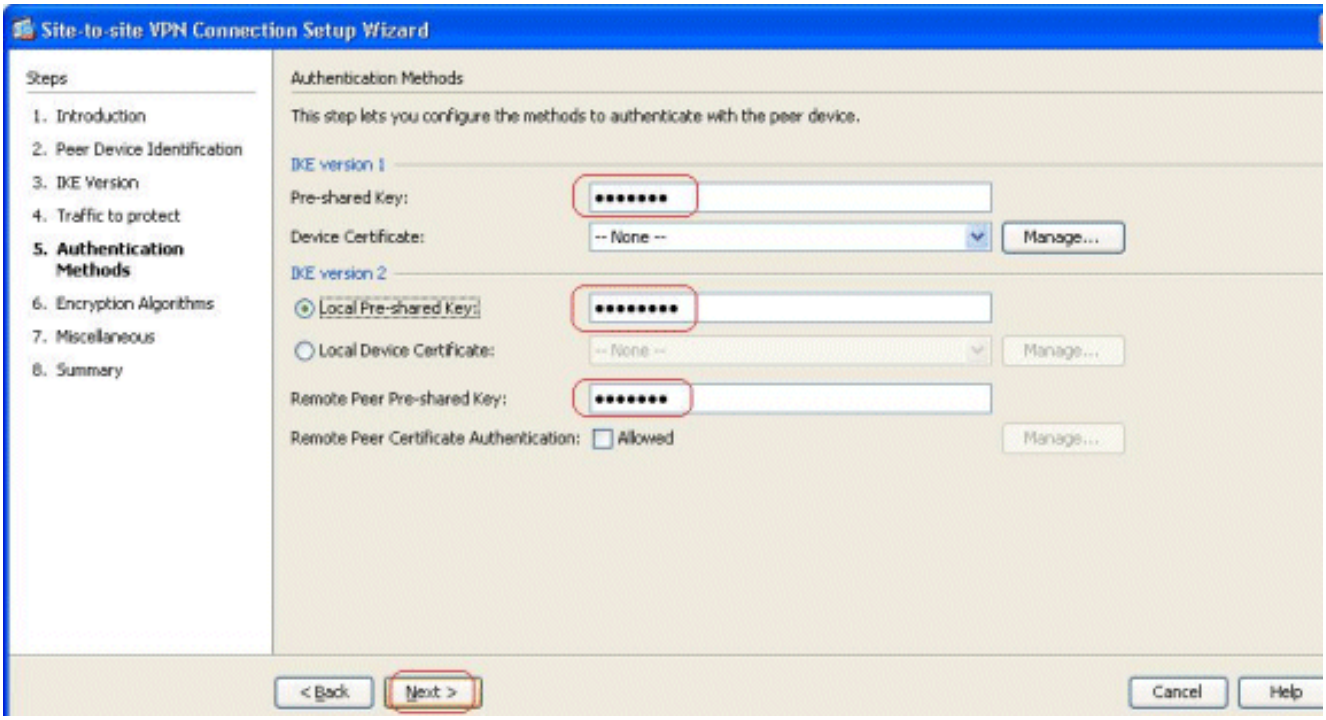


ملاحظة: تم تكوين كلا الإصدارين من IKE هنا لأن البادئ قد يكون لديه نسخة إحتياطية من IKEv2 إلى IKEv1 عند فشل IKEv2.

5. حدد الشبكة المحلية والشبكة البعيدة حتى يتم تشفير حركة مرور البيانات بين هذه الشبكات وتمريرها عبر نفق VPN. انقر فوق **Next (التالي)**.

