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
使用本地身份验证配置VPN 3000集中器
Microsoft PPTP 客户端配置
Windows 98 — 安装和配置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
检验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Windows客户端的点对点隧道协议(PPTP)隧道方法。这些VPN集中器上提供40位和128位加密支持，以实现安全可靠的连接。

要使用思科安全访问控制服务器(ACS)通过扩展身份验证为PPTP用户配置VPN集中器VPN集中器PPTP，请参阅为Windows RADIUS身份验证配置Cisco Secure ACS。

先决条件

要求

确保满足Cisco VPN 3000集中器上何时支持PPTP加密中提到的先决条件？在您尝试此配置之前。

使用的组件

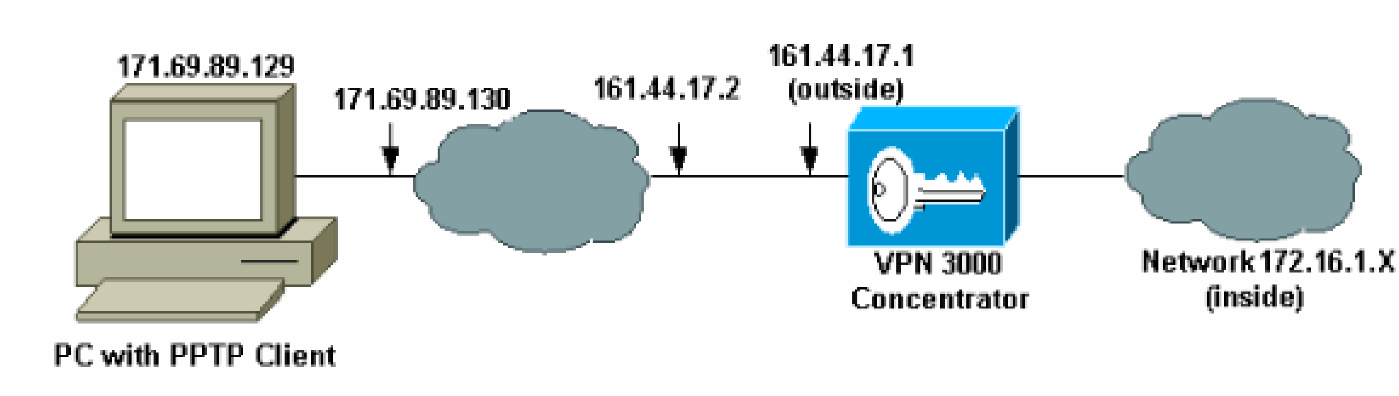
本文档中的信息基于以下软件和硬件版本：

- VPN 3015集中器，版本4.0.4.A
- 带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：



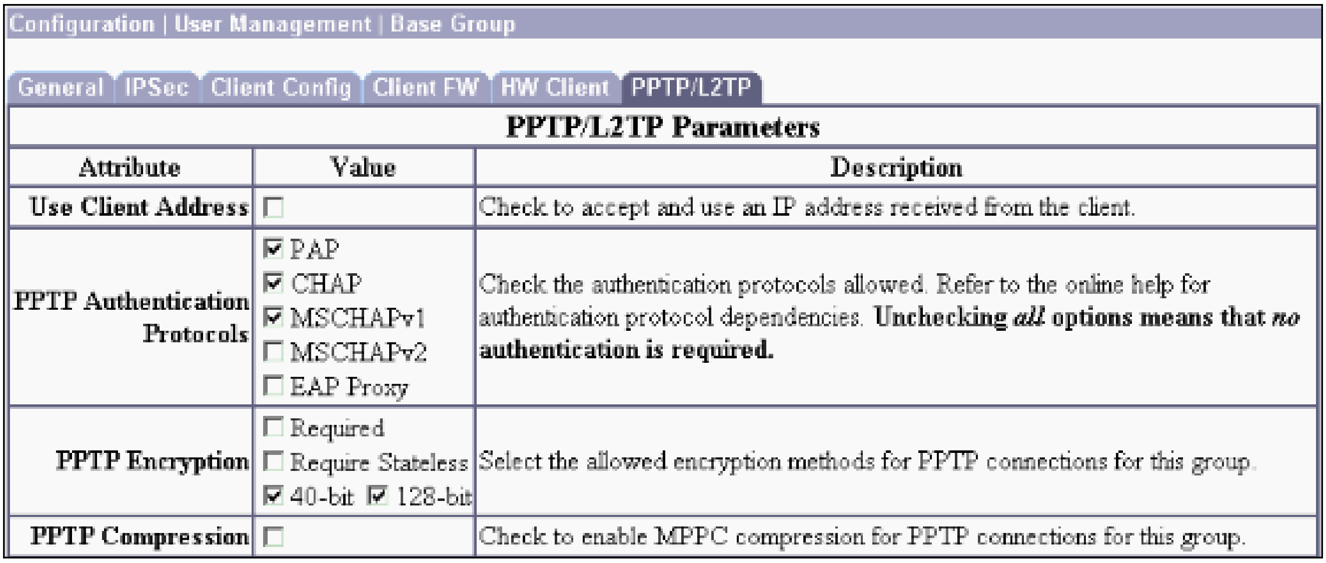
规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

使用本地身份验证配置VPN 3000集中器

完成以下步骤，使用本地身份验证配置VPN 3000集中器。

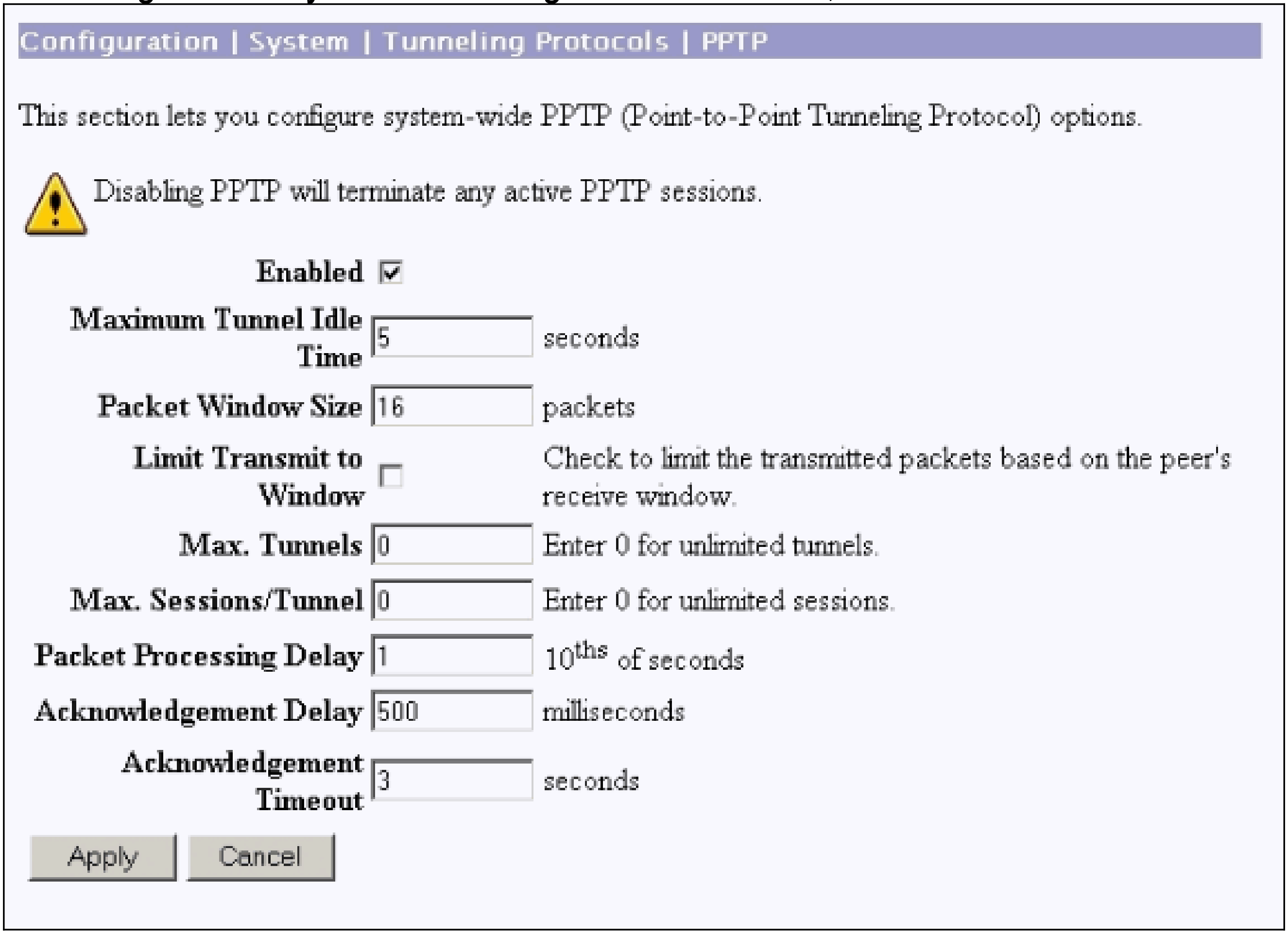
1. 在VPN集中器中配置各自的IP地址，并确保您具有连接。
2. 确保在**Configuration > User Management > Base Group PPTP/L2TP选项卡中**选择了PAP身份验证。



