Como configurar o PPTP do concentrador VPN 3000 com autenticação local

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. Há um suporte de criptografia 40-bit e de 128-bit disponível nestes concentradores VPN para uma conexão confiável fixada.

Refira configurar o VPN 3000 concentrator PPTP com autenticação RADIUS do Cisco Secure ACS for Windows a fim configurar o concentrador VPN para usuários PPTP com autenticação extendida usando o Serviço de controle de acesso Cisco Secure (ACS).

Pré-requisitos

Requisitos

Assegure-se de que você encontre as condições prévias mencionadas em quando for a criptografia de PPTP apoiada em um Cisco VPN 3000 Concentrator? antes que você tentar esta configuração.

Componentes Utilizados

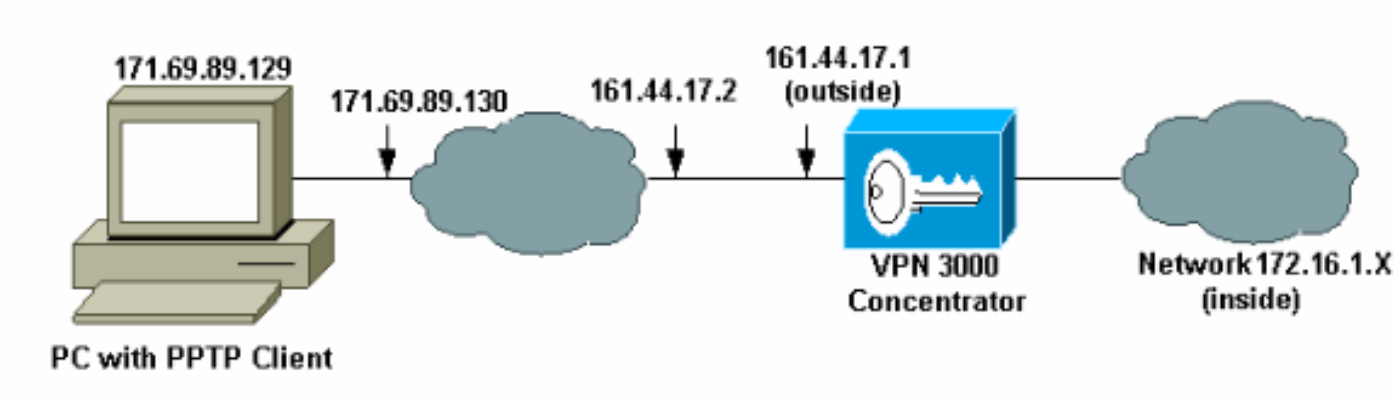
As informações neste documento são baseadas nestas versões de software e hardware:

- Concentrador VPN 3015 com versão 4.0.4.A
- PC Windows com cliente de PPTP

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



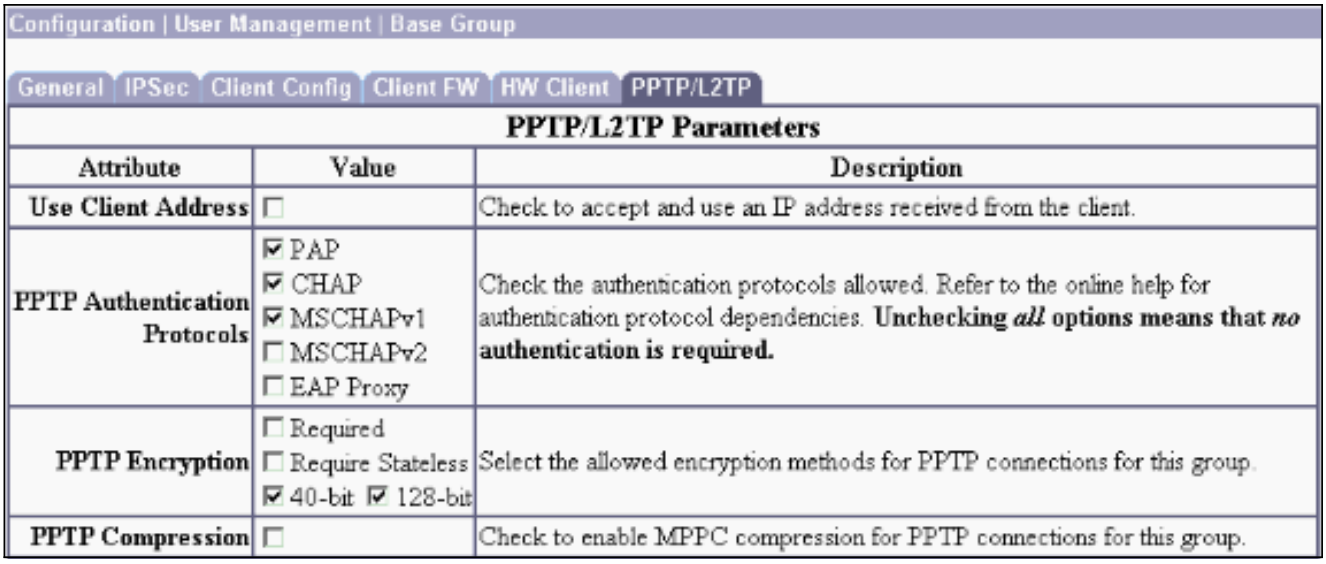
Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar o VPN 3000 concentrator com autenticação local

Termine estas etapas para configurar o VPN 3000 concentrator com autenticação local.

1. Configurar os endereços IP de Um ou Mais Servidores Cisco ICM NT respectivos no concentrador VPN e assegure-se de que você tenha a Conectividade.
2. Assegure-se de que a **autenticação pap** esteja selecionada na aba do **configuration > user management > do grupo base**
   PPTP/L2TP.



