# Configurando o VPN 3000 concentrator PPTP com autenticação RADIUS do Cisco Secure ACS for Windows

## Índice



## Introdução

O Cisco VPN 3000 Concentrator apoia o método de tunelamento do protocolo de túnel Point-to-Point (PPTP) para clientes das janelas nativas. Os suportes de concentrador 40-bit e criptografia do 128-bit para uma conexão confiável fixada. Este original descreve como configurar o PPTP em um concentrador VPN 3000 com o Cisco Secure ACS for Windows para a autenticação RADIUS.

Refira configurar o firewall PIX segura Cisco para usar o PPTP para configurar conexões PPTP ao PIX.

Refira configurar a autenticação de PPTP do roteador do Cisco Secure ACS for Windows para estabelecer uma conexão PC ao roteador; isto fornece a autenticação de usuário ao Cisco Secure Access Control System (ACS) 3.2 para o server de Windows antes que você permita o usuário na rede.

## Antes de Começar

### Convenções

Para obter mais informações sobre das convenções de documento, veja as convenções dos dicas técnicas da Cisco.

## Pré-requisitos

Este original supõe que a autenticação de PPTP local está trabalhando antes de adicionar a autenticação RADIUS do Cisco Secure ACS for Windows. Veja por favor como configurar o VPN 3000 concentrator PPTP com autenticação local para obter mais informações sobre da autenticação de PPTP local. Para uma lista completa das exigências e das limitações, refira por favor quando é a criptografia de PPTP apoiada em um Cisco VPN 3000 Concentrator?

## Componentes Utilizados

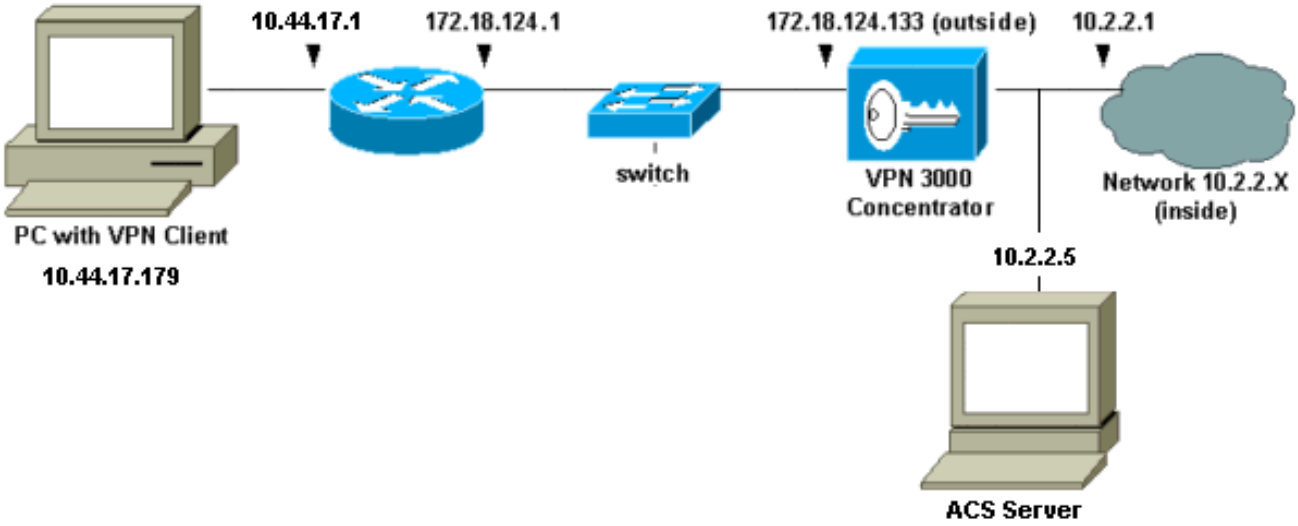
As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Versões 2.5 e mais recente do Cisco Secure ACS for Windows
- Versões do concentrador 2.5.2.C VPN 3000 e mais tarde (esta configuração foi verificada com versão 4.0.x.)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você está trabalhando em uma rede viva, assegure-se de que você compreenda o impacto potencial do comando any antes do usar.

## Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.

