在VPN 3000集中器和VPN客户端4.x之间的RADIUS使用用户认证和记帐的IPSec配置示例

目录

简介

本文描述如何设立在Cisco VPN 3000集中器和使用RADIUS用户认证和核算的Cisco VPN Client Microsoft Windows的4.x之间的一个IPSec隧道。本文推荐思科安全访问控制服务器(ACS)更加容易的RADIUS配置的Windows的能验证连接到VPN 3000集中器的用户。VPN 3000集中器的一组是对待单个实体用户的一集。组的配置，与个人用户相对，能简单化系统管理和简化配置任务。

参考的Windows的PIX/ASA 7.x和Cisco VPN Client 4.x与Microsoft Windows 2003 IAS RADIUS验证配置示例为了设置Cisco VPN Client (4.x Windows的)和使用一个Microsoft Windows 2003年互联网认证服务(IAS) RADIUS服务器的PIX 500系列安全工具7.x之间的远程访问虚拟专用网连接。

参考配置在Cisco IOS路由器和Cisco VPN Client Windows的4.x之间的IPsec使用用户认证的RADIUS为了配置路由器和使用RADIUS用户认证的Cisco VPN Client 4.x之间的一连接。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure ACS for Windows RADIUS正常安装并且用其它设备运行。
- Cisco VPN 3000集中器配置并且可以管理与HTML界面。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 与版本4.0的Cisco Secure ACS for Windows
- Cisco VPN 3000系列集中器用镜像文件4.7.2.B
- Cisco VPN 客户端 4.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

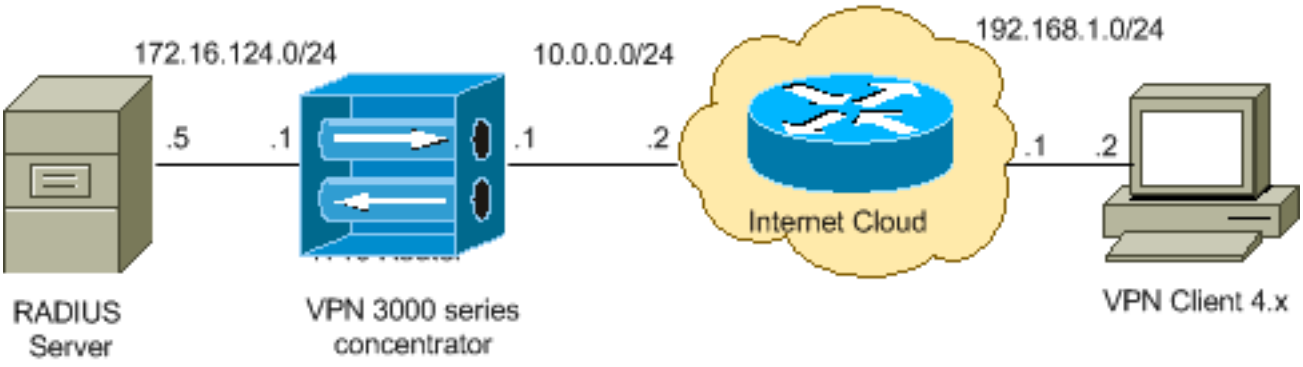
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

请使用VPN 3000集中器的组

组可以为两Cisco Secure ACS for Windows和VPN 3000集中器定义，但是他们某种程度不同使用组。执行这些任务为了简化事：

- 当您设立最初的通道时，请**配置VPN 3000集中器的一组**为。这经常呼叫隧道组使用预先共享密钥(组密码)，并且用于建立一个已加密Internet Key Exchange (IKE)会话到VPN 3000集中器。这是在所有Cisco VPN Client应该配置要连接到VPN集中器的同一个组名和密码。
- **配置**使用标准RADIUS属性和卖方细节属性**Cisco Secure ACS for Windows服务器的组**(VSAs)策略管理。应该用VPN 3000集中器使用的VSAs是RADIUS (VPN3000)属性。
- **配置Cisco Secure ACS for Windows RADIUS服务器的用户并且分配他们到**在同一个服务器配置的其中**一组**。用户继承为他们的组定义的属性，并且Cisco Secure ACS for Windows发送那些属性到VPN集中器，当用户验证时。

VPN 3000 集中器如何使用组和用户属性

在VPN 3000集中器验证有VPN集中器和用户的隧道组有RADIUS的后，接收的必须组织属性。VPN集中器在此优先级顺序使用属性，验证是否执行在VPN集中器或与RADIUS ：

1. **用户属性**—这些属性总是优先于所有其他。
2. **隧道组属性**—没返回的所有属性，当用户验证由隧道组属性填写。
3. **基本组属性**—所有属性未命中从用户的或隧道组属性由VPN集中器基本组属性填写。

VPN 3000系列集中器配置

完成在此部分的步骤为了配置参数的Cisco VPN 3000集中器要求对IPSec连接以及AAA客户端VPN用户的能用RADIUS服务器验证。

在此实验室设置， VPN集中器通过控制台端口首先访问，并且最小配置被添加，当此输出显示：

```
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 -
>
```

VPN集中器在快速配置方面出现，并且这些项目配置。

- 时间/日期
- 接口/掩码在**Configuration > Interfaces** (public=10.0.0.1/24， private=172.16.124.1/24)
- 在**Configuration > System > IP Routing > Default_Gateway** (10.0.0.2)的默认网关

这时， VPN集中器通过从网络内部的HTML是可取得。

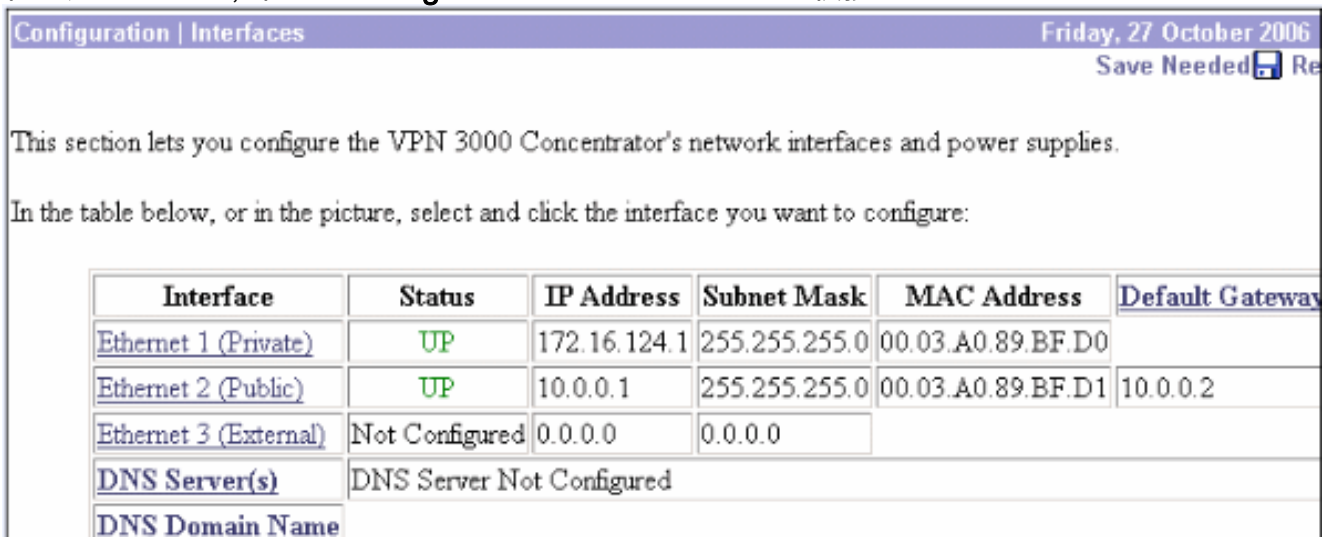
注意： 如果VPN集中器从外面被管理，您也执行这些步骤：

1. 选择**Configuration> 1接口> 2公共> 4精选的IP过滤器> 1.私有(默认)**。
2. 选择**Administration > 7访问权利> 2访问控制列表> 1添加管理器工作站**为了添加外部管理器的IP地址。

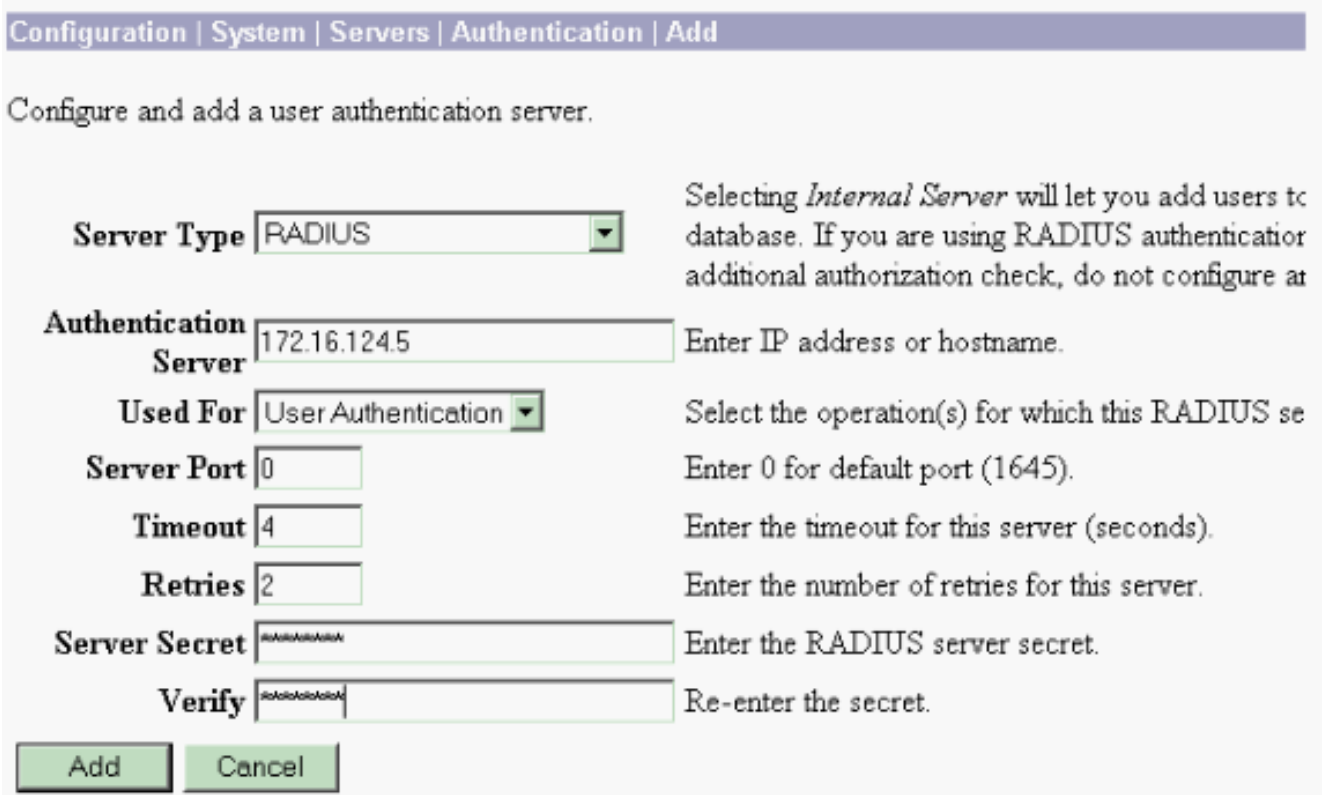
如果管理VPN集中器从外面，这些步骤只要求。

一旦完成这两个步骤，配置的其余可以通过GUI通过使用Web浏览器和连接完成对您配置接口的IP。在本例中和这时， VPN集中器通过从网络内部的HTML是可取得：

1. 在您启动GUI后，请选择**Configuration > Interfaces**为了复校接口。

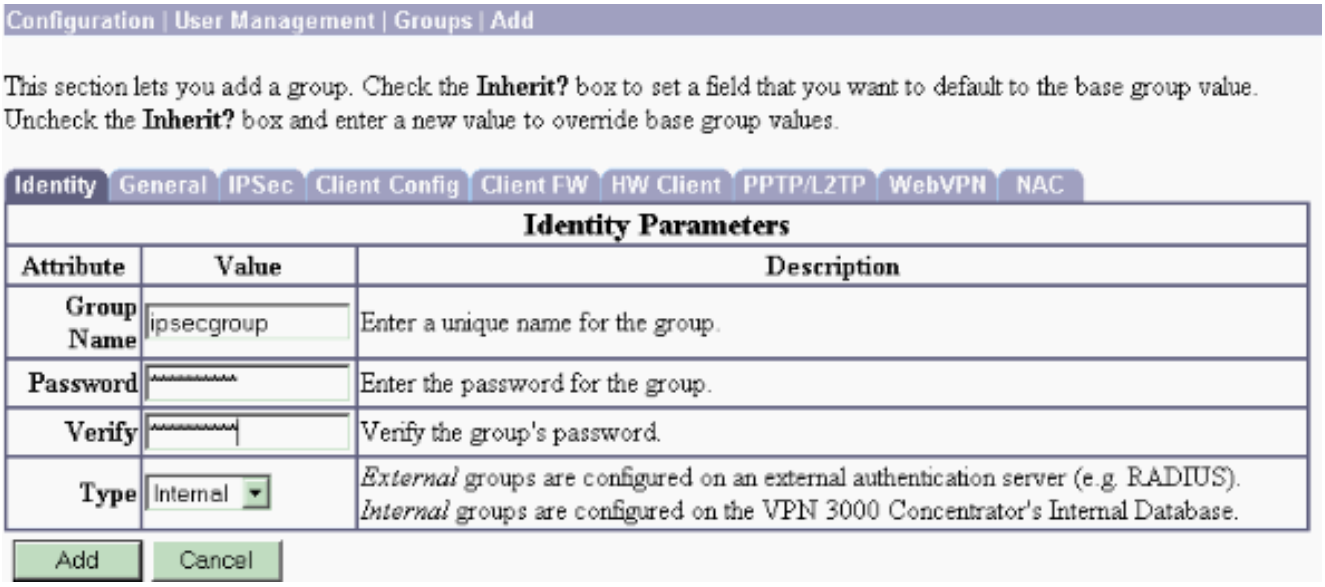


2. 完成这些步骤为了添加Cisco Secure ACS for Windows RADIUS服务器到VPN 3000集中器配置。选择**Configuration > System > Servers > Authentication**，并且单击从左菜单**添加**。