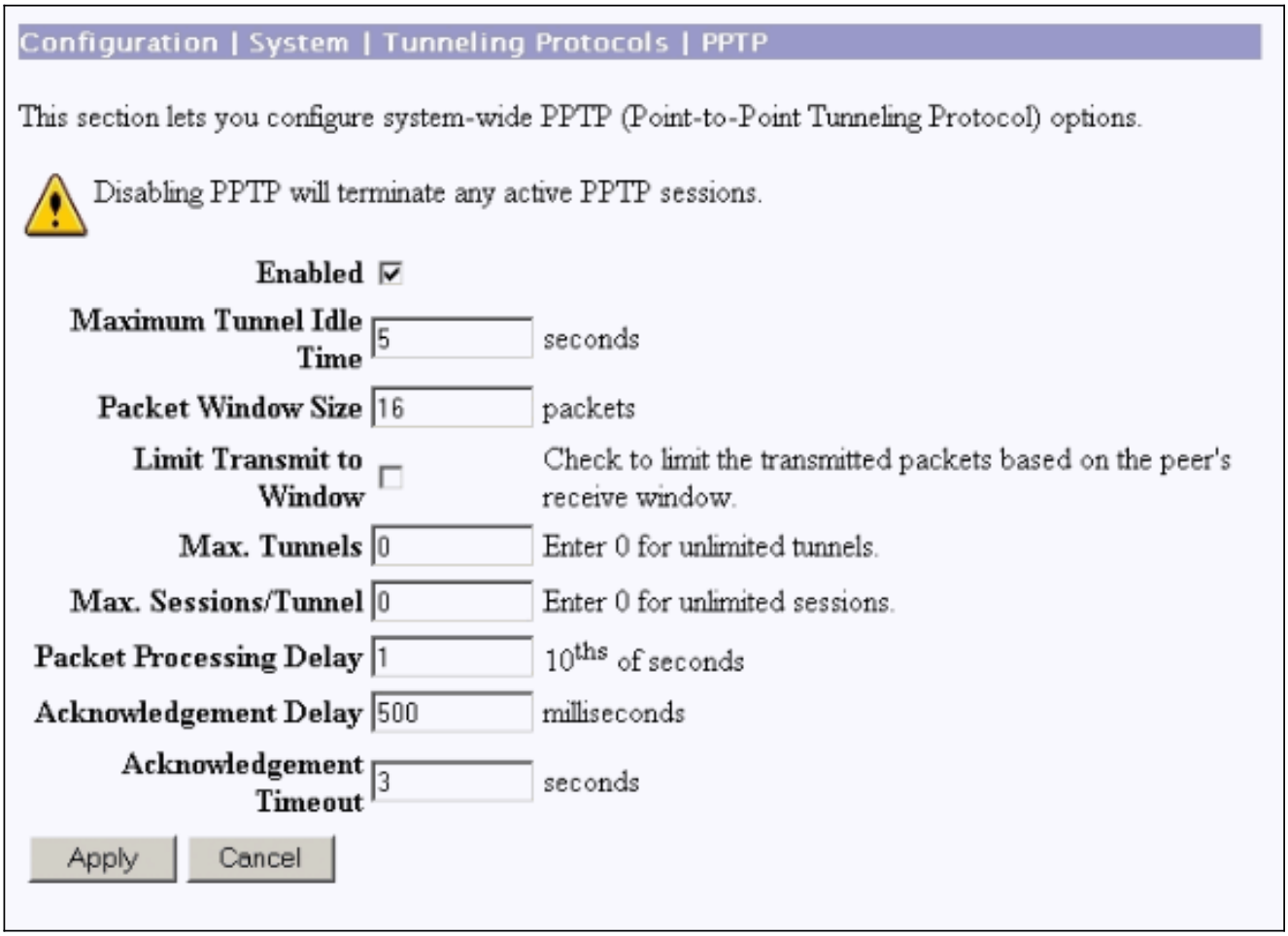
Configuration | User Management | Base Group

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. Selecione o **Configuration > System > Tunneling Protocols > o PPTP** e assegure-se de que que **permitiu** é
verificado.



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.

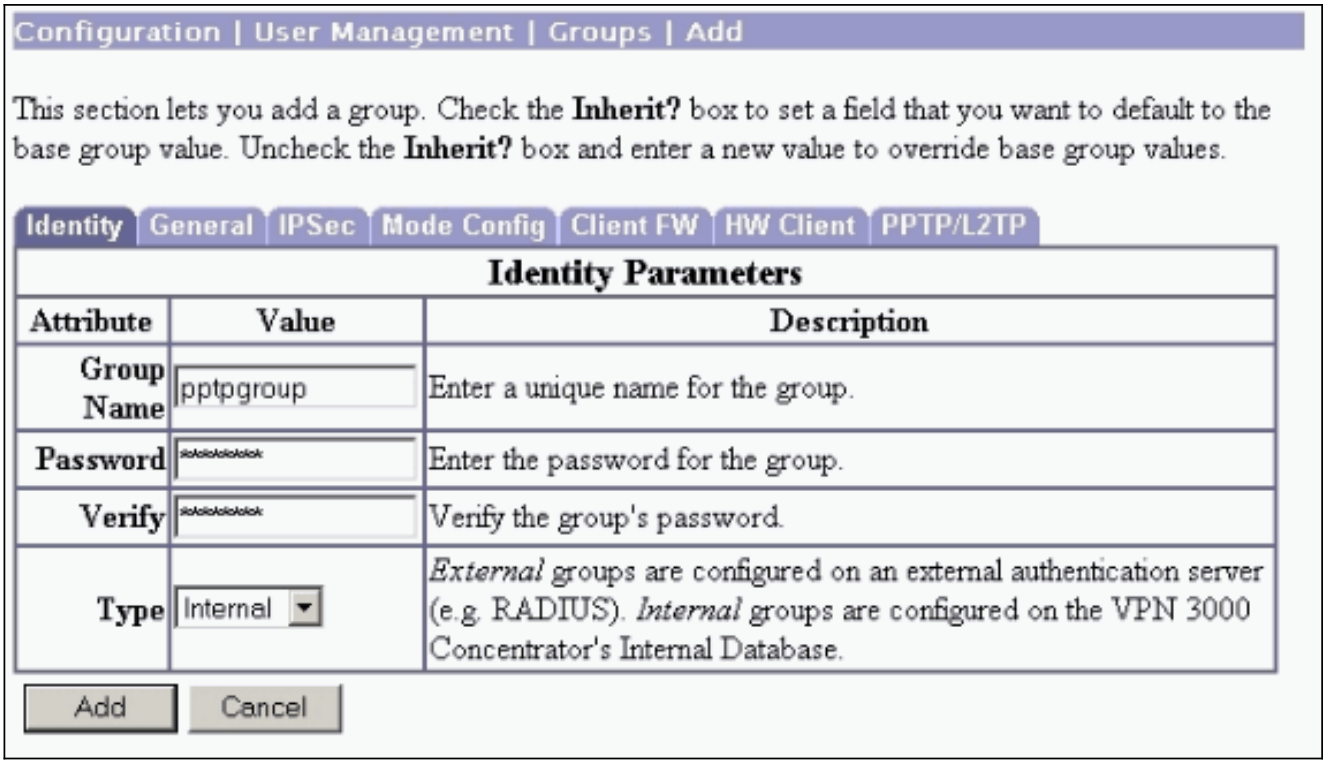
Packet Processing Delay 1 10^{ths} of seconds

