为 Windows RADIUS认证配置使用Cisco Secure ACS 的VPN 3000集中器PPTP

目录

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。集中器支持40位和128位加密，以实现安全可靠的连接。本文档介绍如何在VPN 3000集中器上配置PPTP，使用Cisco Secure ACS for Windows进行RADIUS身份验证。

请参阅配置Cisco安全PIX防火墙以使用PPTP配置到PIX的PPTP连接。

请参阅配置Cisco Secure ACS for Windows Router PPTP Authentication以设置与路由器的PC连接；这为Cisco Secure Access Control System(ACS)3.2 for Windows服务器提供用户身份验证，然后再允许用户进入网络。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档假设本地PPTP身份验证在添加Cisco Secure ACS for Windows RADIUS身份验证之前正常工作。有关本地PPTP身份验证的详细信息，请参阅如何使用本地身份验证配置VPN 3000集中器PPTP。有关要求和限制的完整列表，请参阅Cisco VPN 3000集中器何时支持PPTP加密？

使用的组件

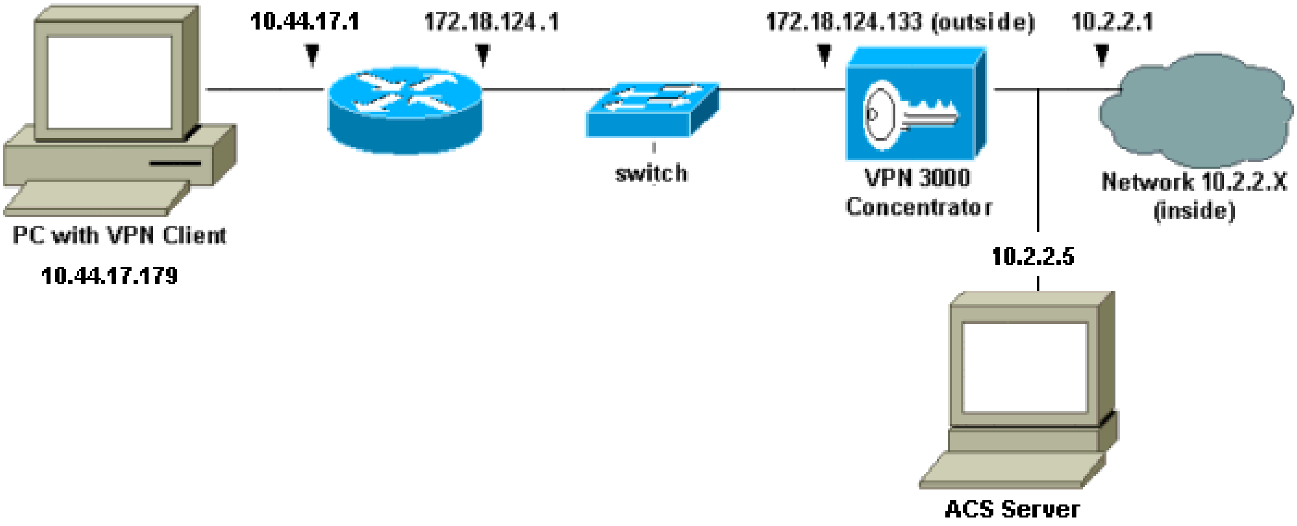
本文档中的信息基于以下软件和硬件版本。

- 适用于Windows 2.5及更高版本的思科安全ACS
- VPN 3000集中器版本2.5.2.C及更高版本（此配置已通过版本4.0.x验证）

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

网络图

本文档使用下图所示的网络设置。

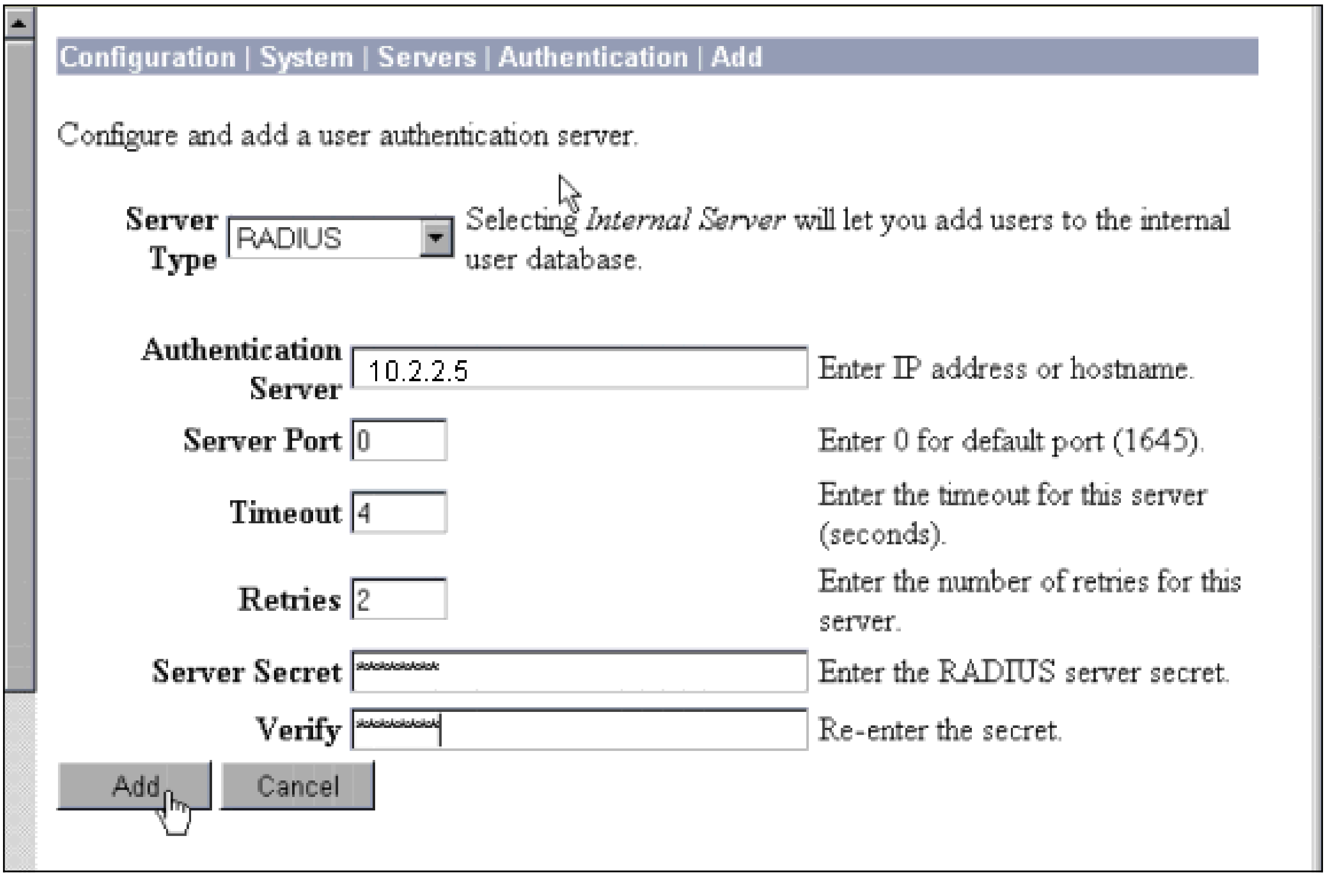


配置 VPN 3000 集中器

添加和配置Cisco Secure ACS for Windows

按照以下步骤配置VPN集中器以使用Cisco Secure ACS for Windows。

1. 在VPN 3000集中器上，转到**Configuration > System > Servers > Authentication Servers**，并添加Cisco Secure ACS for Windows服务器和密钥（本例中为“cisco123”）。



Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type: RADIUS — Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server: 10.2.2.5 — Enter IP address or hostname.