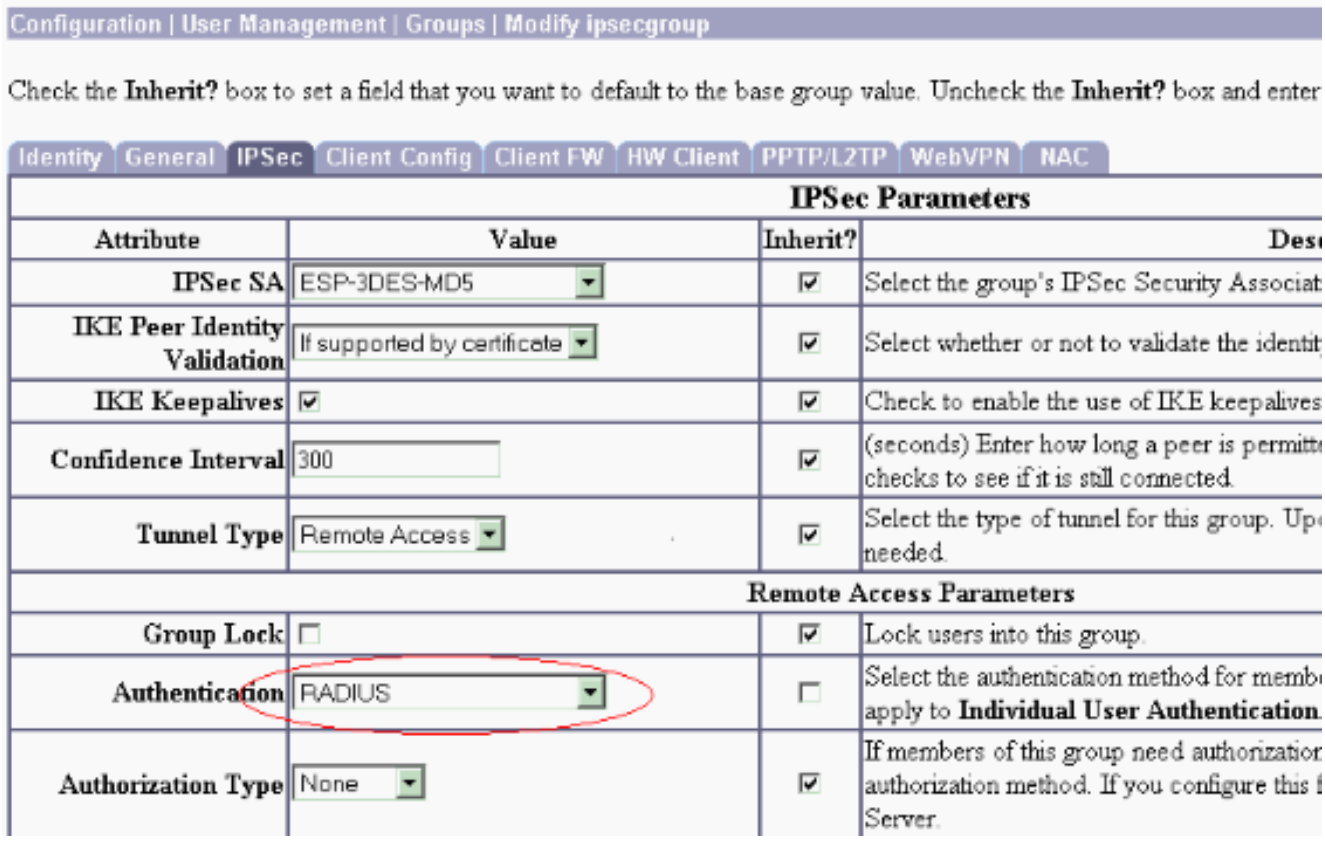
选择服务器类型RADIUS并且添加您的Cisco Secure ACS for Windows RADIUS服务器的这些参数。在他们的默认状态留下其他参数。**认证服务器**—输入您的Cisco Secure ACS for Windows RADIUS服务器的IP地址。**服务器秘密**—输入RADIUS服务器秘密。这必须是您使用的同样机密，当您在Cisco Secure ACS for Windows配置里时配置VPN 3000集中器。**验证**—重新输入验证的密码。这在VPN 3000集中器的全局配置里添加认证服务器。当认证服务器特别地定义时，所有组使用此服务器除了。如果认证服务器没有为组配置，恢复到全局认证服务器。

3. 完成这些步骤为了配置VPN 3000集中器的隧道组。从左菜单选择**Configuration > User Management > Groups**并且单击**添加**。更改或添加在Configuration选项的这些参数。请勿单击应用，直到您更改所有这些参数：**注意：** 这些参数是为远程访问虚拟专用网连接需要的最低。这些参数也假设默认设置在VPN 3000集中器的基本组中未更改。**标识**



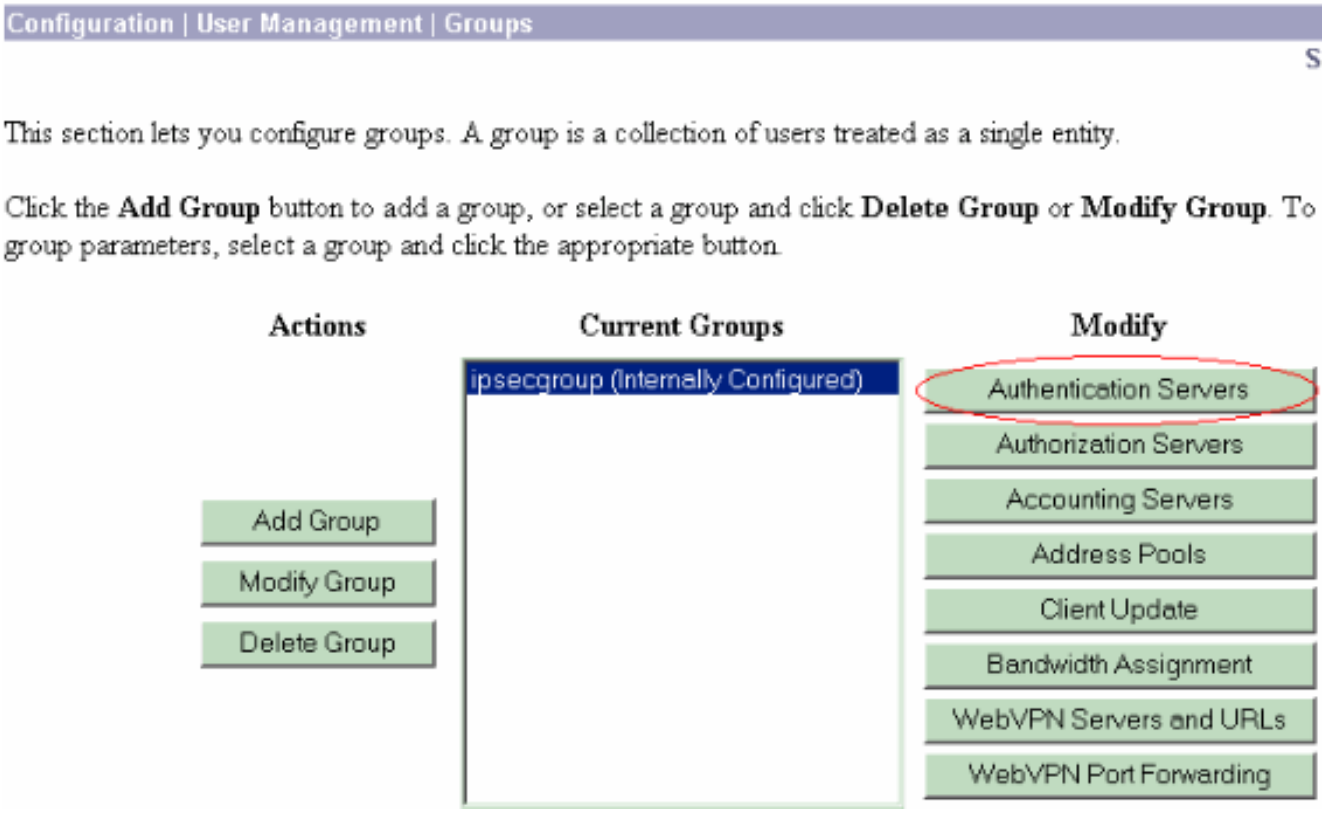
组名—键入组名。例如， Ipsecuser。**密码**—输入组的一个密码。这是IKE会话的预先共享密钥。**验证**—重新输入验证的密码。**类型**—留下此作为默认：内部。

IPsec



隧道类型—选择**远程访问**。**验证**— RADIUS.这告诉VPN集中器使用的什么方法验证用户。**模式配置**—检查**模式配置**。单击 **Apply**。

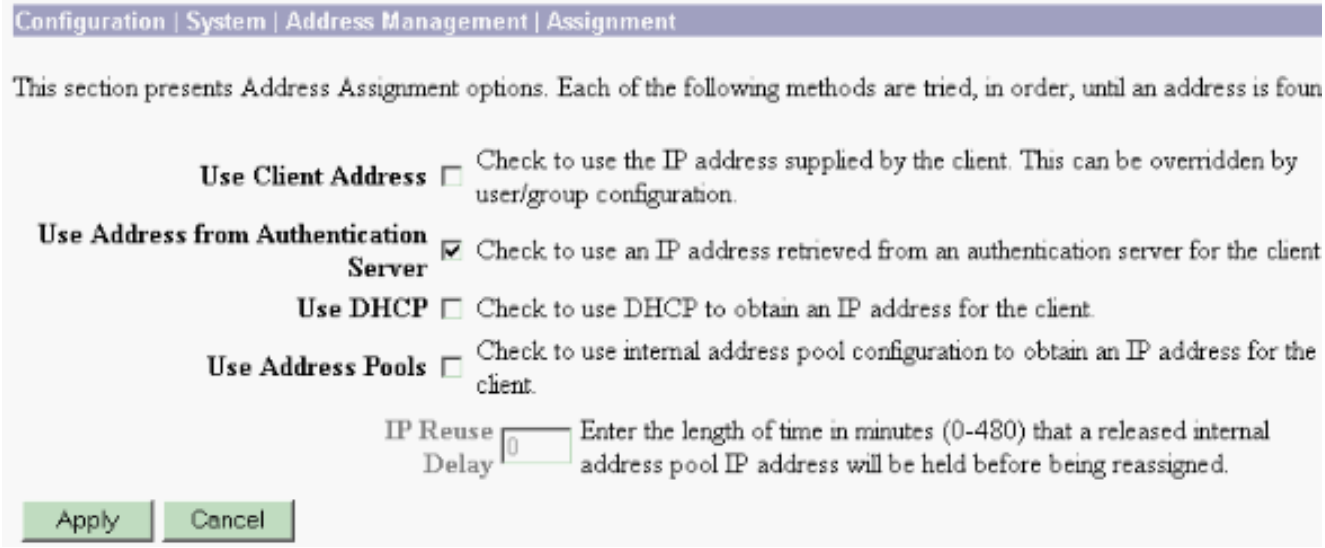
4. 完成这些步骤为了配置在VPN 3000集中器的多次认证服务器。一旦组定义，请选定该组，并且单击**认证服务器**在修改名下。各自的认证服务器可以为每组定义，即使这些服务器在全局服务器不存在。



选择服务器类型RADIUS，并且添加您的Cisco Secure ACS for Windows RADIUS服务器的这些参数。在他们的默认状态留下其他参数。**认证服务器**—输入您的Cisco Secure ACS for Windows RADIUS服务器的IP地址。**服务器秘密**—输入RADIUS服务器秘密。这必须是您使用的同样机密，当您在Cisco Secure ACS for Windows配置里时配置VPN 3000集中器。**验证**

—重新输入验证的密码。

5. 一旦客户端得到验证，请选择**Configuration > System > Address Management > Assignment**并且检查**从认证服务器的使用地址**为了分配IP地址到从在RADIUS服务器创建的IP池的VPN客户端。