Acknowledgement Delay 500 milliseconds

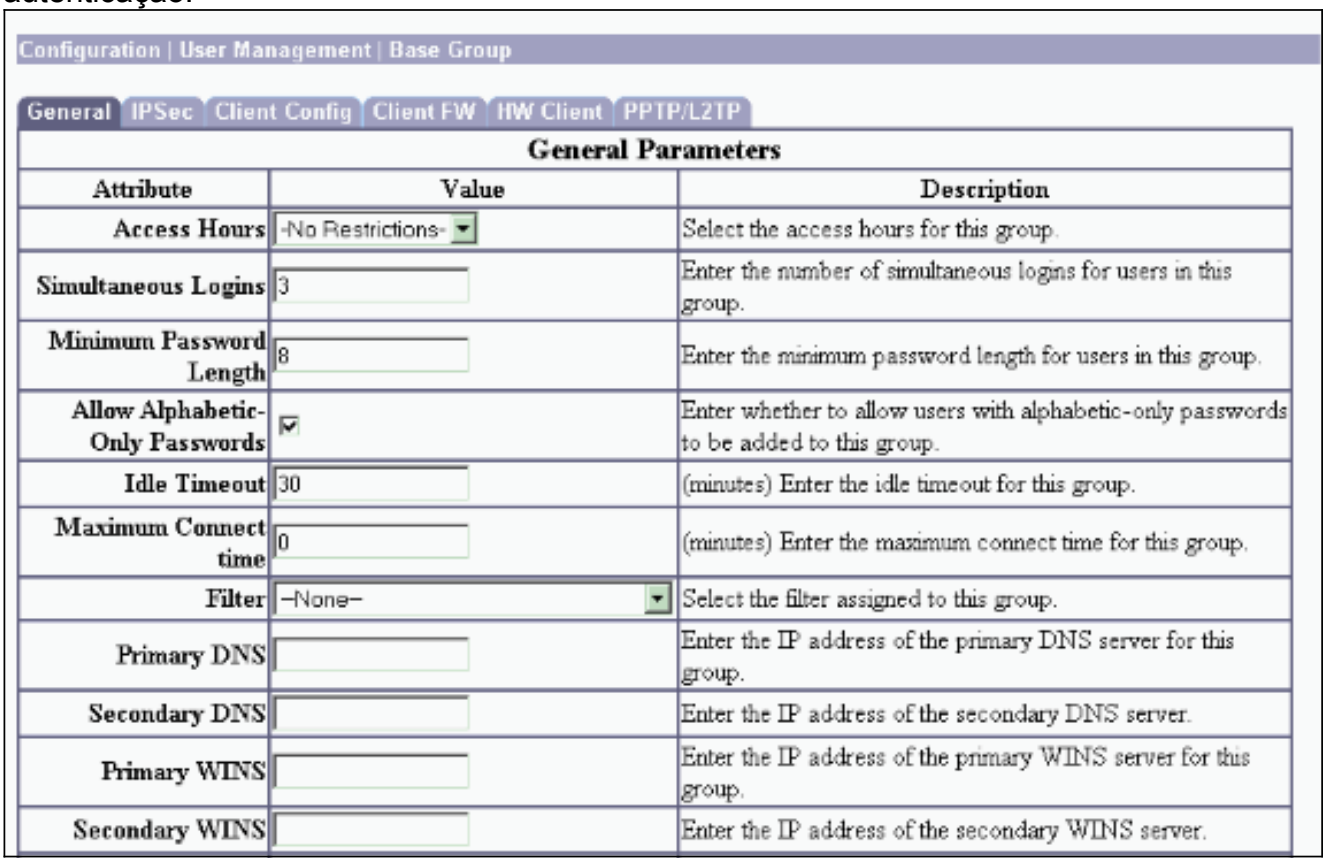
Acknowledgement Timeout 3 seconds

Apply Cancel

4. Selecione o **configuração > gerenciamento de usuário > grupos > adicionar**, e configure um grupo PPTP. Neste exemplo, o nome do grupo é “pptpgroup” e a senha (e verifique a senha) é
"cisco123".



5. Sob o tab geral do grupo, assegure que a **opção de PPTP** esteja permitida nos Protocolos de
autenticação.



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. Sob a aba PPTP/L2TP, permita a **autenticação pap**, e desabilite a **criptografia** (a criptografia pode ser permitida a qualquer hora no futuro).

Configuration | User Management | Groups | Modify pptpgroup

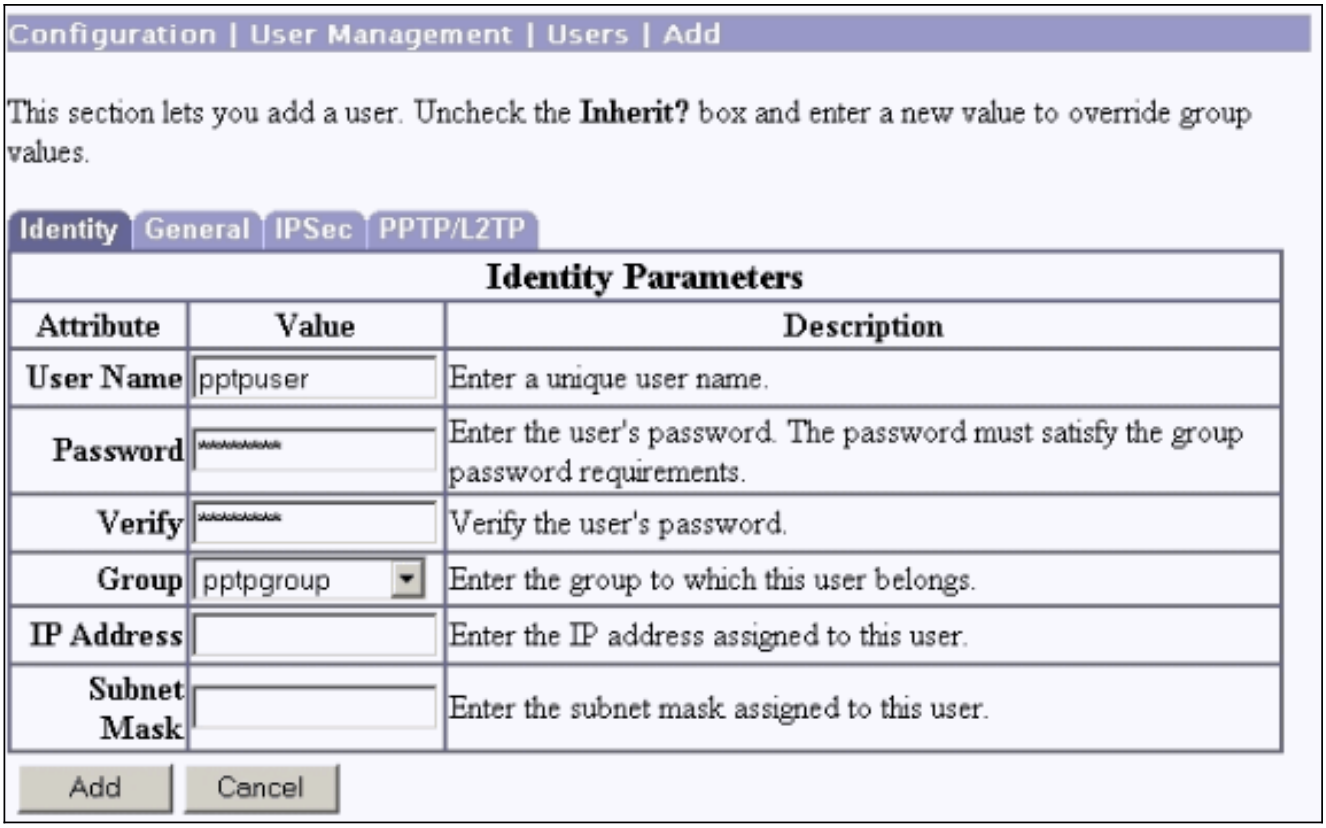
Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