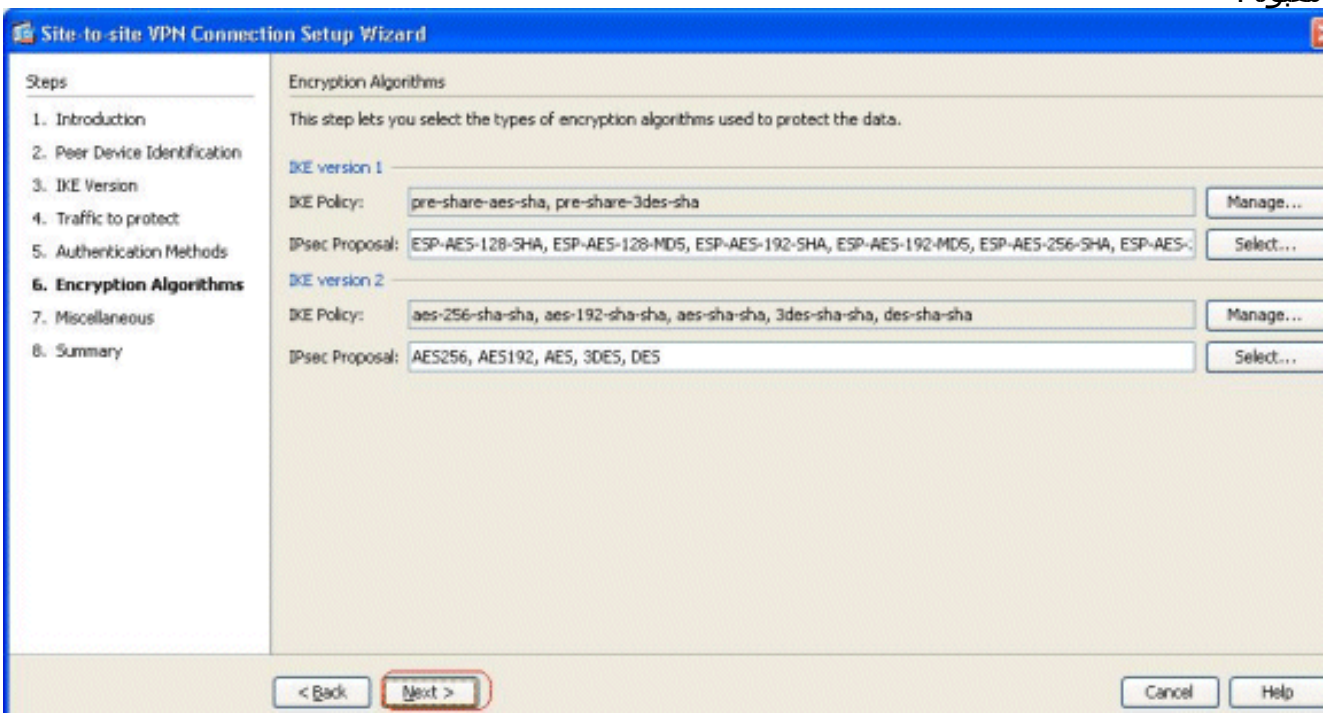


6. حدد المفاتيح المشتركة مسبقا لكل من إصداري IKE.

