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

本文档介绍如何在Cisco VPN 3000集中器与使用RADIUS进行用户身份验证和记帐的Microsoft Windows的Cisco VPN客户端4.x之间建立IPsec隧道。本文档建议使用适用于Windows的思科安全访问控制服务器(ACS)，以便更轻松地进行RADIUS配置，以验证连接到VPN 3000集中器的用户。VPN 3000集中器上的组是被视为单个实体的用户集合。组的配置可以简化系统管理并简化配置任务。

要在Cisco VPN客户端(4.x for Windows)和PIX 500系列安全之间设置远程访问VPN连接，请参阅PIX/ASA 7.x和Cisco VPN客户端4.x for Windows with Microsoft Windows 2003 IAS RADIUS身份验证配置示例。使用Microsoft Windows 2003 Internet Authentication Service(IAS)RADIUS服务器的设备7.x。

要配置路由器与使用RADIUS进行用户身份验证的Cisco VPN客户端4.x之间的连接，请参阅在Cisco IOS路由器和Cisco VPN客户端4.x之间为Windows配置IPsec。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure ACS for Windows RADIUS已安装，并可与其他设备正常运行。
- Cisco VPN 3000集中器已配置，可通过HTML界面进行管理。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 适用于Windows的思科安全ACS，版本4.0
- 带映像文件4.7.2.B的Cisco VPN 3000系列集中器
- 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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

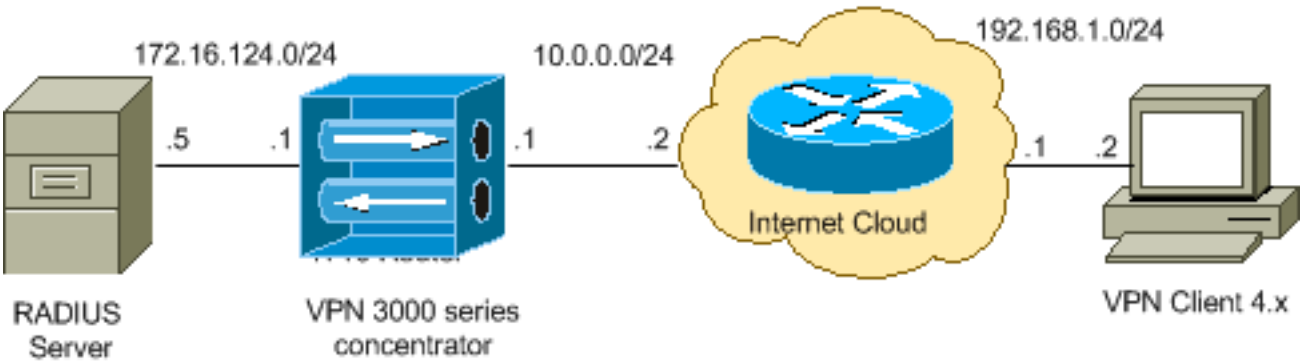
配置

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(仅限注册客户)可获取有关本节中使用的命令的详细信息。

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。

在VPN 3000集中器上使用组

可以为Cisco Secure ACS for Windows和VPN 3000集中器定义组，但它们使用的组略有不同。执行以下任务以简化操作：

- **在VPN 3000集中器上为建立初**始隧道时配置单个组。这通常称为隧道组，用于使用预共享密钥（组密码）建立到VPN 3000集中器的加密互联网密钥交换(IKE)会话。 这是应在所有要连接到VPN集中器的思科VPN客户端上配置的相同组名称和密码。
- **在Cisco Secure ACS for Windows服务器上配置使用标**准RADIUS属性和供应商特定属性(VSA)进行策略管理的组。应与VPN 3000集中器一起使用的VSA是RADIUS(VPN 3000)属性。
- **在Cisco Secure ACS for Windows RADIUS服务器上配置用户，并将其分配到同一服务器**上配置的其中一个组。用户继承为其组定义的属性，当用户通过身份验证时，Cisco Secure ACS for Windows将这些属性发送到VPN集中器。

VPN 3000 集中器如何使用组和用户属性

在VPN 3000集中器使用VPN集中器对隧道组和使用RADIUS的用户进行身份验证后，它必须组织它收到的属性。VPN集中器按照以下优先顺序使用属性，无论身份验证是在VPN集中器中完成还是使用RADIUS:

1. **用户属**性 — 这些属性始终优先于任何其他属性。
2. **隧道组属性** — 当用户通过身份验证时未返回的任何属性由隧道组属性填充。
3. **基本组属性** - VPN集中器基本组属性填充用户或隧道组属性中缺少的任何属性。

