تقسيم الاتصال النفقي لعملاء VPN على مثال تكوين مركز VPN 3000

المحتويات

المقدمة

يقدم هذا المستند إرشادات خطوة بخطوة حول كيفية السماح لعملاء الشبكة الخاصة الظاهرية (VPN) بالوصول إلى الإنترنت أثناء إنشاء قنوات لهم في مركز تجميع الشبكة الخاصة الظاهرية (VPN) من السلسلة 3000. يتيح هذا التكوين لعملاء الشبكات الخاصة الظاهرية (VPN) إمكانية الوصول الآمن إلى موارد الشركة عبر IPsec أثناء منح وصول غير آمن إلى الإنترنت.

ملاحظة: قد يشكل تقسيم الاتصال النفقي خطرا على الأمان عند تكوينه. نظرا لأن عملاء الشبكة الخاصة الظاهرية (VPN) لديهم وصول غير آمن إلى الإنترنت، يمكن أختراق هذه الشبكات بواسطة المهاجم. وقد يتمكن هذا المهاجم بعد ذلك من الوصول إلى شبكة LAN الخاصة بالشركة عبر نفق IPsec. يمكن أن يكون هناك حل وسط بين الاتصال النفقي الكامل والنفقي المنقسم للسماح بوصول عملاء VPN للشبكة المحلية الظاهرية (LAN) فقط. راجع السماح بالوصول إلى شبكة LAN المحلية لعملاء VPN على مثال تكوين مركز VPN 3000 للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن تكوين شبكة VPN للوصول عن بعد يعمل موجود بالفعل على مركز الشبكة الخاصة الظاهرية (VPN). ارجع إلى IPsec مع عميل VPN إلى مثال تكوين مركز VPN 3000 إذا لم يتم تكوين واحد بالفعل.

المكونات المستخدمة

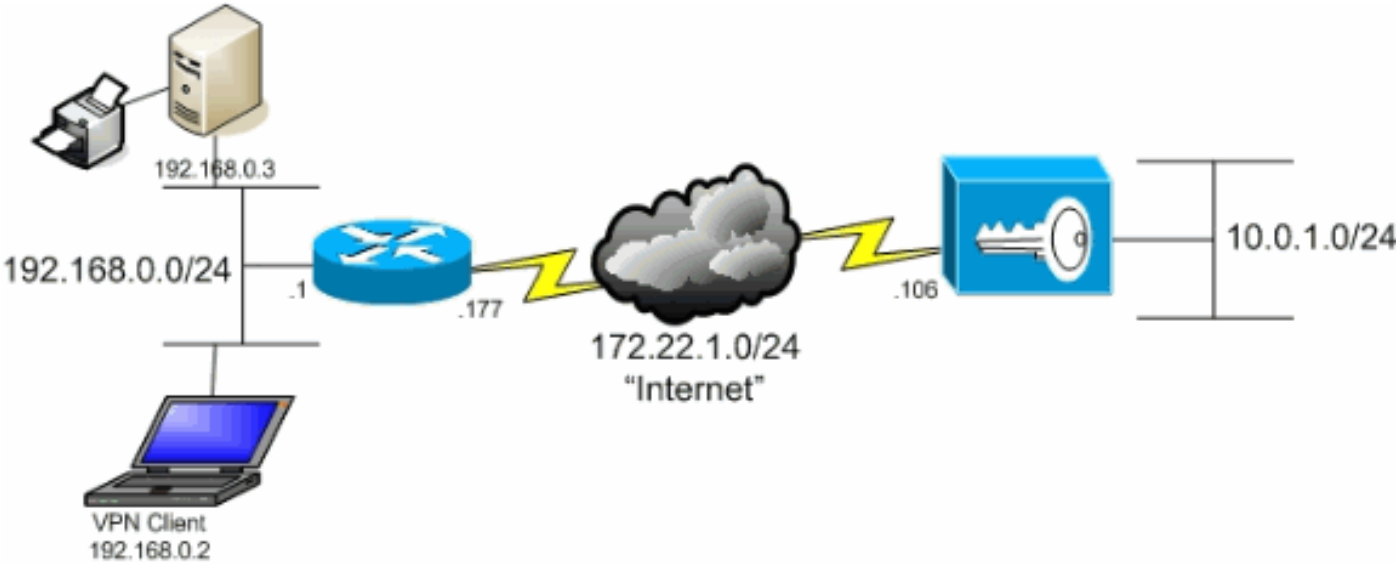
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج Cisco VPN 3000 Concentrator Series، الإصدار H.4.7.2
- Cisco VPN Client، الإصدار 4.0.5

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الرسم التخطيطي للشبكة

يتواجد عميل شبكة VPN على شبكة SOHO نموذجية ويتصل عبر الإنترنت بالمكتب الرئيسي.