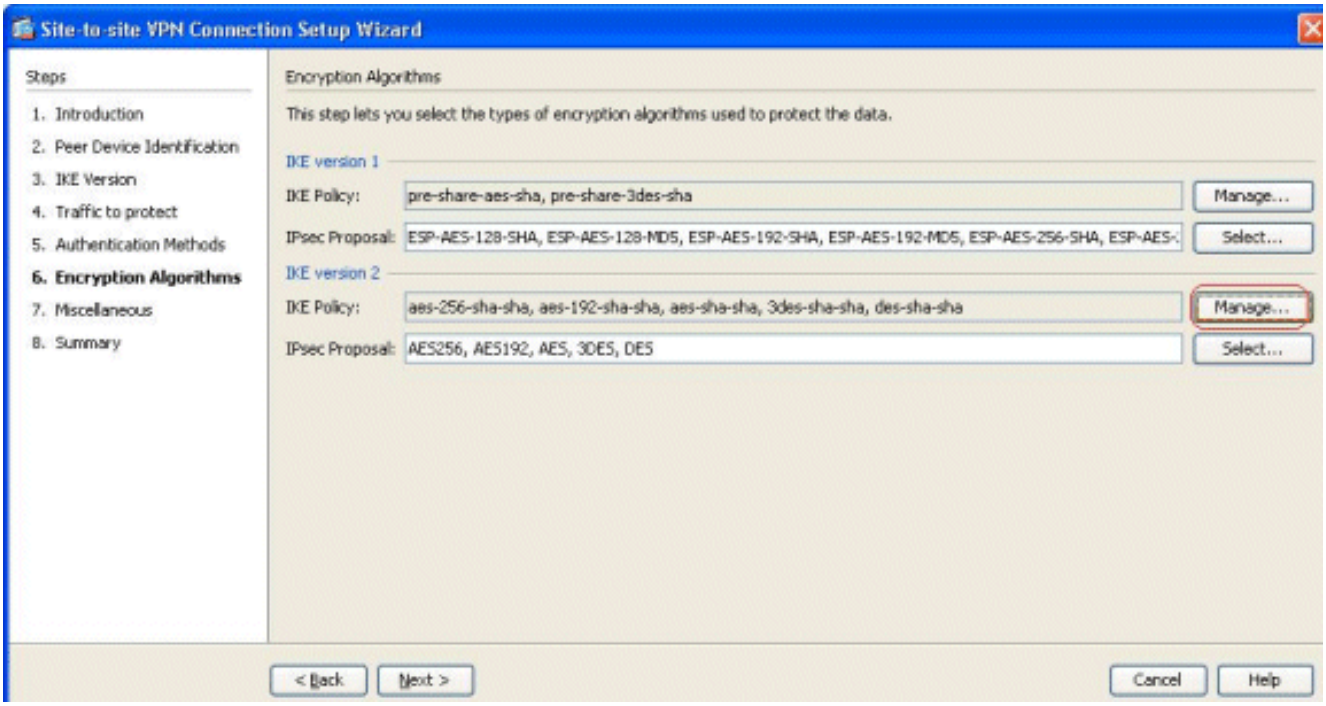


يكمن الاختلاف الرئيسي بين الإصدارين 1 و 2 من IKE في طريقة المصادقة التي تسمح بها. يسمح IKEv1 بنوع واحد فقط من المصادقة في كلا نهايتي VPN (أي إما مفتاح مشترك مسبقا أو شهادة). ومع ذلك، يسمح IKEv2 بتكوين طرق المصادقة غير المتماثلة (أي مصادقة المفتاح المشترك مسبقا للمنشئ، ومصادقة الشهادة للمستجيب) باستخدام CLIs منفصلة للمصادقة المحلية والبعيدة.علاوة على ذلك، يمكنك الحصول على مفاتيح مشتركة مسبقا مختلفة في كلا الطرفين. ويصبح المفتاح المشترك مسبقا المحلي في نهاية HQ-ASA هو المفتاح المشترك مسبقا البعيد في نهاية BQ-ASA. وبالمثل، يصبح المفتاح المشترك مسبقا عن بعد في نهاية HQ-ASA المفتاح المشترك مسبقا المحلي في نهاية BQ-ASA.

7. حدد خوارزميات التشفير لكل من الإصدارين 1 و 2 من IKE. هنا، القيم الافتراضية تكون مقبولة:



8. انقر فوق **إدارة**.. لتعديل نهج IKE.