VPN 3000系列集中器配置

完成本节中的步骤，以便为IPsec连接所需的参数配置Cisco VPN 3000集中器，以及为VPN用户配置AAA客户端以向RADIUS服务器进行身份验证。

在本实验设置中，首先通过控制台端口访问VPN集中器，然后添加最小配置，如以下输出所示：

```
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集中器显示在快速配置中，并且这些项目已配置。

- 时间/日期
- “Configuration > Interfaces”中的接口/掩码（public=10.0.0.1/24，private=172.16.124.1/24）
- Configuration > System > IP routing > Default_Gateway**(10.0.0.2)中的Default Gateway（默认网关）**

此时，VPN集中器可通过HTML从内部网络访问。

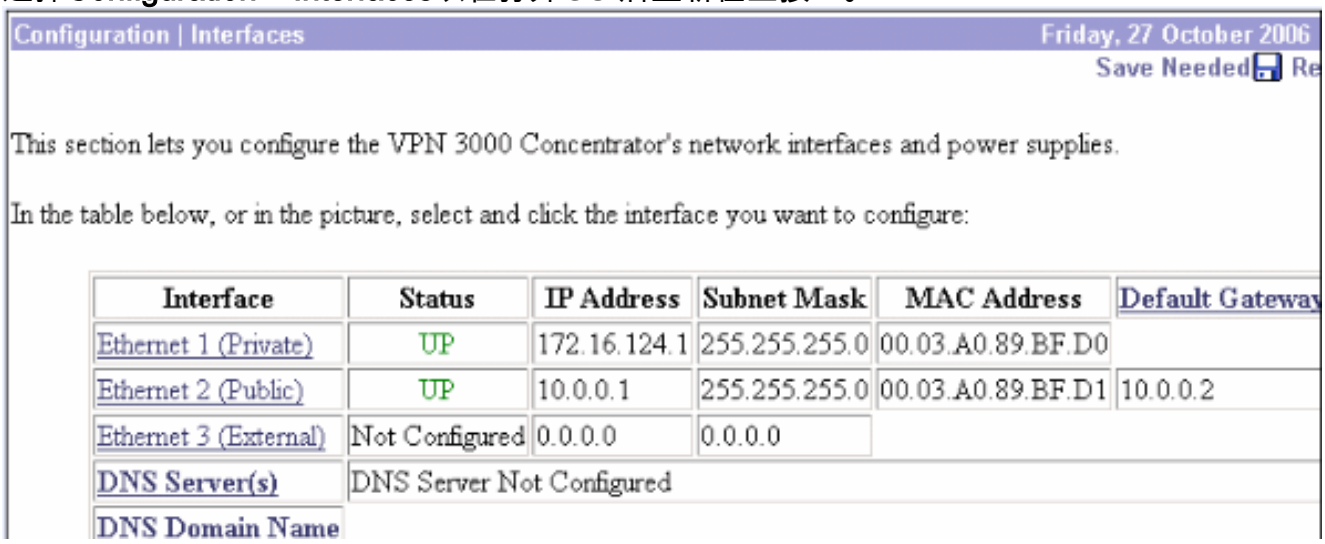
注：如果VPN集中器是从外部管理的，则您还执行以下步骤：

1. 选择**Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1. Private（默认）**。
2. 选择**Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager Workstation**以添加外部管理器的IP地址。

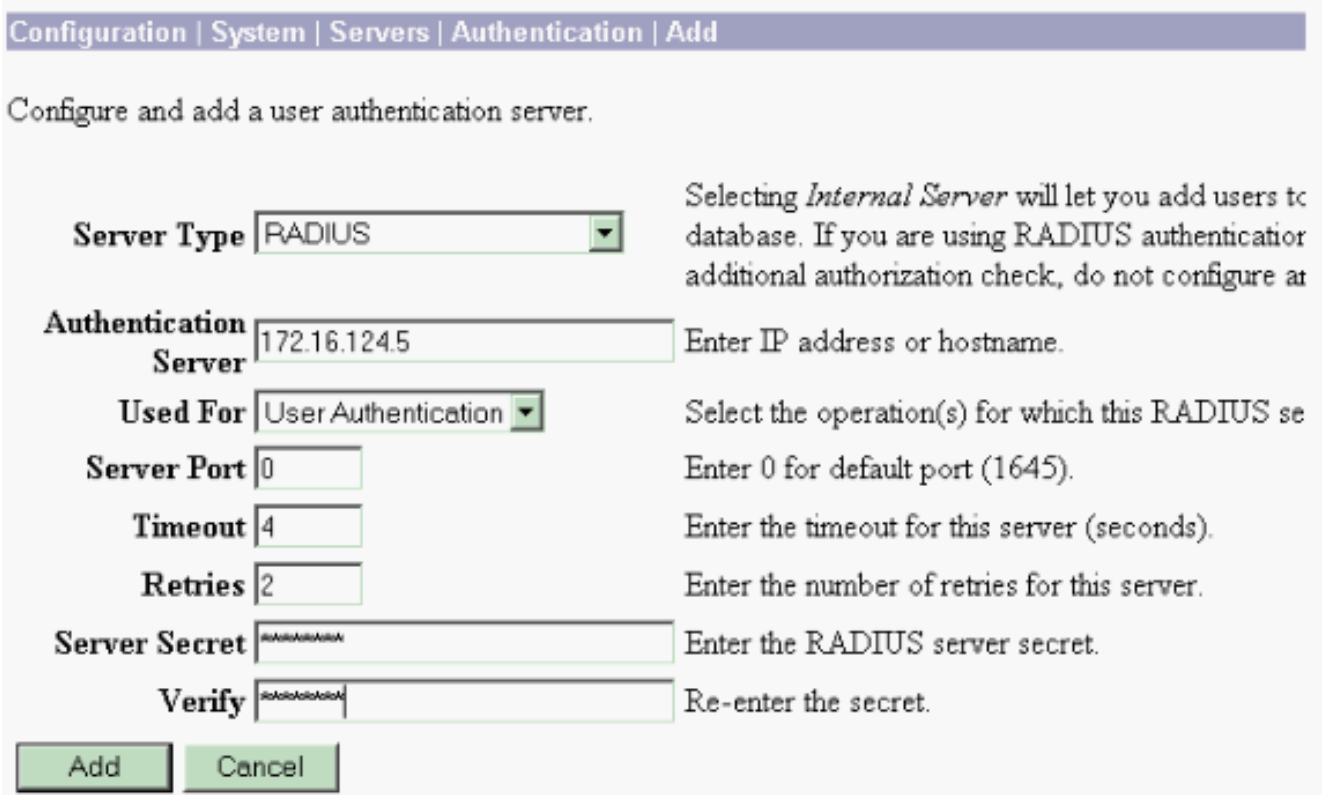
仅当从外部管理VPN集中器时，才需要执行这些步骤。

完成这两个步骤后，可通过GUI使用Web浏览器并连接到刚配置的接口的IP，完成其余配置。在本示例中，此时可从内部网络通过HTML访问VPN集中器：

1. 选择**Configuration > Interfaces**以在打开GUI后重新检查接口。

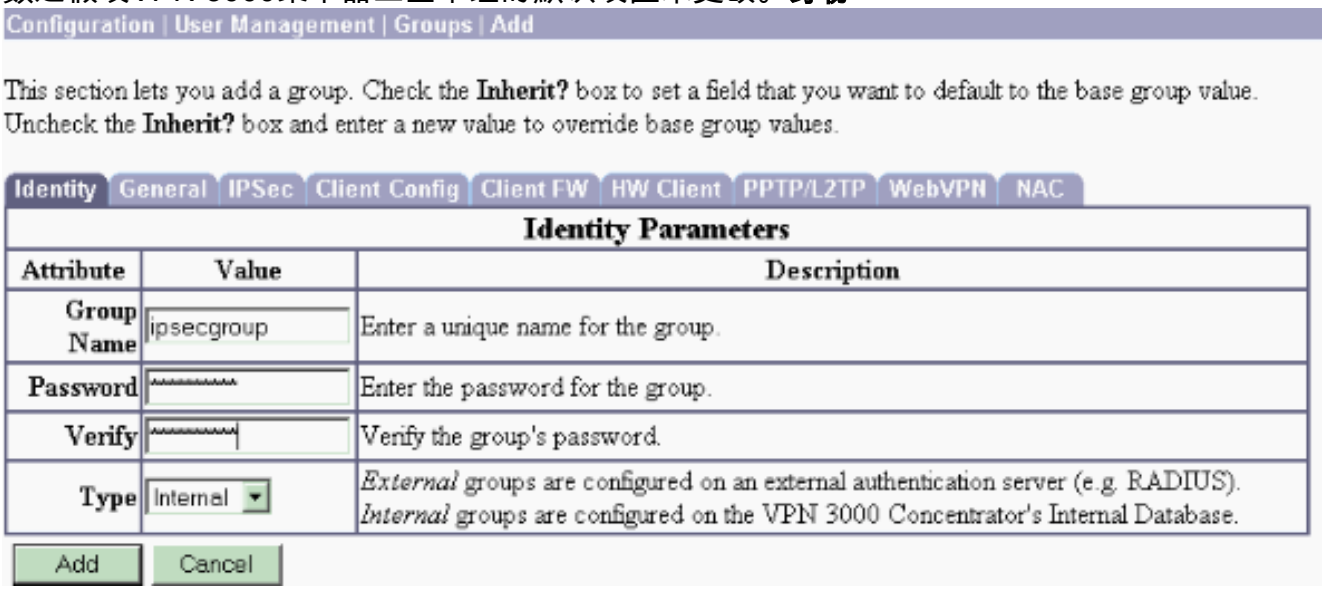


2. 要将Cisco Secure ACS for Windows RADIUS服务器添加到VPN 3000集中器配置，请完成以下步骤。选择**Configuration > System > Servers > Authentication**，然后从左**菜单**中单击Add。



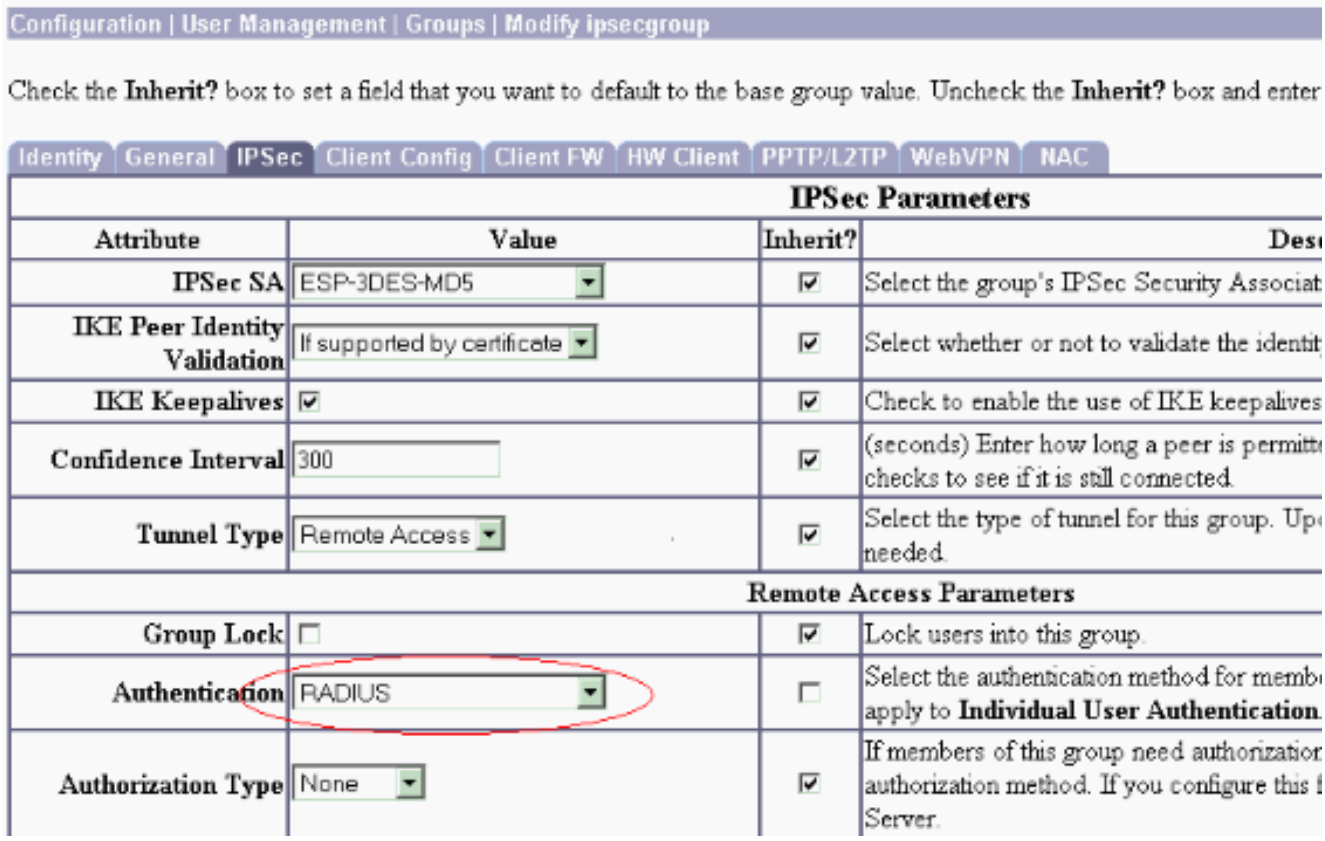