الاصطلاحات

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

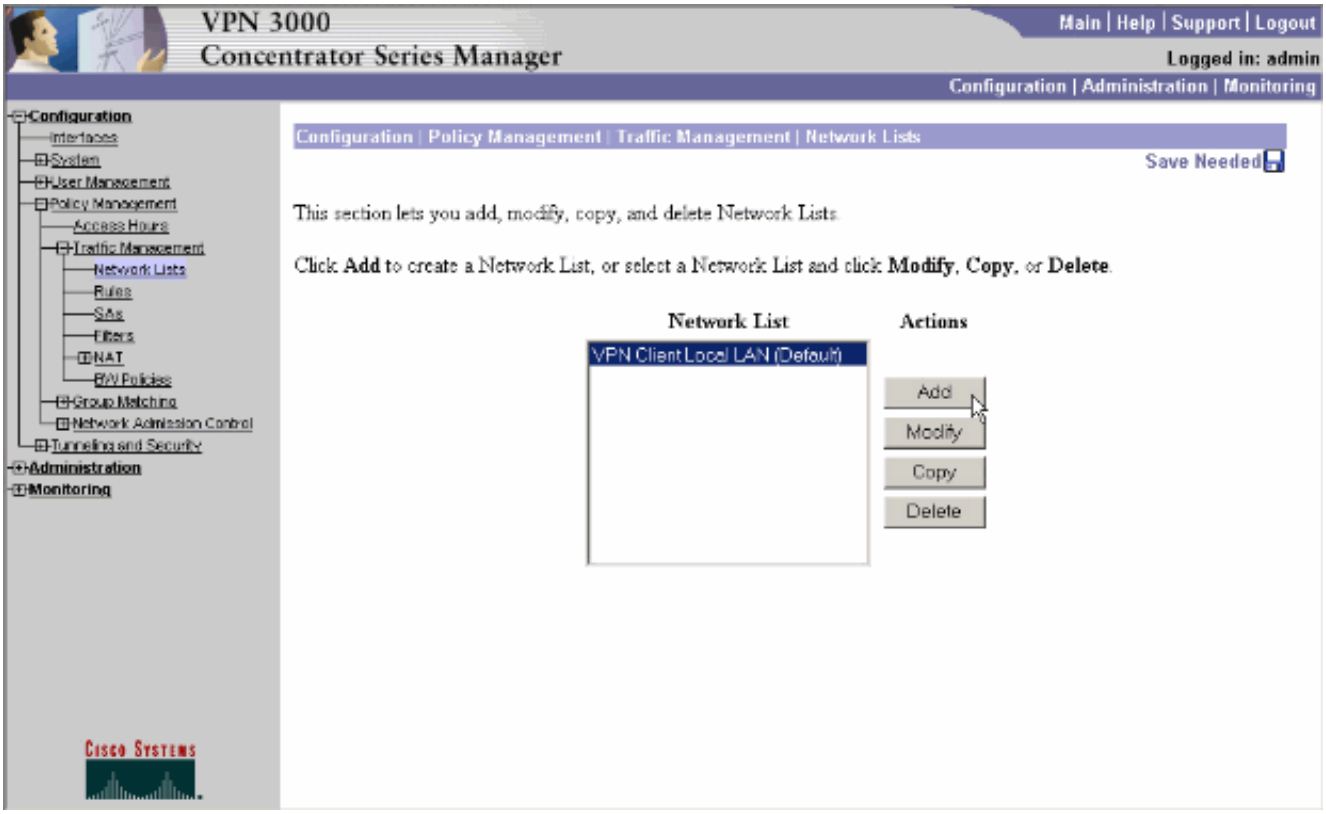
معلومات أساسية

في سيناريو عميل شبكة VPN الأساسية إلى مركز شبكة VPN، يتم تشفير جميع حركات مرور البيانات من عميل شبكة VPN وإرسالها إلى مركز الشبكة الخاصة الظاهرية (VPN) بغض النظر عن الوجهة. استنادا إلى التكوين الخاص بك وعدد المستخدمين المدعومين، يمكن أن تصبح عملية إعداد كهذه ذات نطاق ترددي كبير. يمكن أن تعمل ميزة تقسيم الاتصال النفقي على تخفيف هذه المشكلة من خلال السماح للمستخدمين بإرسال حركة المرور الموجهة فقط إلى شبكة الشركة عبر النفق. يتم إرسال جميع حركات المرور الأخرى مثل المراسلة الفورية أو البريد الإلكتروني أو الاستعراض العرضي إلى الإنترنت عبر الشبكة المحلية (LAN) لعميل الشبكة الخاصة الظاهرية (VPN).

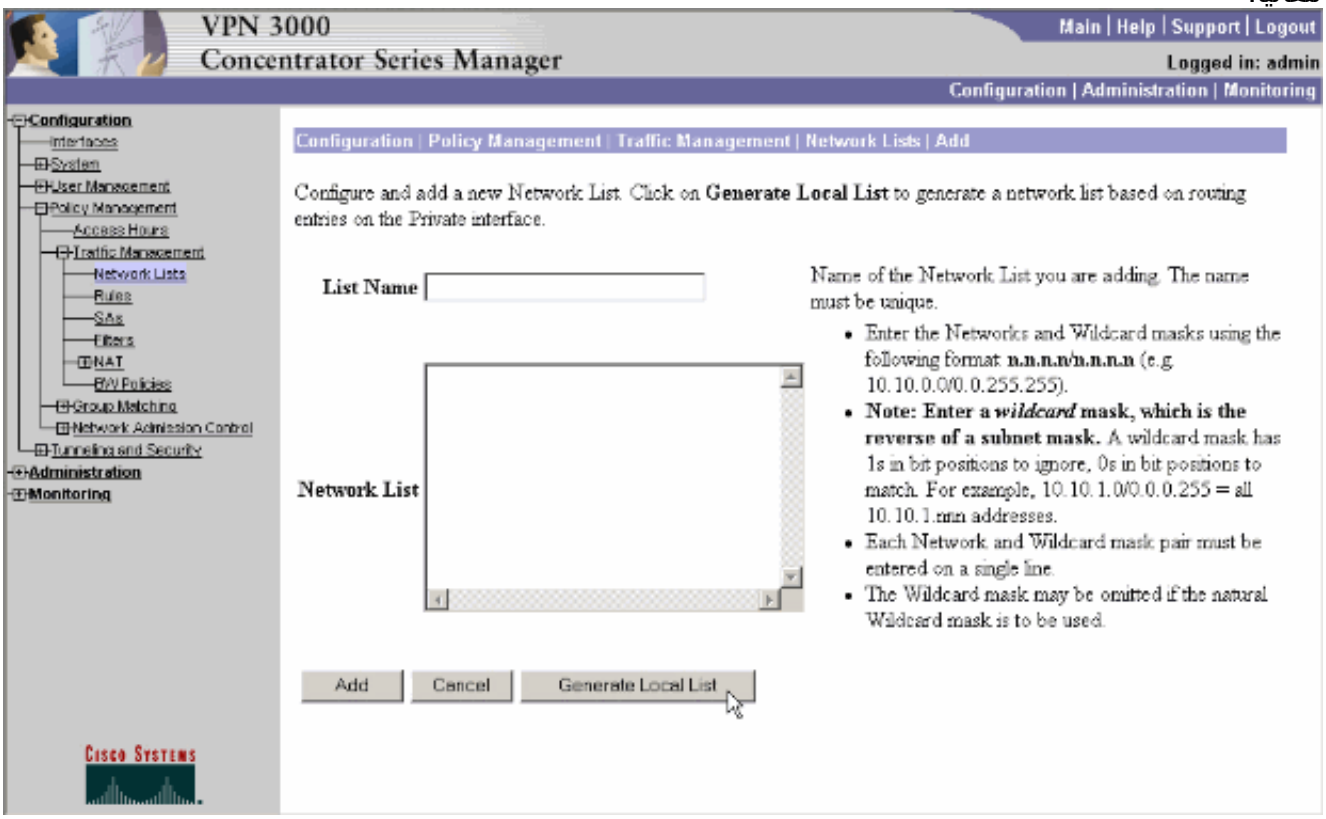
تكوين الاتصال النفقي المنقسم على مركز VPN