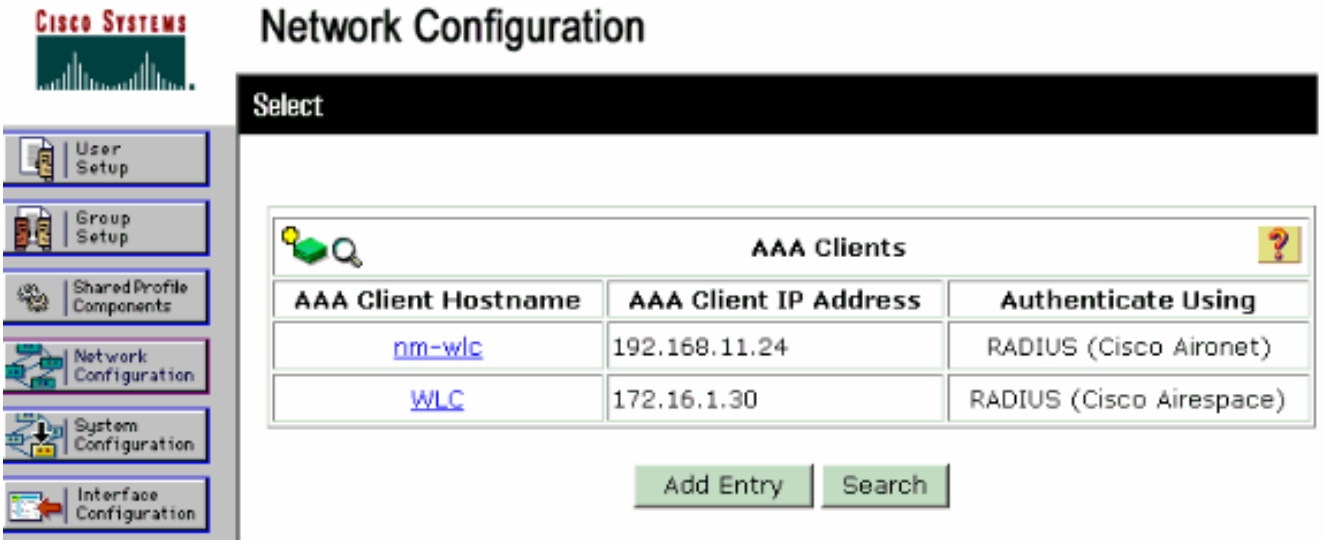


RADIUS 服务器配置

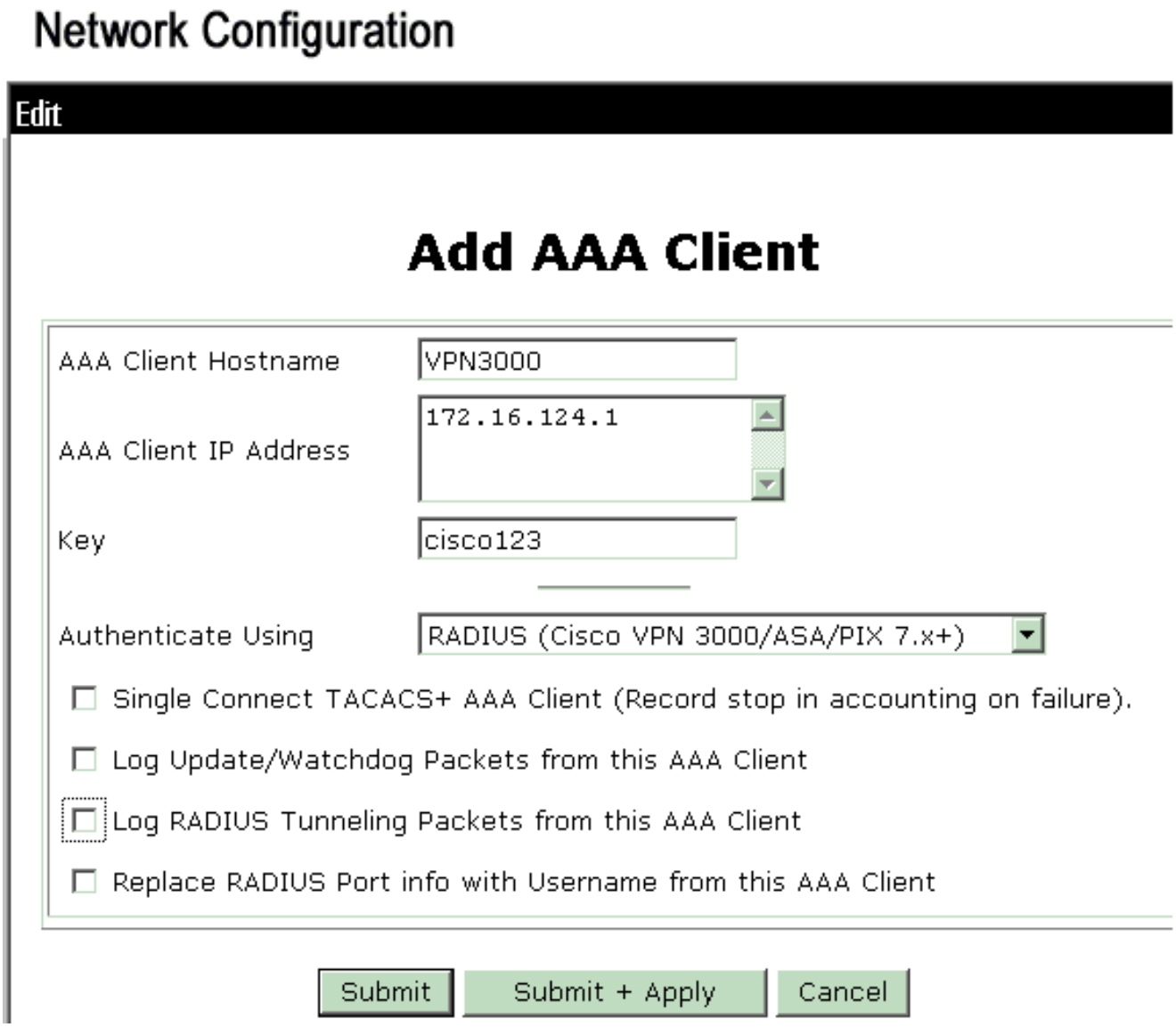
本文的此部分描述要求的步骤配置Cisco Secure ACS作为Cisco VPN 3000系列集中器转发的VPN客户端用户认证的一个RADIUS服务器- AAA客户端。

双击**ACS Admin图标**为了启动运行Cisco Secure ACS for Windows RADIUS服务器的PC的admin会话。用适当的用户名和密码登陆，如果必须。

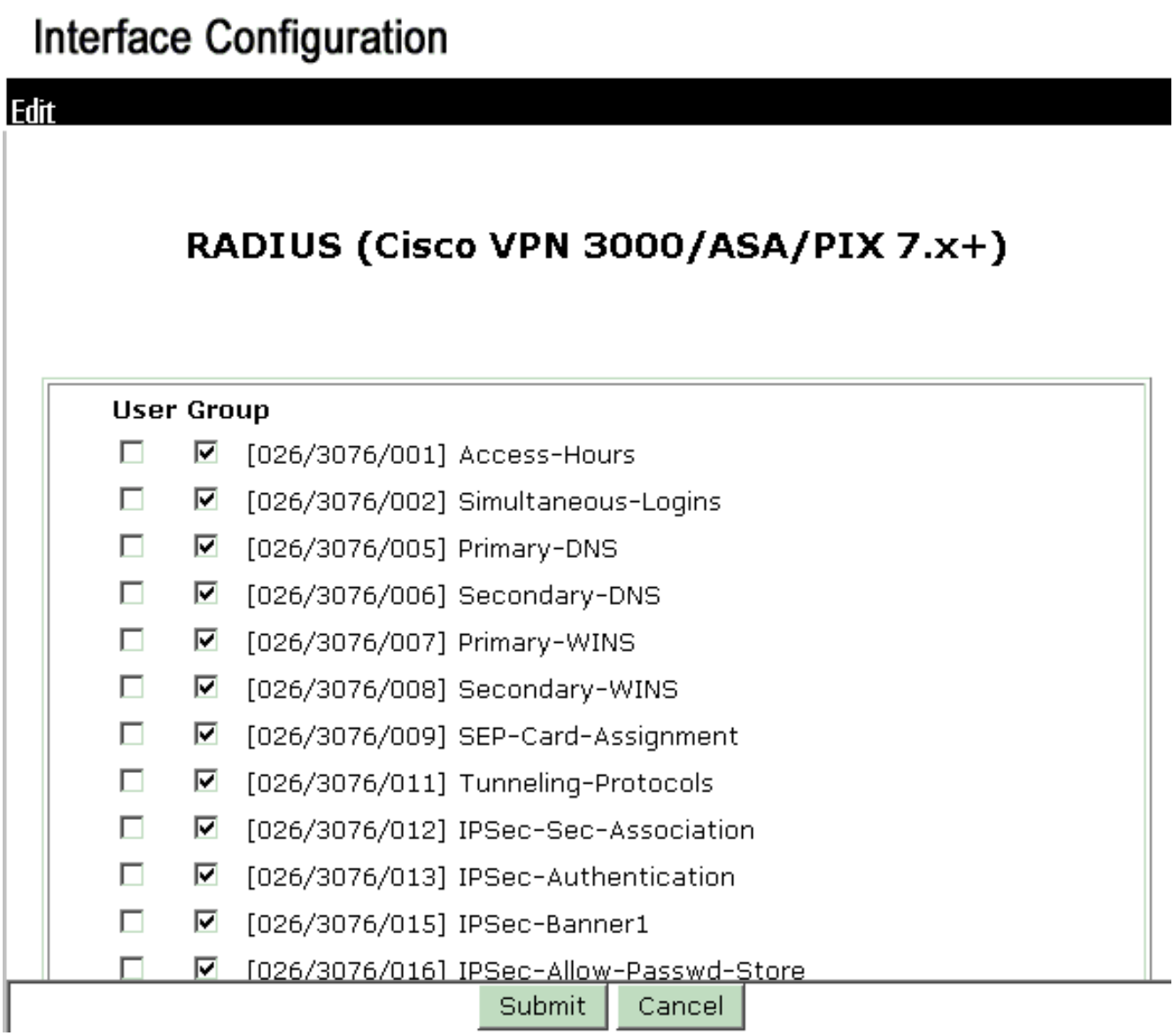
1. 完成这些步骤为了添加VPN 3000集中器到Cisco Secure ACS for Windows服务器配置。选择**网络配置**并且单击**Add条目**为了添加AAA客户端到RADIUS服务器。



添加您的VPN 3000集中器的这些参数：

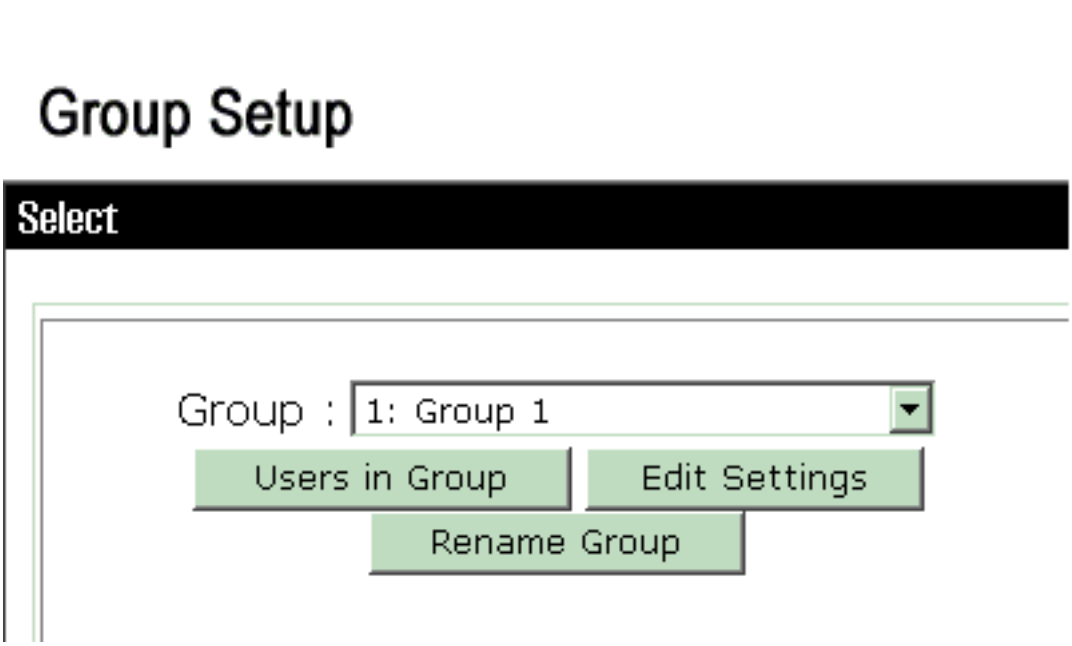


AAA客户端主机名-进入您的VPN 3000集中器主机名(DNS解析)。**AAA客户端IP地址**—输入您的VPN 3000集中器的IP地址。**密钥**—输入RADIUS服务器秘密。这必须是您配置的同样机密，当您添加了在VPN集中器的认证服务器。**验证使用**—选择**RADIUS (思科VPN 3000/ASA/PIX 7.x+)**。这在组配置窗口允许VPN3000 VSAs显示。单击 **submit**。选择**接口配置**，点击**RADIUS (思科VPN 3000/ASA/PIX 7.x+)**，并且检查**根据厂商的组[26]**。

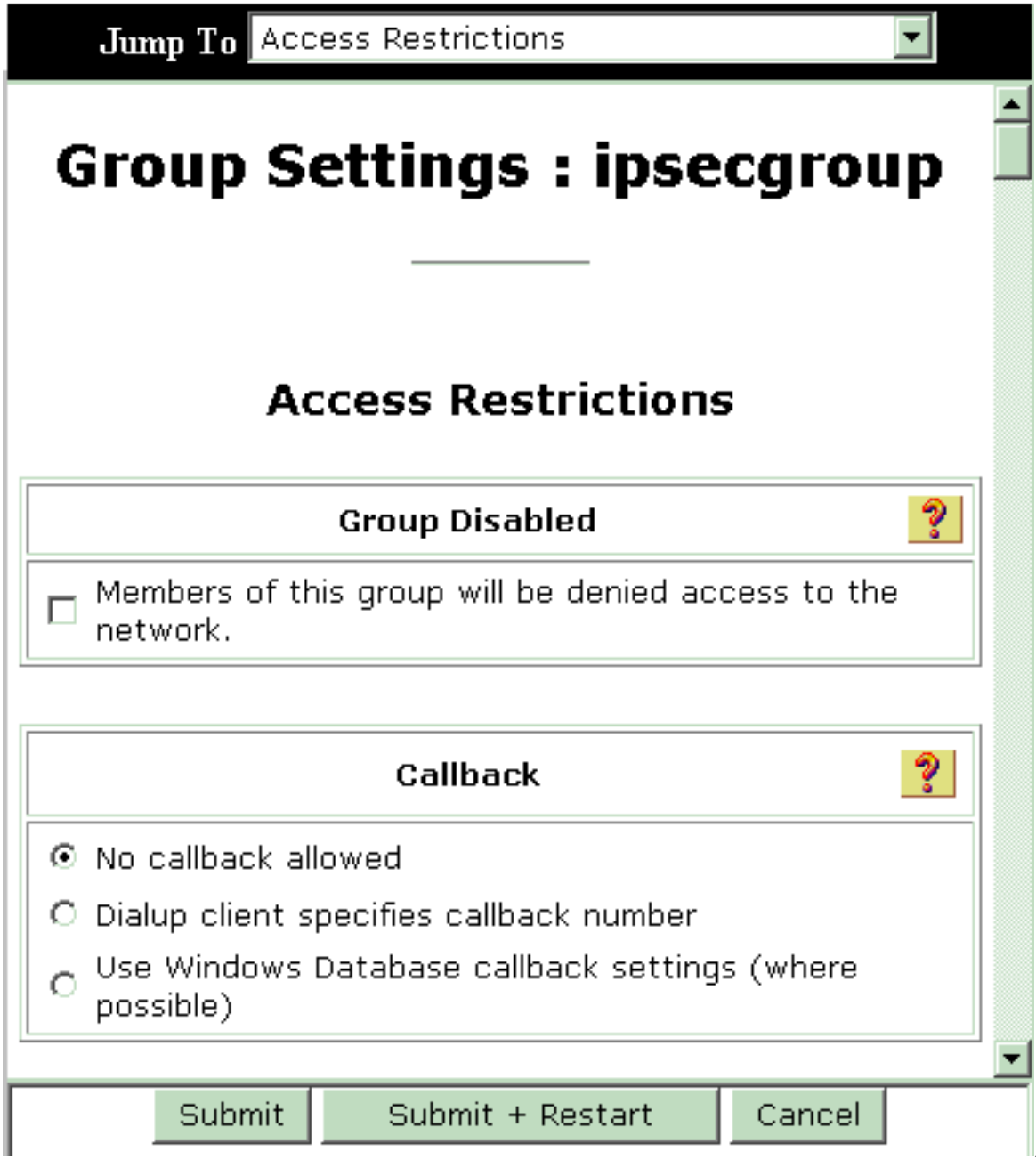


注意： 'RADIUS属性26'是指所有卖方细节属性。例如，请选择**接口配置> RADIUS (Cisco VPN 3000)**并且请参阅所有可用的属性从026开始。这显示所有这些卖方细节属性属于IETF RADIUS 26标准。默认情况下这些属性在用户或组建立没出现。为了出现在组建立，请创建在网络配置里验证与RADIUS的AAA客户端(在这种情况下VPN 3000集中器)。然后请检查在用户设置，组建立或者两个需要出现从接口配置的属性。参考RADIUS属性关于可用的属性和他们的使用情况的更多信息。单击 **submit**。

