IPsec entre um VPN 3000 concentrator e um cliente VPN 4.x para Windows usando o RAIO para o exemplo de configuração da autenticação de usuário e explicar

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Configurar
Diagrama de Rede
Use grupos no VPN 3000 concentrator
Como o VPN 3000 Concentrator usa os atributos de grupo e de usuário
Configuração do VPN 3000 series concentrator
Configuração de servidor RADIUS
Atribua um endereço IP estático ao usuário de cliente VPN
Configuração de cliente VPN
Adicionar relatório
Verificar
Verifique o concentrador VPN
Verifique o cliente VPN
Troubleshooting
Pesquise defeitos o cliente VPN 4.8 para Windows
Informações Relacionadas

Introdução

Este documento descreve como estabelecer um túnel de IPsec entre um Cisco VPN 3000 Concentrator e um Cisco VPN Client 4.x para Microsoft Windows que use o RAIO para a autenticação de usuário e a contabilidade. Este documento recomenda o Serviço de controle de acesso Cisco Secure (ACS) para Windows para que a configuração RADIUS mais fácil autentique os usuários que conectam a um VPN 3000 concentrator. Um grupo em um VPN 3000 concentrator é uma coleção de usuários tratada como uma entidade única. A configuração dos grupos, ao contrário dos usuários individuais, pode simplificar tarefas de configuração do gerenciamento de sistema e da aerodinâmica.

Refira PIX/ASA 7.x e Cisco VPN Client 4.x para Windows com exemplo de configuração da autenticação RADIUS de Microsoft Windows 2003 IAS a fim estabelecer a conexão VPN de

acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500 que usa um servidor Radius do Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refira configurar o IPsec entre um roteador do Cisco IOS e um Cisco VPN Client 4.x para Windows usando o RAIO para a autenticação de usuário a fim configurar uma conexão entre um roteador e o Cisco VPN Client 4.x que usa o RAIO para a autenticação de usuário.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O RAIO do Cisco Secure ACS for Windows é instalado e opera-se corretamente com outros dispositivos.
- O Cisco VPN 3000 Concentrator é configurado e pode ser controlado com a interface HTML.

Componentes Utilizados

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

- Cisco Secure ACS for Windows com versão 4.0
- Concentrador da Cisco VPN 3000 Series com arquivo de imagem 4.7.2.B
- Cisco VPN Client 4.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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

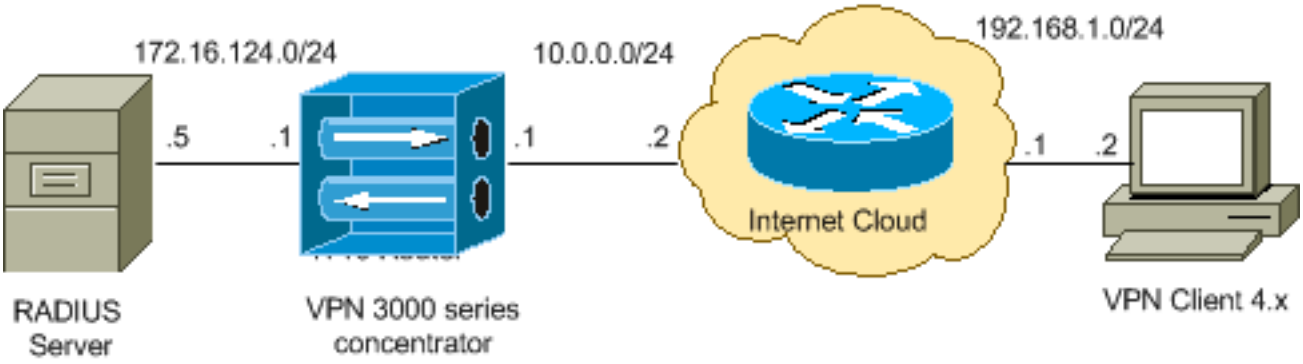
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Use grupos no VPN 3000 concentrator

Os grupos podem ser definidos para ambo o Cisco Secure ACS for Windows e o VPN 3000 concentrator, mas usam grupos um tanto diferentemente. Execute estas tarefas a fim simplificar coisas:

- **Configurar um único grupo no VPN 3000 concentrator** para quando você estabelece o túnel inicial. Isto é chamado frequentemente o grupo de túneis e é usado para estabelecer uma sessão cifrada do Internet Key Exchange (IKE) ao VPN 3000 concentrator usando uma chave pré-compartilhada (o group password). Esta é o mesmos nome do grupo e senha que devem ser configurados em todos os Cisco VPN Client que querem conectar ao concentrador VPN.
- **Configurar os grupos no server do Cisco Secure ACS for Windows** que usam atributos de RADIUS padrão e específico do vendedor atribui (VSA) para o Gerenciamento de políticas. Os VSA que devem ser usados com o VPN 3000 concentrator são os atributos do RAIO (VPN3000).
- **Configurar usuários no servidor Radius do Cisco Secure ACS for Windows e atribua-os a um dos grupos** configurados no mesmo server. Os usuários herdam os atributos definidos para seu grupo e o Cisco Secure ACS for Windows envia aqueles atributos ao concentrador VPN quando o usuário é autenticado.

Como o VPN 3000 Concentrator usa os atributos de grupo e de usuário

Depois que o VPN 3000 concentrator autentica o grupo de túneis com o concentrador VPN e o usuário com RAIO, deve organizar os atributos que recebeu. O concentrador VPN usa os atributos neste ordem de preferência, se a autenticação está feita no concentrador VPN ou com RAIO:

1. **Atributos de usuário** — Estes atributos tomam sempre a precedência sobre toda a outro.
2. **Atributos do grupo de túneis** — Todos os atributos não retornados quando o usuário foi autenticado são preenchidos pelos atributos do grupo de túneis.
3. **Atributos de grupo base** — Algum atribui desaparecidos do usuário ou os atributos do grupo de túneis são preenchidos pelos atributos de grupo base do concentrador VPN.

Configuração do VPN 3000 series concentrator

Termine o procedimento nesta seção a fim configurar um Cisco VPN 3000 Concentrator para os parâmetros exigidos à conexão IPSec assim como ao cliente de AAA para que o usuário VPN autentique com o servidor Radius.

Nesta configuração de laboratório, o concentrador VPN é alcançado primeiramente através da porta de Console e uma configuração mínima é adicionada enquanto esta saída mostra:

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address ----------------------------------------------------------------
-------------- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | --------------------
---------------------------------------------------------- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
---------------------------------------------------------------------- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | ----------------------------------------------------------
--------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----------
---------------------------------------------------------------------- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | ----------------------------------------------------
--------------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>
```

O concentrador VPN aparece na configuração rápida, e estes artigos são configurados.

- Hora/Data
- Relações/máscaras no **configuração > interfaces** (public=10.0.0.1/24, private=172.16.124.1/24)
- Gateway padrão no **> IP Routing do Configuration > System > no Default_Gateway** (10.0.0.2)

Neste momento, o concentrador VPN é acessível com o HTML da rede interna.

Nota: Se o concentrador VPN é controlado de fora, você igualmente executa estas etapas:

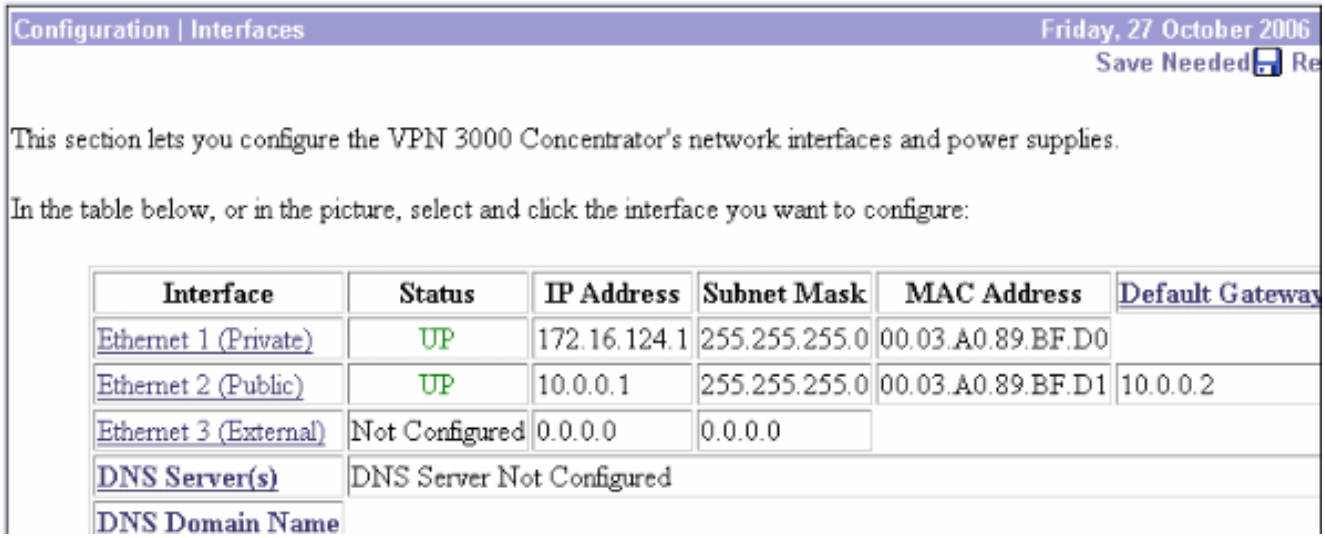
1. Escolha a **configuração > o filtro IP 1-Interfaces > 2-Public > 4-Select > 1. privado (padrão)**.
2. Escolha a **administração > 7-Access endireita > estação de trabalho da lista de controle 2-**

Access > do gerente 1-Add a fim adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do gerenciador externo.

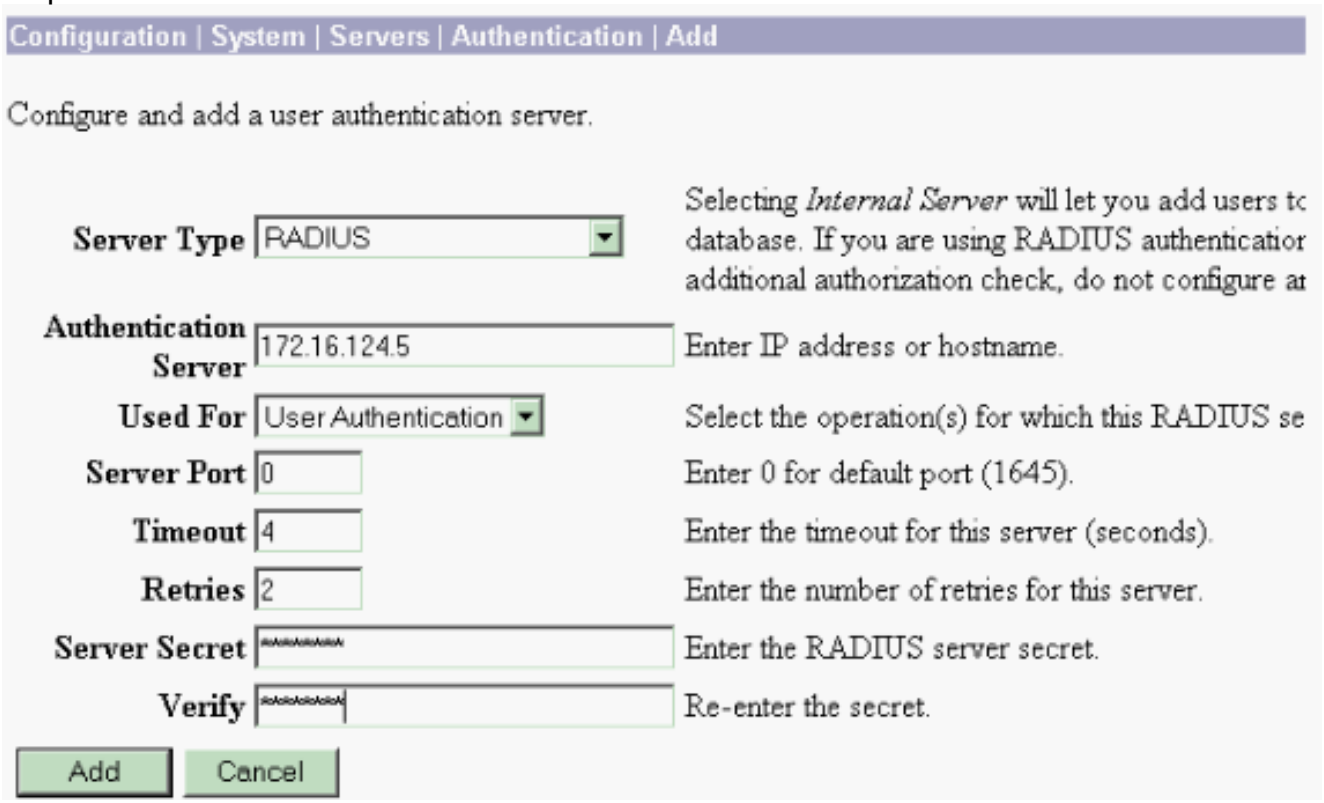
Estas etapas são exigidas somente se você controla o concentrador VPN da parte externa.

Uma vez que você terminou estas duas etapas, o resto da configuração pode ser feito com o GUI usando um navegador da Web e conectando ao IP da relação que você apenas configurou. Neste exemplo e neste momento, o concentrador VPN é acessível com o HTML da rede interna:

1. Escolha o **configuração > interfaces** a fim verificar novamente as relações depois que você traz acima o
   GUI.



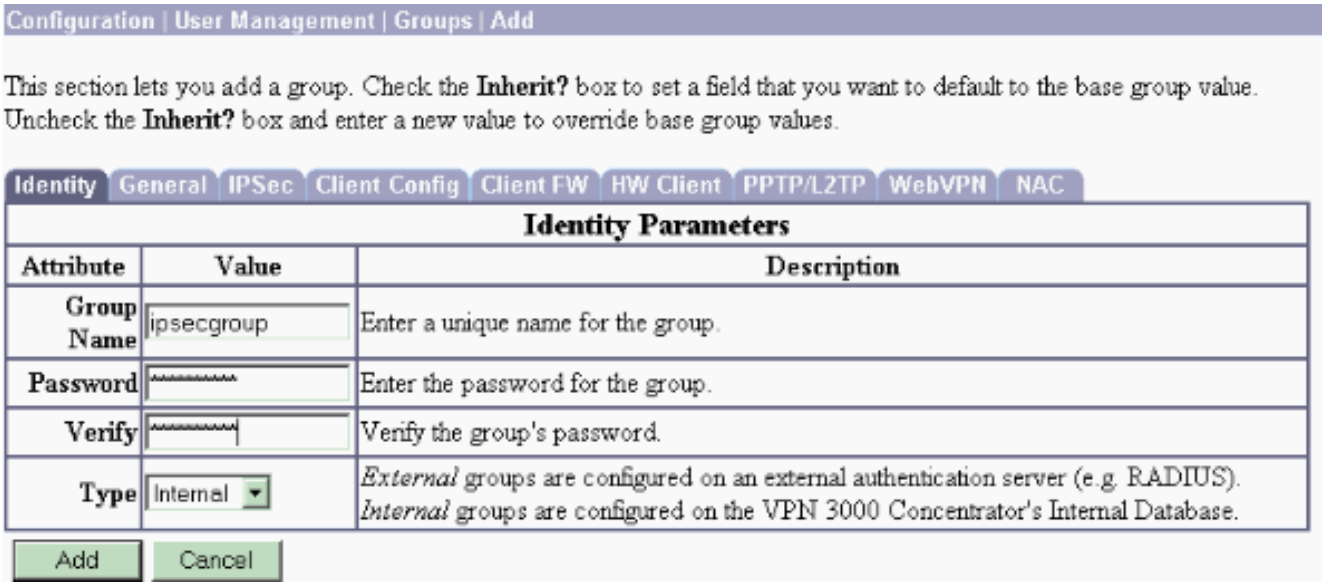
2. Termine estas etapas a fim adicionar o servidor Radius do Cisco Secure ACS for Windows à configuração do VPN 3000 concentrator.Escolha o **configuração > sistema > servidores > autenticação**, e o clique **adiciona do** menu
   esquerdo.



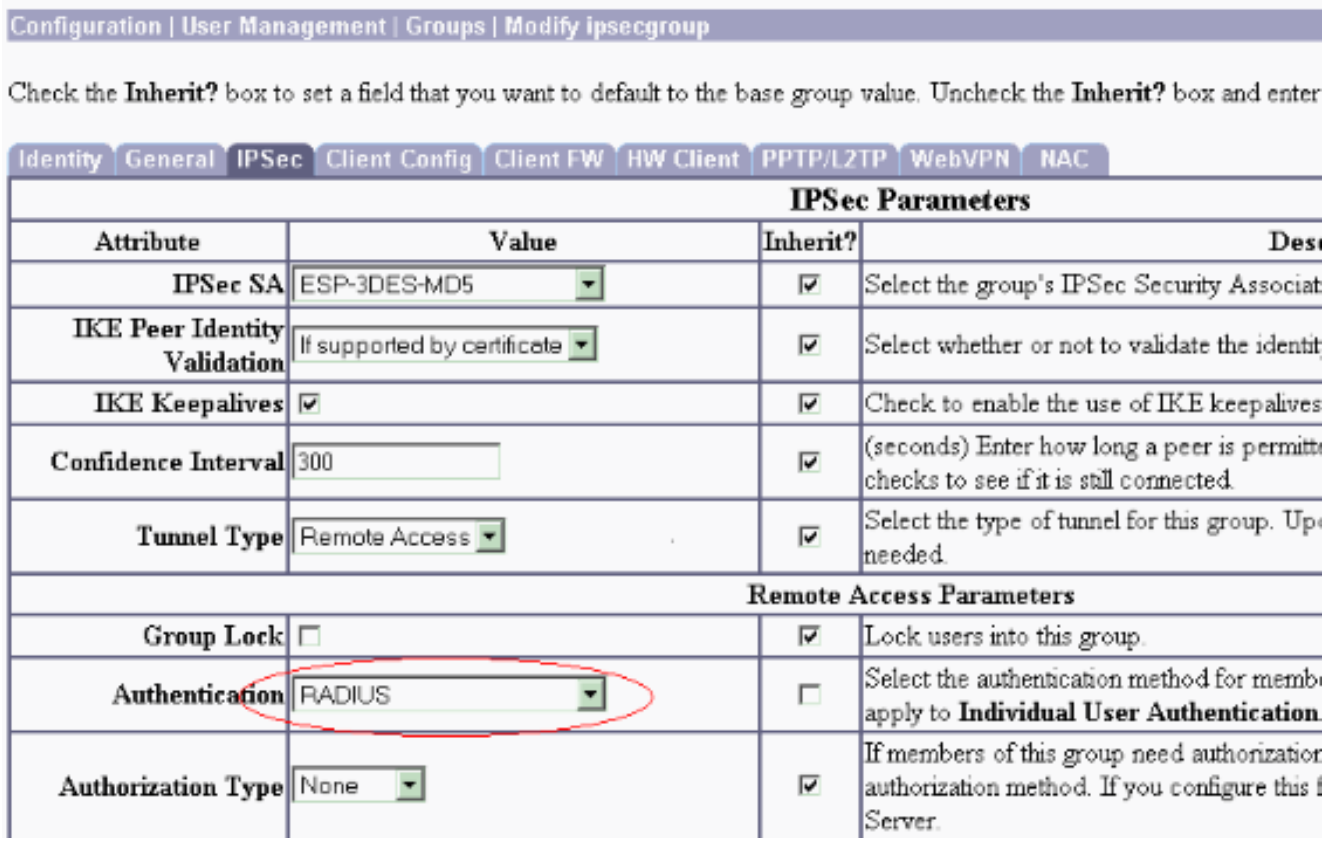
   Escolha o tipo de servidor radius e adicionar estes parâmetros para seu servidor Radius do Cisco Secure ACS for Windows. Deixe todos parâmetros restantes em seu estado