أتمت هذا steps in order to شكلت ك نفق مجموعة أن يسمح انقسام tunneling للمستخدمين في المجموعة. قم أولا بإنشاء قائمة شبكات. تقوم هذه القائمة بتعريف الشبكات الوجهة التي يرسل إليها عميل VPN حركة مرور مشفرة. بمجرد إنشاء القائمة، أضف القائمة إلى نهج تقسيم الاتصال النفقي الخاص بمجموعة النفق العميل.

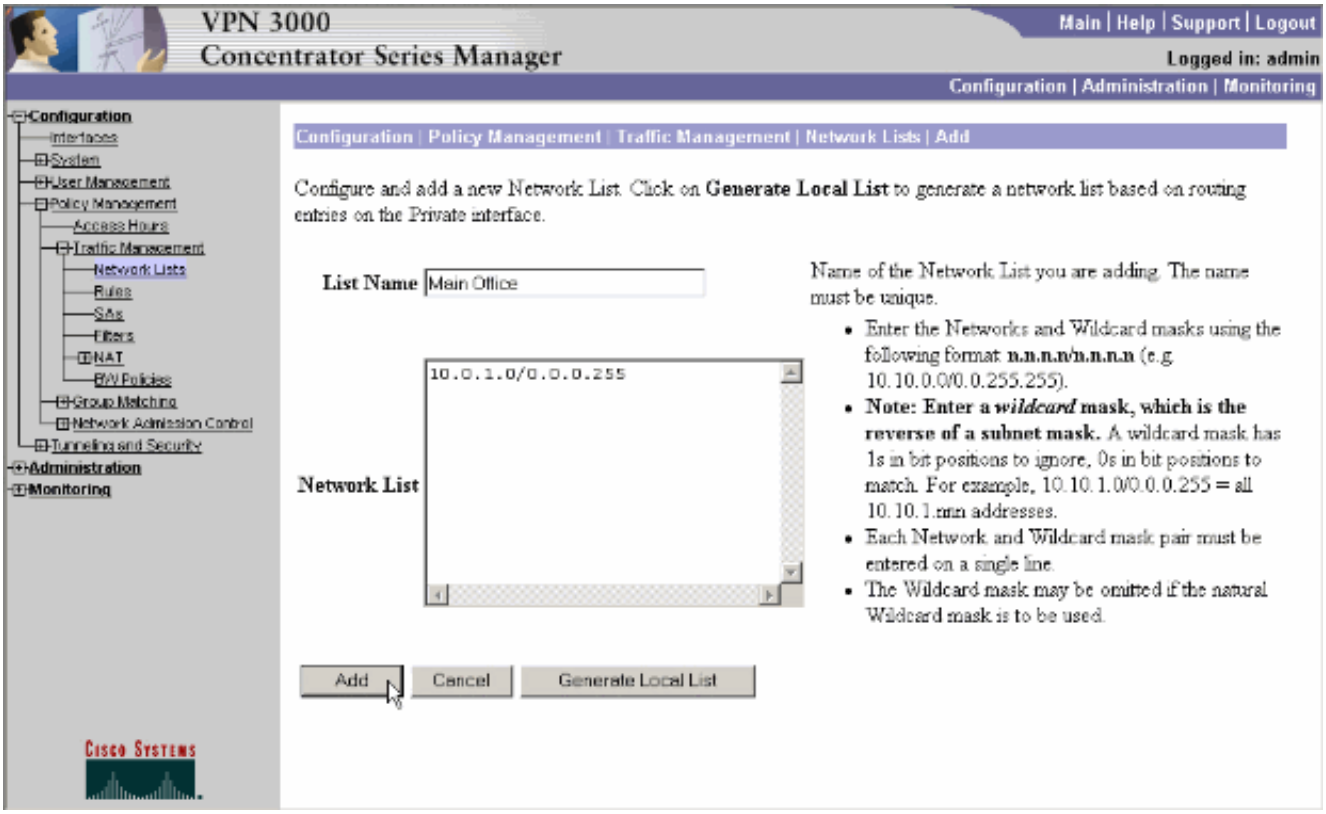
1. أخترت **تشكيل>إدارة سياسة>حركة مرور إدارة>شبكة قائمة** وطقطقة **يضيف**.



2. تقوم هذه القائمة بتعريف الشبكات الوجهة التي يرسل إليها عميل VPN حركة مرور مشفرة. قم بإدخال هذه الشبكات يدويا، أو انقر فوق **إنشاء قائمة محلية** لإنشاء قائمة تستند إلى إدخالات التوجيه على الواجهة الخاصة لمركز VPN.في هذا المثال، تم إنشاء القائمة تلقائيا.

