IPsec بين مركز VPN 3000 وزبون VPN 4.x لـ Cisco VPN Client 4.x و PIX/ASA 7.x مع مثال تكوين مصادقة Microsoft Windows باستخدام RADIUS

المحتويات

المقدمة

يوضح هذا المستند كيفية إنشاء نفق IPsec بين مركز Cisco VPN 3000 وعميل Cisco VPN 4.x لـ Microsoft Windows الذي يستخدم RADIUS لمصادقة المستخدم ومحاسبته. يوصي هذا المستند بخادم التحكم في الوصول الآمن (ACS) من Cisco لأنظمة التشغيل Windows للحصول على تكوين RADIUS أسهل لمصادقة المستخدمين الذين يقومون بالاتصال بموجه VPN 3000. مجموعة على مركز VPN 3000 هي مجموعة من المستخدمين تتم معاملتهم ككيان واحد. ويمكن لتهيئة المجموعات، مقارنة بالمستخدمين الأفراد، تبسيط إدارة النظام وتنظيم مهام التهيئة.

ارجع إلى تكوين مصادقة Microsoft Windows مع مثال تكوين Cisco VPN Client 4.x لـ Windows و PIX/ASA 7.x لإعداد اتصال VPN للوصول عن بعد بين عميل Cisco VPN 4.x) لـ Windows) وجهاز الأمان PIX 500 Series 7.x الذي يستخدم خادم RADIUS لخدمة مصادقة الإنترنت (IAS) في Microsoft Windows 2003 IAS RADIUS.

ارجع إلى تكوين IPsec بين موجه Cisco IOS وعميل Cisco VPN 4.x لـ Windows الذي يستخدم RADIUS

لمصادقة المستخدم لتكوين اتصال بين موجه وعميل Cisco VPN 4.x الذي يستخدم RADIUS لمصادقة المستخدم.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- يتم تثبيت مصدر المحتوى الإضافي الآمن من Cisco ل Windows RADIUS ويعمل بشكل صحيح مع الأجهزة الأخرى.
- تم تكوين مركز Cisco VPN 3000 ويمكن إدارته باستخدام واجهة HTML.

المكونات المستخدمة

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

- Cisco Secure ACS ل Windows مع الإصدار 4.0
- مركز Cisco VPN 3000 Series مع ملف الصورة B.4.7.2
- عميل شبكة Cisco VPN 4.x من Cisco

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.

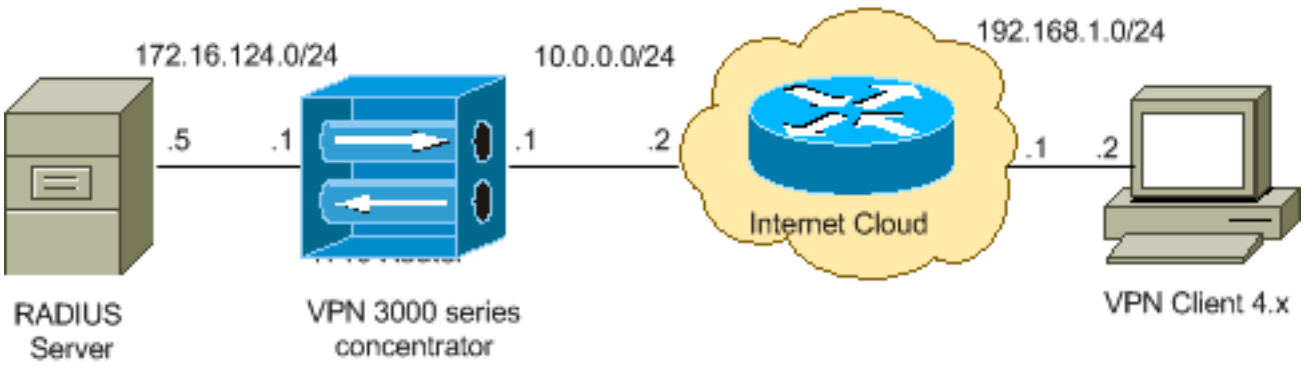
التكوين

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:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

إستخدام المجموعات على مركز VPN 3000

يمكن تحديد مجموعات لكل من مصدر المحتوى الإضافي الآمن من Cisco ل Windows و مركز VPN 3000، ولكنهم يستخدمون المجموعات بشكل مختلف بعض الشيء. قم بتنفيذ هذه المهام من أجل تبسيط الأمور:

- **قم بتكوين مجموعة واحدة على مركز VPN 3000** عندما تقوم بإنشاء النفق الأولي. وهذا غالبا ما يسمى مجموعة النفق وهو يستخدم لإنشاء جلسة عمل مشفرة لتبادل مفتاح الإنترنت (IKE) إلى مركز VPN 3000 باستخدام مفتاح مشترك مسبقا (كلمة مرور المجموعة). هذا هو نفس اسم المجموعة وكلمة المرور التي يجب تكوينها على جميع عملاء Cisco VPN الذين يرغبون في الاتصال بمركز VPN.
- **قم بتكوين المجموعات على Cisco Secure ACS لخادم Windows** الذي يستخدم سمات RADIUS القياسية وسمات المورد المحددة (VSAs) لإدارة النهج. ال VSAs أن ينبغي استعملت مع ال VPN 3000 مركز يكون ال RADIUS (VPN 3000) سمة.
- **قم بتكوين المستخدمين على مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows RADIUS وقم بتعيينهم إلى إحدى المجموعات** التي تم تكوينها على الخادم نفسه. يرث المستخدمون السمات المحددة لمجموعتهم ويرسل Cisco Secure ACS ل Windows هذه السمات إلى مركز VPN عندما يكون المستخدم مصدقا.

كيف يستخدم مركز VPN 3000 سمات المجموعة والمستخدم

بعد أن يقوم مركز VPN 3000 بمصادقة مجموعة النفق مع مركز VPN والمستخدم مع RADIUS، يجب أن يقوم بتنظيم السمات التي تلقيتها. يستخدم مركز VPN الخصائص في هذا الترتيب من التفضيلات، سواء تمت المصادقة في مركز VPN أو مع RADIUS:

1. **سمات المستخدم**- تكون هذه السمات دائما ذات أسبقية على غيرها.
2. **سمات مجموعة النفق**- أي سمات لم يتم إرجاعها عند مصادقة المستخدم يتم تعبئتها بسمات مجموعة النفق.
3. **خصائص المجموعة الأساسية**- أي خصائص مفقودة من المستخدم أو مجموعة النفق تعبأ بخصائص مجموعة قاعدة مركز VPN.

تكوين مركز VPN 3000 Series

أكمل الإجراء في هذا القسم لتكوين مركز Cisco VPN 3000 للمعلمات المطلوبة لاتصال IPsec بالإضافة إلى عميل AAA لمستخدم VPN للمصادقة مع خادم RADIUS.

في إعداد المختبر هذا، يتم الوصول إلى مركز VPN أولا من خلال منفذ وحدة التحكم ويتم إضافة تكوين أدنى كما يوضح هذا الإخراج:

```
Login: admin
The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator ---!
   Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
 Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
    1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address ---------------------------------------------------------------
    --------------- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | ----------------------
        ------------------------------------------------------------ DNS Server(s): DNS Server Not
        Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
  Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
```

```
  Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
        MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
  Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
  ---------------------------------------------------------------------------- Ether1-Pri| DOWN |
 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | ----------------------------------------------------------
---------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
          Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
  172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
  Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
      02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
    Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
    Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
        MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
    Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----------
          ---------------------------------------------------------------------- Ether1-Pri| Up |
     172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | ------------------------------------------------------
  ---------------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
- #2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces
<
```

يظهر مركز VPN في التكوين السريع، ويتم تكوين هذه العناصر.

- الوقت/التاريخ
- الواجهات/الأقنعة في **التكوين > الواجهات** (عام=24/10.0.0.1، خاص=24/172.16.124.1)
- البوابة الافتراضية في **التكوين > النظام > توجيه** 10.0.0.2) **IP > Default_Gateway**)

عند هذه النقطة، يمكن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) من خلال HTML من الشبكة الداخلية.

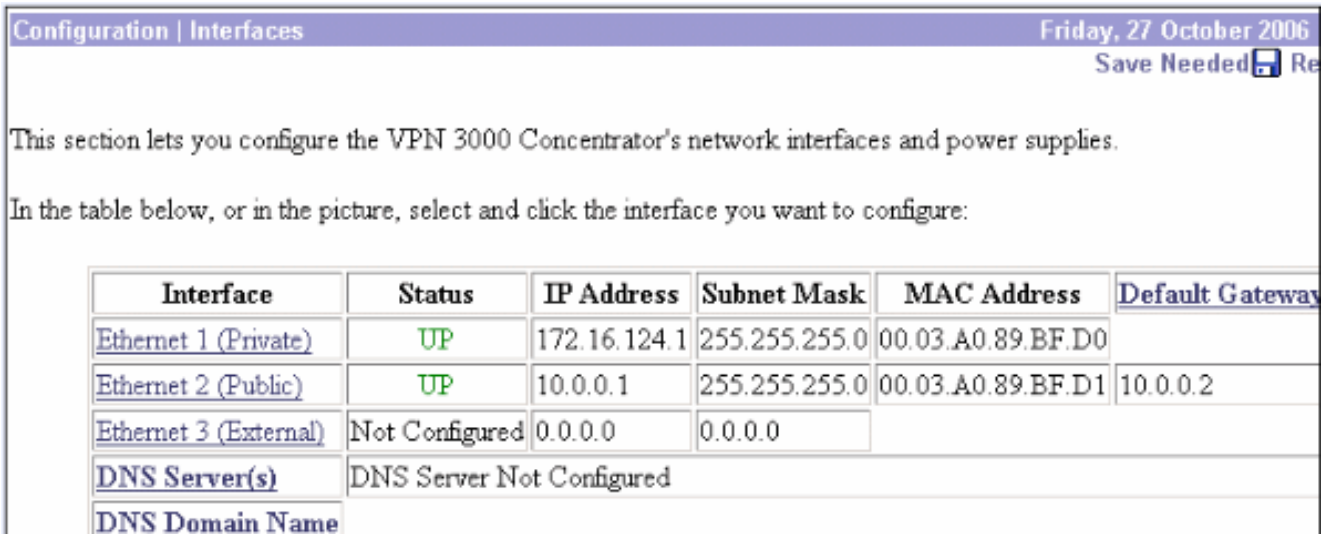
ملاحظة: إذا تمت إدارة مركز الشبكة الخاصة الظاهرية (VPN) من الخارج، فعليك أيضا تنفيذ الخطوات التالية:

1. أختر **تكوين > 1-واجهات > 2-عام > 4-تحديد مرشح 1 < IP. خاص (افتراضي)**.
2. أختر **إدارة > حقوق الوصول 7 > قائمة التحكم في الوصول > محطة عمل مدير إضافة 1** لإضافة عنوان IP الخاص بالمدير الخارجي.

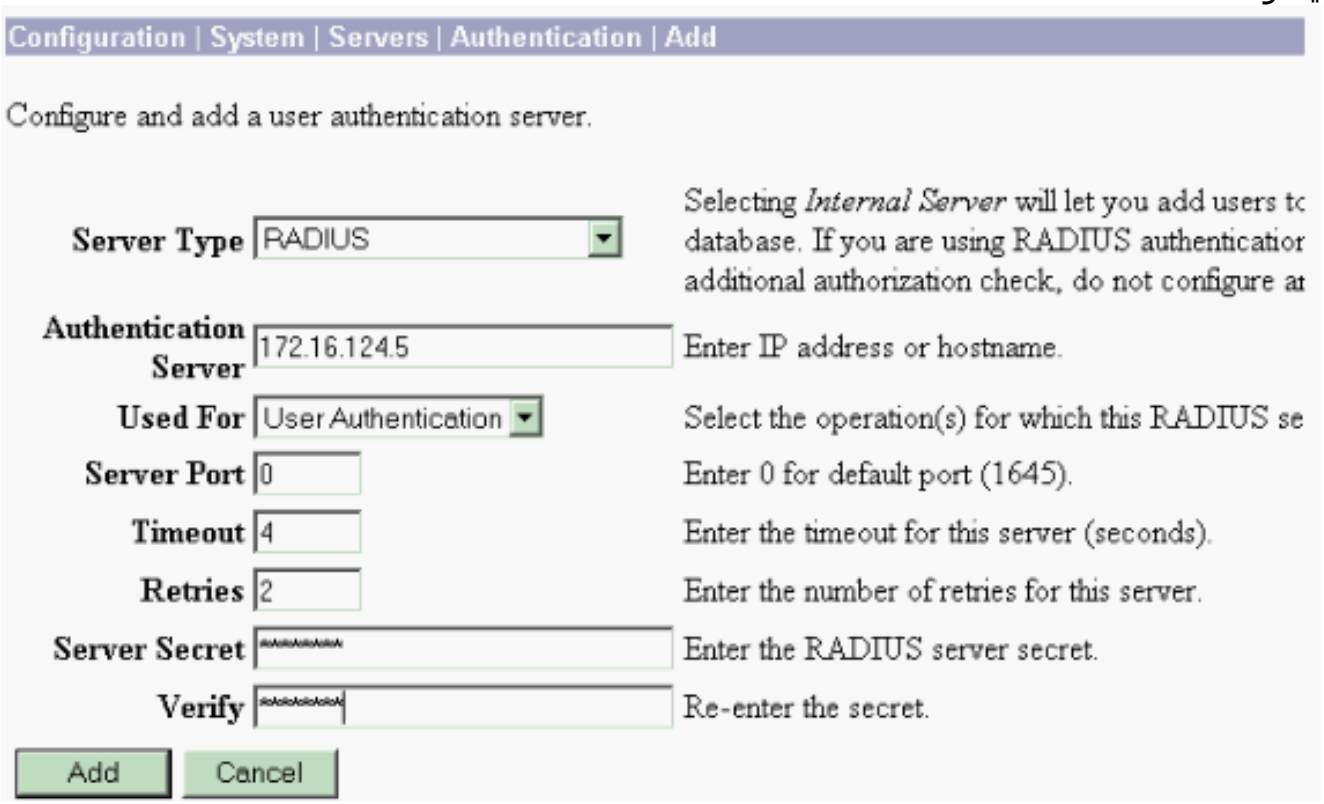
لا تكون هذه الخطوات مطلوبة إلا إذا قمت بإدارة مركز VPN من الخارج.

بمجرد اكتمال هاتين الخطوتين، يمكن تنفيذ بقية التكوين من خلال واجهة المستخدم الرسومية (GUI) باستخدام مستعرض ويب والاتصال ب IP الخاص بالواجهة التي قمت بتكوينها للتو. في هذا المثال وعند هذه النقطة، يمكن الوصول إلى مركز VPN من خلال HTML من الشبكة الداخلية:

1. أخترت **تشكيل>قارن** in order to recheck القارن بعد أن يشكل أنت ال gui.