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**Configuration > System > Tunneling Protocols > PPTP**，并确保选中**Enabled**。



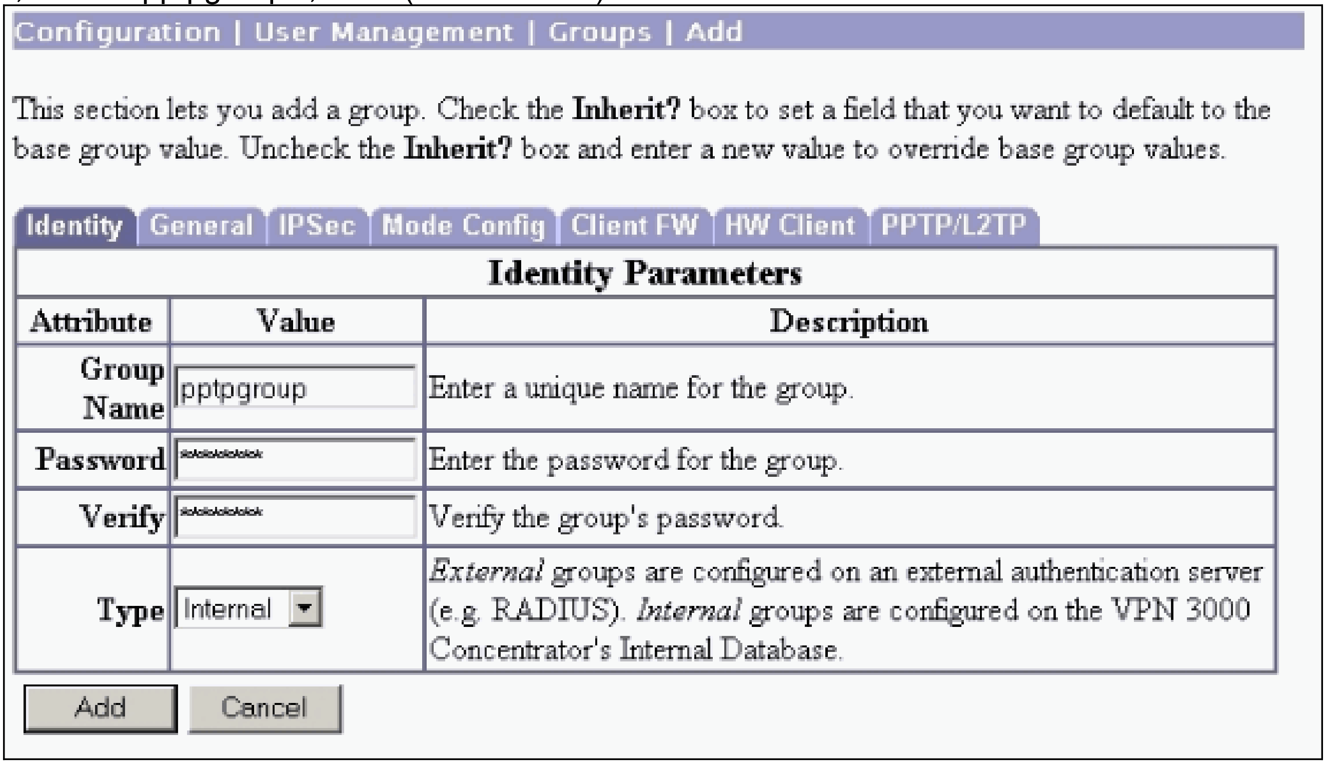
Configuration | System | Tunneling Protocols | PPTP

This section lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) options.

Disabling PPTP will terminate any active PPTP sessions.

Enabled	☑	
Maximum Tunnel Idle Time	5	seconds
Packet Window Size	16	packets
Limit Transmit to Window	□	Check to limit the transmitted packets based on the peer's receive window.
Max. Tunnels	0	Enter 0 for unlimited tunnels.
Max. Sessions/Tunnel	0	Enter 0 for unlimited sessions.
Packet Processing Delay	1	10ths of seconds
Acknowledgement Delay	500	milliseconds
Acknowledgement Timeout	3	seconds

4. 选择**Configuration > User Management > Groups > Add**，然后配置PPTP组。在本示例中，组名为“pptpgroup”，密码（和验证密码）为“cisco123”。