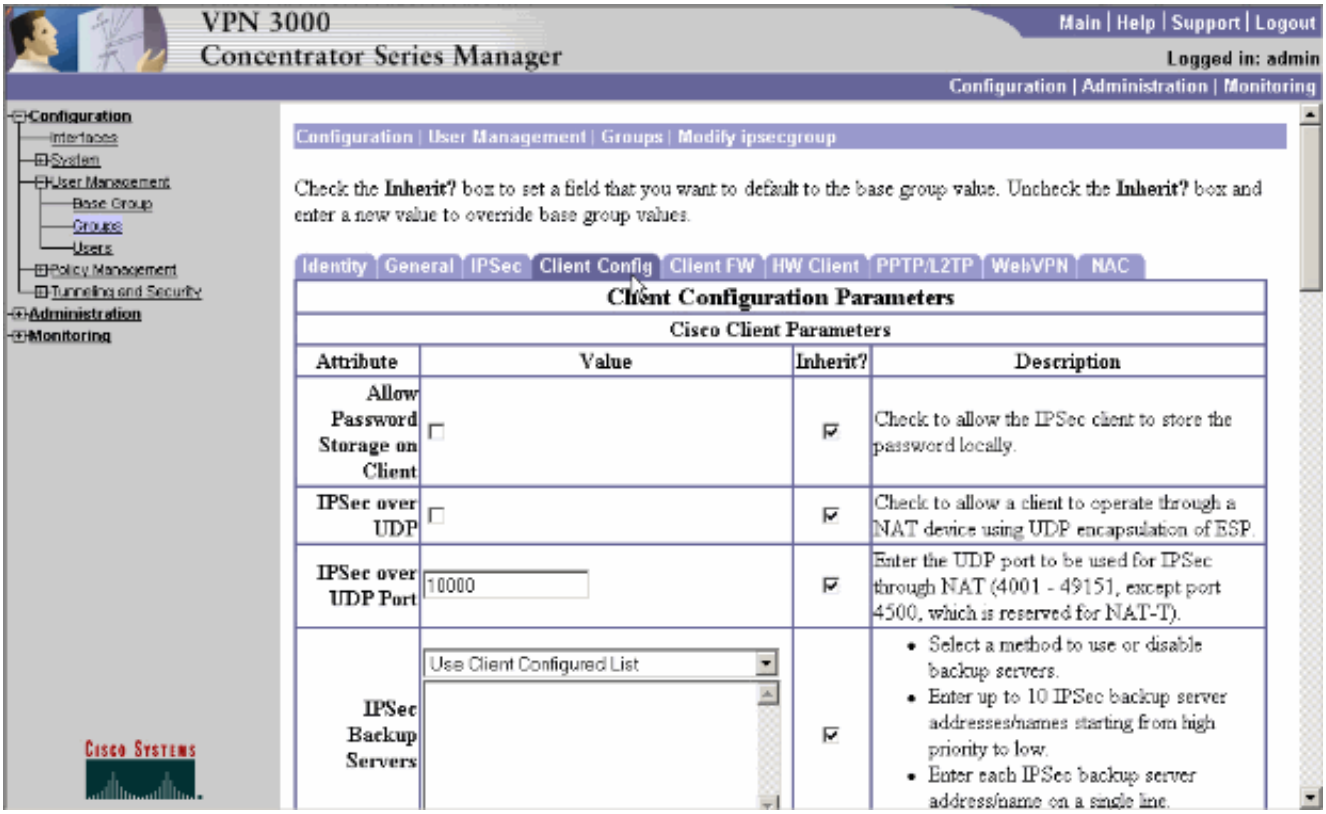


3. بمجرد أن يتم إنشائها أو تعبئتها، قم بتوفير اسم للقائمة وانقر **إضافة**.