padrão.**Authentication Server** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor Radius do Cisco Secure ACS for Windows.**Segredo de servidor** — Incorpore o servidor secreto radius. Este deve ser o mesmo segredo que você se usa quando você configura o VPN 3000 concentrator na configuração do Cisco Secure ACS for Windows.**Verifique** — Reenter a senha para verificação.Isto adiciona o Authentication Server na configuração global do VPN 3000 concentrator. Este server está usado por todos os grupos à exceção de quando um Authentication Server foi definido especificamente. Se um Authentication Server não é configurado para um grupo, reverte ao server da autenticação global.

3. Termine estas etapas a fim configurar o grupo de túneis no VPN 3000 concentrator.Escolha o **configuration > user management > os grupos do** menu esquerdo e o clique **adiciona**.Mude ou adicionar estes parâmetros nos guias de configuração. Não clique aplicam-se até que você mude todos estes parâmetros:**Nota:** Estes parâmetros são o mínimo necessário para conexões VPN de acesso remoto. Estes parâmetros igualmente supõem que as configurações padrão no grupo base no VPN 3000 concentrator não estiveram mudadas.**Identidade**

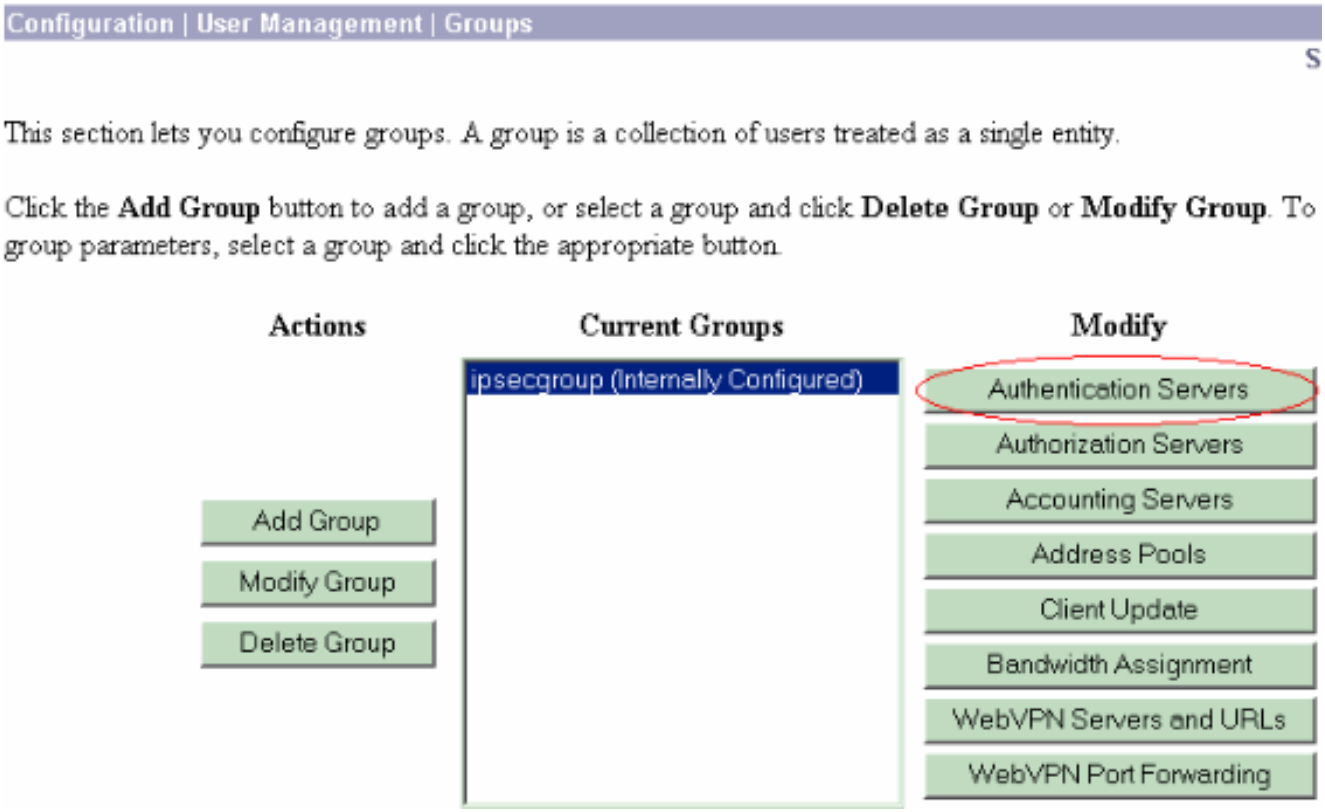


Nome do grupo — Datilografe um nome do grupo. Por exemplo, IPsecUsers.**Senha** — Incorpore uma senha para o grupo. Esta é a chave pré-compartilhada para a sessão de IKE.**Verifique** — Reenter a senha para verificação.**Tipo** — Deixe isto como o padrão: Interno.**IPsec**



Tipo de túnel — Escolha o **acesso remoto**.**Autenticação** — RAIO. Isto diz ao concentrador VPN que método a se usar para autenticar usuários.**Config de modo** — Verifique o **config de modo**.Clique em Apply.

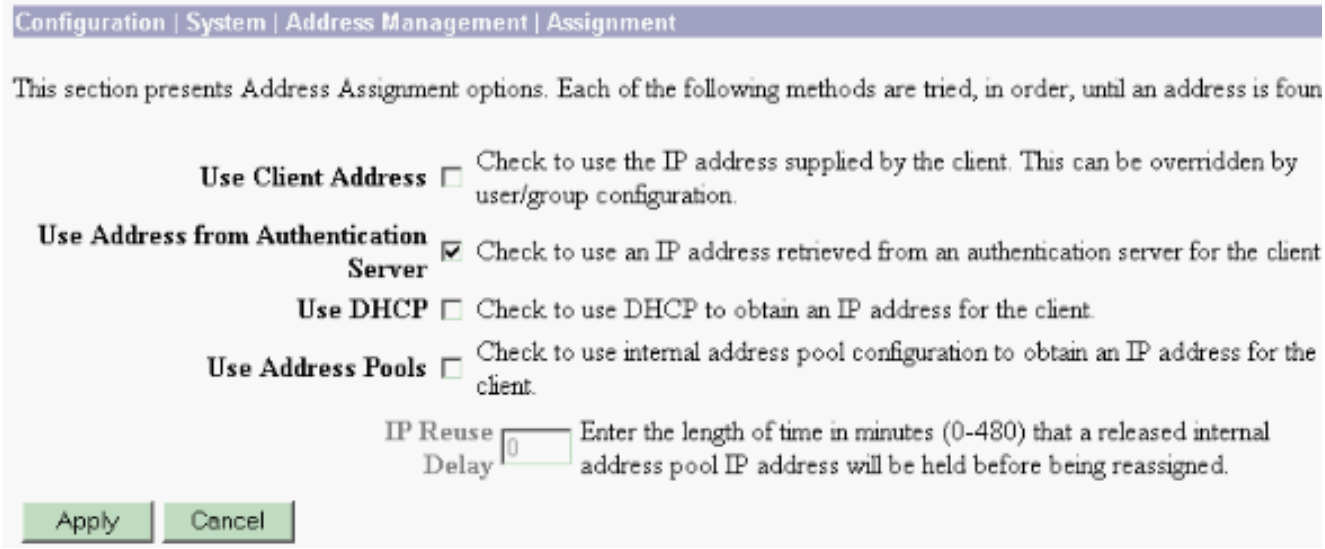
4. Termine estas etapas a fim configurar server da autenticação múltipla no VPN 3000 concentrator.Uma vez que o grupo é definido, destaque esse grupo, e clique **Authentication Server** sob a coluna da alteração. Os Authentication Server individuais podem ser definidos para cada grupo mesmo se estes server não existem nos server globais.



Escolha o tipo de servidor radius, e adicionar estes parâmetros para seu servidor Radius do

Cisco Secure ACS for Windows. Deixe todos parâmetros restantes em seu estado padrão.**Authentication Server** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor Radius do Cisco Secure ACS for Windows.**Segredo de servidor** — Incorpore o servidor secreto radius. Este deve ser o mesmo segredo que você se usa quando você configura o VPN 3000 concentrator na configuração do Cisco Secure ACS for Windows.**Verifique** — Reenter a senha para verificação.