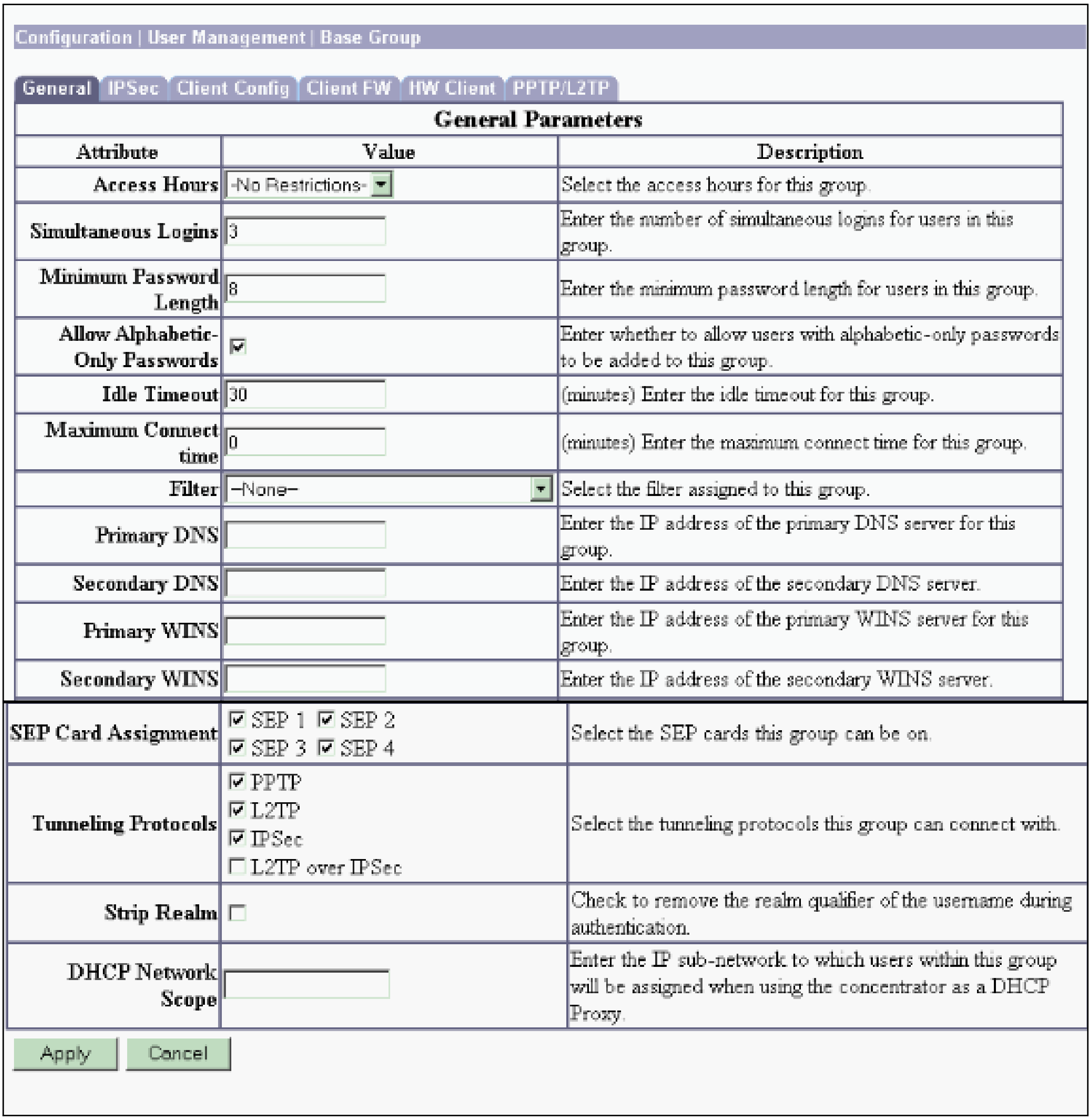
Configuration | User Management | Groups | Add

This section lets you add a group. 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 Parameters

Attribute	Value	Description
Group Name	pptpgroup	Enter a unique name for the group.
Password	*********	Enter the password for the group.
Verify	*********	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

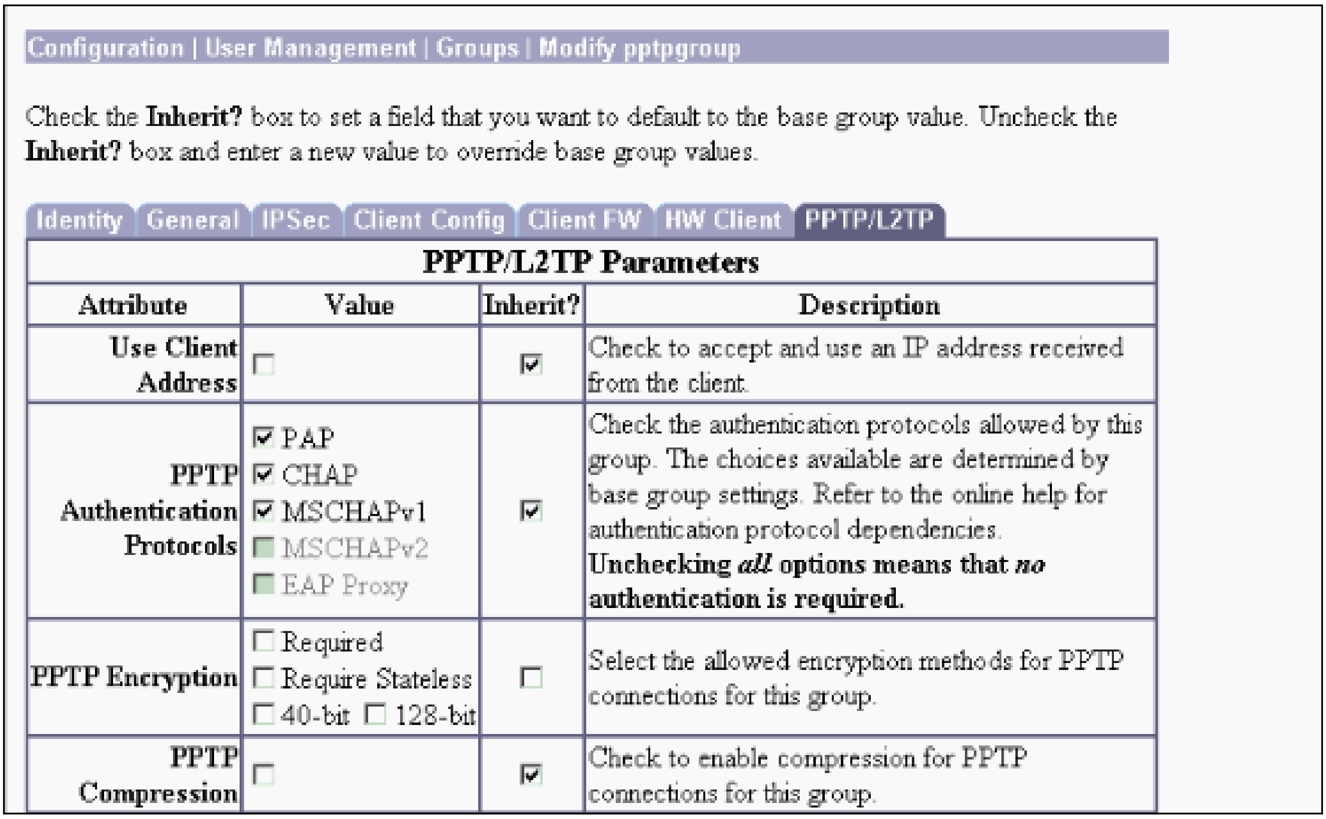
5. 在组的General选项卡下，确保在身份验证协议**中启**用了PPTP选项。



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.