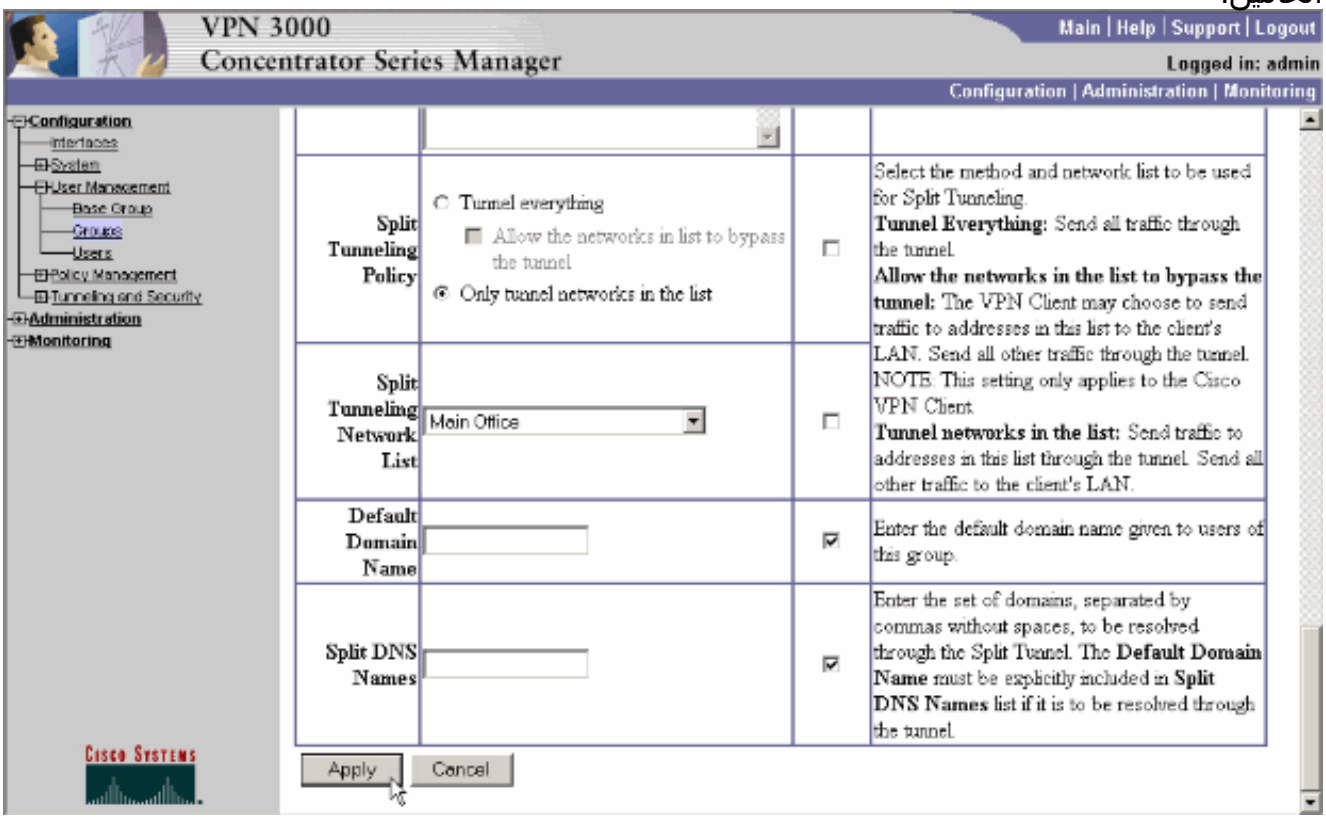


4. بمجرد إنشاء قائمة الشبكة، قم بتعيينها على مجموعة نفق. أختر **تكوين > إدارة المستخدم > مجموعات**، وحدد المجموعة التي تريد تغييرها، وانقر فوق **تعديل المجموعة**.

5. انتقل إلى علامة التبويب تكوين العميل الخاصة بالمجموعة التي أخترت تعديلها.



6. قم بالتمرير لأسفل إلى مقاطع "سياسة تقسيم الاتصال النفقي" و"قائمة تقسيم الاتصال النفقي للشبكة" وانقر فوق **شبكات النفق فقط في القائمة**.
7. أختر القائمة التي تم إنشاؤها مسبقا من القائمة المنسدلة. في هذه الحالة يكون **المكتب الرئيسي**. خانات الاختيار Inherit؟ يتم إفراغ خانات الاختيار تلقائيا في كلتا الحالتين.



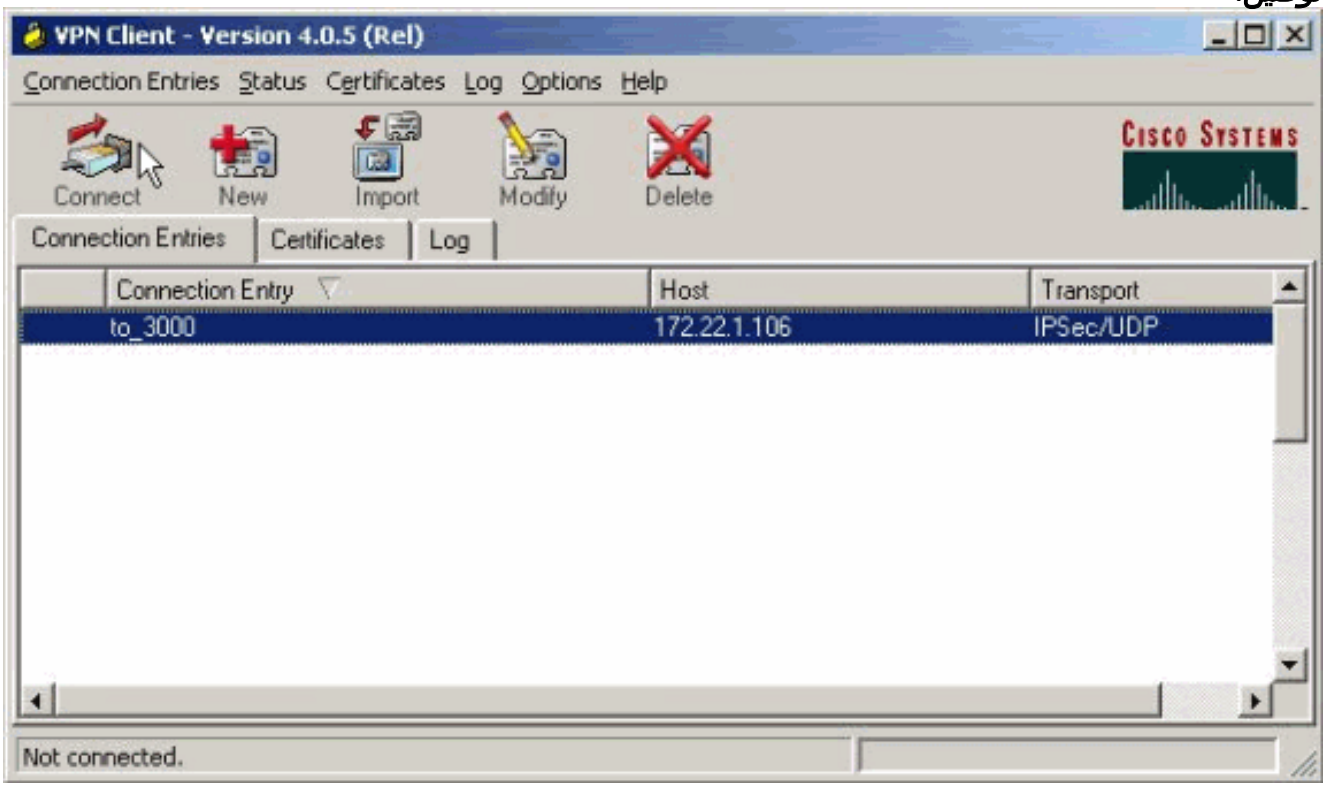
8. انقر فوق **تطبيق** عند الانتهاء.