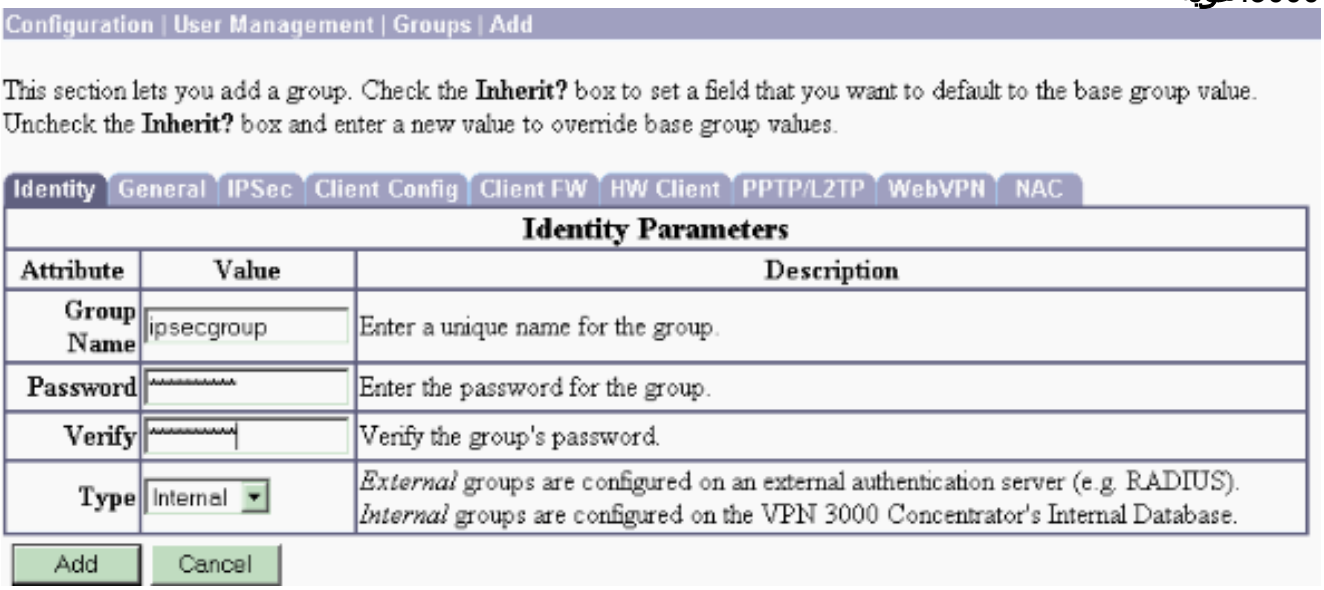
2. أتمت هذا steps in order to أضفت ال cisco يؤمن acs ل Windows RADIUS نادل إلى ال VPN 3000 مركز تشكيل.أخترت **تشكيل > نظام > خادم > مصادقة**، **ويضيف** طقطقة من القائمة يسار.



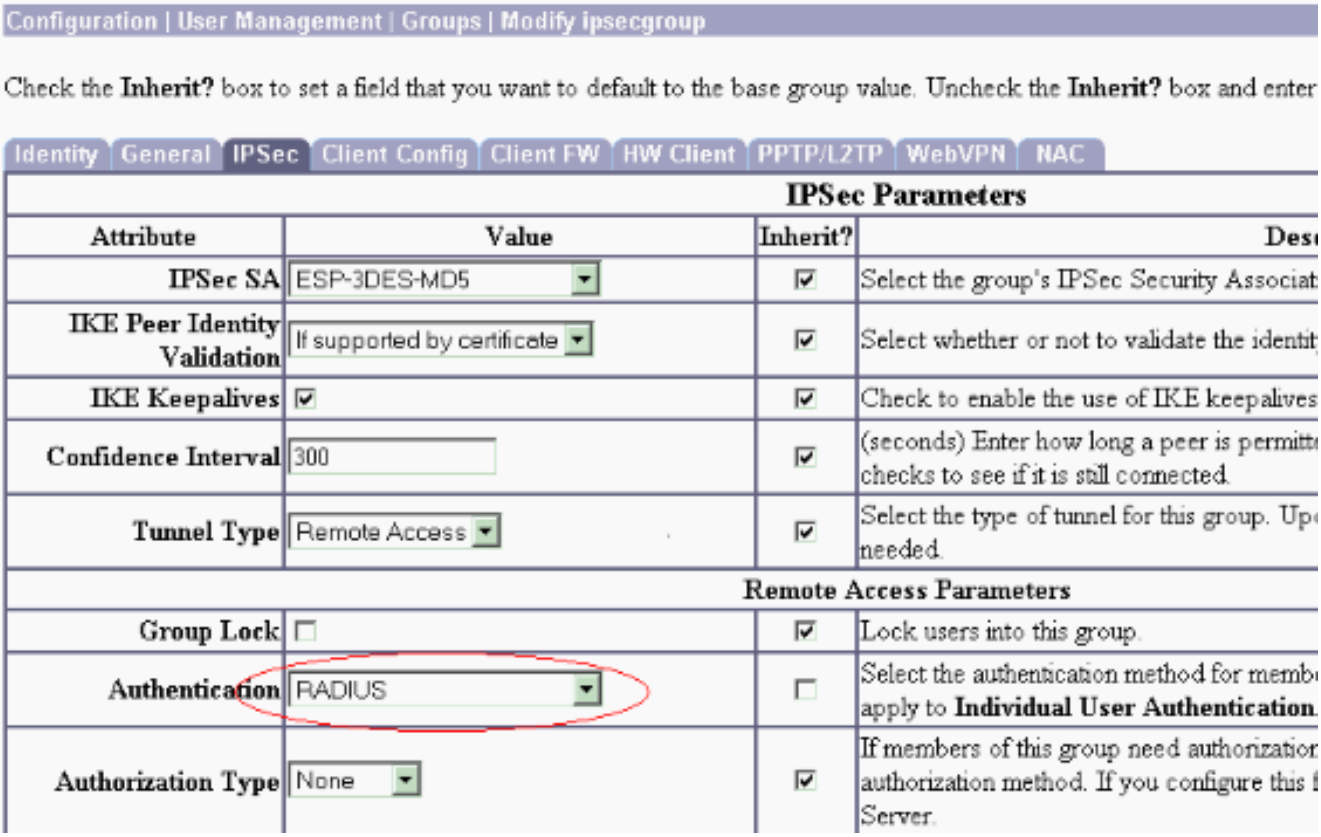
أختر **RADIUS** لنوع الخادم وأضف هذه المعلمات ل Cisco ACS الآمن لخادم Windows RADIUS. أترك كافة المعلمات الأخرى في حالتها الافتراضية.**خادم المصادقة**—أدخل عنوان IP الخاص بمصدر المحتوى الإضافي الآمن من Cisco لخادم Windows RADIUS.**سر الخادم**—أدخل سر خادم RADIUS. هذا ينبغي كنت ال نفسه سر يستعمل أنت عندما يشكل أنت ال VPN 3000 مركز في ال cisco يأمن ACS ل Windows تشكيل.**دققت**—أعدت الكلمة للتحقق.وهذا يضيف خادم المصادقة في التكوين العام ل VPN 3000 Concentrator. يتم إستخدام هذا الخادم من قبل جميع المجموعات باستثناء الحالات التي يتم فيها تعريف خادم مصادقة بشكل محدد. في حالة عدم تكوين خادم مصادقة لمجموعة، فإنه يرجع إلى خادم المصادقة العام.

3. أتمت هذا steps in order to شكلت مجموعة النفق على ال VPN 3000 مركز.أختر **تشكيل > إدارة المستخدم > مجموعات** من القائمة اليسرى وانقر **إضافة**.قم بتغيير هذه المعلمات أو إضافتها في علامات تبويب التكوين. لا تنقر فوق تطبيق حتى تقوم بتغيير كافة المعلمات التالية:**ملاحظة:** هذه المعلمات هي الحد الأدنى المطلوب لاتصالات VPN للوصول عن بعد. تفترض هذه المعلمات أيضا أنه لم يتم تغيير الإعدادات الافتراضية في المجموعة الأساسية على مركز VPN

3000.**هوية**

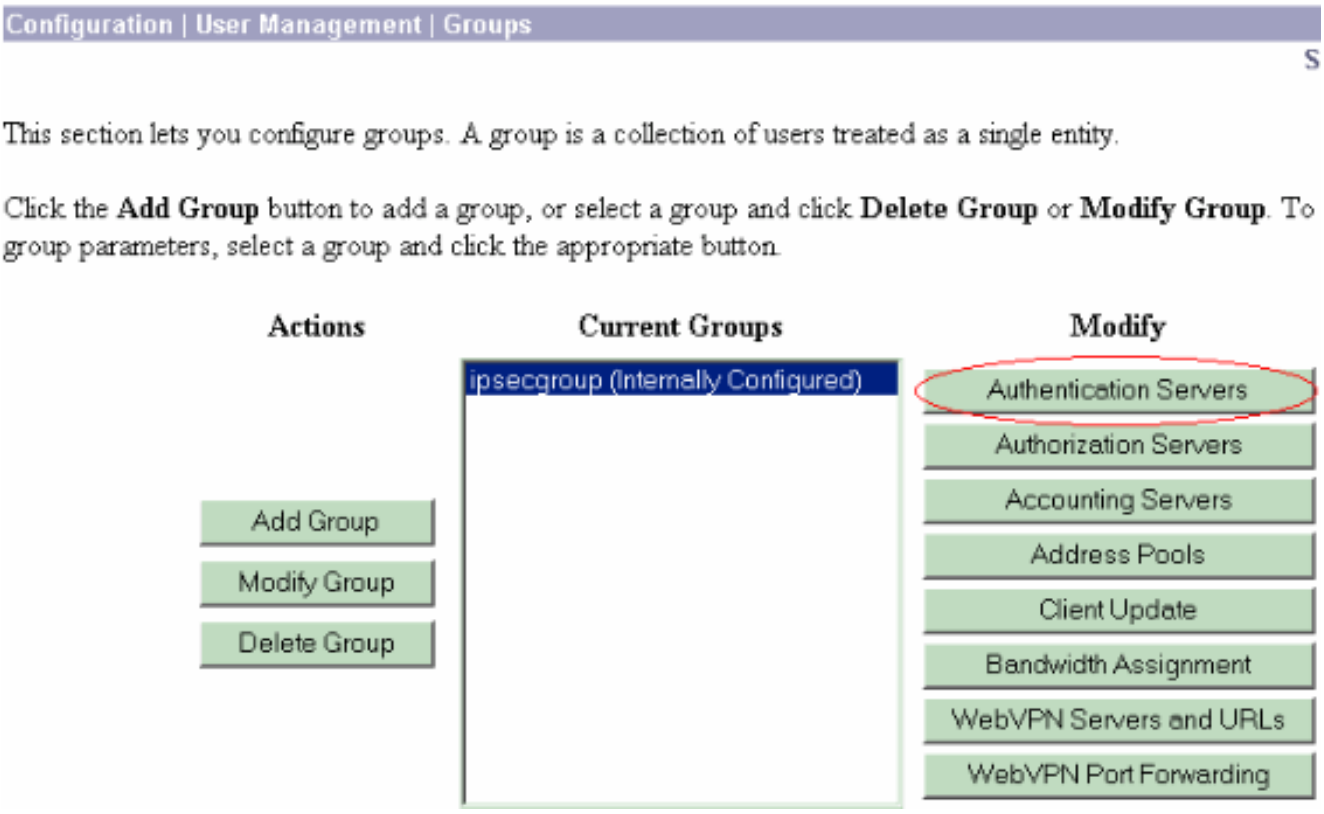


اسم المجموعة- اكتب اسم المجموعة. على سبيل المثال، IPsecUsers.أدخل كلمة **مرور**- كلمة مرور للمجموعة. هذا هو المفتاح المشترك مسبقا لجلسة عمل IKE.**دققت**—أعدت الكلمة للتحقق.**الكتابة**- أترك هذا كافتراضي:
داخلي.**IPsec**



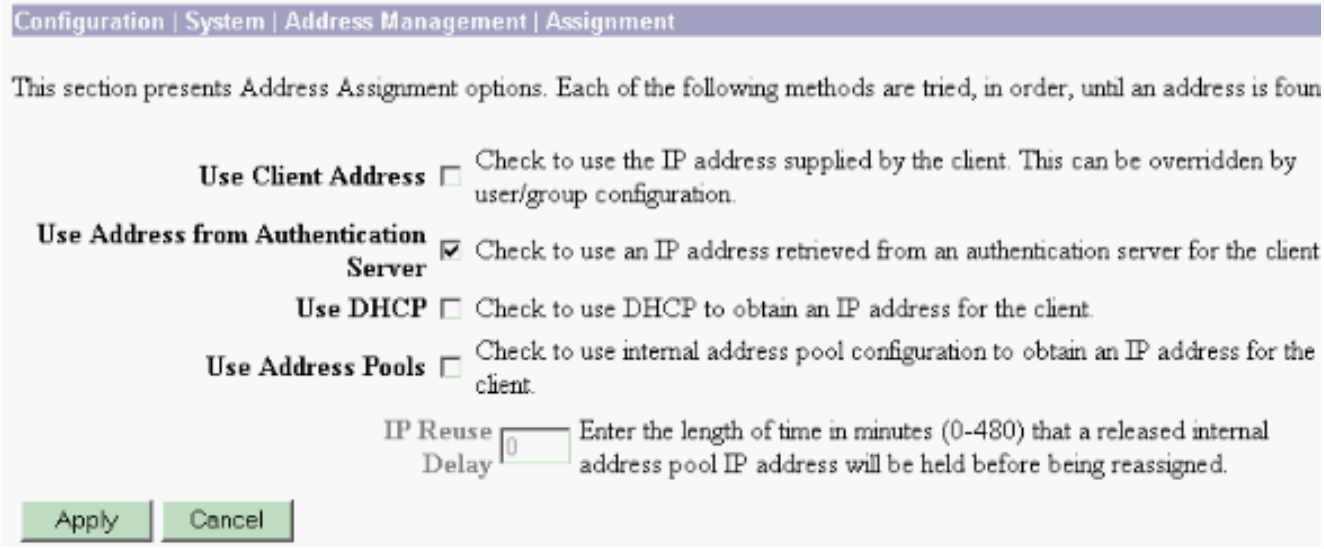
نوع النفق — أختر **الوصول عن بعد**.**المصادقة**—RADIUS. وهذا يوضح مركز الشبكة الخاصة الظاهرية (VPN) الطريقة التي يتم إستخدامها لمصادقة المستخدمين.**mode config**—**check mode config**.طقطقة **يطبق**.

4. أتمت هذا steps in order to شكلت يتعدد صحة هوية نادل على ال VPN 3000 مركز.بمجرد تعريف المجموعة، قم بتمييز هذه المجموعة، ثم انقر فوق **خوادم المصادقة** أسفل عمود التعديل. يمكن تعريف خوادم المصادقة الفردية لكل مجموعة حتى إذا لم تكن هذه الخوادم موجودة في الخوادم العمومية.



أخترت الخادم نوع **RADIUS**، وأضفت هذا معلم ل cisco يأمن ACS ل Windows RADIUS نادل. أترك كافة المعلمات الأخرى في حالتها الافتراضية.**خادم المصادقة**—أدخل عنوان IP الخاص بمصدر المحتوى الإضافي الآمن من Cisco لخادم Windows RADIUS.**سر الخادم**—أدخل سر خادم RADIUS. هذا ينبغي كنت ال نفسه سر يستعمل أنت عندما يشكل أنت ال VPN 3000 مركز في ال cisco يأمن ACS ل Windows تشكيل.**دققت**—أعدت الكلمة للتحقق.

5. أخترت **تشكيل>نظام>إدارة عنوان>تعيين** وفحصت **إستعمال عنوان من صحة هوية نادل** in order to عينت العنوان إلى ال VPN زبون من ال ip بركة يخلق في ال RADIUS نادل ما إن الزبون يحصل صحة هوية.