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

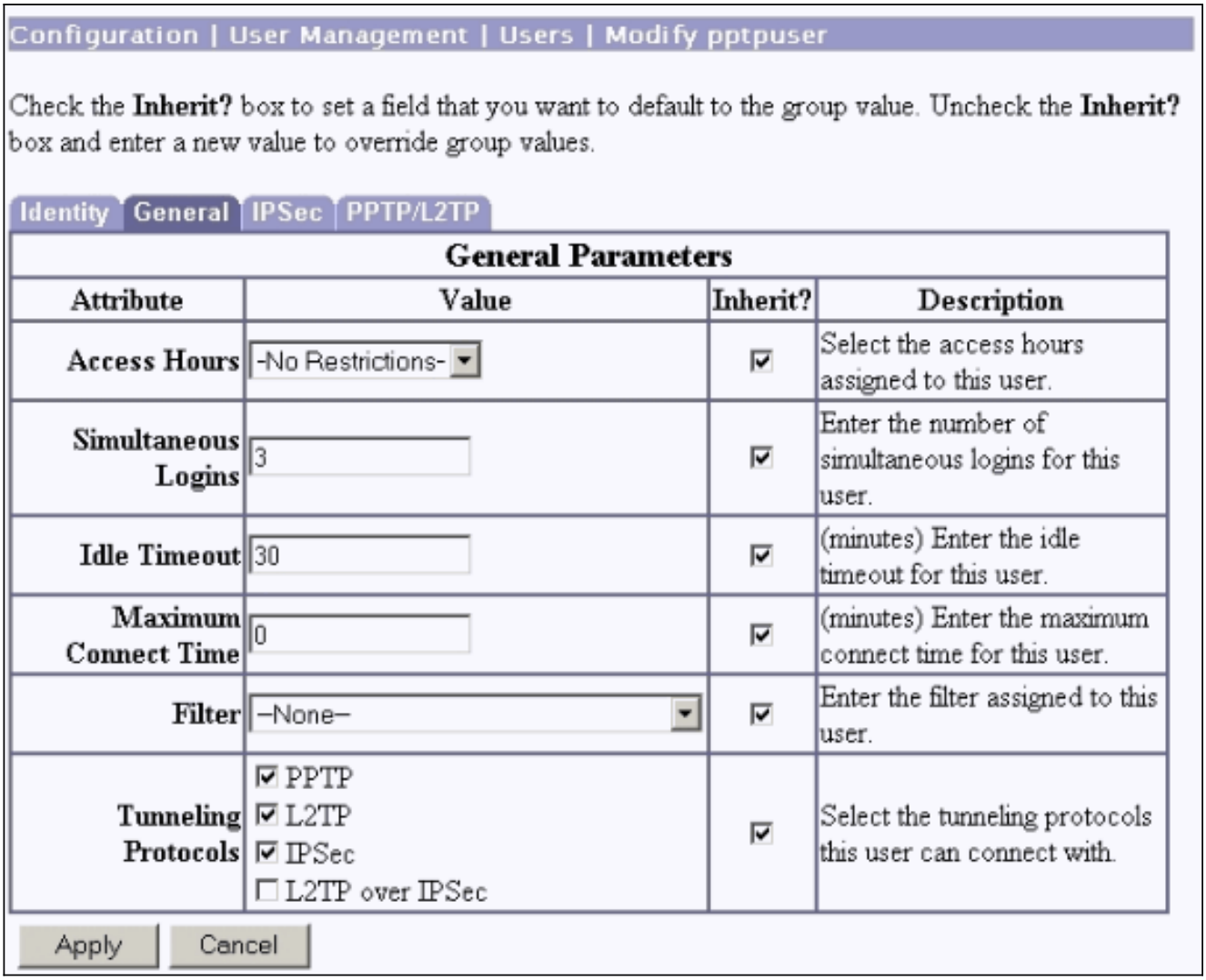
PPTP/L2TP Parameters

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.

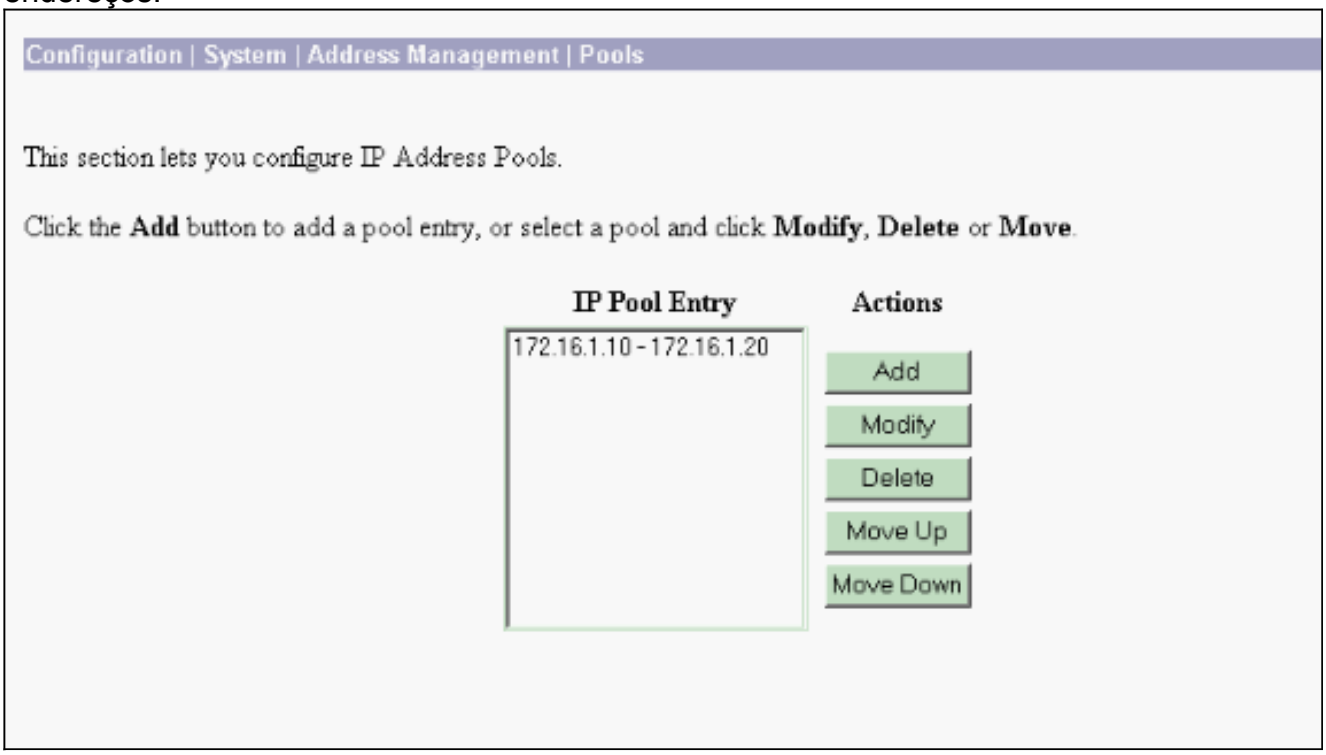
7. Selecione o **configuração > gerenciamento de usuário > usuários > adicionar**, e configure um usuário local (chamado “pptpuser”) com o **cisco123 da** senha para a autenticação de PPTP. Põe o usuário no “pptpgroup previamente definido”:



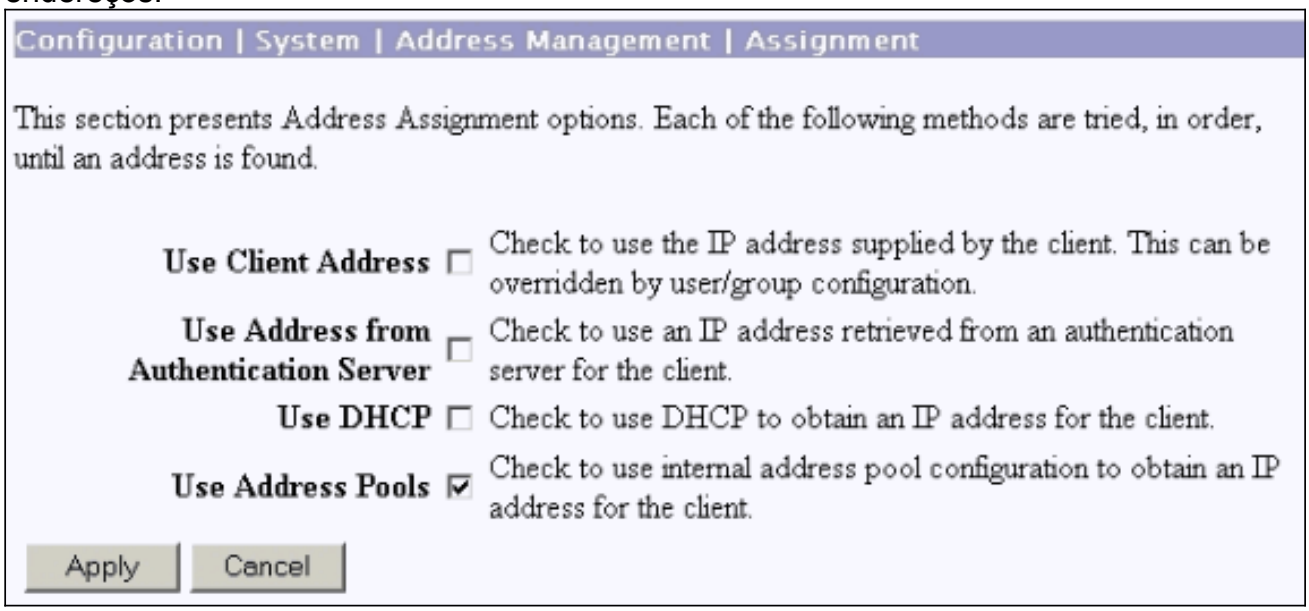
8. Sob o tab geral para o usuário, certifique-se de que a **opção de PPTP** está permitida nos protocolos de
tunelamento.



9. Selecione o **Configuração > Sistema > Gerenciamento de Endereço > Pools** para definir um conjunto de endereços para a gerência de endereços.



10. Selecione o **configuração > sistema > gerenciamento de endereço > atribuição** e dirija o concentrador VPN para usar o conjunto de endereços.



Configuração do Microsoft PPTP Client

Note: Nenhuma da informações disponíveis aqui em configurar o software Microsoft vem com toda a garantia ou apoio para o software Microsoft. O apoio para o software Microsoft está disponível de Microsoft .

Windows 98 - Instale e configurar a característica PPTP

Instalação

Termine estas etapas para instalar a característica PPTP.

1. Selecione o **Iniciar > Configurações > Painel de Controle > Adicionar Novo Hardware (seguinte) > selecionam da lista > do adaptador de rede (em seguida)**.
2. Selecione **Microsoft no** painel esquerdo e no **adaptador de Microsoft VPN no** painel direito.

Configurar

Termine estas etapas para configurar a característica PPTP.

1. Selecione o **Iniciar > Programas > Acessórios > Comunicações > Rede Dial-up > o Make New Connection**.
2. Conecte usando o adaptador de Microsoft VPN no seleto uma alerta do dispositivo. O IP do servidor de VPN é o ponto final de túnel 3000.

A autenticação padrão de Windows 98 usa a criptografia de senha (por exemplo, RACHADURA ou MSCHAP). A fim desabilitar esta criptografia, selecionar o **propriedades > tipos de servidor**, e desmarcar a **senha criptografada** e **exigir** inicialmente caixas da **criptografia de dados**.

Windows 2000 - Configurando o recurso PPTP

Termine estas etapas para configurar a característica PPTP.

1. Selecione o **Iniciar > Programas > Acessórios > Comunicações > Conexões de Rede e de Dial-up > o Make New Connection**.
2. Clique **em seguida**, e seleto **conecte a uma rede privada através do Internet > do seletor um anterior à conexão** (não selecione isto se você usa um LAN).
3. Clique **em seguida** outra vez, e incorpore o hostname ou o IP do ponto final de túnel, que é a interface externa do VPN 3000 concentrator. Neste exemplo o endereço IP de Um ou Mais Servidores Cisco ICM NT é 161.44.17.1.

Selecione o **Propriedades > Segurança de Conexão > Avançado** para adicionar um tipo de senha como o PAP. O padrão é MSCHAP e MSCHAPv2, não RACHADURA ou PAP.

A criptografia de dados é configurável nesta área. Você pode desabilitá-la inicialmente.

Windows NT

Você pode informação de acesso sobre clientes do Windows NT da fundação para o PPTP no Web site de Microsoft .

Windows Vista

Termine estas etapas para configurar a característica PPTP.

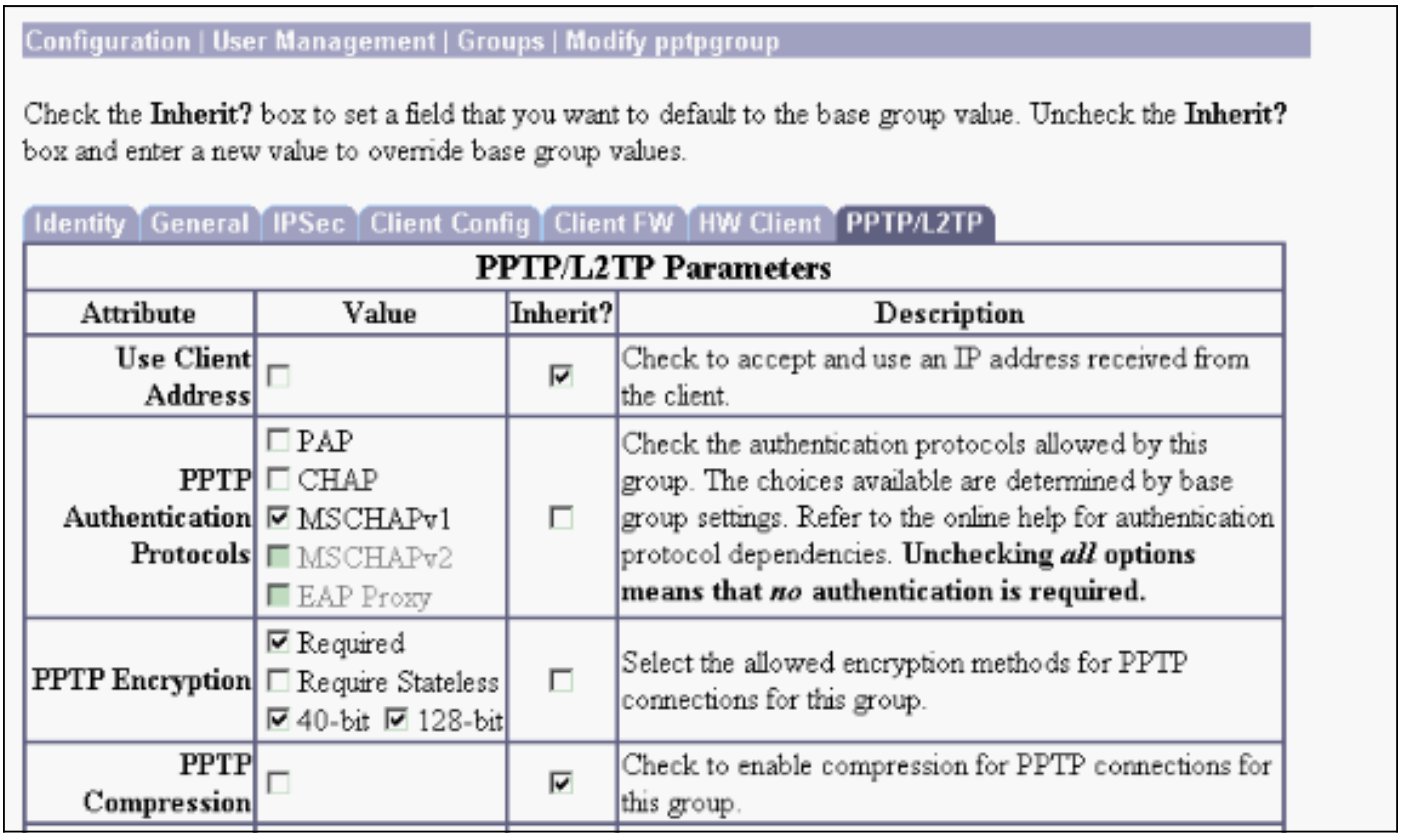
1. **Do botão Start Button**, escolha **conectam a**.
2. Escolha **estabelece uma conexão ou uma rede**.
3. Escolha **conectam a um local de trabalho** e clicam **em seguida**.
4. Escolha o **uso minha conexão com o Internet (VPN).Note**: Se alertado para “você quer usar uma conexão que você já tenha,” escolhe o **nenhum, cria uma nova conexão** e clica-a **em**