التحقق من الصحة

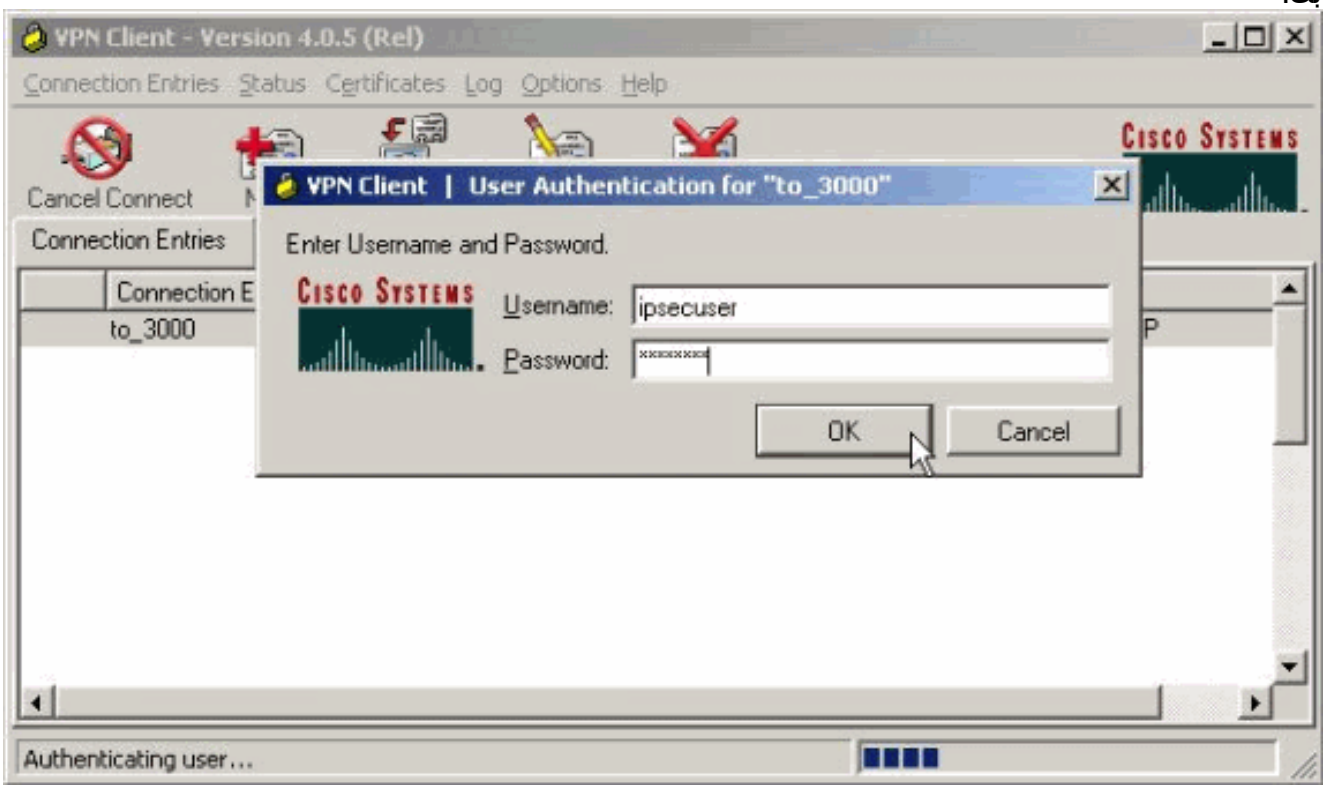
الاتصال بعميل شبكة VPN

قم بتوصيل عميل الشبكة الخاصة الظاهرية (VPN) بمركز الشبكة الخاصة الظاهرية (VPN) للتحقق من التكوين الخاص بك.

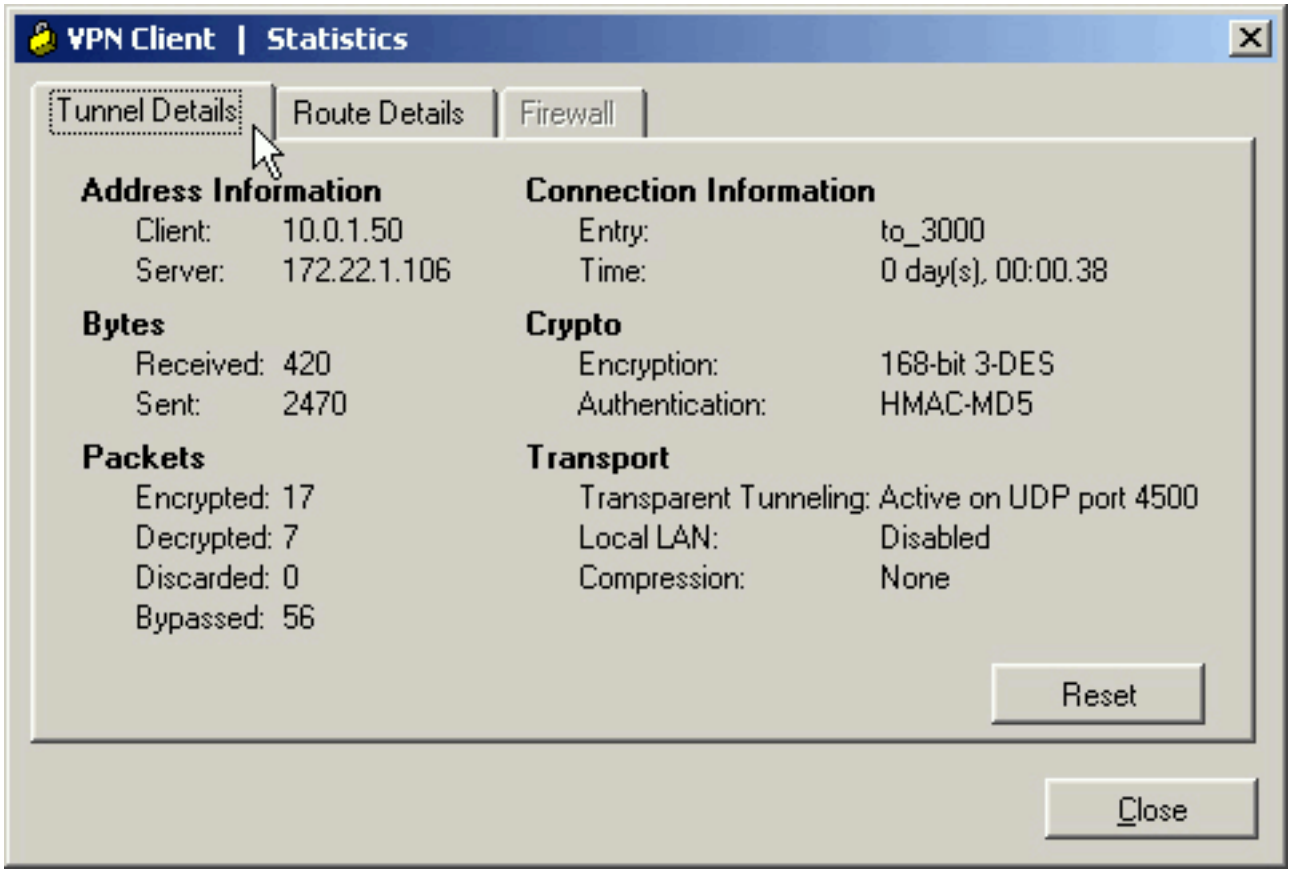
1. أختر إدخال الاتصال الخاص بك من القائمة ثم انقر على **توصيل**.



