如何配置 VPN 3000 集中器 PPTP 以使用本地认证

目录

简介
先决条件
要求
使用的组件
网络图
规则
配置有本地认证的VPN 3000集中器
Microsoft PPTP 客户端配置
Windows 98 -配置并且配置PPTP功能
Windows 2000 - 配置 PPTP 功能
Windows NT
Windows Vista
添加MPPE (加密)
验证
验证VPN集中器
验证PC
调试
VPN 3000 调试 – 成功验证
故障排除
要解决的可能的 Microsoft 问题
相关信息

简介

Cisco VPN 3000集中器支持本地窗口客户端的点对点隧道协议(PPTP)建立隧道的方法。有在这些VPN集中器的40位和128-bit加密支持联机受保护的可靠连接的。

使用思科安全访问控制服务器(ACS)，参考配置有Cisco Secure ACS for Windows RADIUS验证的VPN 3000集中器PPTP为了配置PPTP用户的VPN集中器有扩展认证的。

先决条件

要求

保证您满足前提条件提及在，当是支持PPTP加密Cisco VPN 3000集中器？在您尝试此配置前。

使用的组件

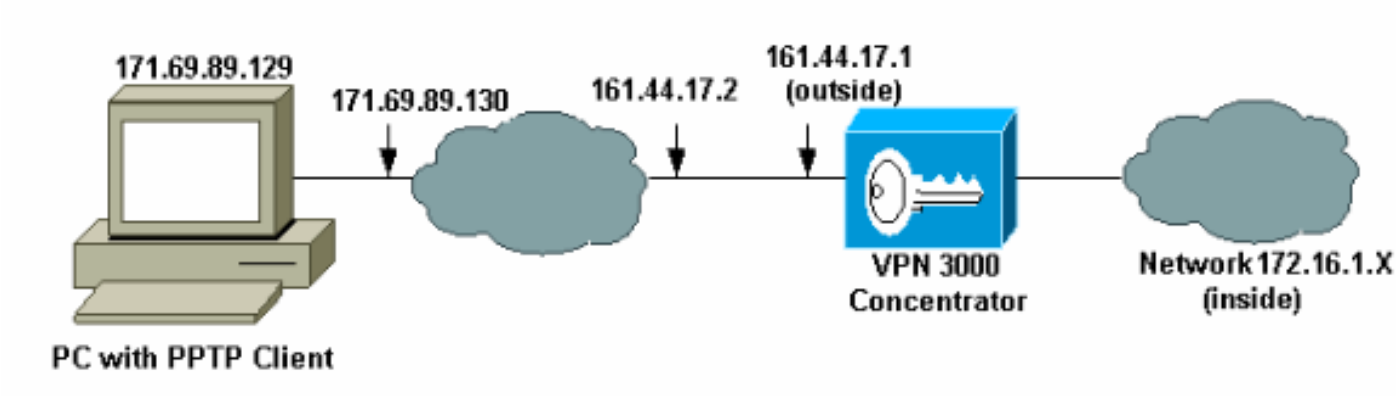
本文档中的信息基于以下软件和硬件版本：

- 有版本4.0.4.A的VPN 3015集中器
- 与PPTP客户端的Windows PC

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。

网络图

本文档使用以下网络设置：



规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置有本地认证的VPN 3000集中器

完成这些步骤配置有本地认证的VPN 3000集中器。

1. 配置在VPN集中器的各自IP地址并且保证您有连接。
2. 保证**PAP认证**在**Configuration > User Management > Base Group** PPTP/L2TP选项卡选择。

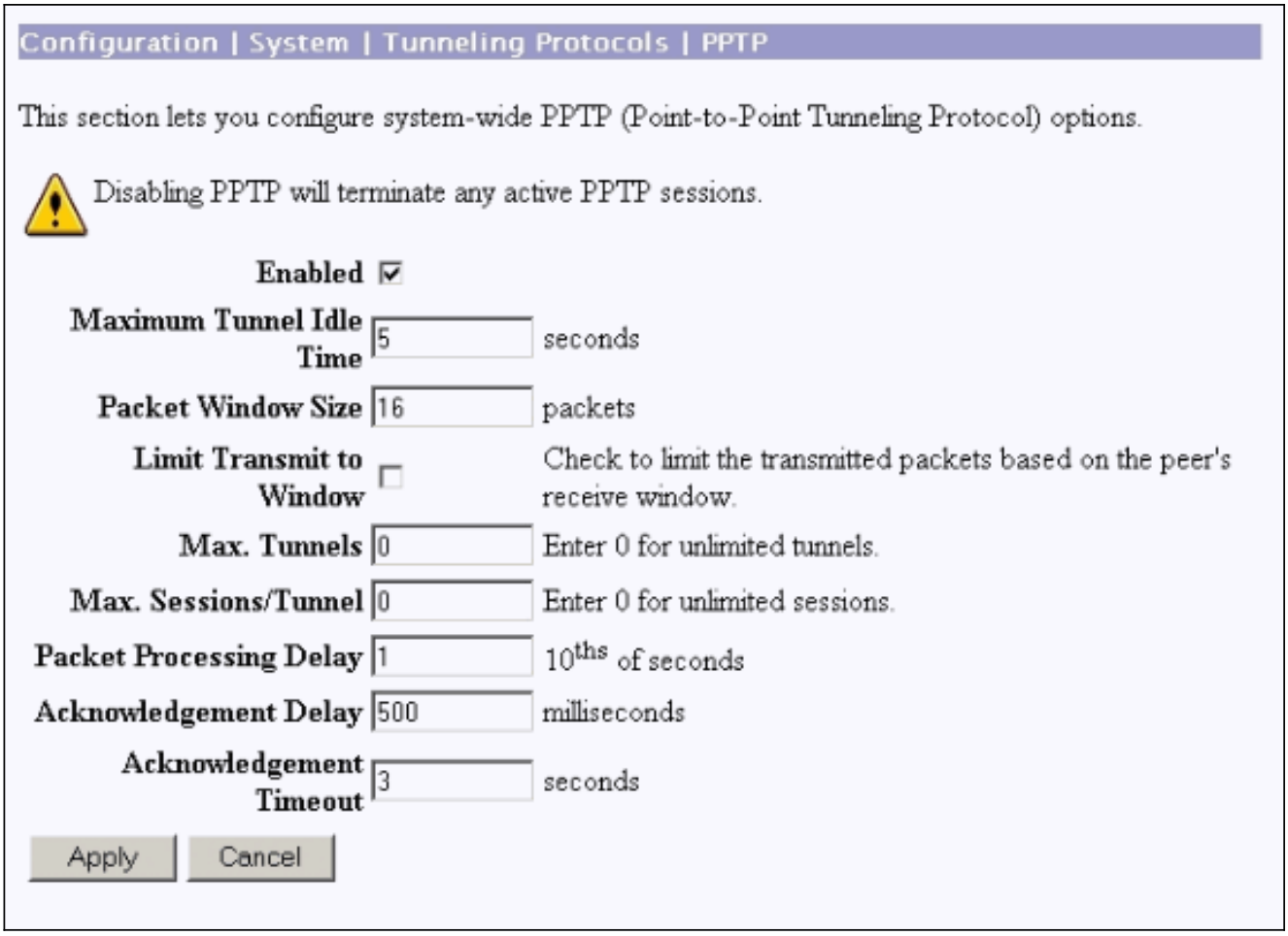
Configuration | User Management | Base Group