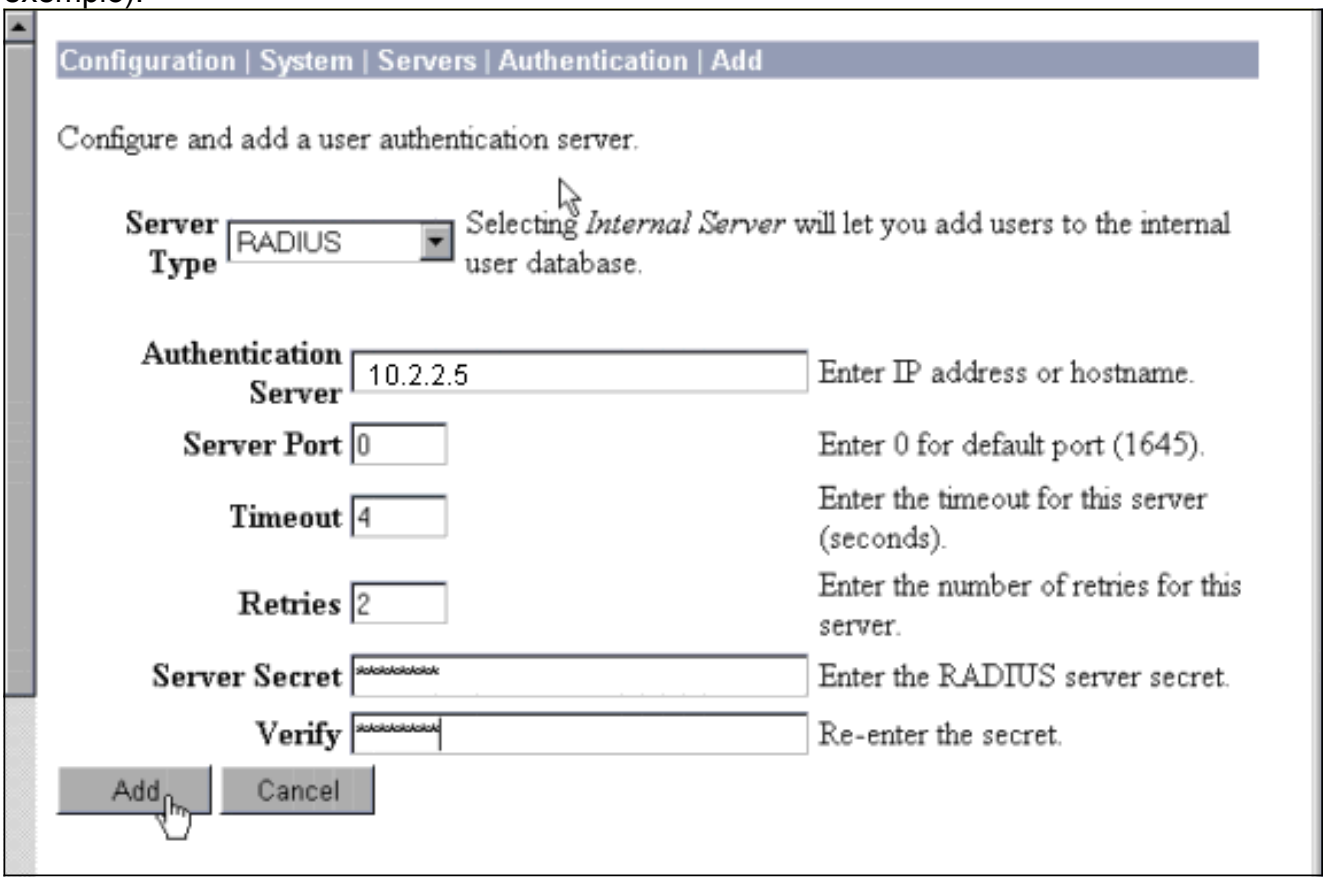



# Configurando o VPN 3000 Concentrator

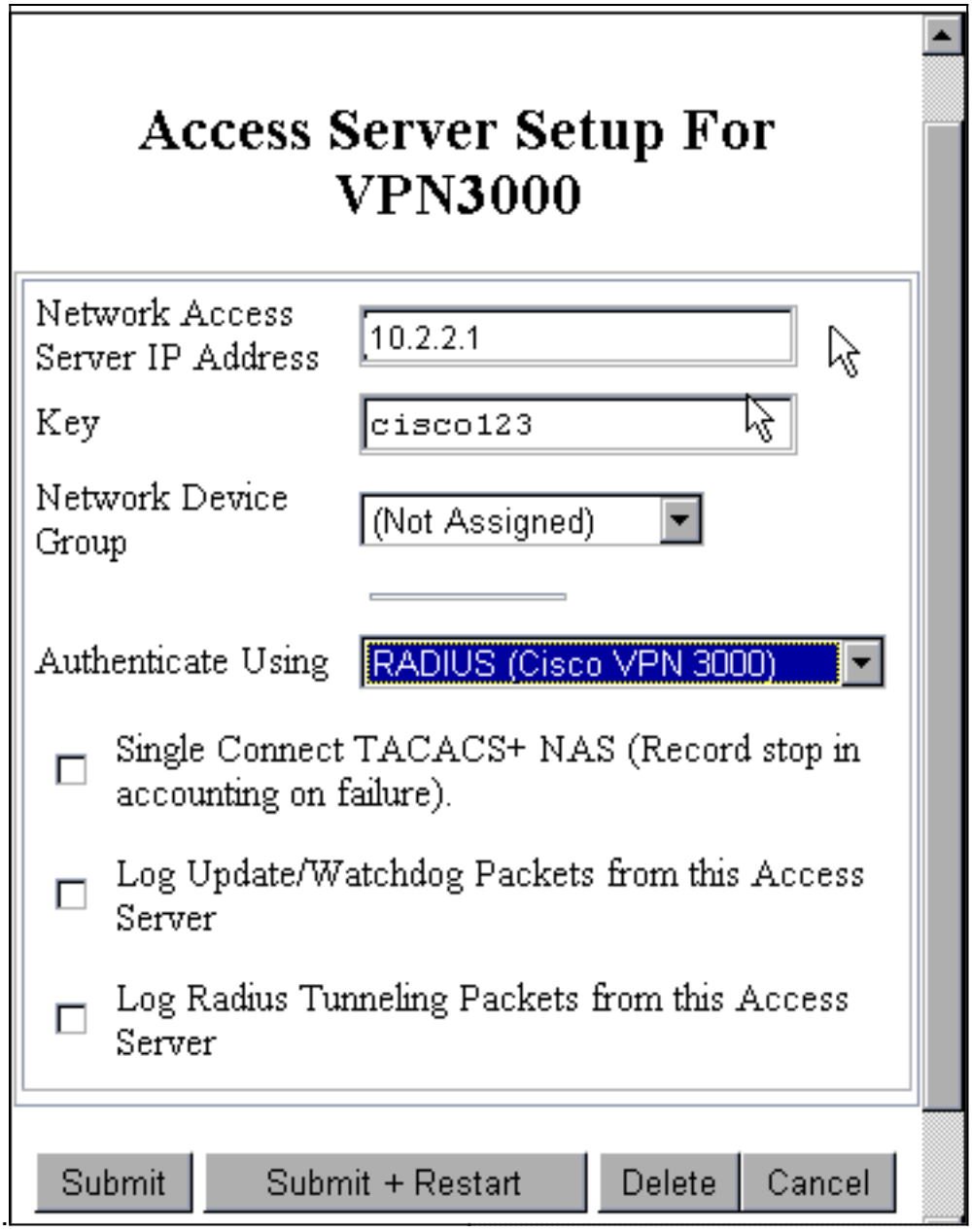
## Adicionando e configurando o Cisco Secure ACS for Windows

Siga estas etapas para configurar o concentrador VPN para usar o Cisco Secure ACS for Windows.

1. No concentrador VPN 3000, vá ao **Configuration > System > aos server > aos Authentication Server** e adicionar o server do Cisco Secure ACS for Windows e a chave ("cisco123" neste exemplo).