6. 在PPTP/L2TP选项卡下，启用**PAP**身份验证并禁用**加**密（加密可以在将来的任何时间启用）。



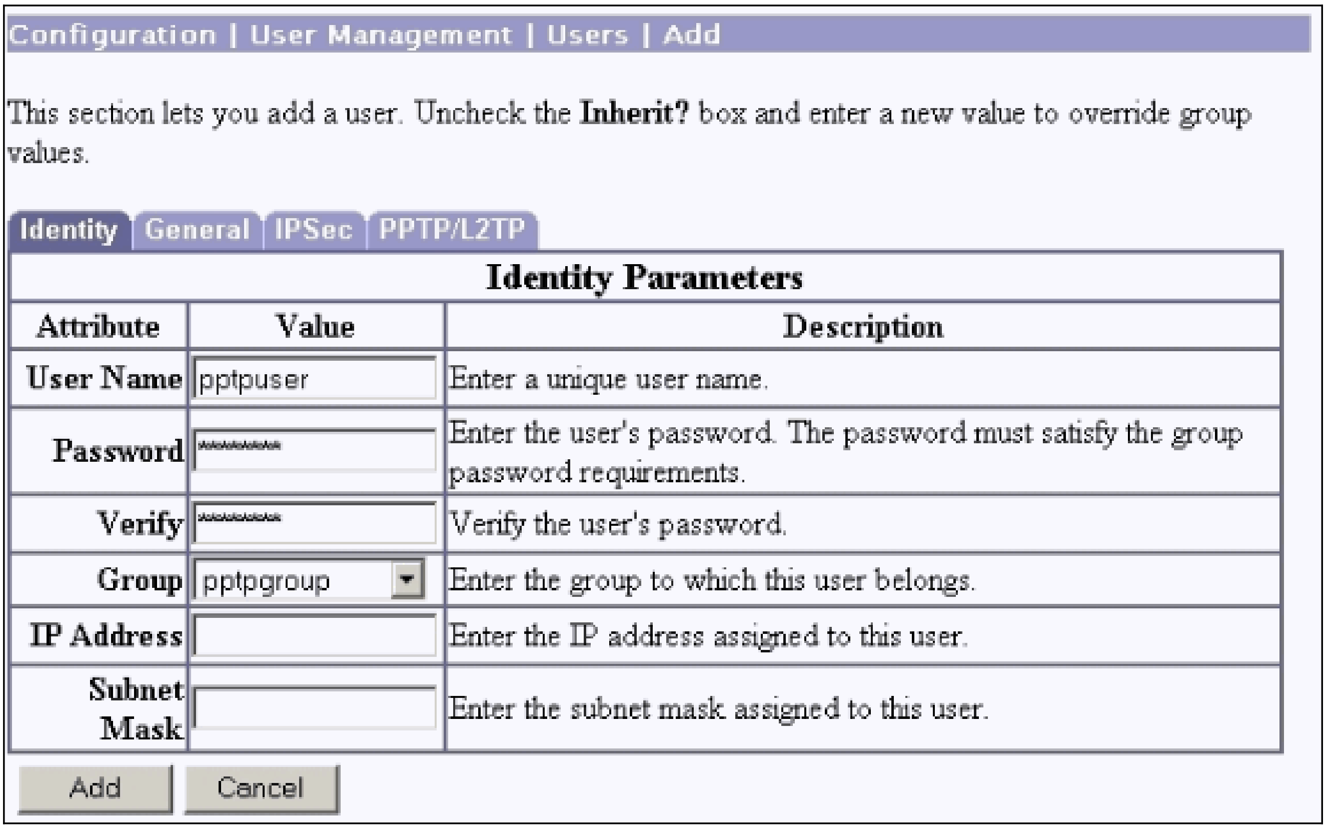
Configuration | User Management | Groups | Modify pptpgroup

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.

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**，并使用密码cisco123配置本地用户（称为“pptpuser”）**以进行**PPTP身份验证。将用户置于之前定义的“pptpgroup”中：



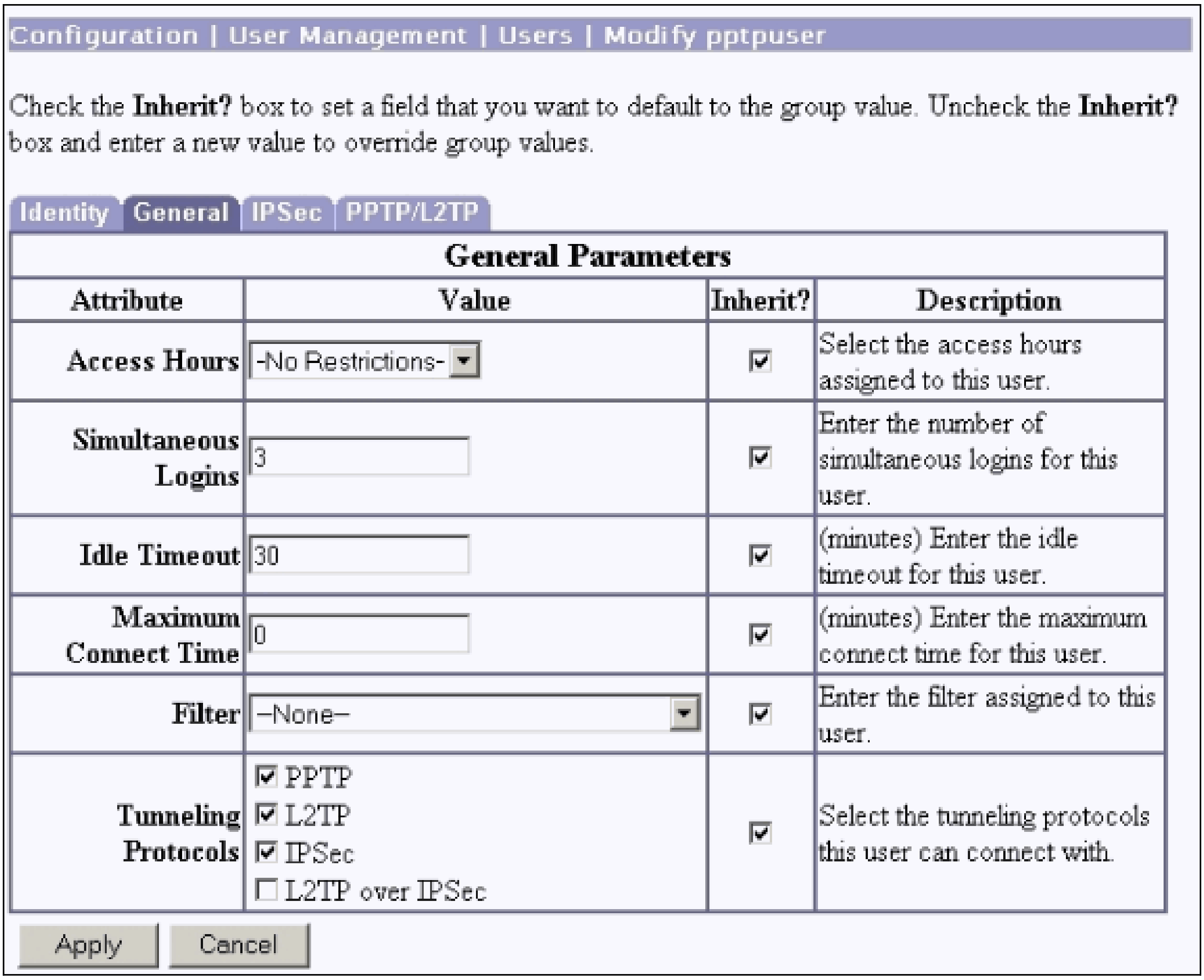
Configuration | User Management | Users | Add

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

Identity 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.

