تكوين مركز Cisco VPN 3000 وعميل PGP لشبكة المرتبط

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل على حد سواء ال cisco VPN 3000 مركز والشبكة يربط جيد جدا خصوصية (PGP) زبون يركض صيغة 6.5.1 أن يقبل إتصالات من بعضهم بعضا.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- مركز Cisco VPN 3000، الإصدار 4.7
- Networks Associates PGP Client، الإصدار 6.5.1

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.

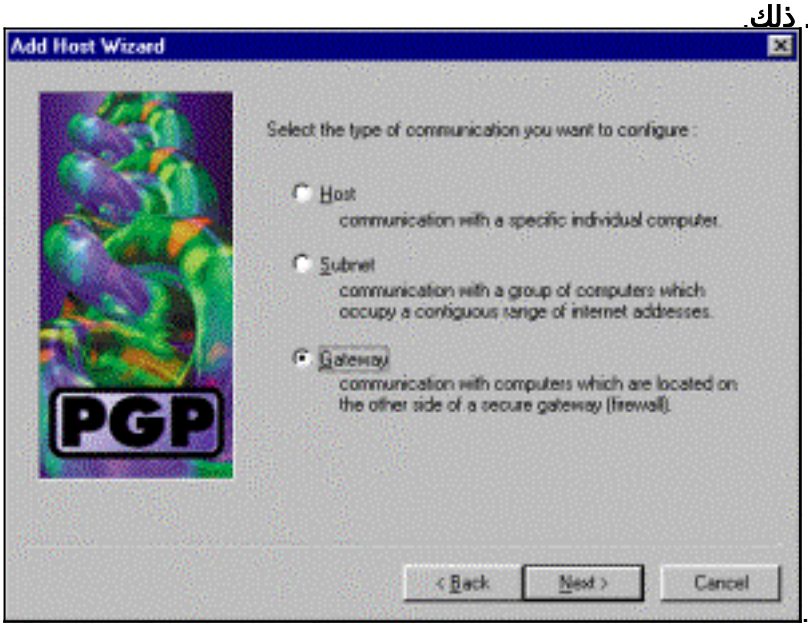
الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

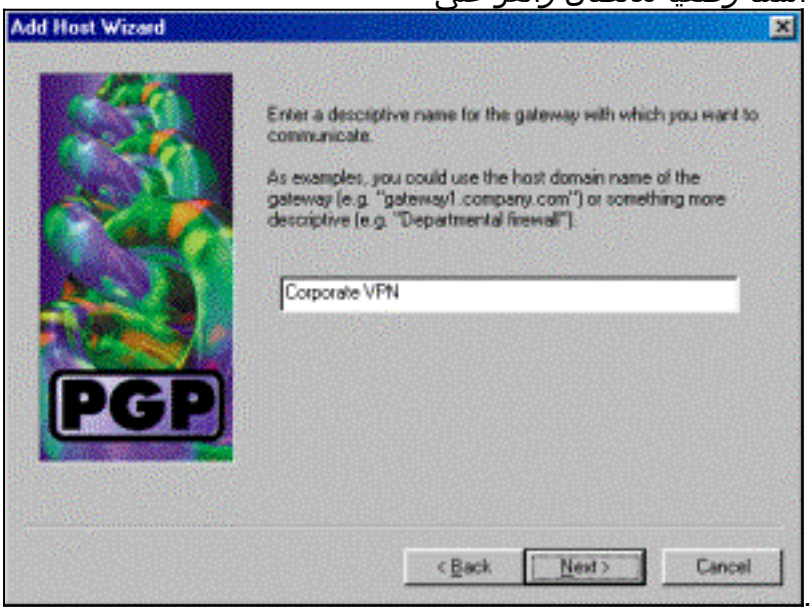
تكوين عميل PGP المقترنة بالشبكة للاتصال بموجه Cisco VPN 3000

أستخدم هذا الإجراء لتكوين عميل PGP المشارك للشبكة للاتصال بموجه VPN 3000.

1. إطلاق **PGPNet > الأجهزة المضيفة**.
2. طقطقة **يضيف** وبعد ذلك يطقطق **بعد ذلك**.