Server Port: 0 — Enter 0 for default port (1645).

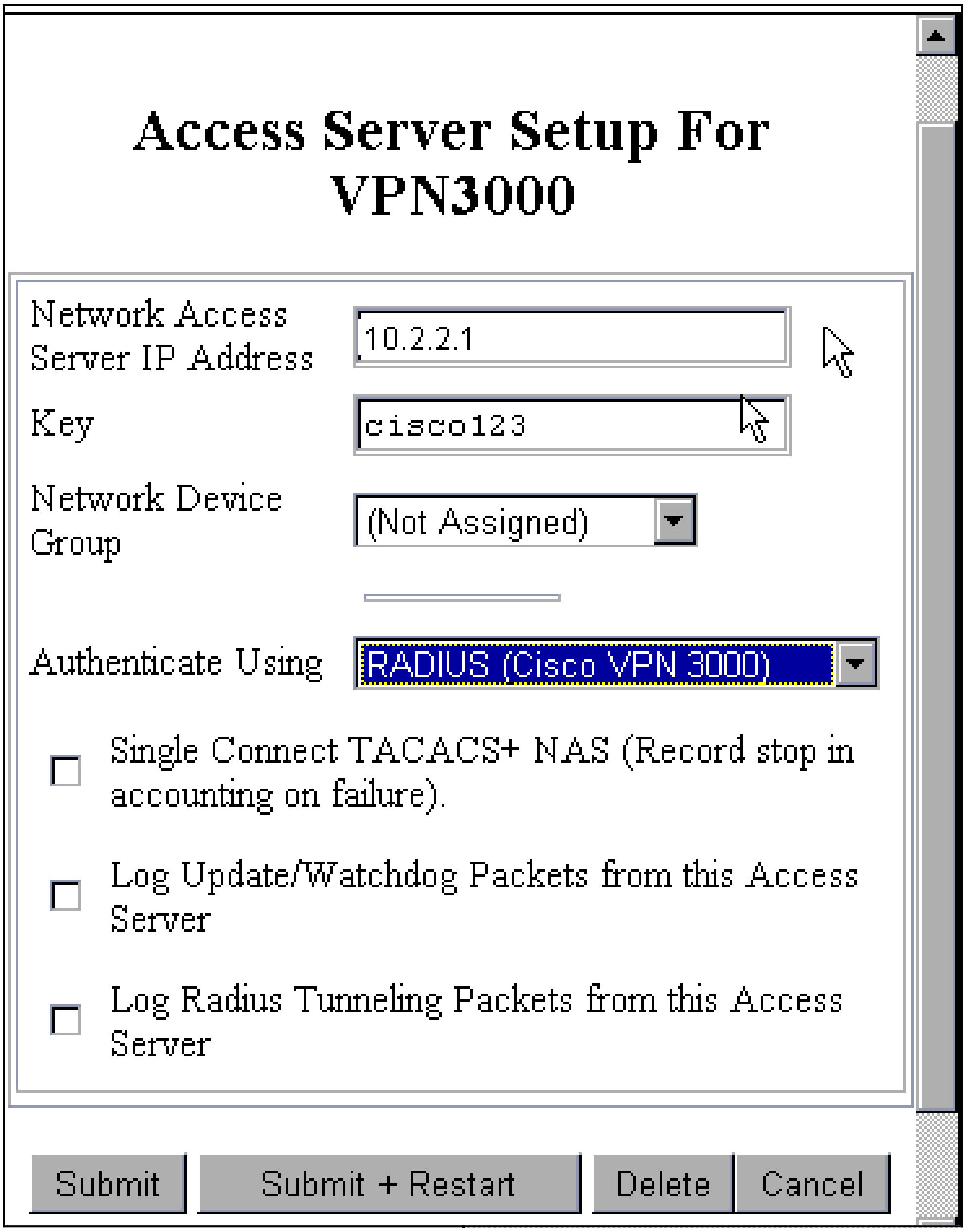
Timeout: 4 — Enter the timeout for this server (seconds).

Retries: 2 — Enter the number of retries for this server.

Server Secret: ******** — Enter the RADIUS server secret.

Verify: ******** — Re-enter the secret.

2. 在Cisco Secure ACS for Windows中，将VPN集中器添加到ACS服务器网络配置，并确定字典



Access Server Setup For VPN3000

Network Access Server IP Address	10.2.2.1
Key	cisco123
Network Device Group	(Not Assigned)
Authenticate Using	RADIUS (Cisco VPN 3000)