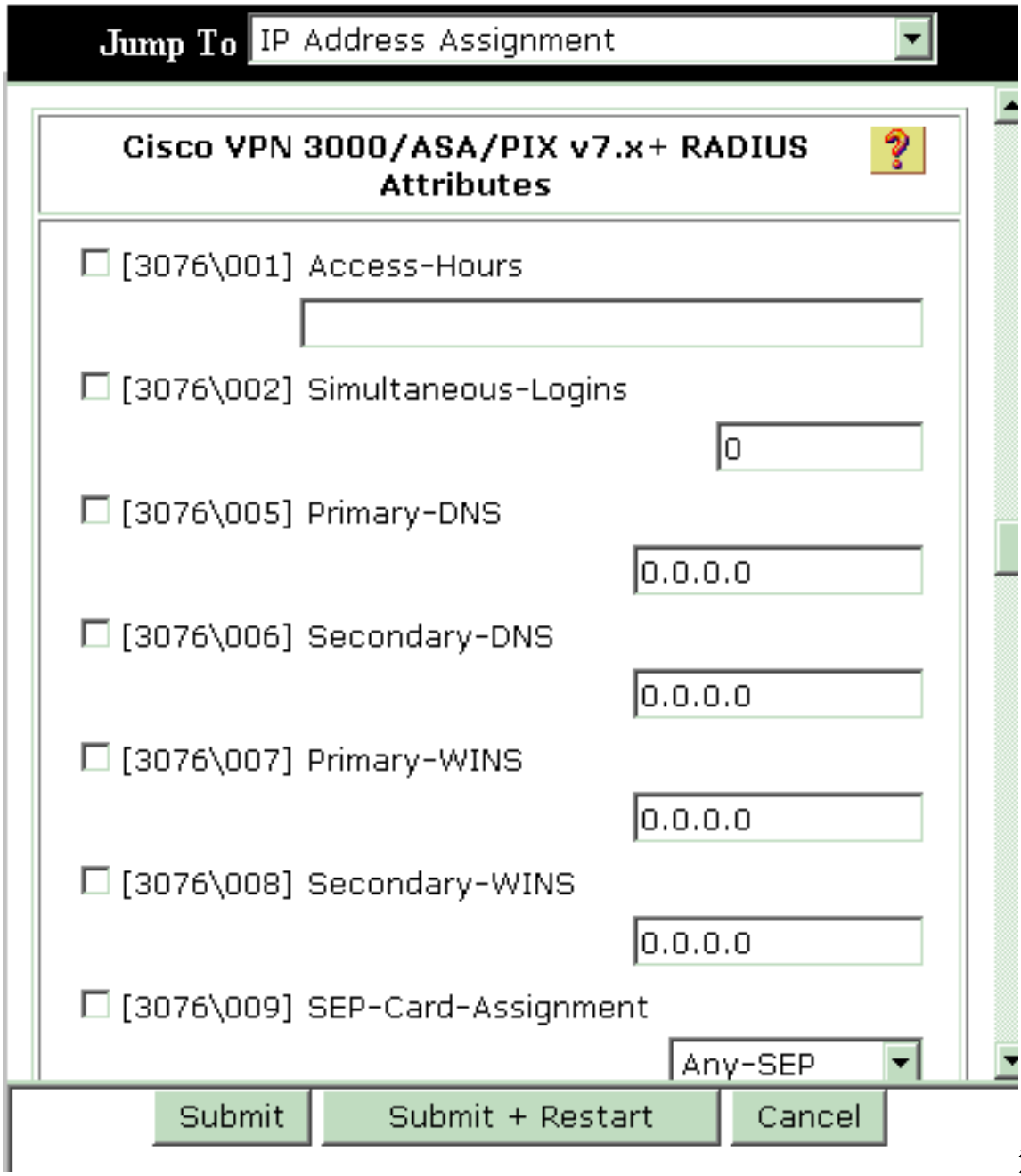
2. 完成这些步骤为了添加组到Cisco Secure ACS for Windows配置。选择**组建立**，然后选择其中一模板组，例如， Group1，并且点击**重命名组**。



更改名称对事适当为您的组织。，例如， ipsecgroup。因为用户被添加到这些组，请做组名反射该组实际的目的。如果所有用户被放到同一组，您能告诉它VPN用户组。单击**编辑设置**为了编辑参数在您的最近重命名的组中。

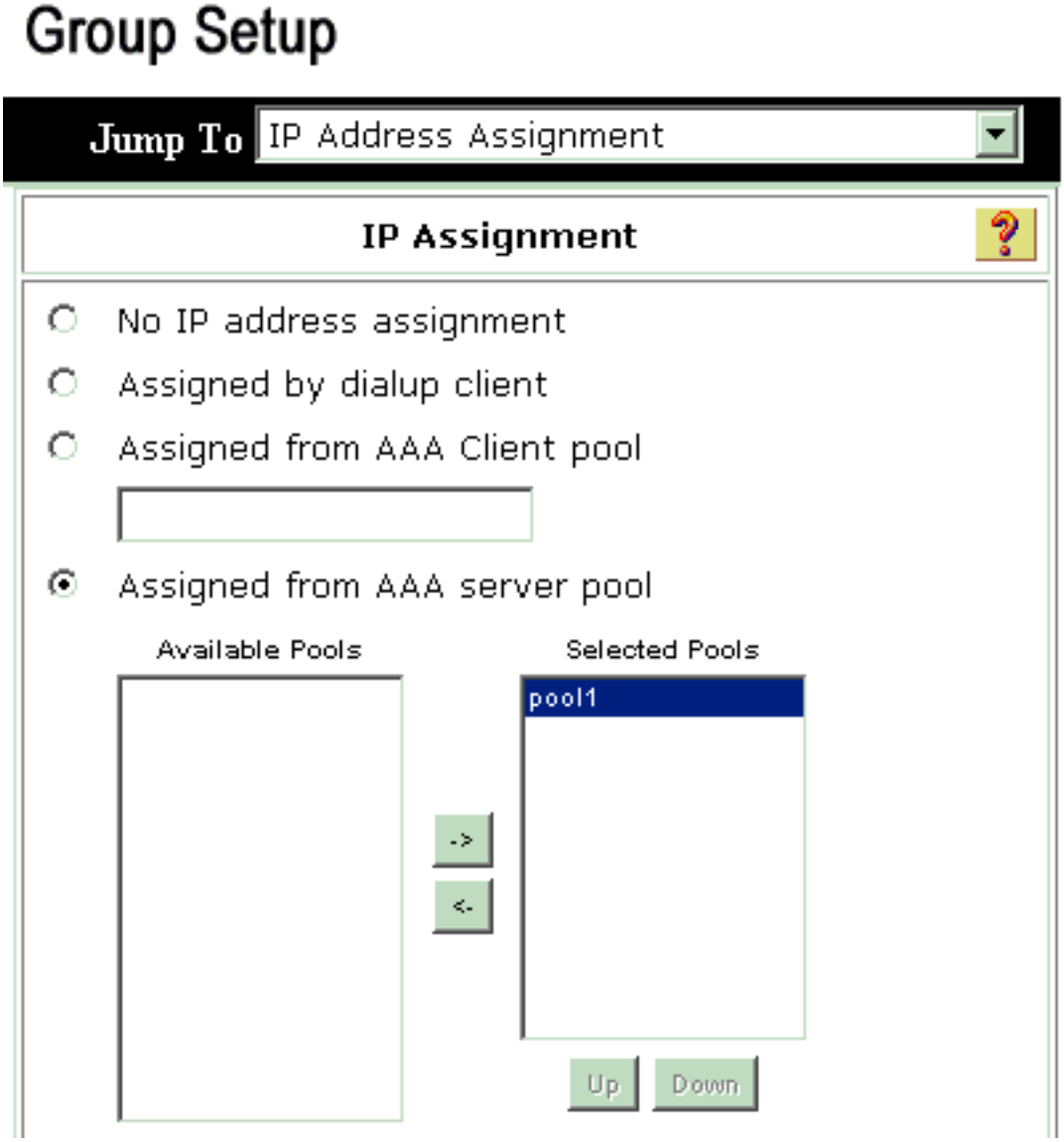


点击**Cisco VPN 3000 RADIUS**并且配置这些推荐的属性。这允许用户分配到此组继承Cisco VPN 3000 RADIUS属性，允许您集中所有用户的策略Cisco Secure ACS for Windows的。

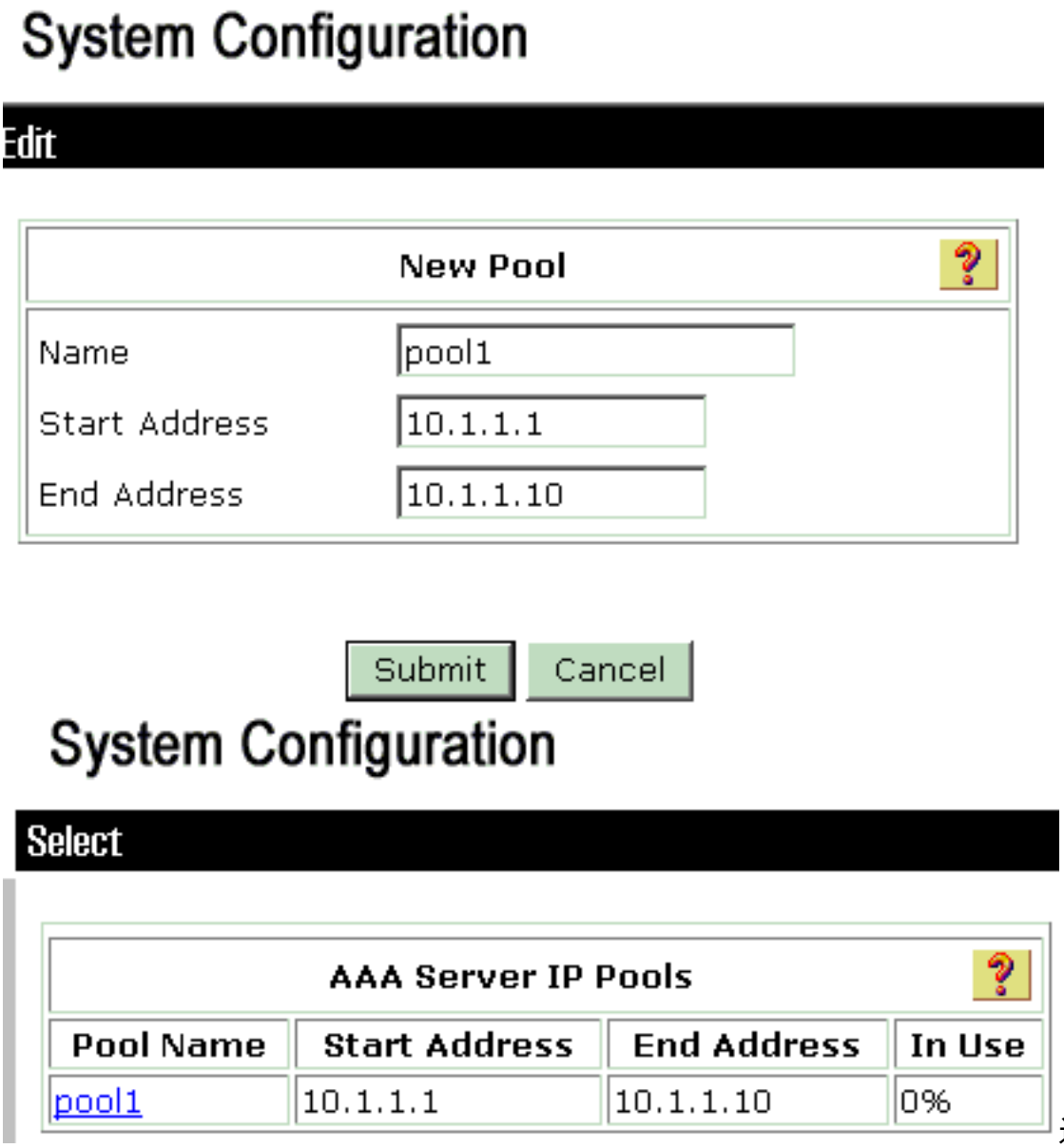


注意： 技术上， VPN3000 RADIUS属性没有要求配置，只要隧道组在VPN 3000系列集中器配置的步骤3组成，并且VPN集中器的基本组不从原始默认设置更改。**推荐的VPN3000属性：主要的DNS**—输入您的主DNS服务器的IP地址。**辅助DNS** —输入您的辅助DNS服务器的IP地址。**主WINS**—输入您的主WINS服务器的IP地址。**第二WINS** —输入您的第二WINS服务器的IP地址。**隧道协议**—选择**IPsec**。这允许仅IPSec客户端连接。PPTP或L2TP没有允许。**IPsec SEC关联**—回车**ESP-3DES-MD5**。这保证所有您的IPSec客户端连接最高的加密联机。**IPsec允许密码存储**—选择**禁止，**因此用户没有允许保存他们的在VPN客户端的密码。**标语**—输入将被提交的欢迎消息横幅对用户在连接。例如， “请欢迎到MyCompany雇员VPN访问!”**IPsec默认域**—输入您的公司域名。例如， “mycompany.com”。此套属性不是必要的。但是，如果是不确定的，如果VPN 3000集中器的基本组属性更改，然后思科建议您配置这些属性：**同时登录**—输入您允许用户同时登陆与相同用户名的次数。建议是1或2。**SEP卡德分配**—选择**任何SEP**。**IPsec模式设置**—选择。**UDP的IPSec** —使用在UDP协议的IPsec，除非在此组中希望用户连接选择**OFF**。如果选择， VPN客户端仍然有能力本地禁用UDP的IPSec和通常连接。**UDP的IPSec端口选择**每在4001至49151范围内的UDP端口号。这，只有当UDP的IPSec打开，使用。在您能使用他们前，属性下一组要求您集某事首先在VPN集中器。这为高级用户只推荐。**访问时段**

—这要求您设置范围在VPN 3000集中器的访问时间在**Configuration > Policy Management**下。反而，请使用访问时间可用在Cisco Secure ACS for Windows管理此属性。**IPsec已分解通道列表**—这要求您设置在VPN集中器的一张网络列表在**Configuration > Policy Management > Traffic Management**下。这是网络列表发送下来对告诉客户端加密数据到在列表的仅那些网络的客户端。选择**在组建立的IP分配**，并且**从AAA服务器池分配的**检查为了分配IP地址到VPN客户端用户，一旦他们是得到验证。