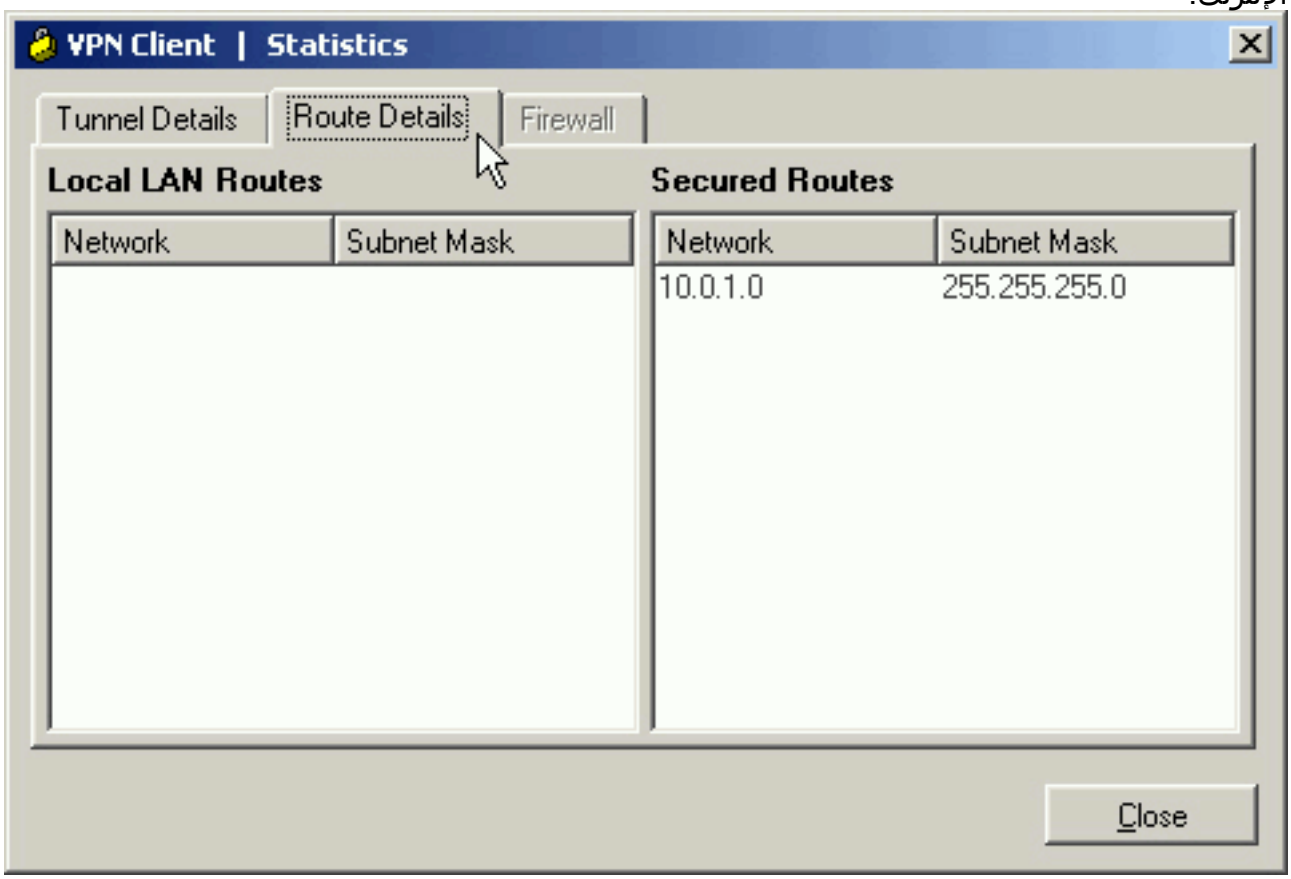
2. أدخل بيانات الاعتماد الخاصة بك.



3. أختر **الحالة > الإحصائيات**.. لعرض نافذة تفاصيل النفق حيث يمكنك فحص تفاصيل النفق ورؤية تدفق حركة المرور.