5. Escolha o **configuração > sistema > gerenciamento de endereço > atribuição** e verifique o **endereço do uso do Authentication Server** a fim atribuir o endereço IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN do IP pool criado no servidor Radius uma vez que o cliente obtém
autenticado.

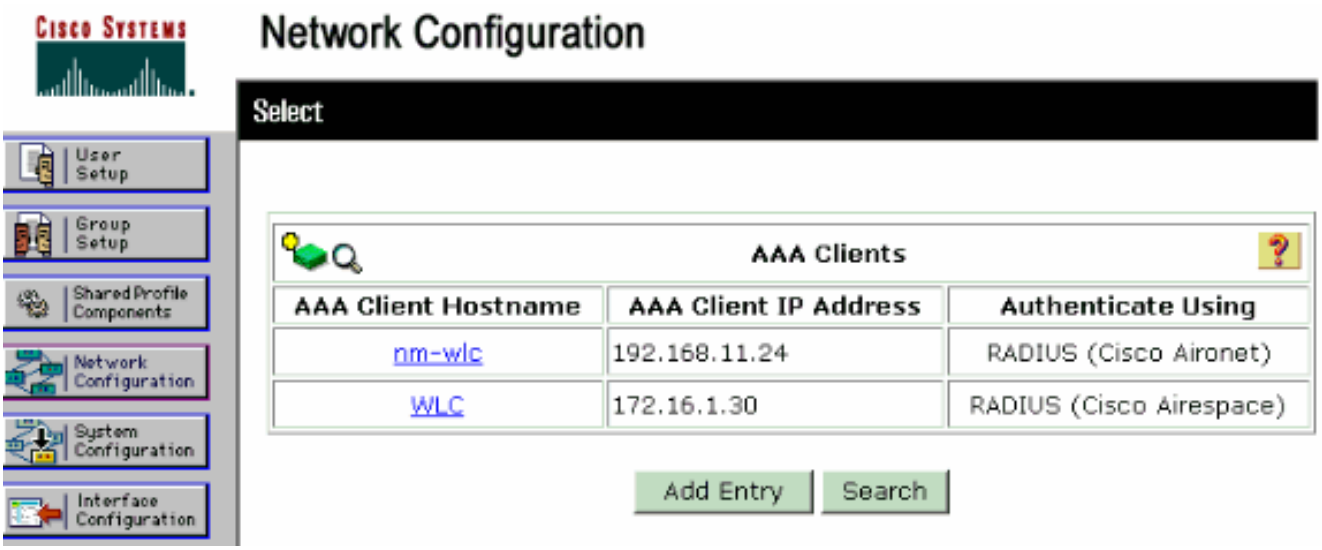


Configuração de servidor RADIUS

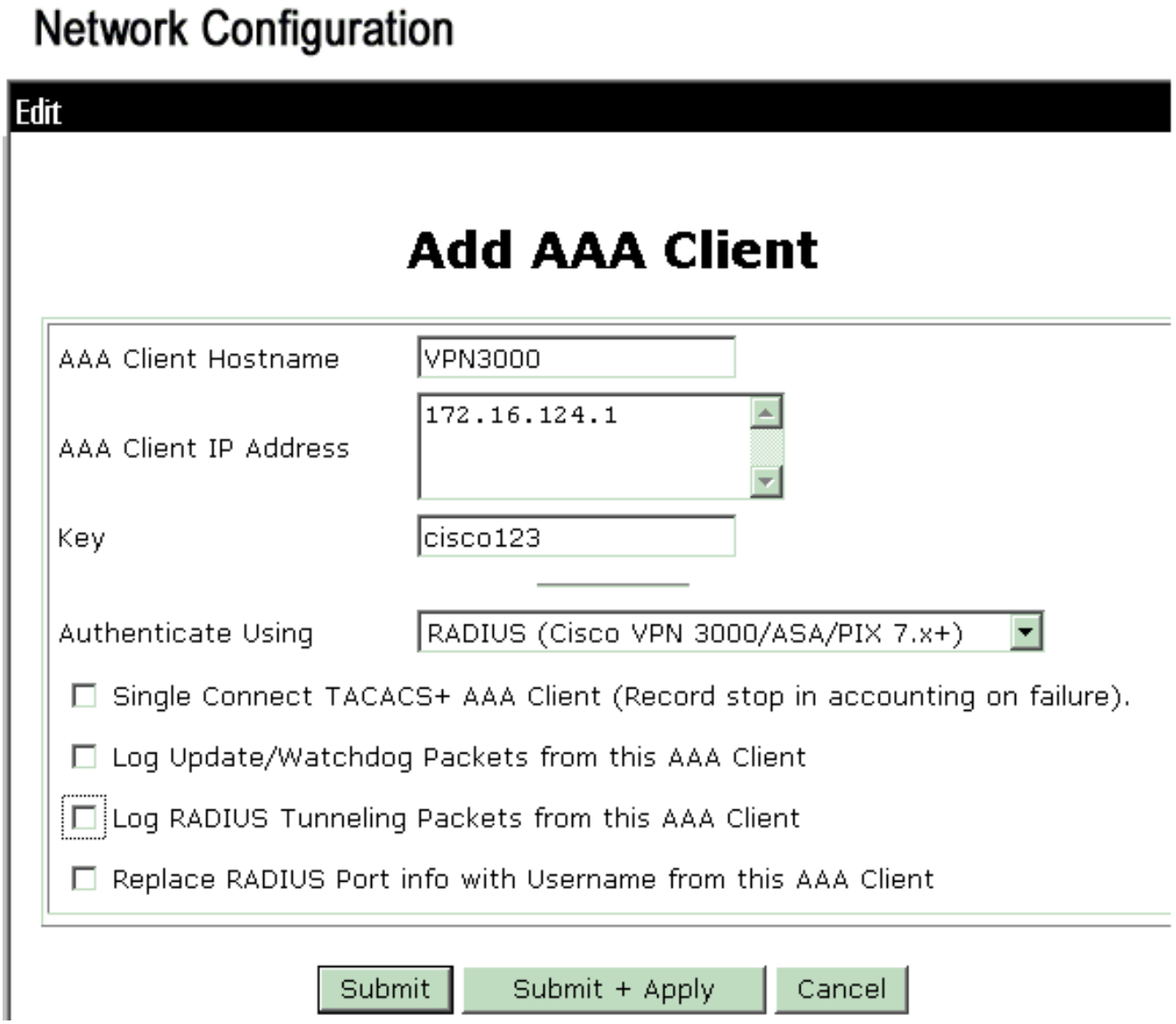
Esta seção do documento descreve o procedimento exigido configurar o Cisco Secure ACS como um servidor Radius para a autenticação de usuário do cliente VPN enviado pelo concentrador da Cisco VPN 3000 Series - cliente de AAA.

Fazer duplo clique o **ícone de Admin do ACS** a fim começar a sessão de administrador no PC que executa o servidor Radius do Cisco Secure ACS for Windows. Entre com o nome de usuário apropriado e a senha, se for necessário.

1. Termine estas etapas a fim adicionar o VPN 3000 concentrator à configuração do servidor do Cisco Secure ACS for Windows.Escolha a **configuração de rede** e o clique **adiciona a entrada** a fim adicionar um cliente de AAA ao servidor
Radius.

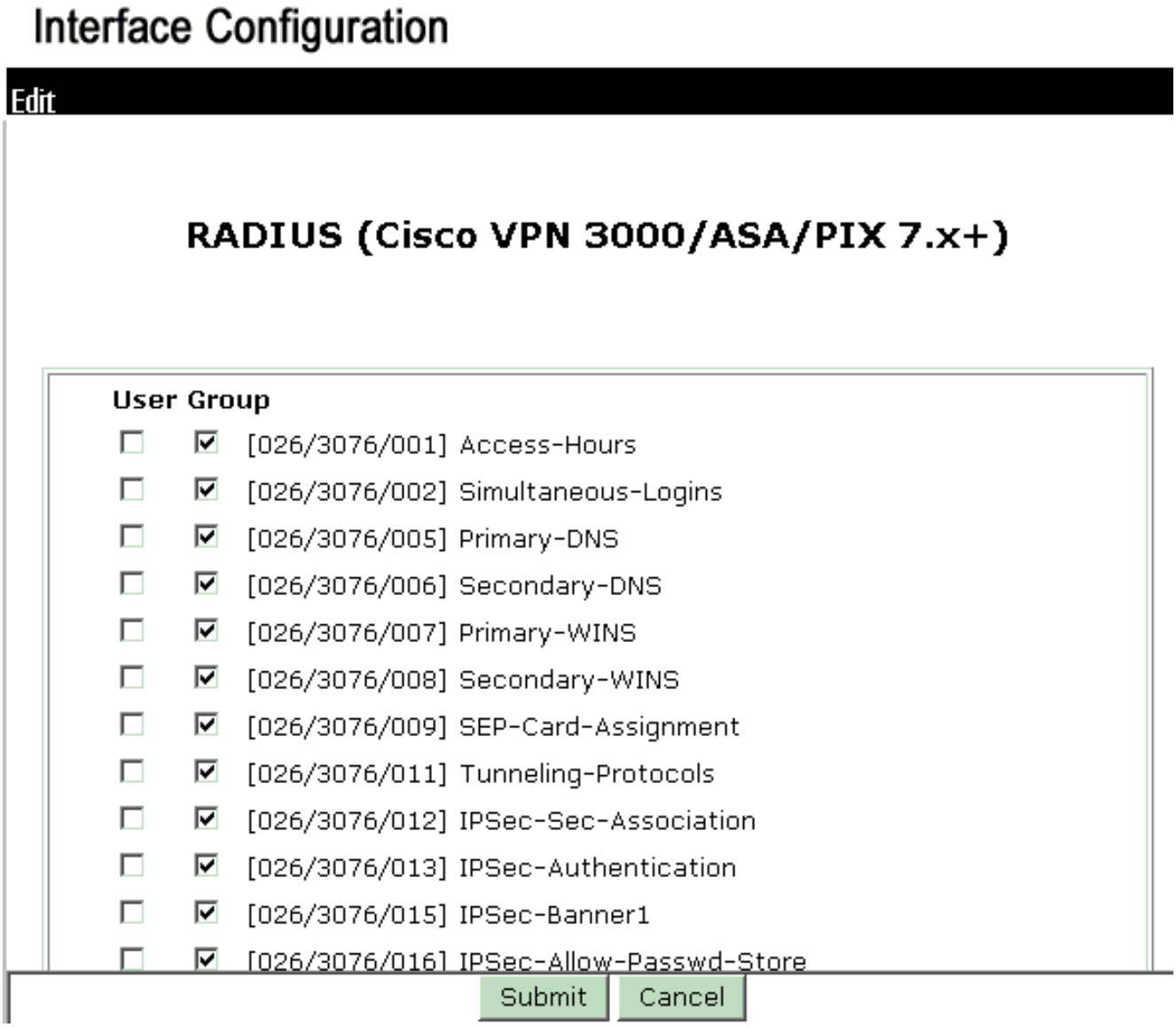


Adicionar estes parâmetros para seu VPN 3000 concentrator:



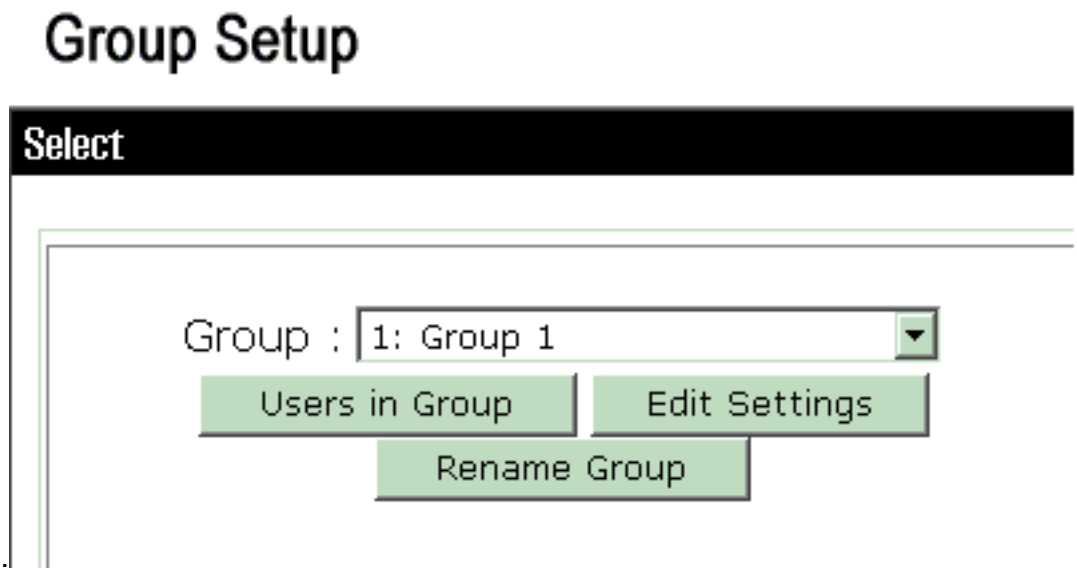
Nome de host do cliente AAA — Entre no hostname de seu VPN 3000 concentrator (para a resolução de DNS).**Endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu VPN 3000 concentrator.**Chave** — Incorpore o servidor secreto radius. Este deve ser o mesmo segredo que você configurou quando você adicionou o Authentication Server no concentrador VPN.**Autentique usando-se** — Escolha o **RAIO (Cisco VPN 3000/ASA/PIX 7.x+)**. Isto permite

que o VPN3000 VSA indique no indicador da configuração de grupo.Clique em Submit.Escolha a **configuração da interface**, clique o **RAIO (Cisco VPN 3000/ASA/PIX 7.x+)**, e verifique o **grupo [26] específico de fornecedor**.

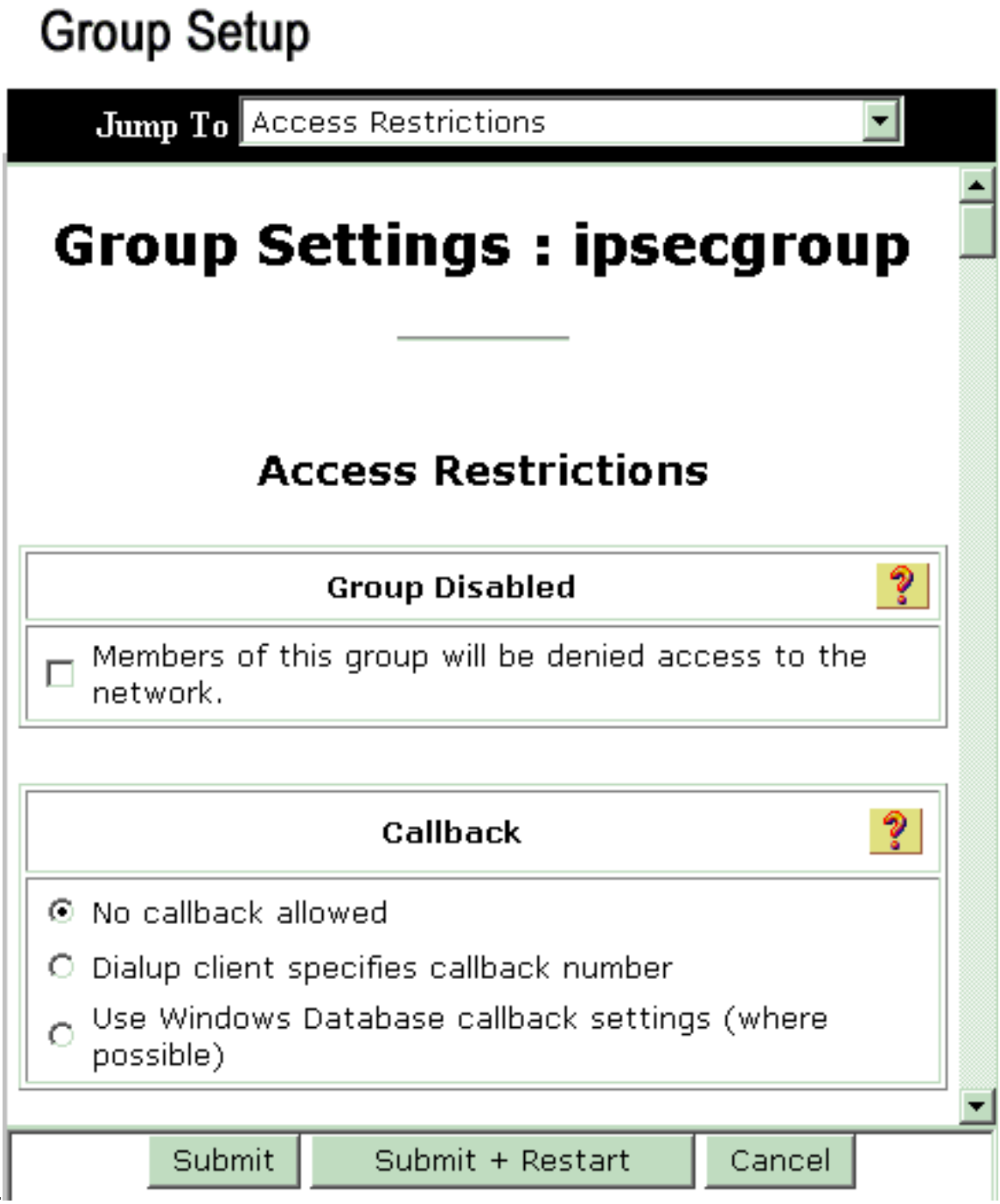


Nota: 'O atributo RADIUS 26' refere todos os atributos específicos do vendedor. Por exemplo, escolha a **configuração da interface > o RAIO (Cisco VPN 3000)** e veja que todos os atributos disponíveis começam com 026. Isto mostra que todos estes atributos específicos do vendedor caem sob o padrão do RADIUS IETF 26. Estes atributos não aparecem no usuário ou na instalação de grupo à revelia. A fim aparecer na instalação de grupo, crie um cliente de AAA (neste caso VPN 3000 concentrator) que autentique com RAIO na configuração de rede. Verifique então os atributos que precisam de aparecer na instalação de usuário, na instalação de grupo, ou em ambos da configuração da interface.Refira atributos RADIUS para obter mais informações sobre dos atributos disponíveis e de seu uso.Clique em Submit.