选择服务器类**型RADIUS**，并为Cisco Secure ACS for Windows RADIUS服务器添加这些参数。将所有其他参数保留为默认状态。**Authentication Server** — 输入Cisco Secure ACS for Windows RADIUS服务器的IP地址。**Server Secret** — 输入RADIUS服务器密钥。这必须是您在Cisco Secure ACS for Windows配置中配置VPN 3000集中器时使用的相同密钥。**Verify** — 重新输入密码以进行验证。这会在VPN 3000集中器的全局配置中添加身份验证服务器。此服务器由所有组使用，除非已明确定义身份验证服务器。如果未为组配置身份验证服务器，则会恢复为全局身份验证服务器。

3. 要在VPN 3000集中器上配置隧道组，请完成以下步骤。从左**菜单中选择Configuration > User Management > Groups**，然后单击“Add”。在“配置”选项卡中更改或添加这些参数。在更改所有这些参数之前，请勿点击应用：**注意：**这些参数是远程访问VPN连接所需的最低值。这些参数还假设VPN 3000集中器上基本组的默认设置未更改。**身份**



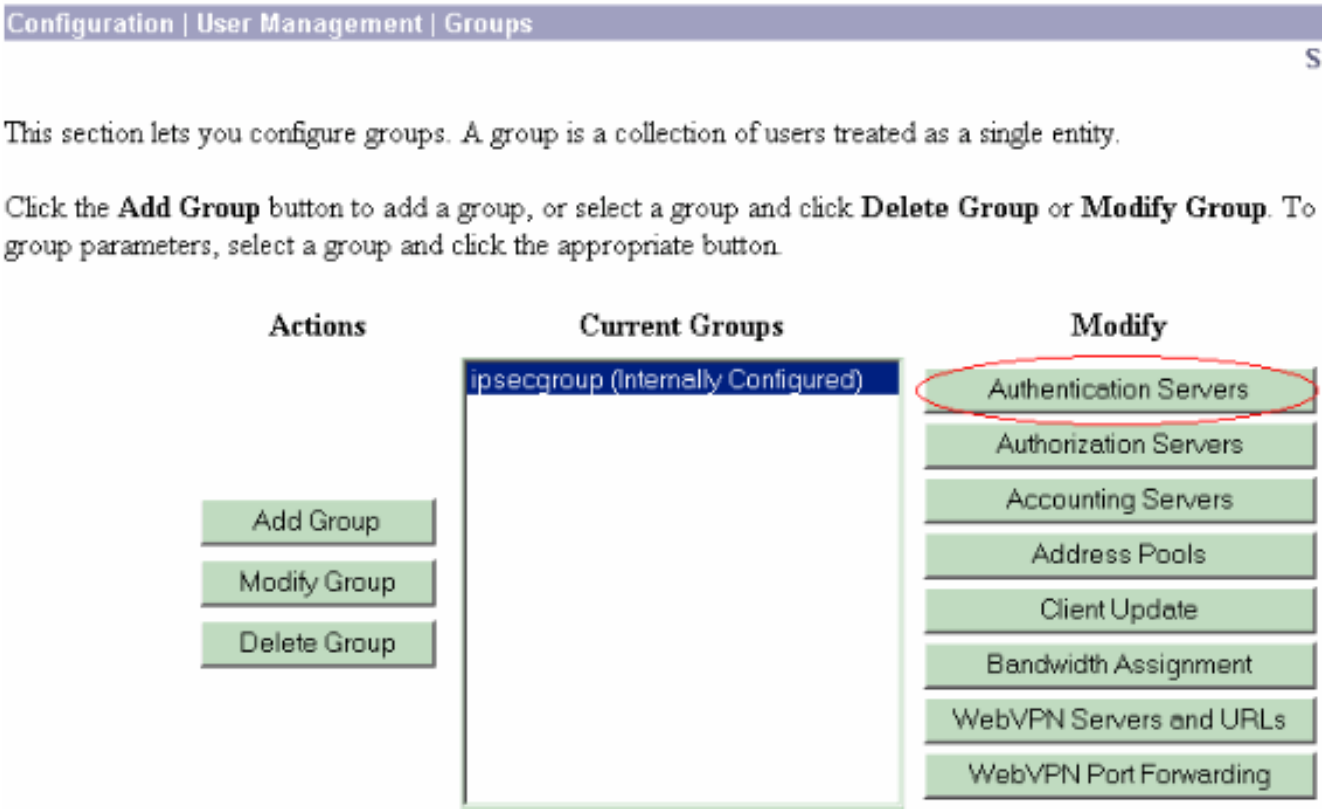
组名(Group Name) — 键入组名。例如，IPsecUsers。**Password** — 输入组的密码。这是IKE会话的预共享密钥。**Verify** — 重新输入密码以进行验证。**类型**(Type) — 保留默认值：内部。

IPsec



Tunnel Type — 选择**Remote-Access**。**身份验**证 — RADIUS。这将告诉VPN集中器使用什么方法来对用户进行身份验证。**模式配置**(Mode Config)-**检查模式配**置。单击 **Apply**。

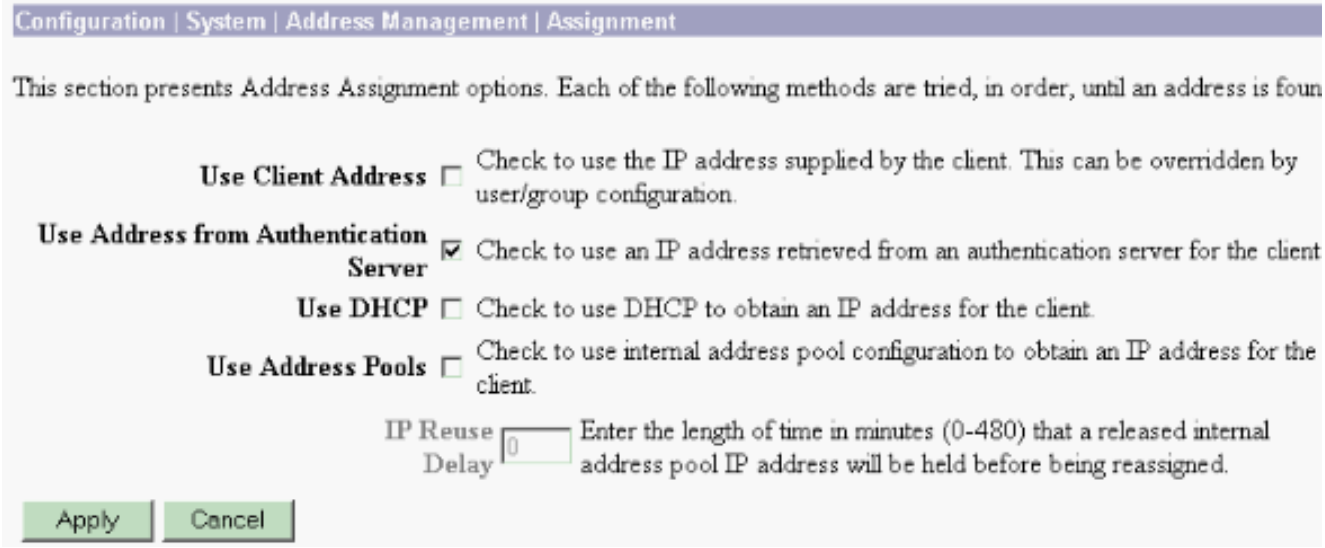
4. 要在VPN 3000集中器上配置多个身份验证服务器，请完成以下步骤。定义组后，突出显示该组，然后单击“修改”列**下的“**身份验证服务器”。即使全局服务器中不存在这些服务器，也可以为每个组定义单个身份验证服务器。



选择服务器类型**RADIUS**，并为Cisco Secure ACS for Windows RADIUS服务器添加这些参数。将所有其他参数保留为默认状态。**Authentication Server** — 输入Cisco Secure ACS for Windows RADIUS服务器的IP地址。**Server Secret** — 输入RADIUS服务器密钥。这必须是您在Cisco Secure ACS for Windows配置中配置VPN 3000集中器时使用的相同密钥。**Verify** —

重新输入密码以进行验证。

5. 选择**Configuration > System > Address Management > Assignment**并选中**Use Address from Authentication Server**，以便在客户端通过身份验证后，将IP地址从RADIUS服务器中创建的IP池分配给VPN客户端。