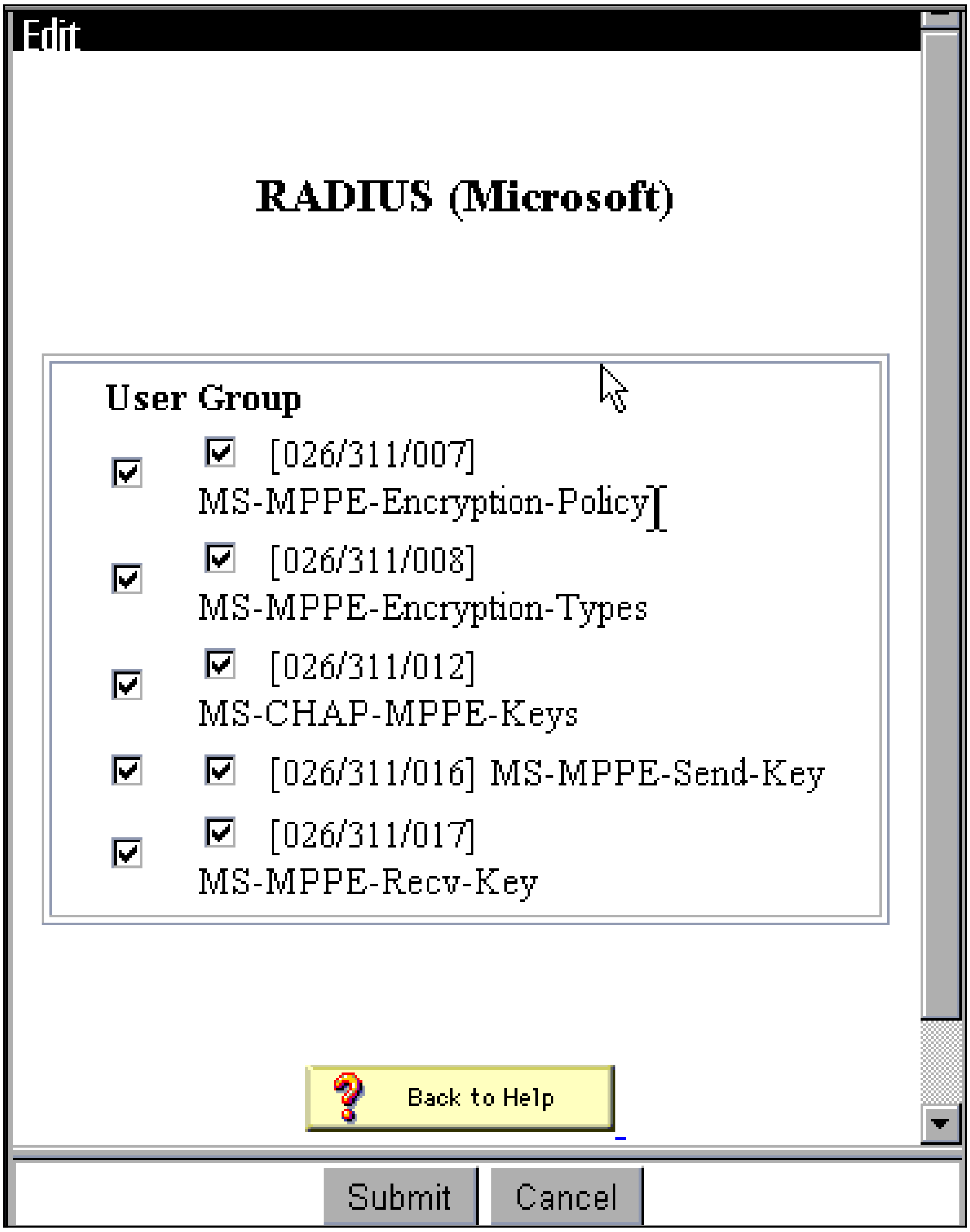
□ Single Connect TACACS+ NAS (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this Access Server

□ Log Radius Tunneling Packets from this Access Server

类型。

3. 在Cisco Secure ACS for Windows中，转到**Interface Configuration > RADIUS(Microsoft)**并检查Microsoft点对点加密(MPPE)属性，以便属性显示在组接口中。



RADIUS (Microsoft)

User Group

☑ ☑ [026/311/007] MS-MPPE-Encryption-Policy

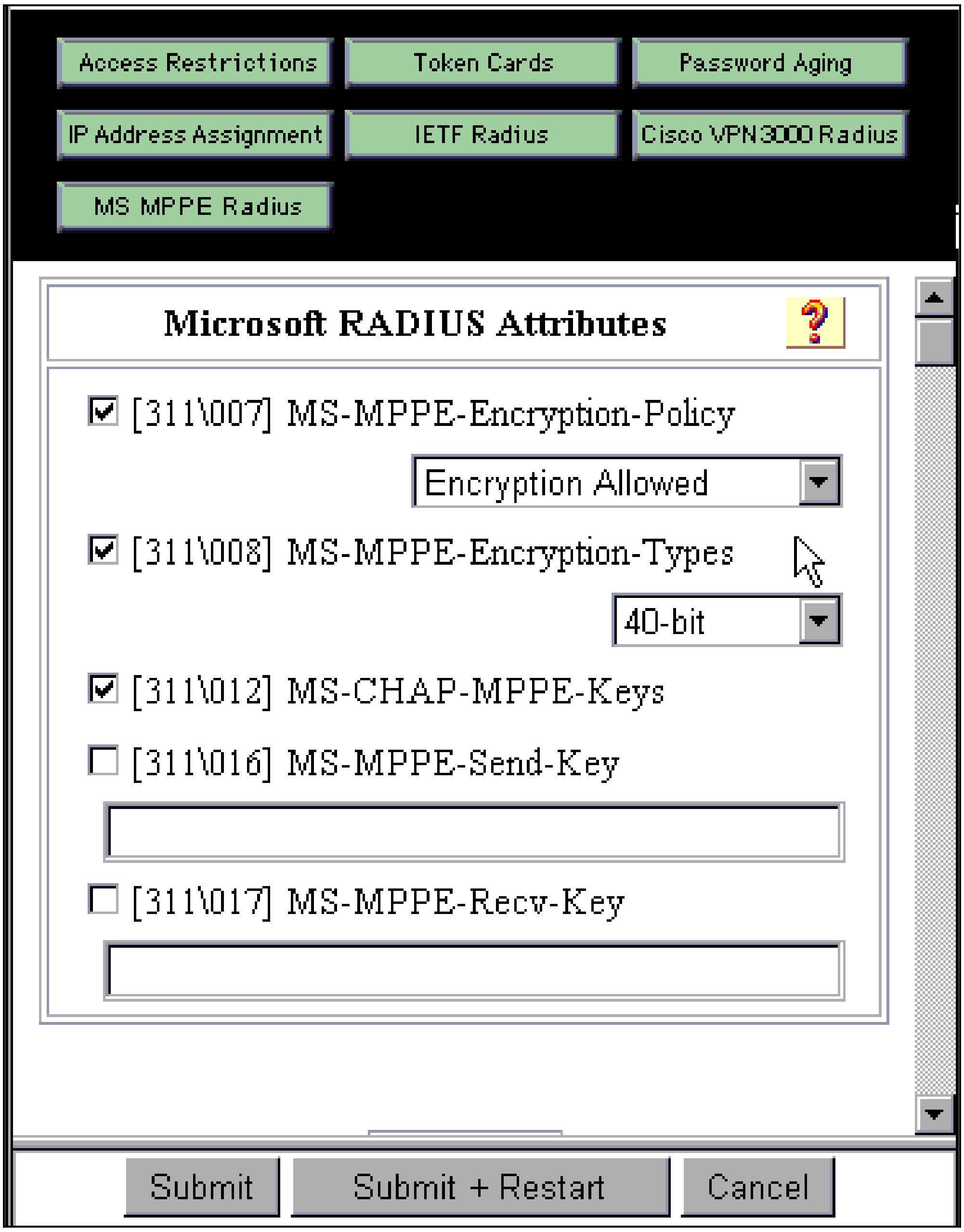
☑ ☑ [026/311/008] MS-MPPE-Encryption-Types