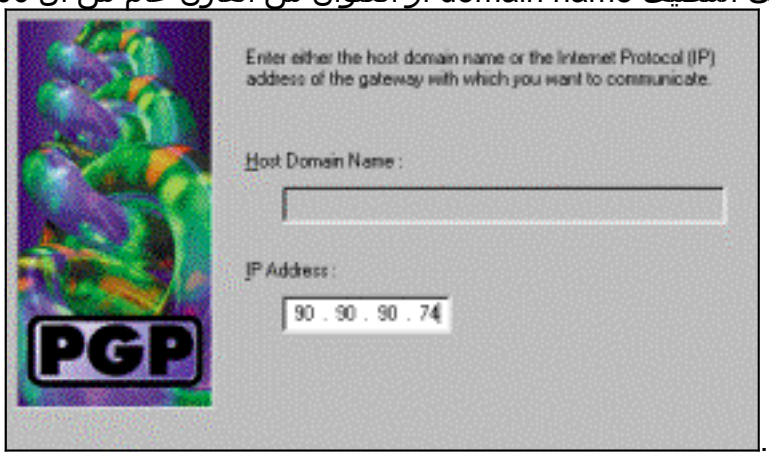


3. أخترت **البوابة** خيار، وطقطقة **بعد ذلك**.
4. أدخل اسما وصفيا للاتصال وانقر على



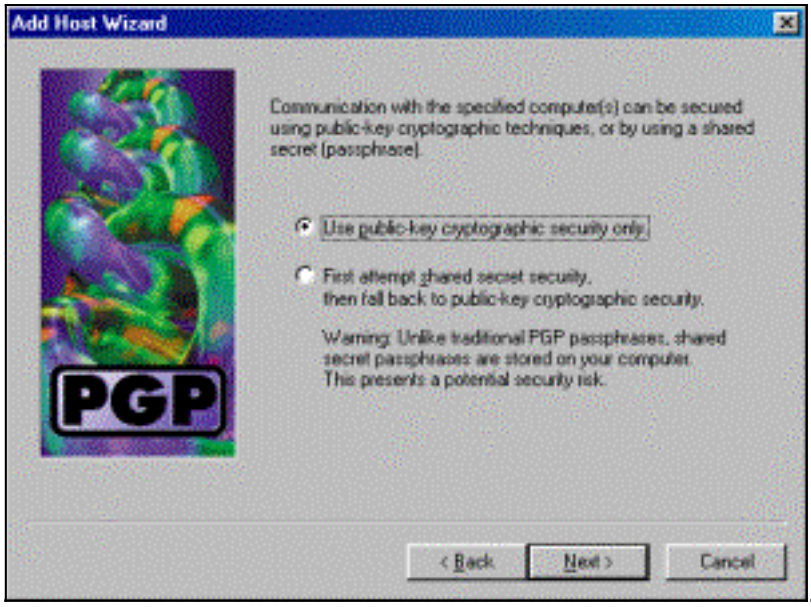
التالي.

5. دخلت المضيف domain name أو العنوان من القارن عام من ال VPN 3000 مركز وطقطقة **بعد**



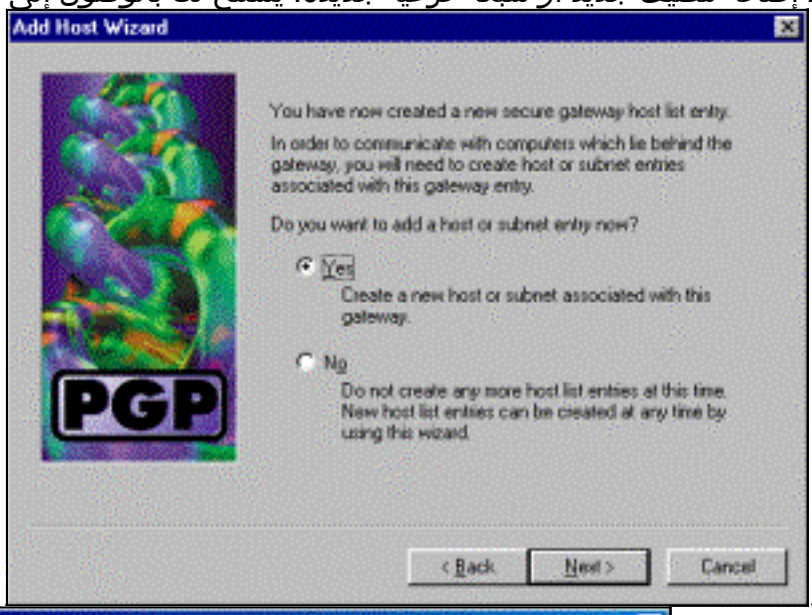
ذلك.