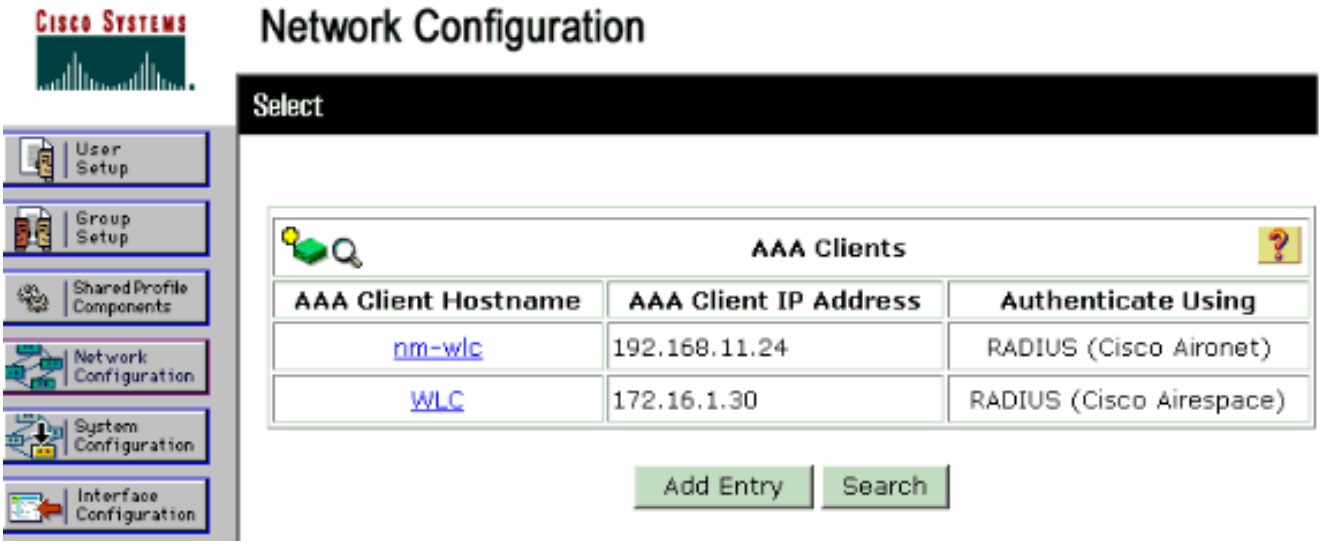
تكوين خادم RADIUS

يصف هذا القسم من المستند الإجراء المطلوب لتكوين ACS الآمن من Cisco كخادم RADIUS لمصادقة مستخدم عميل VPN التي تتم إعادة توجيهها بواسطة مركز سلسلة Cisco VPN 3000 - عميل AAA.

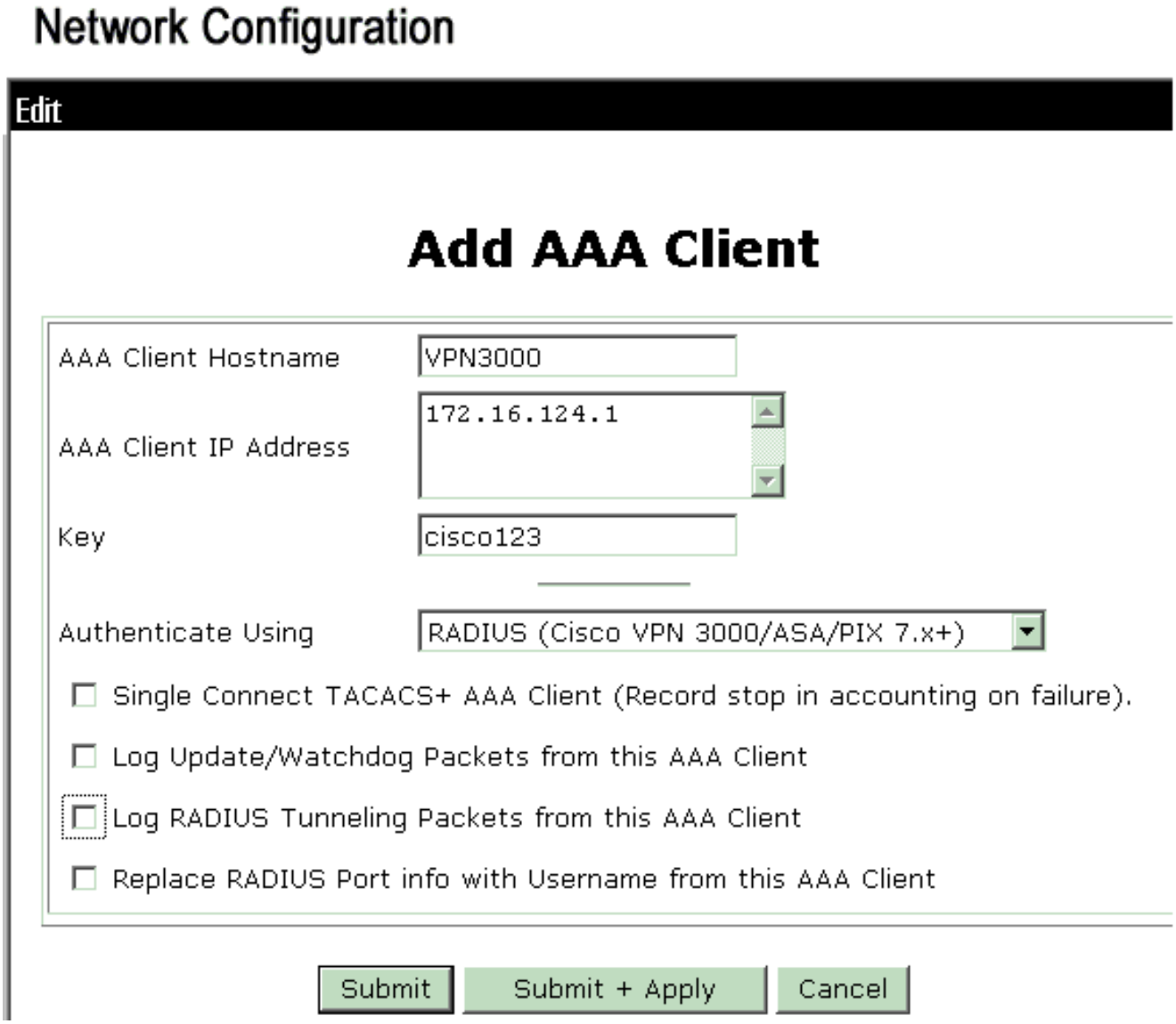
انقر نقرا مزدوجا على رمز **مسؤول ACS** لبدء جلسة عمل الإدارة على الكمبيوتر الشخصي الذي يشغل "مصدر المحتوى الإضافي الآمن من Cisco" لخادم Windows RADIUS. قم بتسجيل الدخول باستخدام اسم المستخدم

وكلمة المرور الملائمين، إذا لزم الأمر.

1. أتمت هذا steps in order to أضفت ال VPN 3000 مركز إلى ال cisco يأمن ACS ل Windows نادل تشكيل.أختر **تكوين الشبكة** وانقر فوق **إضافة إدخال** لإضافة عميل AAA إلى خادم RADIUS.

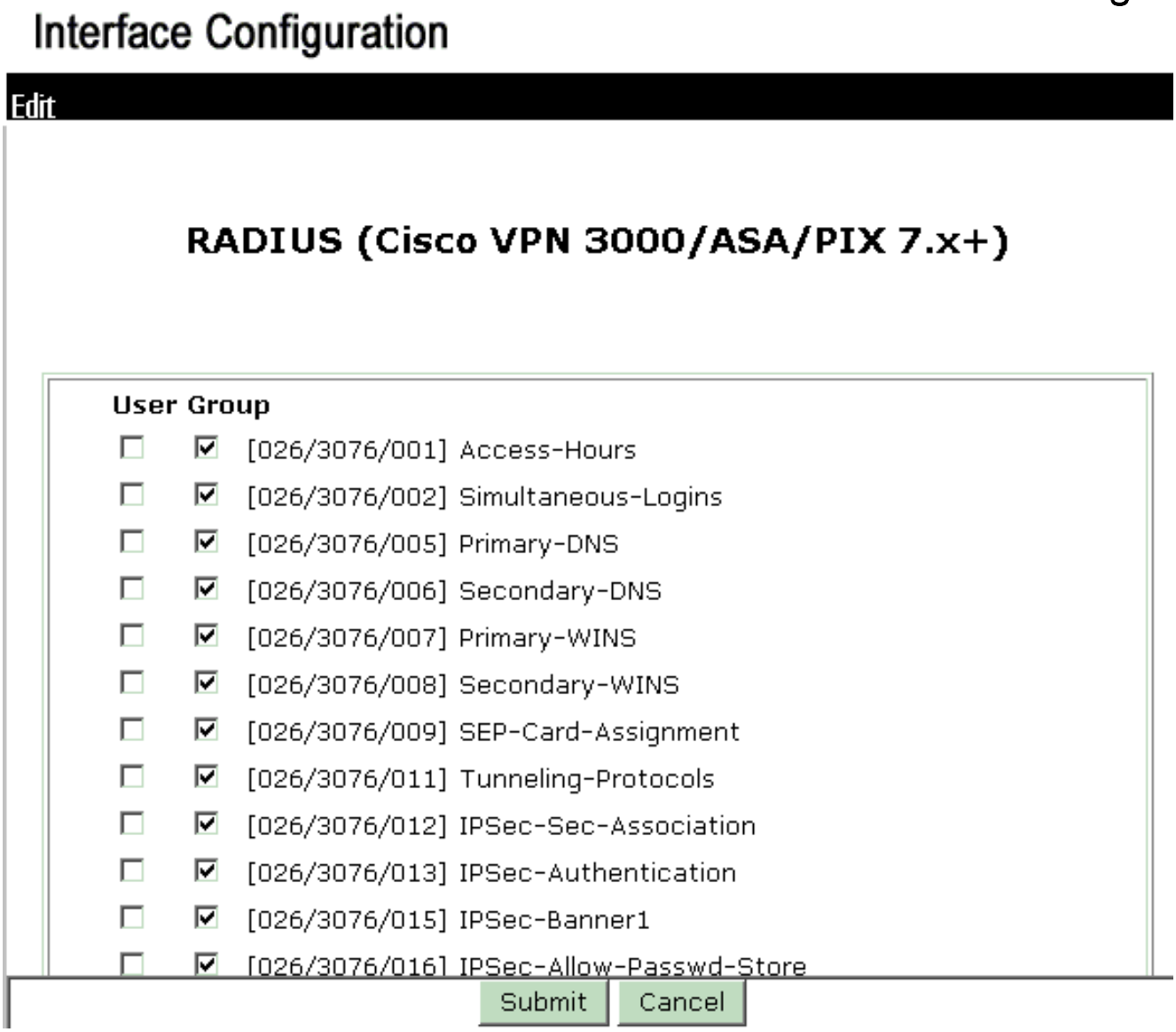


قم بإضافة هذه المعلمات لتمركز VPN 3000 لديك:



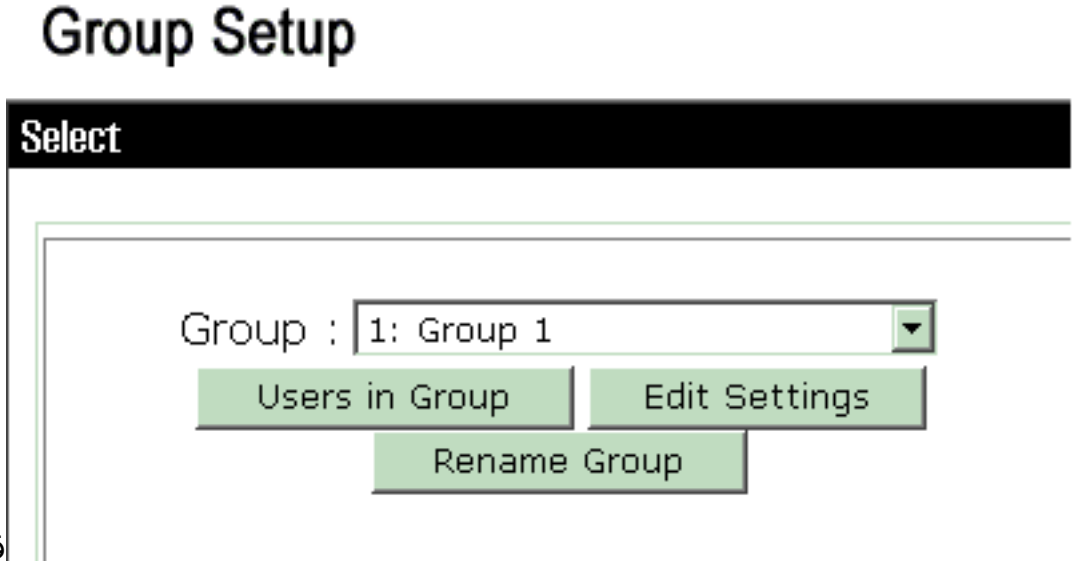
اسم مضيف عميل AAA— أدخل اسم المضيف الخاص بمركز VPN 3000 (لدقة DNS).**عنوان IP لعميل**

AAA—أدخل عنوان IP الخاص بمركز VPN 3000 لديك.**المفتاح**—أدخل سر خادم RADIUS. يجب أن يكون هذا هو السر نفسه الذي قمت بتكوينه عند إضافة خادم المصادقة على مركز VPN.**المصادقة باستخدام**—أختر **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**. وهذا يسمح ال VPN 3000 VSAs أن يعرض في المجموعة تشكيل نافذة.انقر على **إرسال**.أخترت **قارن تشكيل**، طقطقت **RADIUS (cisco VPN 3000/ASA/PIX 7.x+)**، وفحصت **مجموعة [26] بائع خاص**.



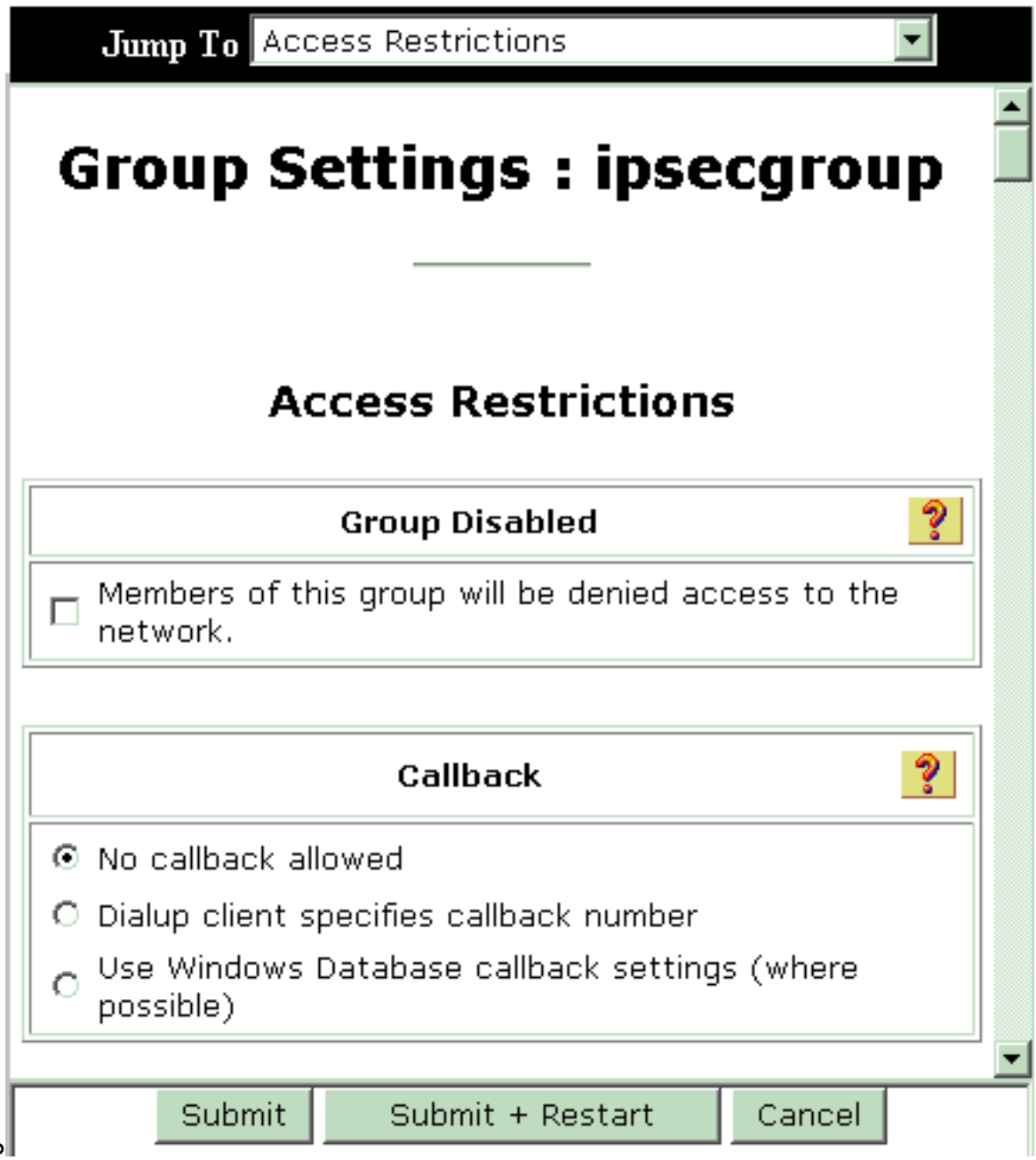
ملاحظة: تشير 'سمة RADIUS 26' إلى جميع السمات الخاصة بالمورد. على سبيل المثال، أختر **تكوين الواجهة > RADIUS (Cisco VPN 3000)** وانظر أن كل السمات المتاحة تبدأ مع 026. وهذا يوضح أن جميع هذه السمات الخاصة بالمورد تقع ضمن معيار IETF RADIUS 26. لا تظهر هذه السمات في إعداد المستخدم أو المجموعة بشكل افتراضي. خلقت in order to ظهرت في المجموعة AAA، setup زبون (في هذه الحالة VPN 3000 مركز) أن يصدق مع RADIUS في الشبكة تشكيل. ثم تحقق من السمات التي تحتاج إلى الظهور في إعداد المستخدم أو إعداد المجموعة أو كليهما من تكوين الواجهة.ارجع إلى سمات RADIUS للحصول على مزيد من المعلومات حول السمات المتاحة واستخدامها.انقر على **إرسال**.