General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

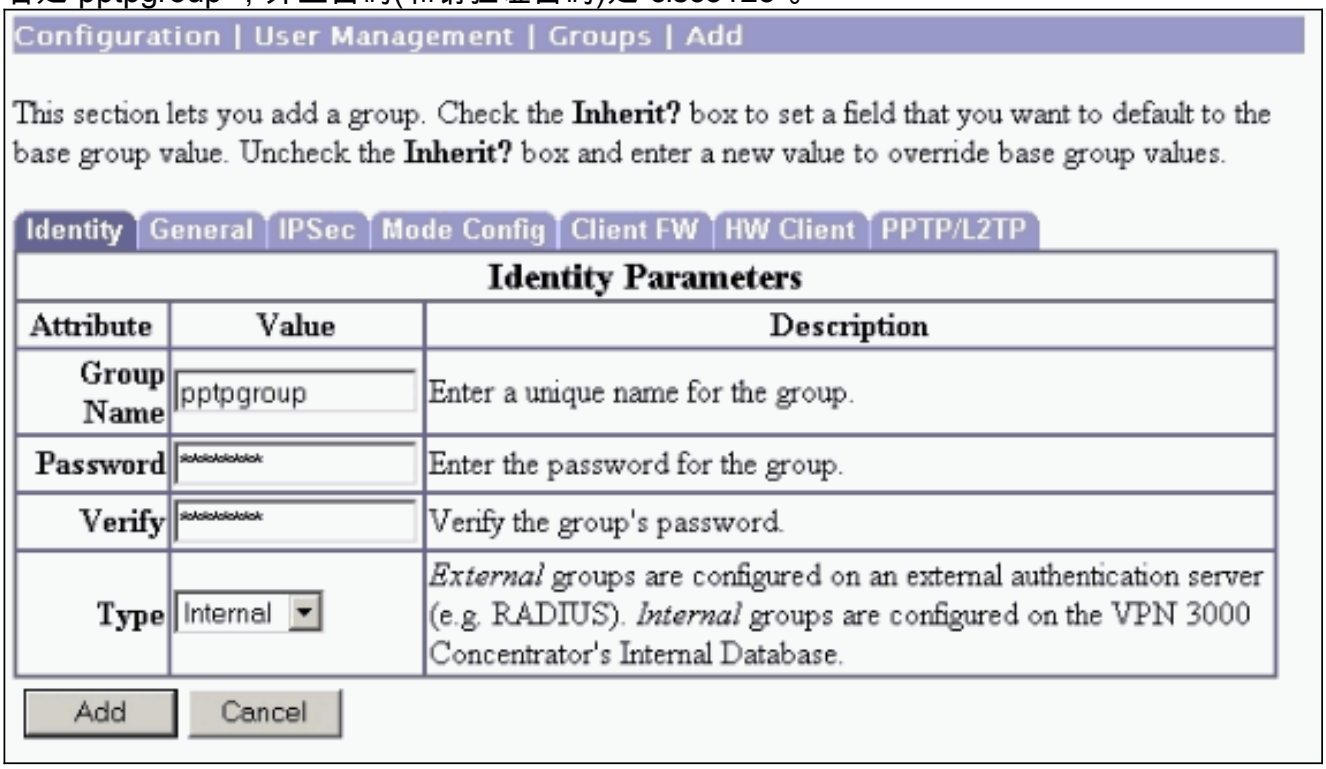
PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	☐	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* authentication is required.**
PPTP Encryption	☐ Required ☐ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	Check to enable MPPC compression for PPTP connections for this group.

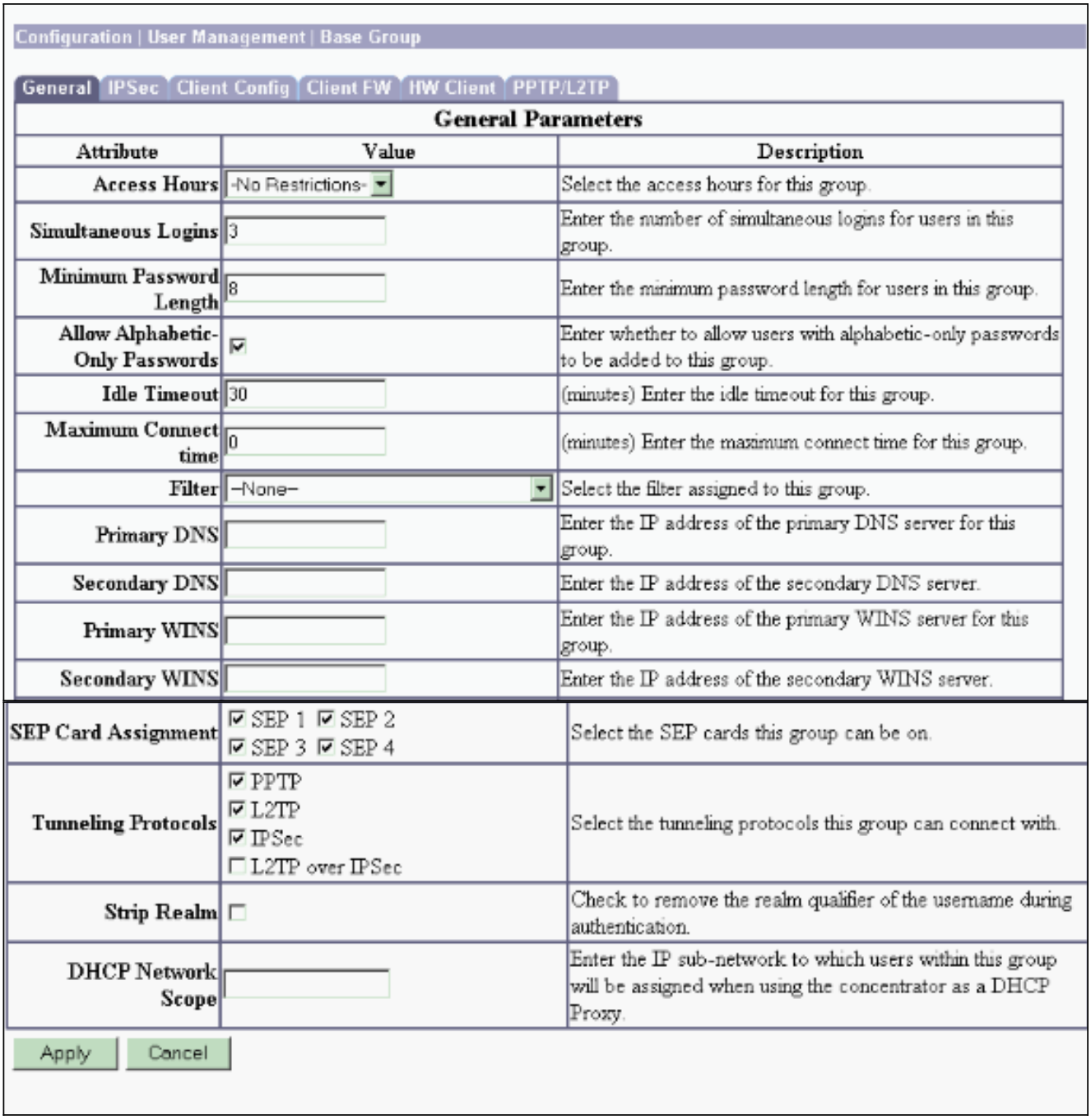
3. 选择**启用**被检查的**Configuration > System > Tunneling Protocols > PPTP**并且保证。