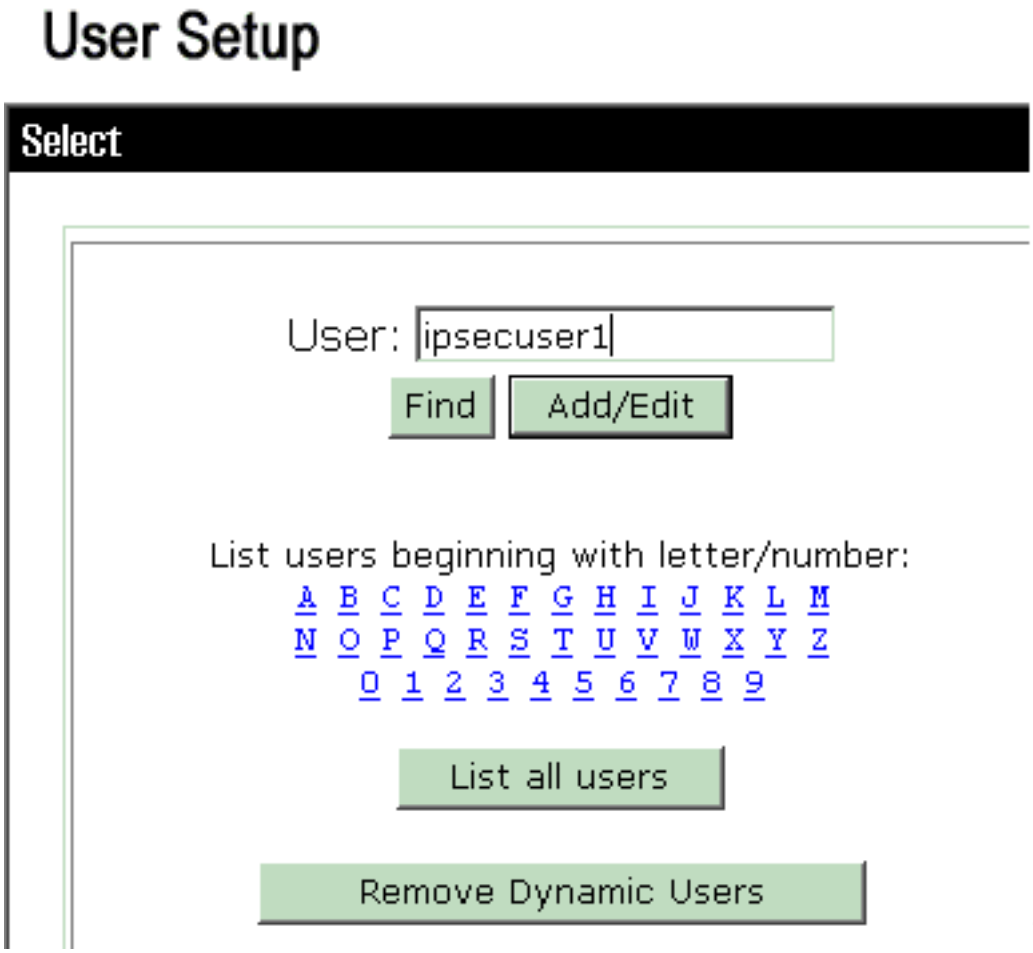


选择**系统配置 > IP池**为了创建VPN客户端用户的一个IP池并且单击**提交**。

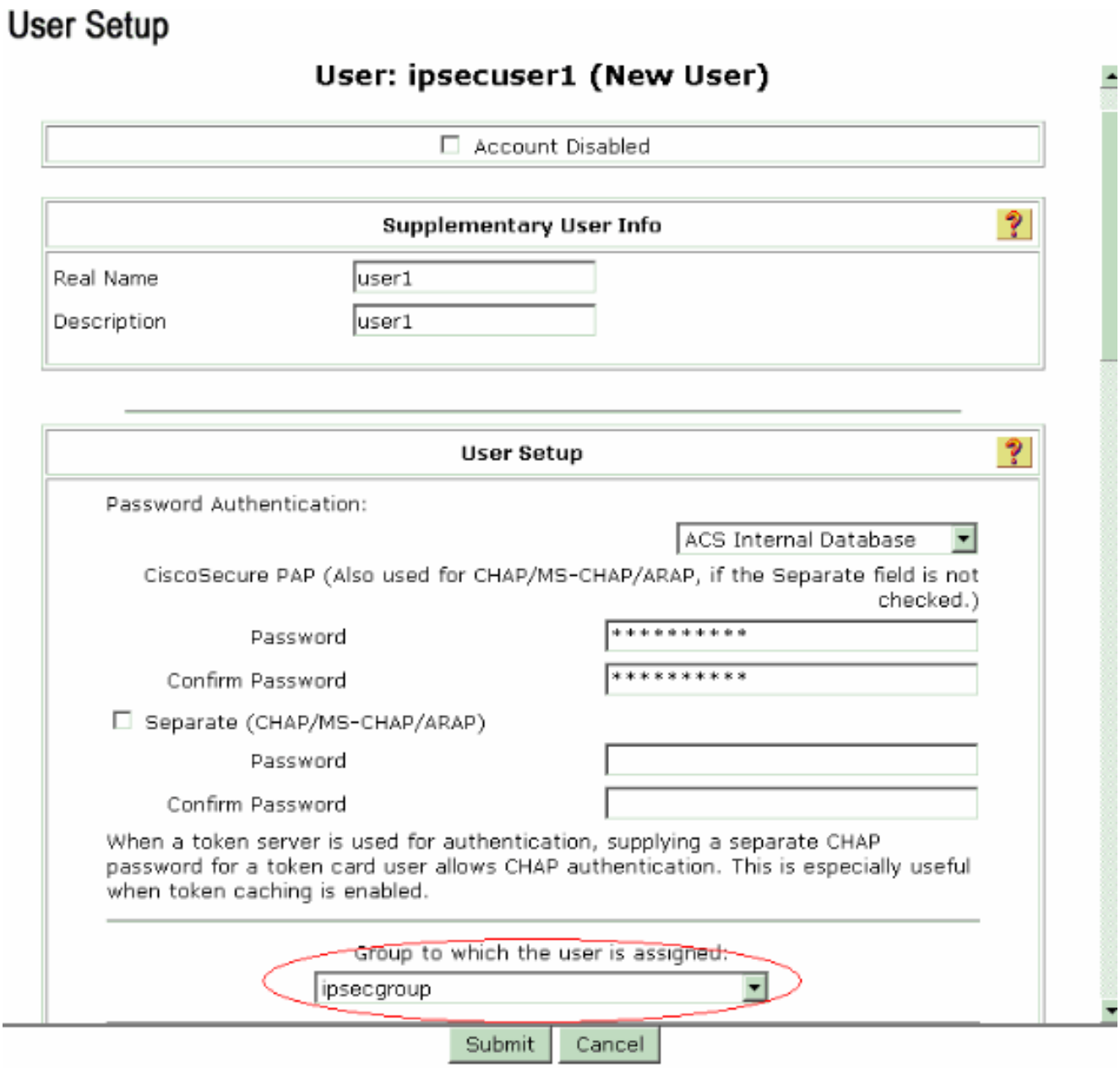


选择**提交>重新启动**为了保存配置和激活新的组。重复这些步骤为了添加更多组。

3. **配置Cisco Secure ACS for Windows的用户。**选择**用户设置**，输入用户名，并且单击**添加/编**



辑。配置这些参数在User Setup部分下：

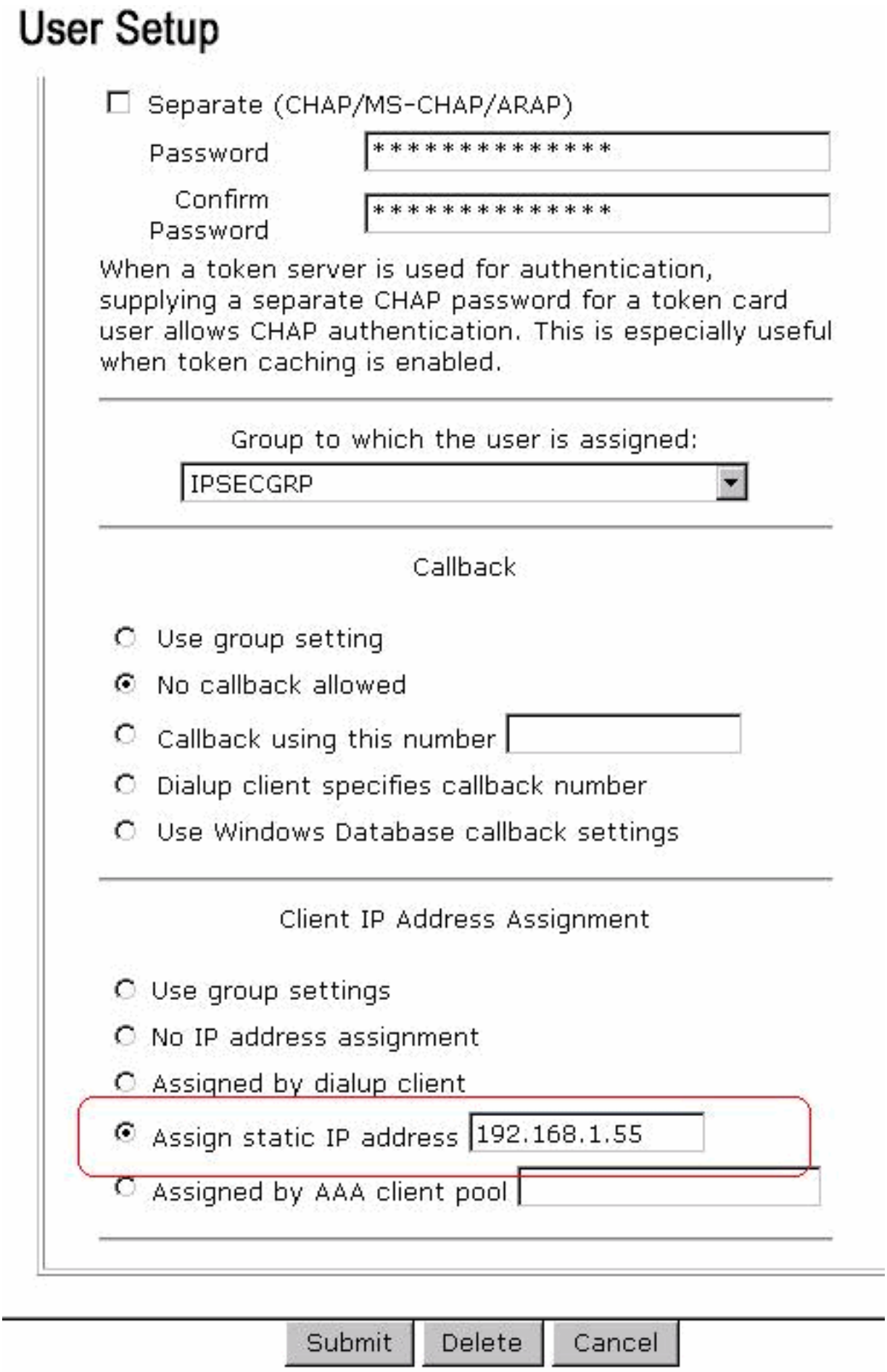


密码验证—选择**ACS内部数据库**。**Cisco Secure PAP口令**—输入用户的一个密码。**Cisco Secure PAP -确认密码**—重新输入新用户的密码。**用户分配**—的**组请**选择您在上一步创建组的名称。单击**提交**为了保存和激活用户设置。重复这些步骤为了添加另外的用户。

分配静态IP地址到VPN客户端用户

完成这些步骤：

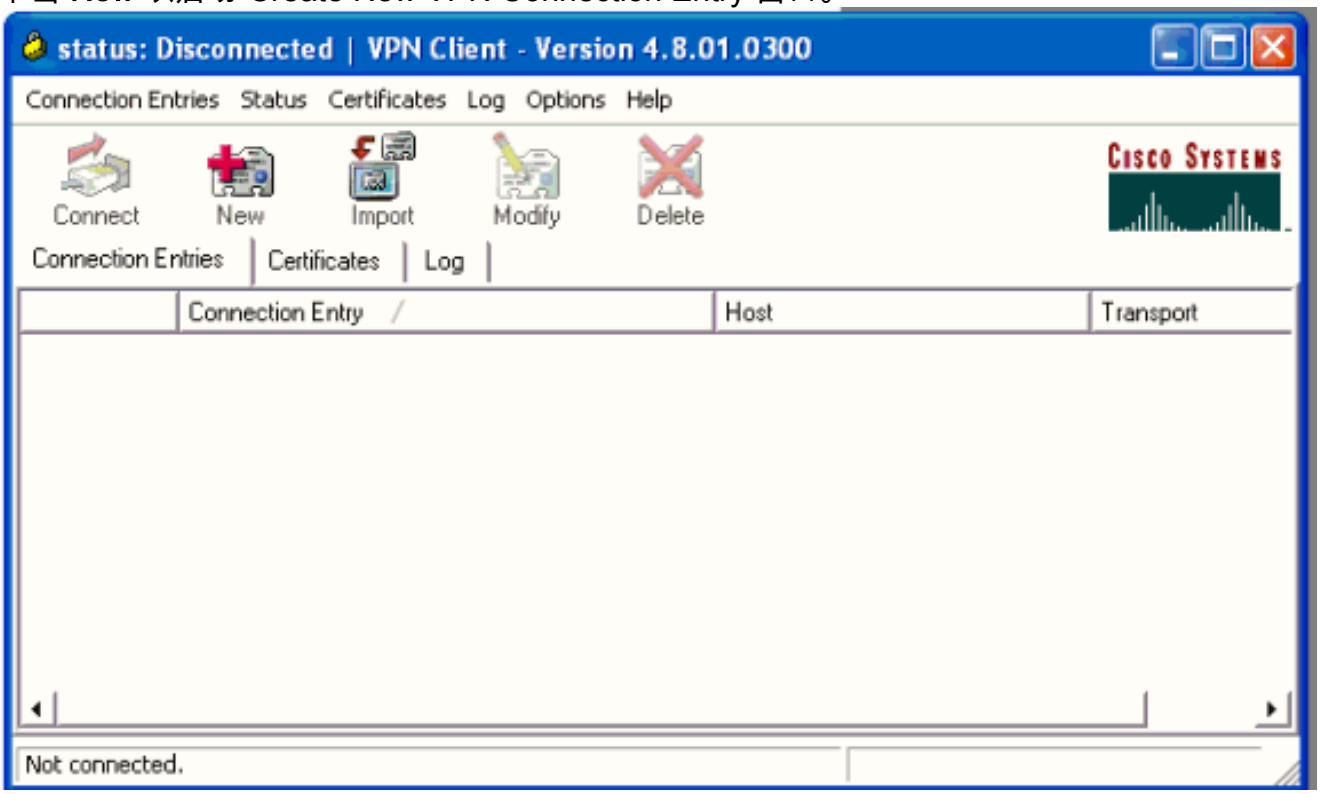
1. 创建一个新的VPN组IPSECGRP。
2. 创建要接收静态IP和选择**IPSECGRP的**用户。选择**分配**与分配在客户端IP地址分配下的静态IP地址的**静态IP地址**。