2. أتمت هذا steps in order to أضفت مجموعة إلى ال cisco يأمن acs ل Windows تشكيل.أختر **إعداد المجموعة**، ثم حدد واحدة من مجموعات القوالب، على سبيل المثال، المجموعة 1، وانقر **إعادة تسمية**



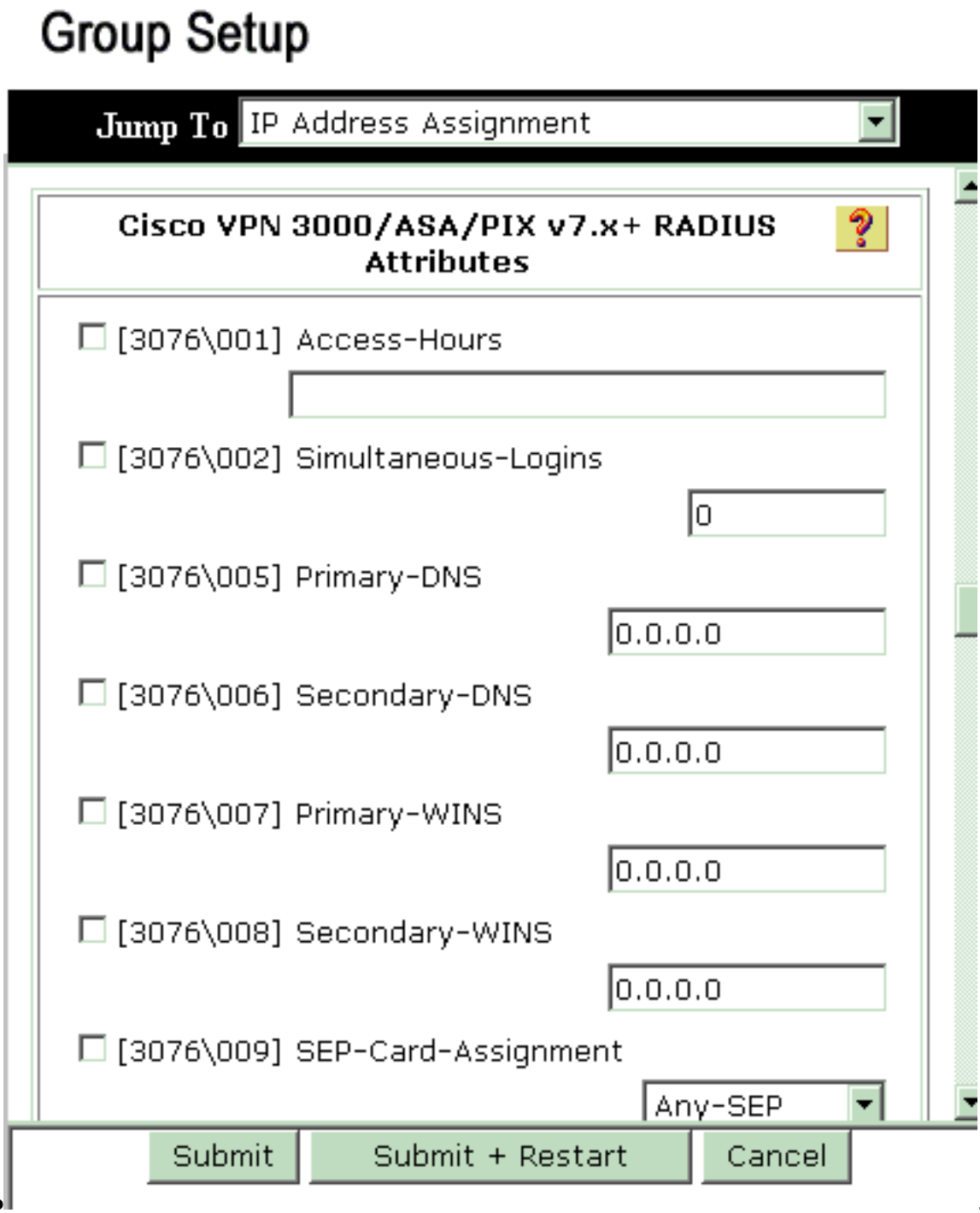
اقم **المجموعة**.

بتغيير الاسم إلى شيء مناسب لمؤسستك. على سبيل المثال، IPSECGROUP. بما أن المستخدمين تتم إضافتهم إلى هذه المجموعات، أجعل اسم المجموعة يعكس الغرض الفعلي لهذه المجموعة. إذا تم وضع جميع المستخدمين في نفس المجموعة، فيمكنك تسميتها مجموعة مستخدمي VPN.انقر فوق **تحرير الإعدادات** لتحرير المعلمات في مجموعتك التي تمت إعادة تسميتها



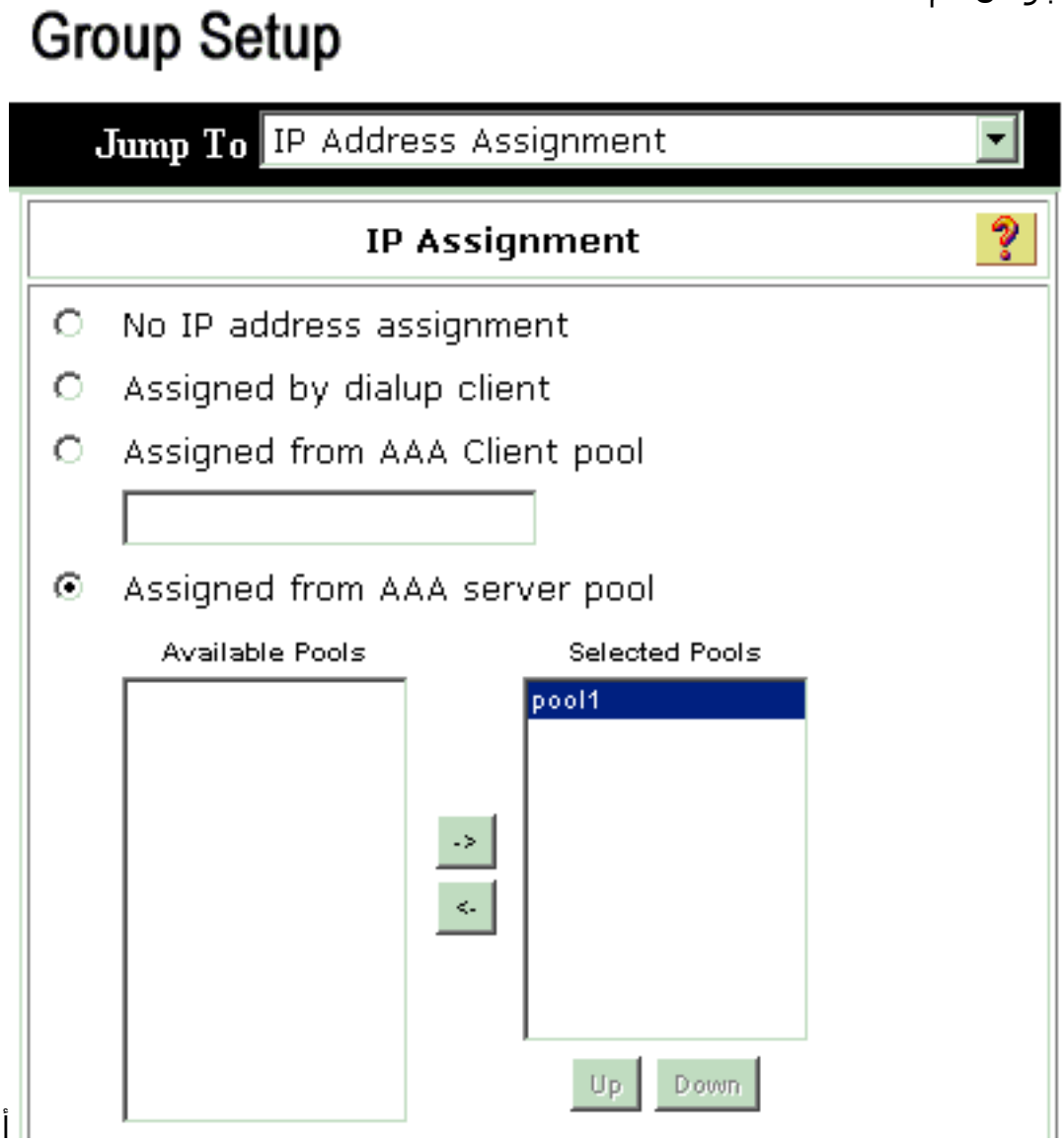
طقطقة حديثا.

ت cisco VPN 3000 RADIUS وشكلت هذا شعار يوصي. وهذا يسمح للمستخدمين المعينين لهذه المجموعة بإرث سمات RADIUS ل Cisco VPN 3000، والتي تتيح لك تمركز السياسات لجميع المستخدمين في Cisco Secure ACS ل



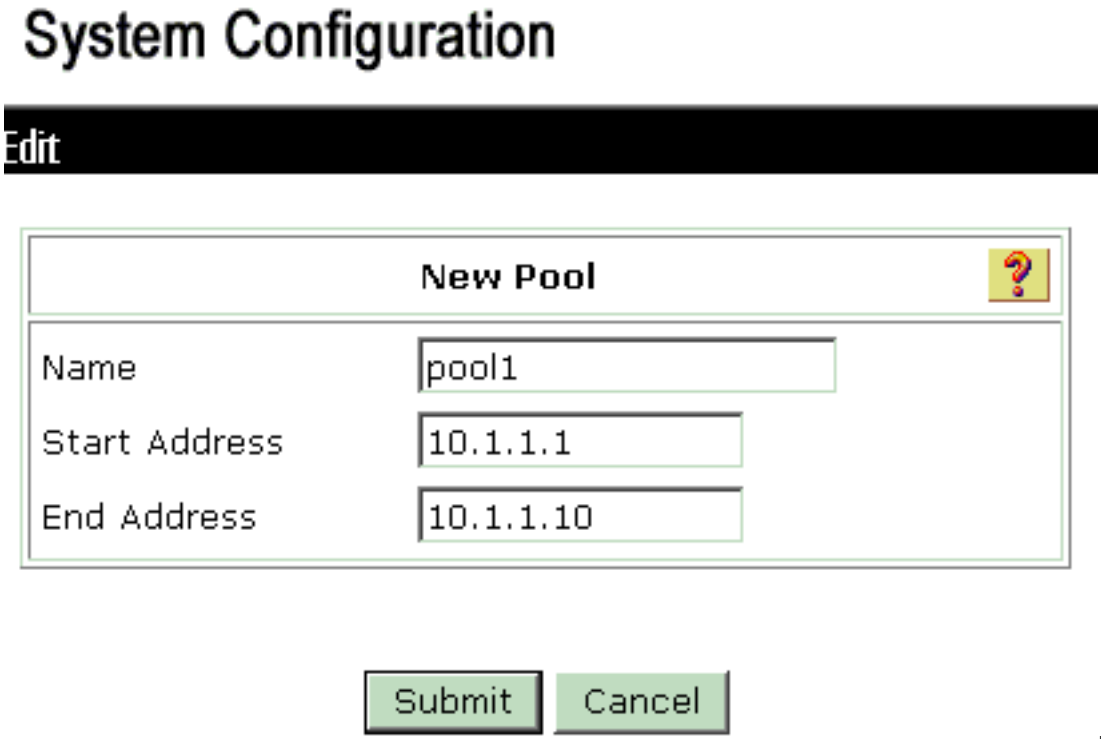
ملاحظة: من الناحية الفنية، لا يلزم تكوين سمات VPN 3000 RADIUS طالما تم إعداد مجموعة النفق في الخطوة 3 من تكوين مركز VPN Series 3000 ولا تتغير المجموعة الأساسية في مركز VPN من الإعدادات الافتراضية الأصلية.**سمات VPN 3000 الموصى بها:Primary-DNS**— أدخل عنوان IP الخاص بخادم DNS الأساسي.**DNS الثانوي**—أدخل عنوان IP الخاص بخادم DNS الثانوي الخاص بك.**Primary-WINS**— أدخل عنوان IP الخاص بخادم WINS الأساسي.**WINS الثانوي**—أدخل عنوان IP الخاص بخادم WINS الثانوي.**بروتوكولات الاتصال النفقي**— أختر **IPsec**. وهذا يسمح باتصالات عميل IPsec *فقط*. غير مسموح ب PPTP أو L2TP.**اقتران IPsec-sec**—أدخل **ESP-3DES-MD5**. وهذا يضمن اتصال جميع عملاء IPsec بأعلى تشفير متاح.**IPsec-allow-password-store**— أختر **عدم السماح** بحيث *لا* يسمح *للمستخدمين* بحفظ كلمة المرور الخاصة بهم في عميل VPN.**شعار IPsec**—أدخل شعار رسالة ترحيب ليتم تقديمه إلى المستخدم عند الاتصال. على سبيل المثال، "مرحبا بك في الوصول إلى الشبكة الخاصة الظاهرية (VPN) الخاصة بموظف شركتي!"**المجال الافتراضي ل IPsec**—أدخل اسم مجال شركتك. على سبيل المثال، "mycompany.com".هذه المجموعة من السمات غير ضرورية. غير أن إن يكون أنت غير متأكد إن القاعدة مجموعة يتغير شعار من ال VPN 3000 مركز، بعد ذلك cisco يوصي أن أنت تشكل هذا شعار:**عمليات تسجيل الدخول المتزامنة** — أدخل عدد المرات التي تسمح فيها للمستخدم بتسجيل الدخول في الوقت نفسه باسم المستخدم نفسه. التوصية هي 1 أو 2.**SEP-Card-Assign**—أختر **IPsec-mode-config**.**Any-SEP**— أختر Windows.