4. 选择**Configuration > User Management > Groups > Add**，并且配置PPTP组。在本例中，组名是“pptpgroup”，并且密码(和请验证密码)是"cisco123"。



5. 在组的常规选项卡下，请确定**PPTP**选项在身份验证协议启用。



Configuration | User Management | Base Group

General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters

Attribute	Value	Description
Access Hours	-No Restrictions-	Select the access hours for this group.
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	8	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	-None-	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	☑ PPTP ☑ L2TP ☑ IPSec ☐ L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm	☐	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply | Cancel

6. 在PPTP/L2TP选项卡下，请启用**PAP认证**，并且禁用**加密**(加密可以在任何时间在将来启用)。

Configuration | User Management | Groups | Modify pptpgroup

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

PPTP/L2TP Parameters

Attribute	Value	Inherit?	Description
Use Client Address	☐	☑	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	☑	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* authentication is required.**
PPTP Encryption	☐ Required ☐ Require Stateless ☐ 40-bit ☐ 128-bit	☐	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	☑	Check to enable compression for PPTP connections for this group.

7. 选择**Configuration > User Management > Users > Add**，并且配置一个本地用户(呼叫“pptpuser”)有PPTP验证的password Cisco123的。放置用户在以前定义“pptpgroup”：

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

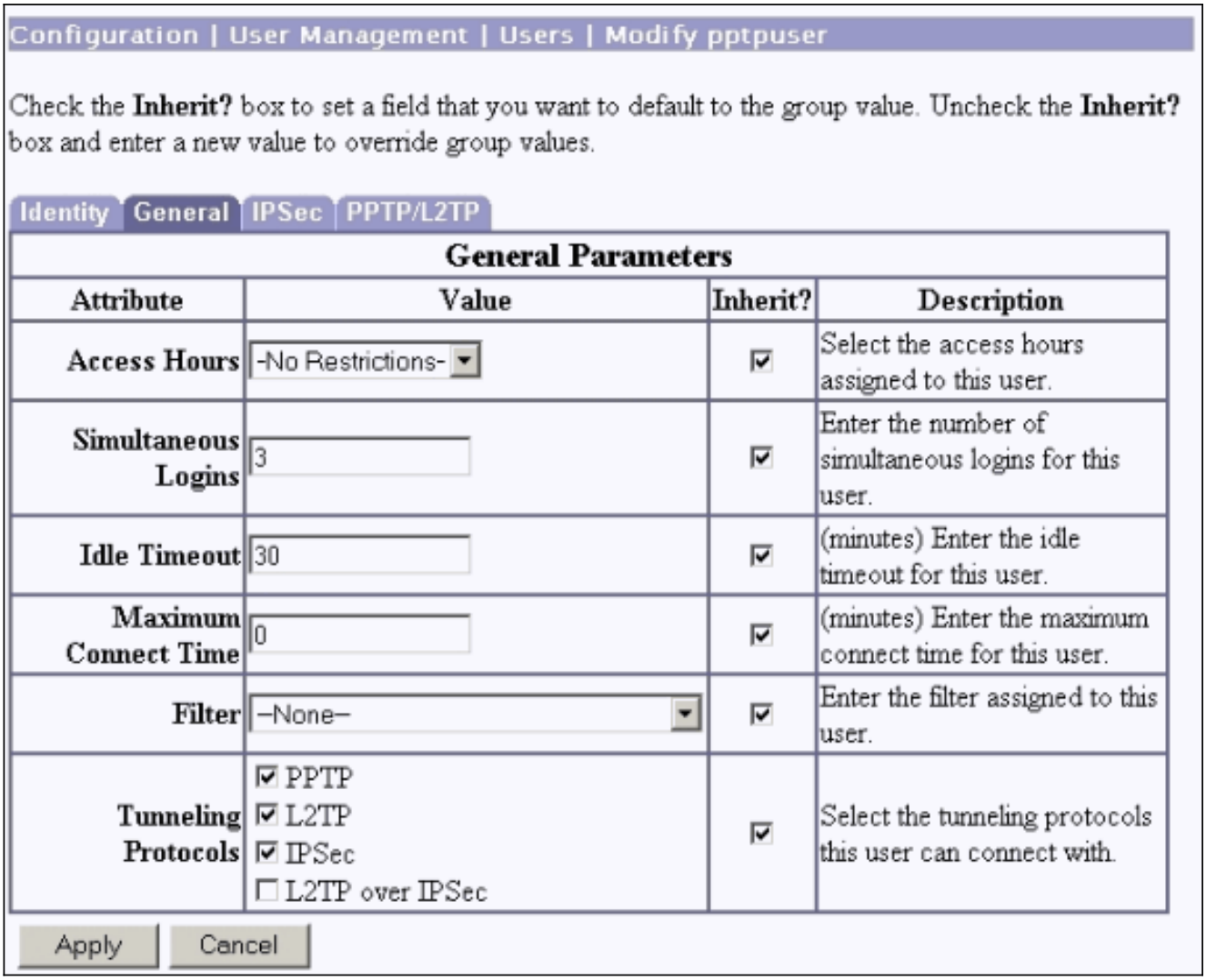
Identity | General | IPSec | PPTP/L2TP

Identity Parameters

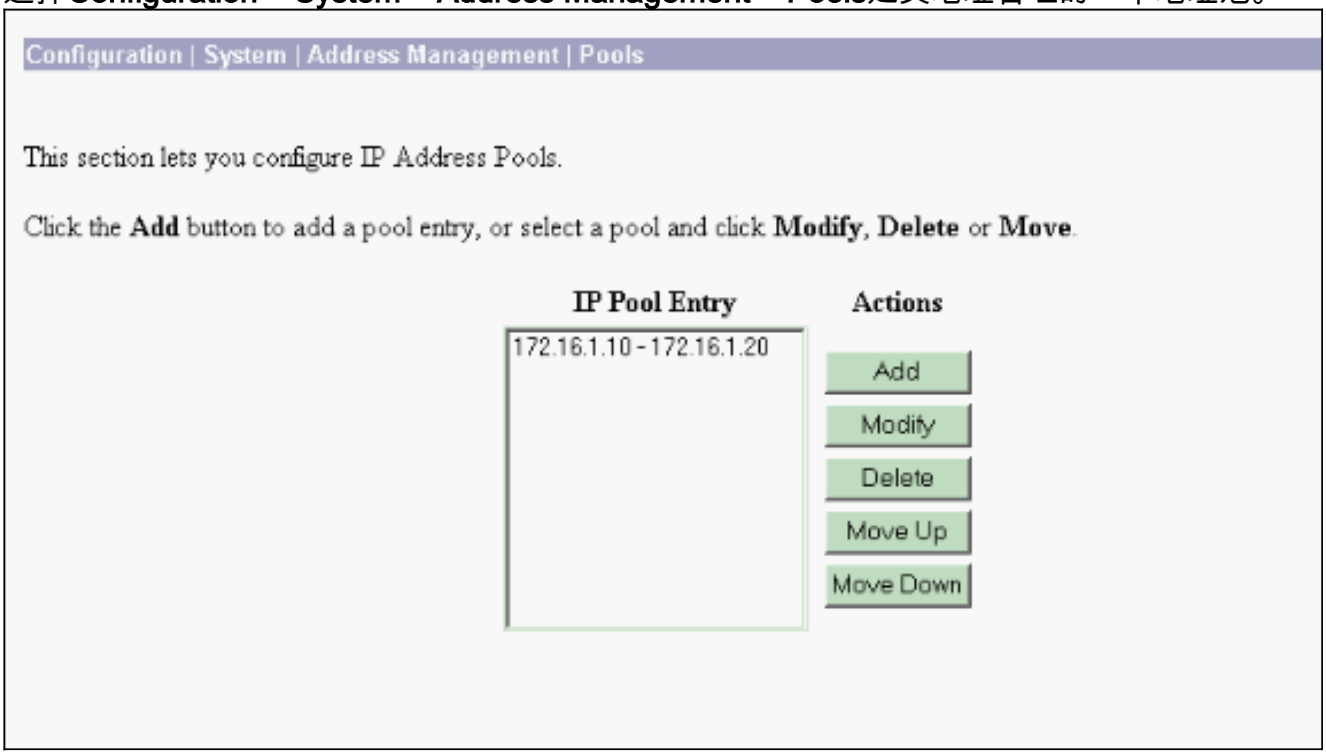
Attribute	Value	Description
User Name	pptpuser	Enter a unique user name.
Password	•••••••••••	Enter the user's password. The password must satisfy the group password requirements.
Verify	•••••••••••	Verify the user's password.
Group	pptpgroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add | Cancel

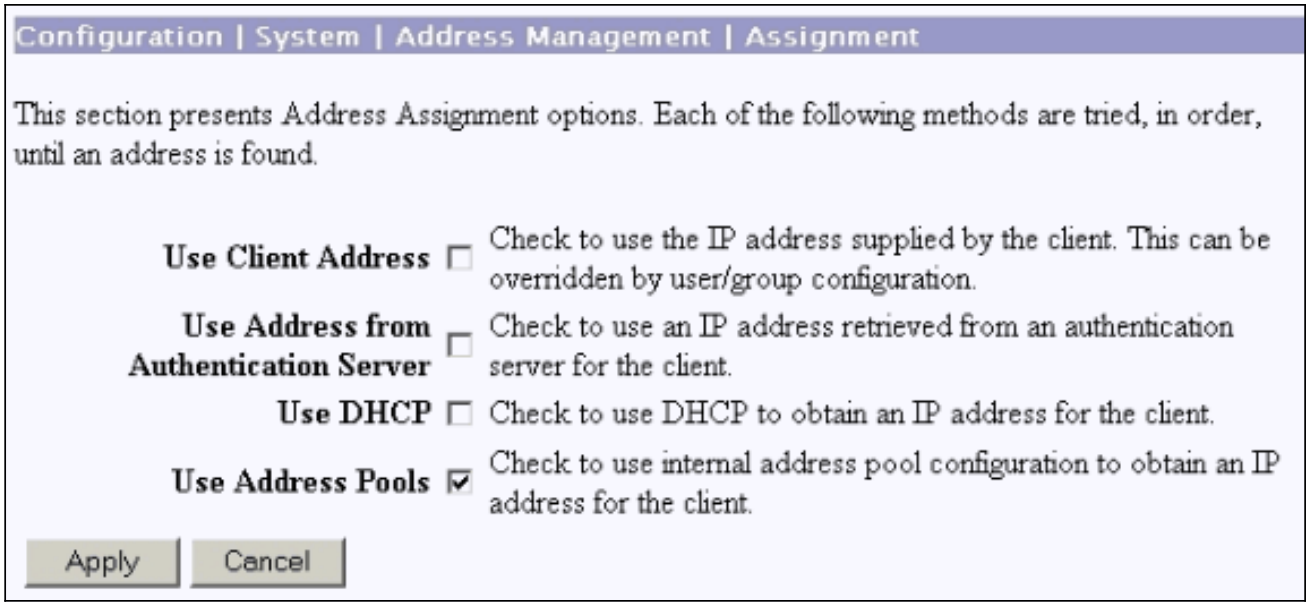
8. 在用户的常规选项卡下，请确保**PPTP**选项在隧道协议启用。



9. 选择Configuration > System > Address Management > Pools定义地址管理的一个地址池。



10. 选择Configuration > System > Address Management > Assignment并且处理VPN集中器使用地址池。



Microsoft PPTP 客户端配置

注意： 有用的资料都此处在配置Microsoft软件不附有任何质保或支持Microsoft软件的。Microsoft软件的支持从Microsoft是可得到 。

Windows 98 -配置并且配置PPTP功能

安装

完成这些步骤配置PPTP功能。

1. 选择**Start > Settings > Control Panel > Add New Hardware (下) >从列表>网络适配器挑选(其次)**。
2. 选择在左面板和**Microsoft VPN适配器的Microsoft**在右侧面板。