8. 在用户的General选项卡下，确保在隧道协议**中启**用了PPTP选项。



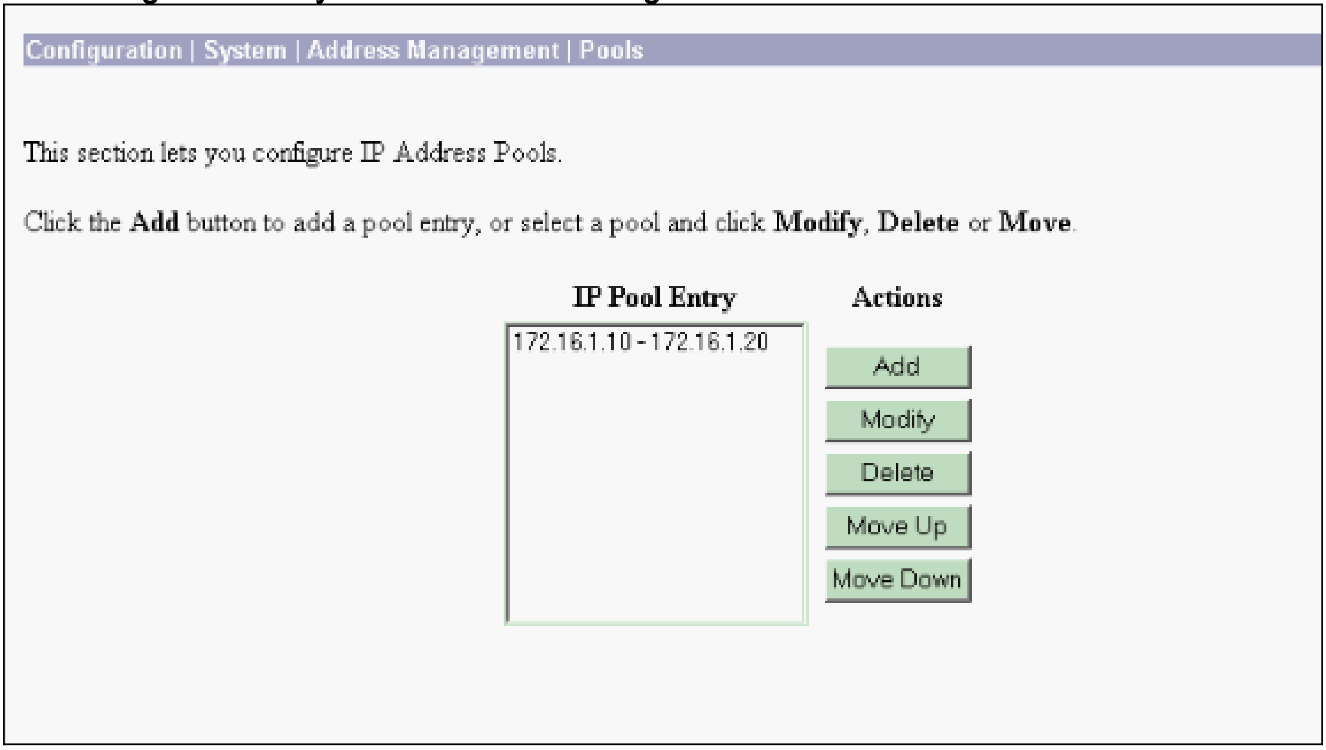
Configuration | User Management | Users | Modify pptpuser

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

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this user.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this user.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this user.
Filter	–None–	☑	Enter the filter assigned to this user.
Tunneling Protocols	☑ PPTP ☑ L2TP ☑ IPSec ☐ L2TP over IPSec	☑	Select the tunneling protocols this user can connect with.

9. 选择**Configuration > System > Address Management > Pools**以定义地址管理的地址池。



Configuration | System | Address Management | Pools

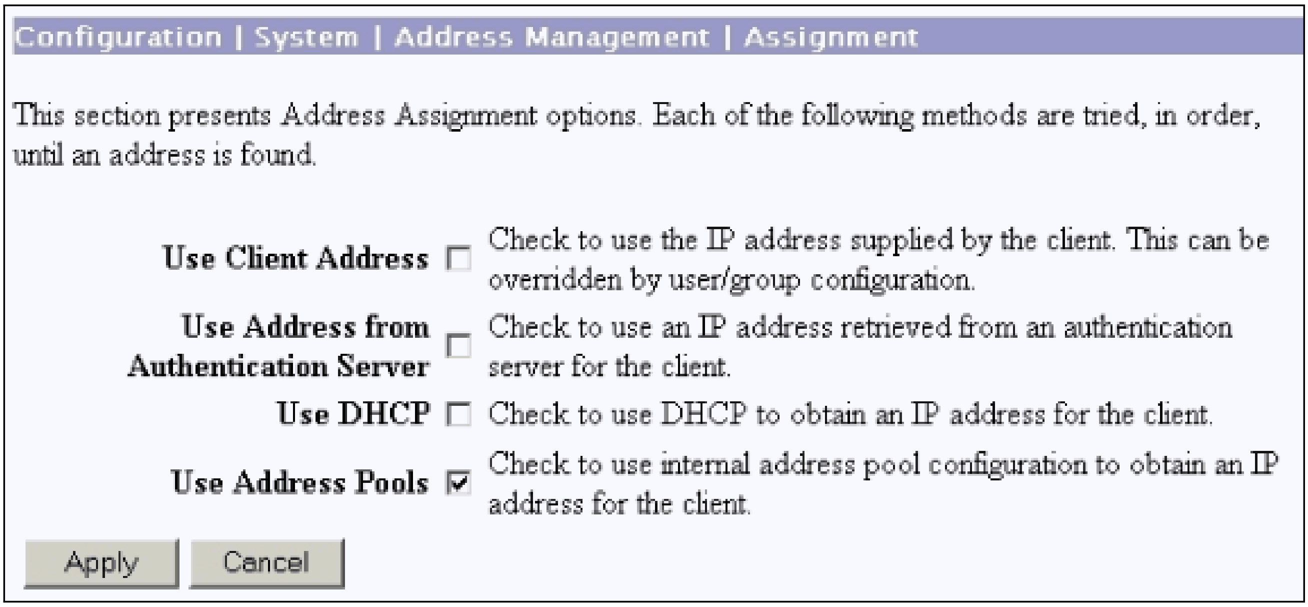
This section lets you configure IP Address Pools.

Click the **Add** button to add a pool entry, or select a pool and click **Modify**, **Delete** or **Move**.

IP Pool Entry

172.16.1.10 - 172.16.1.20

10. 选择**Configuration > System > Address Management > Assignment**，并指示VPN集中器使用地址池。



Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address	□	Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
Use Address from Authentication Server	□	Check to use an IP address retrieved from an authentication server for the client.
Use DHCP	□	Check to use DHCP to obtain an IP address for the client.
Use Address Pools	☑	Check to use internal address pool configuration to obtain an IP address for the client.

Microsoft PPTP 客户端配置

注意：此处提供的有关配置Microsoft软件的信息均不附带任何Microsoft软件保修或支持。Microsoft提供对Microsoft软件的支持 。

Windows 98 — 安装和配置PPTP功能

安装

完成以下步骤以安装PPTP功能。

1. 选择**开始>设置>控制面板>添加新硬件（下一步）>从列表>网络适配器（下一步）中选择。**
2. 在左**面板**中选择Microsoft，在**右面板**中选择Microsoft VPN适配器。

配置

完成以下步骤以配置PPTP功能。

1. 选择**开始>程序>附件>通信>拨号网络>建立新连接。**
2. 在“Select a device（选择设备）”提示符下，使用Microsoft VPN适配器进行连接。VPN服务器IP是3000隧道终端。

Windows 98默认身份验证使用密码加密（例如，CHAP或MSCHAP）。 要初始禁用此加密，请选择“属性”**>“服务器类型”**，并取消选中“加密密**码”和“需**要数据**加密**”框。

Windows 2000 - 配置 PPTP 功能

完成以下步骤以配置PPTP功能。

1. 选择**开始>程序>附件>通信>网络和拨号连接>建立新连接。**
2. 单击**Next**，然后选**择Connect to a private network through the Internet > Dial a connection prior（如果使用LAN，请不要选择此选项）。**
3. 再次单击**Next**，然后输入隧道终端的主机名或IP，隧道终端是VPN 3000集中器的外部接口。