☑ ☑ [026/311/012] MS-CHAP-MPPE-Keys

☑ ☑ [026/311/016] MS-MPPE-Send-Key

☑ ☑ [026/311/017] MS-MPPE-Recv-Key

4. 在适用于Windows的思科安全ACS中，添加用户。在用户组中，添加MPPE(Microsoft RADIUS)属性，以防以后需要加密。



Microsoft RADIUS Attributes

☑ [311\007] MS-MPPE-Encryption-Policy

Encryption Allowed

☑ [311\008] MS-MPPE-Encryption-Types

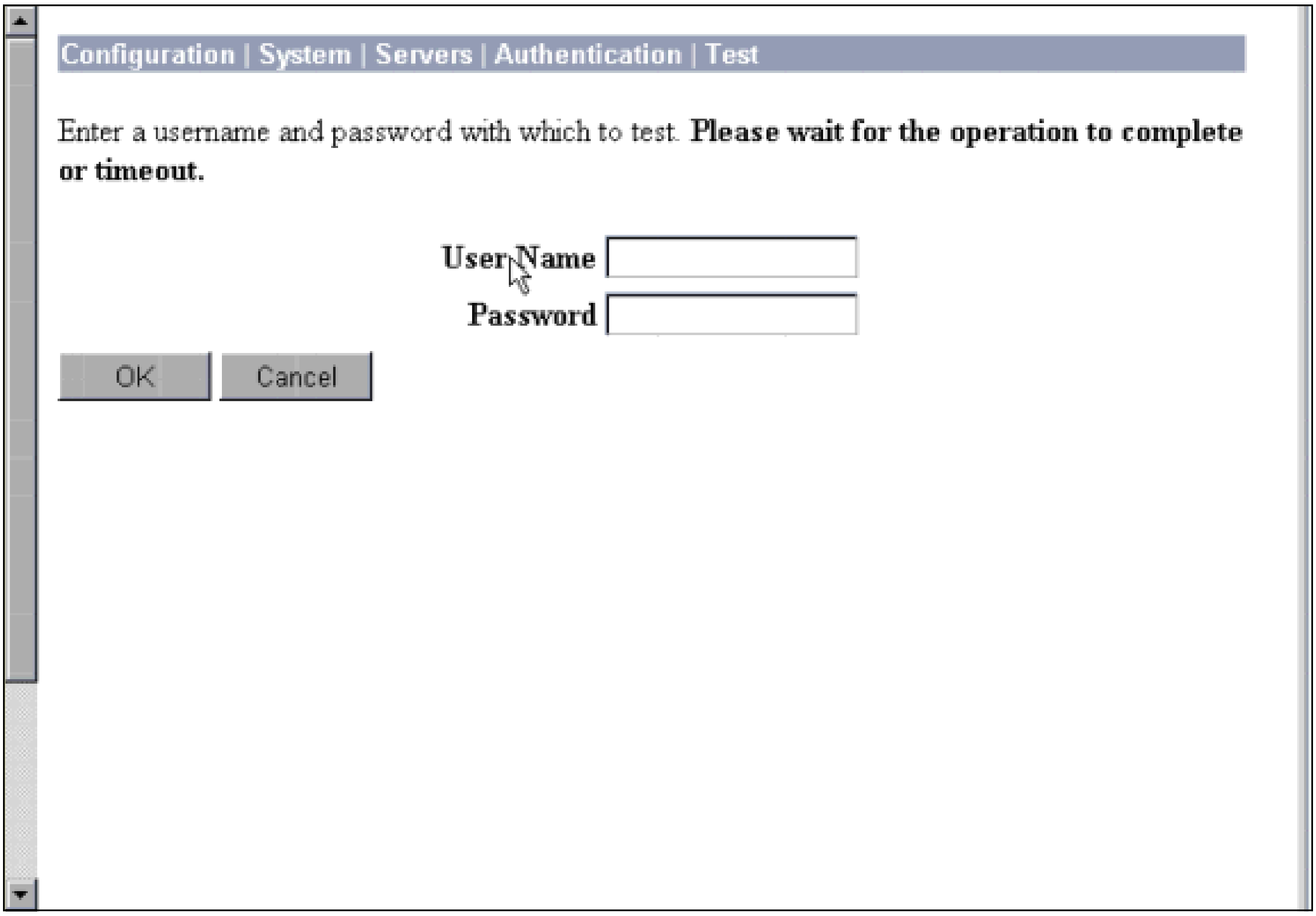
40-bit

☑ [311\012] MS-CHAP-MPPE-Keys

□ [311\016] MS-MPPE-Send-Key

□ [311\017] MS-MPPE-Recv-Key

5. 在VPN 3000集中器上，转到Configuration > System > Servers **> Authentication Servers**。从列表中选择身份验证服务器，然后选择**Test**。输入用户名和密码，测试从VPN集中器到Cisco Secure ACS for Windows服务器的身份验证。在良好的身份验证中，VPN集中器应显示“身份验证成功”消息。Cisco Secure ACS for Windows中的失败记录在“报告和活**动”>“失败尝试”中**。在默认安装中，这些报告存储在C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts中的磁盘上。



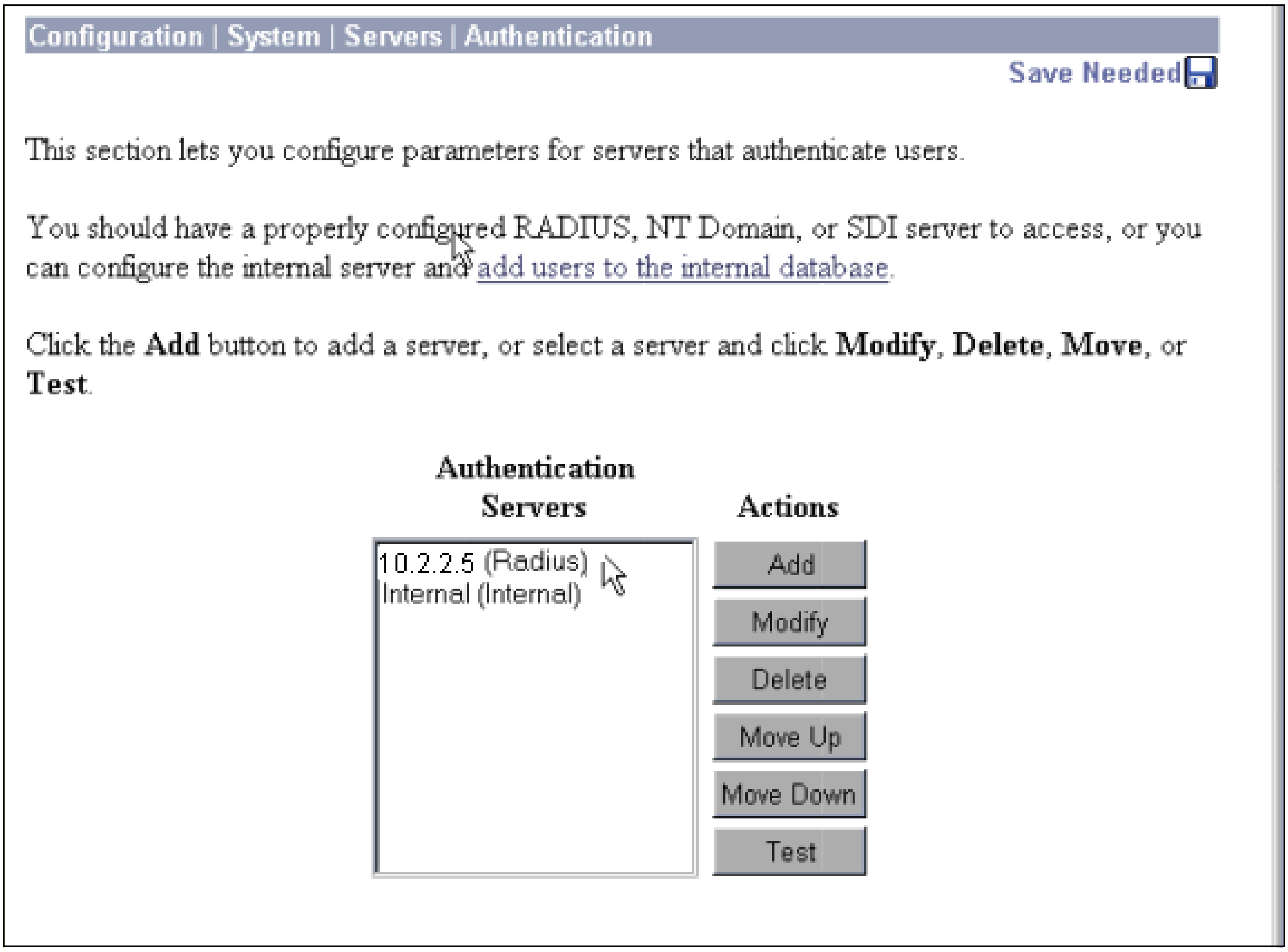
Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