配置

完成这些步骤配置PPTP功能。

1. 选择**Start > Programs > Accessories > Communications > Dial Up Networking > Make New Connection**。
2. 连接使用Microsoft VPN适配器在精选设备提示符。VPN服务器IP是3000隧道终点。

Windows 98默认验证使用密码加密(例如， CHAP或MSCHAP)。为了禁用此加密，选择**Properties > Server types**和最初不选定**加密密码**和**要求数据加密**方框。

Windows 2000 - 配置 PPTP 功能

完成这些步骤配置PPTP功能。

1. 选择**Start > Programs > Accessories > Communications > Network及Dialup connections > Make New Connection**。
2. 单击**其次**，并且选择**连接对私有网络通过互联网>拨号连接优先**(请勿选择此，如果使用LAN)。

3. 单击**其次**再，并且输入隧道终点的主机名或IP，是VPN 3000集中器的外部接口。在本例中IP地址是161.44.17.1。

选择**Properties > Security for the connection > Advanced**添加密码类型作为PAP。默认是MSCHAP和MSCHAPv2、不是CHAP或者PAP。

数据加密是可配置在此区域。您能最初禁用它。

Windows NT

您在Microsoft的网站能关于安装Windows NT客户端的访问信息PPTP的 。

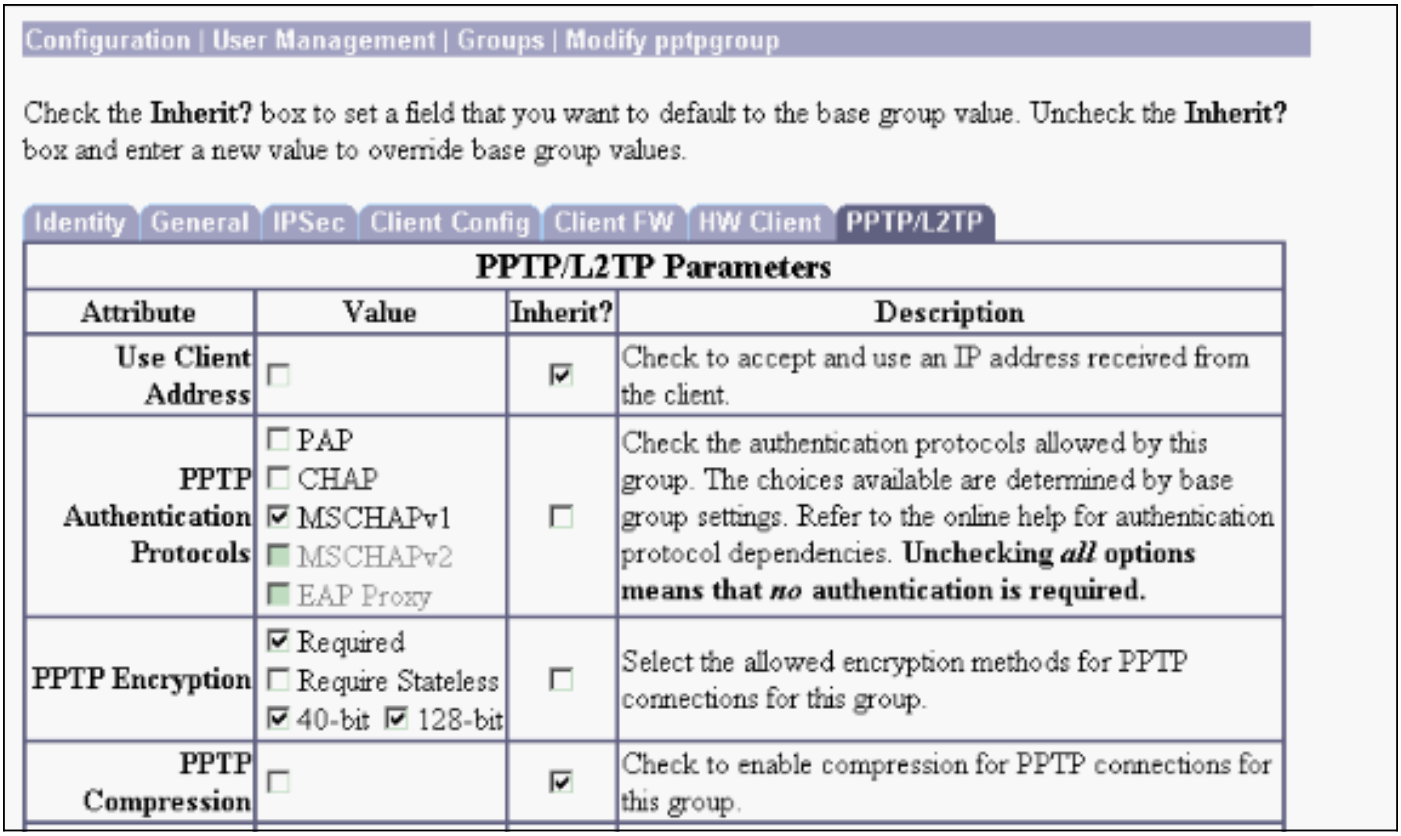
Windows Vista

完成这些步骤配置PPTP功能。

1. 从一开始按钮，选择**连接**。
2. 选择**建立连接或网络**。
3. 选择**连接到工作场所**并且**其次**单击。
4. 选择**使用我的互联网连接(VPN)**。**注意：** 如果提示输入“您要使用您已经有的连接”，选择**没有，创建新连接**并且**其次**单击。
5. 例如在**互联网地址**字段，类型**pptp.vpn.univ.edu**。
6. 例如在**目的地Name字段**，类型**UNIVVPN**。
7. 在**用户名字段**，请键入您的UNIV登录ID。您的UNIV登录ID是您的电子邮件地址的部分在**@univ.edu前。**
8. 在**密码字段**，请键入您的UNIV登录ID密码。
9. 点击**创建按钮**然后单击**关闭按钮**。
10. 为了连接到VPN服务器，在您创建VPN连接后，请点击开始，然后**连接**。
11. 选择在窗口的VPN连接并且点击**连接**。

添加MPPE (加密)

确保PPTP连接工作，不用加密，在您添加加密前。例如，请点击**Connect按钮**在PPTP客户端确保，连接完成。如果决定需要加密，必须使用MSCHAP验证。在VPN3000，请选择**Configuration > User Management > Groups**。然后，在组的PPTP/L2TP选项卡下，请不选定**PAP**，检查**MSCHAPv1**，并且检查**需要的PPTP加密**。