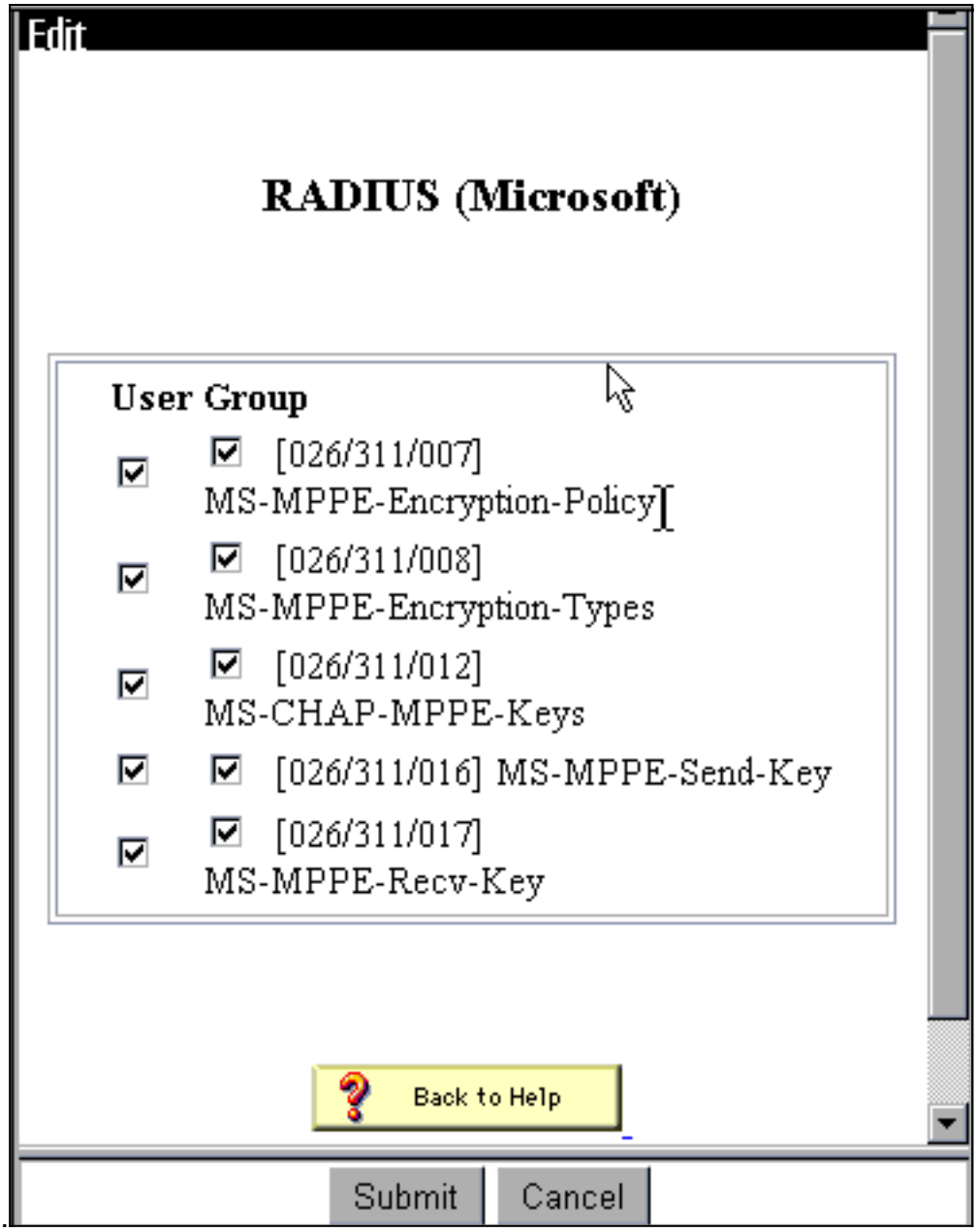



2. No Cisco Secure ACS for Windows, adicionar o concentrador VPN à configuração de rede do servidor ACS, e identifique o tipo de



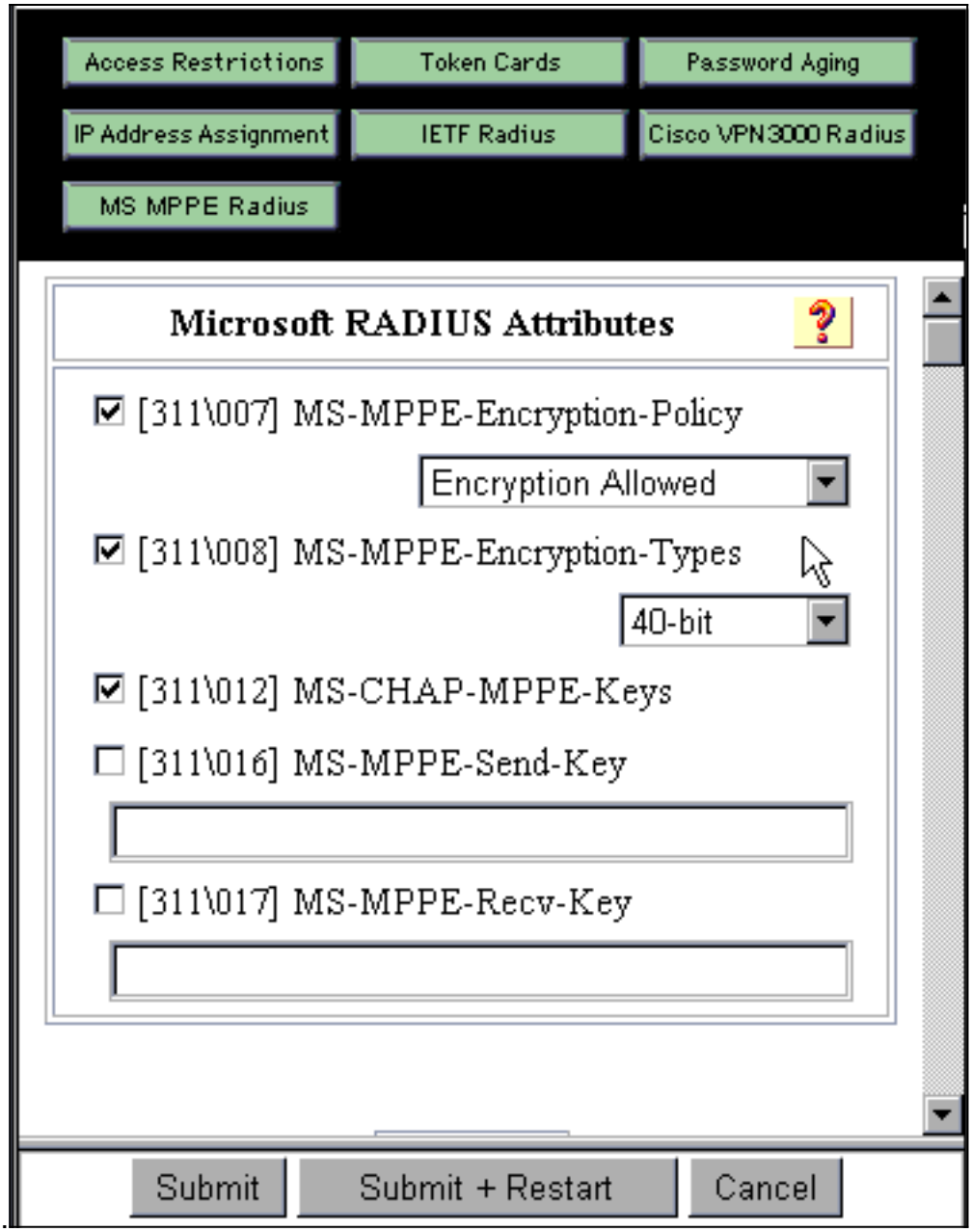

dicionário.