User Name

Password

6. 由于您现在已验证从PC到VPN集中器的身份验证工作，以及从集中器到Cisco Secure ACS for Windows服务器的身份验证，因此可以通过将Cisco Secure ACS for Windows服务器移至服务器列表顶部来重新配置VPN集中器，以将PPTP用户发送到Cisco Secure ACS for Windows RADIUS。要在VPN集中器上执行此操作，请转到**Configuration > System > Servers > Authentication Servers**。



Configuration | System | Servers | Authentication

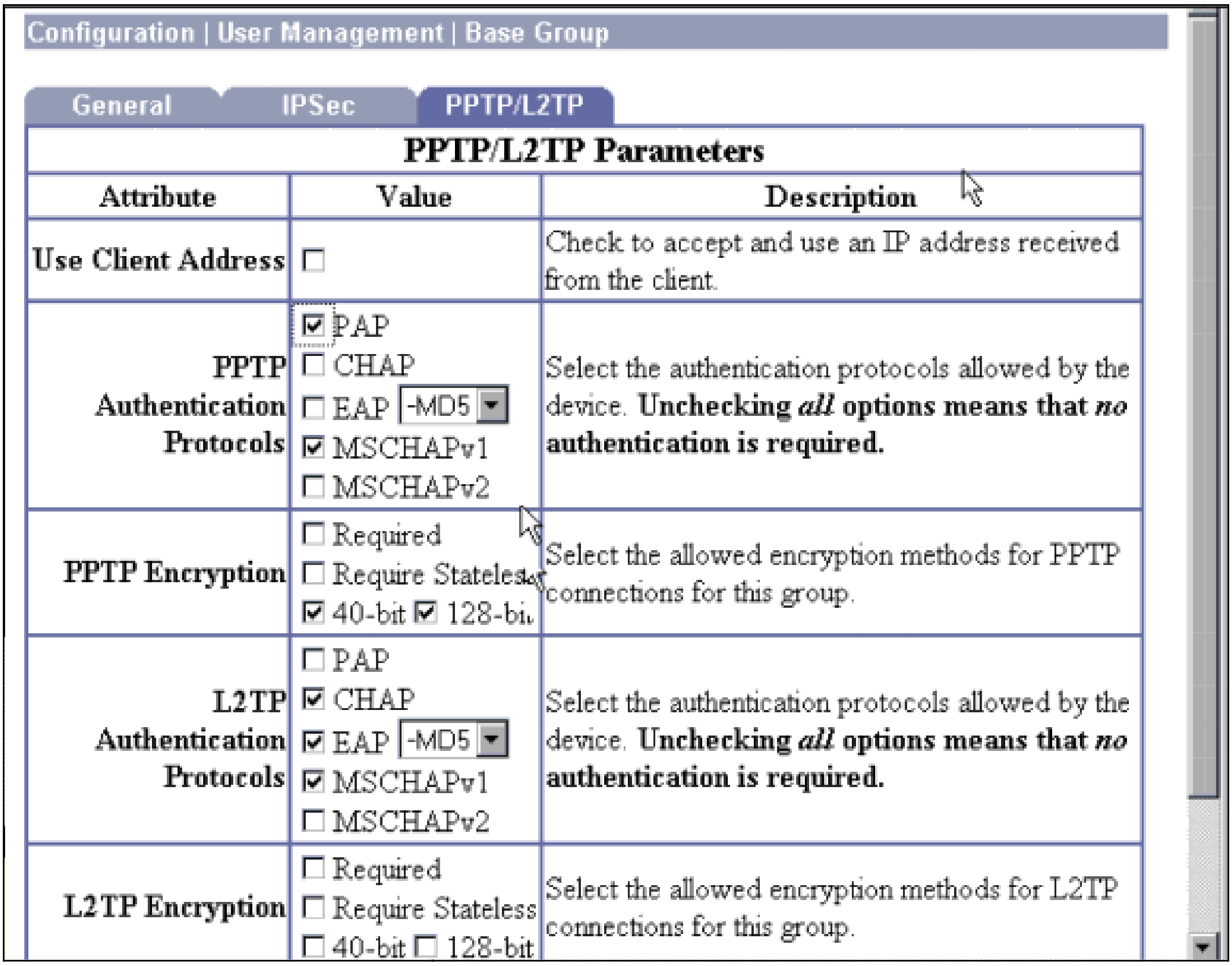
Save Needed

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and add users to the internal database.