seguida.

5. No campo do **endereço do Internet**, datilografe **pptp.vpn.univ.edu**, por exemplo.
6. **No campo de nome do destino**, datilografe **UNIVVPN**, por exemplo.
7. No campo de **nome de usuário**, datilografe seu fazer logon ID UNIV. Seu fazer logon ID UNIV é parte de seu endereço email antes de **@univ.edu.**
8. No campo de **senha**, datilografe sua senha do fazer logon ID UNIV.
9. Clique o **botão Create** e clique então o **botão Close Button**.
10. A fim conectar ao servidor de VPN depois que você cria a conexão de VPN, clique o começo, e **conecte-o** então **a**.
11. Escolha a conexão de VPN no indicador e o clique **conecta**.

Adicionar MPPE (a criptografia)

Certifique-se de que a conexão PPTP funciona sem criptografia antes que você adicione a criptografia. Por exemplo, clique o **botão connect no** cliente de PPTP para certificar-se de que a conexão termina. Se você decide exigir a criptografia, a autenticação MSCHAP deve ser usada. No VPN3000, selecione o **configuration > user management > os grupos**. Então, sob a aba PPTP/L2TP para o grupo, desmarcar o **PAP**, verifique o **MSCHAPv1**, e verifique-o **exigido para a criptografia de PPTP**.



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.

O cliente de PPTP deve ser reconfigurado para o encrytption opcional ou dos dados obrigatórios e o MSCHAPv1 (se é uma opção).

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

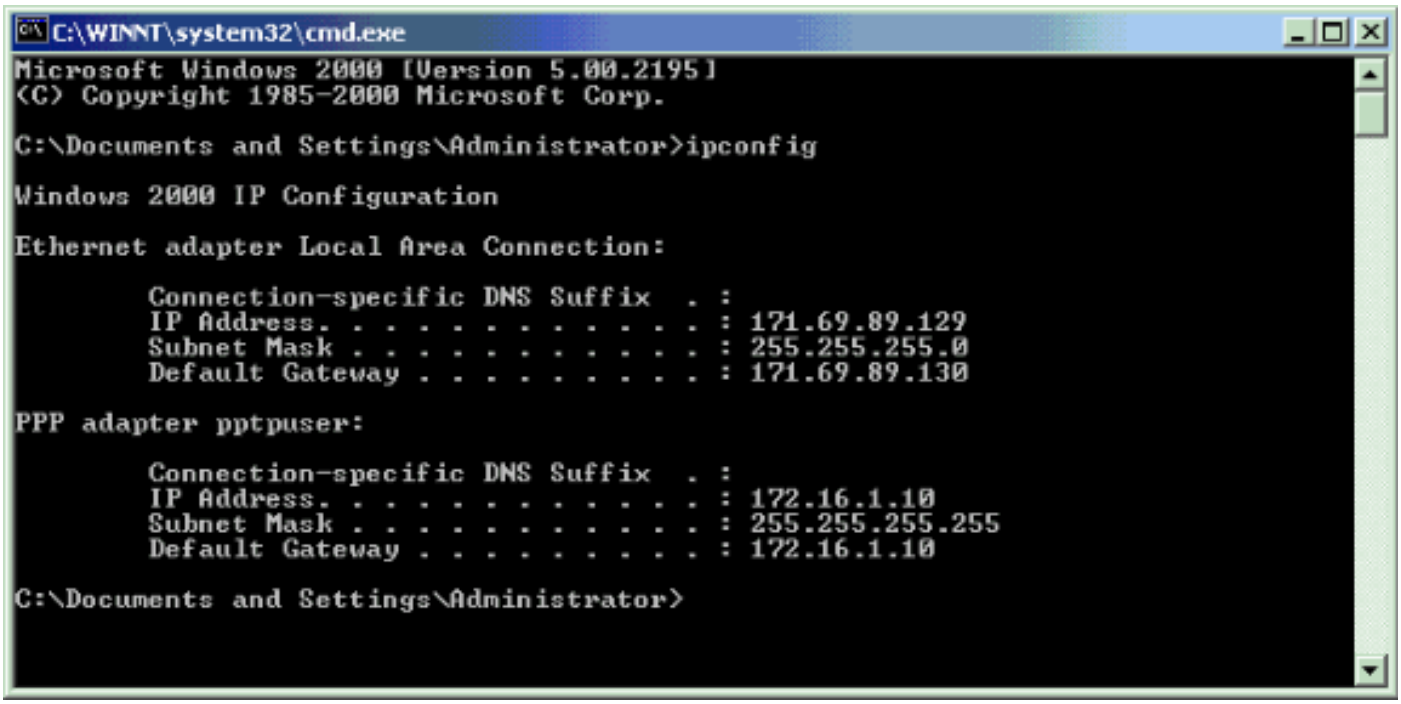
Verifique o concentrador VPN

Você pode começar a sessão de PPTP discando o formulário que o cliente de PPTP criou mais cedo na seção de configuração do cliente de PPTP de Microsoft.

Use a janela sessões do >Administer da administração no concentrador VPN para ver os parâmetros e as estatísticas para todas as sessões de PPTP ativa.