3. No Cisco Secure ACS for Windows, vá a **Interface Configuration > Radius (Microsoft)** e verifique os atributos da criptografia Point-to-Point microsoft (MPPE) de modo que os atributos apareçam na interface de



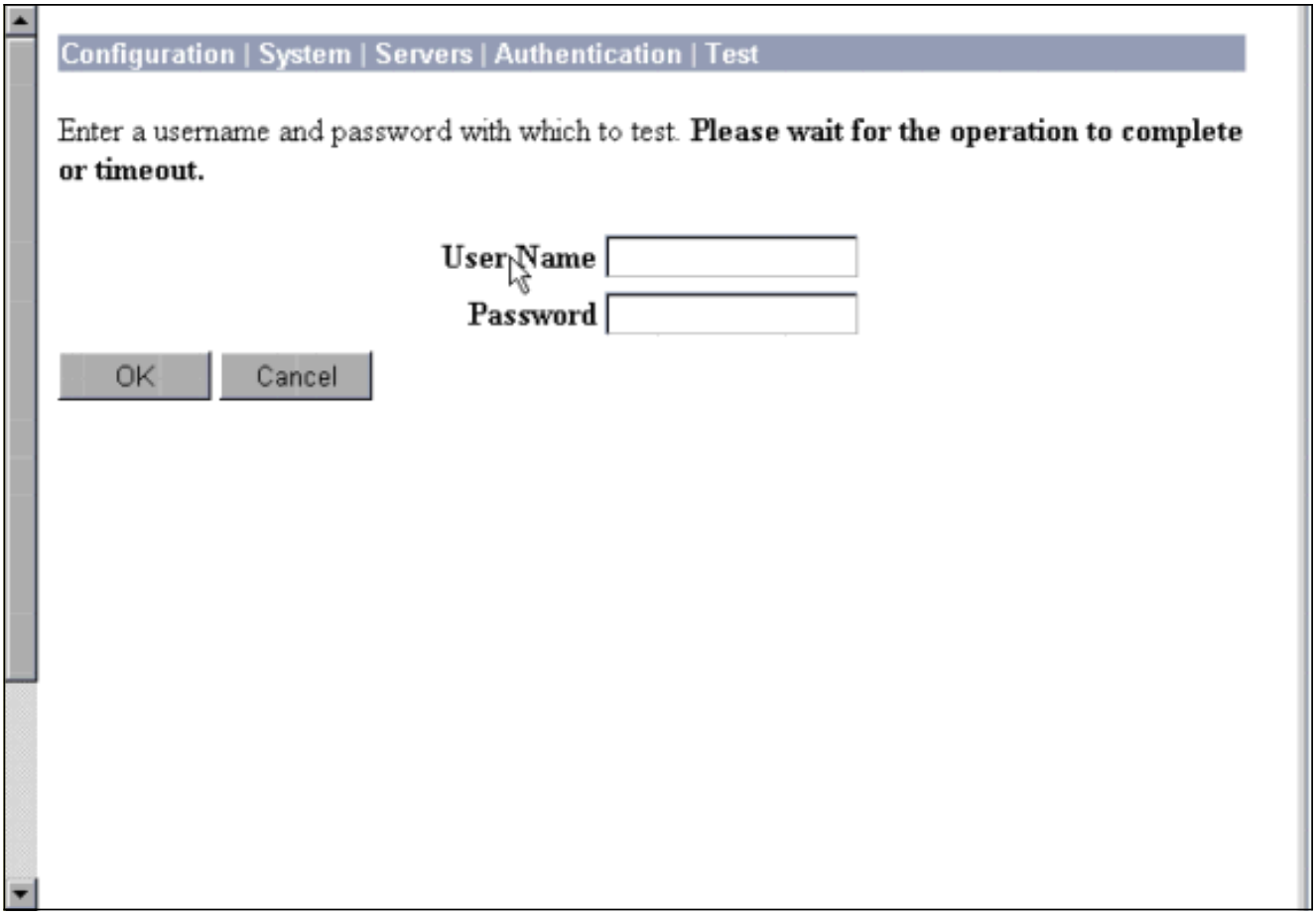

grupo.

4. No Cisco Secure ACS for Windows, adicionar um usuário. No grupo de usuário, adicionar os atributos MPPE (Microsoft RADIUS), caso que você exige a criptografia mais