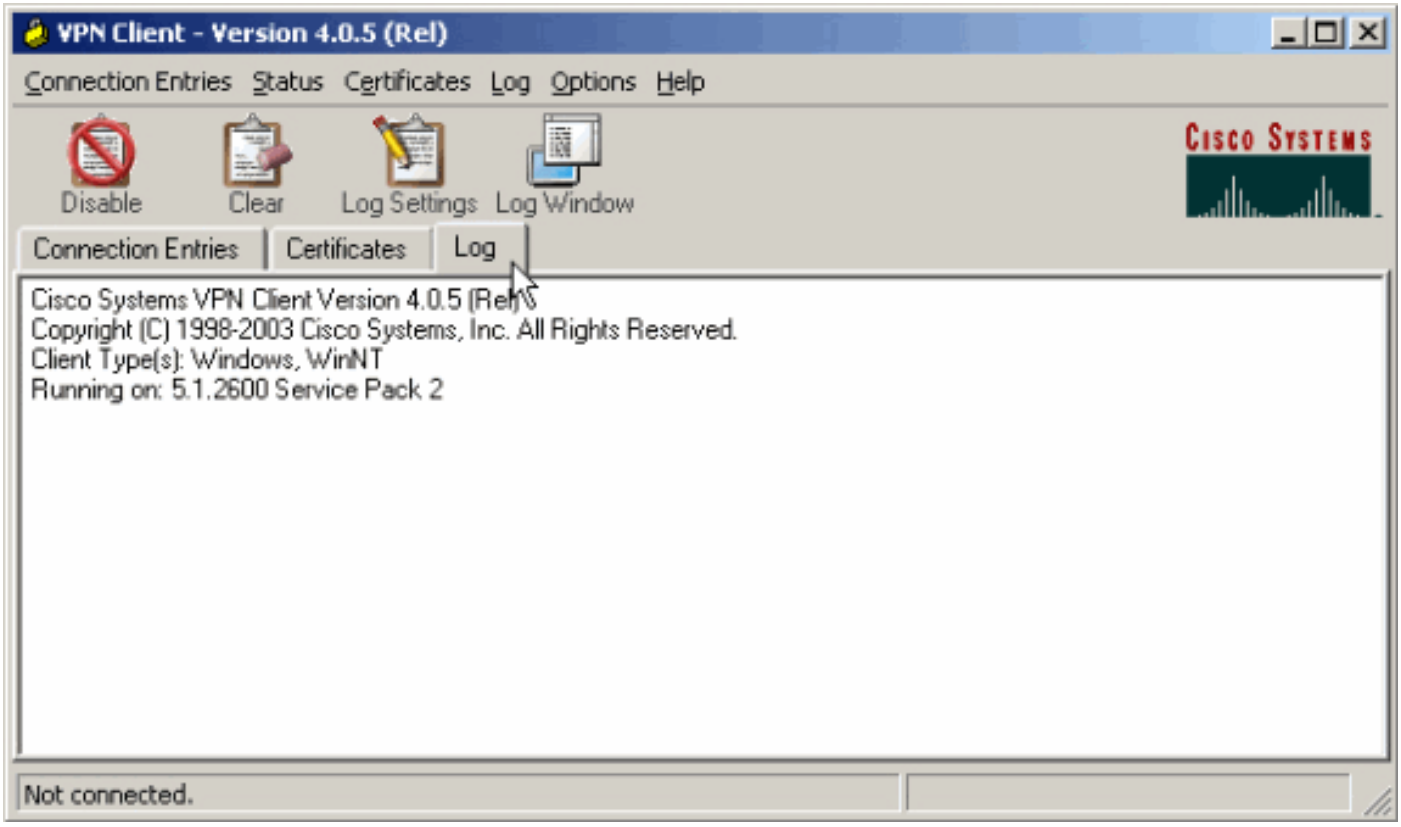


4. انتقل إلى علامة التبويب تفاصيل المسار لمعرفة الشبكات التي يرسل عميل VPN حركة مرور مشفرة إليها. في هذا المثال، يتصل عميل شبكة VPN بشكل آمن مع 24/10.0.1.0 بينما يتم إرسال جميع حركات مرور البيانات الأخرى غير مشفرة إلى
الإنترنت.



عرض سجل عميل شبكة VPN

عندما يفحص أنت ال VPN زبون سجل، أنت يستطيع حددت ما إذا أو لا المعلمة أن يسمح انقسام tunneling ثبتت. انتقل إلى علامة التبويب "سجل" في "عميل VPN" لعرض السجل. انقر فوق **إعدادات السجل** لضبط ما تم تسجيله. في هذا المثال، يتم تعيين IKE و IPsec على **3- مرتفع** بينما يتم تعيين جميع عناصر السجل الأخرى على **1 - منخفض**.




```
                                                (Cisco Systems VPN Client Version 4.0.5 (Rel
                                .Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved
                                                        Client Type(s): Windows, WinNT
                                                    Running on: 5.1.2600 Service Pack 2

                                    Sev=Info/6IKE/0x6300003B  07/21/06  14:21:43.106      1
                                .Attempting to establish a connection with 172.22.1.106

   Output is supressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a ---!
    firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30
        14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
    Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4
       IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114
  07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114
           07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
     172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
   INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010
      MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114
 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
             0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5
 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value
  = 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0
  mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5
          IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40
14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
    value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29
    2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
          .Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed
```

استكشاف الأخطاء وإصلاحها

ارجع إلى IPsec مع عميل VPN إلى مثال تكوين مركز VPN 3000 - أستكشاف الأخطاء وإصلاحها للحصول على معلومات عامة حول أستكشاف أخطاء هذا التكوين وإصلاحها.

معلومات ذات صلة

- IPsec مع عميل VPN إلى مثال تكوين مركز VPN 3000
- مركزات Cisco VPN 3000 Series
- عميل شبكة VPN من Cisco
- 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).