在本例中，IP地址为161.44.17.1。

为连**接选择属性>安全>高级，**将密码类型添加为PAP。默认为MSCHAP和MSCHAPv2，而不是CHAP或PAP。

数据加密可在此区域进行配置。您可以先禁用它。

Windows NT

您可以在Microsoft网站访问有关为PPTP设置Windows NT客户端的信息 。

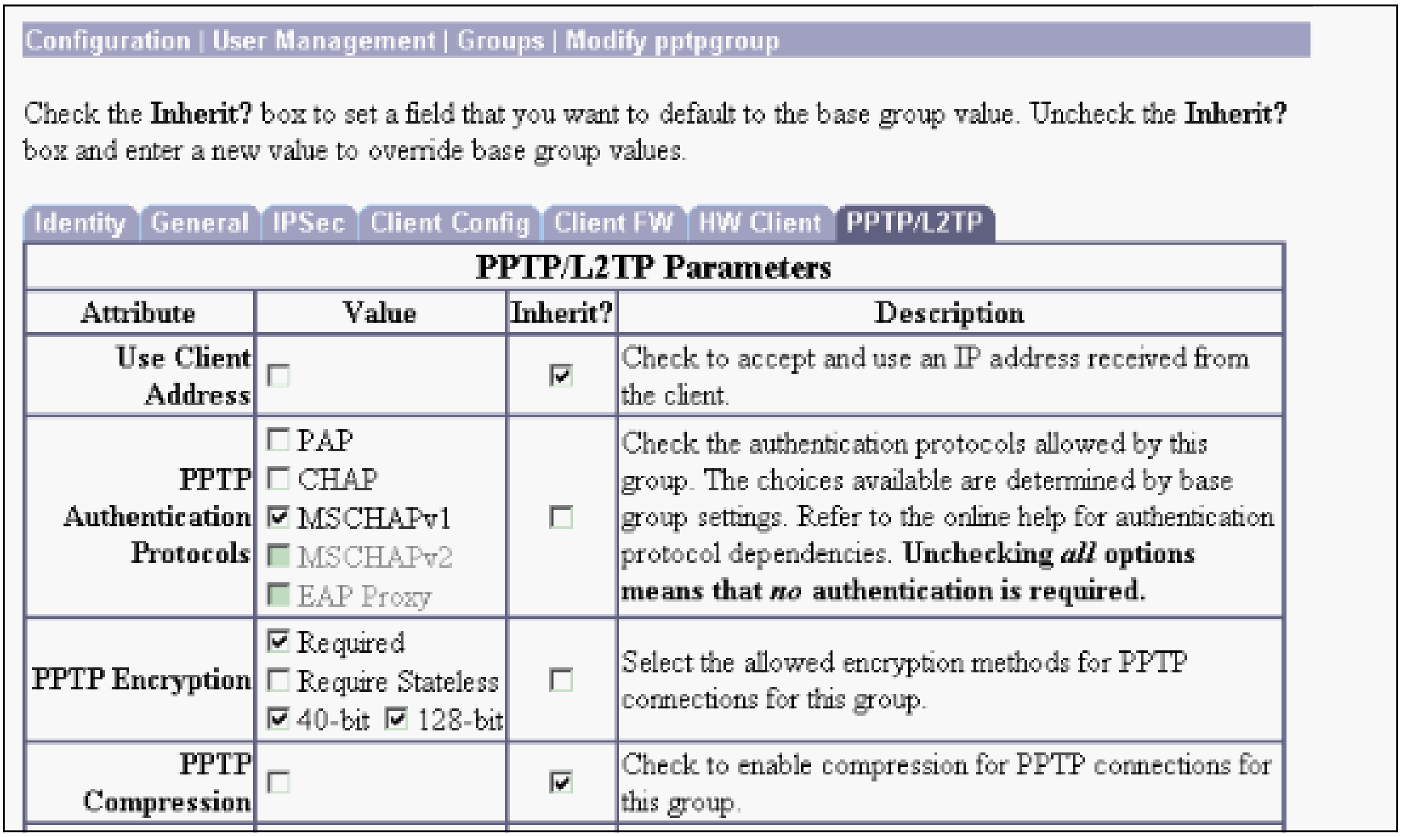
Windows Vista

完成以下步骤以配置PPTP功能。

1. 从“开始**”按**钮中，选**择连接到**。
2. 选**择Set up a connection or network**。
3. 选择“**连接到工作区”**，然后单**击“下一步**”。
4. 选择**Use my Internet Connection(VPN)**。**注意：如**果提示“Do you want to use a connection hare have”，请选择“No”，创建新连接，然后单击**“Next”**。
5. 在“Internet**地址”**字段中，键**入pptp.vpn.univ.edu**，例如。
6. 例如，**在Destination Name**字段中**键入**UNIVVPN。
7. 在“用**户名”**字段中，键入您的UNIV登录ID。您的UNIV登录ID是@univ.edu之前的电子邮件地**址的一部分**。
8. 在**Password**字段中，键入您的UNIV登录ID密码。
9. 单击“Create(**创建)**”按钮，然后单击“**Close(关**闭)”按钮。
10. 要在创建VPN连接后连接到VPN服务器，请单击“开始”，然后单击“连**接到”**。
11. 在窗口中选择VPN连接，然后单击**Connect**。

添加MPPE（加密）

在添加加密之前，请确保PPTP连接在未加密的情况下工作。例如，单击PPTP客户端上的**Connect**按钮，确保连接完成。如果您决定需要加密，则必须使用MSCHAP身份验证。在VPN 3000上，选择**Configuration > User Management > Groups**。然后，在组的PPTP/L2TP选项卡下，取消选中**PAP**，选中**MSCHAPv1**，然后选中**Required for PPTP Encryption**。



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.

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.