6. أخترت **يستعمل مفتاح عام تشفير أمن فقط** وطقطقة **بعد**

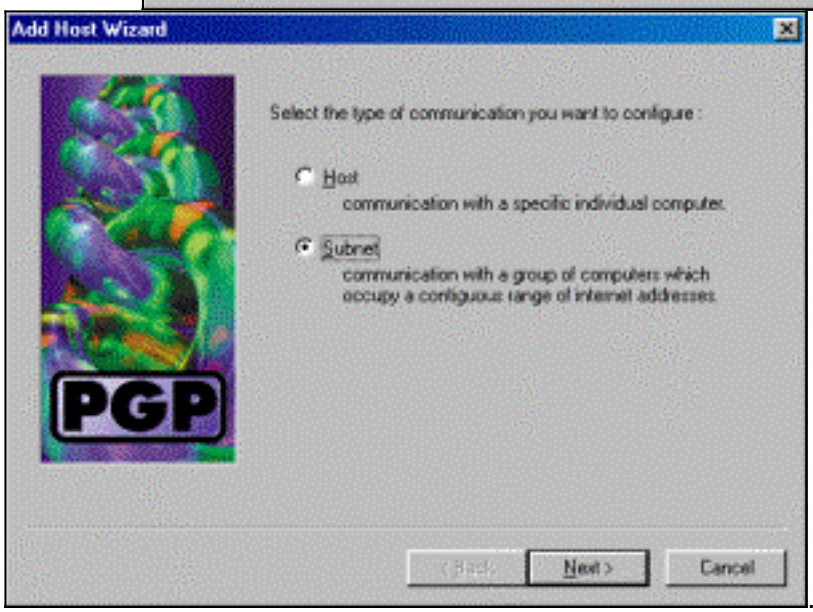


ذلك.

7. حدد **نعم**، وانقر **التالي**. عند إضافة مضيف جديد أو شبكة فرعية جديدة، يسمح لك بالوصول إلى الشبكات



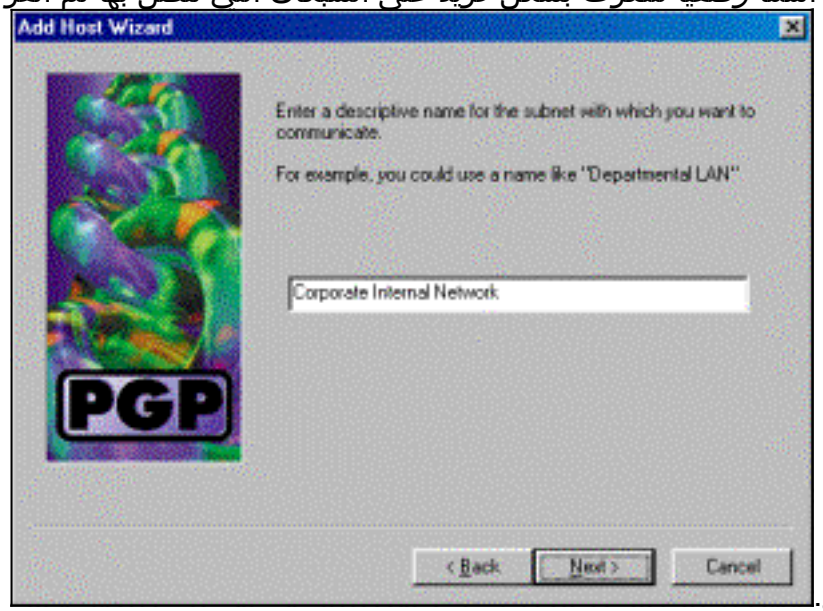
الخاصة بعد تأمين الاتصال.



8. حدد **الشبكة الفرعية** وانقر فوق **التالي**.
9. أختر **السماح بالاتصالات غير الآمنة** وانقر فوق **التالي**.يعالج مركز VPN 3000 أمان الاتصال، وليس برنامج عميل