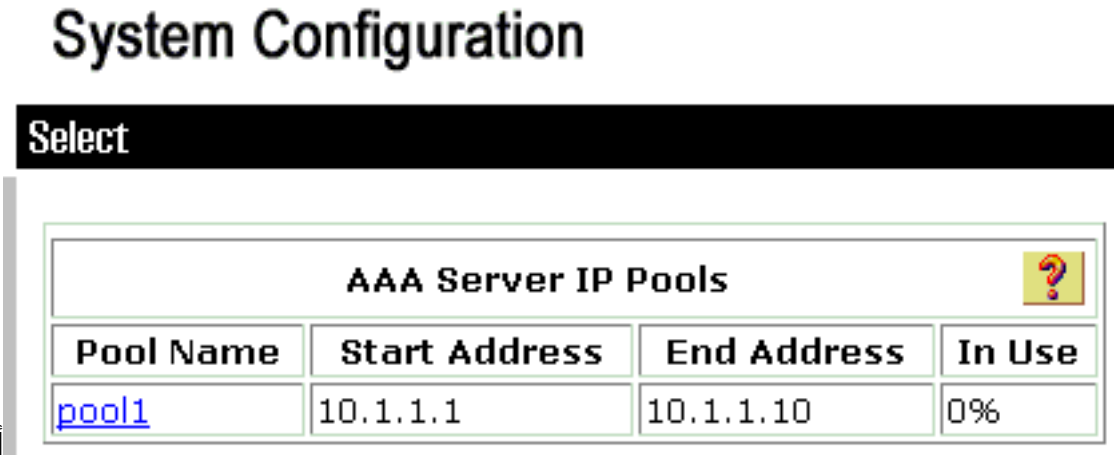
IPsec عبر UDP.ON— أختر **إيقاف التشغيل**، إلا إذا كنت تريد اتصال المستخدمين في هذه المجموعة باستخدام IPsec عبر بروتوكول UDP. إذا قمت بتحديد "تشغيل"، سيظل لعميل شبكة VPN القدرة على تعطيل IPsec محليا عبر بروتوكول UDP والاتصال بشكل طبيعي.**IPsec عبر منفذ UDP**—حدد رقم منفذ UDP في النطاق من 4001 إلى 49151. يتم إستخدام هذا فقط إذا كان IPsec عبر UDP قيد التشغيل.تتطلب المجموعة التالية من الخصائص أن تقوم بضبط شيء ما على مركز VPN أولا قبل أن تتمكن من إستخدامهم. يوصى بذلك للمستخدمين المتقدمين فقط.**ساعات الوصول**— يتطلب ذلك إعداد نطاق من ساعات الوصول على مركز VPN 3000 ضمن **التكوين > إدارة السياسة**. بدلا من ذلك، أستخدم "ساعات الوصول" المتوفرة في "مصدر المحتوى الإضافي الآمن من Cisco" ل Windows لإدارة هذه السمة.**IPsec-split-tunnel-list**— يتطلب هذا إعداد قائمة شبكة على مركز VPN تحت **التكوين > إدارة السياسة > إدارة حركة مرور البيانات**. هذه قائمة بالشبكات التي تم إرسالها إلى العميل والتي تخبر العميل بتشفير البيانات إلى تلك الشبكات الموجودة في القائمة فقط.أختر **تعيين IP في إعداد المجموعة** وفحص **التعيين من تجمع خوادم AAA** لتعيين عناوين IP لمستخدمي عميل VPN بمجرد أن تتم



مصادقتهم.

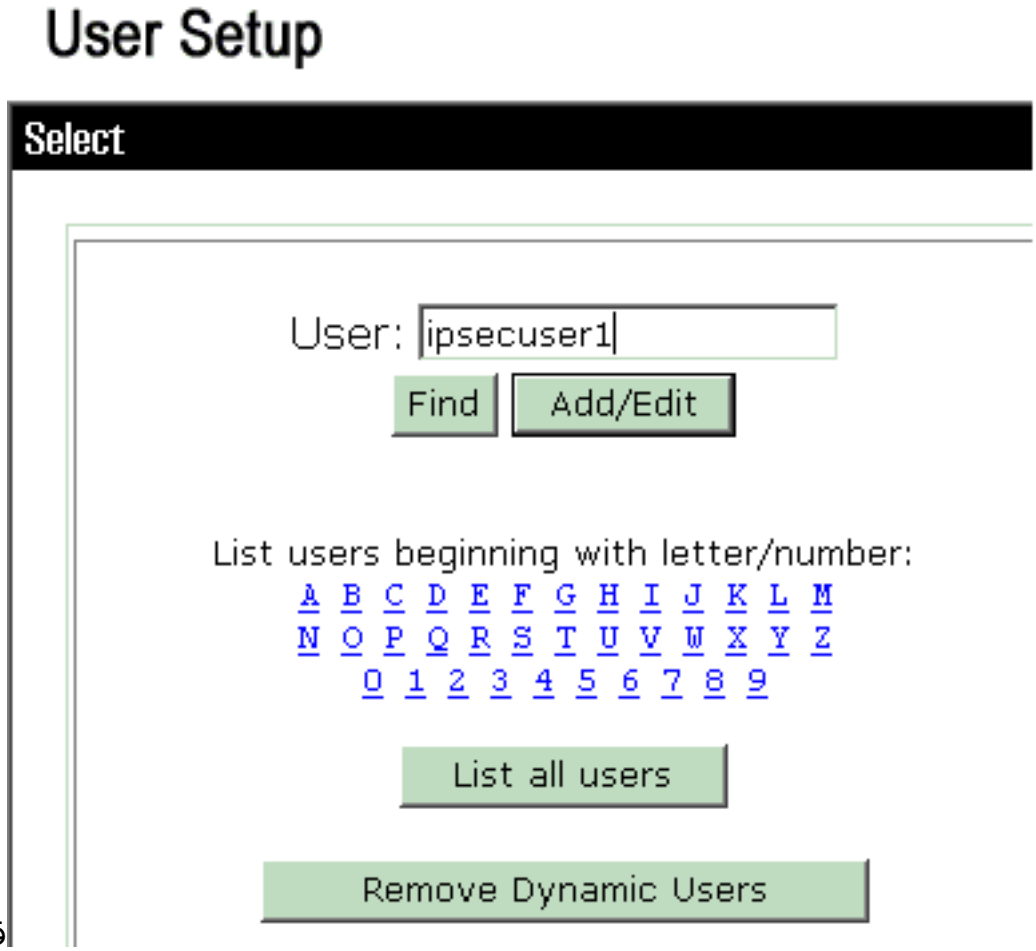
أخترت **نظام تشكيل>IP بركة** in order to خلقت IP بركة ل VPN زبون مستعمل وطقطقة **يرسل**





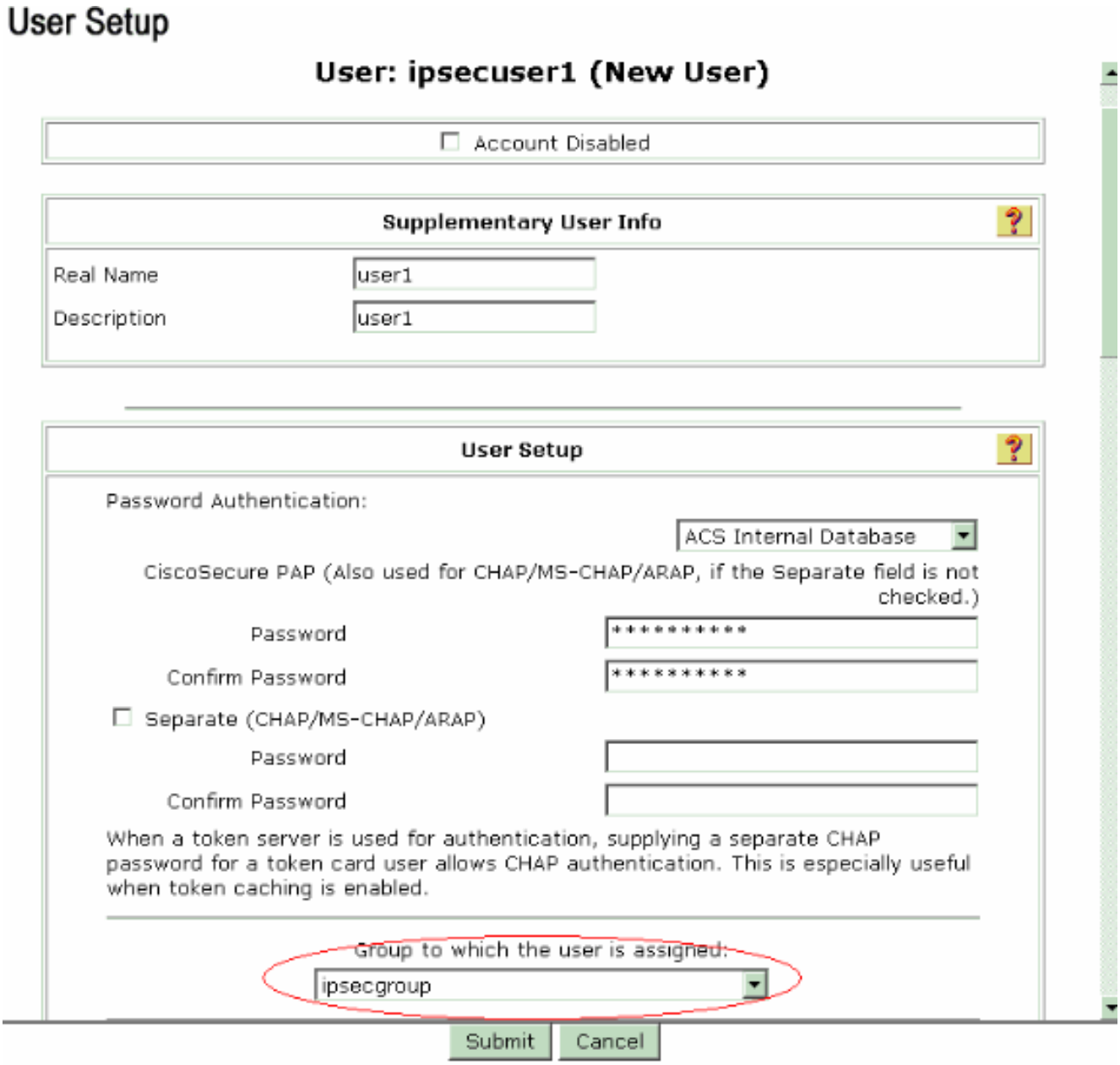
أختر **إرسال** >
إعادة التشغيل لحفظ التكوين وتنشيط المجموعة الجديدة.كرر هذه الخطوات لإضافة المزيد من المجموعات.

3. **تكوين المستخدمين على مصدر المحتوى الإضافي الآمن من Cisco ل Windows.**أختر **إعداد المستخدم**، وأدخل اسم مستخدم، وانقر فوق



قم بتكوين **إضافة/تحرير**.

هذه المعلمات ضمن قسم إعداد المستخدم:

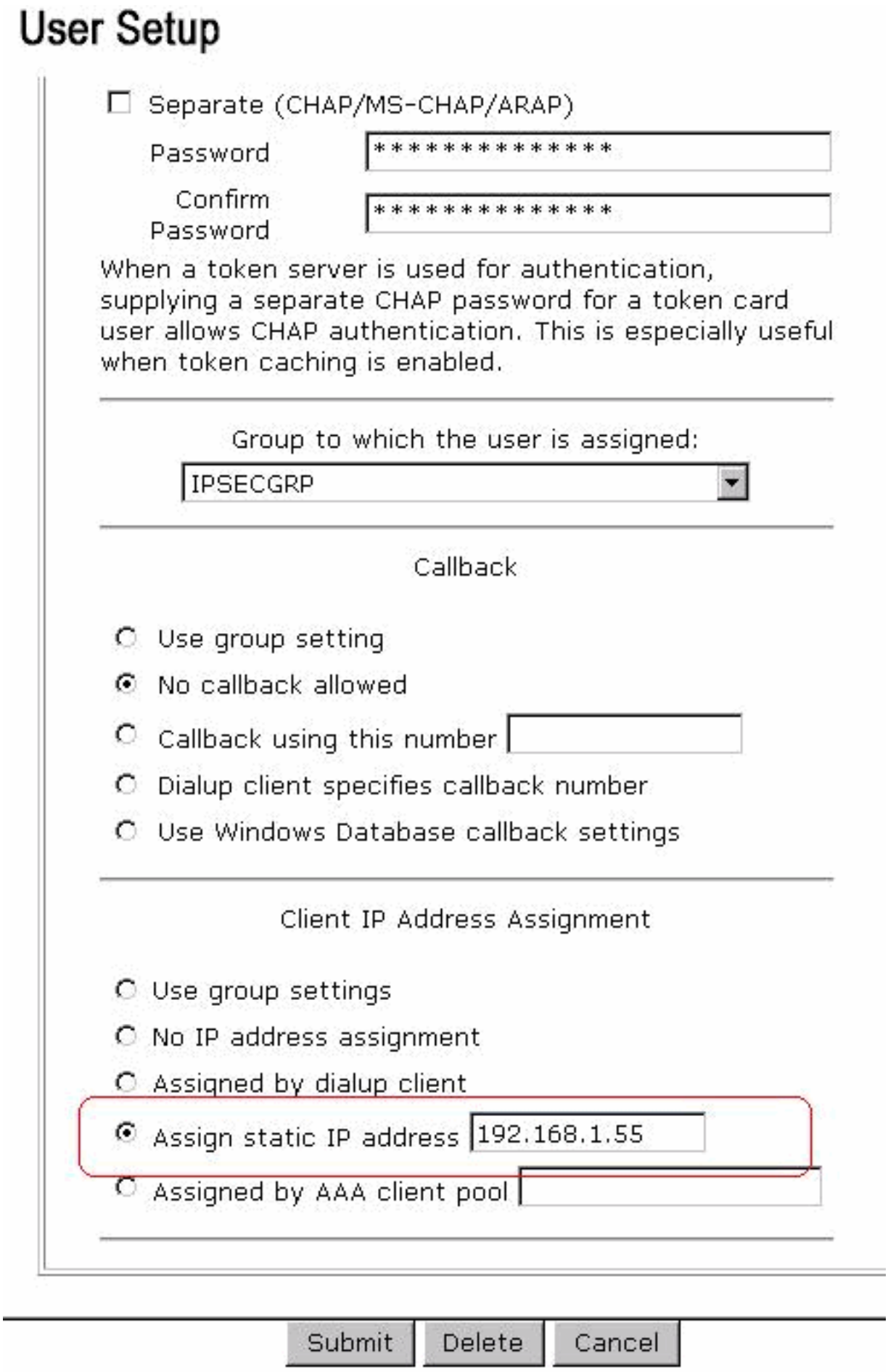


مصادقة كلمة المرور— أختر **قاعدة بيانات ACS الداخلية**.يدخل **PAP الآمن من Cisco كلمة** مرور للمستخدم.**Cisco Secure PAP** - تأكيد **كلمة المرور**- أعد إدخال كلمة المرور للمستخدم الجديد.**المجموعة التي يتم تعيين المستخدم لها**- حدد اسم المجموعة التي قمت بإنشائها في الخطوة السابقة.انقر فوق **إرسال** لحفظ إعدادات المستخدم وتنشيطها.كرر هذه الخطوات لإضافة مستخدمين إضافيين.