(如果它是选项)，PPTP客户端应该为可选或所需的数据加密和MSCHAPv1被重新配置。

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

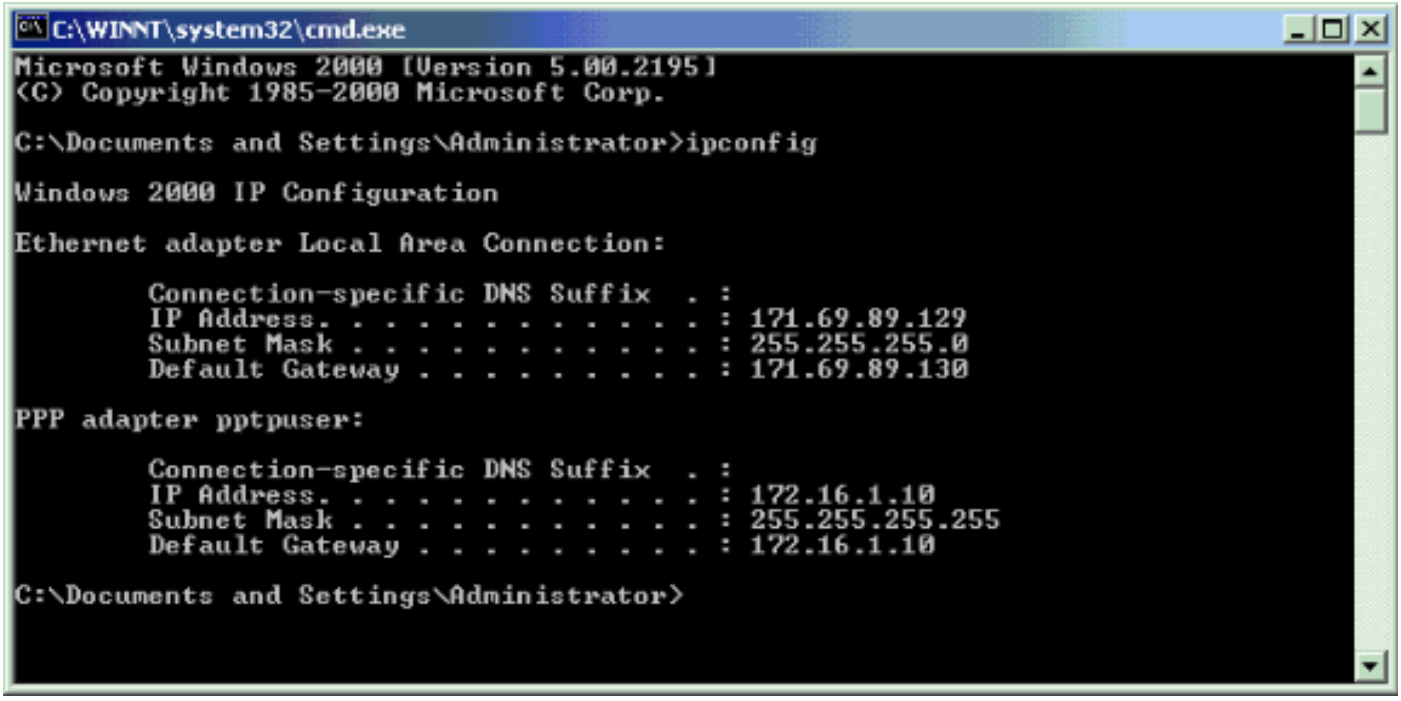
验证VPN集中器

您能通过拨号PPTP客户端在Microsoft PPTP客户端配置部分创建前的表启动PPTP会话。

请使用在VPN集中器的管理>Administer会话窗口查看参数和统计信息所有激活PPTP会话的。

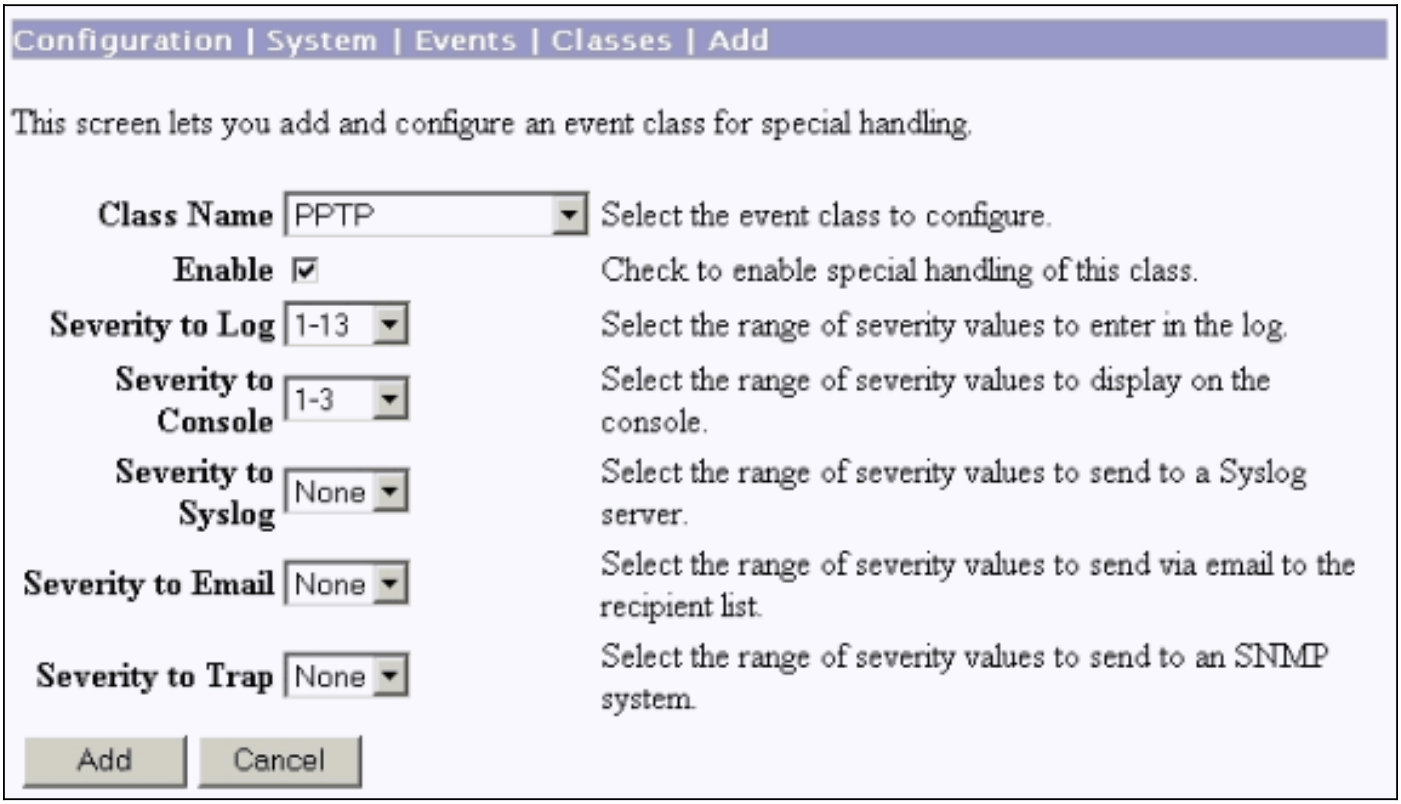