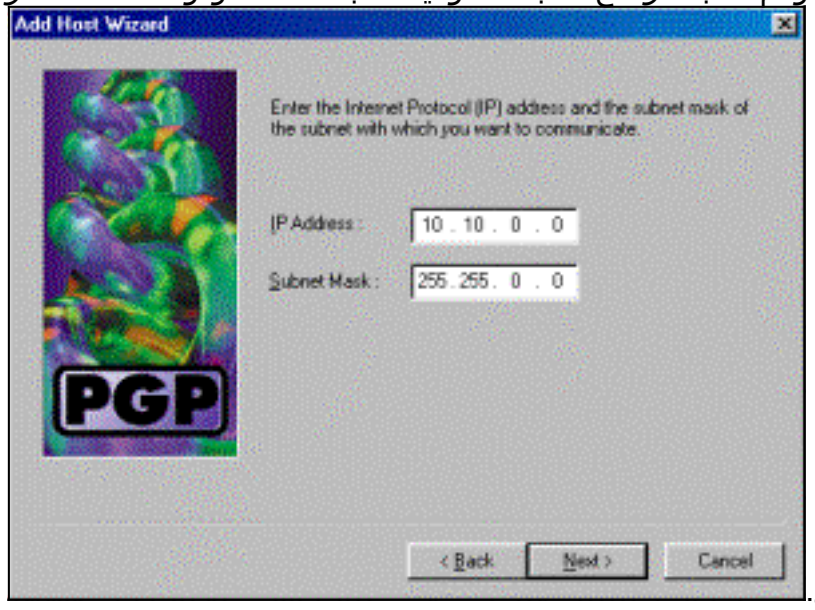
.PGP

10. أدخل اسما وصفيا للتعرف بشكل فريد على الشبكات التي تتصل بها ثم انقر فوق



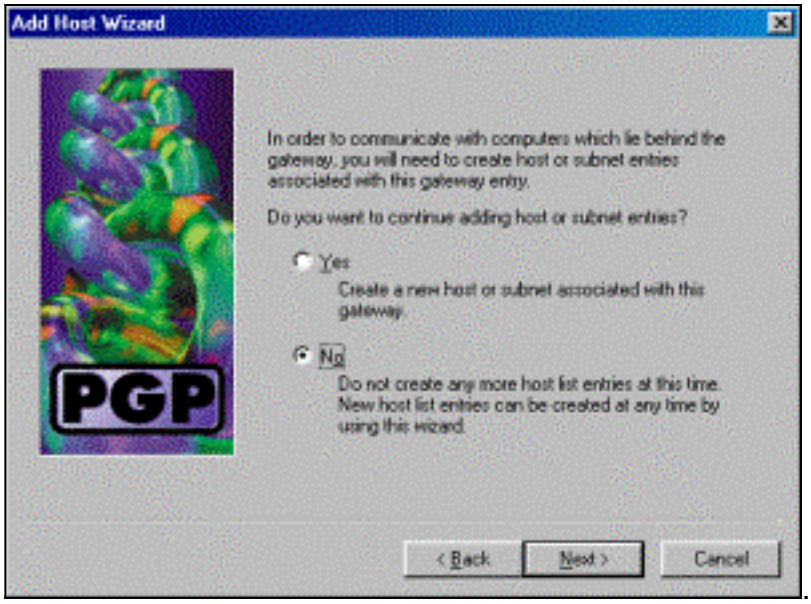
التالي.

11. أدخل رقم الشبكة وقناع الشبكة الفرعية للشبكة خلف مركز VPN 3000 وانقر على



التالي.

12. إذا كانت هناك شبكات داخلية أكثر، أختر **نعم**. وإلا، أختر **لا** وانقر **بعد**



ذلك.

تكوين مركز Cisco VPN 3000 لقبول الاتصالات من عميل PGP لمشاركات الشبكة

أستخدم هذا الإجراء لتكوين مركز Cisco VPN 3000 لقبول الاتصالات من عميل PGP Network Associates:

1. حدد **التكوين > الاتصال النفقي والأمان > IPSec > مقترحات IKE**.
2. تنشيط مقترح **IKE-3DES-SHA-DSA** بتحديده في عمود الاقتراحات غير النشطة. بعد ذلك، انقر زر **تنشيط** ثم انقر زر **حفظ المطلوب**.
3. حدد **تشكيل > إدارة السياسة > إدارة حركة مرور البيانات > SAs**.
4. انقر فوق **إضافة (Add)**.
5. أترك الكل ما عدا هذه الحقول عند إعداداتها الافتراضية:**اسم SA:** قم بإنشاء اسم فريد لتعريف هذا.**الشهادة الرقمية:** أختر شهادة تعريف الخادم المثبتة.**اقتراح IKE:** حدد **IKE-3DES-SHA-DSA**.
6. انقر فوق **إضافة (Add)**.
7. حدد **تكوين > إدارة المستخدم > مجموعات**، انقر فوق **إضافة مجموعة**، ثم قم بتكوين هذه الحقول:**ملاحظة:** إذا كان جميع المستخدمين لديك من عملاء PGP، فيمكنك إستخدام المجموعة الأساسية (**التكوين > إدارة المستخدم > المجموعة الأساسية**) بدلا من إنشاء مجموعات جديدة. إذا كان الأمر كذلك، فقم بتخطي الخطوات لعلامة التبويب "الهوية" واكمال الخطوات 1 و 2 لعلامة التبويب IPSec فقط.تحت علامة التبويب الهوية ، قم بإدخال هذه المعلومات:**اسم المجموعة:** أدخل اسما فريدا. (يجب أن يكون اسم المجموعة هذا مساويا لحقل OU في الشهادة الرقمية لعميل PGP.)**كلمة المرور:** أدخل كلمة المرور للمجموعة.تحت علامة التبويب IPSec، أدخل المعلومات التالية:**المصادقة:** قم بتعيين هذا على **بلا**.**تشكيل الوضع:** قم بإلغاء تحديد هذا.
8. انقر فوق **إضافة (Add)**.
9. وفر حسب الحاجة خلال.

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم IPSec
- تنزيل برنامج VPN (للعملاء المسجلين فقط)
- الدعم الفني - 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).