عينت عنوان ساكن إستاتيكي إلى ال VPN زبون مستعمل

أكمل الخطوات التالية:

1. إنشاء IPsecgrp جديد لمجموعة VPN.
2. قم بإنشاء مستخدم يريد تلقي IP الثابت واختر **IPSECGRP**. أخترت **يعين عنوان ساكن إستاتيكي** مع العنوان ساكن إستاتيكي أن يكون عينت تحت الزبون عنوان

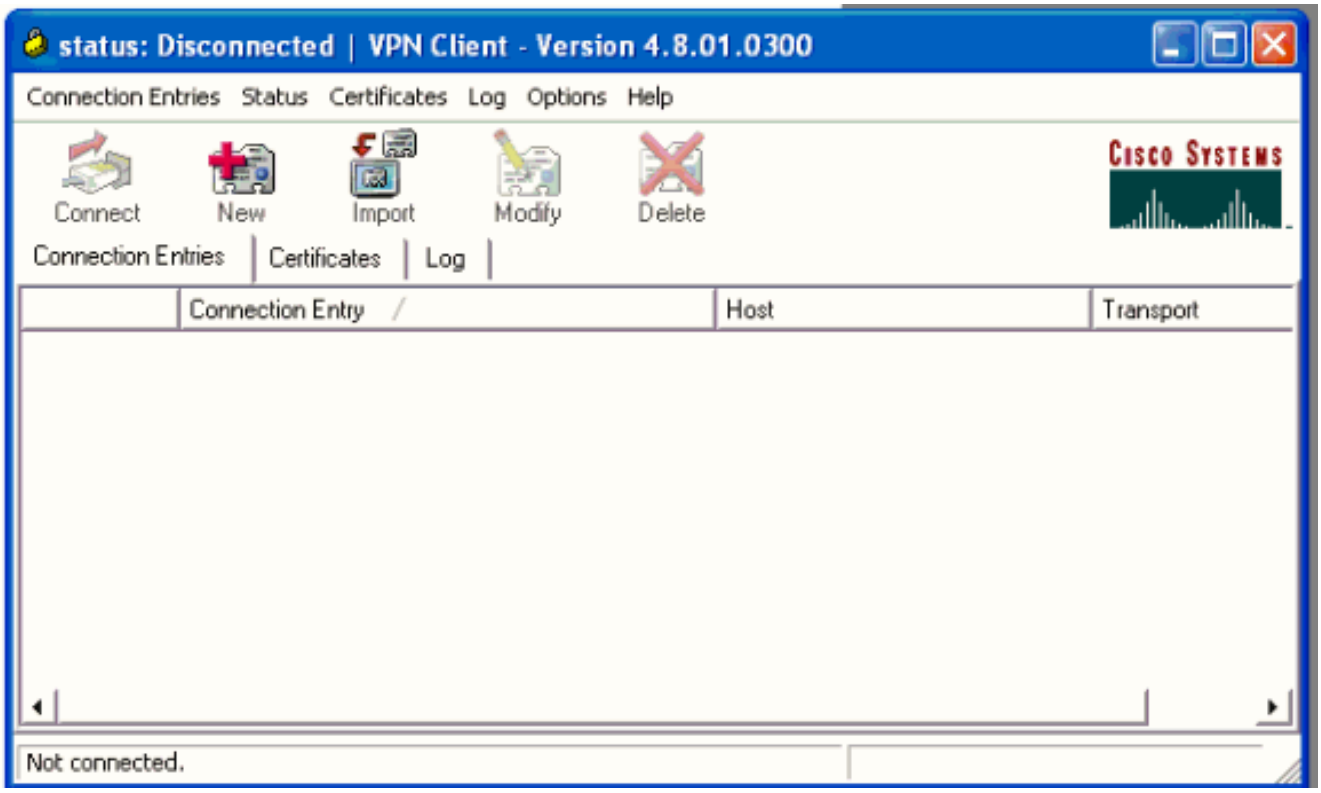


تنازل.

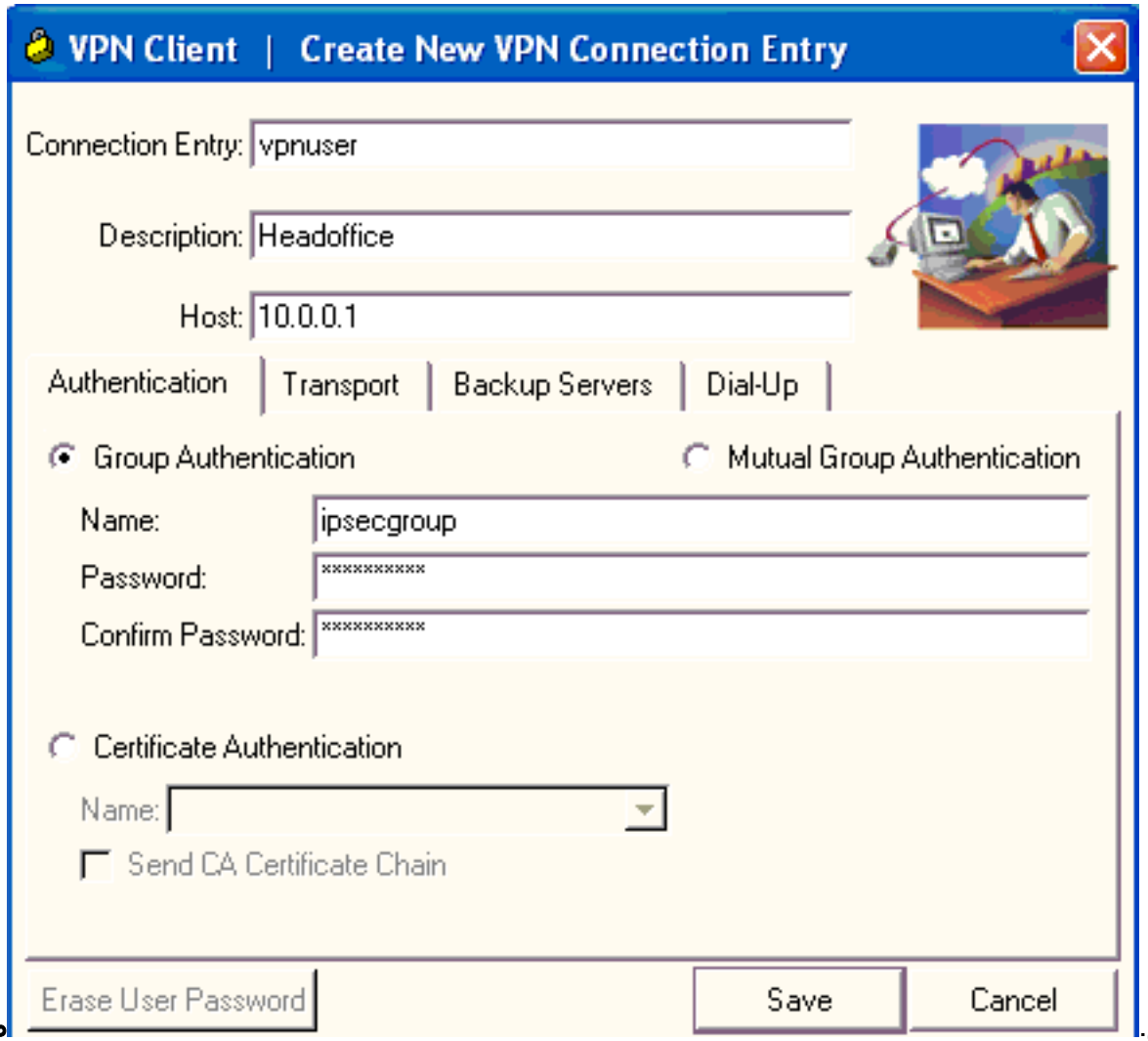
[تكوين عميل شبكة VPN]

يصف هذا القسم تكوين جانب عميل شبكة VPN.

1. أخترت **بداية>برنامج>Cisco Systems VPN زبون>VPN زبون**.
2. طقطقت **جديد** in order to أطلقت ال create جديد VPN توصيل مدخل نافذة.



3. عند مطالبتك، قم بتعيين اسم لإدخالك. يمكنك أيضا إدخال وصف إذا كنت تريد. عينت ال VPN 3000 مركز قارن عام عنوان في المضيف عمود واخترت **مجموعة صحة هوية** . ثم قم بتوفير اسم المجموعة وكلمة المرور. طقطقة **حفظ** in order to أتمت الجديد VPN توصيل

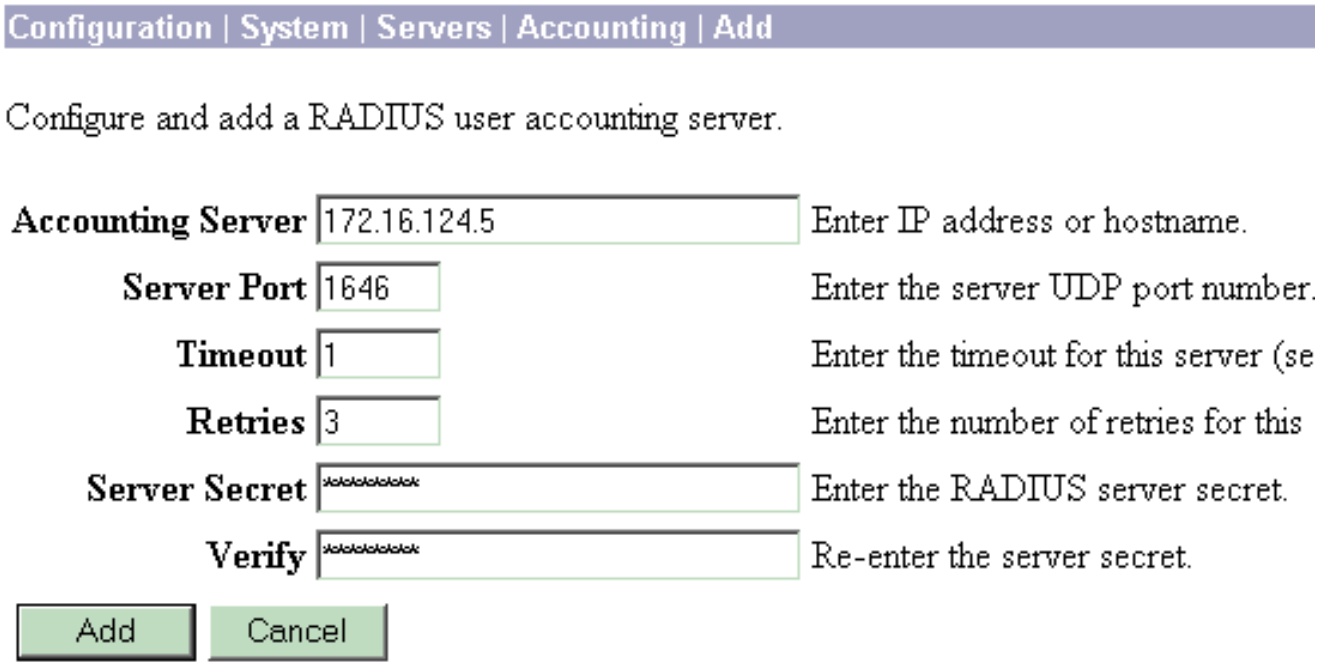


ملاحظة: تأكد من تكوين عميل VPN لاستخدام نفس اسم المجموعة وكلمة المرور التي تم تكوينها في مركز VPN 3000 Series من Cisco.

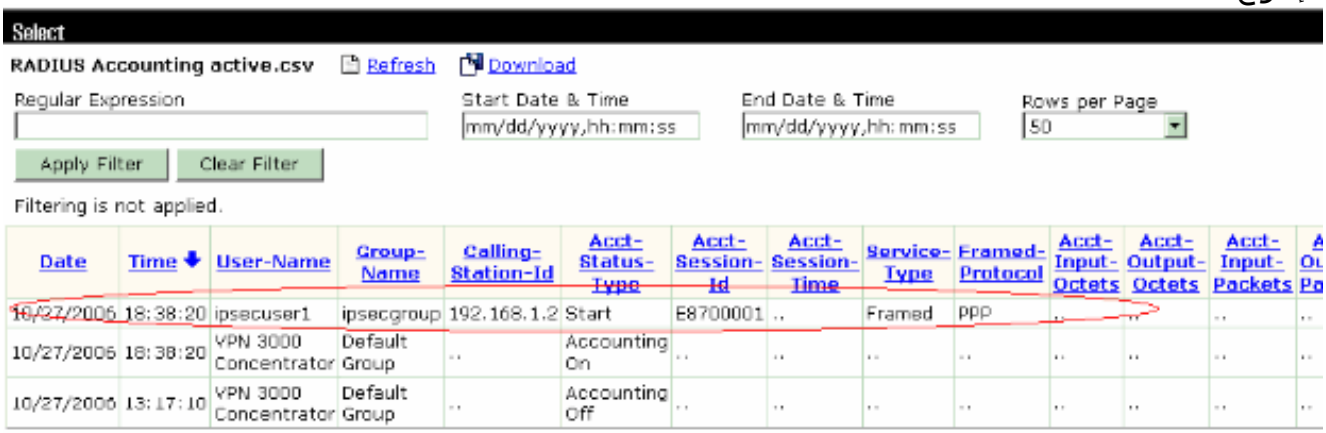
إضافة محاسبة

بعد عمل المصادقة، يمكنك إضافة عملية محاسبة.

1. على ال VPN 3000، أخترت **تشكيل>نظام>خادم>حساب نادل**، **وأضفت ال cisco يأمن ACS ل Windows** نادل.
2. يمكنك إضافة خوادم محاسبة فردية إلى كل مجموعة عندما تختار **تكوين > إدارة المستخدم > مجموعات**، يبرز مجموعة وانقر فوق **تعديل الوصول. الخوادم**. ثم أدخل عنوان IP الخاص بخادم المحاسبة مع سر الخادم.



في مصدر المحتوى الإضافي الآمن من Cisco ل Windows، تظهر سجلات المحاسبة كما يوضح هذا الإخراج:



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** .

التحقق من مركز VPN

على جانب مركز الشبكة الخاصة الظاهرية (VPN) 3000، أختر **إدارة > إدارة جلسات العمل** للتحقق من إنشاء نفق VPN البعيد.

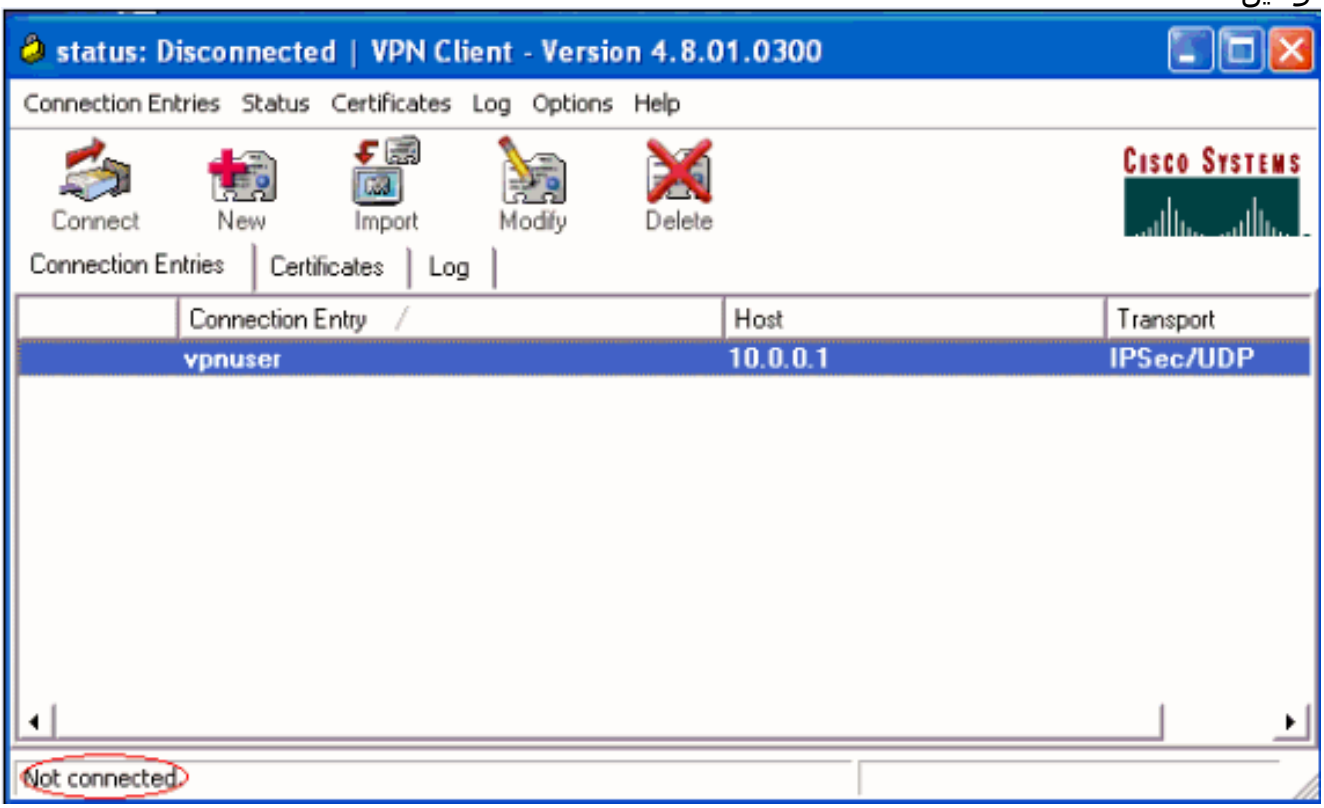
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout	Ping]