应重新配置PPTP客户端，以进行可选或必需的数据加密和MSCHAPv1（如果是选项）。

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。

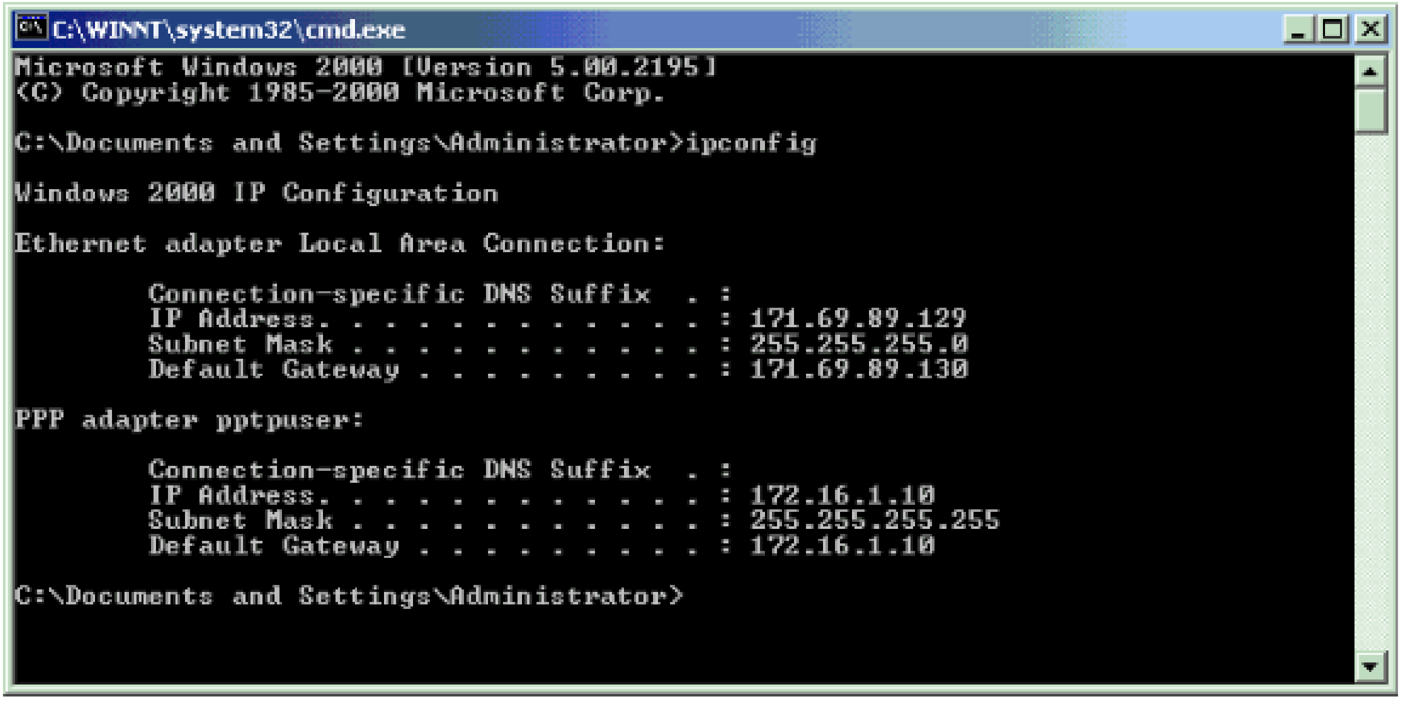
验证VPN集中器

您可以通过拨打之前在“Microsoft PPTP客户端配置”部分创建的PPTP客户端来启动PPTP会话。

使用VPN集中器上的Administration > Administer Sessions窗口查看所有活动PPTP会话的参数和统计信息。

检验PC

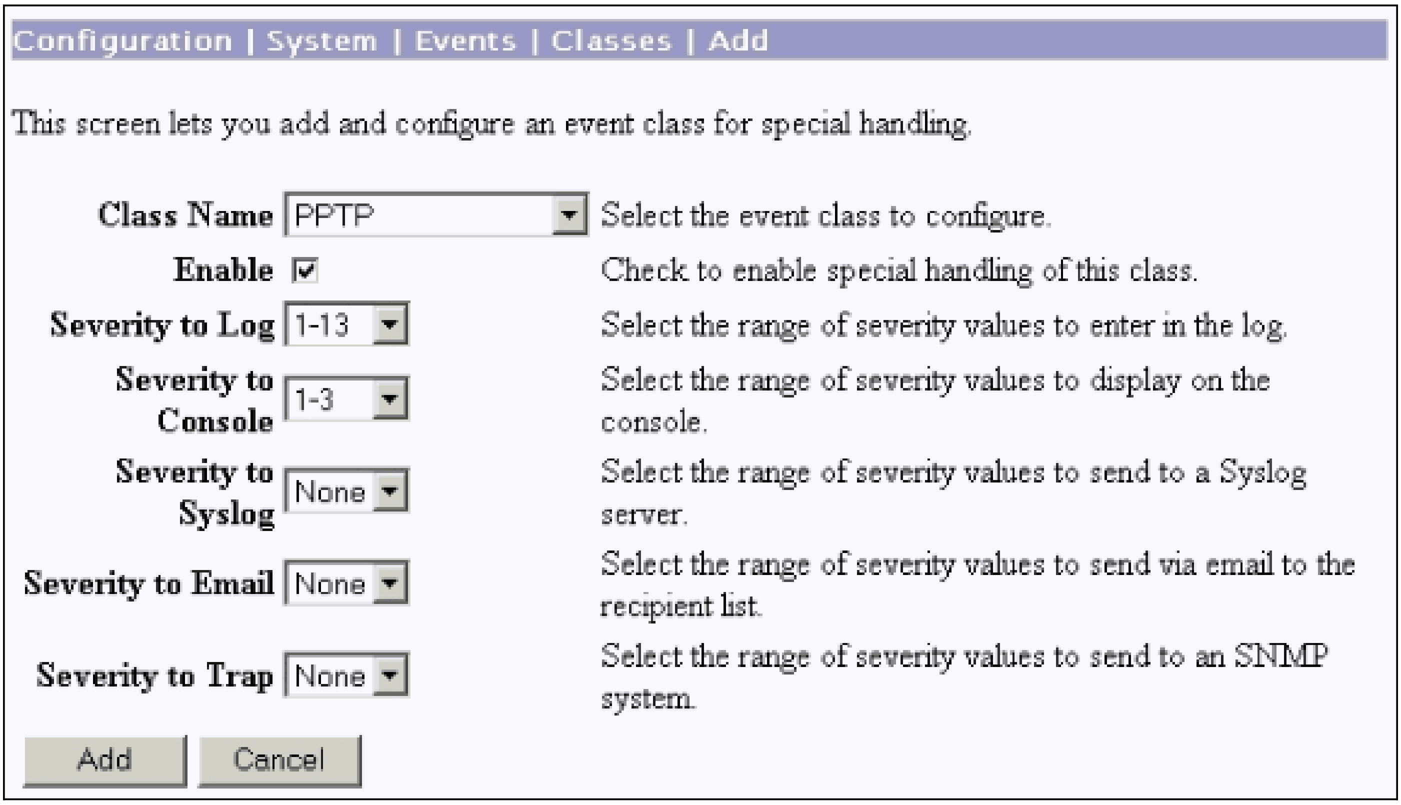
在PC的命令模式下发出**ipconfig**命令，以查看PC有两个IP地址。一个是自己的IP地址，另一个由VPN集中器从IP地址池分配。在本示例中，IP地址172.16.1.10是VPN集中器分配的IP地址。



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 171.69.89.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 171.69.89.130

PPP adapter pptpuser:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.1.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 172.16.1.10