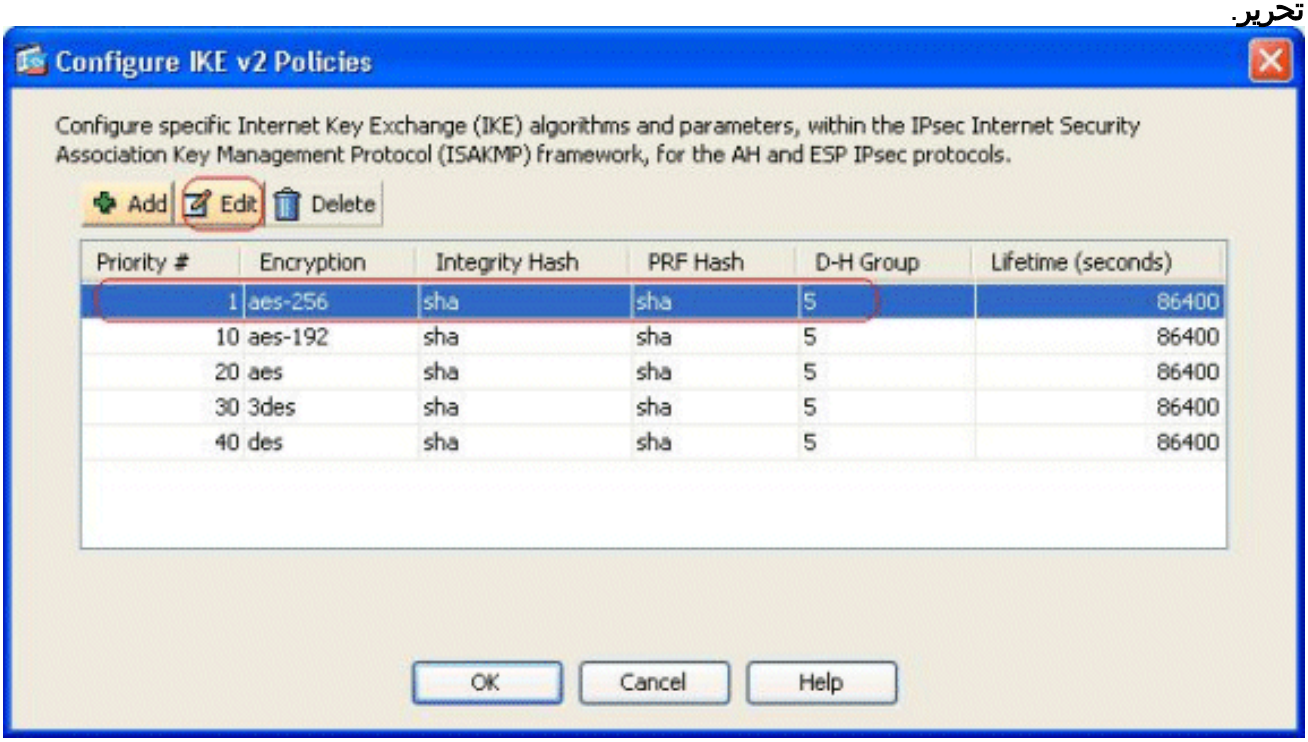


ملاحظة: نهج IKE في IKEv2 مرادف **لنهج ISAKMP** في IKEv1.**يعد مقترح IPsec** في IKEv2 مرادفا **لمجموعة التحويل** في IKEv1.

9. تظهر هذه الرسالة عندما تحاول تعديل النهج الموجود:

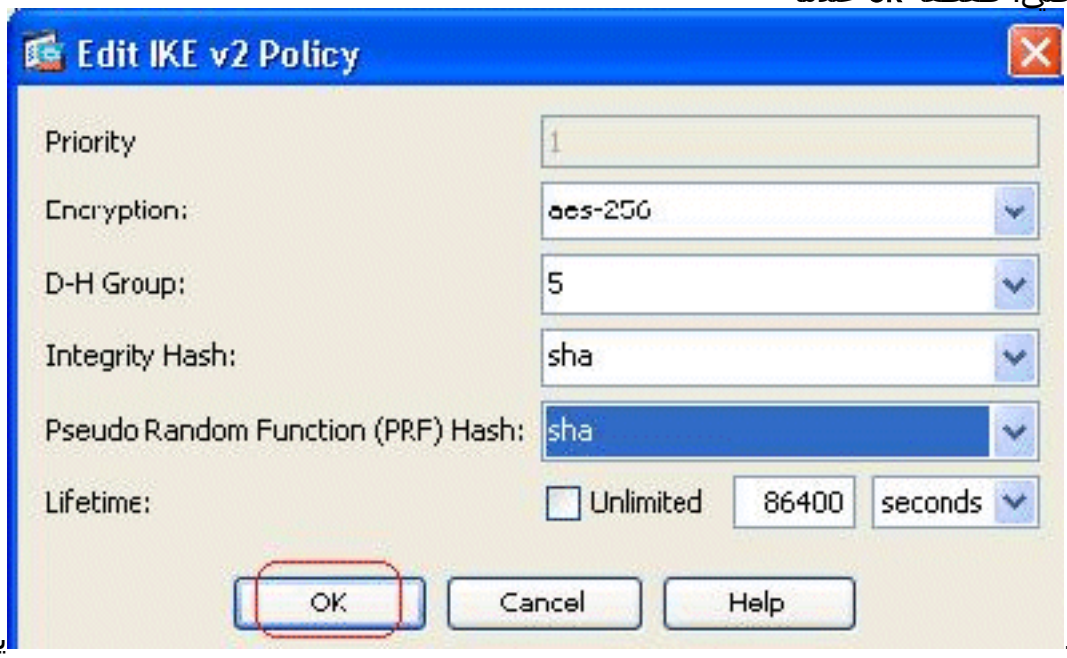
طقطقة in **ok** order to باشرت.