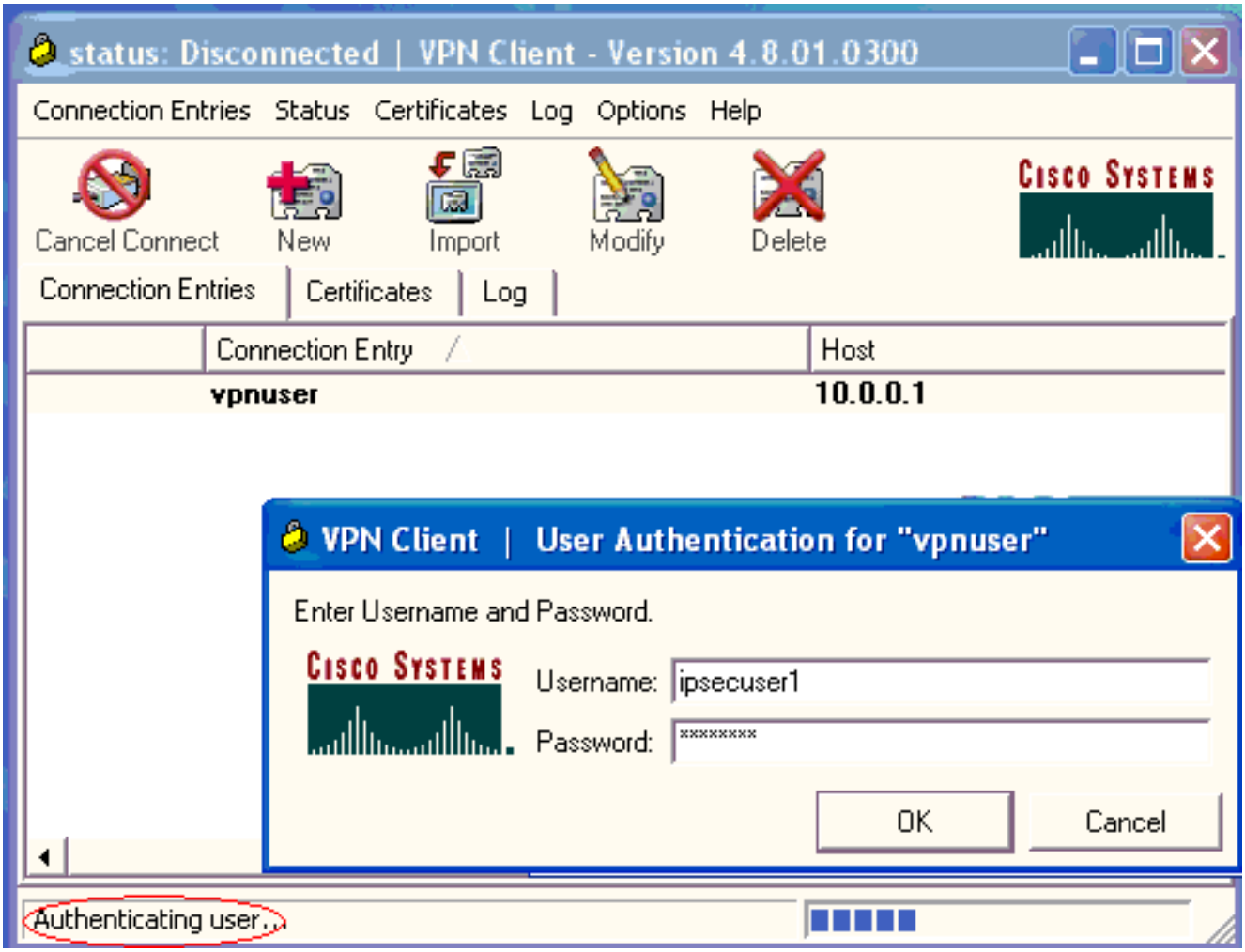
التحقق من عميل شبكة VPN

أتمت هذا steps in order to دققت ال VPN عميل.

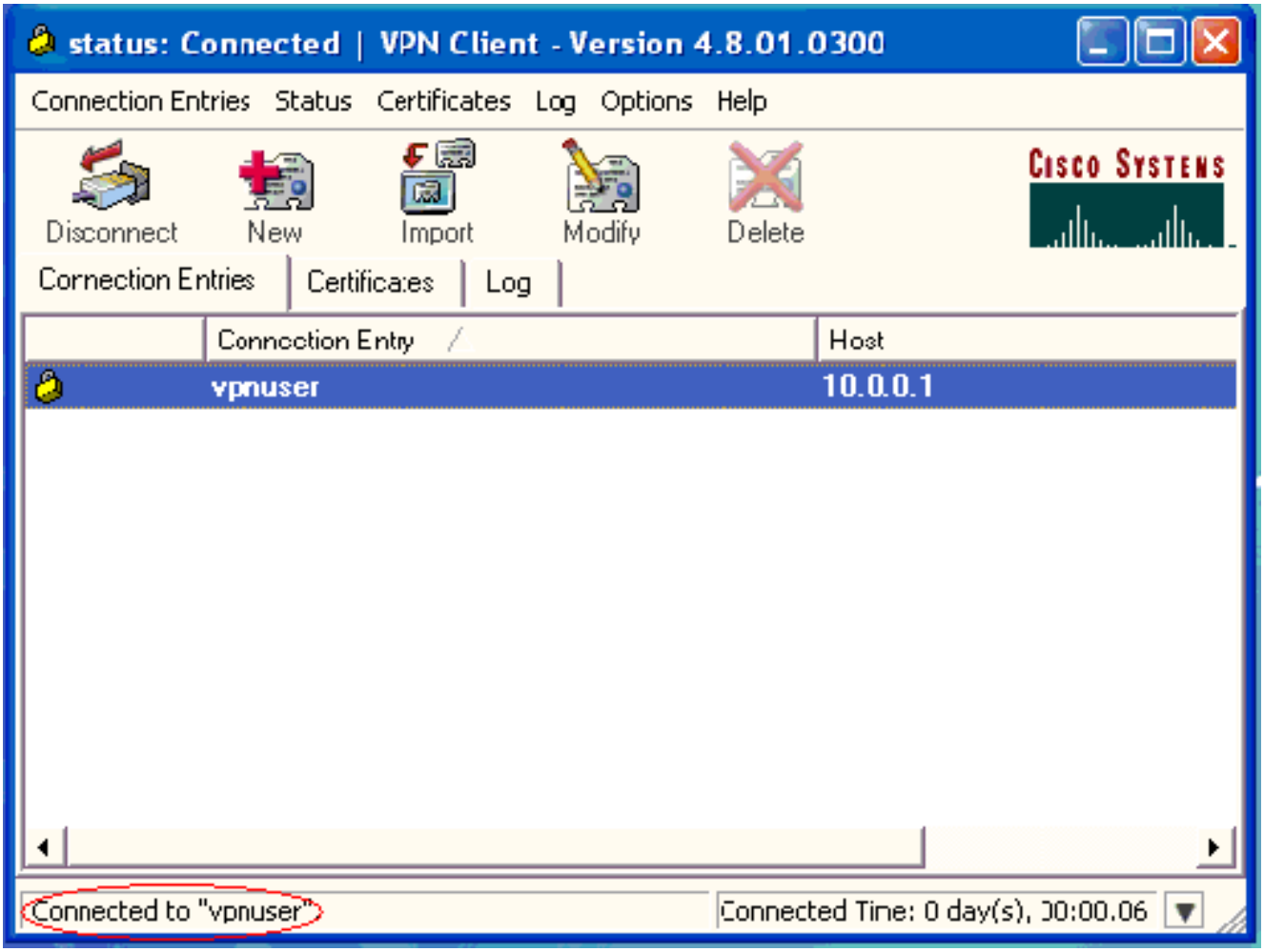
1. طقطقة **يربط** in order to بدأت VPN توصيل.



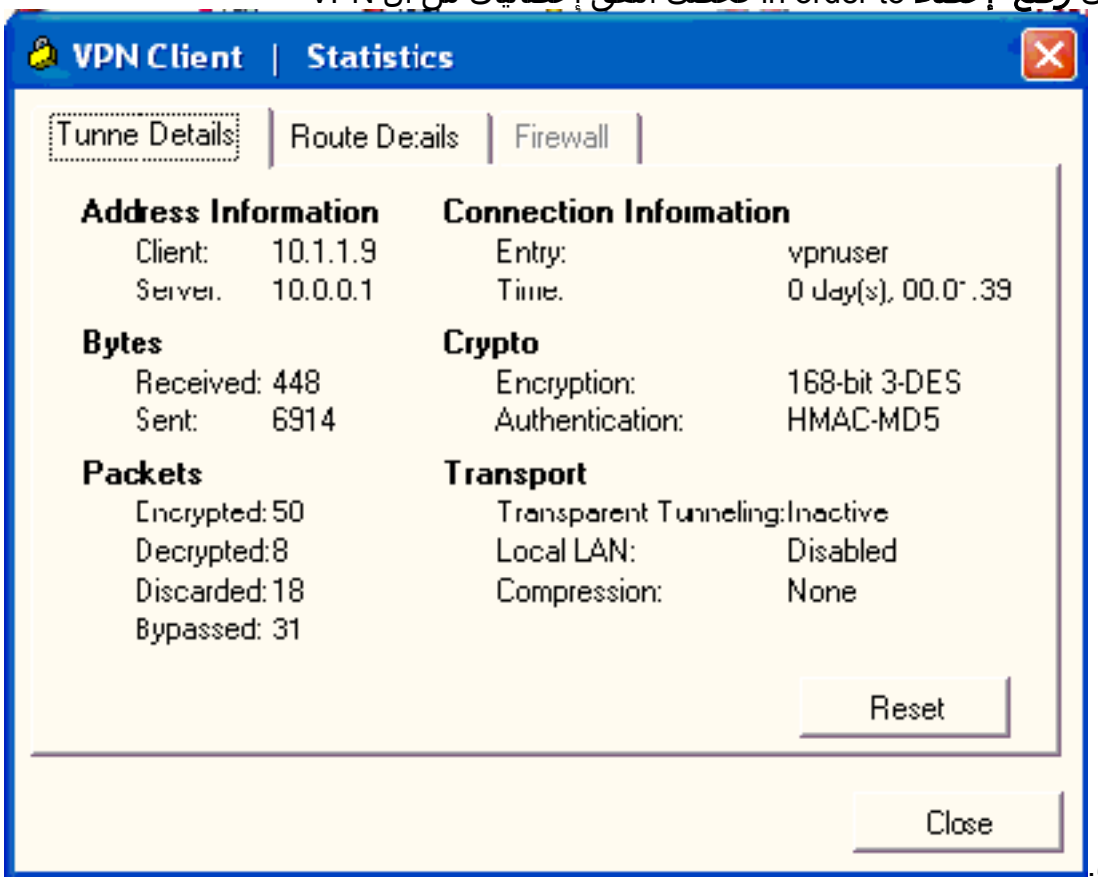
2. يظهر هذا نافذة لمصادقة المستخدم. أدخل اسم مستخدم وكلمة مرور صحيحين لإنشاء اتصال VPN.



3. يتم توصيل عميل الشبكة الخاصة الظاهرية (VPN) بمركز الشبكة الخاصة الظاهرية (3000 (VPN في الموقع المركزي.



4. أخترت **وضع>إحصاء** in order to فحصت النفق إحصائيات من إل VPN

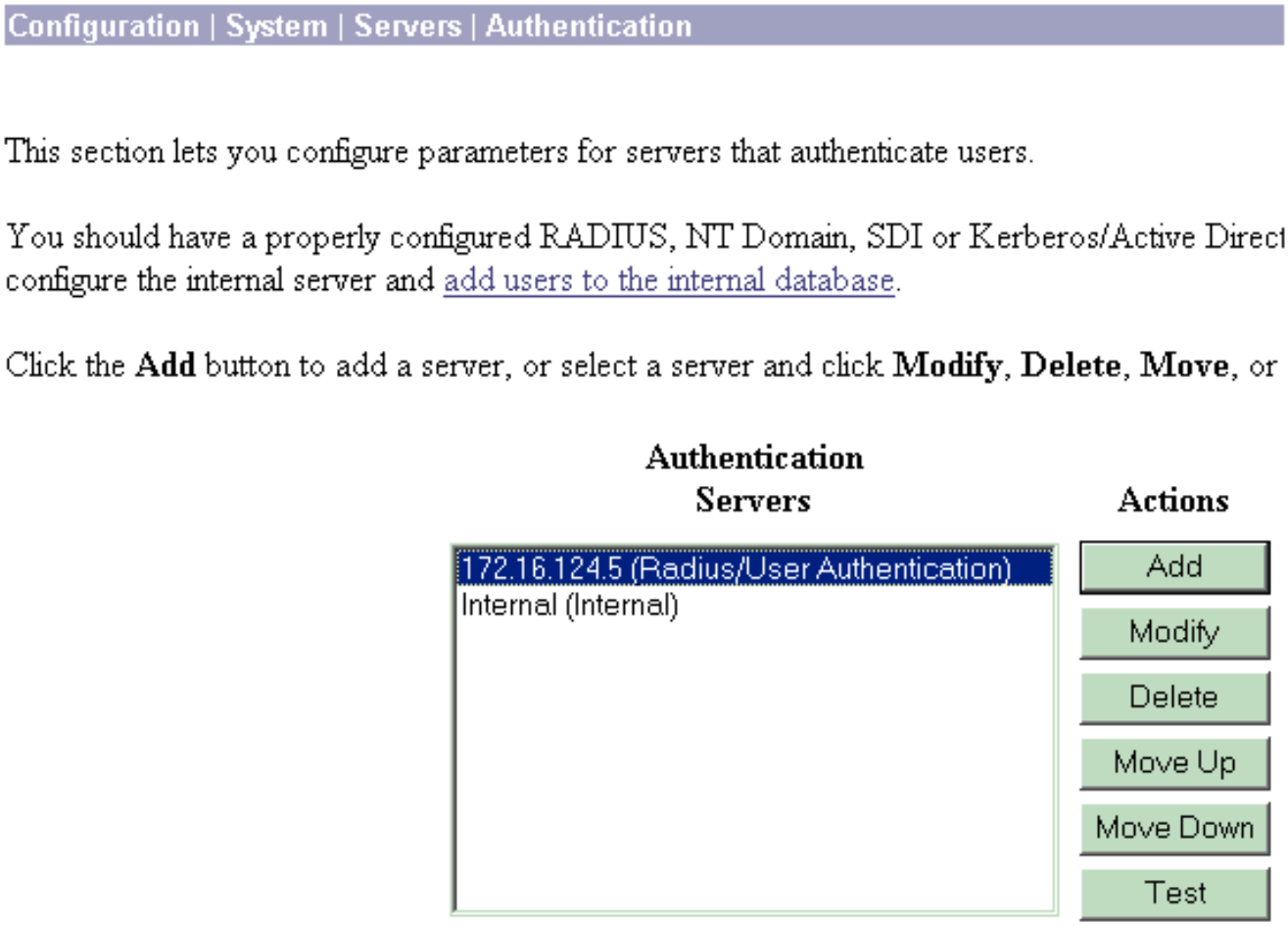


زبون.