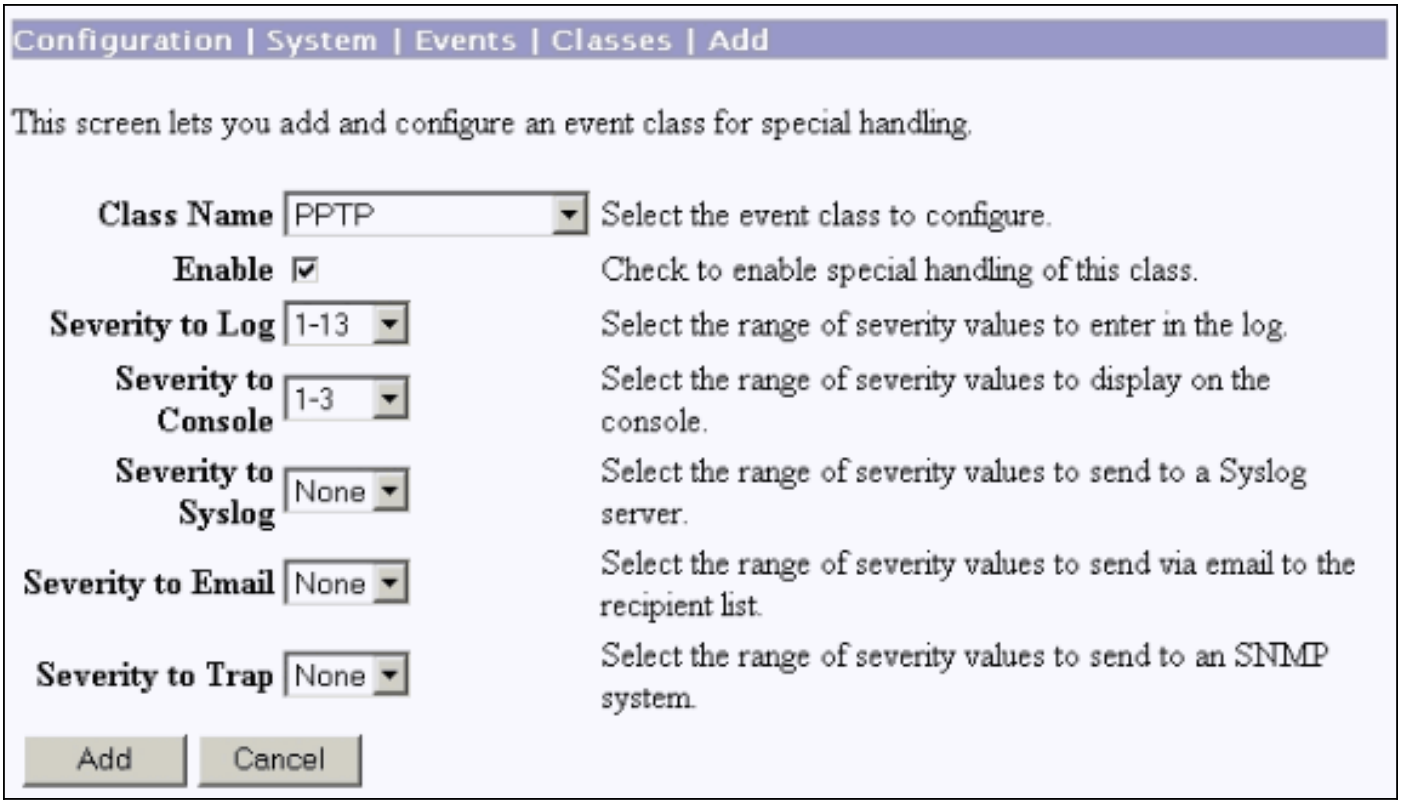
Verifique o PC

Emita o **comando ipconfig no** modo de comando do PC ver que o PC tem dois endereços IP de Um ou Mais Servidores Cisco ICM NT. Um é seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT e o outro é atribuído pelo concentrador VPN do pool do endereço IP de Um ou Mais Servidores Cisco ICM NT. Neste exemplo o endereço IP 172.16.1.10 é o endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído pelo concentrador VPN.

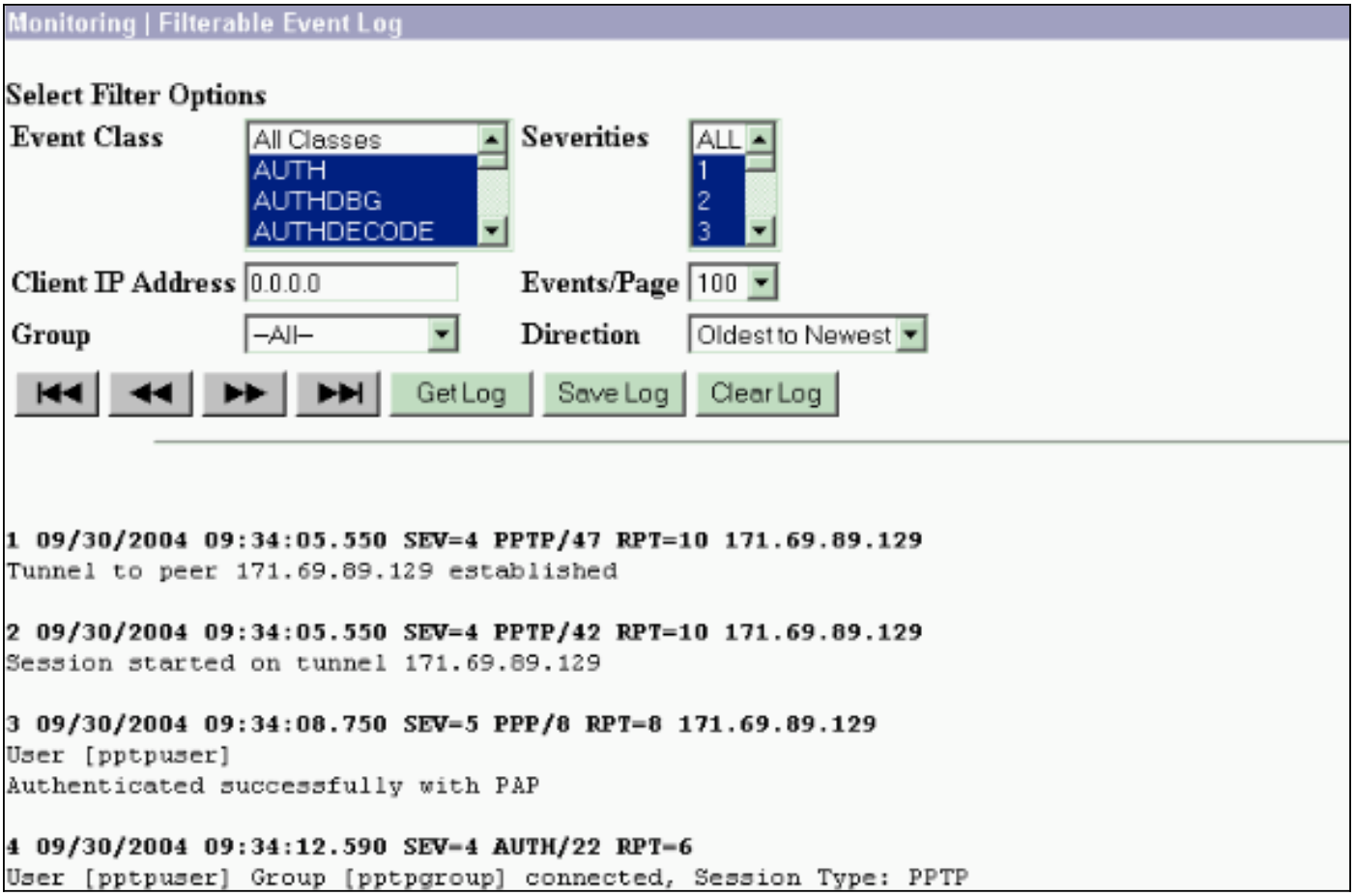


Debug

Se a conexão não trabalha, a classe de evento PPTP debuga pode ser adicionada ao concentrador VPN. Selecione o **Configuração > Sistema > Eventos > Classes > Modificar** ou **adicionar-lo** (mostrado aqui). As classes de evento PPTPDBG e PPTPDECODE estão igualmente disponíveis, mas puderam fornecer demasiada informação.