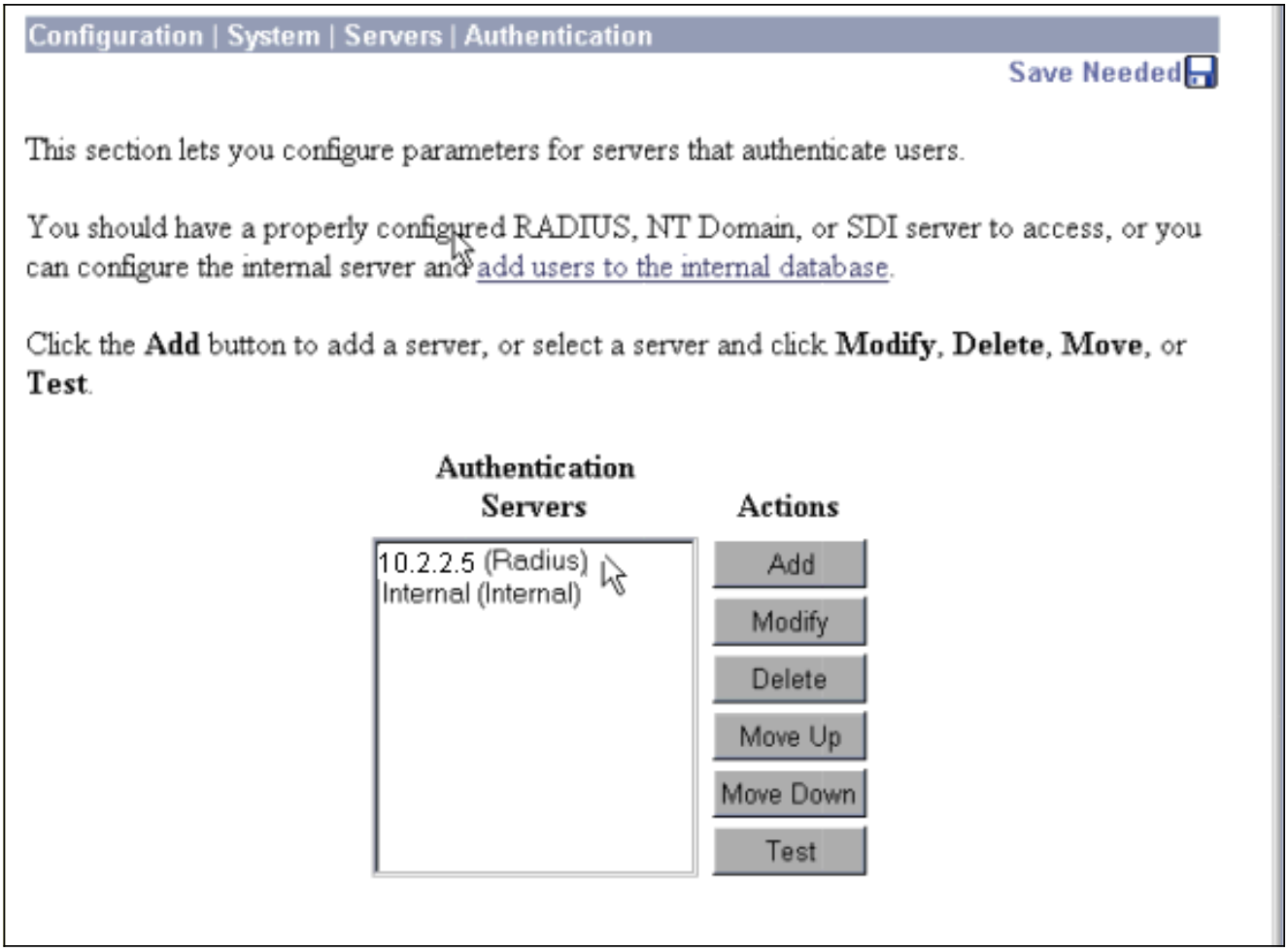


tarde.

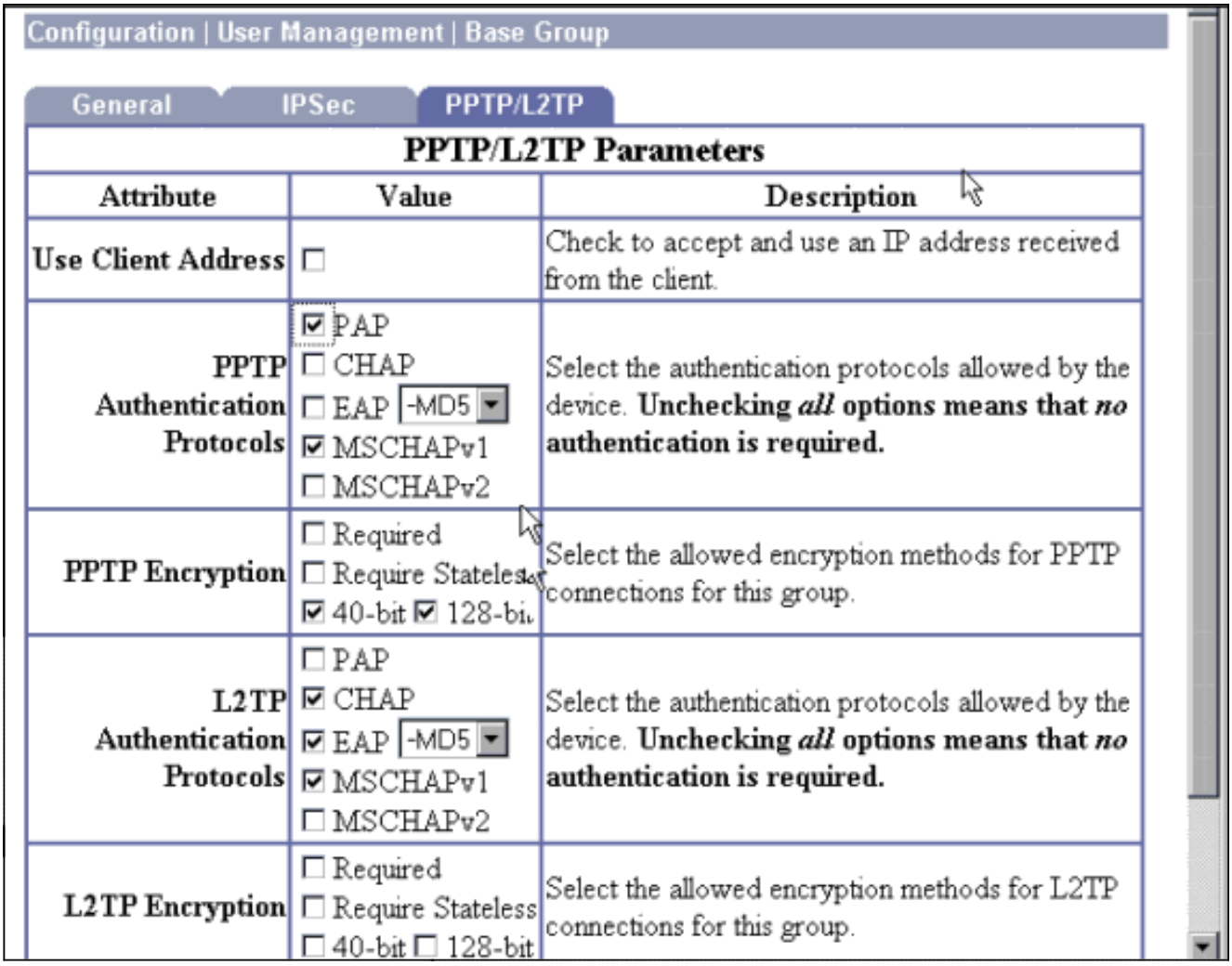
5. No concentrador VPN 3000, vá ao **Configuration > System > aos server > aos Authentication Server**. Selecione um Authentication Server da lista, e selecione então o **teste**. Autenticação de teste do concentrador VPN ao server do Cisco Secure ACS for Windows incorporando um nome de usuário e senha.Em uma boa autenticação, o concentrador VPN deve mostrar a uma “autenticação” a mensagem bem sucedida. As falhas no Cisco Secure ACS for Windows são **relatórios e atividade > falhas de tentativa** entrados. Em um padrão instale, estes relatórios são armazenados no disco em tentativas de C:\Program Files\CiscoSecure ACS
v2.5\Logs\Failed.