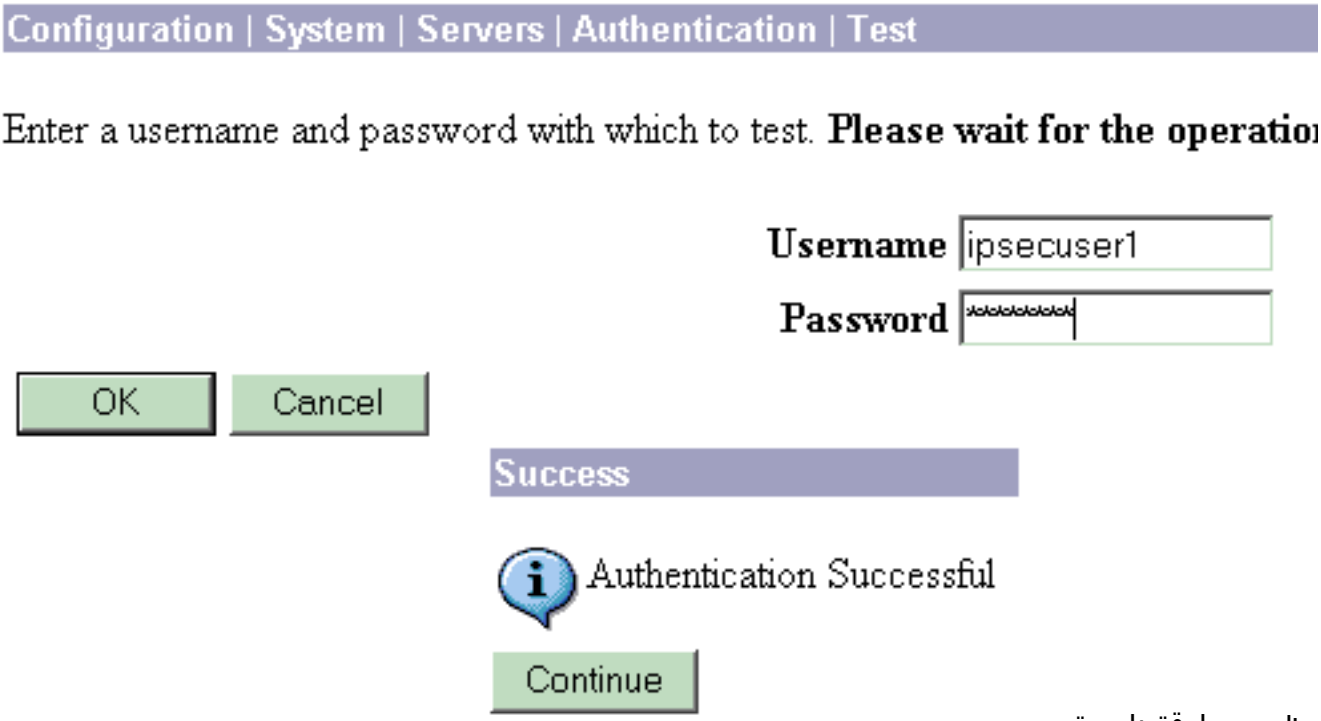
استكشاف الأخطاء وإصلاحها

أتمت هذا steps in order to تحريت تشكيلك.

1. أخترت **تشكيل>نظام>نادل>صحة هوية** وأتمت هذا steps in order to اختبرت الموصولية بين ال RADIUS نادل و VPN 3000 مركز.حدد الخادم، ثم انقر فوق **إختبار**.



أدخل اسم مستخدم وكلمة مرور RADIUS وانقر على **موافق**.

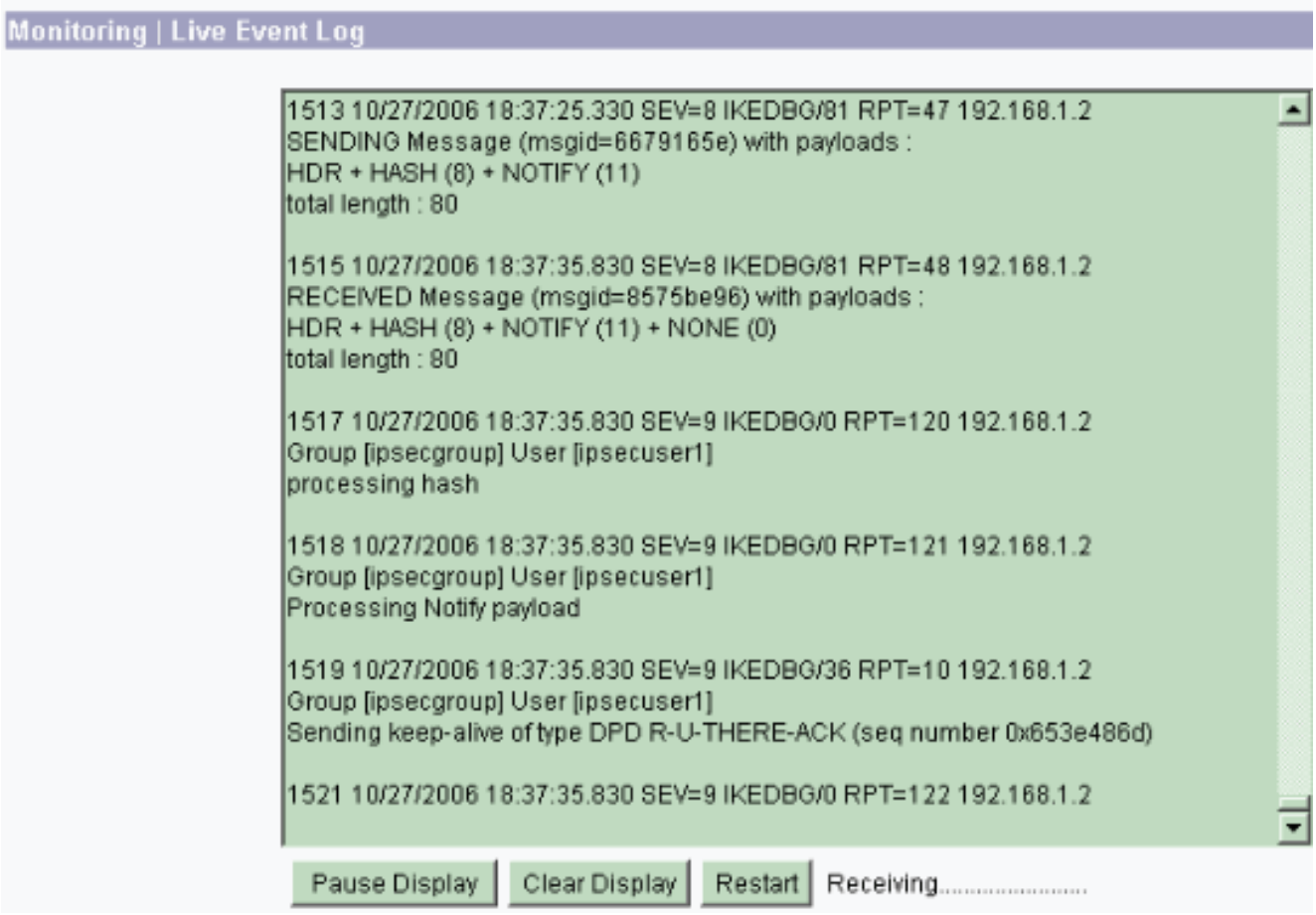


تظهر مصادقة ناجحة.

2. إن يفشل هو، هناك إما مشكلة تشكيل أو ip موصولية إصدار. تحقق من "سجل المحاولات الفاشلة" الموجود

على خادم ACS بحثا عن الرسائل المتعلقة بهذا الفشل.إذا لم تظهر أي رسائل في هذا السجل، فمن المحتمل أن تكون هناك مشكلة في اتصال IP. لا يصل طلب RADIUS إلى خادم RADIUS. تحقق من المرشحات المطبقة على واجهة مركز VPN 3000 المناسبة التي تسمح لحزم (1645 RADIUS) بالدخول والخروج.إذا كانت مصادقة الاختبار ناجحة، وتستمر عمليات التسجيل في الدخول إلى مركز VPN 3000 في الفشل، فتحقق من سجل الأحداث القابل للتصفية عبر منفذ وحدة التحكم.إذا لم تعمل الاتصالات، فيمكنك إضافة فئات أحداث AUTH و IKE و IPsec إلى مركز VPN عند تحديد **التكوين > النظام > الأحداث > الفئات > التعديل (الخطورة إلى السجل=1-9، الخطورة إلى وحدة التحكم=1-3)**. كما تتوفر AUTHDBG و AUTHDECODE و iKEDBG و iKedecode و IPSECDBG و IPSECDECODE، ولكنها يمكن أن توفر معلومات كثيرة جدا. إذا كانت هناك حاجة إلى معلومات تفصيلية حول السمات التي يتم تمريرها من خادم RADIUS، فإن AUTHDECODE و iKedecode و IPSECDECODE توفر هذا عند مستوى مستوى مستوى مستوى مستوى مستوى مستوى الخطورة إلى سجل=1-13.

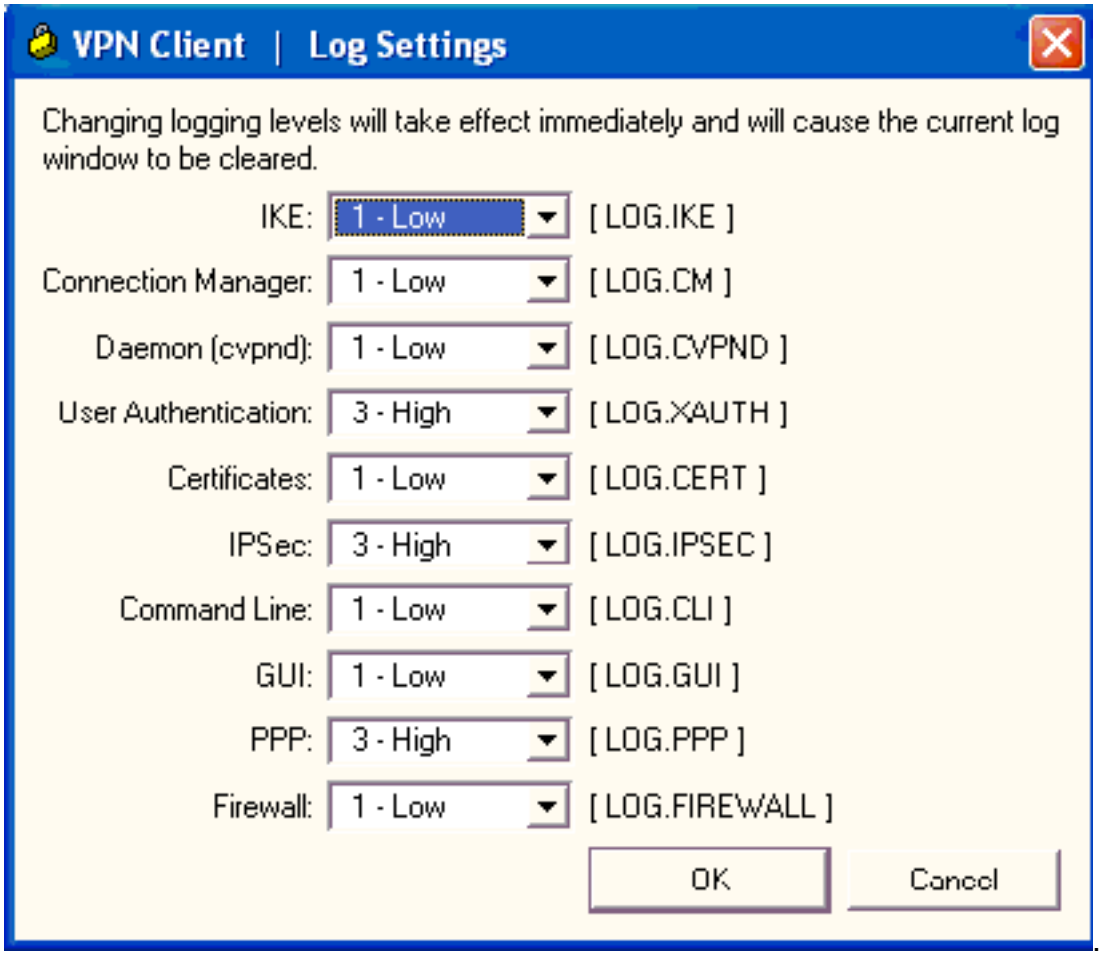
3. قم باسترداد سجل الأحداث من **المراقبة > سجل الأحداث**.



أستكشاف أخطاء VPN Client 4.8 وإصلاحها ل Windows

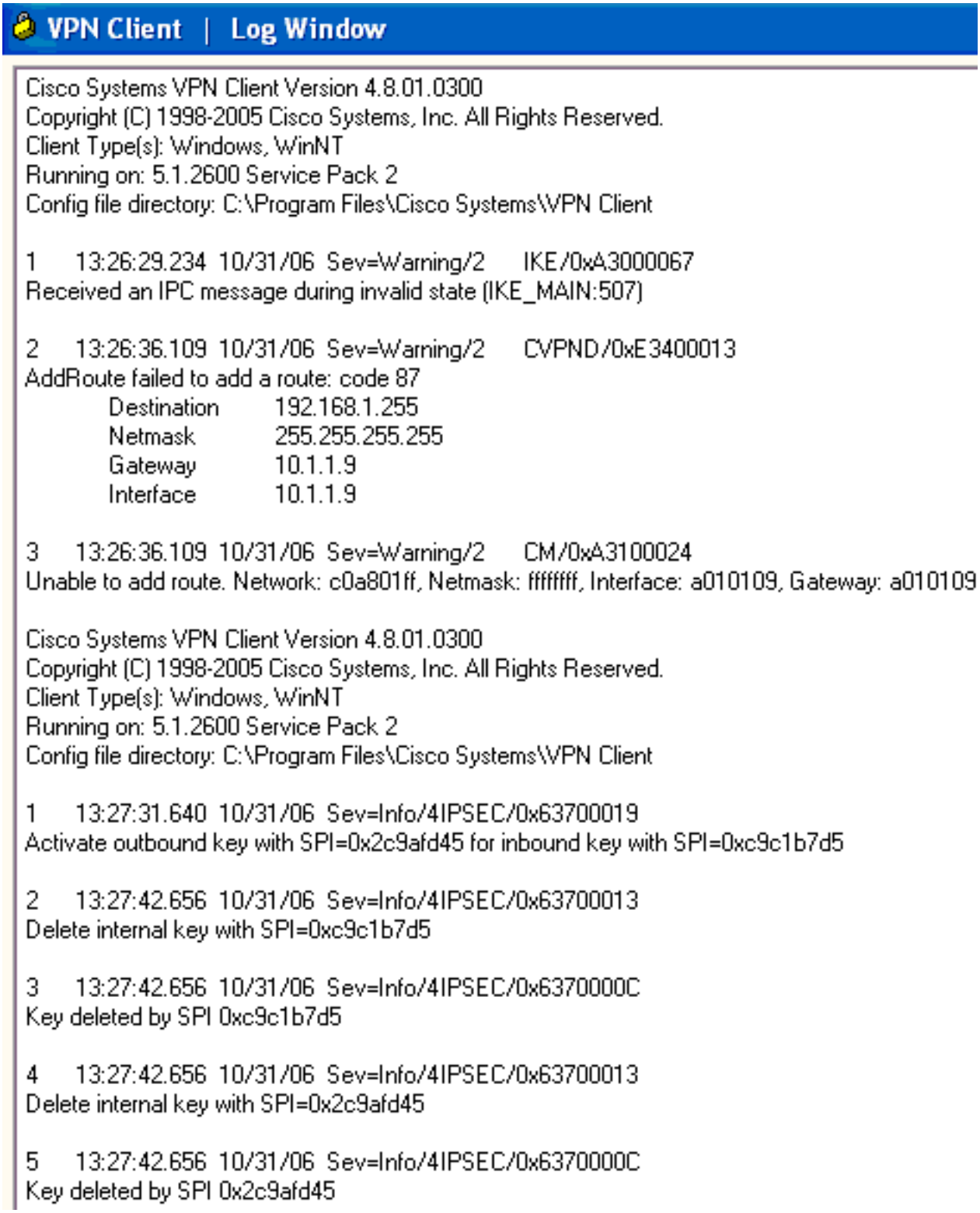
أتمت هذا steps in order to تحريت VPN زبون 4.8 ل Windows.

1. أخترت **سجل>سجل عملية إعداد** in order to مكنت السجل مستوى في ال VPN



زبون.

2. أخترت **سجل>سجل نافذة** in order to شاهدت ال log مدخل في ال VPN زبون.



معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم عميل شبكة VPN من Cisco
- مفاوضة IPSec/بروتوكولات IKE
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- تكوين المرشحات الديناميكية على خادم RADIUS
- 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).