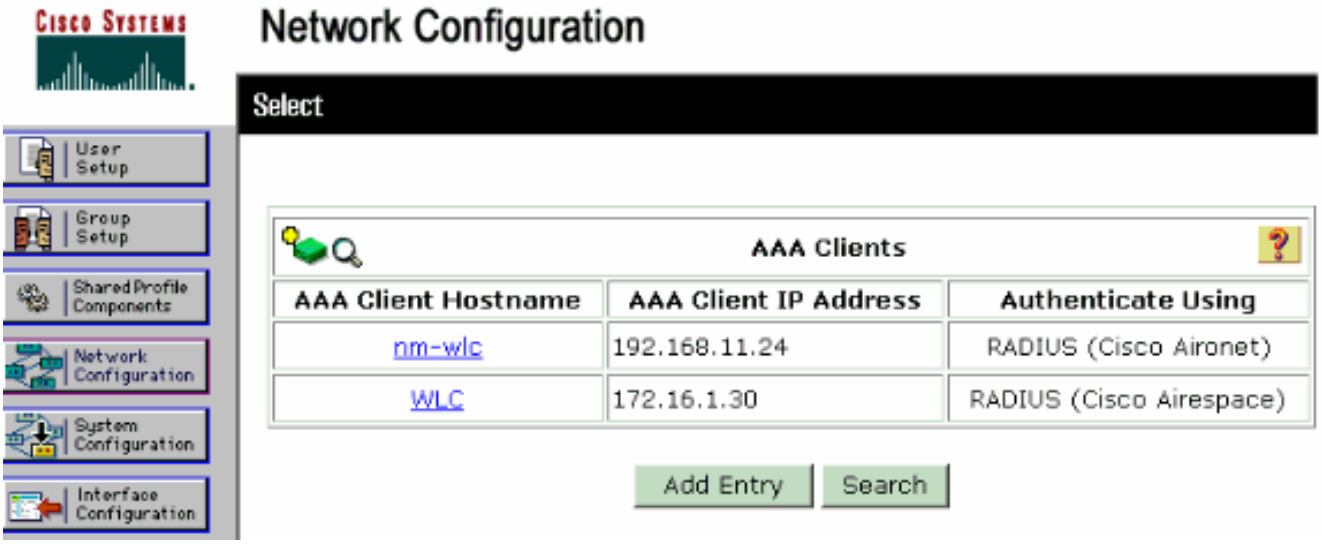


RADIUS 服务器配置

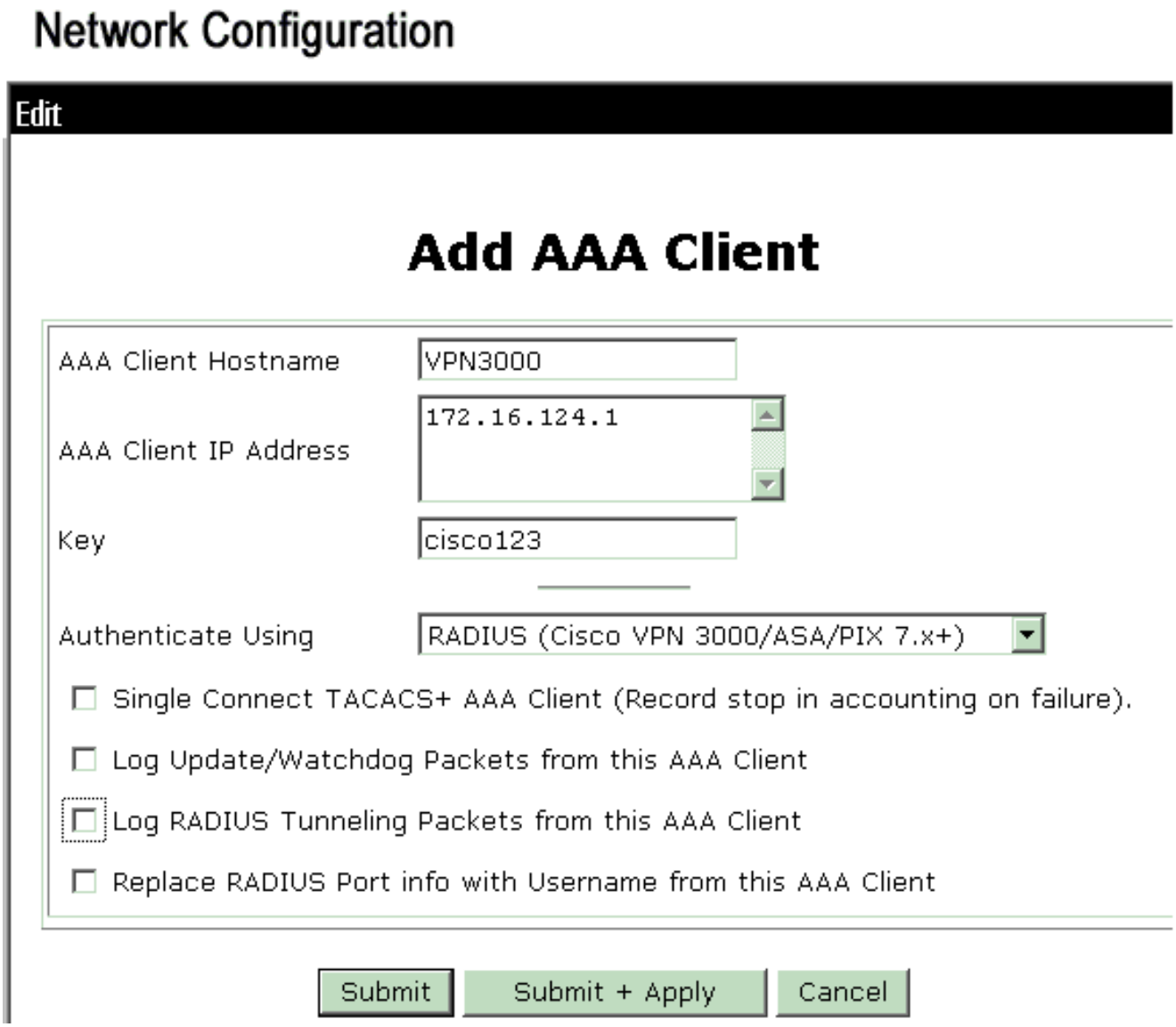
本文档的此部分介绍将Cisco Secure ACS配置为RADIUS服务器，以便Cisco VPN 3000系列集中器— AAA客户端转发VPN客户端用户身份验证。

双击**ACS Admin**图标，以在运行Cisco Secure ACS for Windows RADIUS服务器的PC上启动管理会话。如果需要，使用正确的用户名和密码登录。

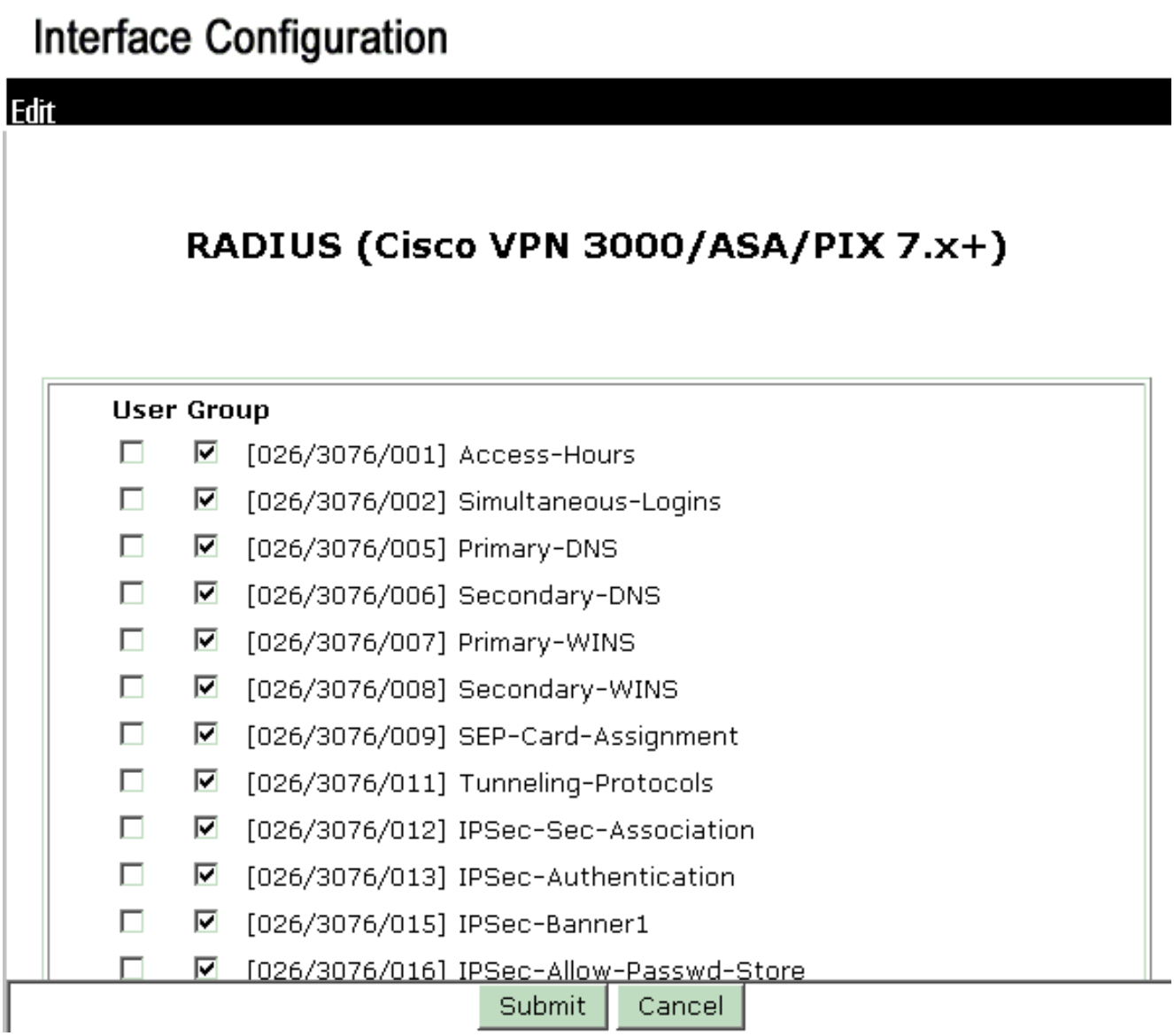
1. 要将VPN 3000集中器添加到Cisco Secure ACS for Windows服务器配置，请完成以下步骤。选择**网络配置**并单**击添**加条目以将AAA客户端添加到RADIUS服务器。



为VPN 3000集中器添加以下参数：

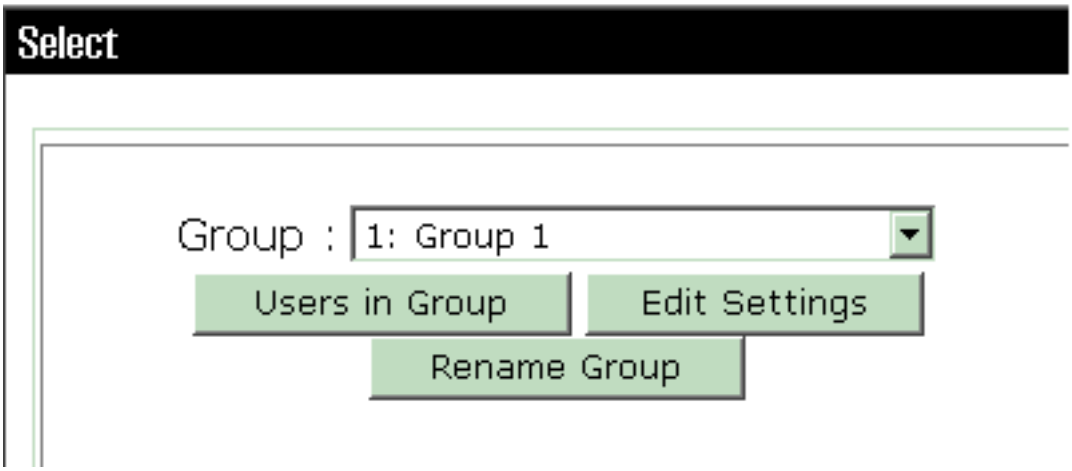


AAA Client Hostname — 输入VPN 3000集中器的主机名（用于DNS解析）。**AAA Client IP Address** — 输入VPN 3000集中器的IP地址。**Key** — 输入RADIUS服务器密钥。这必须是您在VPN集中器上添加身份验证服务器时配置的密钥。**Authenticate Using** — 选**择RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**。 这允许VPN 3000 VSA显示在Group配置窗口中。单击“Submit”。选择**Interface Configuration**，单**击RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**，然后选中**Group [26] Vendor-Specific**。

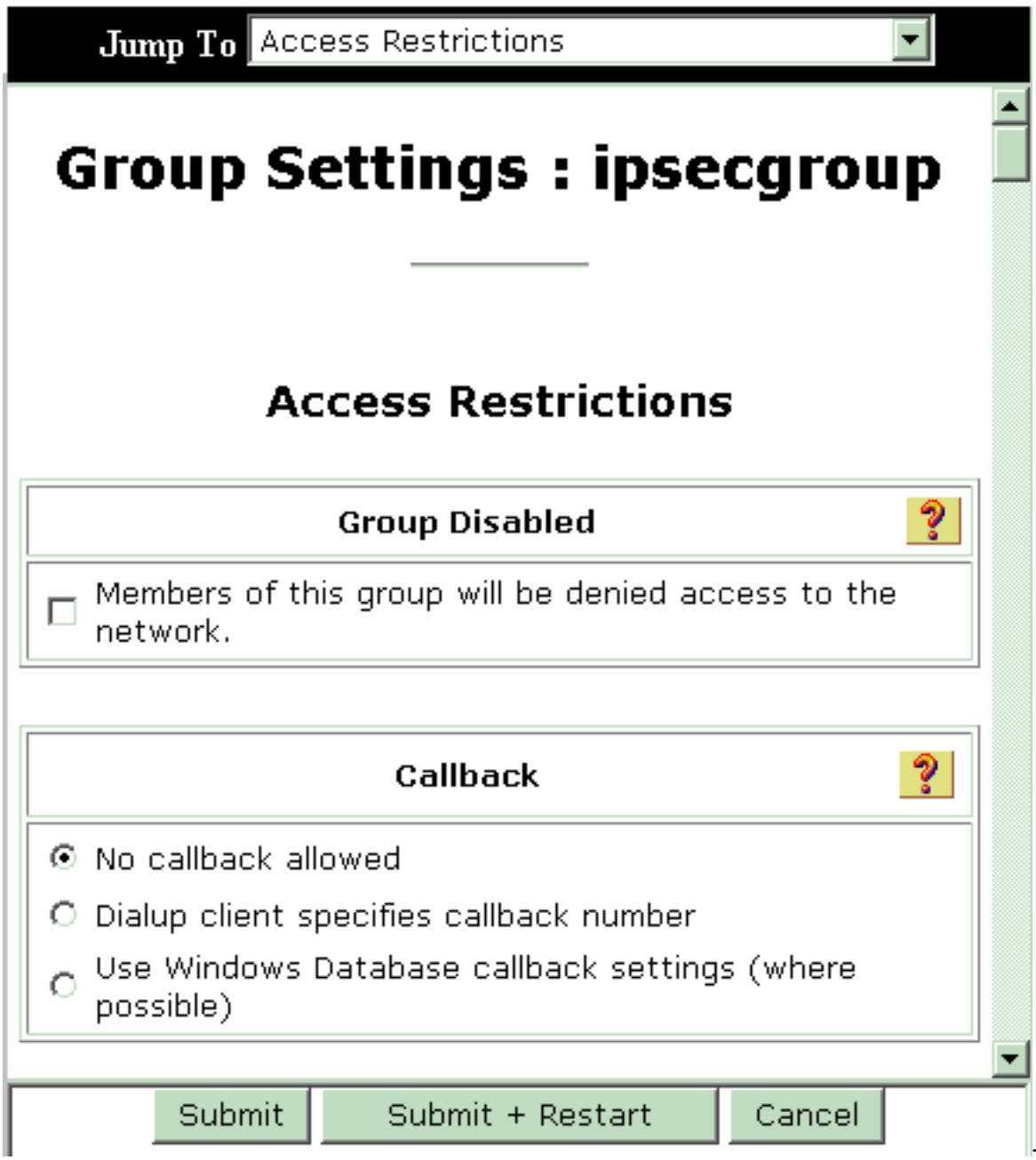


注意：“RADIUS属性26”是指所有供应商特定属性。例如，选择**Interface Configuration > RADIUS(Cisco VPN 3000)**，并查看所有可用属性以026开头。这显示所有这些供应商特定属性都属于IETF RADIUS 26标准。默认情况下，这些属性不会在“用户”或“组”设置中显示。要在组设置中显示，请创建在网络配置中使用RADIUS进行身份验证的AAA客户端（在本例中为VPN 3000集中器）。然后，从接口配置中检查需要在用户设置、组设置或两者中显示的属性。有关可用属性及其用法的详细信息，请参阅RADIUS属性。单击“Submit”。