10. حدد نهج IKE المحدد، وانقر فوق **تحرير**.



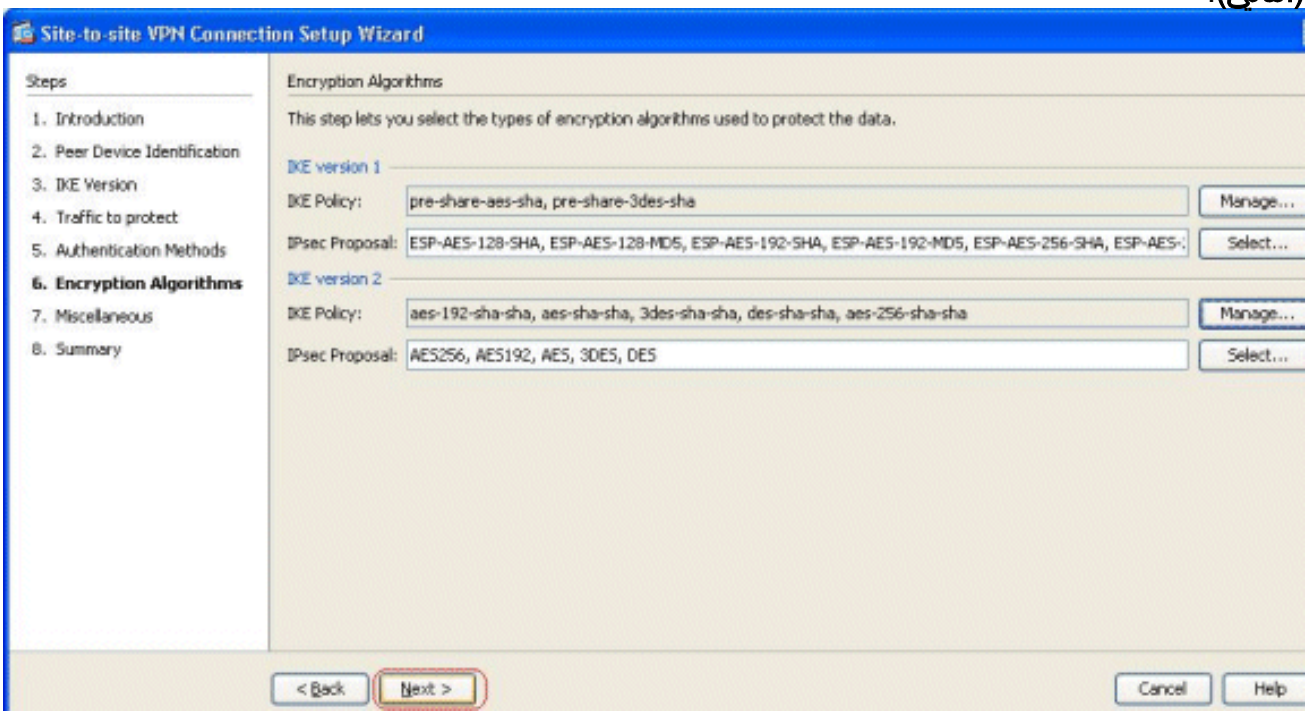
11. يمكنك تعديل المعلمات مثل الأولوية والتشفير ومجموعة D-H وتجزئة التكامل وتجزئة PRF وقيم العمر