2. Termine estas etapas a fim adicionar grupos à configuração do Cisco Secure ACS for Windows.Escolha a **instalação de grupo**, a seguir selecione um dos grupos do molde, por exemplo, o grupo1, e o clique **rebatizam o**

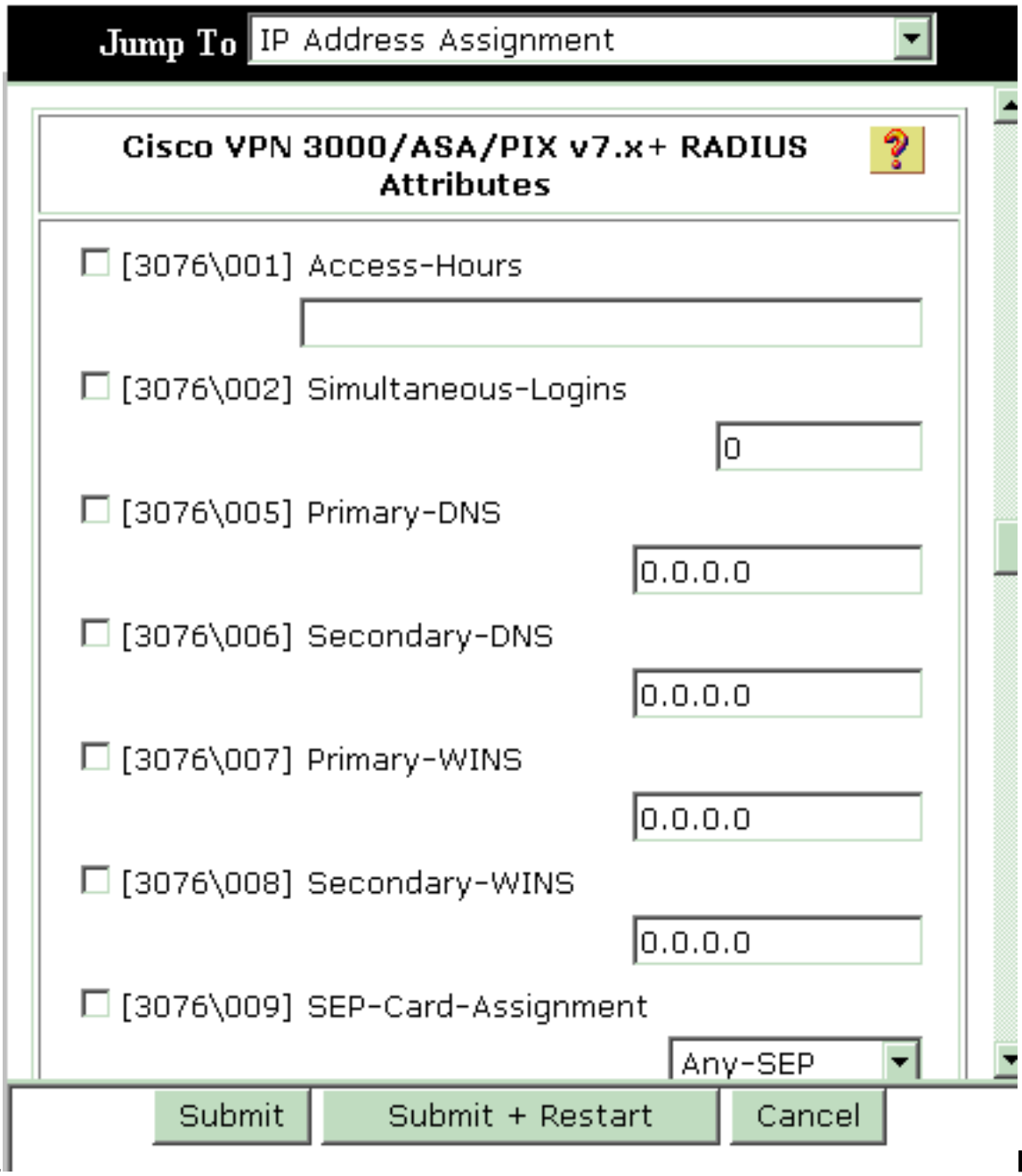


grupo. Mude o nome a algo apropriado para sua organização., por exemplo, ipsecgroup. Desde que os usuários são adicionados a estes grupos, faça o nome do grupo refletir a finalidade real desse grupo. Se todos os usuários são postos no mesmo grupo, você pode chamá-lo grupo de usuários VPN.O clique **edita ajustes** a fim editar os parâmetros em seu grupo recentemente



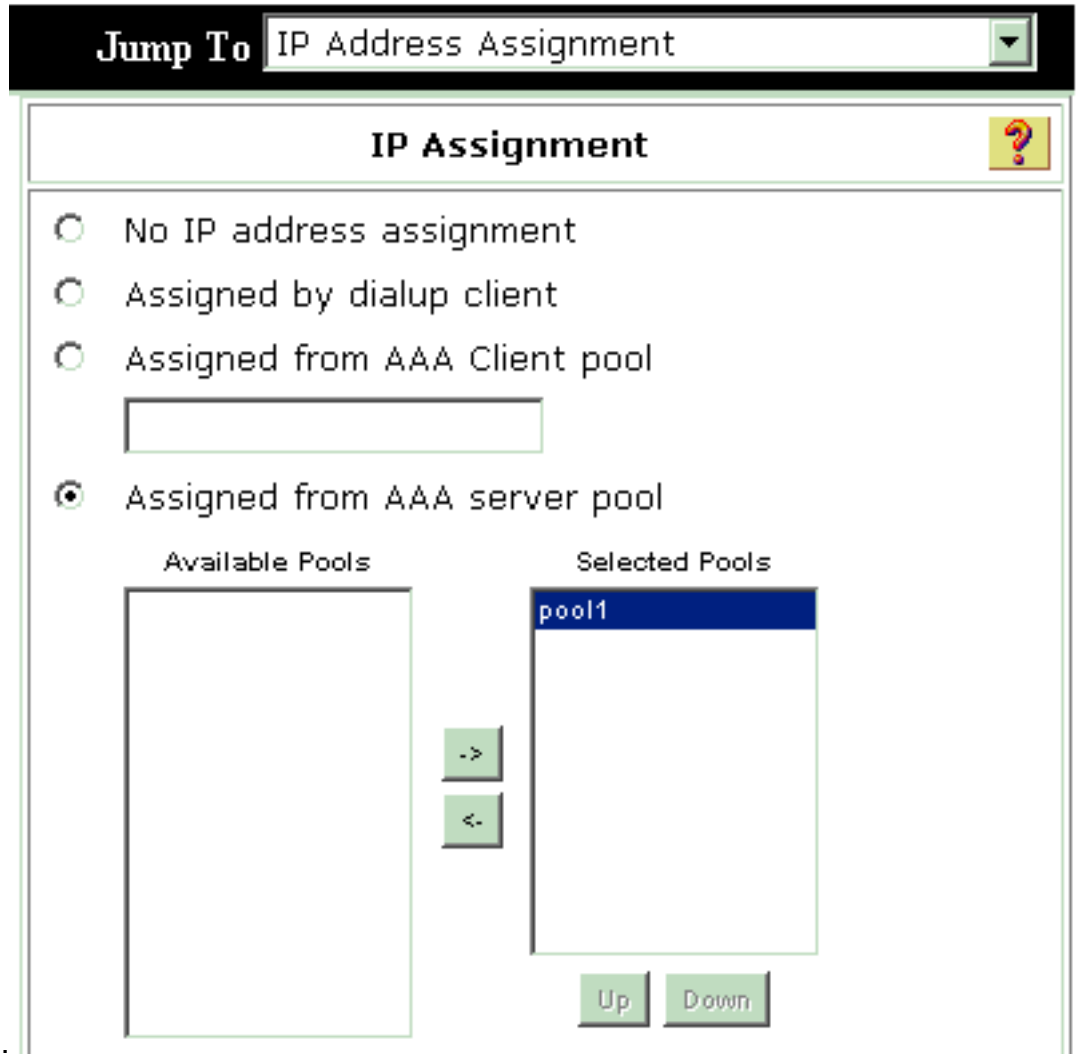
rebatizado.

Clique o **RAIO do Cisco VPN 3000** e configurar estes atributos recomendados. Isto permite os usuários atribuídos a este grupo para herdar os atributos RADIUS do Cisco VPN 3000, que permite que você centralize políticas para todos os usuários no Cisco Secure ACS for

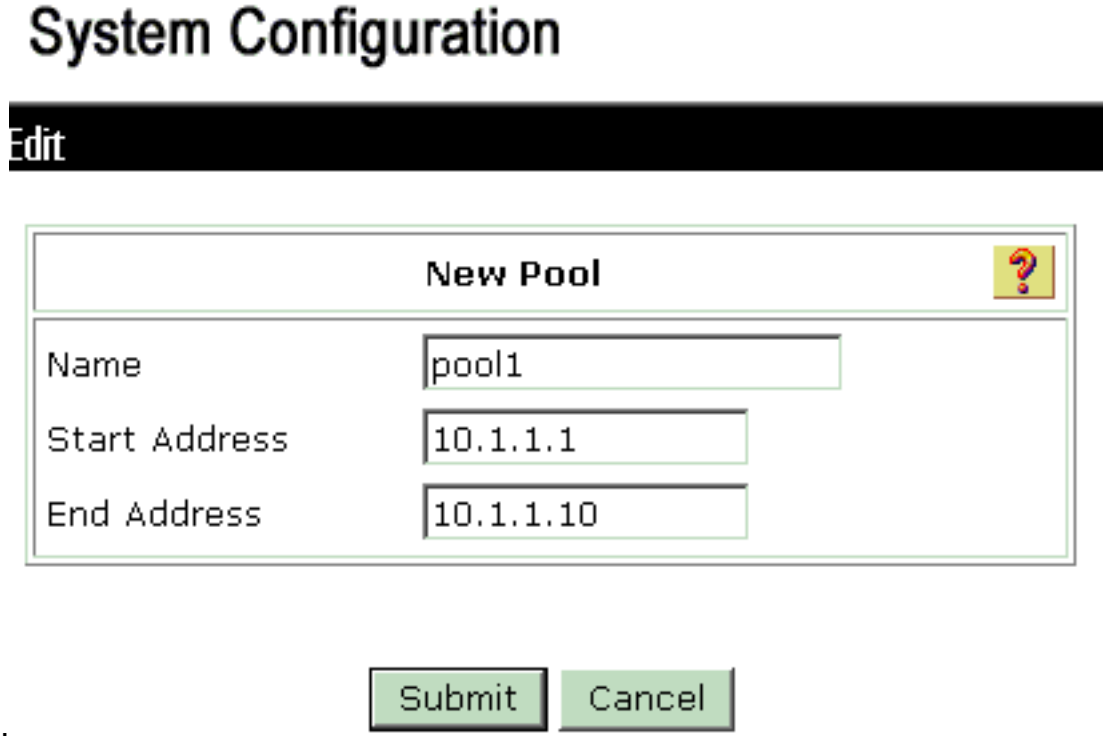


Windows. **No ta:** Tecnicamente, os atributos RADIUS VPN3000 não estão exigidos ser configurados enquanto o grupo de túneis se estabelece em etapa 3 da configuração do VPN 3000 series concentrator e o grupo base no concentrador VPN não muda das configurações padrão originais.**Atributos VPN3000 recomendados:DN principais** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor de DNS principal.**DN secundários** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor de DNS secundário.**Preliminar-VITÓRIAS** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor WINS principal.**Secundário-VITÓRIAS** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor secundário WINS.**Protocolos de tunelamento** — Escolha o **IPsec**. Isto permite *somente* conexões do cliente de IPSec. O PPTP ou o L2TP não são permitidos.**IPsec-SEC-associação** — Incorpore o **ESP-3DES-MD5**. Isto assegura-se de que todos seus clientes de IPSec conectem com a criptografia mais elevada disponível.**IPsec-Permitir-Senha-loja** — Escolha **recusam** assim que não são permitidos aos usuários salvar sua senha no cliente VPN.**IPsec-bandeira** — Entre em um banner de mensagem de boas-vindas a ser apresentado ao

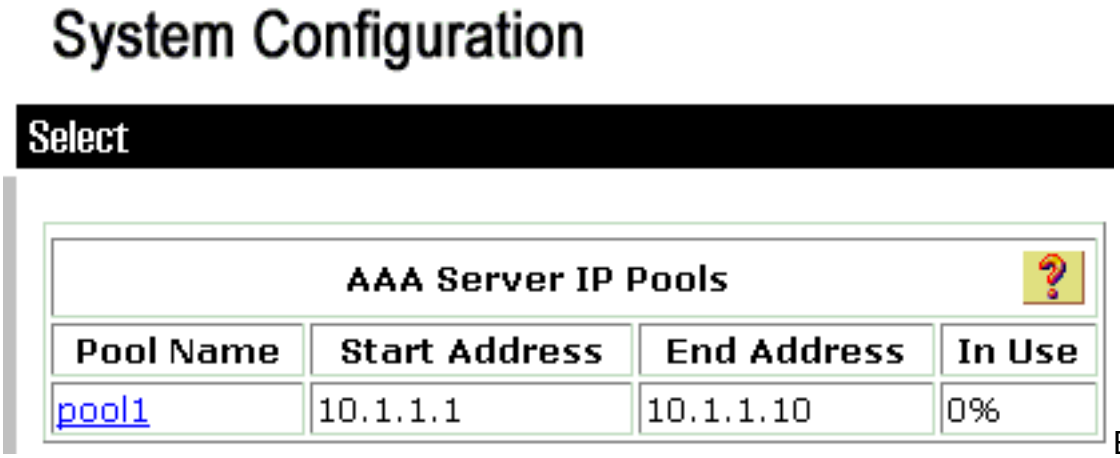
usuário em cima da conexão. Por exemplo, “boa vinda ao acesso do empregado VPN de MyCompany!”**Domínio do IPsec-padrão** — Incorpore o Domain Name de sua empresa. Por exemplo, “mycompany.com”.Este grupo de atributos não é necessário. Mas se você é incerto se os atributos de grupo base do VPN 3000 concentrator mudaram, a seguir Cisco recomenda que você configura estes atributos:**Simultâneo-inícios de uma sessão** — Entre no número de vezes que você permite que um usuário entre simultaneamente com o mesmo nome de usuário. A recomendação é 1 ou 2.