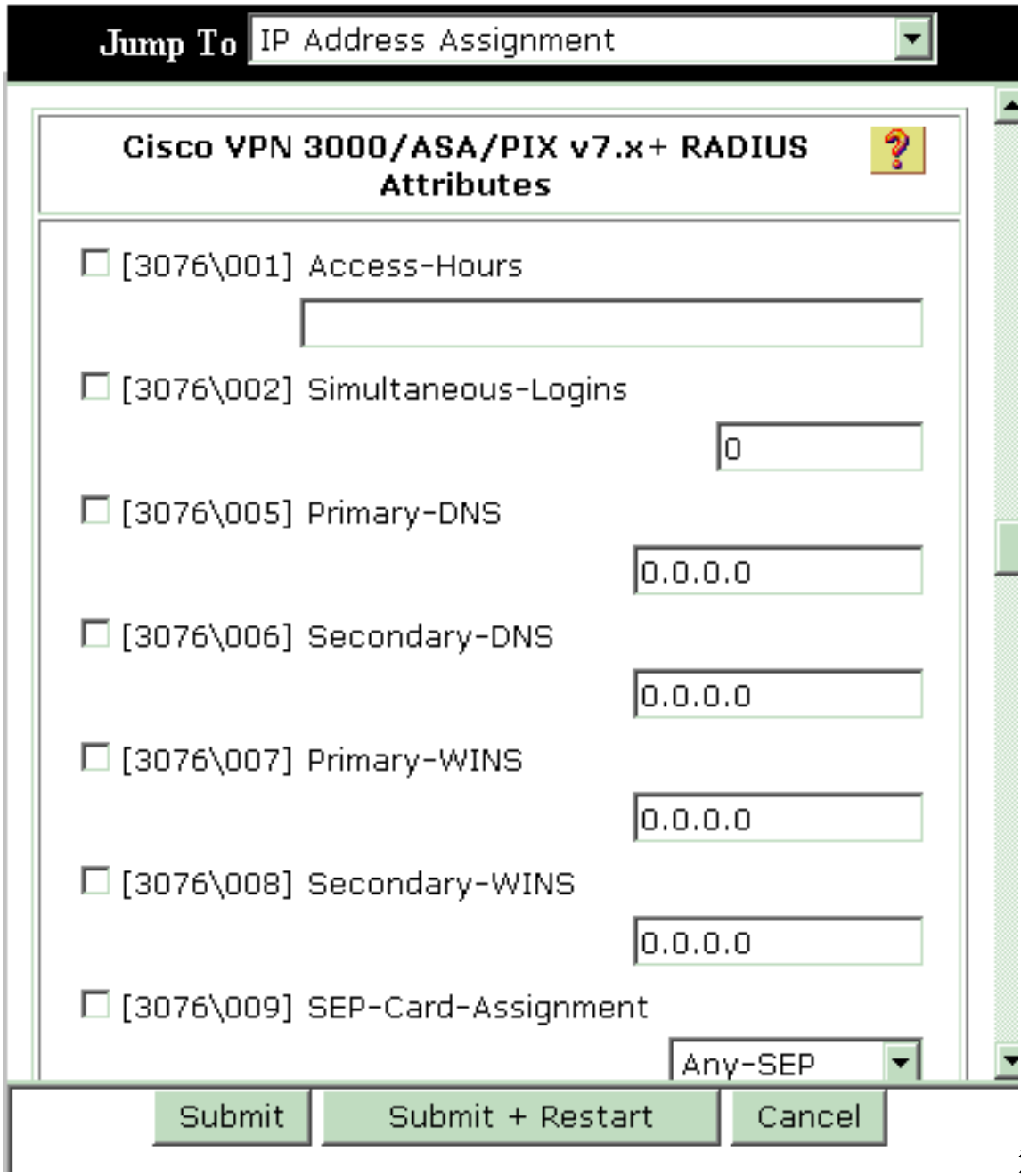
2. 要向Cisco Secure ACS for Windows配置添加组，请完成以下步骤。选择**Group Setup**，然后选择其中一个模板组，例如Group 1，然后单击**Rename Group**。



将名称更改为适合贵组织的名称。例如，ipsecgroup。由于用户已添加到这些组，因此请使组名称反映该组的实际用途。如果所有用户都放在同一组中，您可以将其称为VPN用户组。单击**Edit Settings**以编辑新重命名的组中的参数。

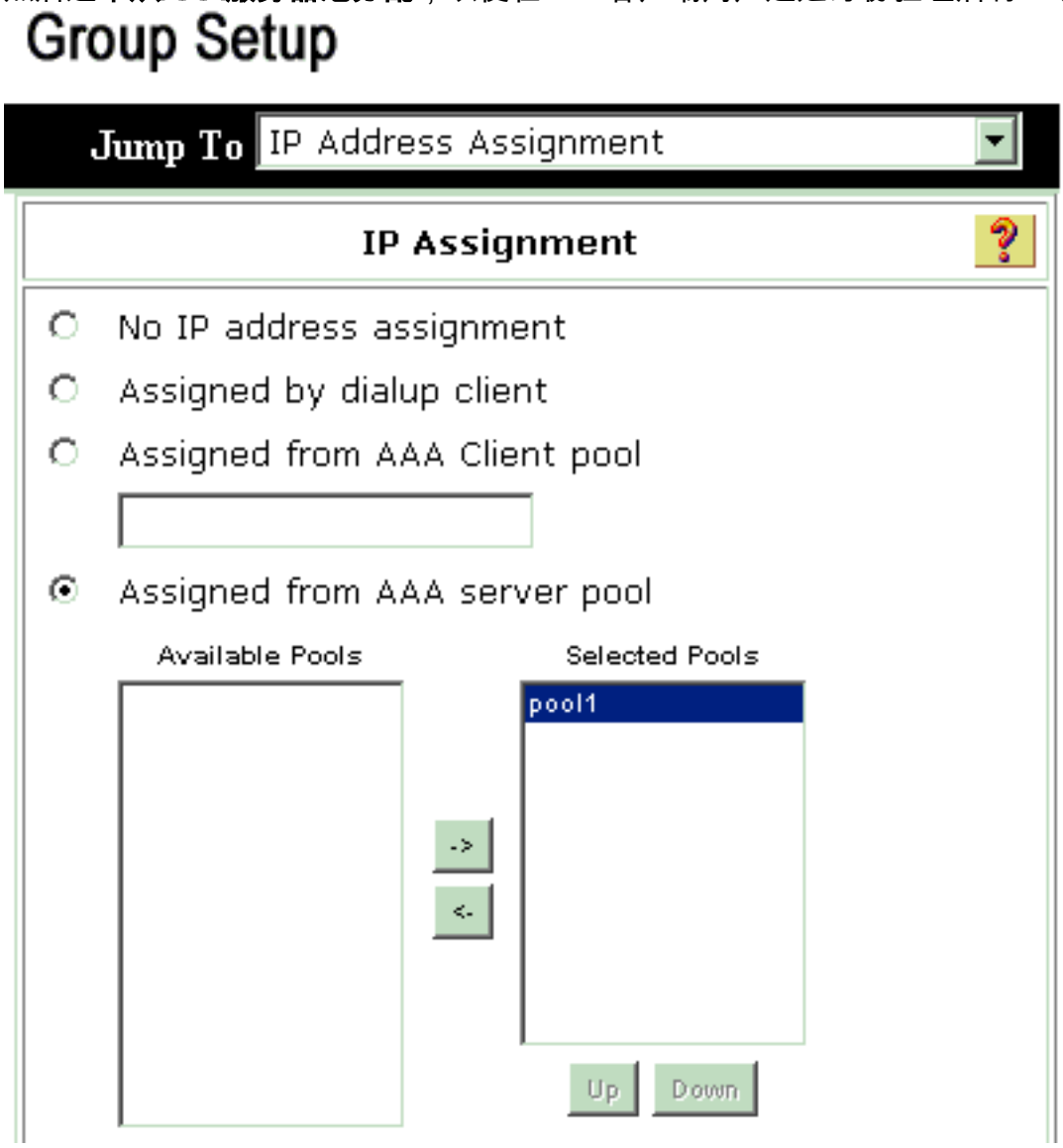


单击**Cisco VPN 3000 RADIUS**并配置这些推荐属性。这允许分配给此组的用户继承Cisco VPN 3000 RADIUS属性，这允许您集中Cisco Secure ACS for Windows中所有用户的策略。

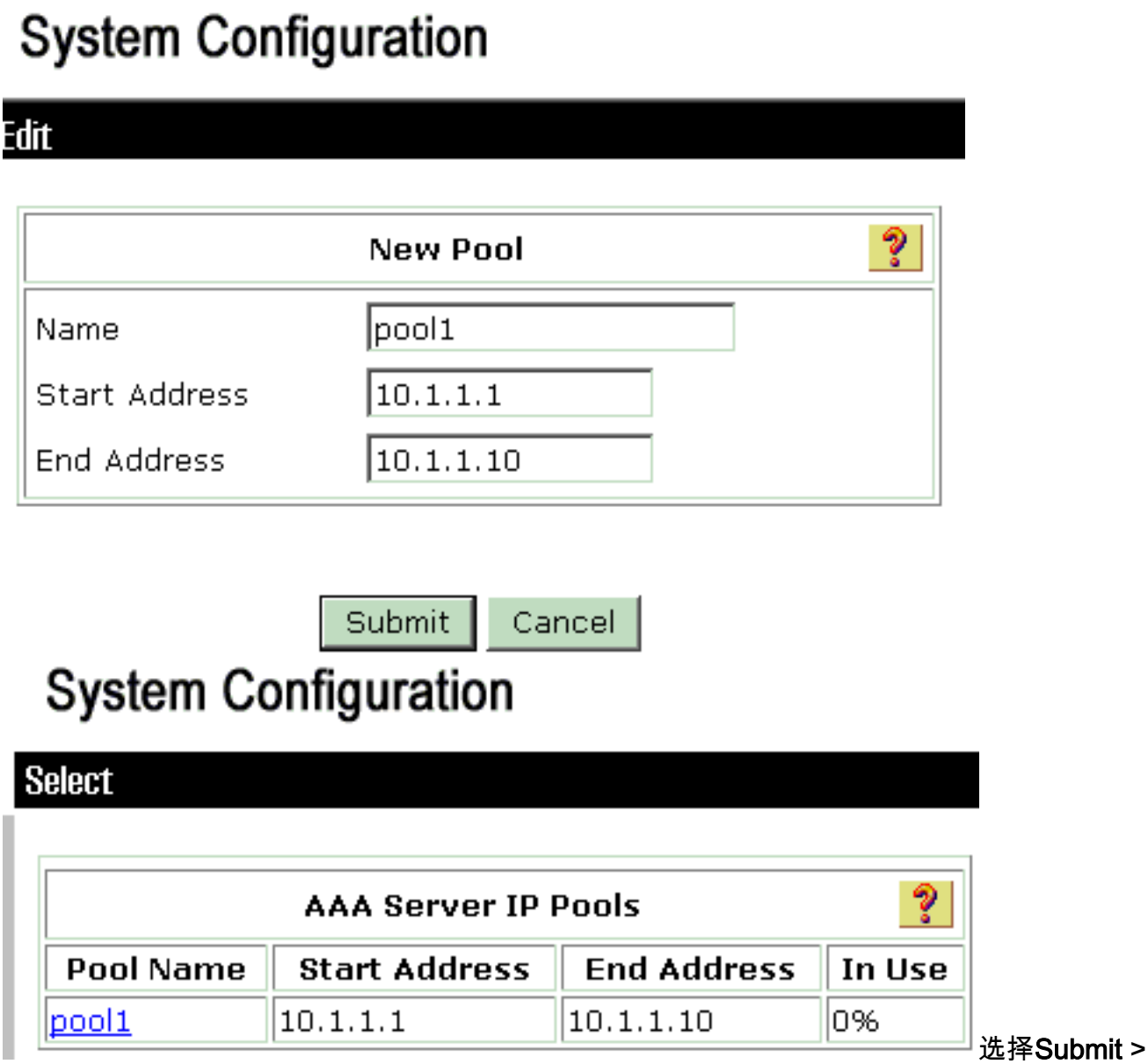


注：从技术上讲，只要在VPN 3000系列集中器配置的步骤3中设置隧道组，并且VPN集中器中的基组不会从原始默认设置更改，就无需配置VPN 3000 RADIUS属性。**推荐的VPN 3000属性：Primary-DNS** — 输入主DNS服务器的IP地址。**Secondary-DNS** — 输入辅助DNS服务器的IP地址。**Primary-WINS** — 输入主WINS服务器的IP地址。**Secondary-WINS** — 输入辅助WINS服务器的IP地址。**Tunneling-Protocols** — 选择**IPsec**。这仅允*许*IPsec客户端连接。不允许使用PPTP或L2TP。**IPsec-Sec-Association** — 输入**ESP-3DES-MD5。这**可确保所有IPsec客户端都使用可用的最高加密进行连接。**IPsec-Allow-Password-Store** — 选择**Disallow**，使*用*户不能将其密码保存在VPN客户端。**IPsec-Banner** — 输入欢迎消息标语，在连接时向用户显示。例如，“欢迎使用MyCompany员工VPN访问！”**IPsec-Default Domain** — 输入您公司的域名。例如，“mycompany.com”。这组属性不是必需的。但是，如果您不确定VPN 3000集中器的基本组属性是否已更改，则思科建议您配置以下属性：**同时登录** — 输入允许用户同时使用同一用户名登录的次数。建议为1或2。**SEP-Card-Assignment** — 选**择任意SEP。IPsec-Mode-Config** — 选**择ON。IPsec over UDP** — 选择**OFF**，除非您希望此组中的用户使用IPsec over UDP协议进行连接。如果选择ON，则VPN客户端仍能够本地禁用IPsec over UDP并正常连接。**IPsec over UDP Port** — 选择范围为4001到49151的UDP端口号。仅当IPsec over UDP处于