User Setup
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
IPSECGRP
Callback
Use group setting
No callback allowed
Callback using this number
Dialup client specifies callback number
Use Windows Database callback settings
Client IP Address Assignment
Use group settings
No IP address assignment
Assigned by dialup client
Assign static IP address 192.168.1.55
Assigned by AAA client pool
Submit
Delete
Cancel

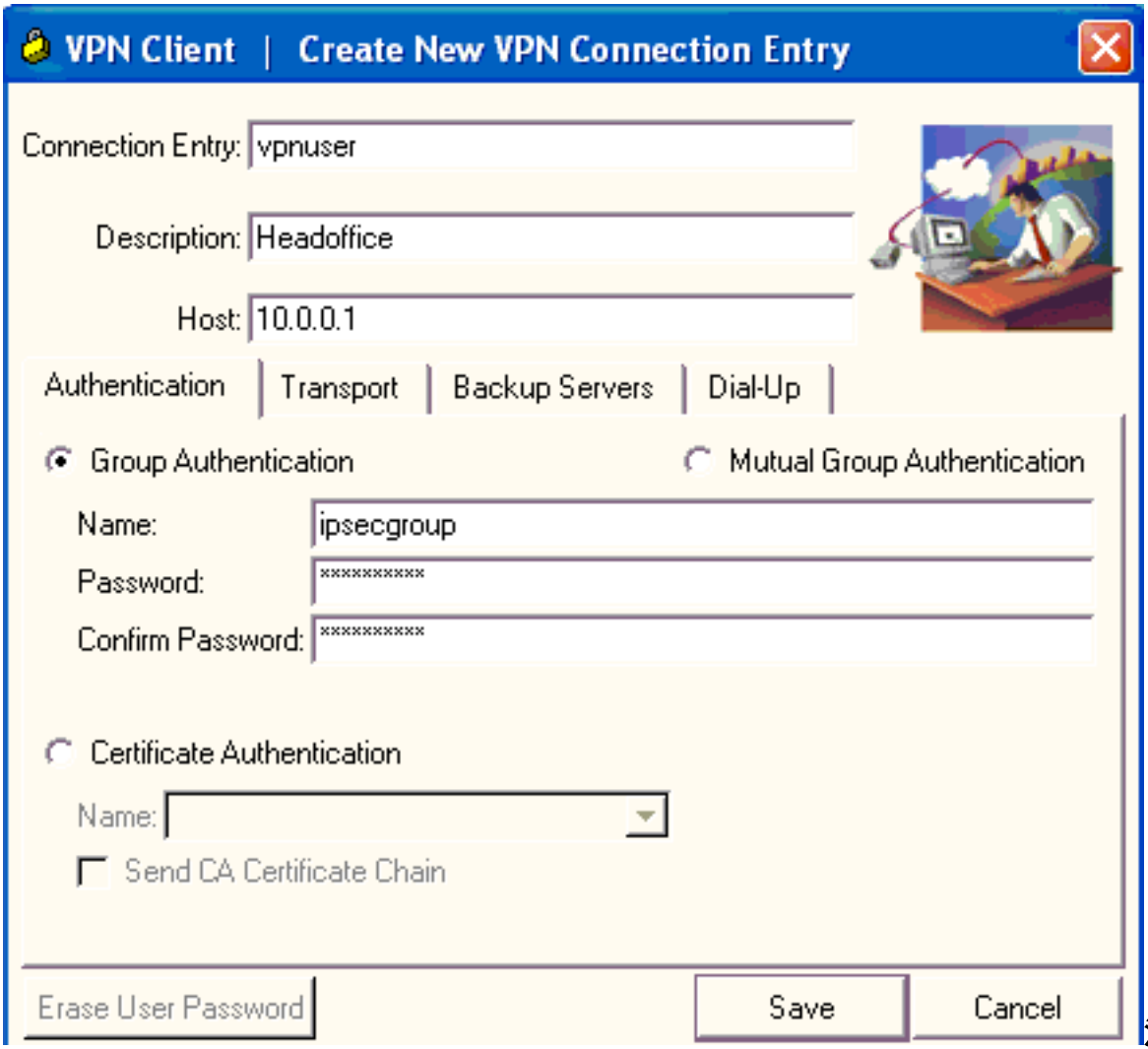
[VPN客户端配置]

此部分描述VPN客户端配置。

1. 选择**开始 > 程序 > Cisco Systems VPN 客户端 > VPN 客户端**。
2. 单击 **New** 以启动 Create New VPN Connection Entry 窗口。



3. 出现提示时，为条目指定一个名称。如果需要，也可以输入说明。指定在主机列的VPN 3000集中器公共接口IP地址并且选择**组验证**。然后请提供组名和密码。点击**"Save"**为了完成新的VPN连接项。

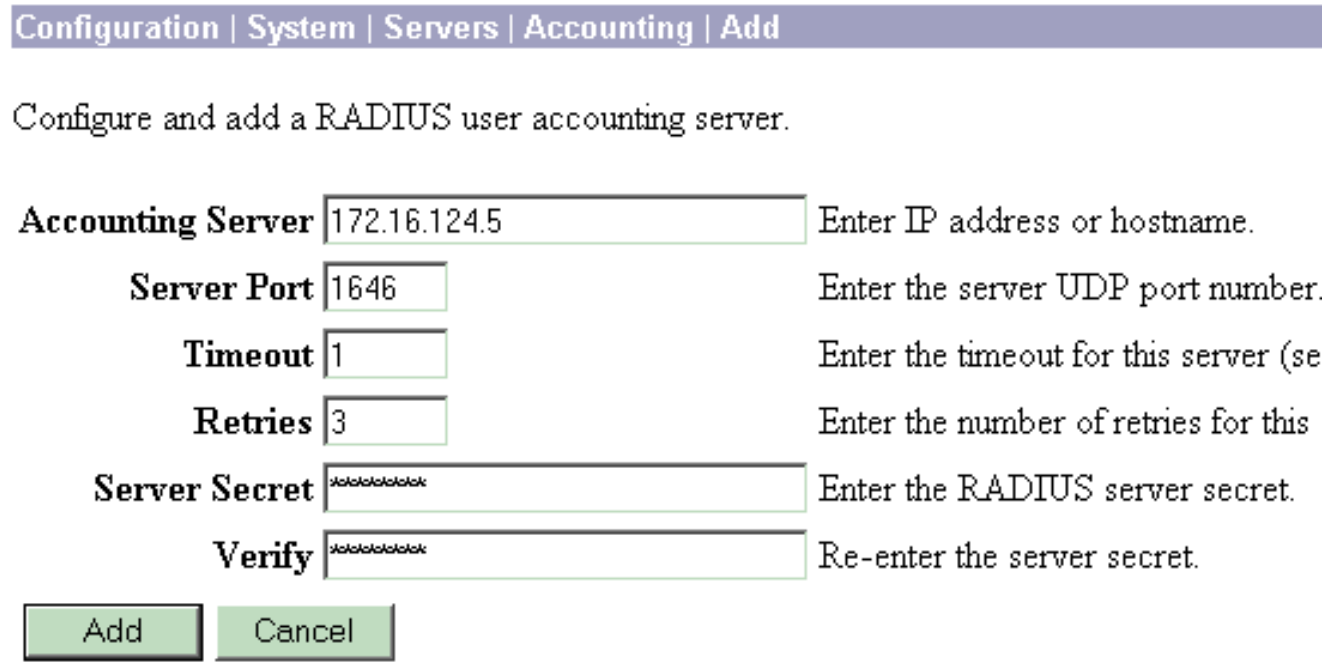


注意： 请务必VPN客户端在Cisco VPN 3000系列集中器配置使用配置的同一个组名和密码。

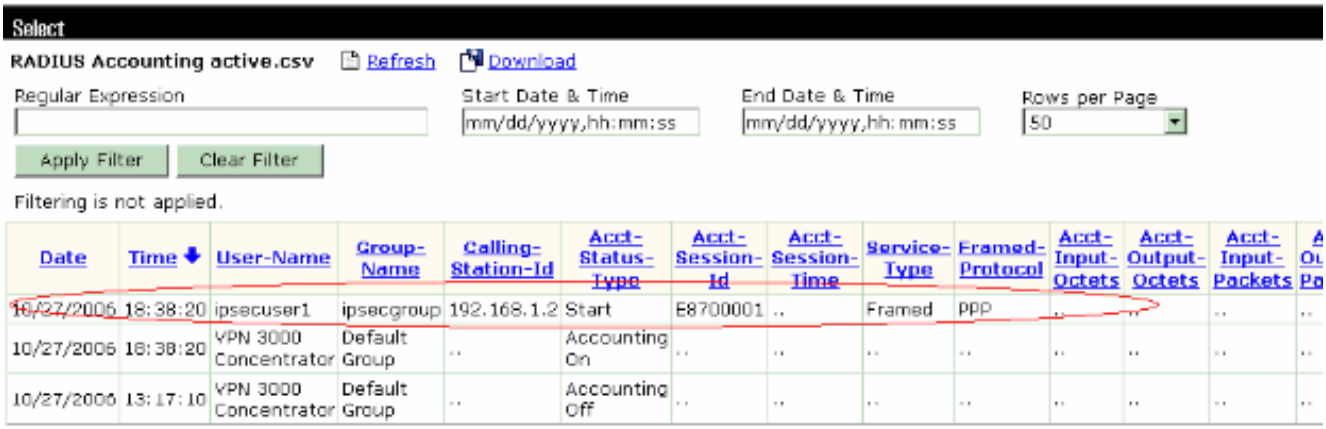
添加记帐

在验证工作后，您能添加核算。

1. 在VPN3000，请选择**Configuration > System > Servers > Accounting Servers**，并且添加**Cisco Secure ACS for Windows**服务器。
2. 当您选择**Configuration > User Management > Groups**，选定组并且点击**修改账户时，**您能添加各自的记帐服务器到每组。**服务器**。然后请输入记帐服务器的IP地址有服务器秘密的。



在Cisco Secure ACS for Windows，当此输出显示，计费记录出现：



验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

验证VPN集中器

在VPN 3000集中器侧，请选择**Administration > Administer Sessions**为了验证远程VPN信道建立。

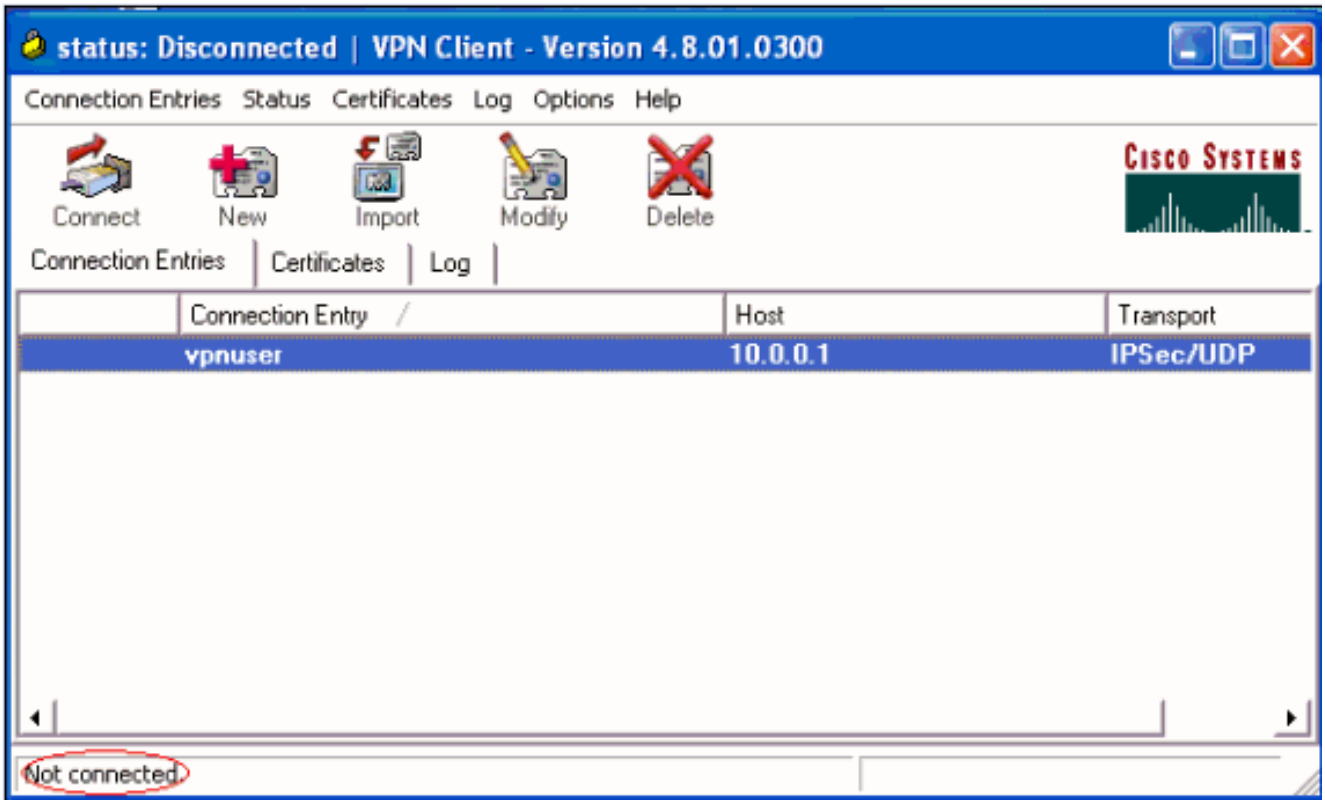
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

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]