**SEP-Cartão-atribuição** — Escolha o Algum-**SEP**.**IPsec-MODE-configuração** — Escolha **SOBRE**.**IPsec sobre o UDP** — Escolha **FORA**, a menos que você quiser usuários neste grupo conectar usando o IPsec sobre o protocolo UDP. Se você seleciona SOBRE, o cliente VPN ainda tem a capacidade para desabilitar o IPsec sobre o UDP e para conectá-lo localmente normalmente.**IPsec sobre a porta UDP** — Selecione um número de porta UDP na escala de 4001 a 49151. Isto é usado somente se o IPsec sobre o UDP está LIGADA.O grupo seguinte de atributos exige que você ajusta algo acima no concentrador VPN primeiramente antes que você possa os usar. Isto é recomendado somente para usuários avançados.**Horas do acesso** — Isto exige-o estabelecer uma escala das horas do acesso no VPN 3000 concentrator sob o **Configuration > Policy Management**. Em lugar de, use as horas do acesso disponíveis no Cisco Secure ACS for Windows para controlar este atributo.**IPsec-Separação-Túnel-lista** — Isto exige-o estabelecer um liste de redes no concentrador VPN sob o **configuração > gerenciamento de política > gerenciamento de tráfego**. Esta é uma lista de rede enviada para baixo ao cliente que diz o cliente para cifrar dados somente 2 aquelas redes na lista.Escolha a **atribuição IP na instalação de grupo** e a verificação **atribuída do pool do servidor AAA** a fim atribuir os endereços IP de Um ou Mais Servidores Cisco ICM NT aos usuários de cliente VPN uma vez que são obtém



autenticada. E scolha a **configuração de sistema > as associações IP** a fim criar um IP pool para usuários de cliente VPN e o clique **submete-**

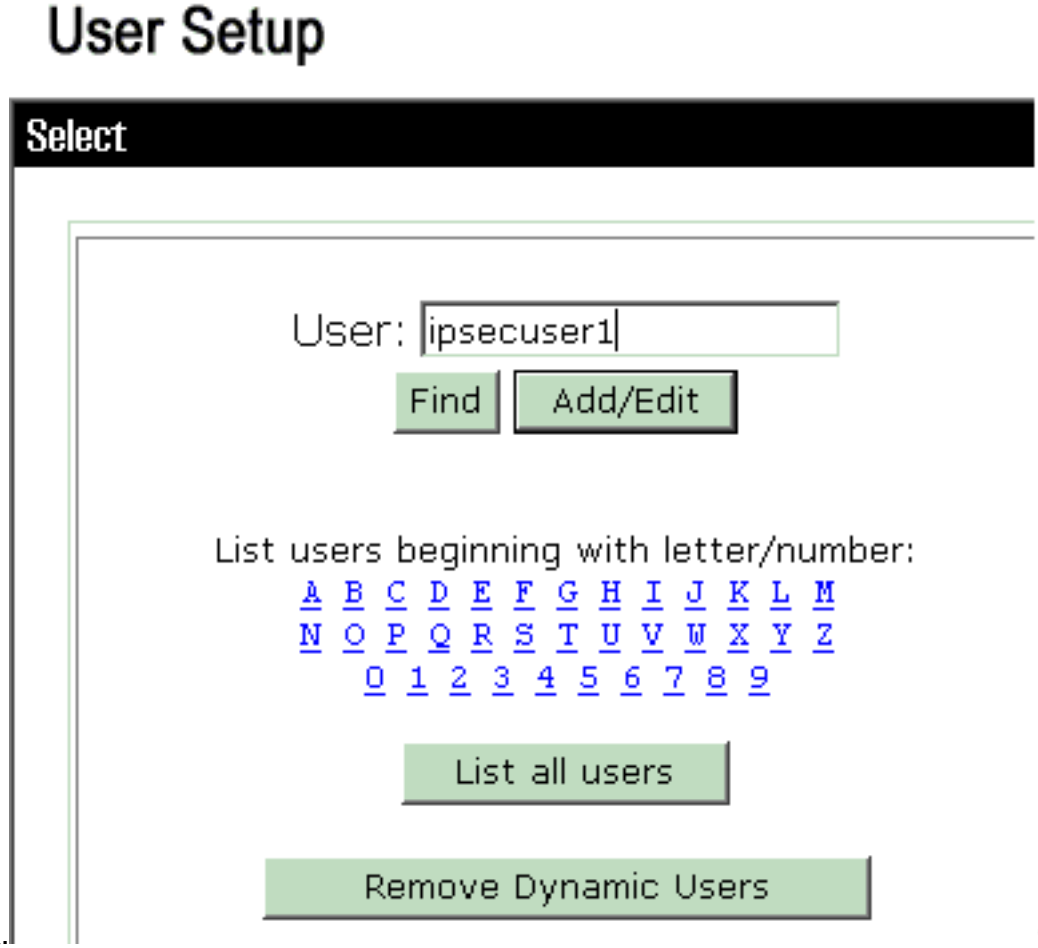


se.

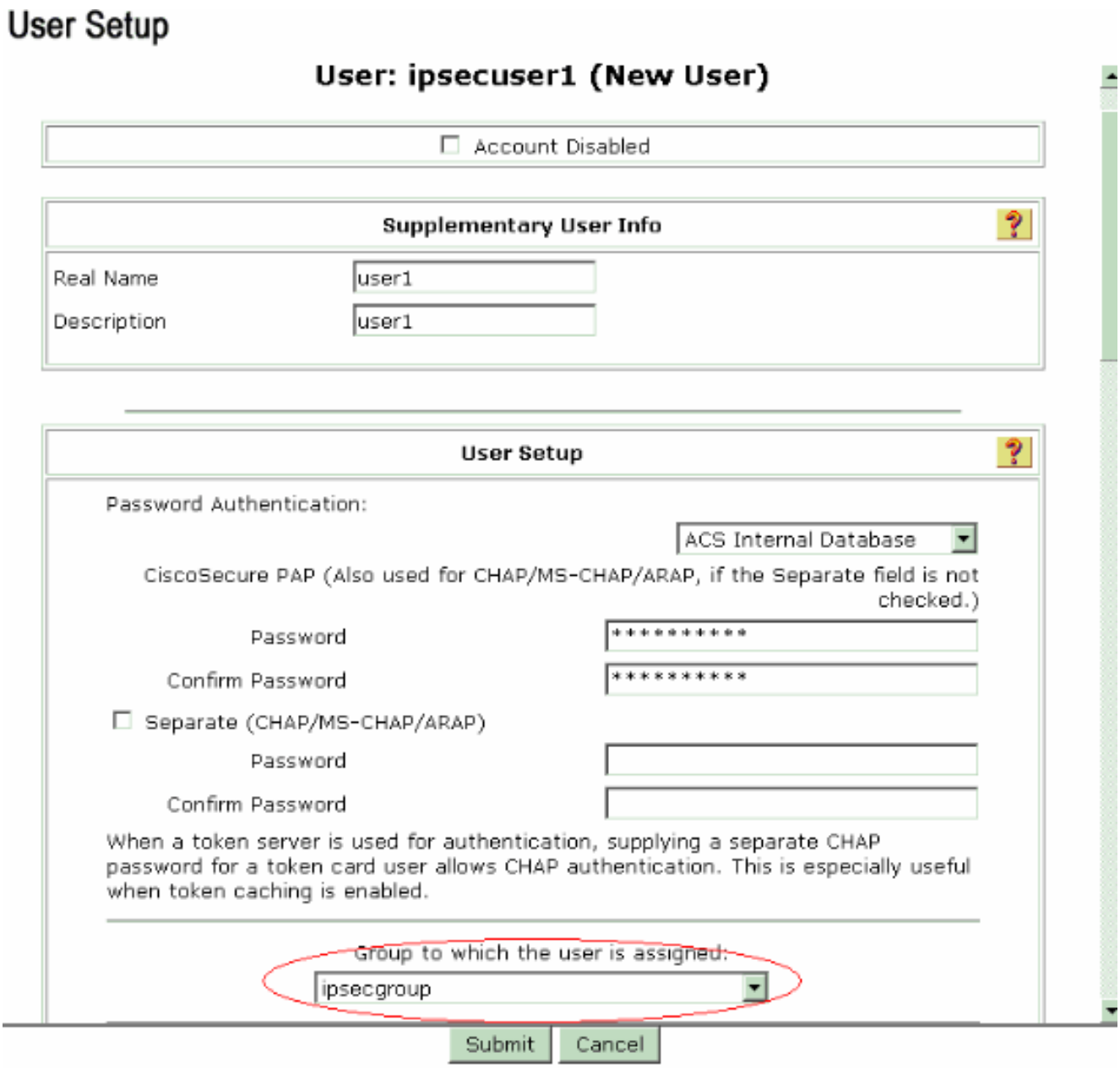


Escolha **submetem-se > reinício** a fim salvar a configuração e ativar o grupo novo.Repita estas etapas a fim adicionar mais grupos.

3. **Configurar usuários no Cisco Secure ACS for Windows.**Escolha a **instalação de usuário**, incorpore um username, e o clique **adiciona/edita**.



Confi gurar estes parâmetros sob a seção de instalação de usuário:

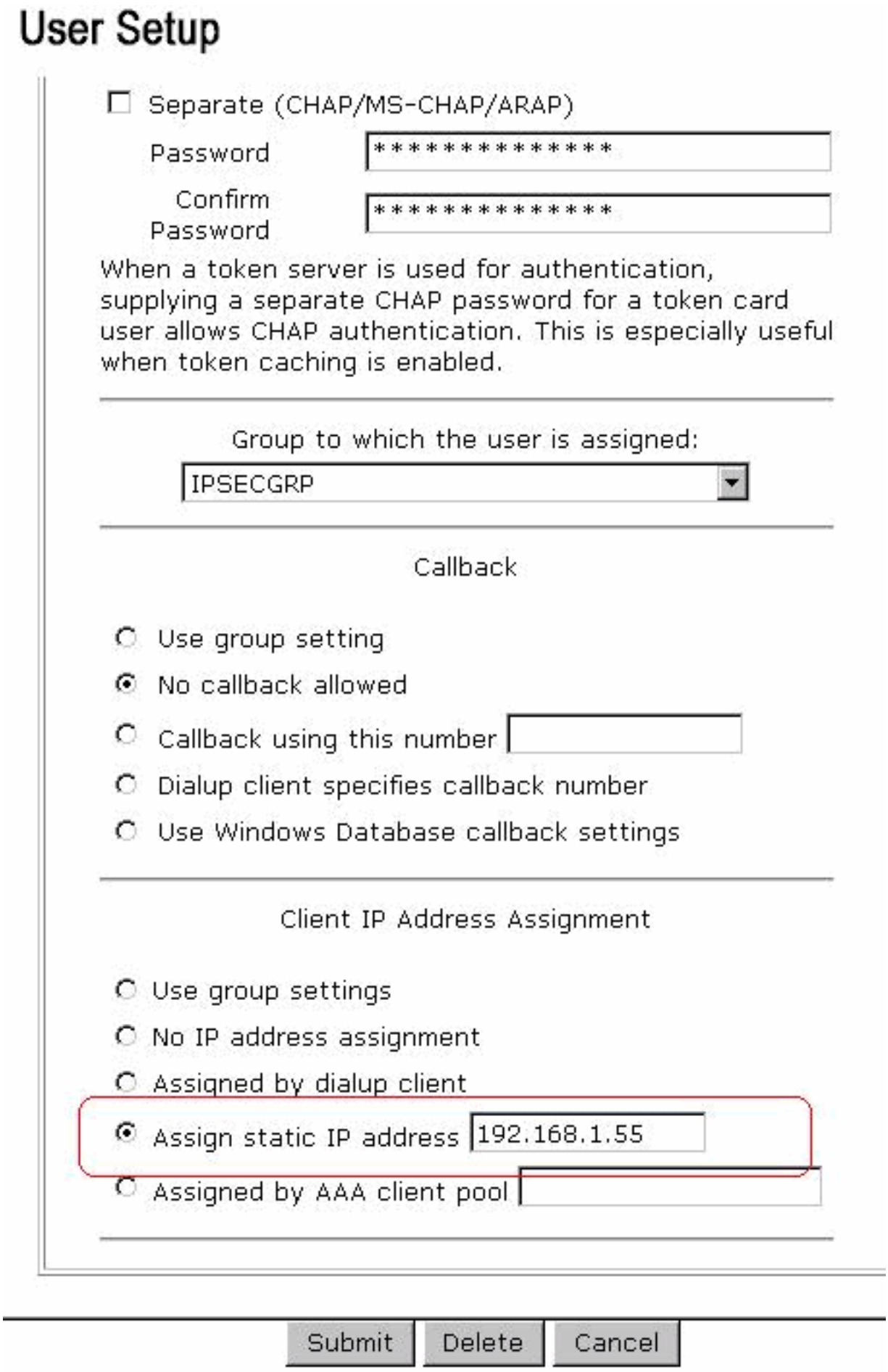


Autenticação de senha — Escolha o **base de dados interno ACS.Senha de PAP segura de Cisco** — Incorpore uma senha para o usuário.**Cisco PAP seguro - Confirme a senha** — Reenter a senha para o novo usuário.**O grupo a que o usuário é atribuído** — selecione o nome do grupo que você criou na etapa precedente.O clique **submete-se** a fim salvar e ativar as configurações de usuário.Repita estas etapas a fim adicionar usuários adicionais.