打开状态时，才使用此端口号。下一组属性要求您首先在VPN集中器上设置某些属性，然后才能使用它们。建议仅对高级用户使用。**Access-Hours** — 这要求您在VPN 3000集中器的Configuration > **Policy Management**下设置一**系列**的Access Hours。而是使用Cisco Secure ACS for Windows中的“访问时数”来管理此属性。**IPsec-Split-Tunnel-List** — 这要求您在VPN集中器上的Configuration > **Policy Management > Traffic Management**下设置网络列表。这是发送到客户端的网络列表，它告诉客户端仅将数据加密到列表中的那些网络。在组**设置中选择IP分配，**然后选**中从AAA服务器池分配**，以便在VPN客户端用户通过身份验证后将IP地址分配给他们。

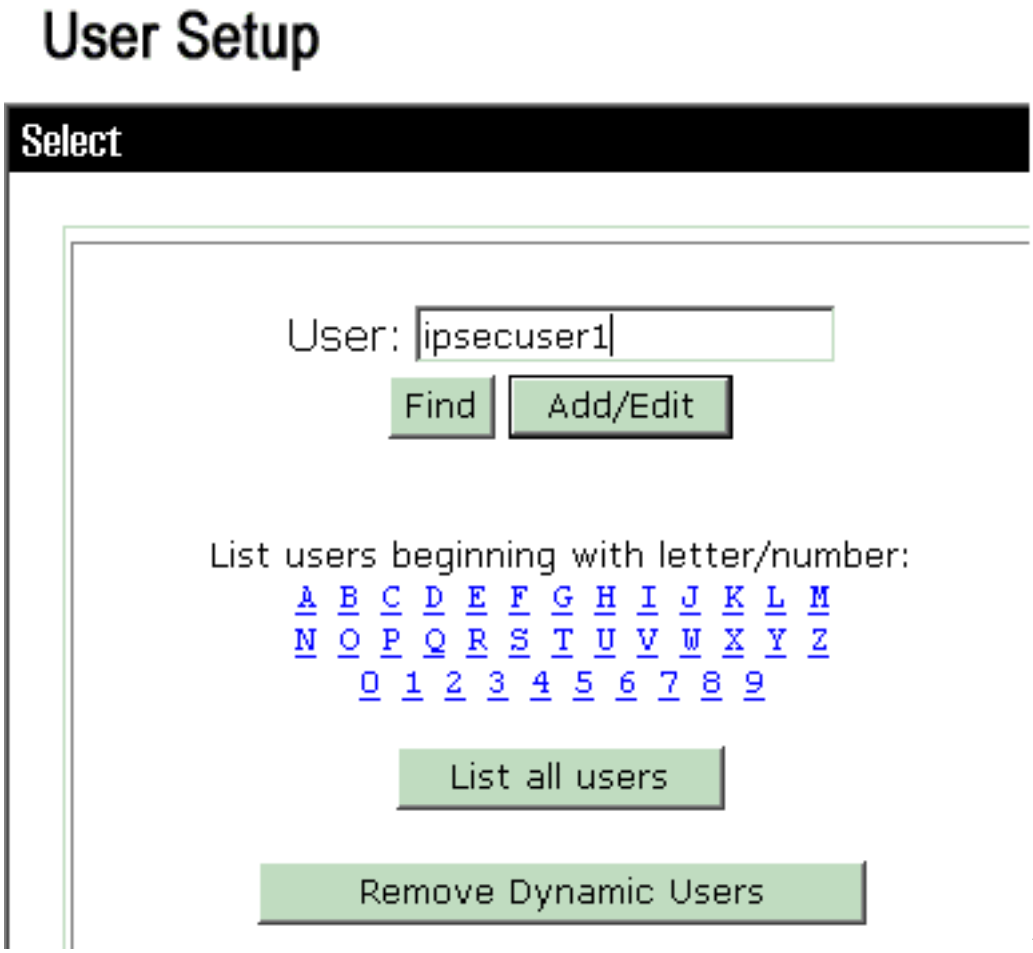


选择**System configuration > IP pools**以为VPN Client用户创建IP池，然后单击**Submit**。

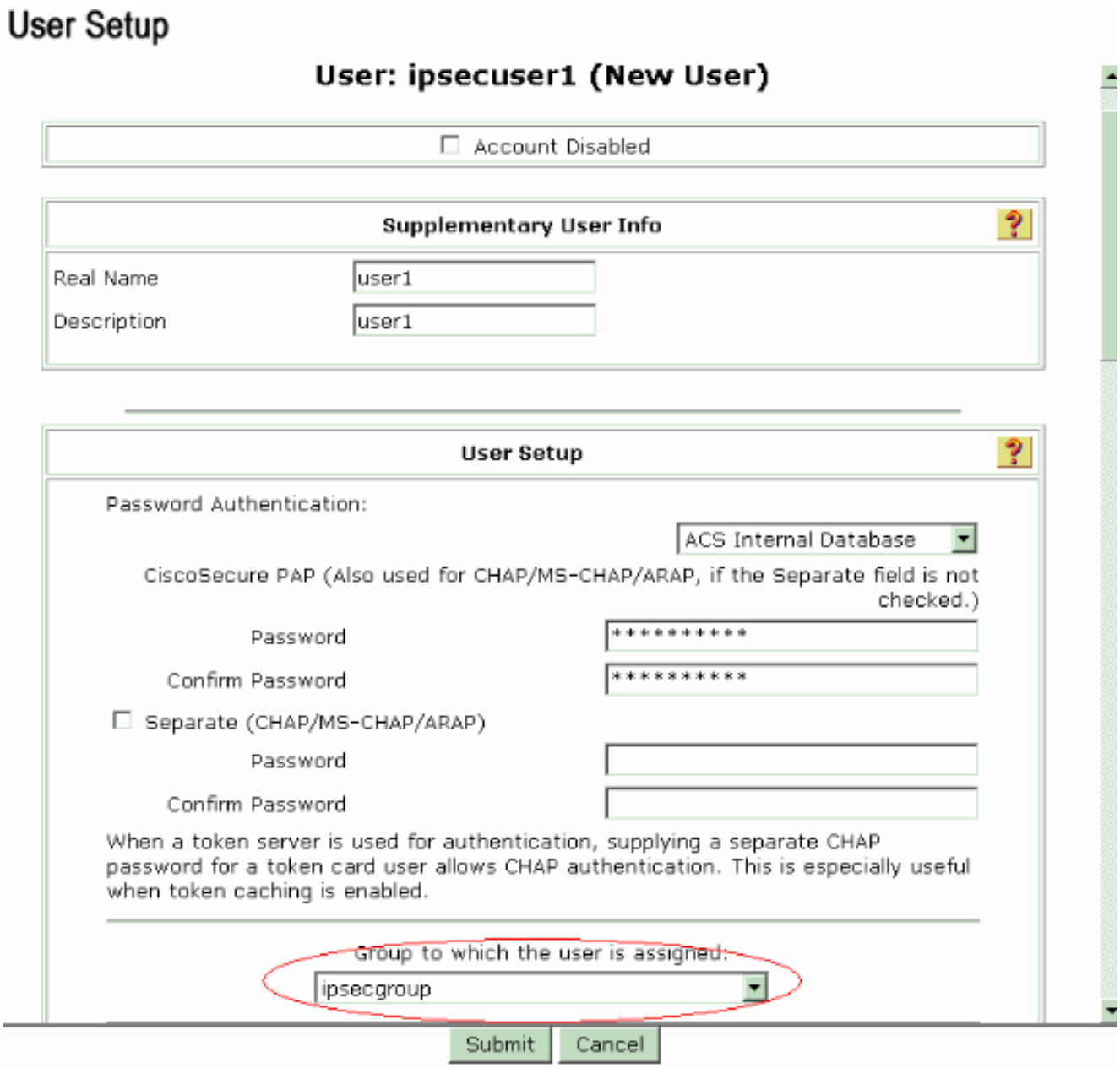


选择**Submit** > **Restart**以保存配置并激活新组。重复这些步骤以添加更多组。

3. **在Cisco Secure ACS for Windows上配置用户。**选择**User Setup**，输入用户名，然后单击



Add/Edit。在用户设置部分下配置以下参数：

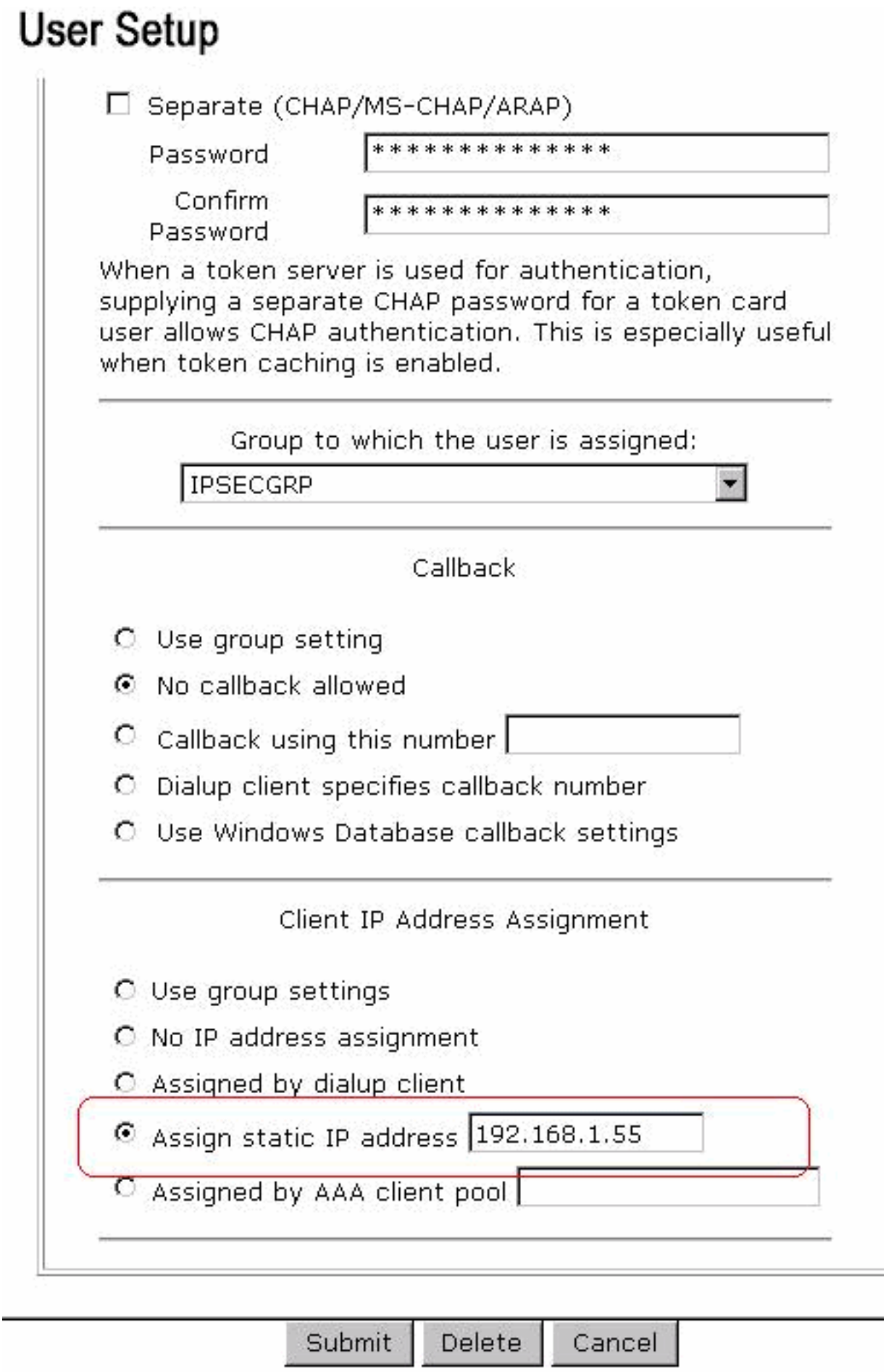


Password Authentication — 选择**ACS Internal Database**。**Cisco Secure PAP - Password** — 输入用户的密码。**Cisco Secure PAP — 确认密码** — 重新输入新用户的密码。**用户分配到的组** — 选择您在上一步中创建的组的名称。单击**Submit**以保存并激活用户设置。重复这些步骤以添加其他用户。

为VPN客户端用户分配静态IP地址

请完成以下步骤：

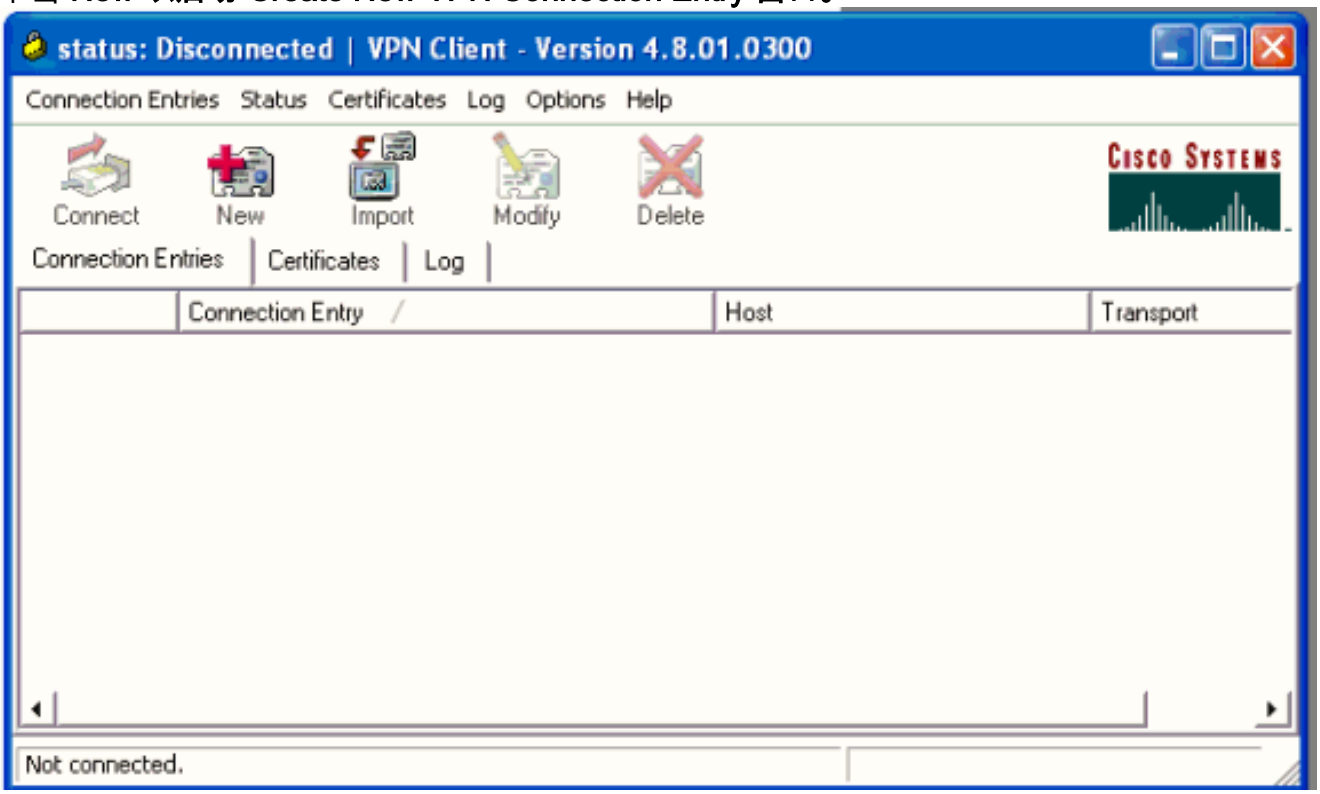
1. 创建新的VPN组IPSECGRP。
2. 创建要接收静态IP的用户并选择**IPSECGRP**。选择**Assign static IP address with the static IP address assignment，该静态IP地址在Client IP Address Assignment下分配。**