验证PC

发出**ipconfig命令**在PC的命令模式发现PC有两个IP地址。一个是其自己的IP地址，并且其他由从IP地址的池的VPN集中器分配。在本例中IP地址172.16.1.10是VPN集中器分配的IP地址。

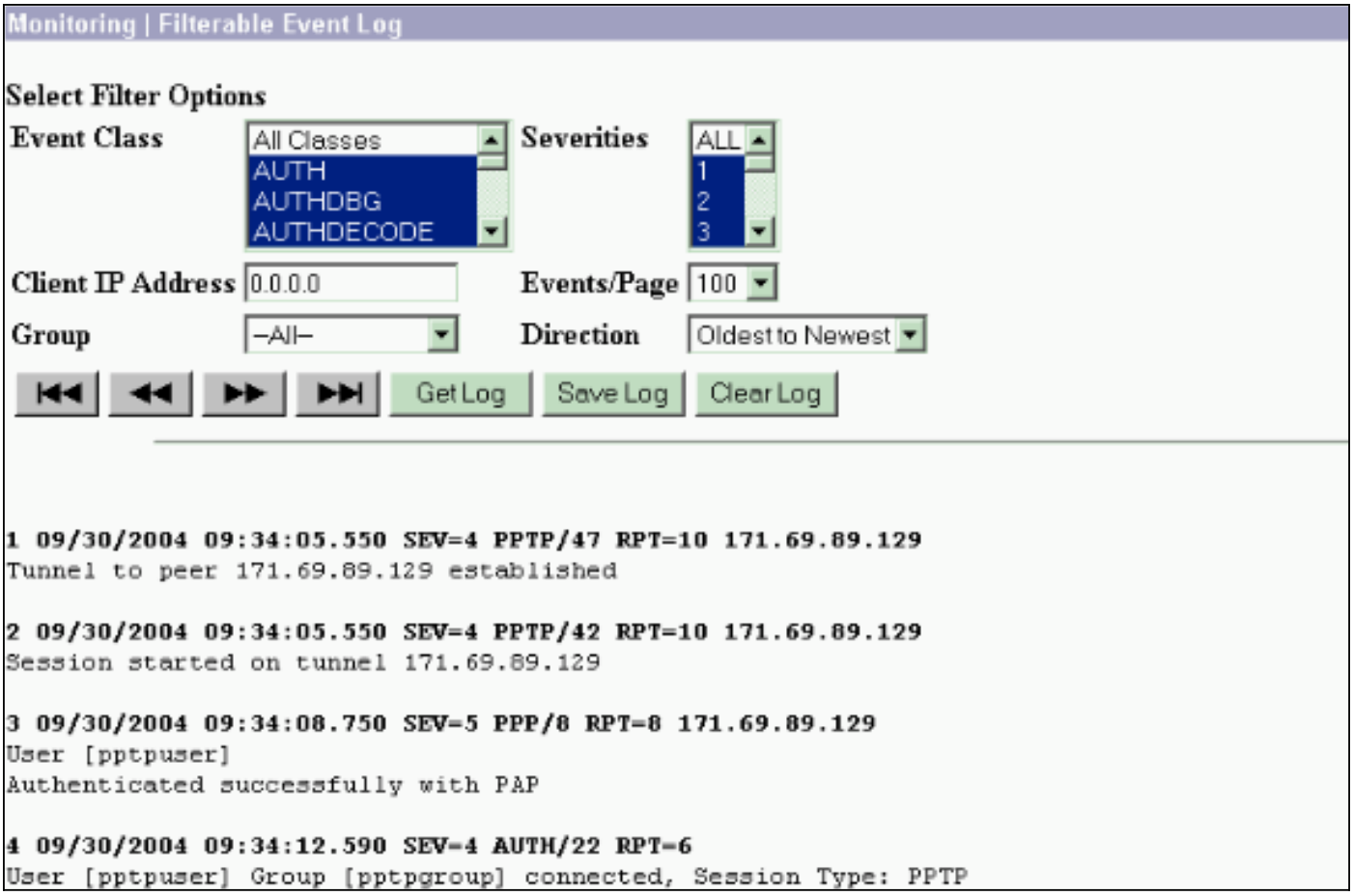


调试

如果连接不工作，PPTP事件类调试可以被添加到VPN集中器。选择**Configuration > System > Events > Classes > Modify**或**添加**(显示此处)。PPTPDBG和PPTPDECODE事件类也是可用的，但是也许提供许多信息。