Atribua um endereço IP estático ao usuário de cliente VPN

Conclua estes passos:

1. Crie um grupo de VPN novo IPSECGRP.
2. Crie um usuário que queira receber o IP Estático e escolher **IPSECGRP**. Escolha **atribuem o endereço IP estático** com o endereço IP estático que é atribuído sob a atribuição de endereço IP

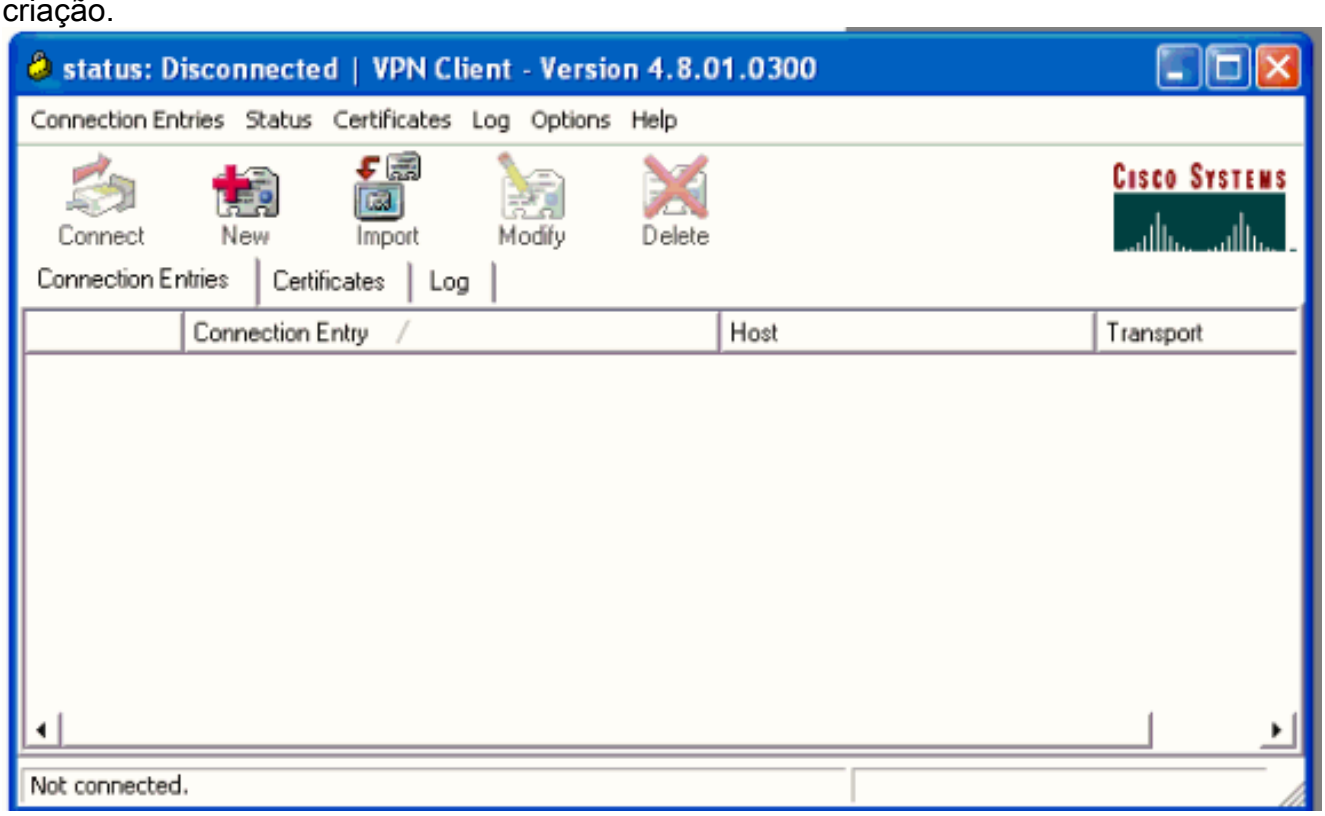


cliente.

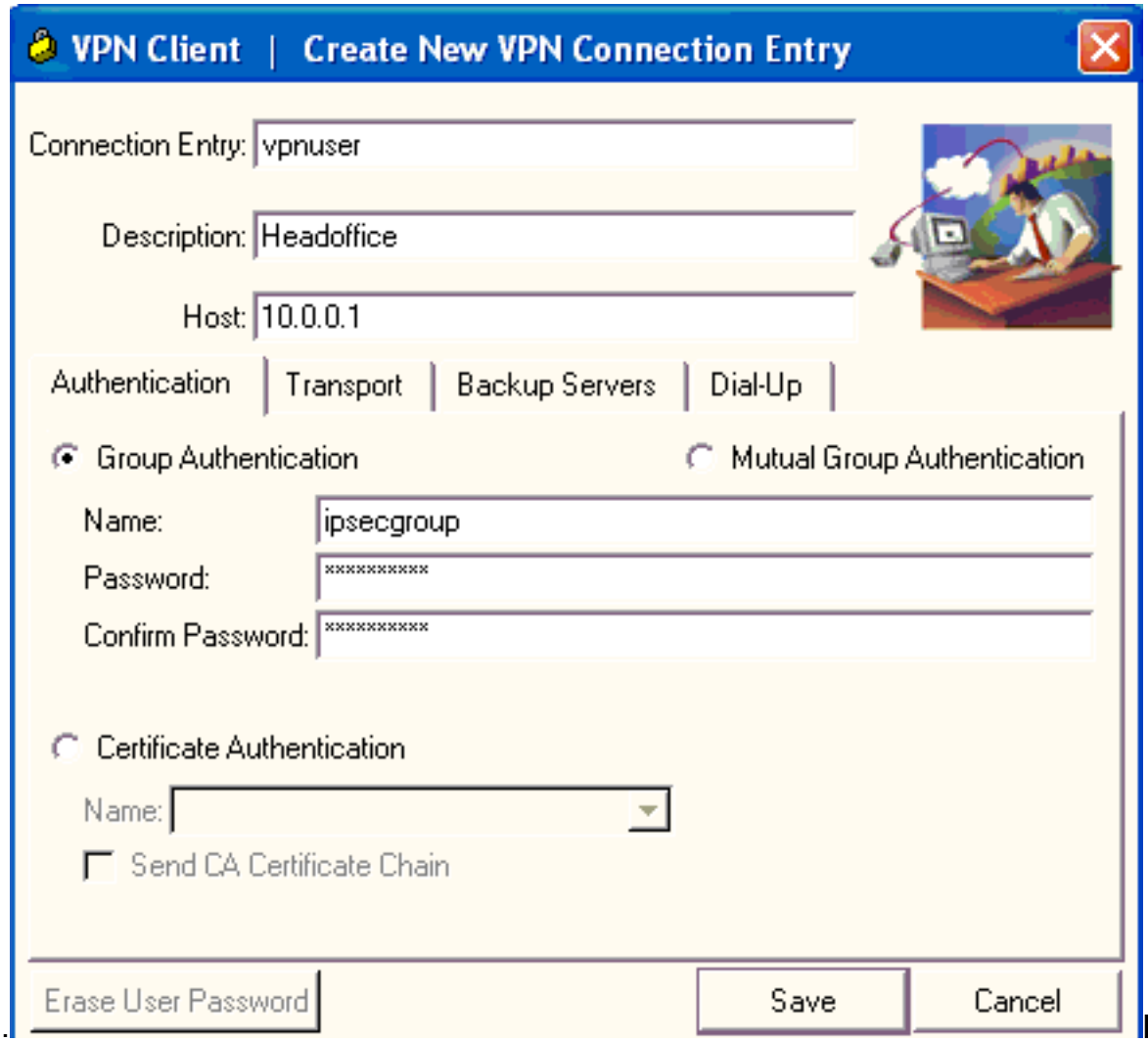
[Configuração de cliente VPN]

Esta seção descreve a configuração do lado do cliente VPN.

1. Escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN**.
2. Clique **novo** a fim lançar a janela de entrada nova da conexão de VPN da criação.



3. Quando solicitado, atribua um nome para sua entrada. Você pode inserir também uma descrição se desejar. Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface pública do VPN 3000 concentrator na coluna do host e escolha a **autenticação do grupo**. Forneça então o nome do grupo e a senha. Clique a **salvaguarda** a fim terminar a entrada nova da conexão de

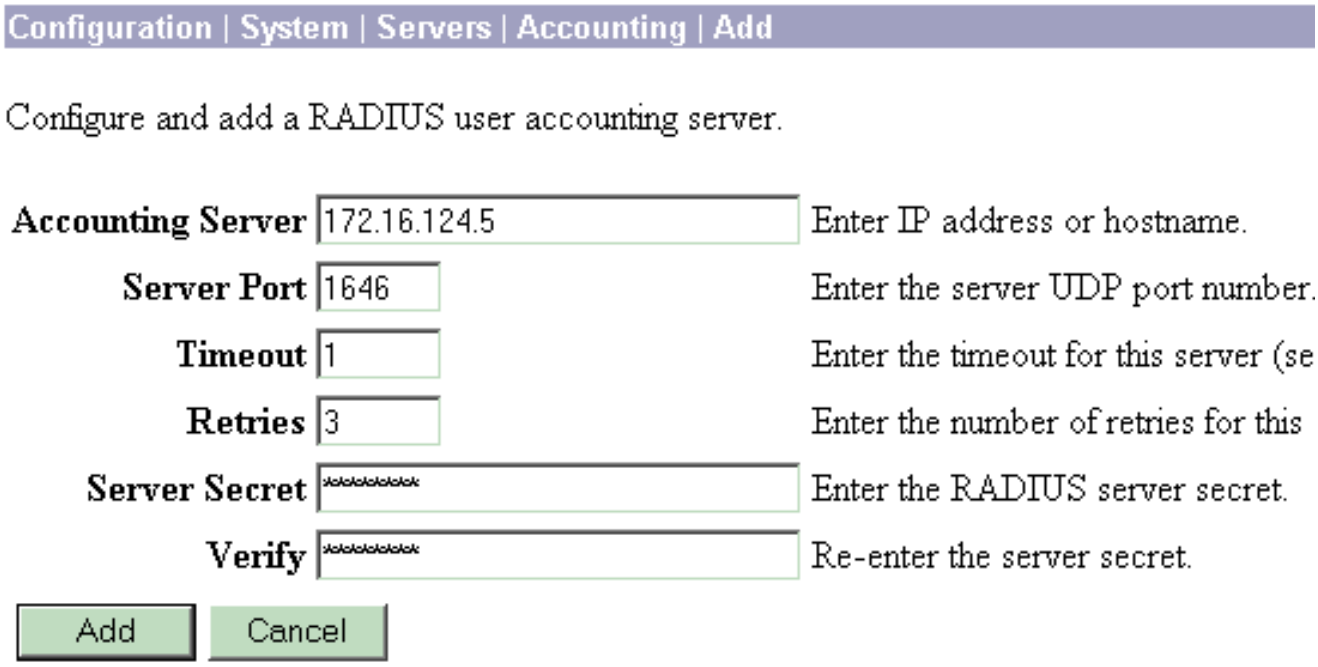


VPN. **Nota:** Seja certo que o cliente VPN está configurado para usar o mesmos nome do grupo e senha configurados no concentrador da Cisco VPN 3000 Series.

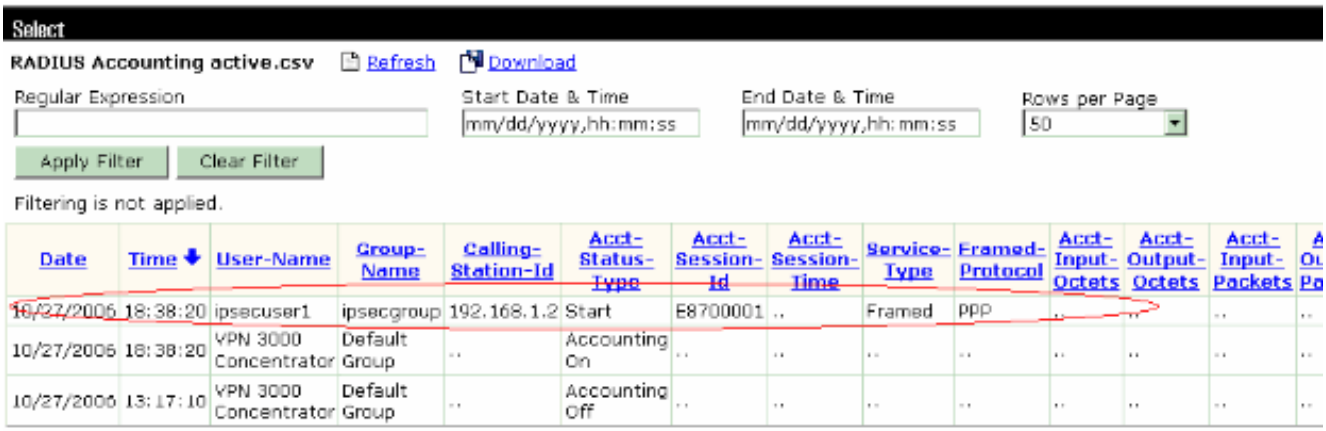
Adicionar relatório

Depois que a autenticação trabalha, você pode adicionar a contabilidade.

1. No VPN3000, escolha o **Configuração > Sistema > Servidores > Servidores de Contabilidade**, e adicionar o server do **Cisco Secure ACS for Windows**.
2. Você pode adicionar servidores de contabilidade individuais a cada grupo quando você escolhe o **configuration > user management > os grupos**, destaca um grupo e o clique **altera Acct. Server**. Incorpore então o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de contabilidade com o segredo de
servidor.



No Cisco Secure ACS for Windows, os registros de contabilidade aparecem enquanto esta saída
mostra:



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Verifique o concentrador VPN

No lado do VPN 3000 concentrator, escolha o **administração > sessões de administrador** a fim verificar o estabelecimento de túnel remoto VPN.

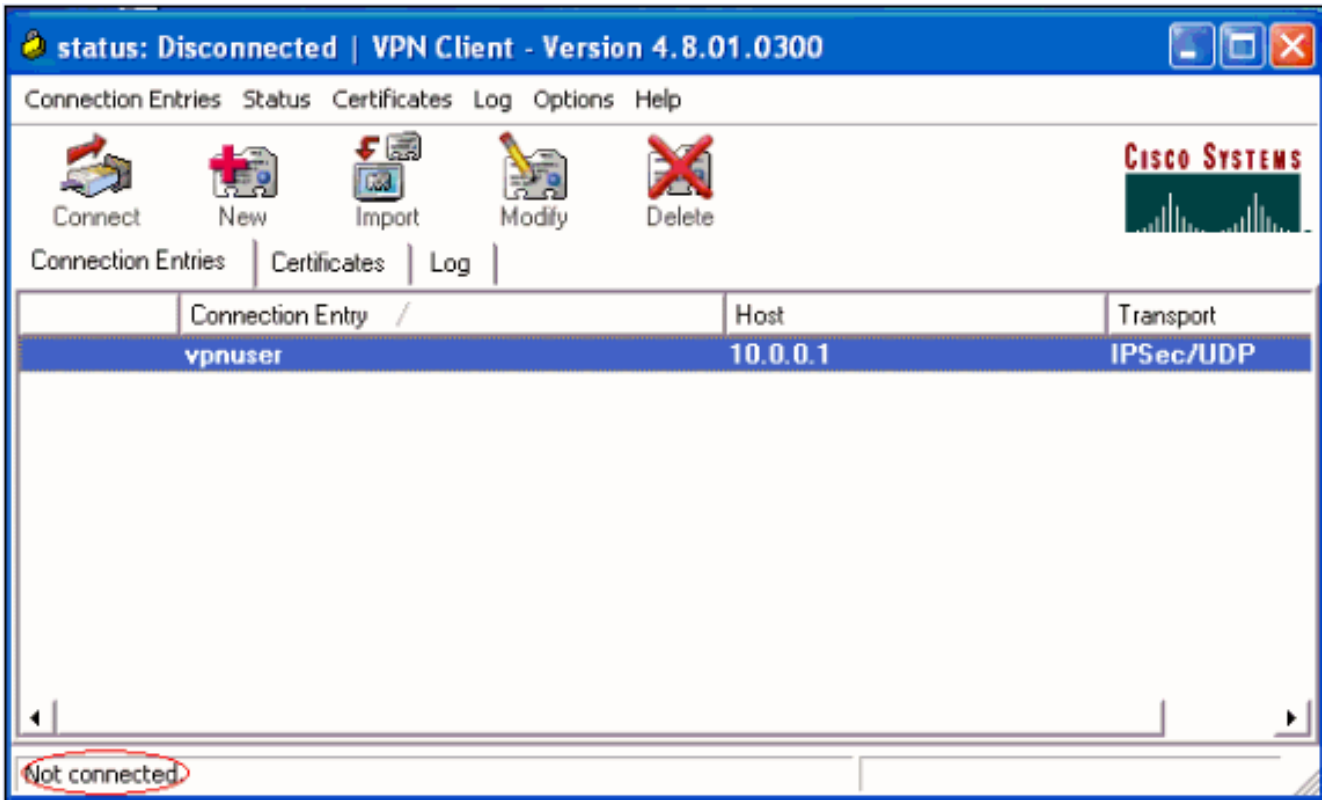
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout	Ping]

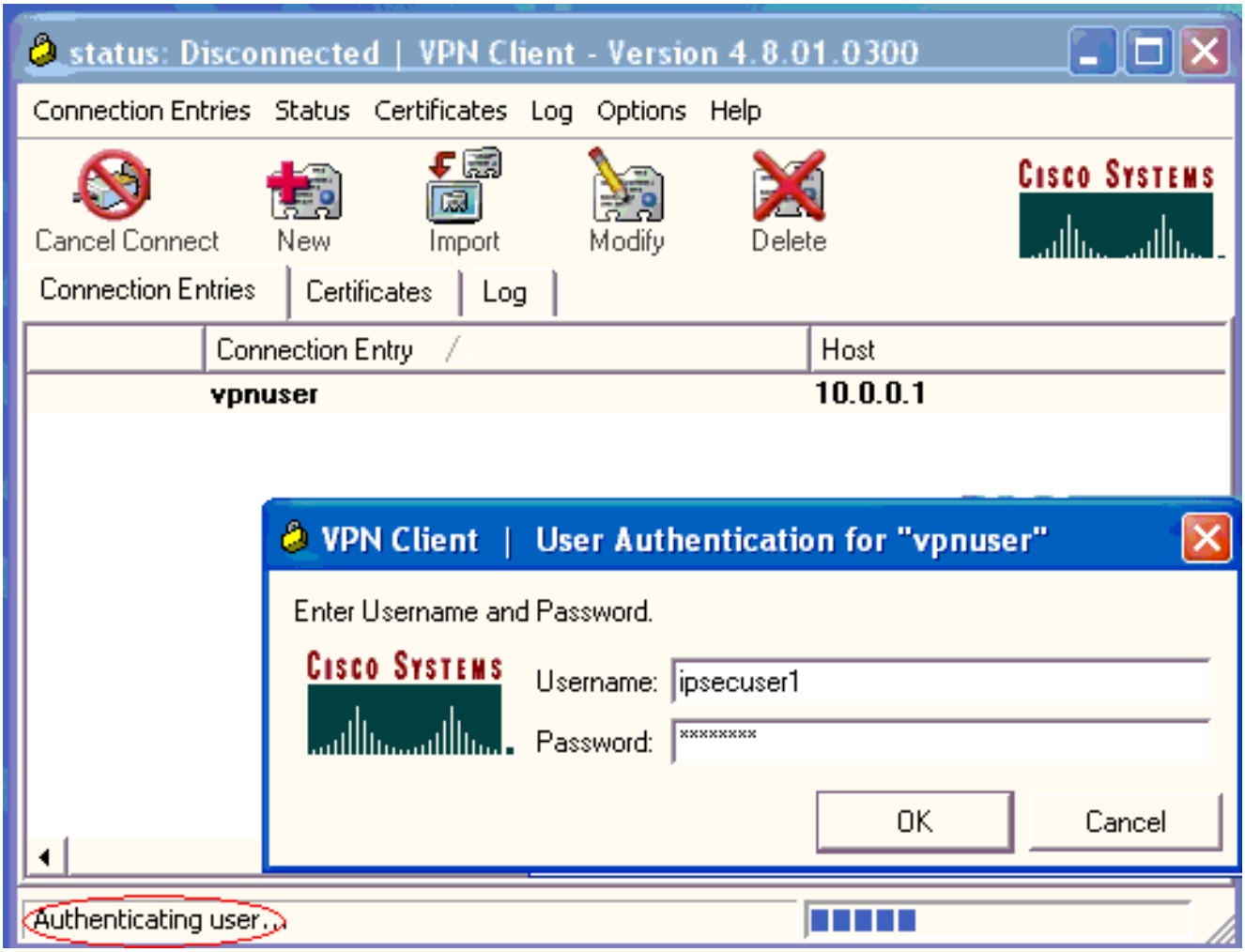
Verifique o cliente VPN

Termine estas etapas a fim verificar o cliente VPN.

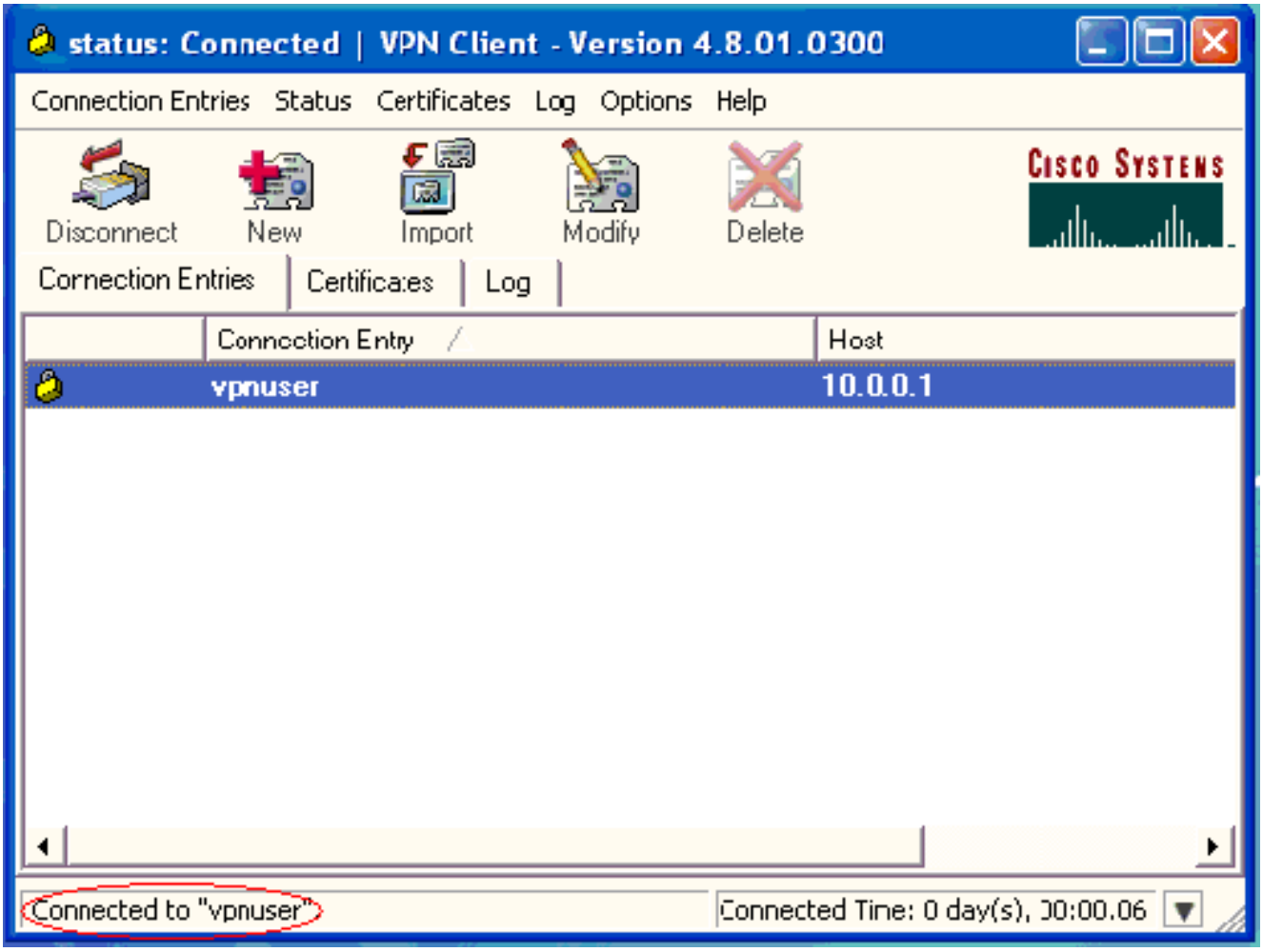
1. O clique **conecta** a fim iniciar uma conexão de VPN.



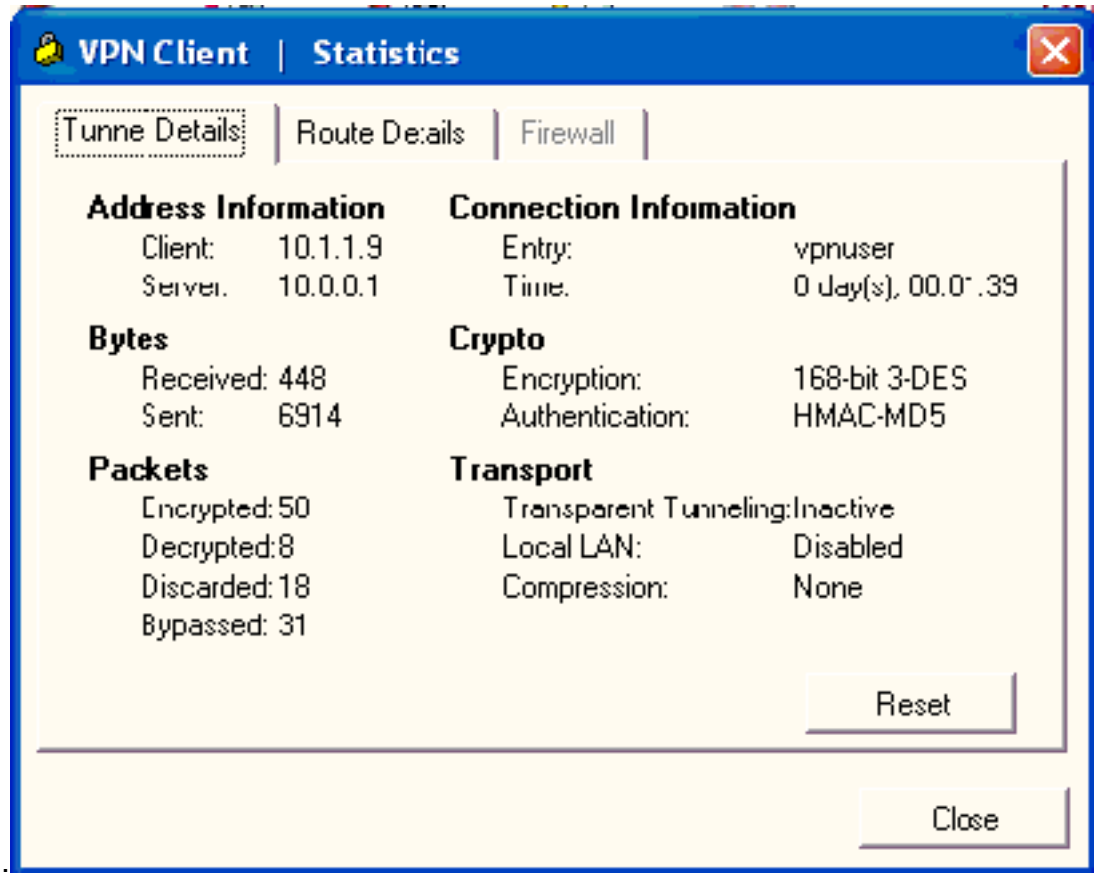
2. Este indicador aparece para a autenticação de usuário. Incorpore um nome de usuário válido e uma senha a fim estabelecer a conexão de VPN.