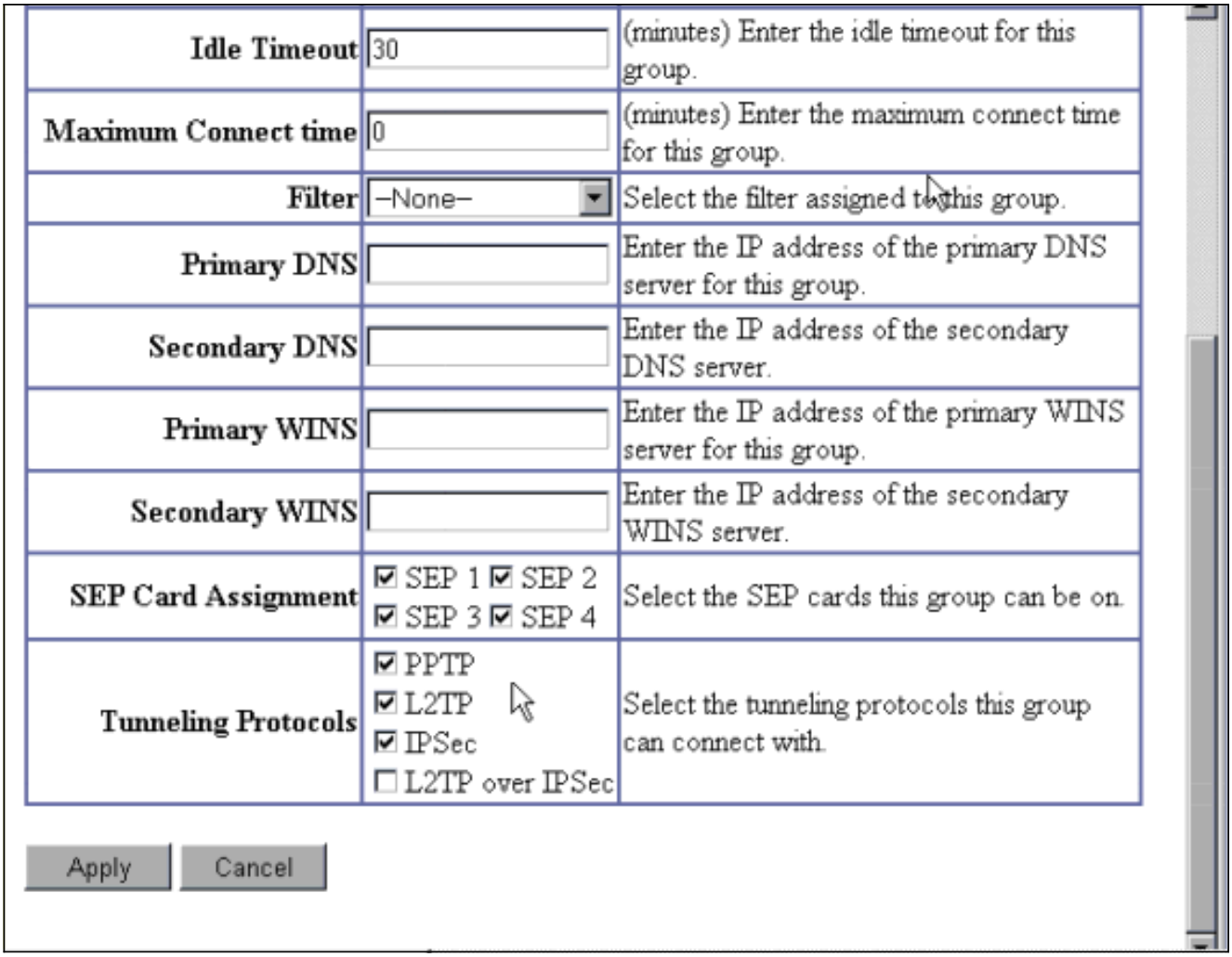

6. Desde que você tem verificado agora a autenticação do PC aos trabalhos do concentrador VPN e do concentrador ao server do Cisco Secure ACS for Windows, você pode reconfigurar o concentrador VPN para enviar usuários PPTP ao RAIO do Cisco Secure ACS for Windows movendo o server do Cisco Secure ACS for Windows para a parte superior da lista de servidor. Para fazer isto no concentrador VPN, vá ao **Configuration > System > aos server > aos Authentication**
**Server**.




7. Vá ao **configuration > user management > ao grupo base** e selecione a aba **PPTP/L2TP**. No grupo base do concentrador VPN, assegure-se de que as opções para o PAP e o MSCHAPv1 estejam
permitidas.