الافتراضي. طقطقة **ok** عندما

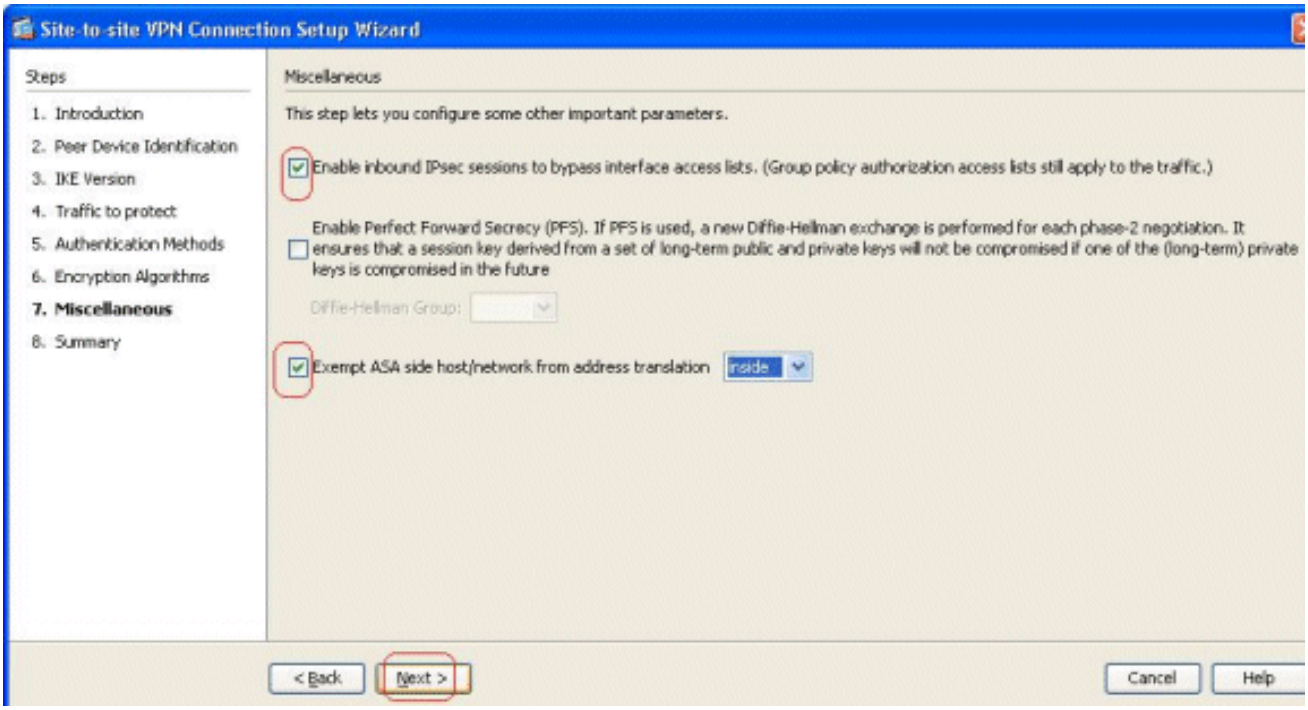


إنتهيت. يسمح IKEv2 بالتفاوض حول خوارزمية التكامل بشكل منفصل عن خوارزمية Pseudo Random Function (PRF). يمكن تكوين هذا في سياسة IKE مع الخيارات الحالية المتاحة التي تكون SHA-1 أو MD5.لا يمكنك تعديل معلمات مقترح IPsec التي تم تعريفها بشكل افتراضي. انقر فوق **تحديد** بجوار حقل مقترح IPsec لإضافة معلمات جديدة. يكمن الاختلاف الرئيسي بين IKEv1 و IKEv2، من حيث مقترحات IPsec، في أن IKEv1 يقبل مجموعة التحويل من حيث مجموعات من خوارزميات التشفير والمصادقة. يقبل IKEv2 معلمي التشفير والسلامة بشكل فردي، وأخيرا يجعل كل ذلك ممكنا أو مزيجا من هذه. يمكنك عرض هذه العناصر في نهاية هذا المعالج، في شريحة "الملخص".