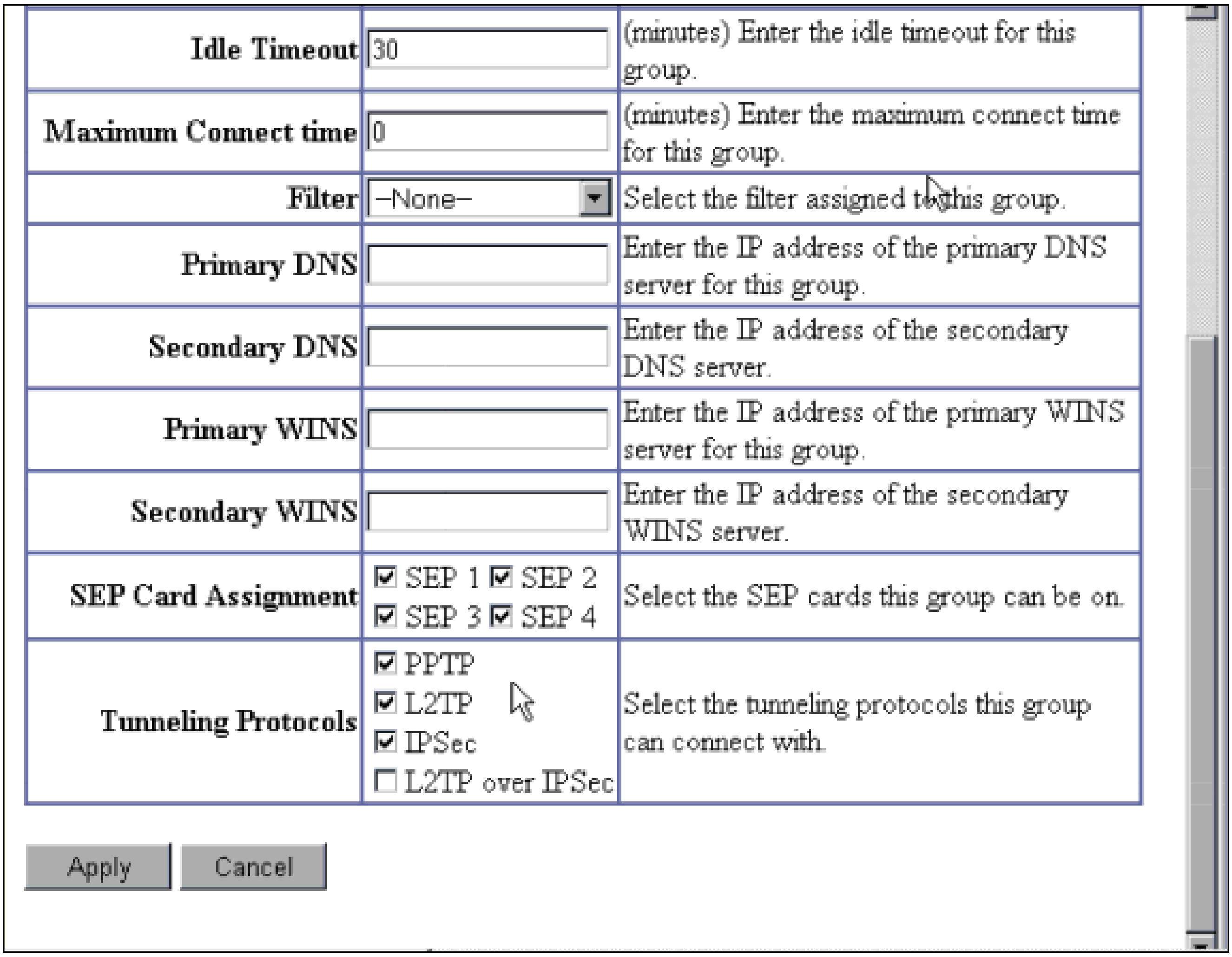
Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

7. 转至**Configuration > User Management > Base Group**，然后选**择PPTP/L2TP选**项卡。在VPN集中器基本组中，确保启用PAP和MSCHAPv1的选项。



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 □ EAP -MD5 ☑ MSCHAPv1 □ MSCHAPv2	Select the authentication protocols allowed by the device. **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.
L2TP Authentication Protocols	□ PAP ☑ CHAP ☑ EAP -MD5 ☑ MSCHAPv1 □ MSCHAPv2	Select the authentication protocols allowed by the device. **Unchecking *all* options means that *no* authentication is required.**
L2TP Encryption	□ Required □ Require Stateless □ 40-bit □ 128-bit	Select the allowed encryption methods for L2TP connections for this group.

8. 选择**General**选项卡，并确保在Tunneling Protocols部分允许PPTP。



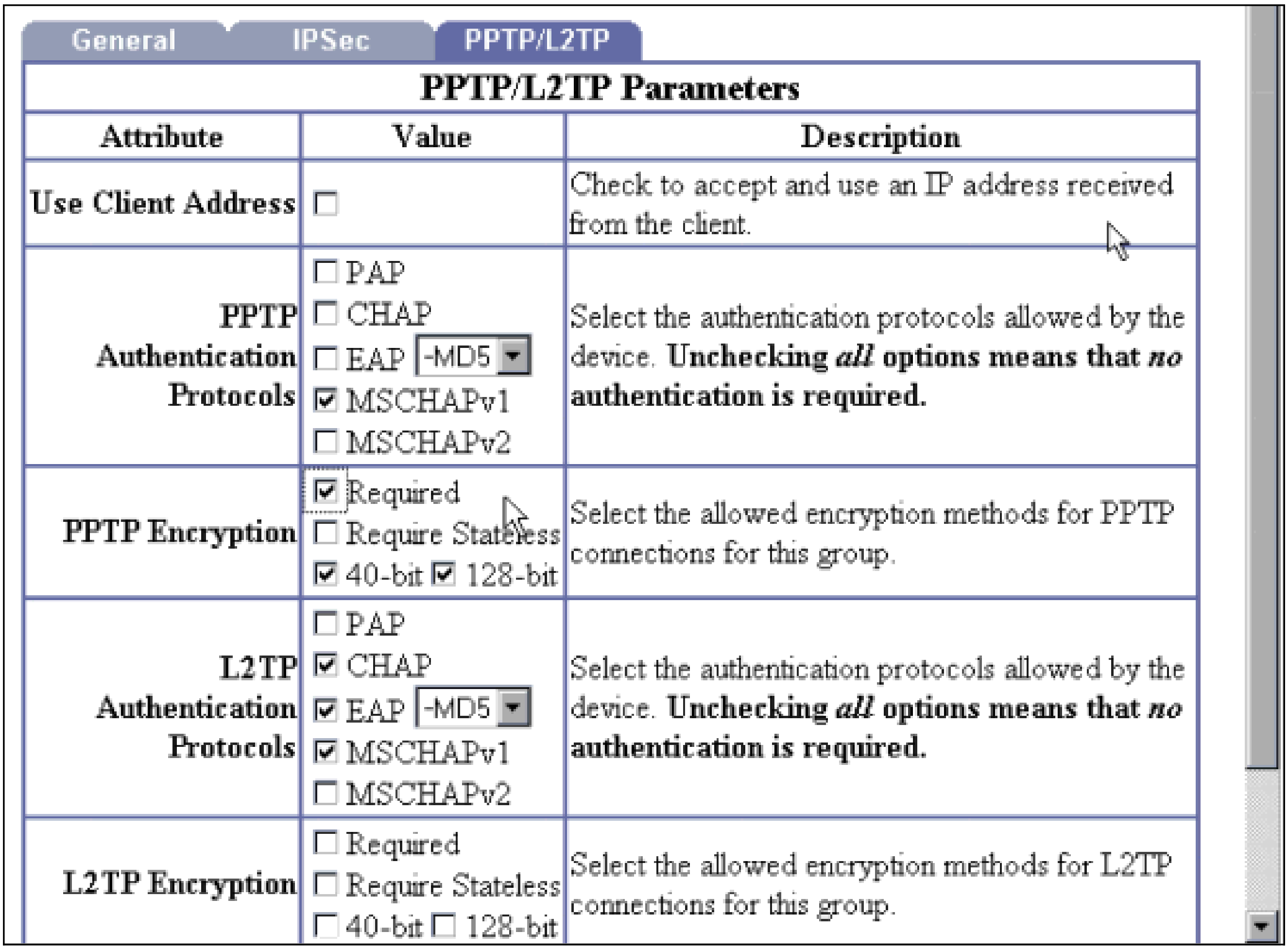
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	–None–	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the 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.

