Configurando o Cisco VPN 3000 Concentrator com Microsoft RADIUS

Contents

Introduction

O Microsoft Internet Authentication Server (IAS) e o Microsoft Commercial Internet System (MCIS 2.0) estão disponíveis no momento. O servidor Microsoft RADIUS é conveniente porque usa o Ative Diretory no Controlador de Domínio Primário para seu banco de dados de usuário. Você não precisa mais manter um banco de dados separado. Também suporta criptografia de 40 e 128 bits para conexões VPN Point-to-Point Tunneling Protocol (PPTP). Consulte a Lista de verificação da Microsoft: Configurando o IAS para a documentação de acesso de discagem e VPN para obter mais informações.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

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

Instalar e configurar o servidor RADIUS no Windows 2000 e Windows 2003

Instale o servidor RADIUS

Se o servidor RADIUS (IAS) já não estiver instalado, execute estas etapas para instalá-lo. Se você já tiver o servidor RADIUS instalado, continue com as etapas de configuração.

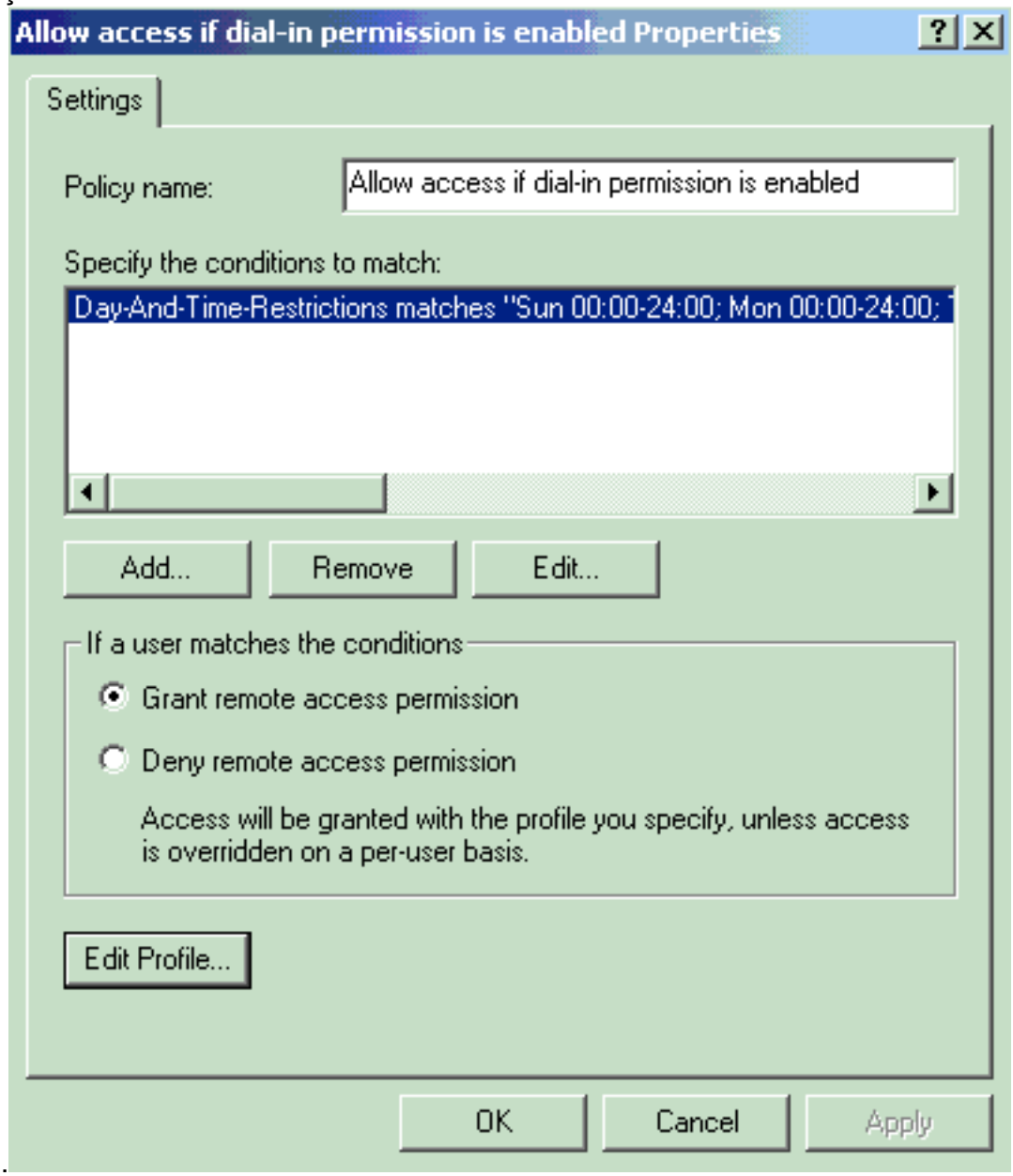
1. Insira o CD do Windows Server e inicie o programa de configuração.
2. Clique em **Install Add-On Components (Instalar componentes complementares)** e clique em **Add/Remove Windows Components (Adicionar/remover componentes do Windows)**.
3. Em Components (Componentes), clique em **Networking Services (Serviços de rede)** (mas não marque ou desmarque a caixa de seleção) e clique em **Details (Detalhes)**.
4. Marque **Internet Authentication Service** e clique em **OK**.
5. Clique em Next.