3. O cliente VPN obtém conectado com o VPN 3000 concentrator na instalação central.



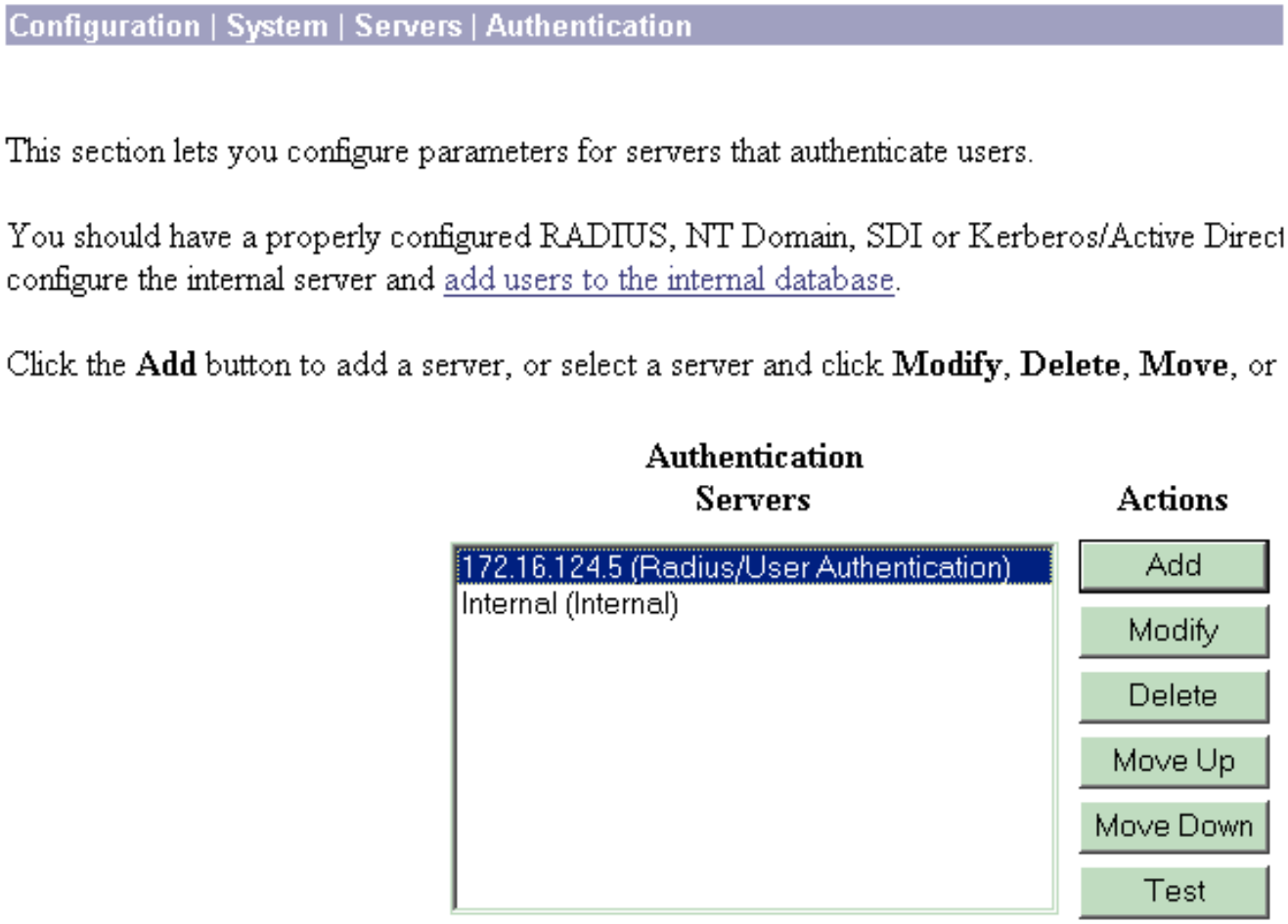
4. Escolha o **estado > as estatísticas** a fim verificar as estatísticas do túnel do cliente VPN.



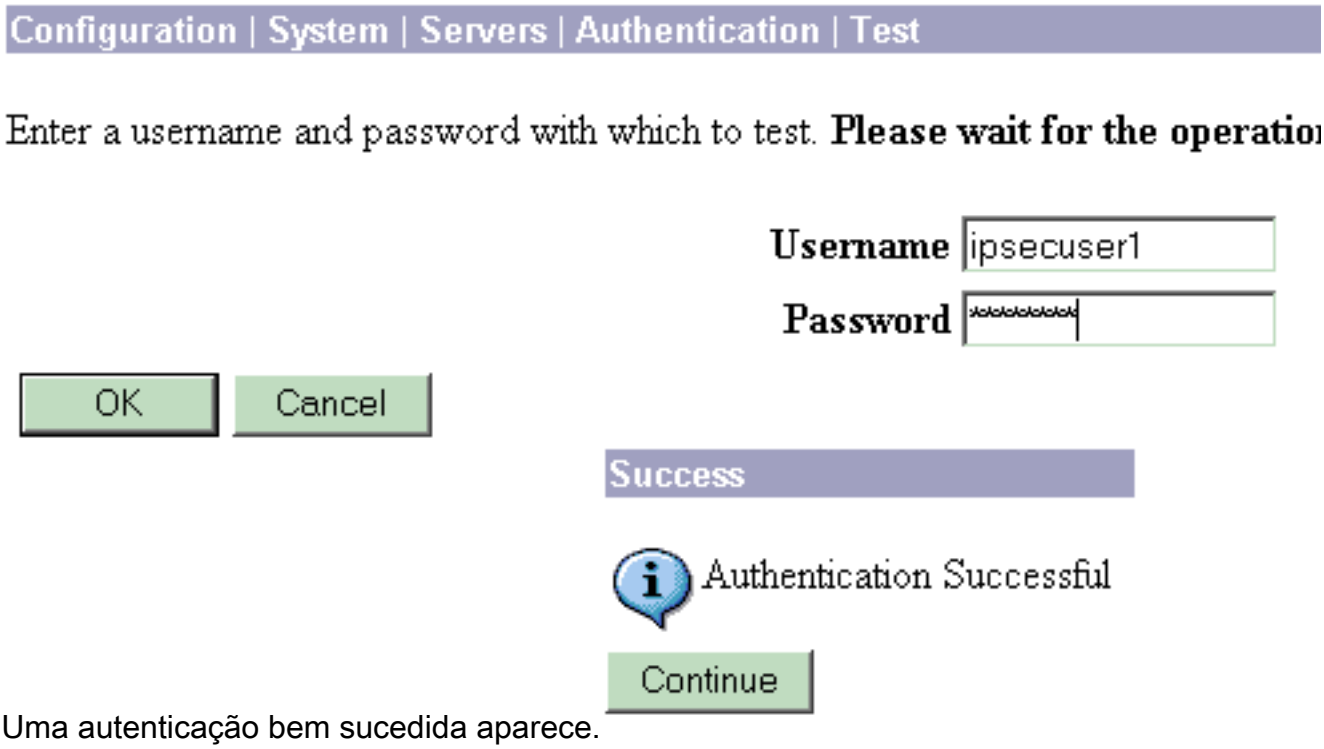
Troubleshooting

Termine estas etapas a fim pesquisar defeitos sua configuração.

1. Escolha o **configuração > sistema > servidores > autenticação** e termine estas etapas a fim testar a Conectividade entre o servidor Radius e o VPN 3000 concentrator.Selecione seu server, e clique então o
teste.

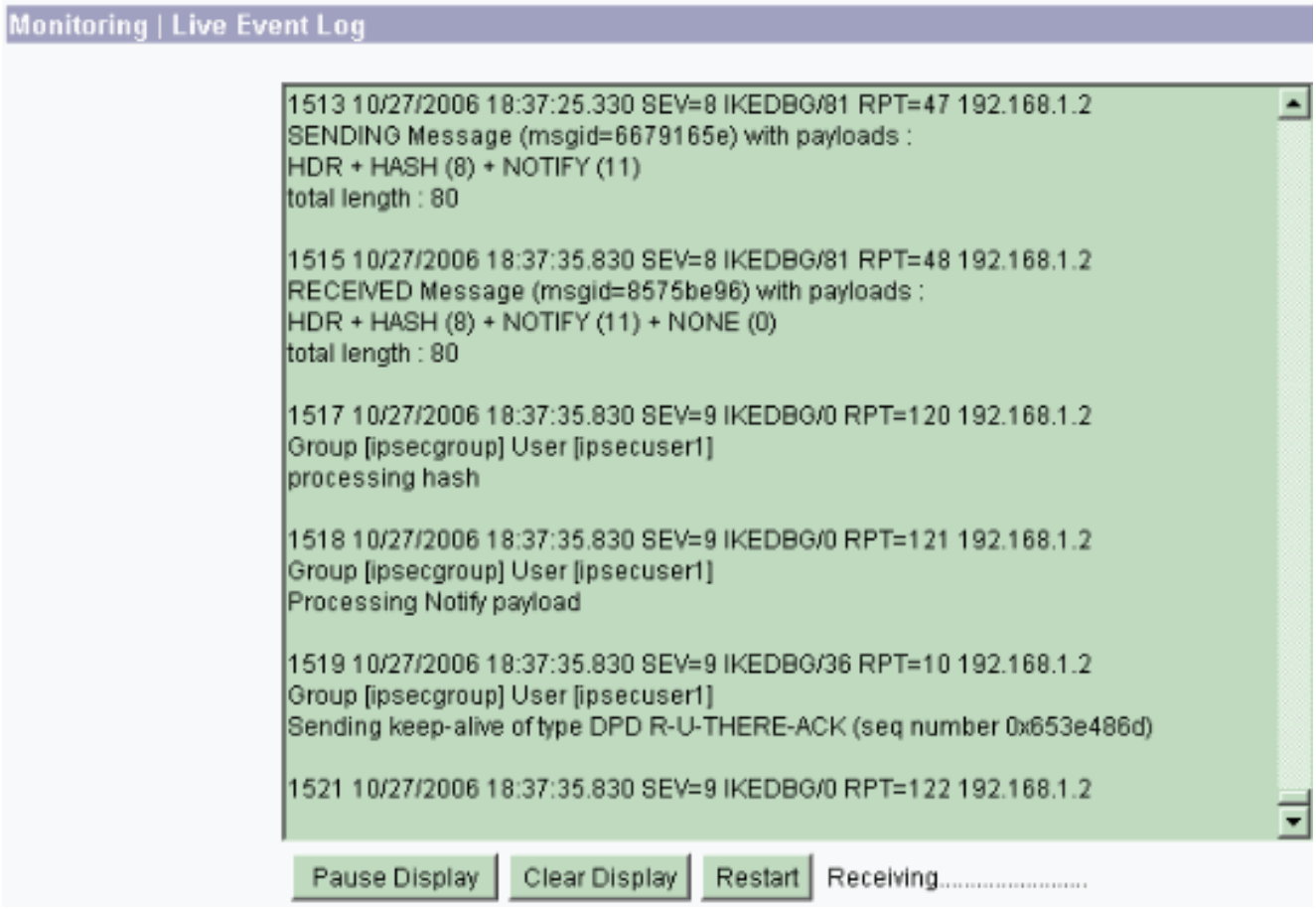


Incorpore o nome de usuário RADIUS e a senha e clique a
APROVAÇÃO.



Uma autenticação bem sucedida aparece.

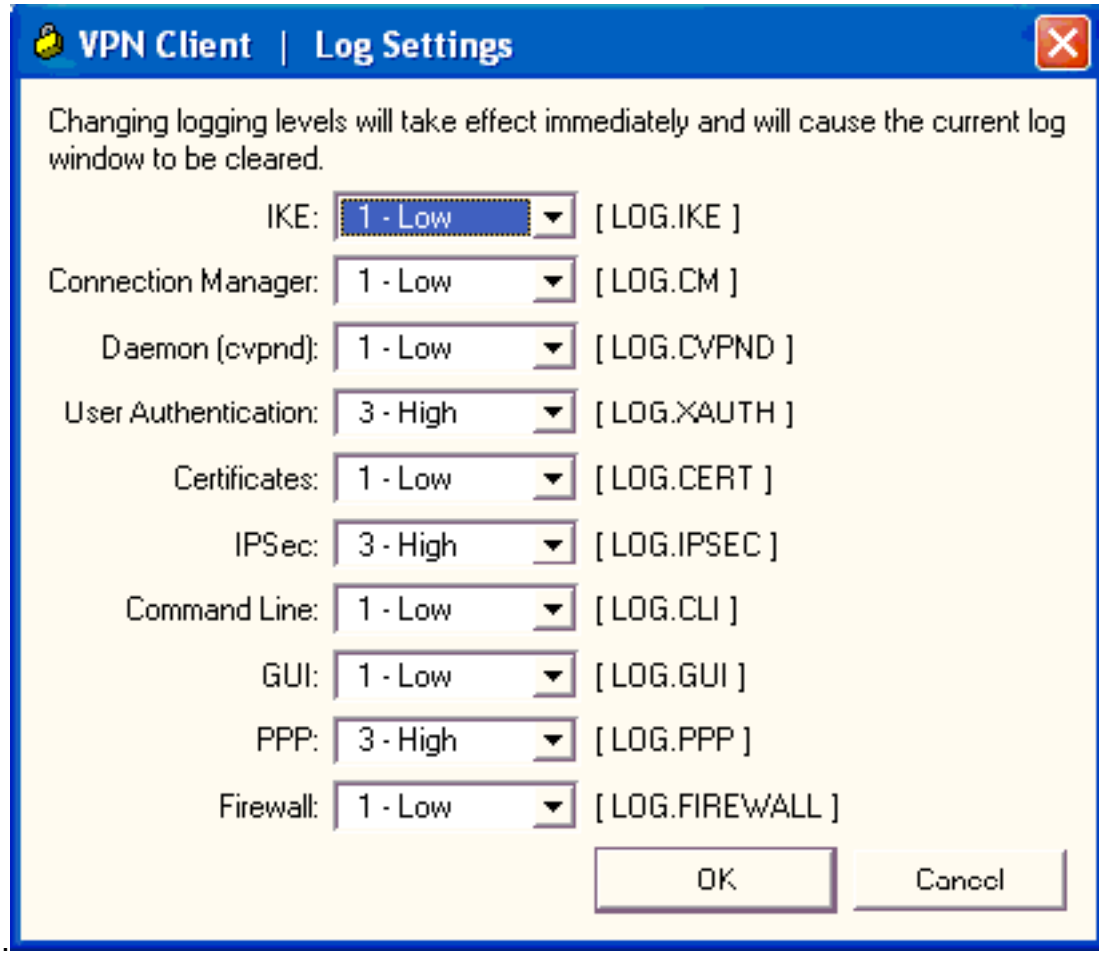
2. Se falha, há um problema de configuração ou um problema de conectividade IP. Verifique o fazer logon das falhas de tentativa o servidor ACS para ver se há mensagens relativas à falha.Se nenhuma mensagem aparece neste log então há provavelmente um problema de conectividade IP. A requisição RADIUS não alcança o servidor Radius. Verifique que os filtros aplicados à relação apropriada do VPN 3000 concentrator permitem 1645) pacotes do RAIO (dentro e para fora.Se a autenticação de teste é bem sucedida, mas os inícios de uma sessão ao VPN 3000 concentrator continuam a falhar, verifique o log filtrável de eventos através da porta de Console.Se as conexões não trabalham, você pode adicionar o AUTH, o IKE, e as classes de evento de IPSec ao concentrador VPN quando você seleciona o **Configuração > Sistema > Eventos > Classes > Modificar (severidade a Log=1-9, severidade a Console=1-3)**. O AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG, e o IPSECDECODE está igualmente disponível, mas pode fornecer demasiada informação. Se a informação detalhada é precisada nos atributos que estão passados para baixo do servidor Radius, o AUTHDECODE, o IKEDECODE, e o IPSECDECODE fornecem este na severidade ao nível Log=1-13.
3. Recupere o log de eventos da **monitoração > do log de eventos**.



Pesquise defeitos o cliente VPN 4.8 para Windows

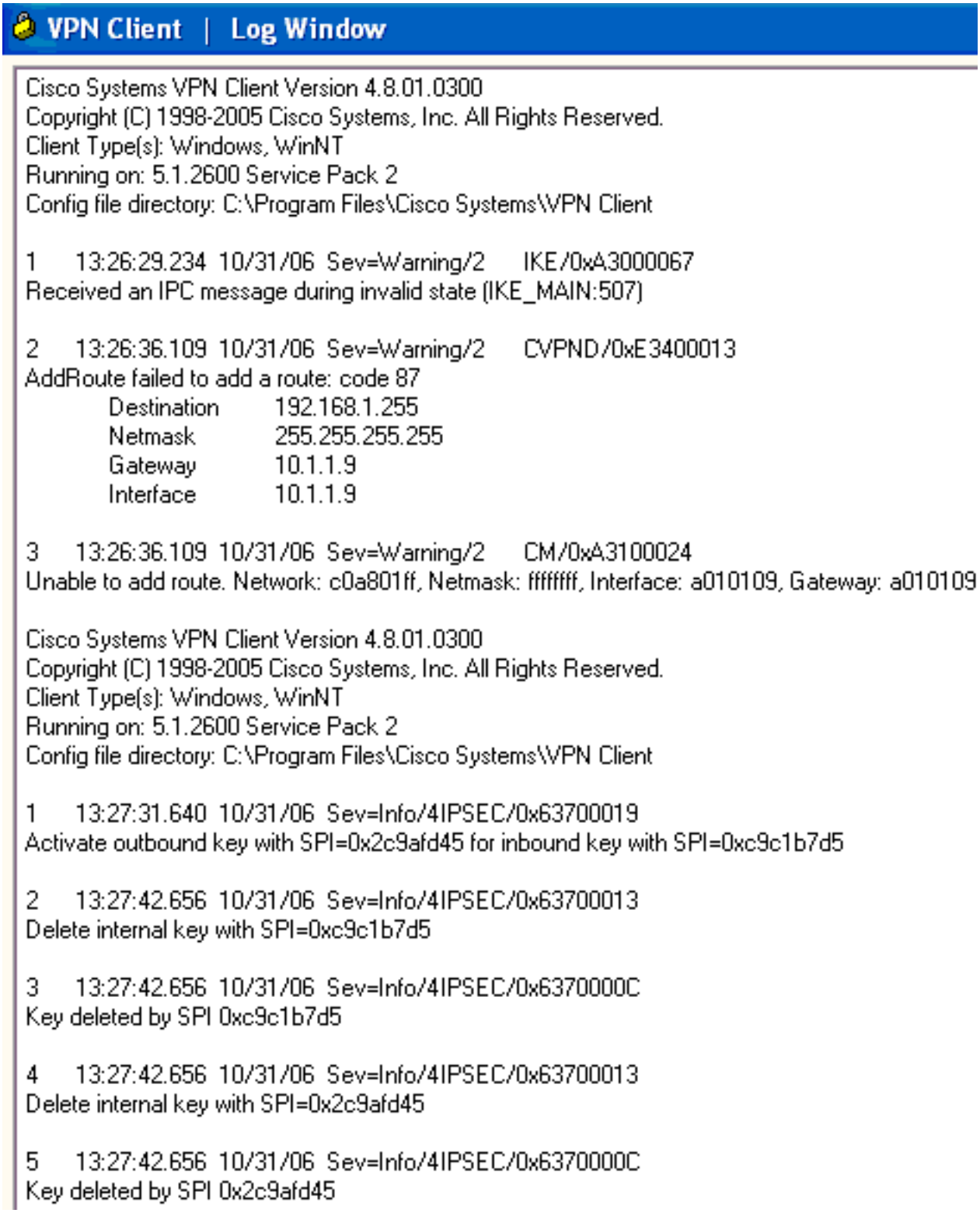
Termine estas etapas a fim pesquisar defeitos o cliente VPN 4.8 para Windows.

1. Escolha o **log > as configurações de registro** a fim permitir os níveis do log no cliente



VPN.

2. Escolha o **log > o indicador do log** a fim ver as entradas de registro no cliente VPN.



Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de Suporte do Cisco VPN Client
- Negociação IPsec/Protocolos IKE
- Cisco Secure ACS para página de suporte do Windows
- Configurando filtros dinâmicos em um servidor Radius
- Suporte Técnico e Documentação - Cisco Systems