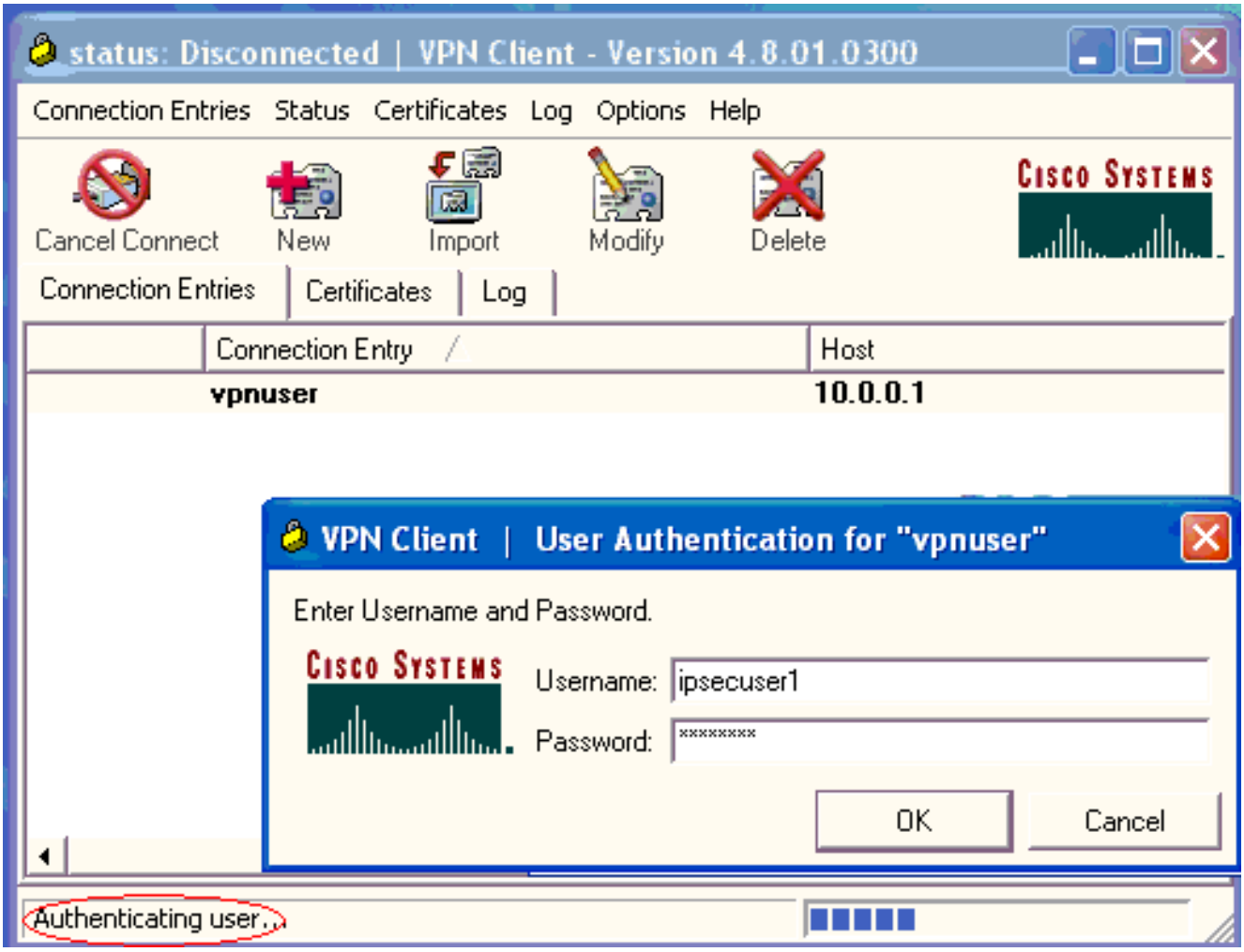
验证VPN客户端

完成以下步骤以验证 VPN 客户端。

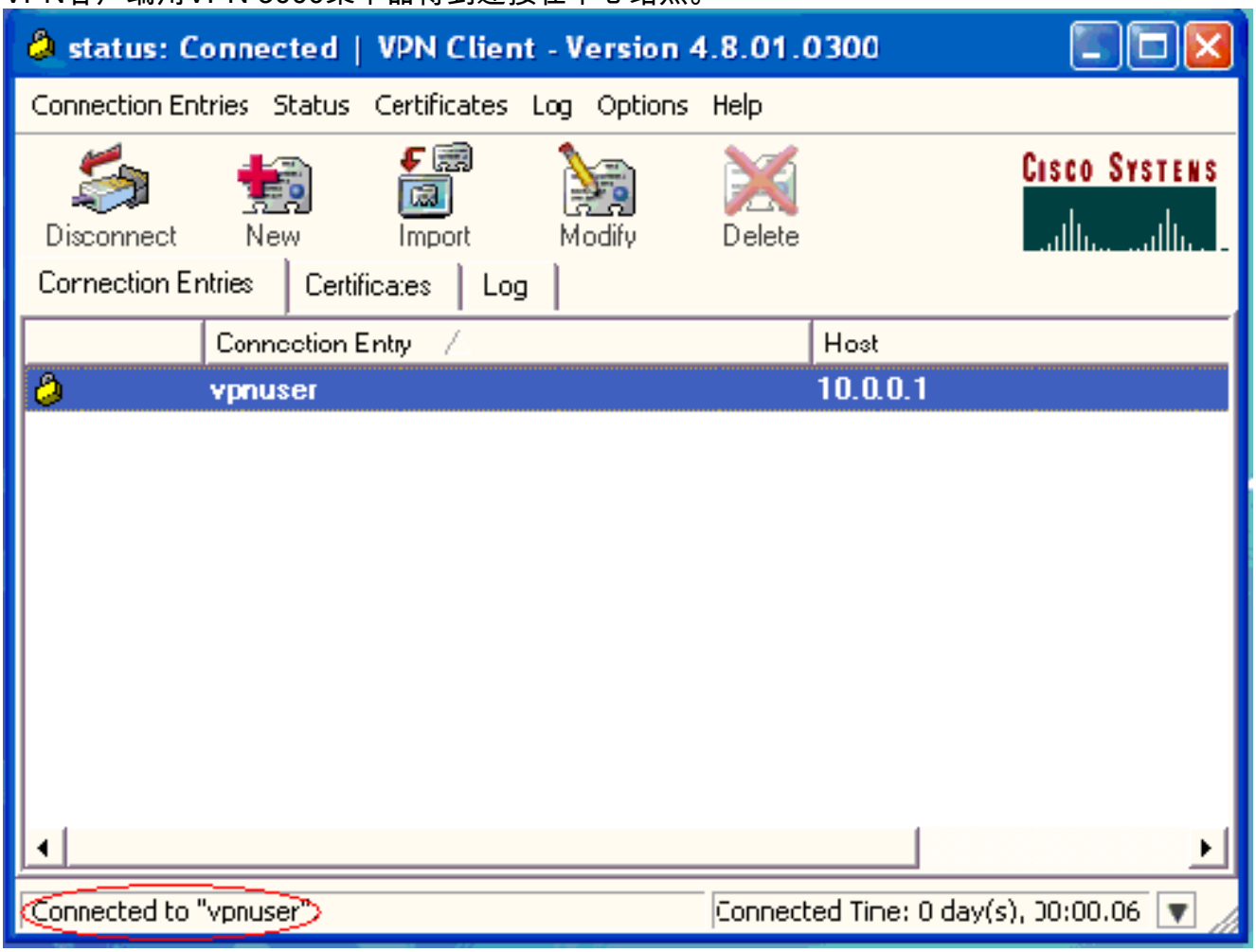
1. 点击**连接**为了首次VPN连接。



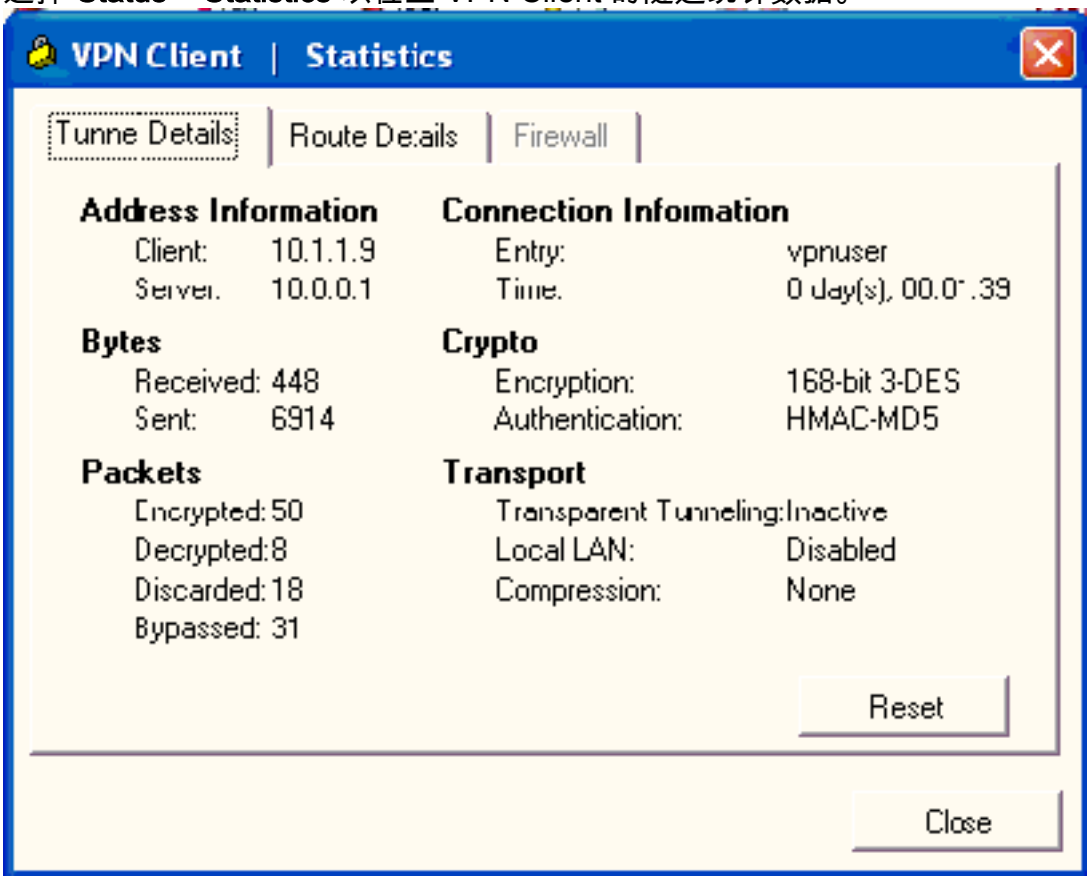
2. 此窗口为用户认证出现。输入有效用户名和密码为了建立VPN连接。



3. VPN客户端用VPN 3000集中器得到连接在中心站点。



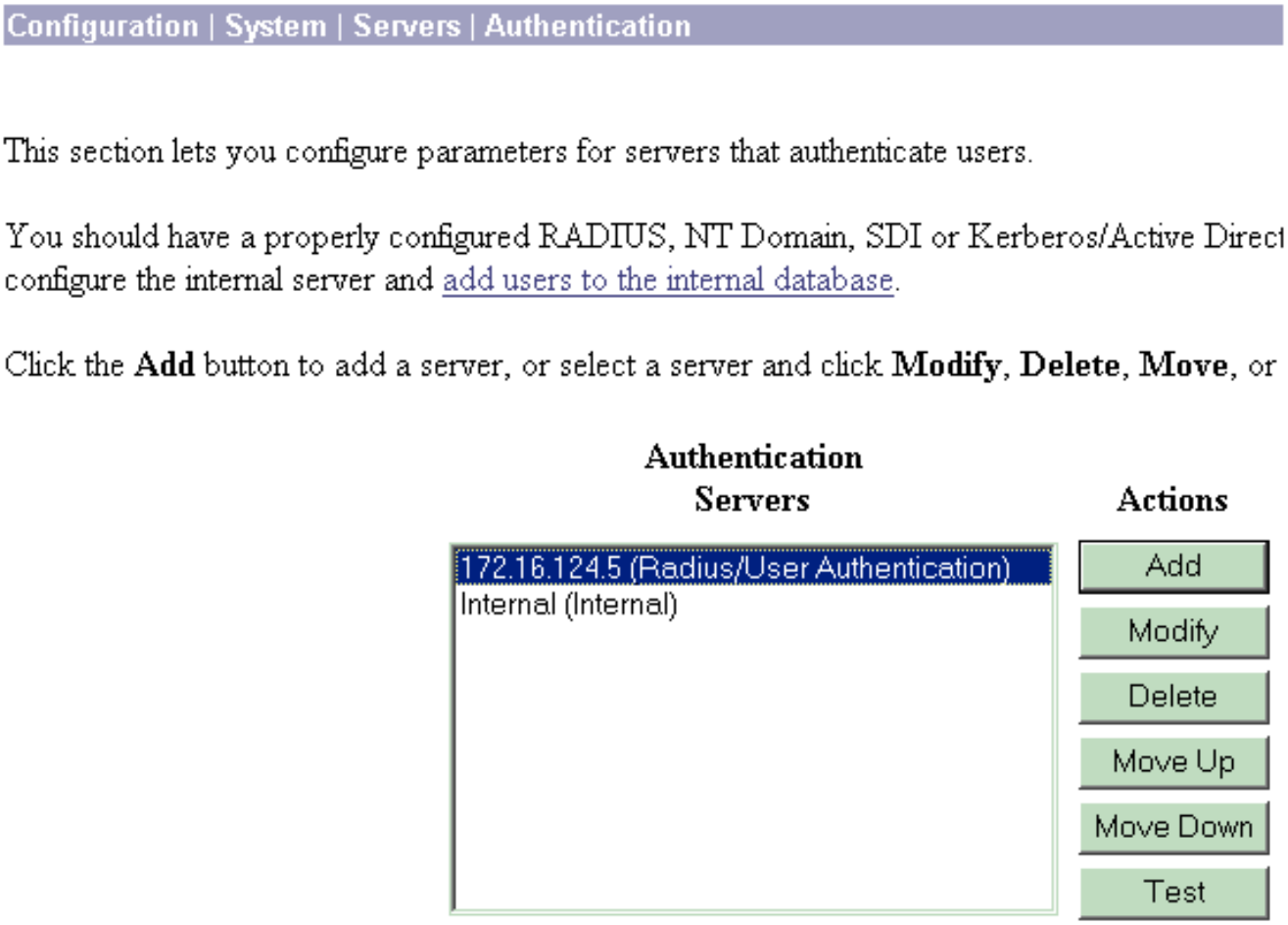
4. 选择 **Status > Statistics** 以检查 VPN Client 的隧道统计数据。



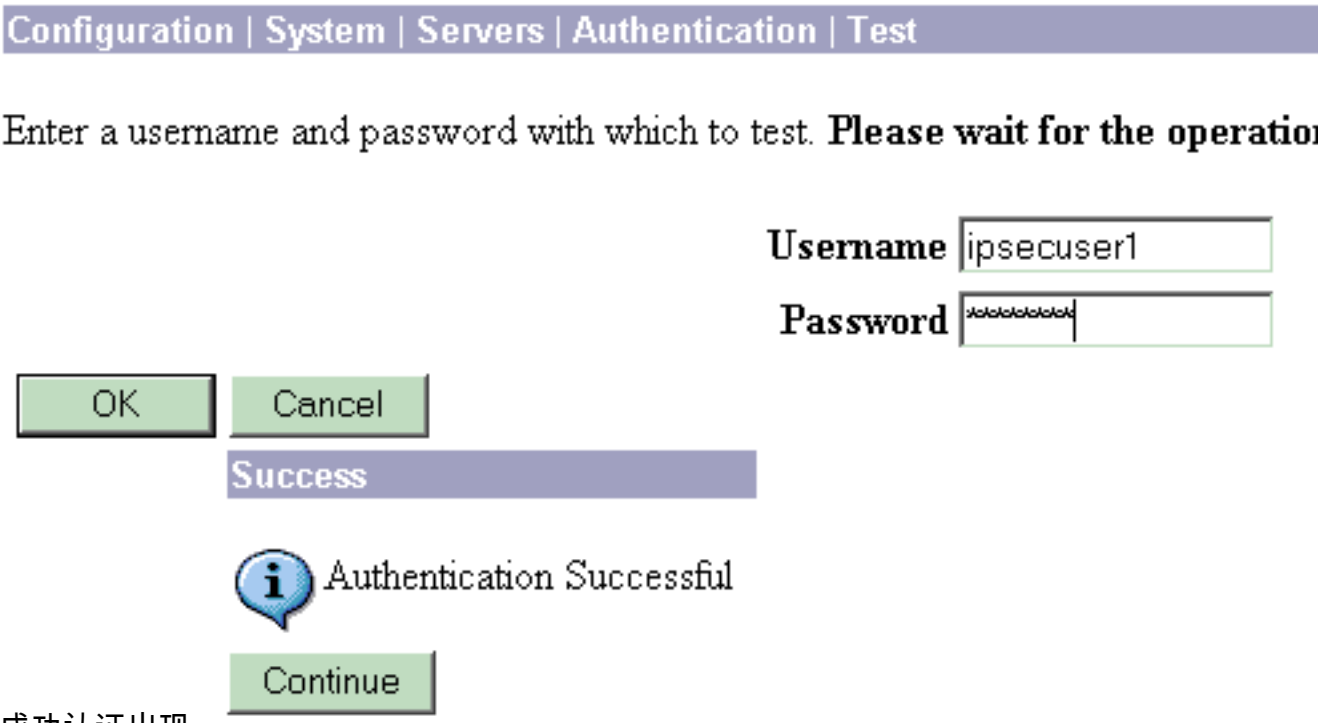
故障排除

完成以下步骤，对配置进行故障排除。

1. 选择**Configuration > System > Servers > Authentication**并且完成这些步骤为了测试RADIUS服务器和VPN 3000集中器之间的连接。选择您的服务器，然后单击**测验**。



输入RADIUS用户名和密码并且点击OK键。

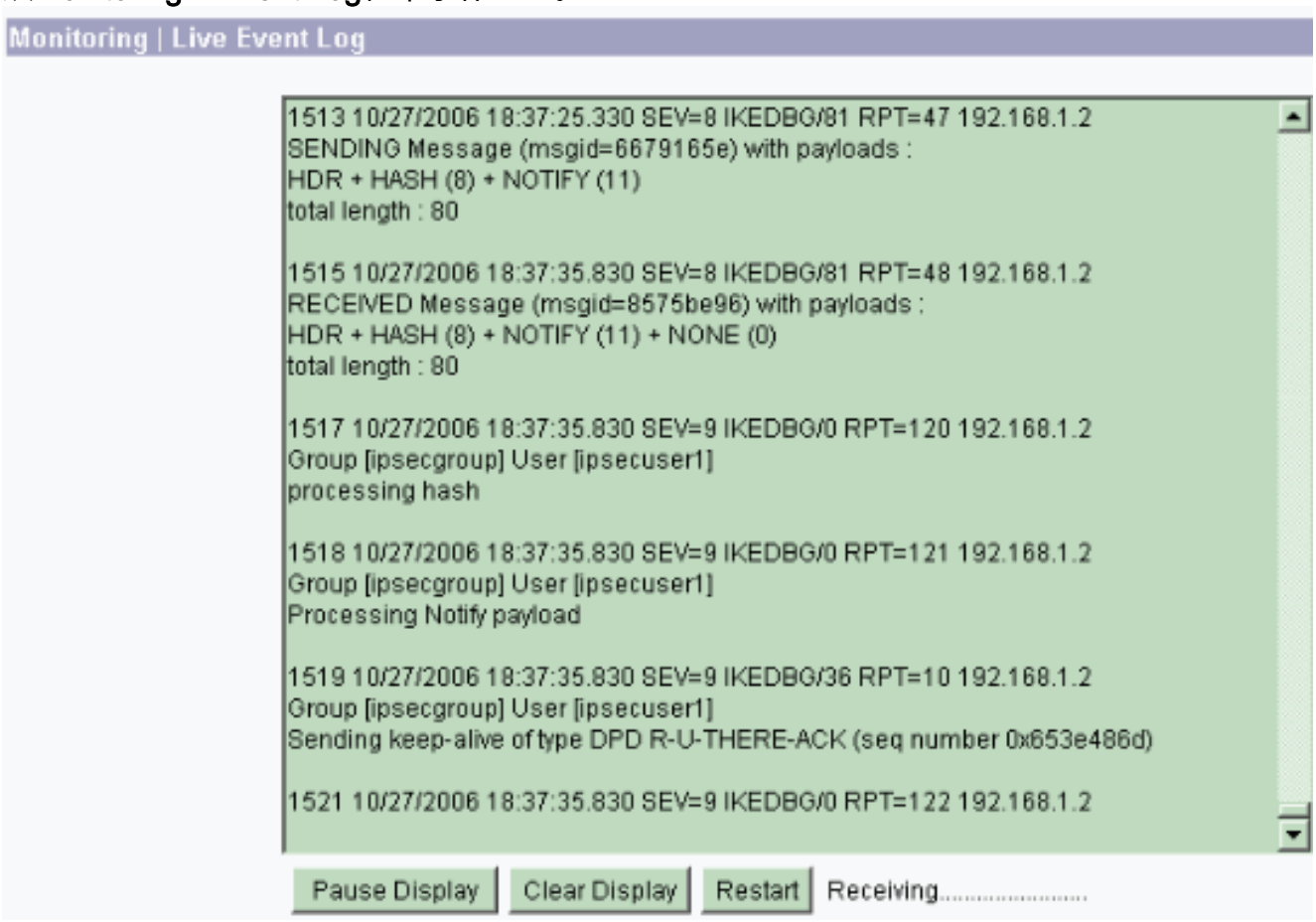


成功认证出现。

2. 如果它失败，有配置问题或IP连通性问题。检查ACS服务器上的Failed Attempts日志与失败相关的消息。如果消息在此日志没出现那么很可能有IP连通性问题。RADIUS请求不到达RADIUS服务器。验证过滤器应用对适当的VPN 3000集中器接口里里外外允许RADIUS (1645)数据包。如果测验验证是成功的，但是对VPN 3000集中器的登录继续发生故障，请通过控制台端口检查可过滤事件日志。如果连接不工作，您能添加验证、IKE和IPSec事件类到VPN集中器，当您选择**Configuration > System > Events > Classes > Modify时(对Log=1-9的**

对Console=1-3的严重性，严重性)。AUTHDBG， AUTHDECODE， IKEDBG， IKEDECODE， IPSECDBG，并且IPSECDECODE也是可用的，但是能提供许多信息。如果详细信息在从RADIUS服务器通过下来的属性必要， AUTHDECODE、IKEDECODE和IPSECDECODE提供此在严重性给级的Log=1-13。

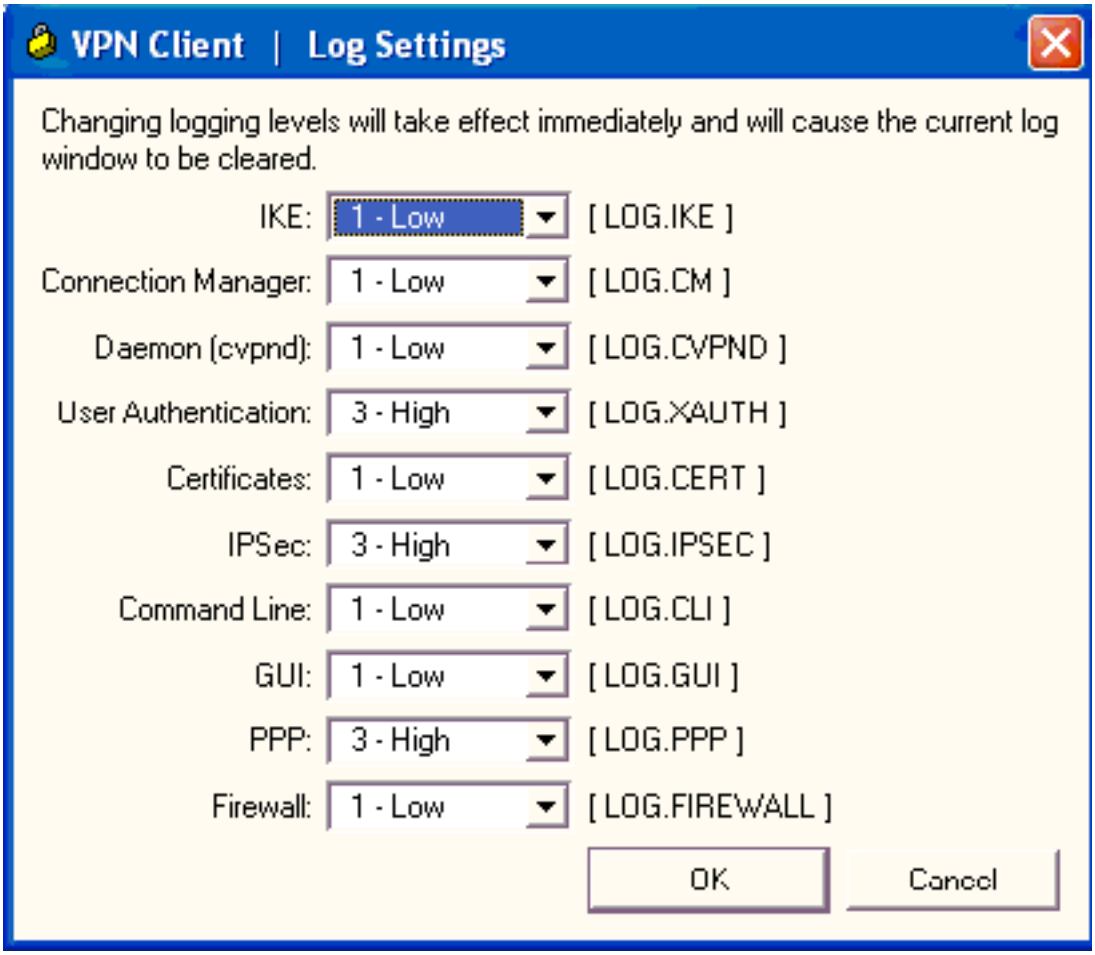
3. 从**Monitoring > Event Log**检索事件日志。



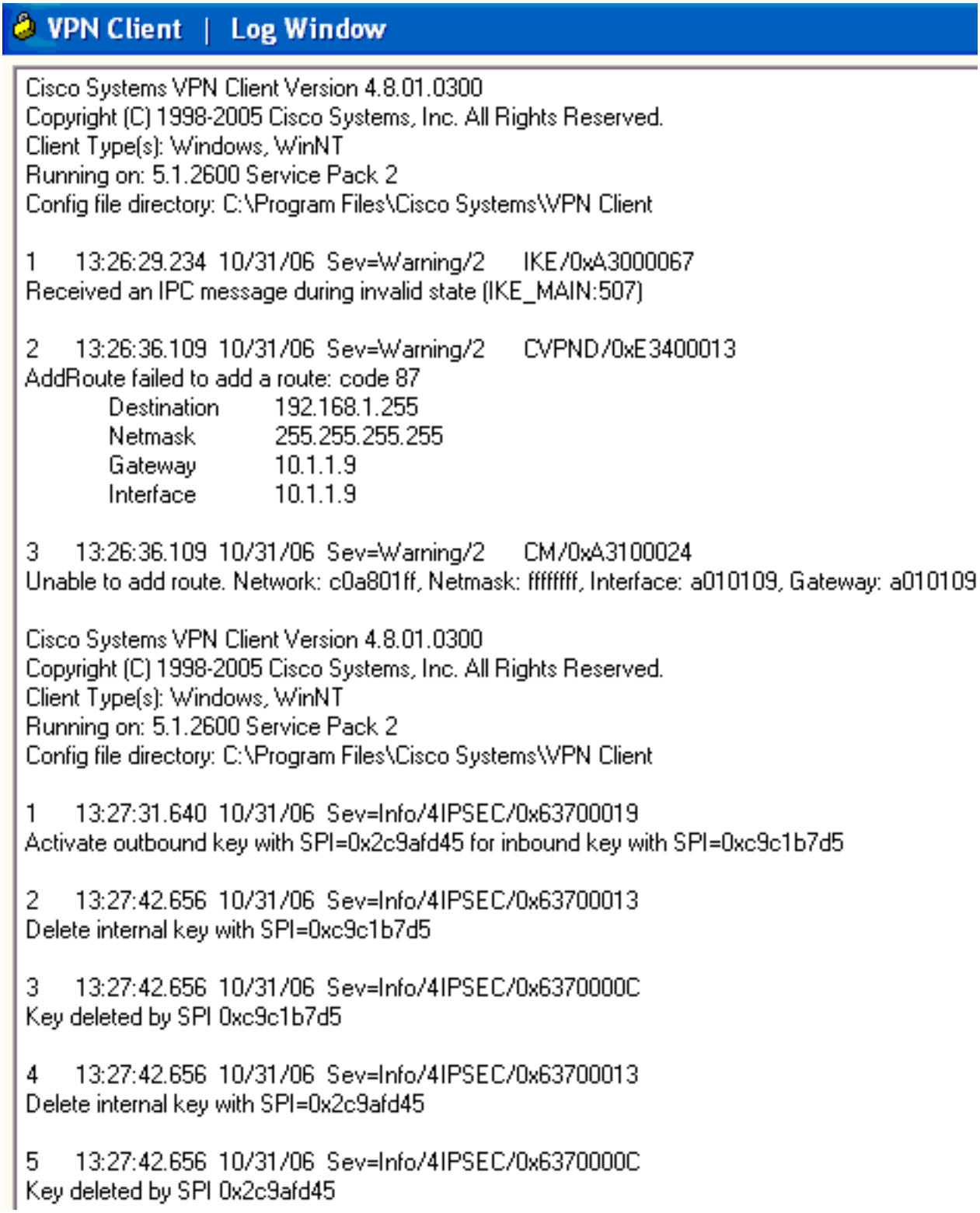
排除故障Windows的VPN客户端4.8

完成这些步骤为了排除故障Windows的VPN客户端4.8。

1. 选择**日志>日志设置**为了启用在VPN客户端的日志级别。



2. 选择**日志>日志窗口**为了查看在VPN客户端的日志条目。



相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 客户端支持页
- IPsec 协商/IKE 协议
- Cisco Secure ACS for Windows 支持页
- 配置在RADIUS服务器的动态过滤器
- 技术支持和文档 - Cisco Systems