9. 在用于Windows RADIUS的思科安全ACS服务器中测试与用户的PPTP身份验证。如果这不起作用，请参阅“调试”部分。

添加 MPPE（加密）

如果Cisco Secure ACS for Windows RADIUS PPTP身份验证在不加密的情况下工作，您可以将MPPE添加到VPN 3000集中器。

1. 在VPN集中器上，转到**Configuration > User Management > Base Group**。
2. 在“PPTP加密”部分下，选中“必**需”、40位和128位选项**。由于并非所有PC都同时支持40位和128位加密，因此请选中这两个选项以允许协商。
3. 在“PPTP身份验证协议”部分下，选中MSCHAPv1**的选项**。（您已在前面的步骤中配置了用于Windows 2.5的思科安全ACS用户属性以进行加密。
   ）



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 □ EAP -MD5 ☑ MSCHAPv1 □ MSCHAPv2	Select the authentication protocols allowed by the device. **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.
L2TP Authentication Protocols	□ PAP ☑ CHAP ☑ EAP -MD5 ☑ MSCHAPv1 □ MSCHAPv2	Select the authentication protocols allowed by the device. **Unchecking *all* options means that *no* authentication is required.**
L2TP Encryption	□ Required □ Require Stateless □ 40-bit □ 128-bit	Select the allowed encryption methods for L2TP connections for this group.

注意：应识别PPTP客户端，以实现最佳或所需的数据加密和MSCHAPv1（如果有选项）。

增加记账功能

建立身份验证后，可以向VPN集中器添加记帐。转到**Configuration > System > Servers > Accounting Servers**并添加Cisco Secure ACS for Windows服务器。

在用于Windows的思科安全ACS中，记帐记录显示如下。

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,Acct-Session-Id,
   Acct-Session-Time,Service-Type,Framed-Protocol,Acct-Input-Octets,Acct-Output-Octets,
   Acct-Input-Packets,Acct-Output-Packets,Framed-IP-Address,NAS-Port,NAS-IP-Address
03/18/2000,08:16:20,CSNTUSER,Default Group,,Start,8BD00003,,Framed,
   PPP,,,,,1.2.3.4,1163,10.2.2.1
03/18/2000,08:16:50,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,
   PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

验证

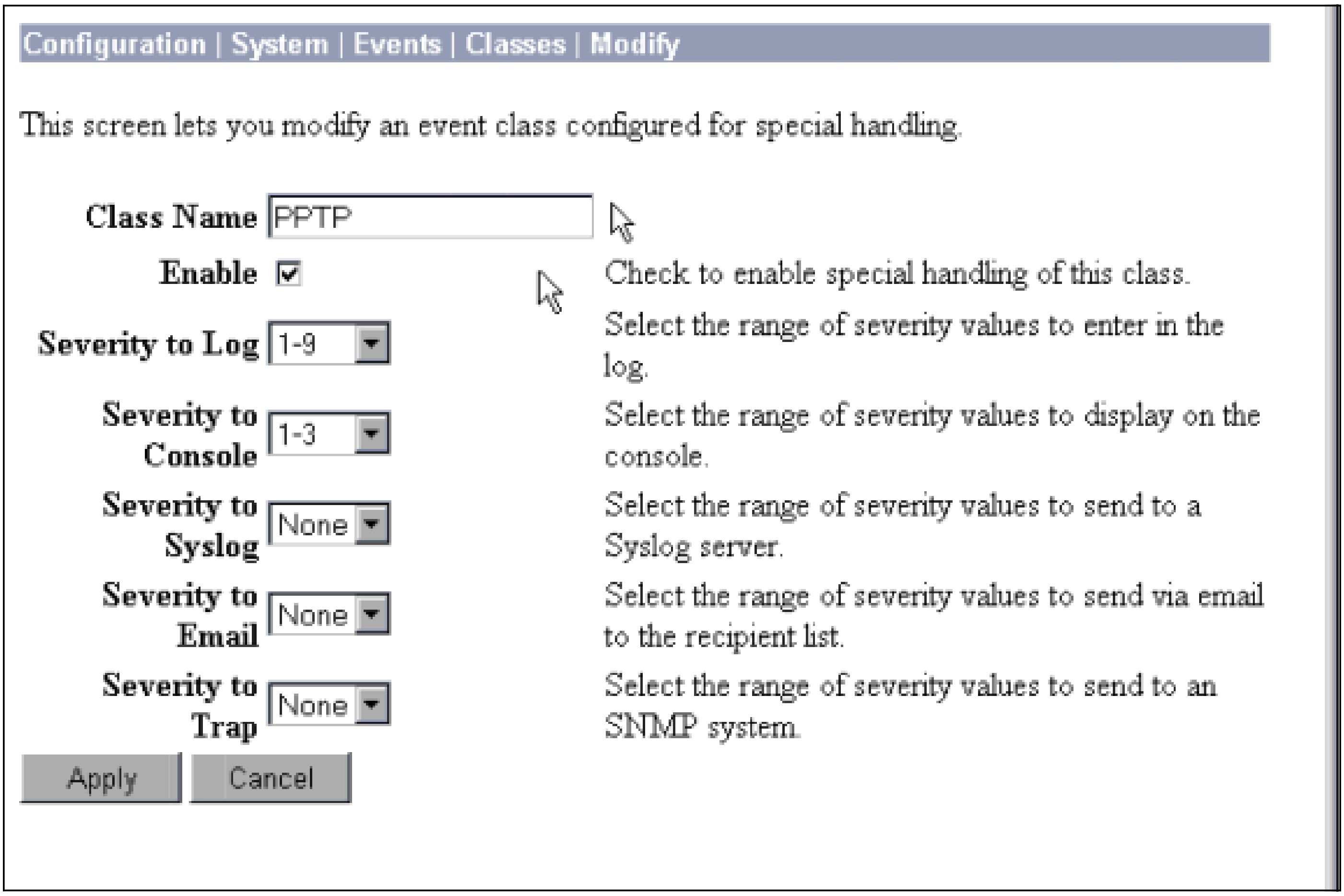
当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

启用调试

如果连接不起作用，您可以通过转到Configuration > System > Events > Classes > Modify将PPTP和AUTH事件类添加到VPN集中器。您还可以添加PPTPDBG、PPTPDECODE、AUTHDBG和AUTHDECODE事件类，但这些选项可能提供太多信息。