事件日志可以从**Monitoring > Filterable Event Log**被检索。



VPN 3000 调试 – 成功验证

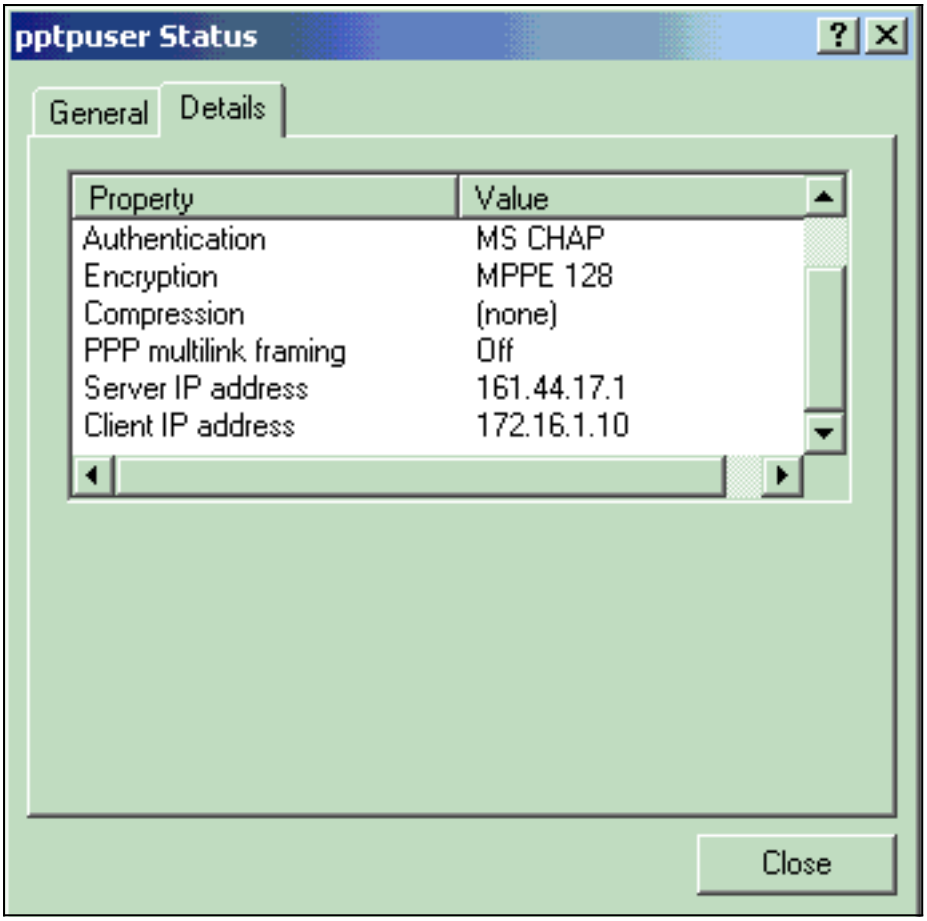
```
1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129
   Tunnel to peer 171.69.89.129 established

2 09/28/2004 21:36:52.800 SEV=4 PPTP/42 RPT=29 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 21:36:55.910 SEV=5 PPP/8 RPT=22 171.69.89.129
   User [pptpuser]
   Authenticated successfully with MSCHAP-V1

4 09/28/2004 21:36:59.840 SEV=4 AUTH/22 RPT=22
   User [pptpuser] Group [Base Group] connected, Session Type: PPTP
```

点击**Details**窗口PPTP用户的状态检查在Windows PC的参数。



故障排除

这些是您能遇到的可能的错误：

- **用户名不正确或密码**VPN 3000集中器debug输出：

```
1 09/28/2004 22:08:23.210 SEV=4 PPTP/47 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 established

2 09/28/2004 22:08:23.220 SEV=4 PPTP/42 RPT=44 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 22:08:26.330 SEV=3 AUTH/5 RPT=11 171.69.89.129
   Authentication rejected: Reason = User was not found
   handle = 44, server = (none), user = pptpusers, domain = <not specified>

5 09/28/2004 22:08:26.330 SEV=5 PPP/9 RPT=11 171.69.89.129
   User [pptpusers]
   disconnected.. failed authentication ( MSCHAP-V1 )

6 09/28/2004 22:08:26.340 SEV=4 PPTP/35 RPT=44 171.69.89.129
   Session closed on tunnel 171.69.89.129 (peer 32768, local 22712, serial 40761),
   reason: Error (No additional info)

8 09/28/2004 22:08:26.450 SEV=4 PPTP/34 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 closed, reason: None (No additional info)
```

用户看到的消息(从Windows 98) ：

```
Error 691: The computer you have dialed in to has denied access
because the username and/or password is invalid on the domain.
```

用户看到的消息(从Windows 2000) ：

```
Error 691: Access was denied because the username and/or
password was invalid on the domain.
```

- **“要求的加密”选择在PC，但是不在VPN集中器**用户看到的消息(从Windows 98) ：
  ```
  Error 742: The computer you're dialing in to does not support the data
  encryption requirements specified.
  Please check your encryption settings in the properties of the connection.
  If the problem persists, contact your network administrator.
  ```
  用户看到的消息(从Windows 2000) ：
  ```
  Error 742: The remote computer does not support
  the required data encryption type
  ```
- **“要求的加密” (128-bit)在VPN集中器选择用PC仅该支持40位加密**VPN 3000集中器debug输出：
  ```
  4 12/05/2000 10:02:15.400 SEV=4 PPP/6 RPT=7 171.69.89.129 User [ pptpuser ] disconnected.
  PPTP Encryption configured as REQUIRED.. remote client not supporting it.
  ```
  用户看到的消息(从Windows 98) ：
  ```
  Error 742:  The remote computer does not support
  the required data encryption type.
  ```
  用户看到的消息(从Windows 2000) ：
  ```
  Error 645 Dial-Up Networking could not complete the connection to the server.
  Check your configuration and try the connection again.
  ```
- **VPN 3000集中器为MSCHAPv1配置，并且PC为PAP配置，但是他们不能对认证方法达成协议**
  VPN 3000集中器debug输出：
  ```
  8 04/22/2002 14:22:59.190 SEV=5 PPP/12 RPT=1 171.69.89.129

  User [pptpuser] disconnected. Authentication protocol not allowed.
  ```
  用户看到的消息(从Windows 2000) ：
  ```
  Error 691:  Access was denied because the username and/or password
  was invalid on the domain.
  ```

要解决的可能的 Microsoft 问题

- **如何在注销后使 RAS 连接保持活动状态**当您从Windows远程访问服务(RAS)时客户端注销，所有RAS连接自动切断。在您注销后，请使在注册的**KeepRasConnections**密钥在RAS客户端保持已连接。参考Microsoft知识库文章- 158909 欲知更多信息。
- **当注册与缓存的证明时，用户没有警告**此问题症状是，当您尝试登录到从Windows工作站时的一个域或成员服务器和域控制器不可能查找，并且错误消息没有显示。而是使用缓存的凭证登录到本地计算机。参考的Microsoft知识库文章- 242536 欲知更多信息。
- **如何为域验证和其他名称解析问题编写 LMHOSTS 文件**可以有实例，当您遇到在您的TCP/IP网络时的名字解析问题，并且您需要使用LMHOST文件解析NetBIOS名称。此条款在名字解析和域确认讨论用于的适当方法创建Lmhosts文件帮助。参考的Microsoft知识库文章- 180094 欲知更多信息。

相关信息

- RFC 2637：点对点隧道协议 (PPTP)
- Cisco Secure ACS for Windows支持页面
- 什么时候Cisco VPN 3000集中器支持PPTP加密？
- 配置VPN 3000集中器和PPTP与Cisco Secure ACS for Windows RADIUS验证
- Cisco VPN 3000 集中器支持页
- Cisco VPN 3000 客户端支持页
- IP 安全 (IPSec) 产品支持页面
- PPTP产品支持页
- 技术支持和文档 - Cisco Systems