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

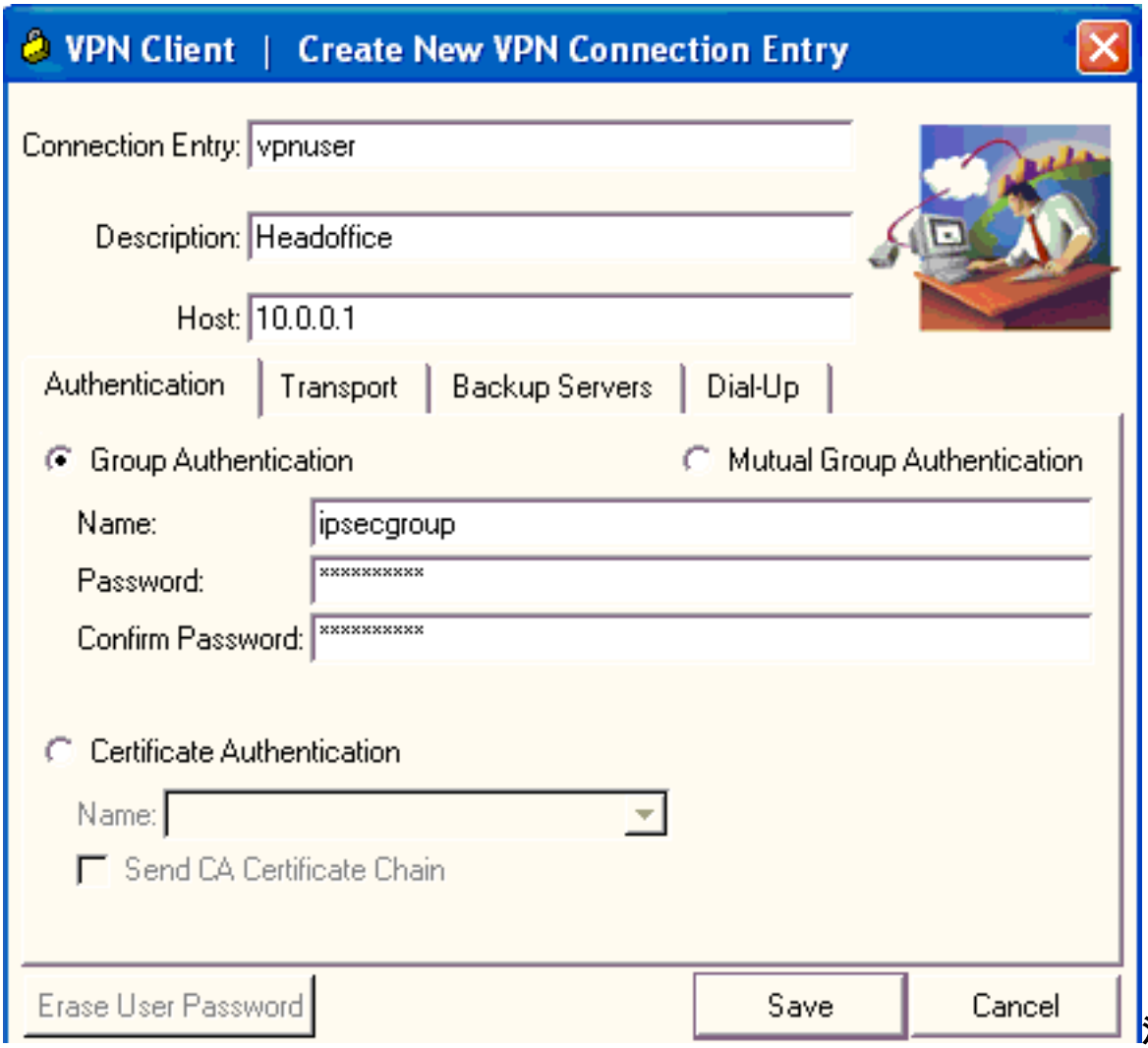
[VPN 客户端配置]

本节介绍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。在Host列中指定VPN 3000集中器公共接口IP地址，然后选择Group **Authentication**。然后提供组名和密码。单击**Save**以完成新的VPN连接条目。

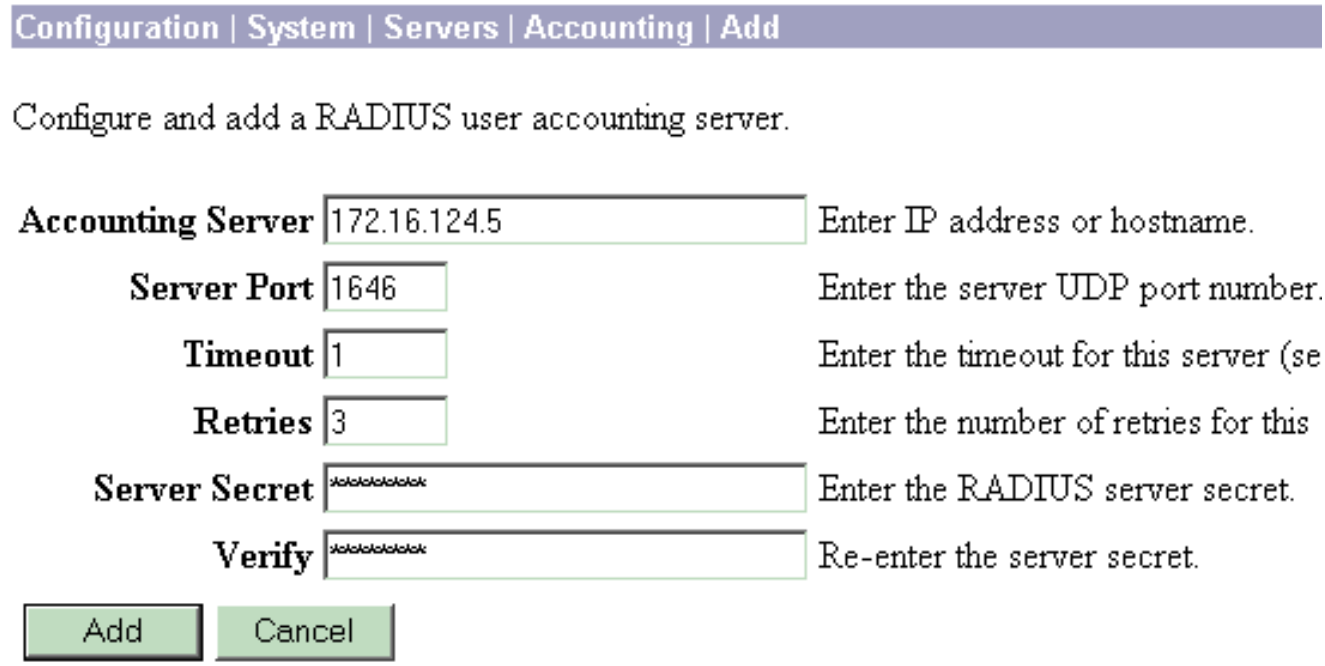


注意：确保VPN客户端已配置为使用在Cisco VPN 3000系列集中器中配置的相同组名称和密码。

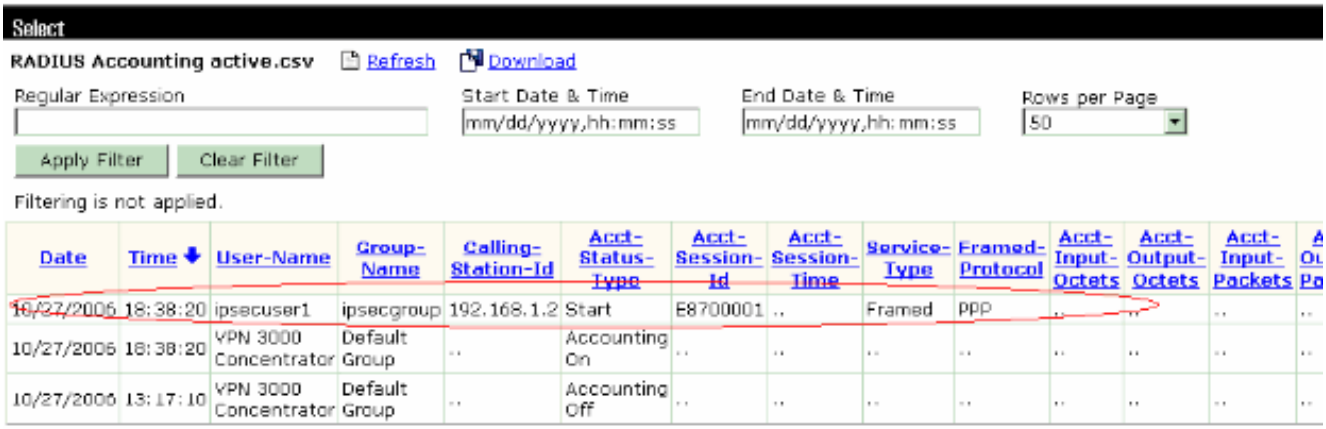
添加记帐

身份验证工作后，您可以添加记帐。

1. 在VPN 3000上，选择**Configuration > System > Servers > Accounting Servers**，然后添**加Cisco Secure ACS for Windows**服务器。
2. 选择Configuration > User Management > Groups，突出显示一个组，然后单击Modify Acct，可**以向每个组添加单个记**帐服务器。**服务器**。然后输入记帐服务器的IP地址和服务器密钥。



在用于Windows的思科安全ACS中，会显示记帐记录，如以下输出所示：



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集中器端，选择**Administration > Administer Sessions**以验证远程VPN隧道的建立。

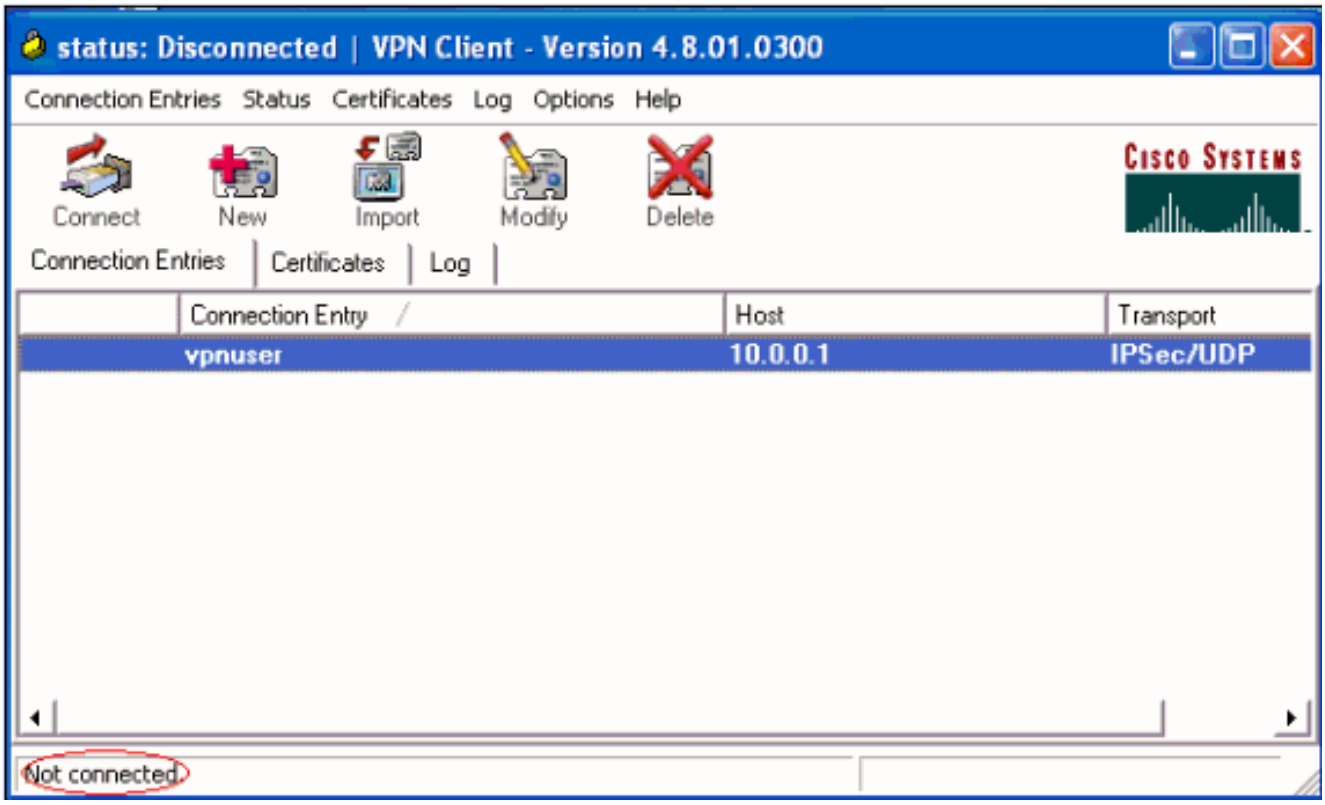
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

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]

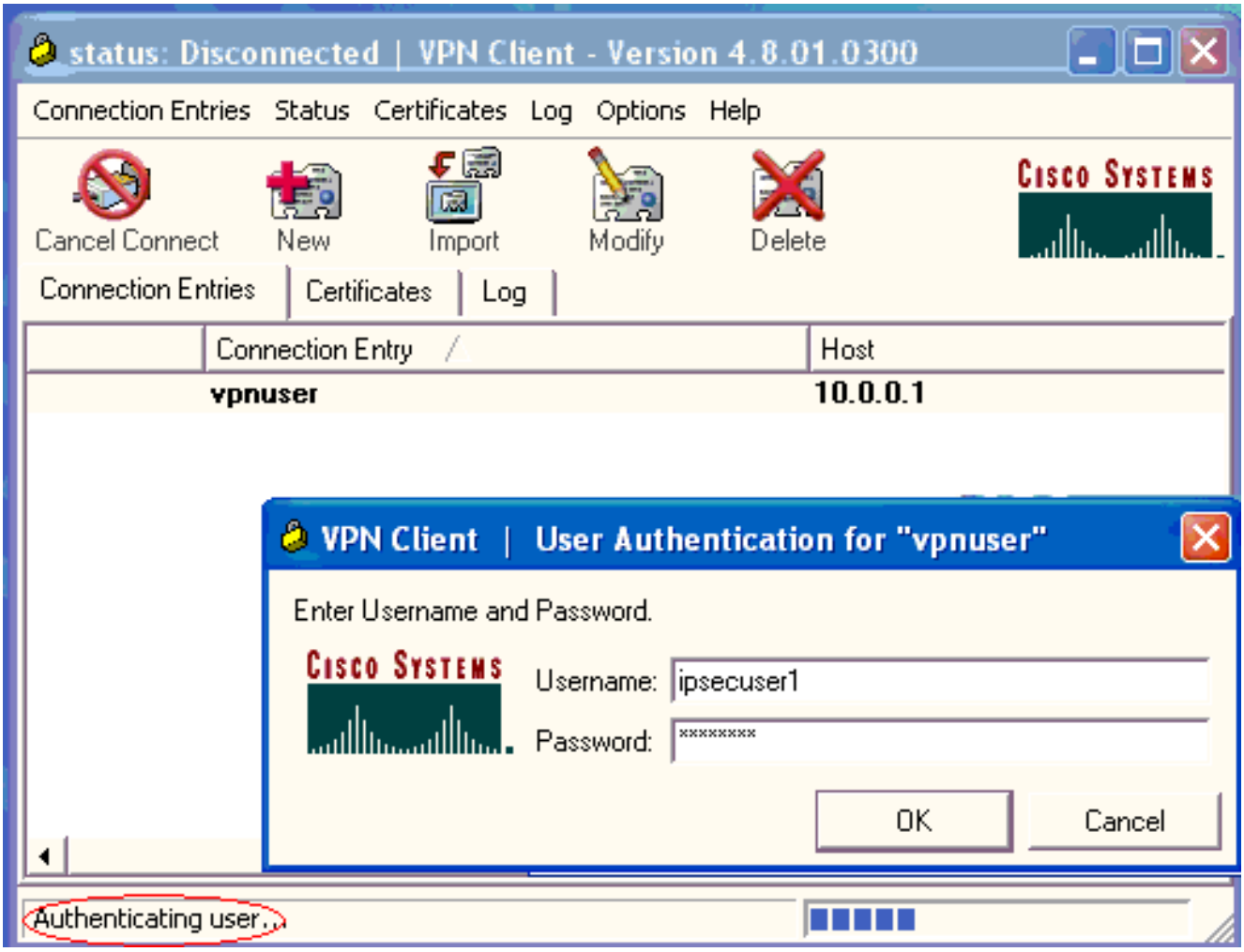
验证VPN客户端

完成以下步骤以验证 VPN 客户端。

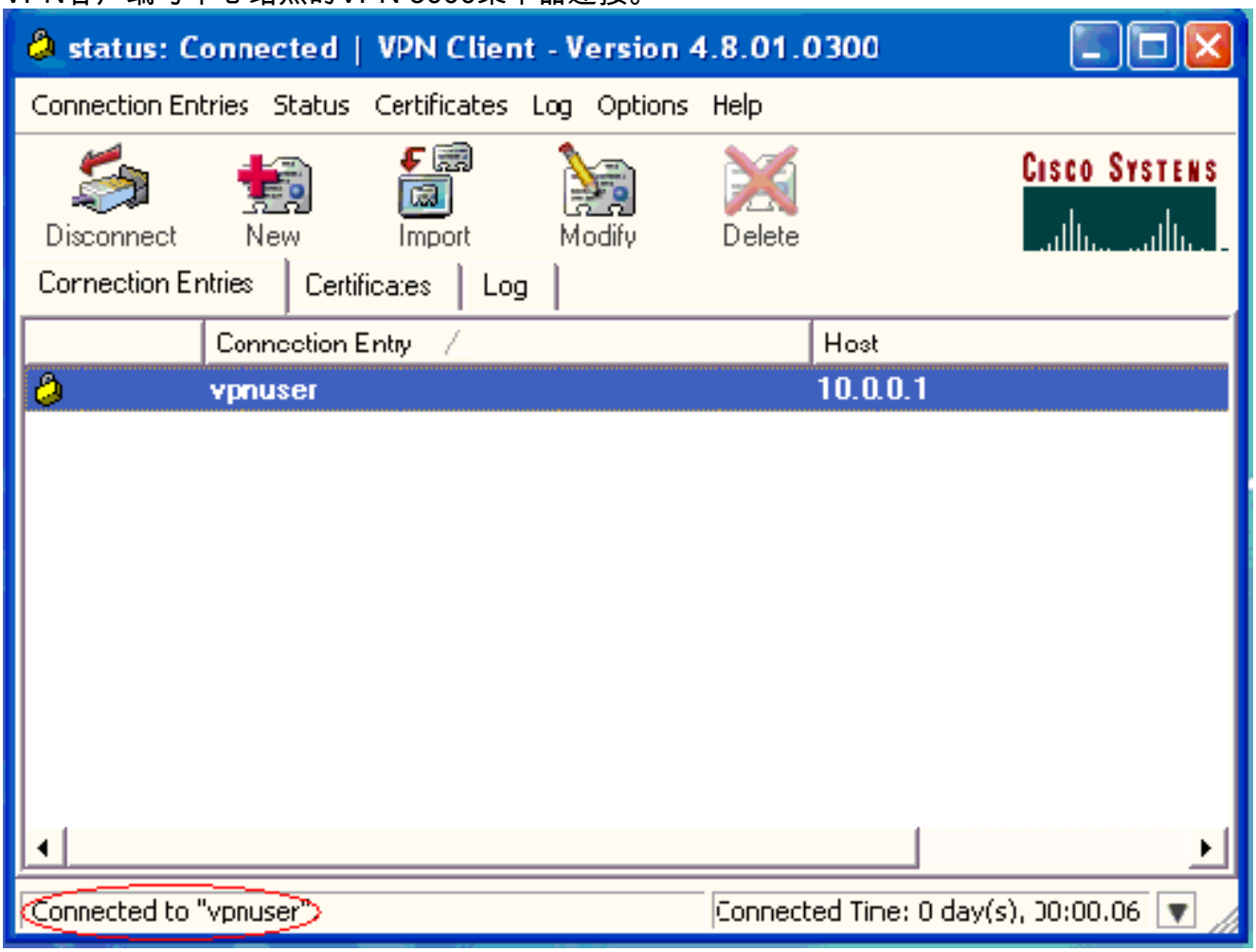
1. 单击**Connect**以启动VPN连接。



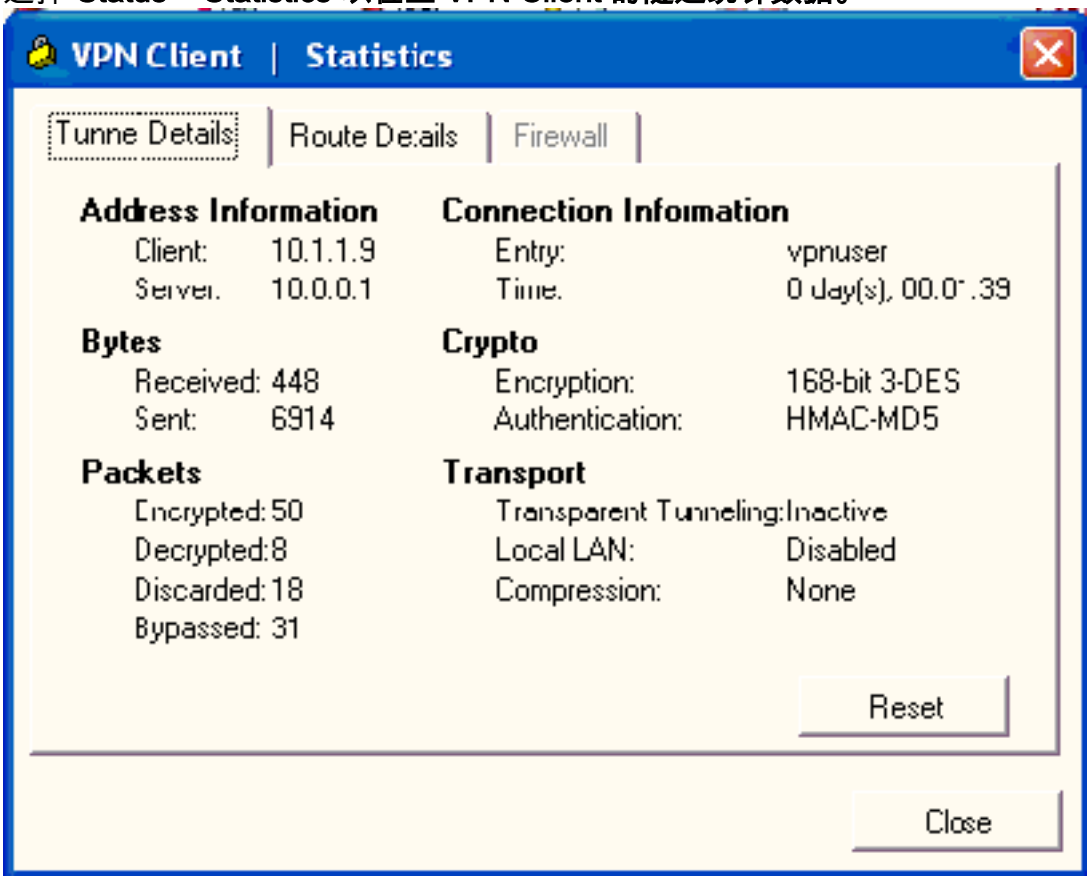
2. 此窗口显示用于用户身份验证。输入有效的用户名和密码以建立VPN连接。



3. VPN客户端与中心站点的VPN 3000集中器连接。