C:\Documents and Settings\Administrator>
```

调试

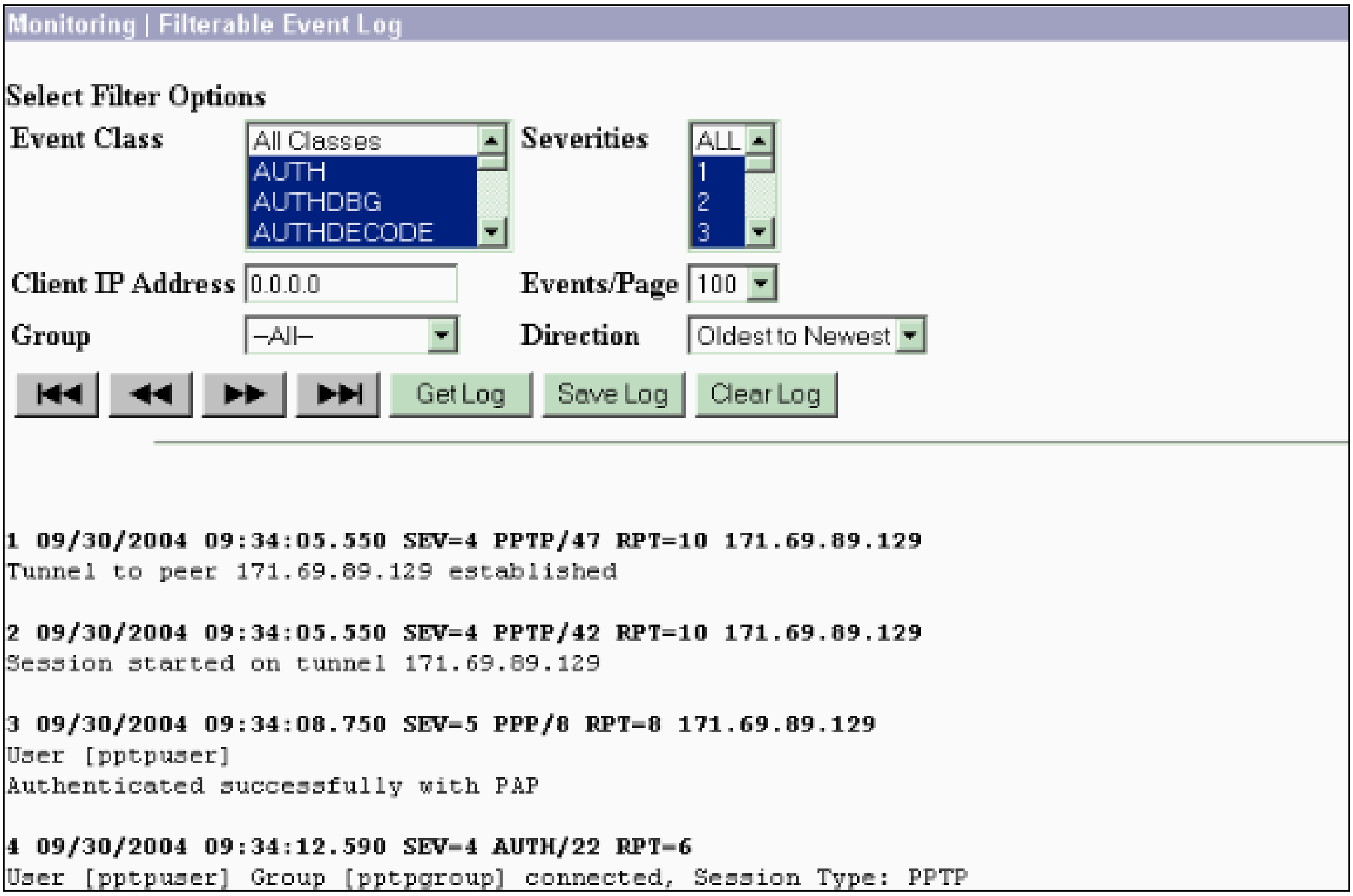
如果连接不工作，PPTP事件类调试可以添加到VPN集中器。选择**Configuration > System > Events > Classes > Modify**或**Add**（此处显示）。PPTPDBG和PPTPDECODE事件类也可用，但可能提供太多信息。


Configuration | System | Events | Classes | Add

This screen lets you add and configure an event class for special handling.

Class Name	PPTP	Select the event class to configure.
Enable	☑	Check to enable special handling of this class.
Severity to Log	1-13	Select the range of severity values to enter in the log.
Severity to Console	1-3	Select the range of severity values to display on the console.
Severity to Syslog	None	Select the range of severity values to send to a Syslog server.
Severity to Email	None	Select the range of severity values to send via email to the recipient list.
Severity to Trap	None	Select the range of severity values to send to an SNMP system.

可以从Monitoring > Filterable Event Log中**检索事件日志**。



Select Filter Options

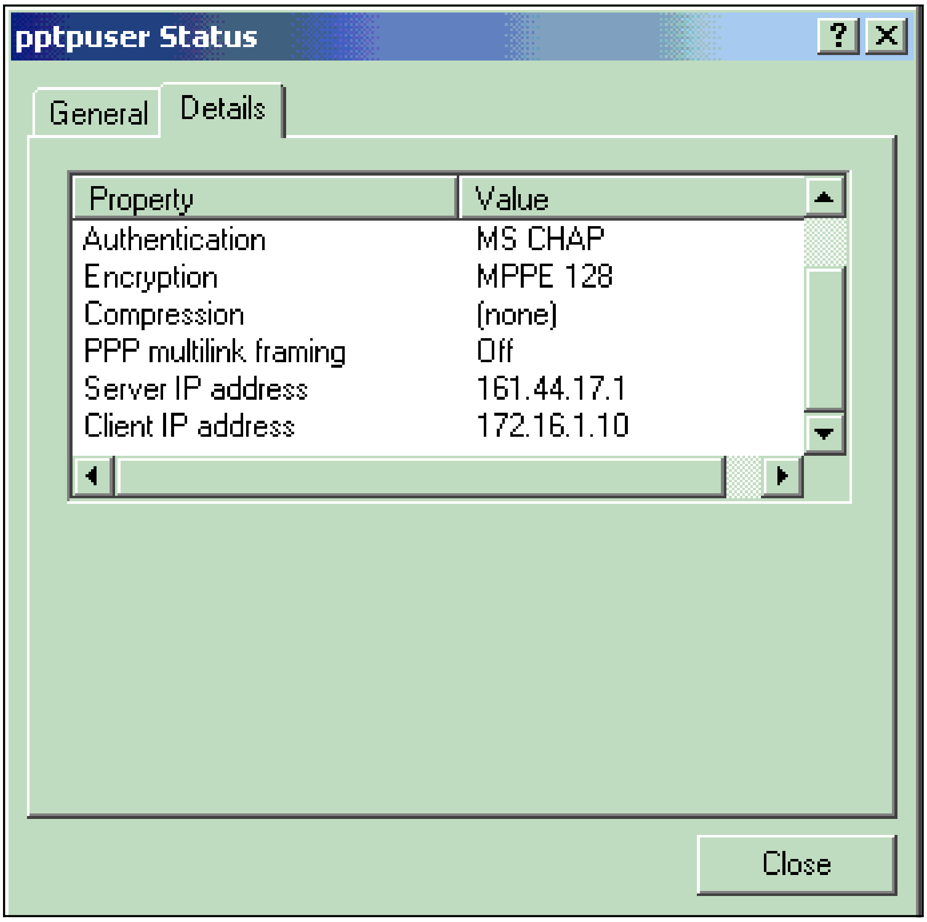
Event Class: All Classes, AUTH, AUTHDBG, AUTHDECODE
Severities: ALL, 1, 2, 3
Client IP Address: 0.0.0.0
Events/Page: 100
Group: -All-
Direction: Oldest to Newest

```
1 09/30/2004 09:34:05.550 SEV=4 PPTP/47 RPT=10 171.69.89.129
Tunnel to peer 171.69.89.129 established

2 09/30/2004 09:34:05.550 SEV=4 PPTP/42 RPT=10 171.69.89.129
Session started on tunnel 171.69.89.129

3 09/30/2004 09:34:08.750 SEV=5 PPP/8 RPT=8 171.69.89.129
User [pptpuser]
Authenticated successfully with PAP

4 09/30/2004 09:34:12.590 SEV=4 AUTH/22 RPT=6
User [pptpuser] Group [pptpgroup] connected, Session Type: PPTP
```

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
```

单击PPTP用户状态详**细信**息窗口，检查Windows PC上的参数。



Property	Value
Authentication	MS CHAP
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Server IP address	161.44.17.1
Client IP address	172.16.1.10

故障排除

您可能会遇到以下错误：

- **用户名或密码错误**VPN 3000集中器调试输出：

```
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（来自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（来自Windows 2000）：

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

- **在PC上选择“需要加密”，但在VPN集中器上未选择**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
  ```
- **在VPN集中器上，在仅支持40位加密的PC上选择“需要加密”（128位）**VPN 3000集中器调试输出：
  ```
  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集中器配置为MSCHAPv1，而PC配置为PAP，但无法就身份验证方法达成一致**VPN 3000集中器调试输出：
  ```
  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**从Windows远程访问服务(RAS)客户端注销时，所有RAS连接都会自动断开。在注销后，**启用RAS客户**端上注册表中的KeepRasConnections项以保持连接。有关详细信息，请参阅Microsoft知识库文章 — 158909 。
- **使用缓存凭证登录时，用户没有收到警报**此问题的症状是您尝试从基于Windows的工作站或成员服务器登录到域，但找不到域控制器，并且未显示错误消息。而是使用缓存的凭证登录到本地计算机。有关详细信息，请参阅Microsoft知识库文章 — 242536 。
- **如何为域验证和其他名称解析问题编写 LMHOSTS 文件**在TCP/IP网络上遇到名称解析问题，并且需要使用LMHOSTS文件解析NetBIOS名称时，可能会出现一些实例。本文讨论了创建LMHOSTS文件的正确方法，以帮助进行名称解析和域验证。有关详细信息，请参阅Microsoft知识库文章 — 180094 。

相关信息

- RFC 2637：点对点隧道协议 (PPTP)
- Cisco Secure ACS for Windows支持页
- Cisco VPN 3000 集中器何时支持 PPTP 加密？
- 使用Cisco Secure ACS for Windows RADIUS身份验证配置VPN 3000集中器和PPTP
- 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