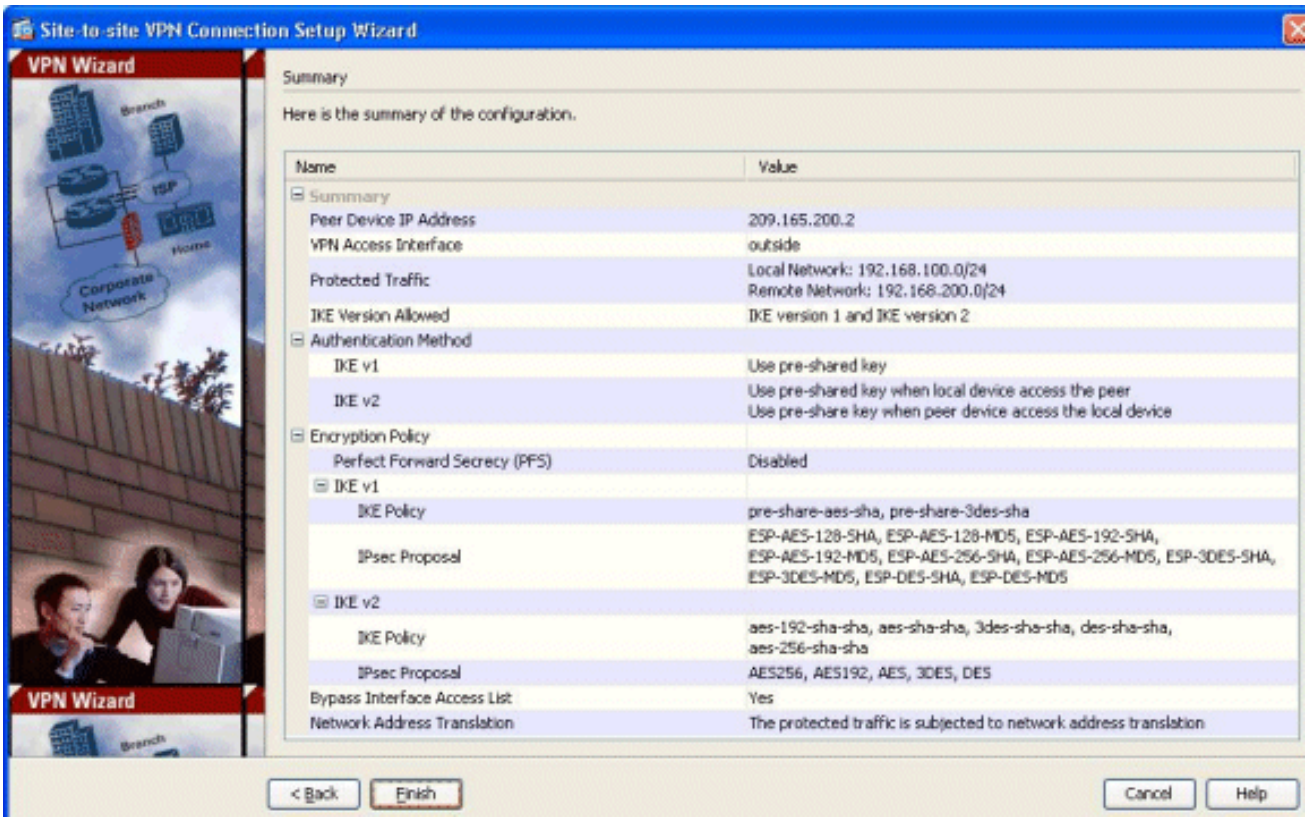
12. انقر فوق **Next (التالي)**.



13. حدد التفاصيل، مثل إعفاء nat، و PFS، وتجاوز قائمة التحكم بالوصول (ACL) للواجهة. أختر **التالي**.



14. يمكن الاطلاع على ملخص التكوين هنا:



طقطقة **إنجاز** in order to أتمت ال موقع إلى موقع VPN نفق معالج. يتم إنشاء ملف تعريف اتصال جديد باستخدام المعلمات التي تم تكوينها.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- show crypto ikev2 sa - يعرض قاعدة بيانات IKEv2 Runtime SA.
- show vpn-sessiondb detail l2l - يعرض المعلومات حول جلسات عمل VPN من موقع إلى موقع.

استكشاف الأخطاء وإصلاحها

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- debug crypto ikev2 - يعرض رسائل **تصحيح الأخطاء** ل IKEv2.

معلومات ذات صلة

- الدعم الفني للأجهزة سلسلة Cisco ASA 5500
- الدعم التقني والمستندات - Cisco Systems

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).