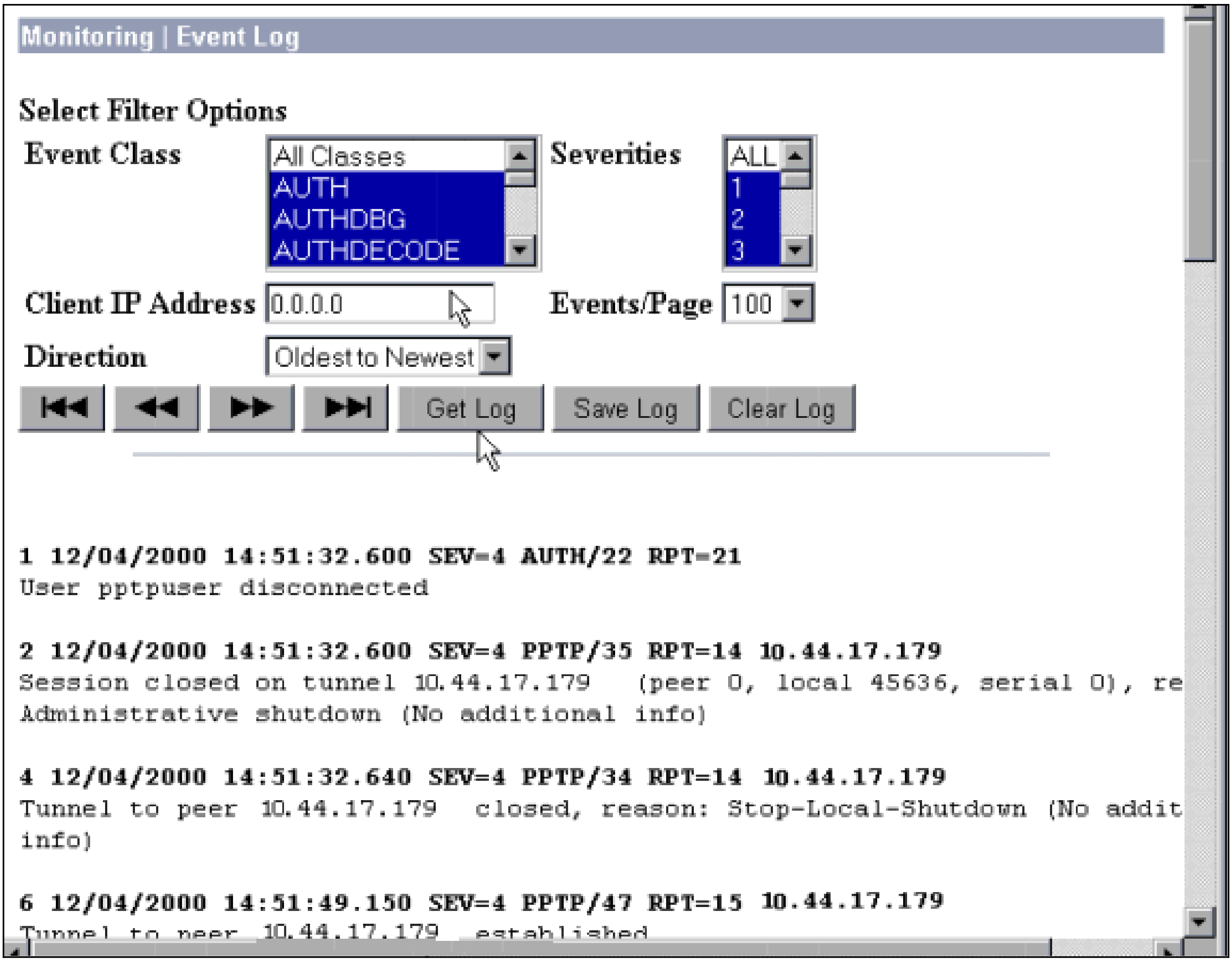


Configuration | System | Events | Classes | Modify

This screen lets you modify an event class configured for special handling.

Class Name	PPTP	
Enable	☑	Check to enable special handling of this class.
Severity to Log	1-9	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.

您可以通过转到Monitoring > Event Log**来检索事件日志。**



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

Direction: Oldest to Newest

```
1 12/04/2000 14:51:32.600 SEV=4 AUTH/22 RPT=21
User pptpuser disconnected

2 12/04/2000 14:51:32.600 SEV=4 PPTP/35 RPT=14 10.44.17.179
Session closed on tunnel 10.44.17.179  (peer 0, local 45636, serial 0), re
Administrative shutdown (No additional info)

4 12/04/2000 14:51:32.640 SEV=4 PPTP/34 RPT=14 10.44.17.179
Tunnel to peer 10.44.17.179  closed, reason: Stop-Local-Shutdown (No addit
info)

6 12/04/2000 14:51:49.150 SEV=4 PPTP/47 RPT=15 10.44.17.179
Tunnel to peer 10.44.17.179  established
```

调试 — 良好身份验证

VPN集中器上的良好调试将类似于以下内容。

```
1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected
```

可能的错误

您可能会遇到如下所示的错误。

Cisco Secure ACS for Windows RADIUS服务器上的用户名或密码错误

- VPN 3000集中器调试输出
  ```
  6 12/06/2000 09:33:03.910 SEV=4 PPTP/47 RPT=21 10.44.17.179
  Tunnel to peer 10.44.17.179 established

  7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
  Session started on tunnel 10.44.17.179

  8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
  Authentication session opened: handle = 23

  9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
  Authentication rejected: Reason = Unspecified
  handle = 23, server = 10.2.2.5, user = baduser

  11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
  User [ baduser ]
  disconnected.. failed authentication ( MSCHAP-V1 )

  12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
  Authentication session closed: handle = 23
  ```
- Cisco Secure ACS for Windows日志输出
  ```
  03/18/2000,08:02:47,Authen failed, baduser,,,CS user
  unknown,,,1155,10.2.2.1
  ```
- 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.
  ```

集中器上选择了“需要MPPE加密”，但Cisco Secure ACS for Windows服务器没有为MS-CHAP-MPPE-Keys和MS-CHAP-MPPE-Types配置

- VPN 3000集中器调试输出如果AUTHDECODE（1-13严重性）和PPTP调试（1-9严重性）打开，日志显示Cisco Secure ACS for Windows服务器未从服务器（部分日志）access-accept中发送供应商特定属性26(0x1A)。
  ```
  2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0 RPT=545
  0000: 024E002C 80AE75F6 6C365664 373D33FE     .N.,..u.l6Vd7=3.
  0010: 6DF74333 501277B2 129CBC66 85FFB40C     m.C3P.w....f....
  0020: 16D42FC4 BD020806 FFFFFFFF                 ../.........

  2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
  User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
  or auth protocol will not support encrypt.
  ```
- Cisco Secure ACS for Windows日志输出显示无故障。
- 用户看到的消息
  ```
  Error 691: The computer you have dialed in to has denied access because
  the username and/or password is invalid on the domain.
  ```

相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPSec 支持页面
- Cisco Secure ACS for Windows 支持页
- RADIUS 支持页
- PPTP 支持页

- RFC 2637：点对点隧道协议 (PPTP)
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems