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集中器支持本地窗口客户端的点对点隧道协议(PPTP)建立隧道的方法。集中器支持40位和128-bit加密受保护的可靠连接的。本文描述如何配置在VPN 3000集中器的PPTP有RADIUS验证的Cisco Secure ACS for Windows的。

参考配置Cisco Secure PIX防火墙使用PPTP配置对PIX的PPTP连接。

参考配置Cisco Secure ACS for Windows路由器PPTP验证设置PC连接到路由器;对思科安全访问控制系统(ACS) 3.2的此提供用户认证Windows服务器的，在您允许用户到网络前。

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

本文假设，本地PPTP验证在添加Cisco Secure ACS for Windows RADIUS验证前工作。请参阅如何配置有本地认证的VPN 3000集中器PPTP关于本地PPTP验证的更多信息。请参考的需求和限制完整列表，当是支持PPTP加密Cisco VPN 3000集中器？

使用的组件

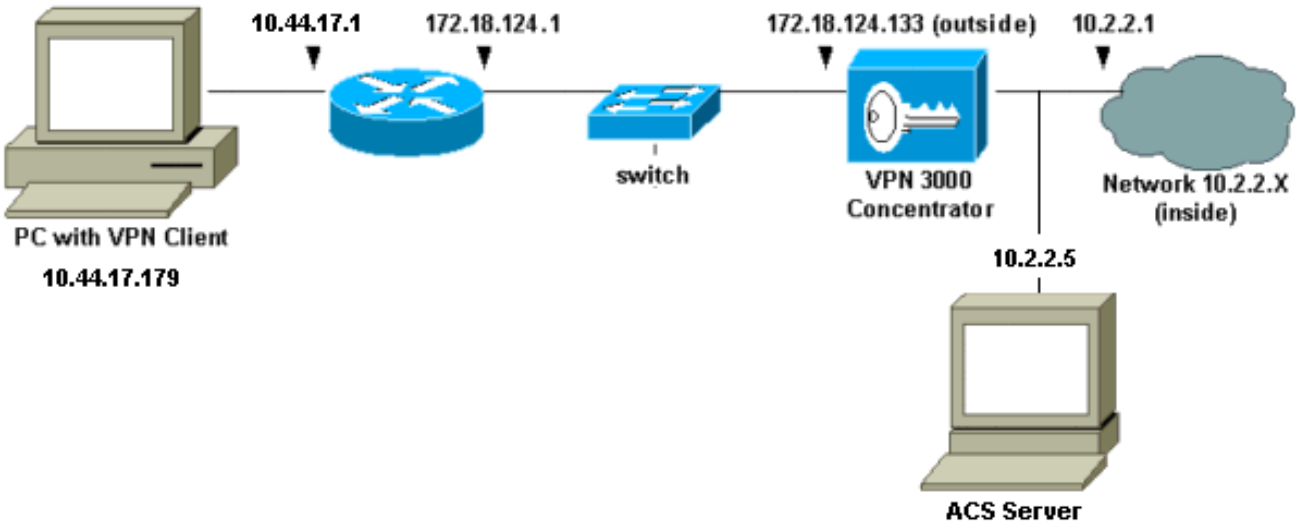
本文档中的信息基于以下软件和硬件版本。

- Cisco Secure ACS for Windows版本2.5和以上
- VPN 3000集中器版本2.5.2.C和以上(此配置验证与版本4.0.x。)

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。

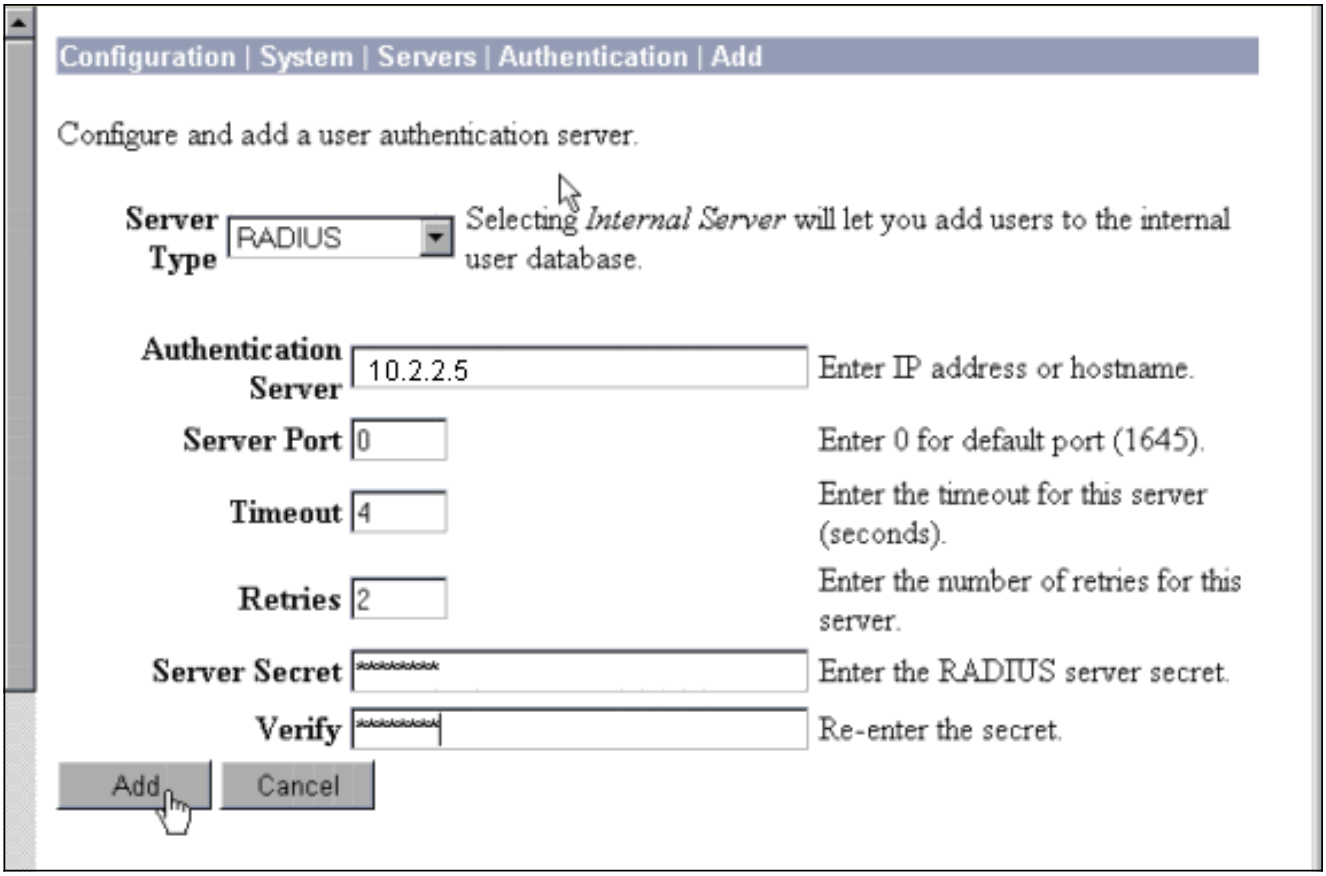


配置 VPN 3000 集中器

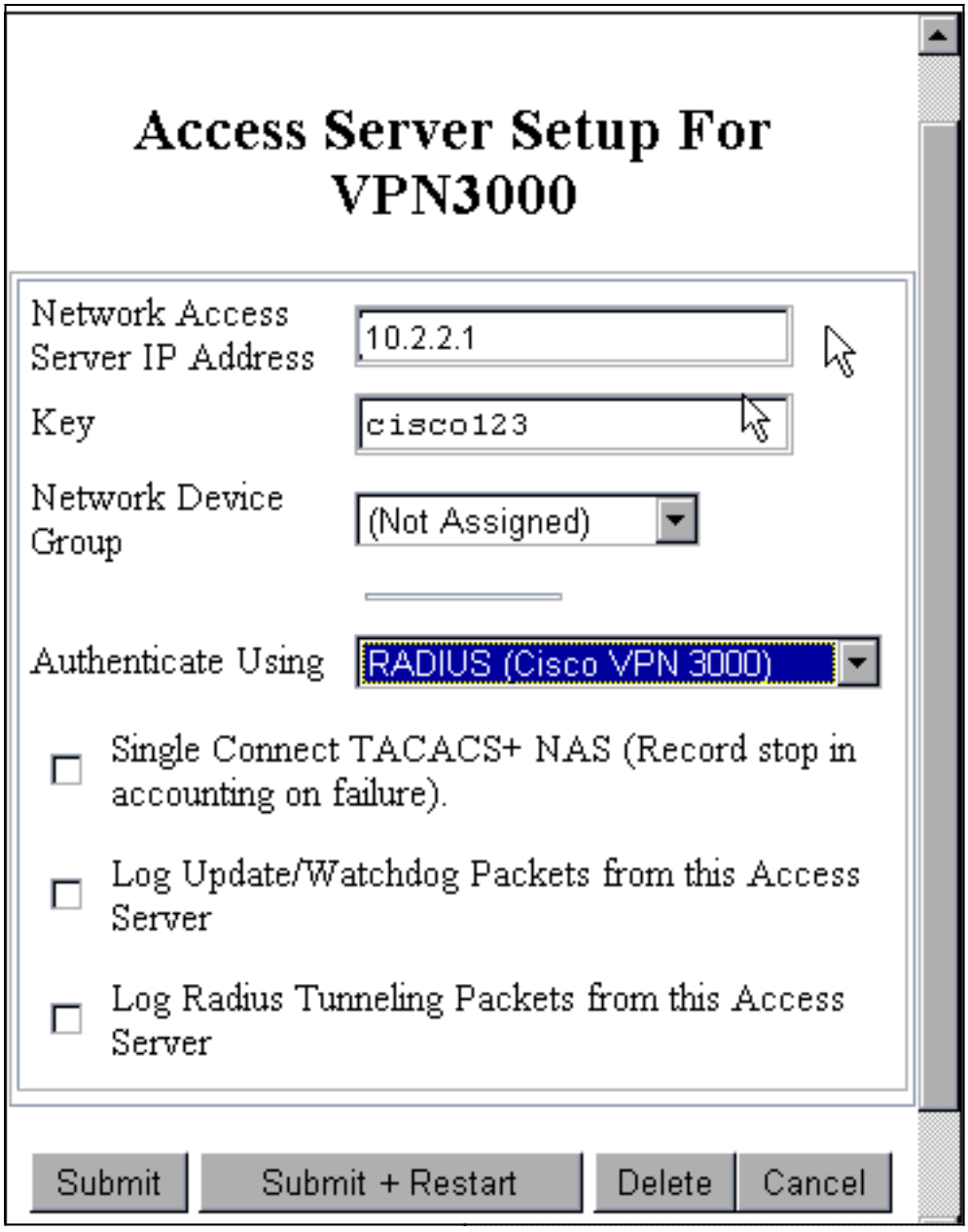
添加和配置Cisco Secure ACS for Windows

遵从这些步骤配置VPN集中器使用Cisco Secure ACS for Windows。

1. 在VPN 3000集中器上，请去**Configuration > System > Servers > Authentication Servers**并且添加Cisco Secure ACS for Windows服务器并且锁上("cisco123"在本例中)。

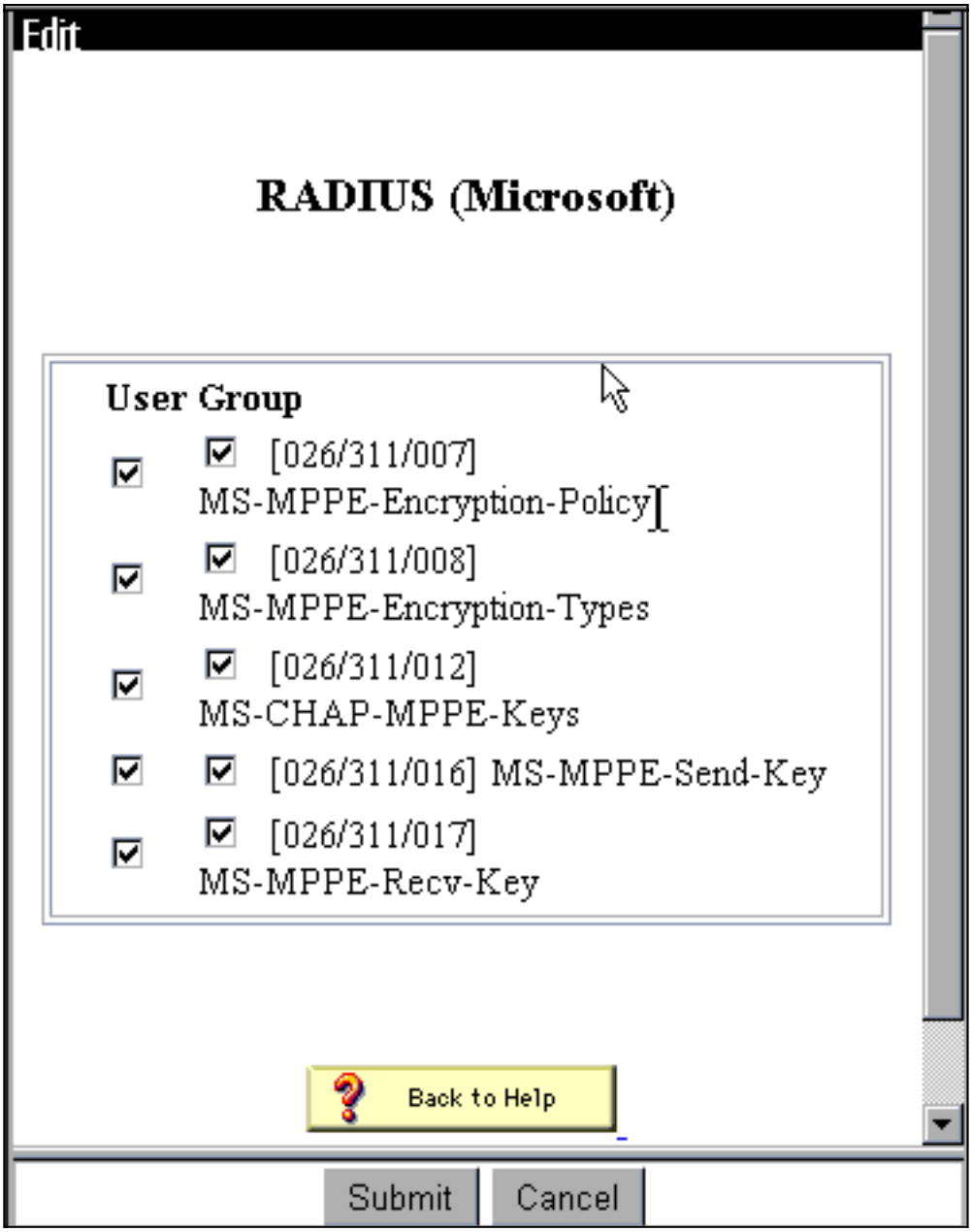


2. 在Cisco Secure ACS for Windows，请添加VPN集中器到ACS服务器网络配置，并且识别词典

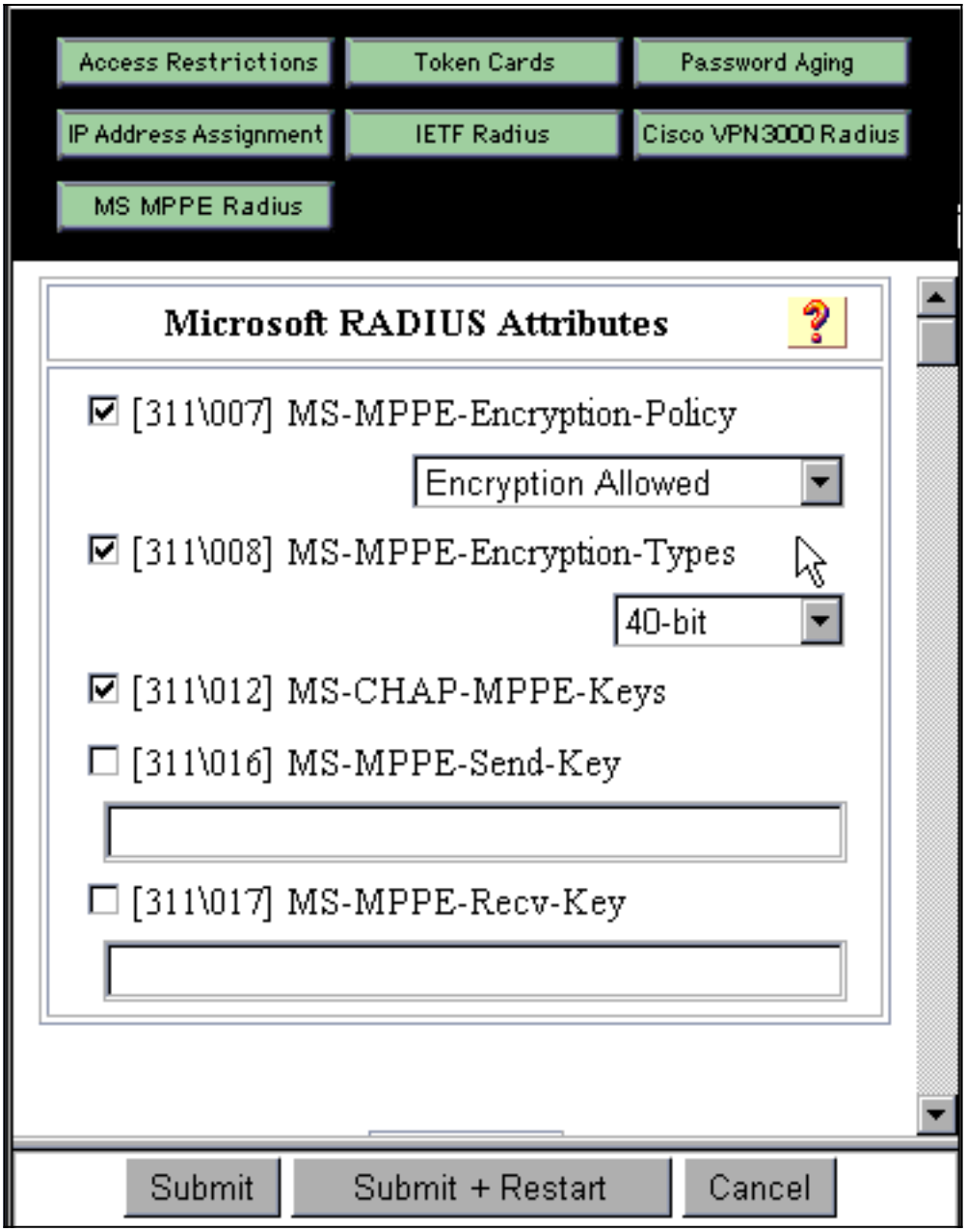


类型。

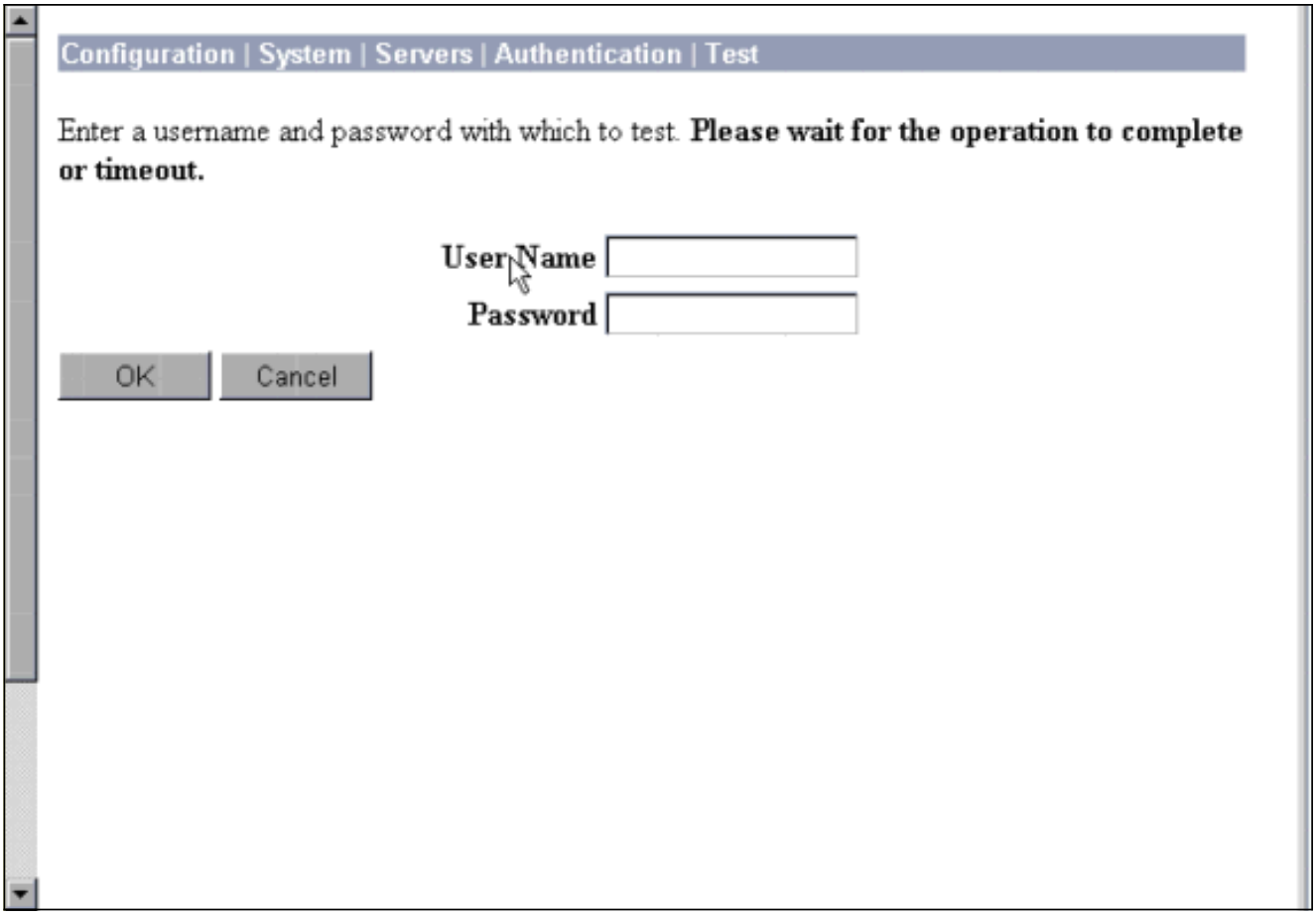
3. 在Cisco Secure ACS for Windows，请去**Interface Configuration > RADIUS (Microsoft)**并且检查Microsoft点对点加密(MPPE)属性，以便属性在组接口出现。



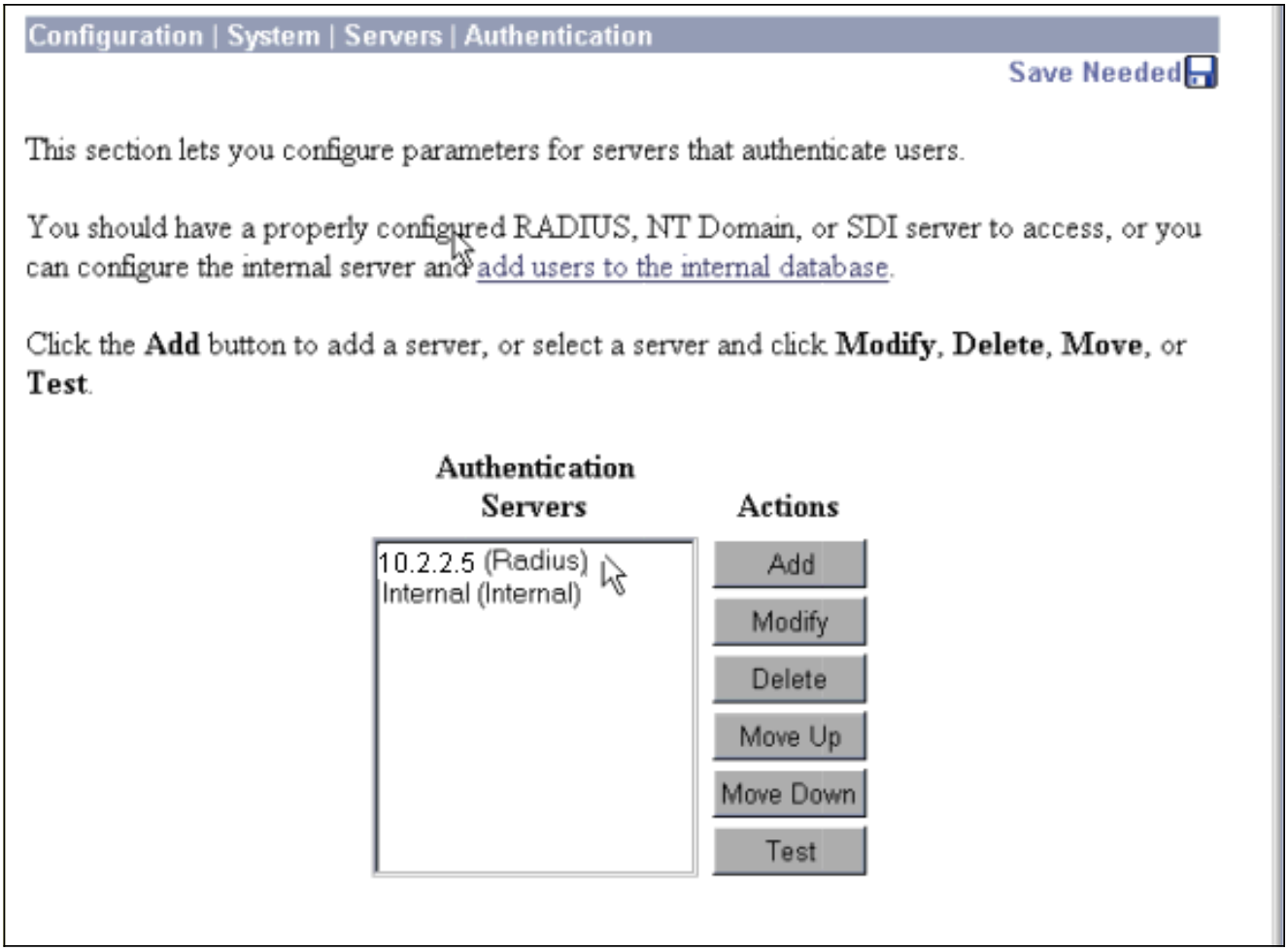
4. 在Cisco Secure ACS for Windows，请添加一个用户。在用户组，请添加MPPE Microsoft RADIUS属性，万一以后需要加密。



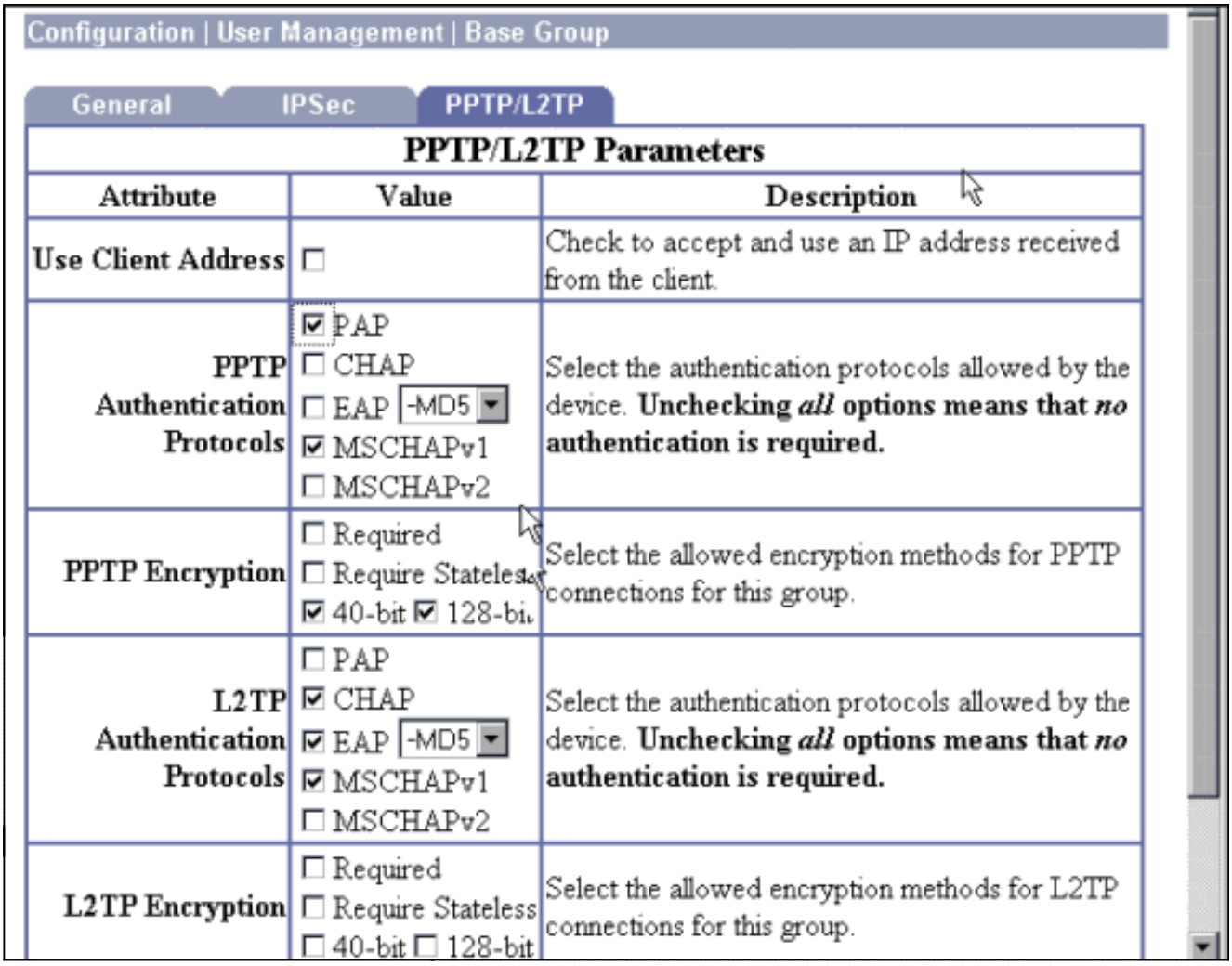
5. 在VPN 3000集中器上，请去**Configuration > System > Servers > Authentication Servers**。选择从列表的一个认证服务器，然后选择**测验**。测试从VPN集中器的验证到Cisco Secure ACS for Windows服务器通过输入用户名和密码。在成功验证， VPN集中器应该显示" Authentication Successful "消息。Cisco Secure ACS for Windows的失败是登陆的**报告和活动>失败的尝试**。在默认安装，这些报告存储关于在C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed尝试的磁盘。



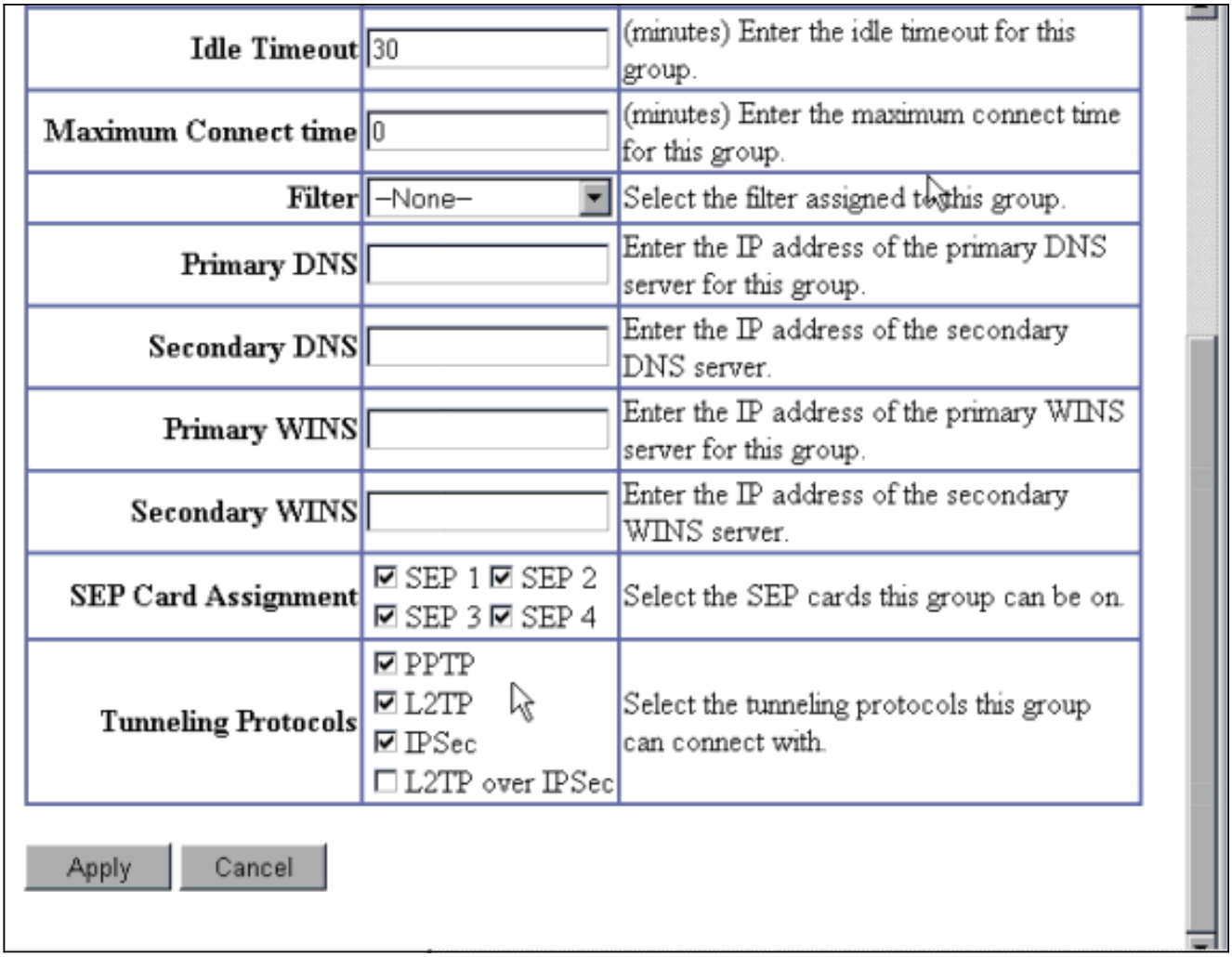
6. 因为您当前验证验证从PC到VPN集中器工作和从集中器到Cisco Secure ACS for Windows服务器，您能重新配置VPN集中器派遣PPTP用户到Cisco Secure ACS for Windows RADIUS通过移动Cisco Secure ACS for Windows服务器对服务器列表的顶部。要执行此在VPN集中器，请去**Configuration > System > Servers > Authentication Servers**。



7. 去**Configuration > User Management > Base Group**并且选择**PPTP/L2TP**选项卡。在VPN集中器基本组中，请保证PAP和MSCHAPv1的选项启用。



8. 选择**常规选项卡**并且保证PPTP在Tunneling Protocols部分允许。

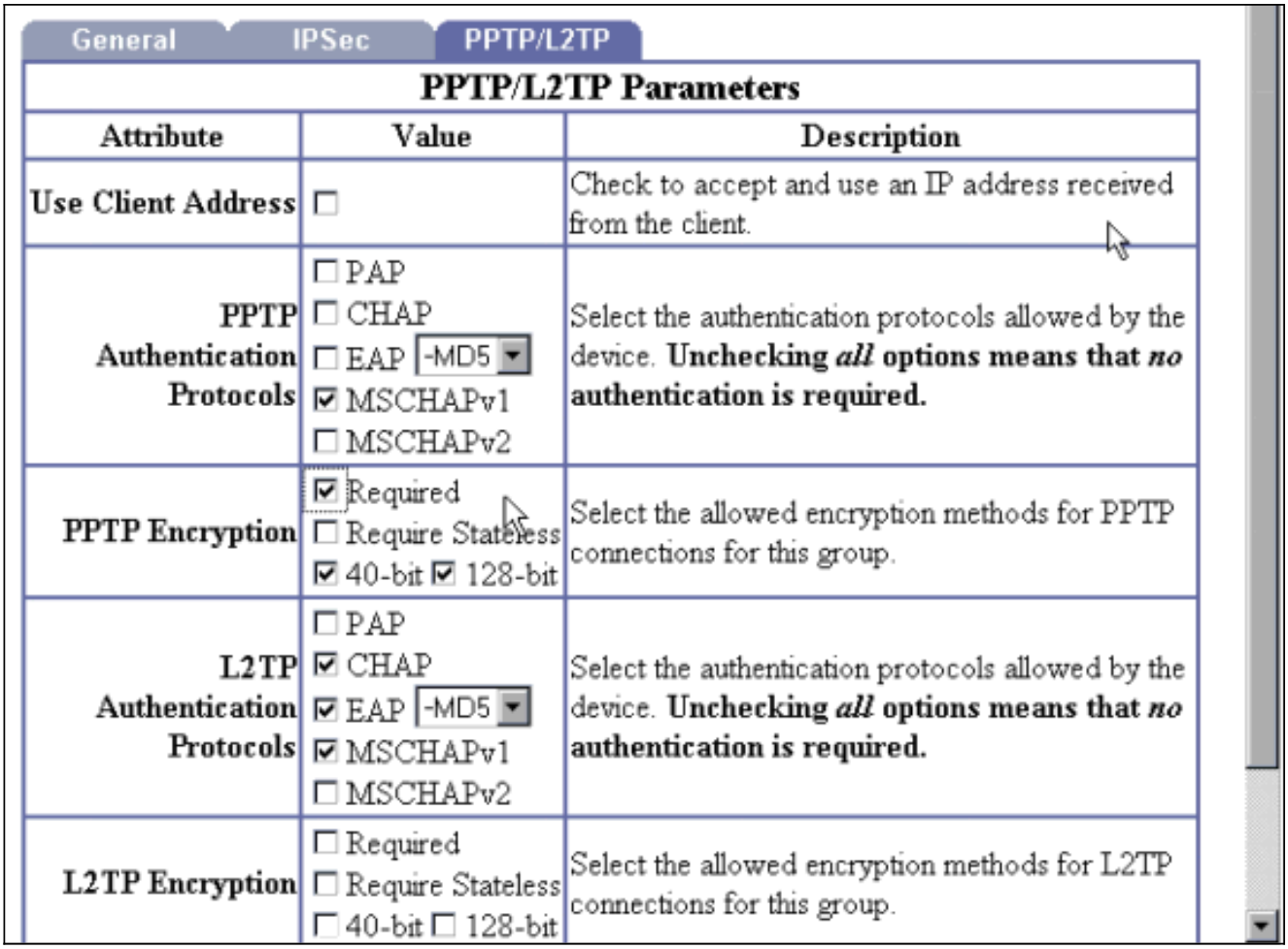


9. 测试与用户的PPTP验证Cisco Secure ACS for Windows RADIUS服务器的。如果这不工作，请参阅Debugging部分。

添加 MPPE（加密）

如果Cisco Secure ACS for Windows RADIUS PPTP验证工作，不用加密，您能添加MPPE到VPN 3000集中器。

1. 在VPN集中器上，请去**Configuration > User Management > Base Group**。
2. 在PPTP加密的部分下，请检查选项**需要的**， 40**位**和**128-bit**。因为不是所有的PCs支持40位和128-bit加密，检查两个选项允许协商。
3. 在PPTP身份验证协议的部分下，请检查选项**MSCHAPv1**。(您已经配置Cisco Secure ACS for Windows加密的2.5用户属性在一个更加早期的步骤。
)



General | IPSec | 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 ☐ 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： PPTP客户端应该为最佳被认可或所需的数据加密和MSCHAPv1 (如果选项)。

增加记账功能

在您设立了验证后，您能添加核算到VPN集中器。去**Configuration > System > Servers > Accounting Servers**并且添加Cisco Secure ACS for Windows服务器。

在Cisco Secure ACS for Windows，计费记录出现如下。

```
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

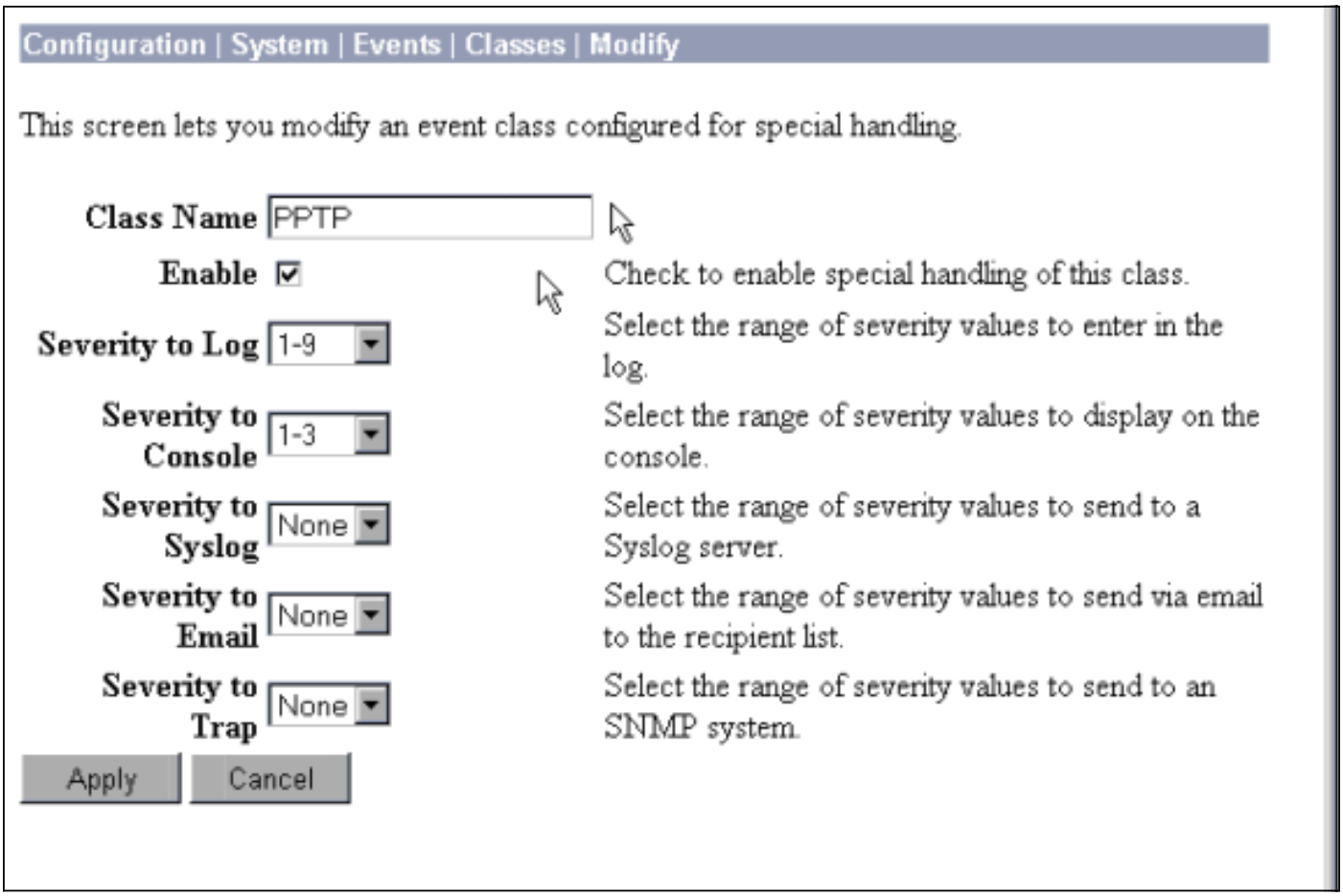
当前没有可用于此配置的验证过程。

故障排除

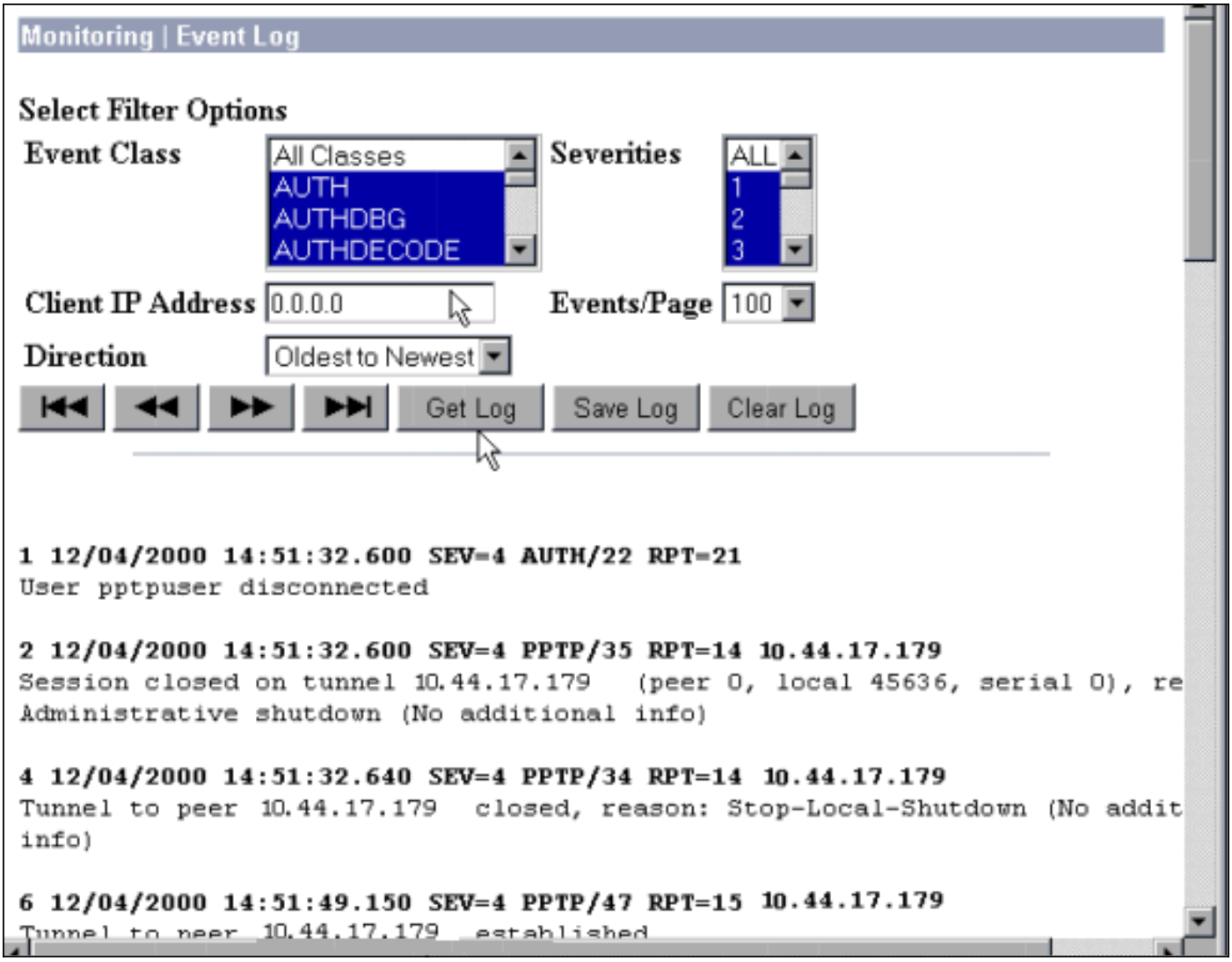
本部分提供的信息可用于对配置进行故障排除。

启用调试

如果连接不工作，您能添加PPTP和认证事件类到VPN集中器通过去**Configuration > System > Events > Classes > Modify**。您能也添加PPTPDBG、PPTPDECODE、AUTHDBG和AUTHDECODE事件类，但是这些选项可能提供许多信息。



您能通过去检索事件日志**Monitoring > Event Log**。



调试-成功验证

在VPN集中器的成功调试将显出类似于以下。

```
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

您可以遇到可能的错误如下所示。

用户名不正确或密码在Cisco Secure ACS for Windows RADIUS服务器

- VPN 3000集中器debug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.
```

“要求的MPPE加密”在集中器选择，但是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debug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服务器不发送在access-accept的供应商专用属性26 (0x1A)从服务器(部分日志)。
```
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日志输出不显示失败。
- 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