O log de eventos pode ser recuperado da **monitoração > do log filtrável de eventos**.



Depuração do VPN 3000 - Boa autenticação

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

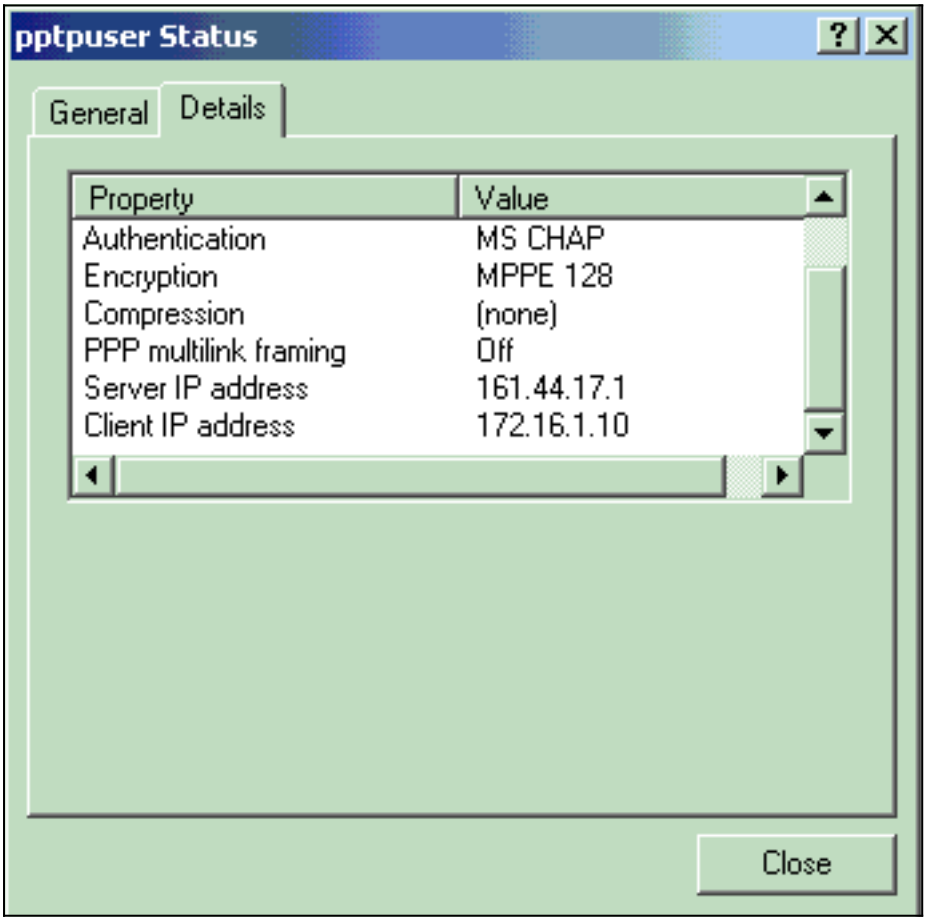
```
   Tunnel to peer 171.69.89.129 established

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
```

Clique sobre o indicador dos **detalhes do** estado do usuário PPTP para verificar os parâmetros no PC Windows.



Troubleshooting

Estes são possíveis erros que você pode encontrar:

- **Nome de usuário incorreto ou senha**Resultado do debug do VPN 3000 concentrator:

```
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)
```

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 mensagem que o usuário vê (do Windows 2000):

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

- **A "criptografia exigida" é selecionada no PC, mas não no concentrador VPN**A mensagem que o usuário vê (de 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.
```

  A mensagem que o usuário vê (do Windows 2000):

```
Error 742: The remote computer does not support
the required data encryption type
```

- **A "criptografia exigida" (128-bit) é selecionada no concentrador VPN com um PC que apoie somente a criptografia 40-bit**Resultado do debug do VPN 3000 concentrator:

```
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.
```

  A mensagem que o usuário vê (de Windows 98):

```
Error 742:  The remote computer does not support
the required data encryption type.
```

  A mensagem que o usuário vê (do Windows 2000):

```
Error 645 Dial-Up Networking could not complete the connection to the server.
Check your configuration and try the connection again.
```

- **O VPN 3000 concentrator é configurado para o MSCHAPv1 e o PC é configurado para o PAP, mas não podem concordar com um método de autenticação**Resultado do debug do VPN 3000 concentrator:

```
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.
```

  A mensagem que o usuário vê (do Windows 2000):

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

Possíveis problemas da Microsoft a serem solucionados

- **Como Manter conexões de RAS Ativas Após o Fim da Sessão**Quando você termina de um cliente do Remote Access Service de Windows (RAS), todas as conexões de RAS estão desligadas automaticamente. Permita a chave dos **KeepRasConnections no** registro no cliente de RAS de permanecer conectada depois que você termina. Refira o artigo da base de conhecimento microsoft - 158909 para mais informação.
- **O usuário não é alertado ao entrar com credenciais em cache**Os sintomas desta edição são quando você tenta entrar a um domínio de uma estação de trabalho com base no Windows ou o servidor membro e um controlador de domínio não podem ser encontrados e nenhum Mensagem de Erro está indicado. Em vez disso, você será conectado ao computador local usando as credenciais em cache. Refira o artigo da base de conhecimento microsoft - 242536

para mais informação.
- Como Escrever um Arquivo LMHOSTS para a Validação de Domínio e Outros Problemas de Resolução de NomesPode haver uns exemplos quando você experimenta edições da resolução de nome em sua rede TCP/IP e você precisa de usar arquivos LMHOSTS para resolver nomes de netbios. Este artigo discute o método apropriado usado para criar um arquivo LMHOSTS para ajudar na resolução de nome e na validação de domínio. Refira o artigo da base de conhecimento microsoft - 180094 para mais informação.

Informações Relacionadas

- RFC 2637: Protocolo de túnel ponto-a-ponto (PPTP)
- Páginas de suporte do Cisco Secure ACS for Windows
- Quando a criptografia de PPTP é apoiada em um Cisco VPN 3000 Concentrator?
- Configurando o VPN 3000 concentrator e o PPTP com autenticação RADIUS do Cisco Secure ACS for Windows
- Página de suporte do Cisco VPN 3000 Concentrator
- Páginas de suporte ao Cisco VPN 3000 Client
- Páginas de Suporte do Produto IPSec (Protocolo de Segurança IP)
- Páginas de suporte dos produtos PPTP
- Suporte Técnico e Documentação - Cisco Systems