8. Selecione o **tab geral** e assegure-se de que o PPTP esteja permitido na seção dos protocolos de
tunelamento.

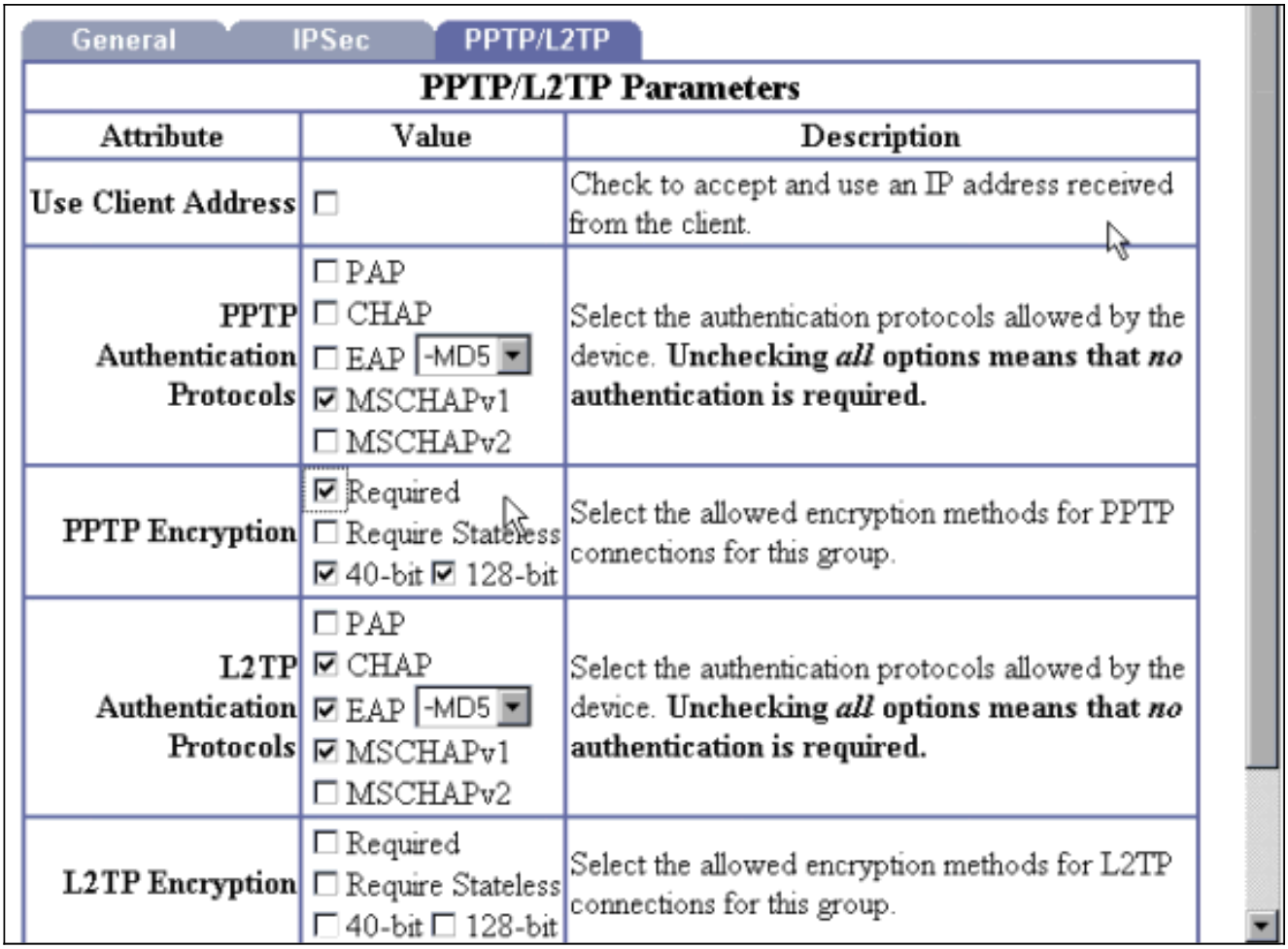



9. Teste a autenticação de PPTP com o usuário no servidor Radius do Cisco Secure ACS for Windows. Se isto não trabalha, para satisfazer veja a seção de debugging.

## Adicionando MPPE (Criptografia)

Se a autenticação de PPTP do RAIO do Cisco Secure ACS for Windows trabalha sem criptografia, você pode adicionar o MPPE ao concentrador VPN 3000.

1. No concentrador VPN, vá ao **configuration > user management > ao grupo base**.
2. Sob a seção para a criptografia de PPTP, verifique as opções para ver se há **exigido**, **40-bit**, e **128-bit**. Desde que não todos os PCes apoiam 40-bit e criptografia do 128-bit, verifique ambas as opções para permitir a negociação.
3. Sob a seção para protocolos de autenticação de PPTP, verifique a opção para ver se há o **MSCHAPv1**. (Você já configurou os atributos de usuário do Cisco Secure ACS for Windows 2.5 para a criptografia em uma etapa mais adiantada.)




**Nota:** O cliente de PPTP deve ser reconhecido para ótimo ou criptografia de dados obrigatória e MSCHAPv1 (se uma opção).

## Relatório de adição

Depois que você estabeleceu a autenticação, você pode adicionar a contabilidade ao concentrador VPN. Vá ao **Configuration > System > aos server > aos servidores de contabilidade** e adicionar o server do Cisco Secure ACS for Windows.

No Cisco Secure ACS for Windows, os registros de contabilidade aparecem como segue.

```
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
```

# Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

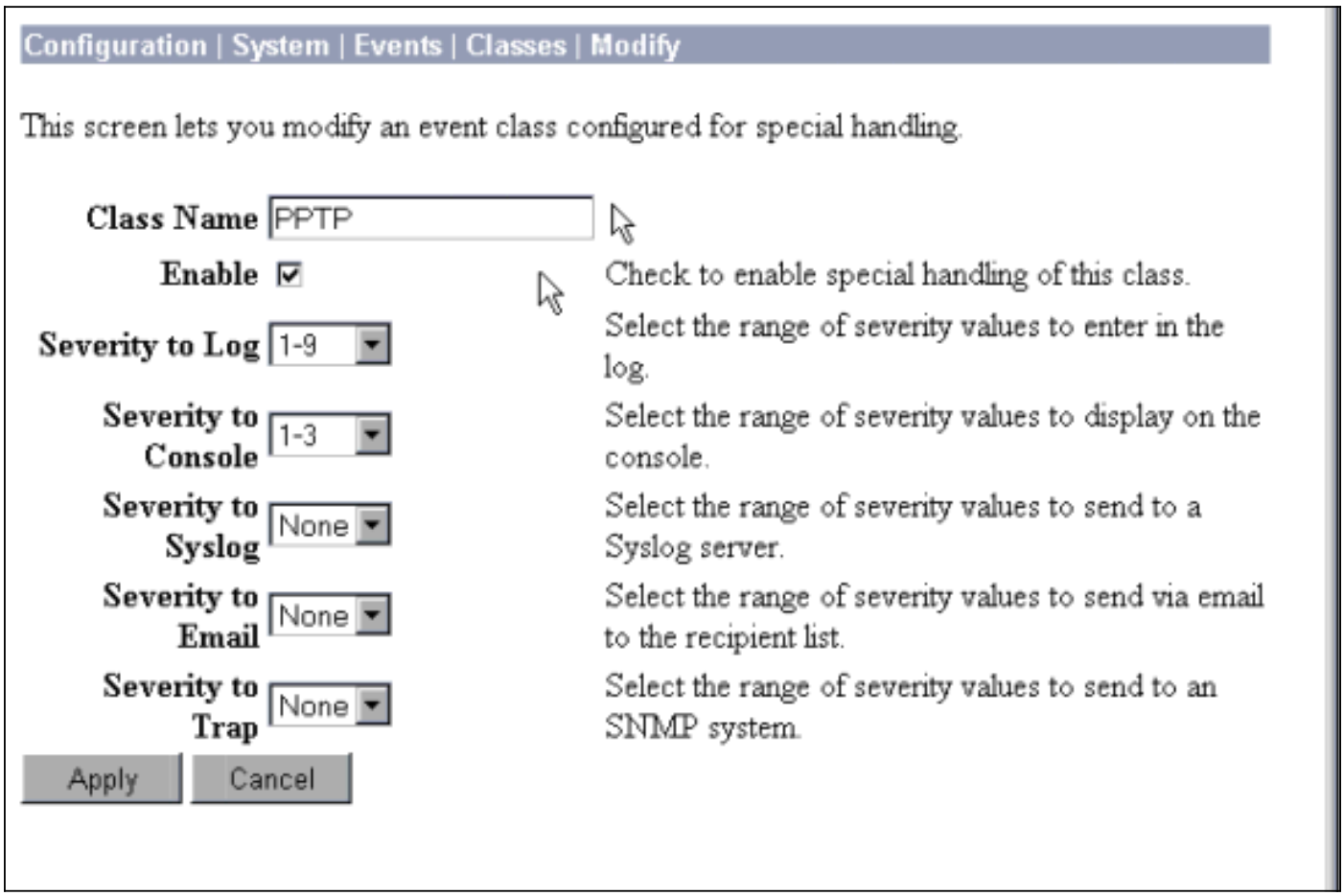
# Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua

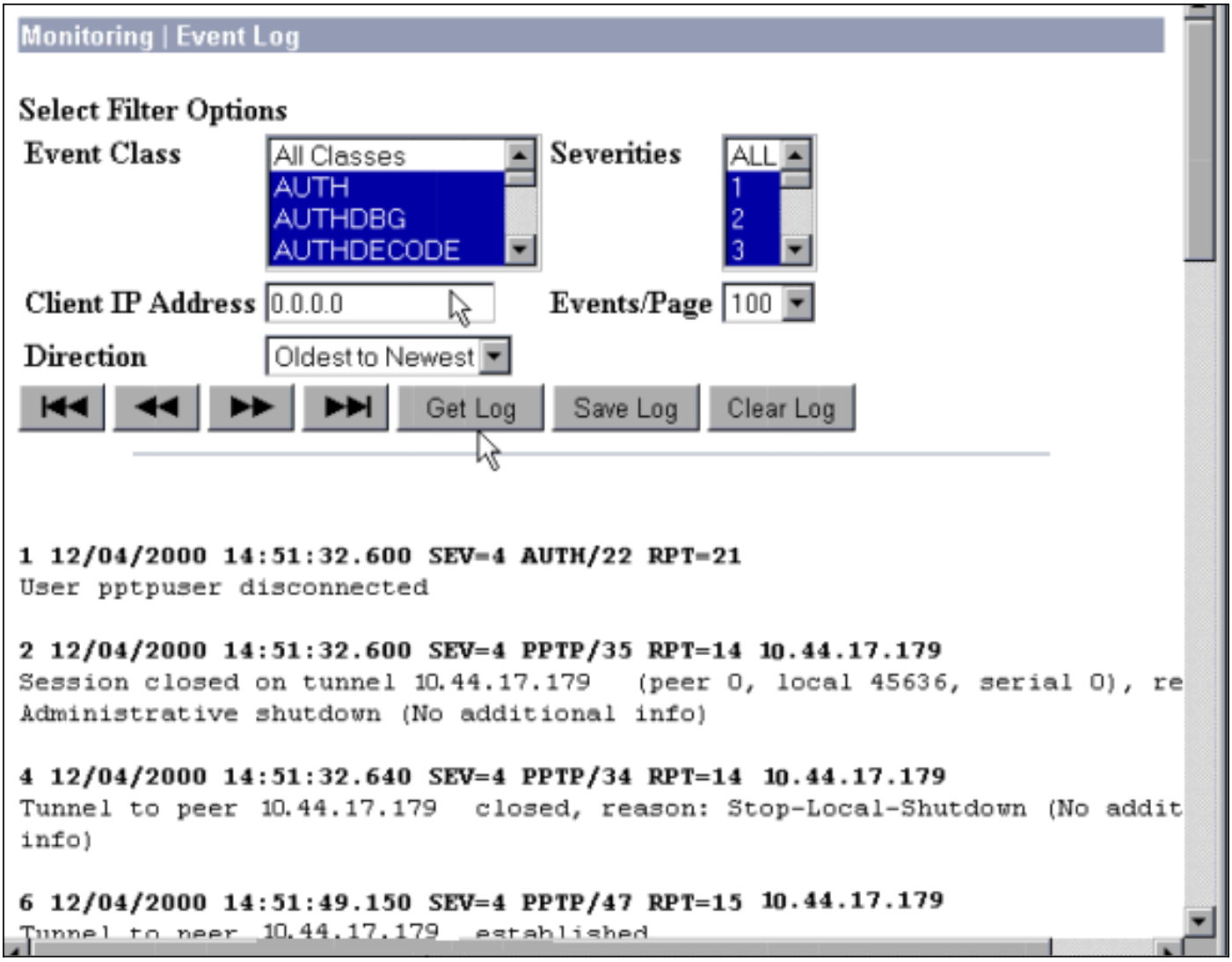
configuração.

## Permitindo a eliminação de erros

Se as conexões não trabalham, você pode adicionar o PPTP e as classes de evento de autenticação ao concentrador VPN indo ao **Configuration > System > aos eventos > classifica > Modify**. Você pode igualmente adicionar o PPTPDBG, o PPTPDECODE, o AUTHDBG, e as classes de evento authdecode, mas estas opções podem fornecer demasiada informação.




Você pode recuperar o log de eventos indo à **monitoração > log de eventos**.




## Debuga - Boa autenticação

Os debug correto no concentrador VPN olharão similares ao seguinte.

```
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
```

## Possíveis erros

Você pode encontrar possíveis erros como mostrado abaixo.

### Nome de usuário incorreto ou senha no servidor Radius do Cisco Secure ACS for Windows

- Resultado do debug do concentrador VPN 3000

```
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
```

- Registro de saída do Cisco Secure ACS for Windows

```
03/18/2000,08:02:47,Authen failed, baduser,,,CS user
unknown,,,1155,10.2.2.1
```

- A mensagem que o usuário vê (de 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.
```

### A “criptografia de MPPE exigida” é selecionada no concentrador, mas o server do Cisco Secure ACS for Windows não é configurado para Senhora-RACHADURA-MPPE-chaves e Senhora-RACHADURA-MPPE-tipos

- Resultado do debug do concentrador VPN 3000Se o AUTHDECODE (severidade 1-13) e o PPTP debugam (severidade 1-9) estão ligada, o log mostram que o server do Cisco Secure ACS for Windows não está enviando o atributo específico de fornecedor 26 (0x1A) na aceitação de acesso do server (log parcial).

```
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.
```

- O registro de saída do Cisco Secure ACS for Windows não mostra nenhuma falha.
- A mensagem que o usuário vê

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

## Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- Cisco Secure ACS para página de suporte do Windows
- Página de suporte RADIUS

- Página de suporte do PPTP
- RFC 2637: Protocolo de túnel ponto-a-ponto (PPTP)
- Request for comments (RFC)
- Suporte Técnico e Documentação - Cisco Systems