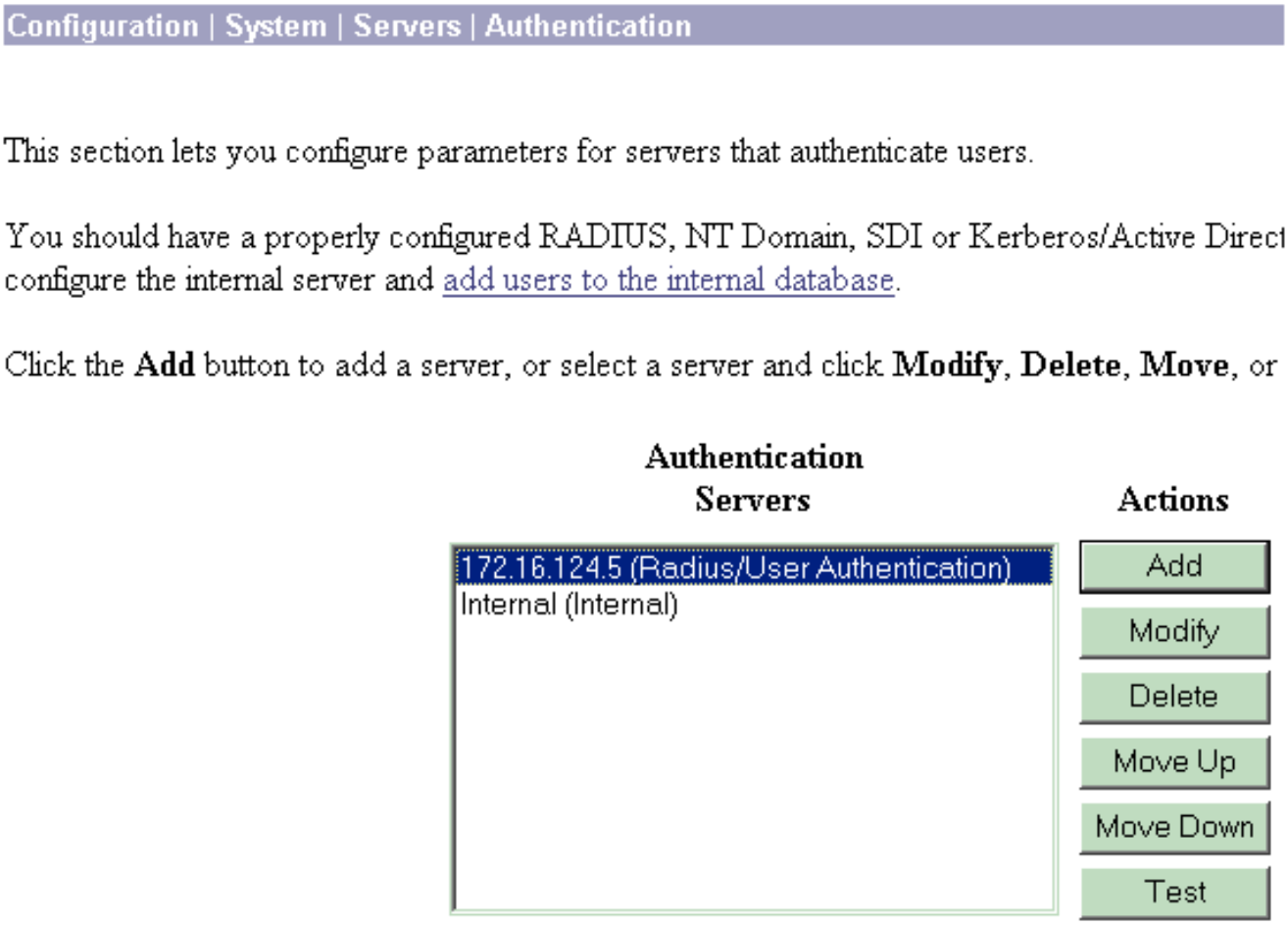
4. 选择 **Status > Statistics 以检查 VPN Client 的隧道统计数据。**



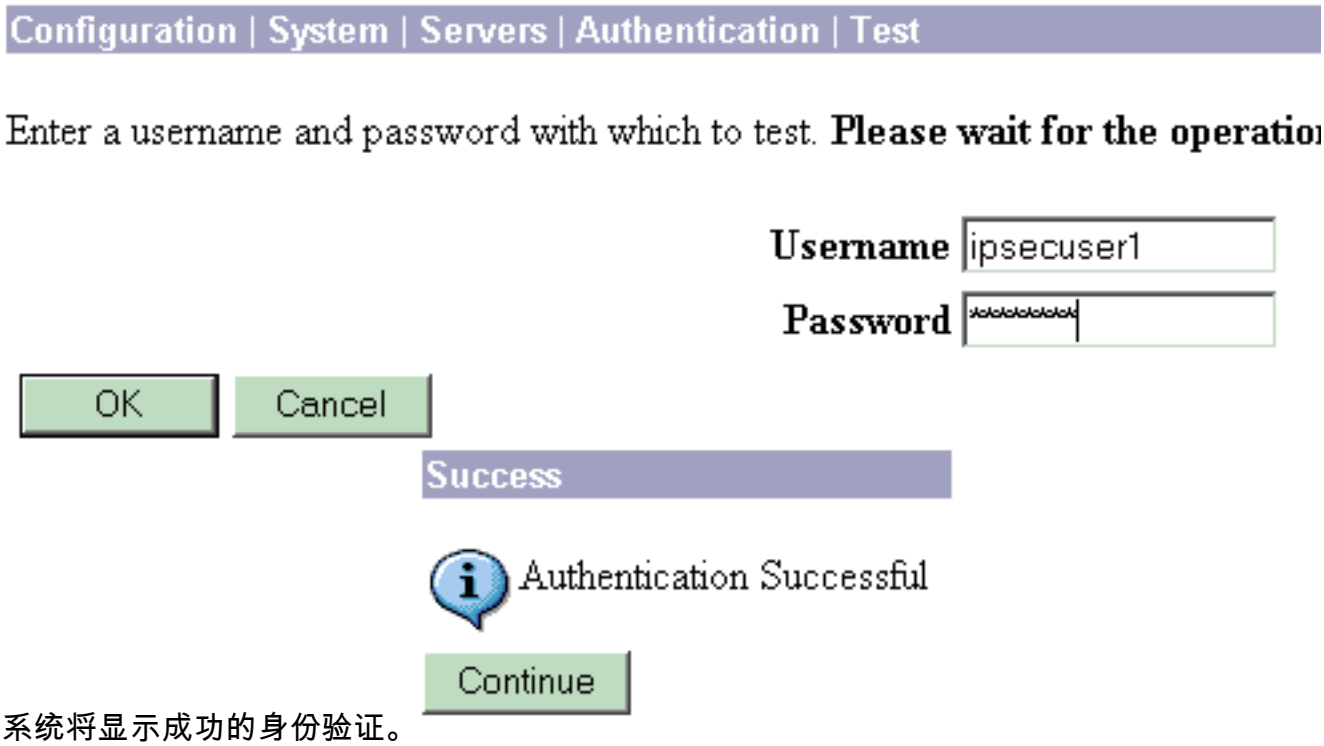
故障排除

完成以下步骤，对配置进行故障排除。

1. 选择**Configuration > System > Servers > Authentication，然后完**成以下步骤，以测试RADIUS服务器与VPN 3000集中器之间的连接。选择您的服务器，然后单击**Test**。



输入RADIUS用户名和密码，然后单击OK。

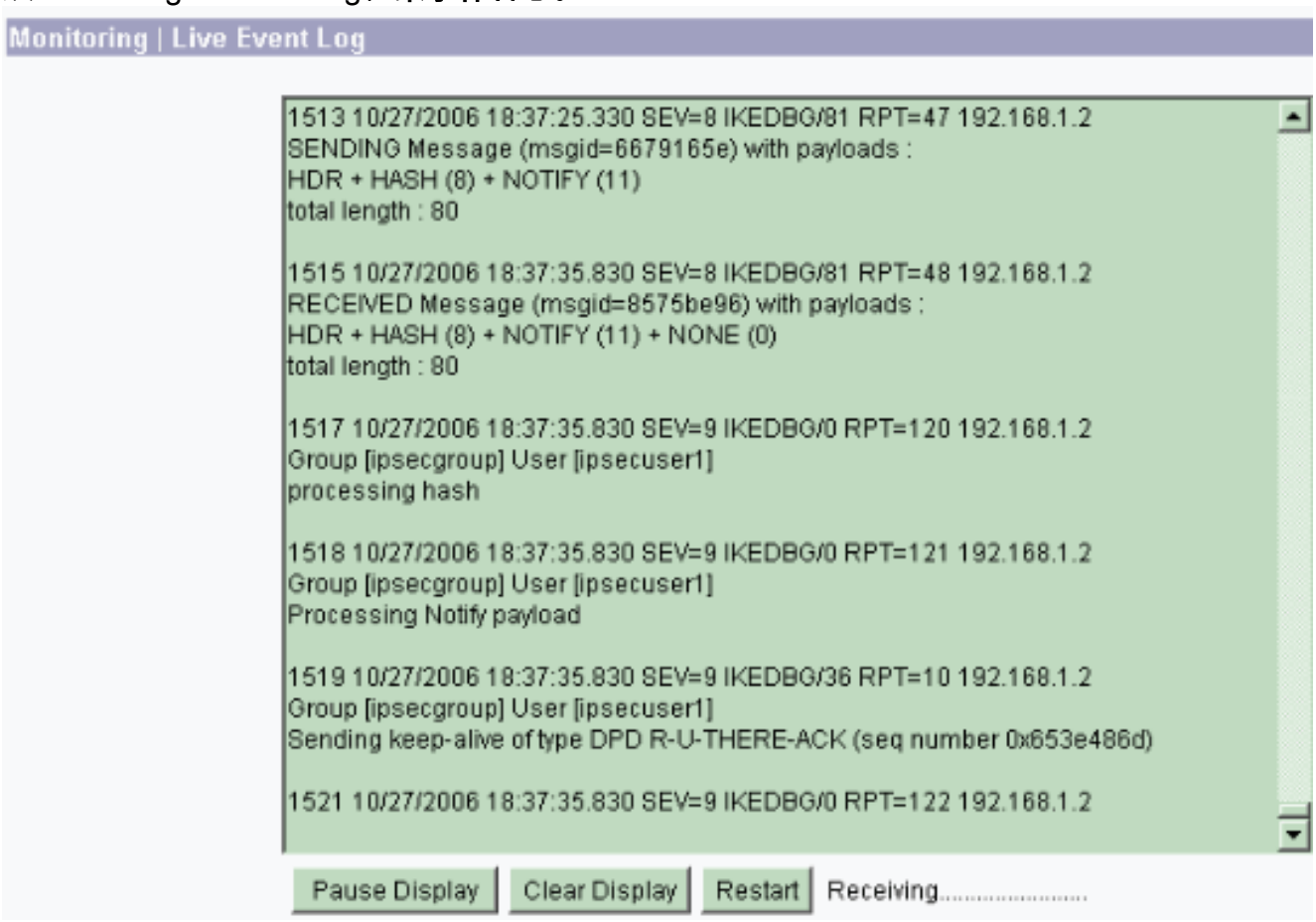


系统将显示成功的身份验证。

2. 如果发生故障，则会出现配置问题或IP连接问题。检查ACS服务器上的Failed Attempts Log（失败尝试日志），查找与故障相关的消息。如果此日志中未显示任何消息，则可能存在IP连接问题。RADIUS请求未到达RADIUS服务器。验证应用于适当VPN 3000集中器接口的过滤器是否允许RADIUS(1645)数据包进出。如果测试身份验证成功，但VPN 3000集中器的登录仍然失败，请通过控制台端口检查可过滤事件日志。如果连接不工作，可以在选择 **Configuration > System > Events > Classes > Modify(Severity to Log=1-9,Severity to**

Console=1-3)时向VPN集中器添加AUTH、IKE和IPsec事件类。AUTHDBG、AUTHDECODE、IKEDBG、IKEDECODE、IPSECDBG和IPSECDECODE也可用，但可提供太多信息。如果需要有关从RADIUS服务器向下传递的属性的详细信息，AUTHDECODE、IKEDECODE和IPSECDECODE将在严重性级别Log=1-13提供此信息。

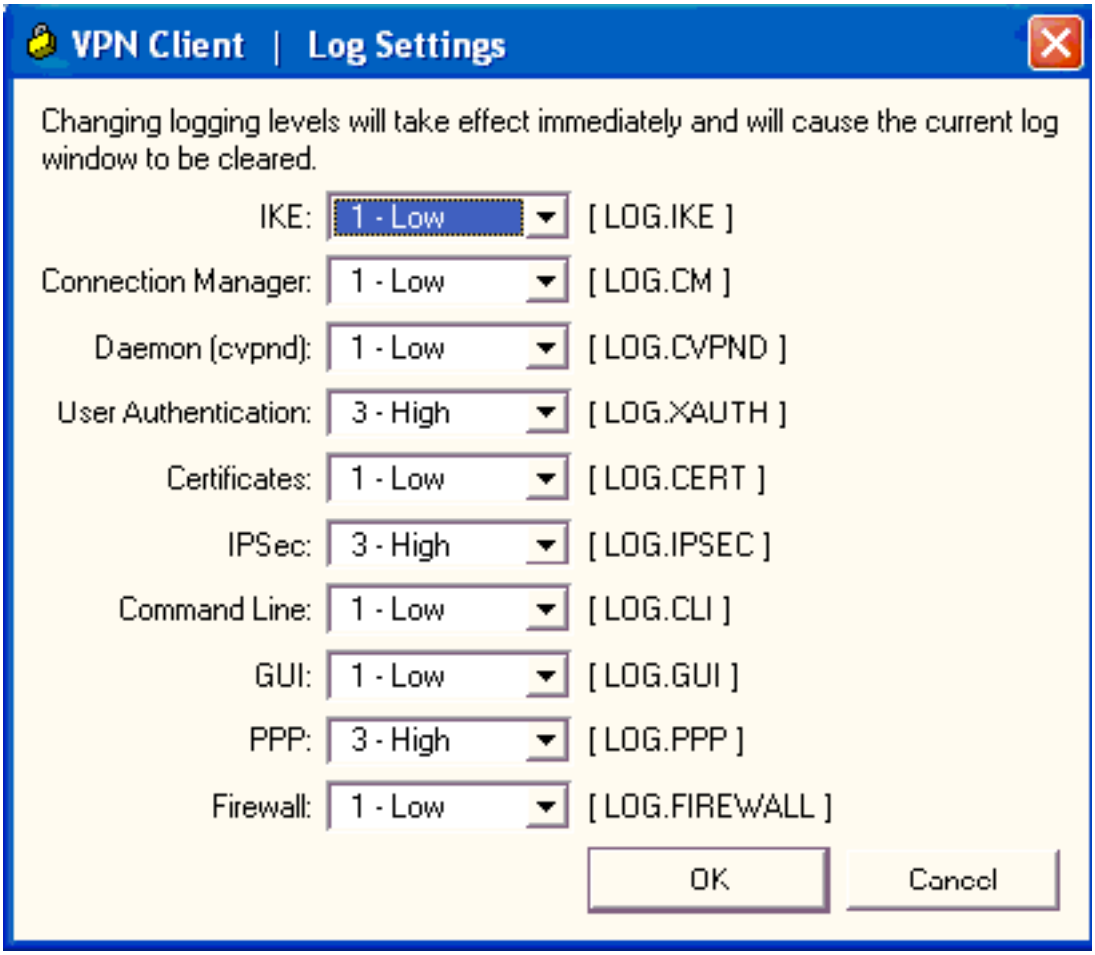
3. 从Monitoring > Event Log检**索事件日志**。



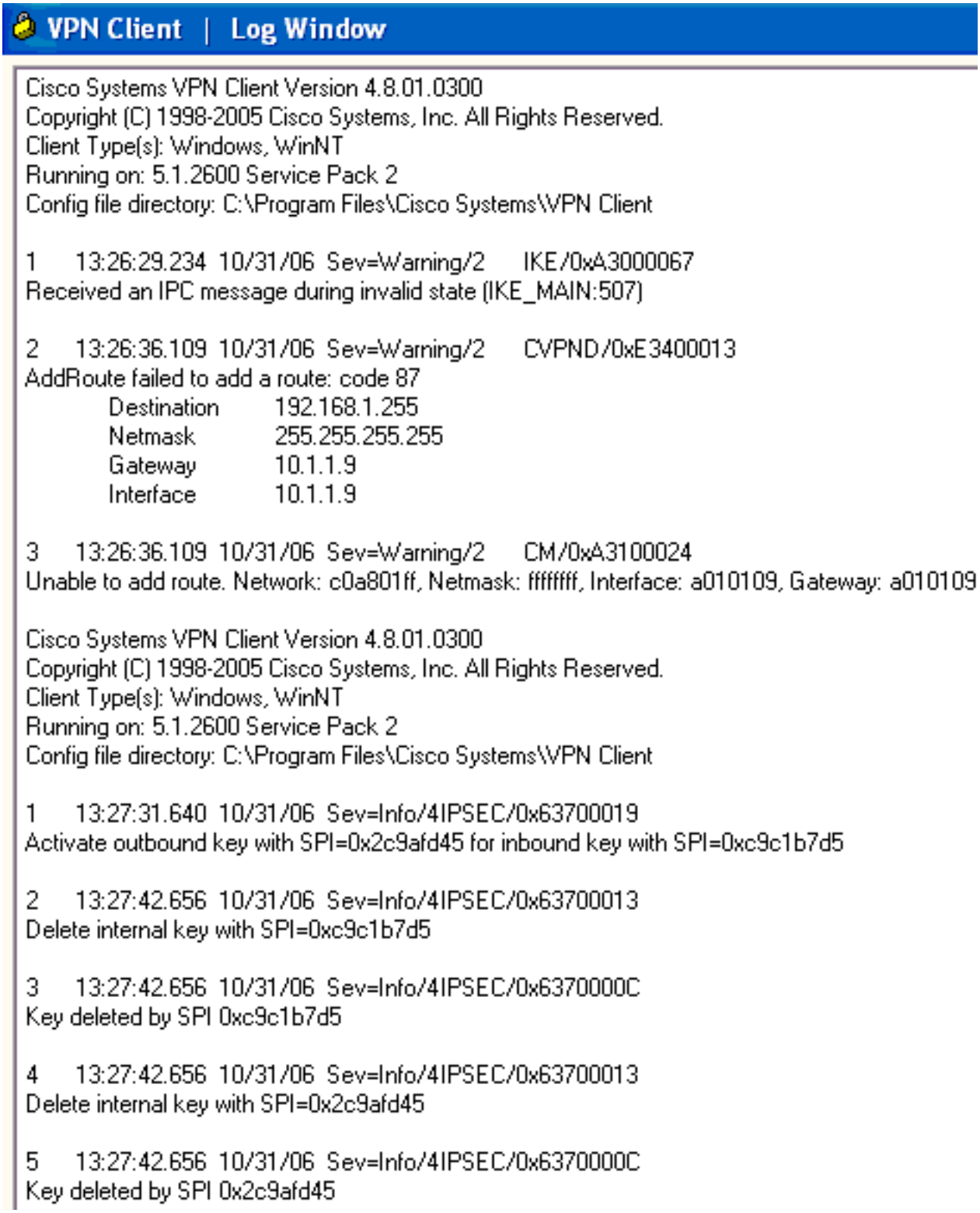
排除VPN客户端4.8 for Windows故障

完成以下步骤以排除Windows版VPN Client 4.8的故障。

1. 选择**Log > Log settings**以在VPN客户端中启用日志级别。



2. 选择**Log > Log Window**以查看VPN Client中的日志条目。



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
- 在RADIUS服务器上配置动态过滤器
- 技术支持和文档 - Cisco Systems