Configurar o Microsoft Windows 2000 Server com IAS

Conclua estes passos para configurar o servidor RADIUS (IAS) e iniciar o serviço para disponibilizá-lo para autenticar usuários no VPN Concentrator.

1. Escolha **Iniciar > Programas > Ferramentas Administrativas > Serviço de Autenticação na Internet**.
2. Clique com o botão direito do mouse em **Internet Authentication Service** e clique em **Properties** no submenu exibido.
3. Acesse a guia RADIUS para examinar as configurações das portas.Se a autenticação RADIUS e as portas UDP (User Datagram Protocol) de contabilidade RADIUS diferirem dos valores padrão fornecidos (1812 e 1645 para autenticação, 1813 e 1646 para contabilização) em Authentication and Accounting, digite suas configurações de porta. Clique em **OK** quando terminar.**Observação:** não altere as portas padrão. Separe as portas usando vírgulas para usar várias configurações de porta para solicitações de autenticação ou tarifação.
4. Clique com o botão direito do mouse em **Clients** e escolha **New Client** para adicionar o VPN Concentrator como um cliente de autenticação, autorização e contabilização (AAA) ao servidor RADIUS (IAS).**Observação:** se a redundância for configurada entre dois Cisco VPN 3000 Concentrators, o Cisco VPN 3000 Concentrator de backup também deverá ser adicionado ao servidor RADIUS como um cliente RADIUS.
5. Digite um nome amigável e selecione como **Protocol Radius**.
6. Defina o VPN Concentrator com um endereço IP ou nome DNS na próxima janela.
7. Escolha **Cisco** na barra de rolagem Client-Vendor.
8. Insira um segredo compartilhado.**Observação:** você deve se lembrar do segredo *exato* que usa. Você precisa dessas informações para configurar o VPN Concentrator.

9. Clique em Finish.
10. Clique duas vezes em **Políticas de acesso remoto** e clique duas vezes na diretiva exibida no lado direito da janela.**Observação:** depois de instalar o IAS, uma política de acesso remoto já deve existir.No Windows 2000, a autorização é concedida com base nas propriedades de discagem de uma conta de usuário e nas políticas de acesso remoto. As políticas de acesso remoto são um conjunto de condições e configurações de conexão que dão aos administradores de rede mais flexibilidade na autorização de tentativas de conexão. O serviço de Roteamento e Acesso Remoto do Windows 2000 e o IAS do Windows 2000 usam políticas de acesso remoto para determinar se aceita ou rejeita tentativas de conexão. Em ambos os casos, as políticas de acesso remoto são armazenadas localmente. Consulte a documentação do IAS do Windows 2000 para obter mais informações sobre como as tentativas de conexão são processadas.



11. Escolha **Conceder permissão de acesso remoto** e clique em **Editar perfil** para configurar propriedades de discagem.
12. Selecione o protocolo a ser usado para autenticação na guia Autenticação. Verifique a **Microsoft Encrypted Authentication versão 2** e desmarque todos os outros protocolos de autenticação.**Observação:** as configurações neste perfil de discagem devem corresponder às configurações na configuração do VPN 3000 Concentrator e no cliente de discagem de

entrada. Neste exemplo, é usada a autenticação MS-CHAPv2 sem criptografia PPTP.

13. Na guia Encryption (Criptografia), marque **No Encryption** only (**Nenhuma criptografia** apenas).
14. Clique em **OK** para fechar o perfil de discagem de entrada e clique em **OK** para fechar a janela da política de acesso remoto.
15. Clique com o botão direito do mouse em **Internet Authentication Service** e clique em **Start Service** na árvore do console.**Observação:** você também pode usar esta função para interromper o serviço.
16. Conclua estes passos para modificar os usuários para permitir a conexão.Escolha **Console > Add/Remove Snap-in**.Clique em **Adicionar** e escolha **snap-in Usuários locais e grupos**.Clique em Add.Selecione **Computador local**Clique em **Concluir** e em **OK**.
17. Expanda **Usuário e grupos locais** e clique na pasta **Usuários** no painel esquerdo. No painel direito, clique duas vezes no usuário (usuário VPN) que deseja permitir o acesso.
18. Vá para a guia Discar e escolha **Permitir acesso** em Permissão de acesso remoto (discagem ou

VPN).

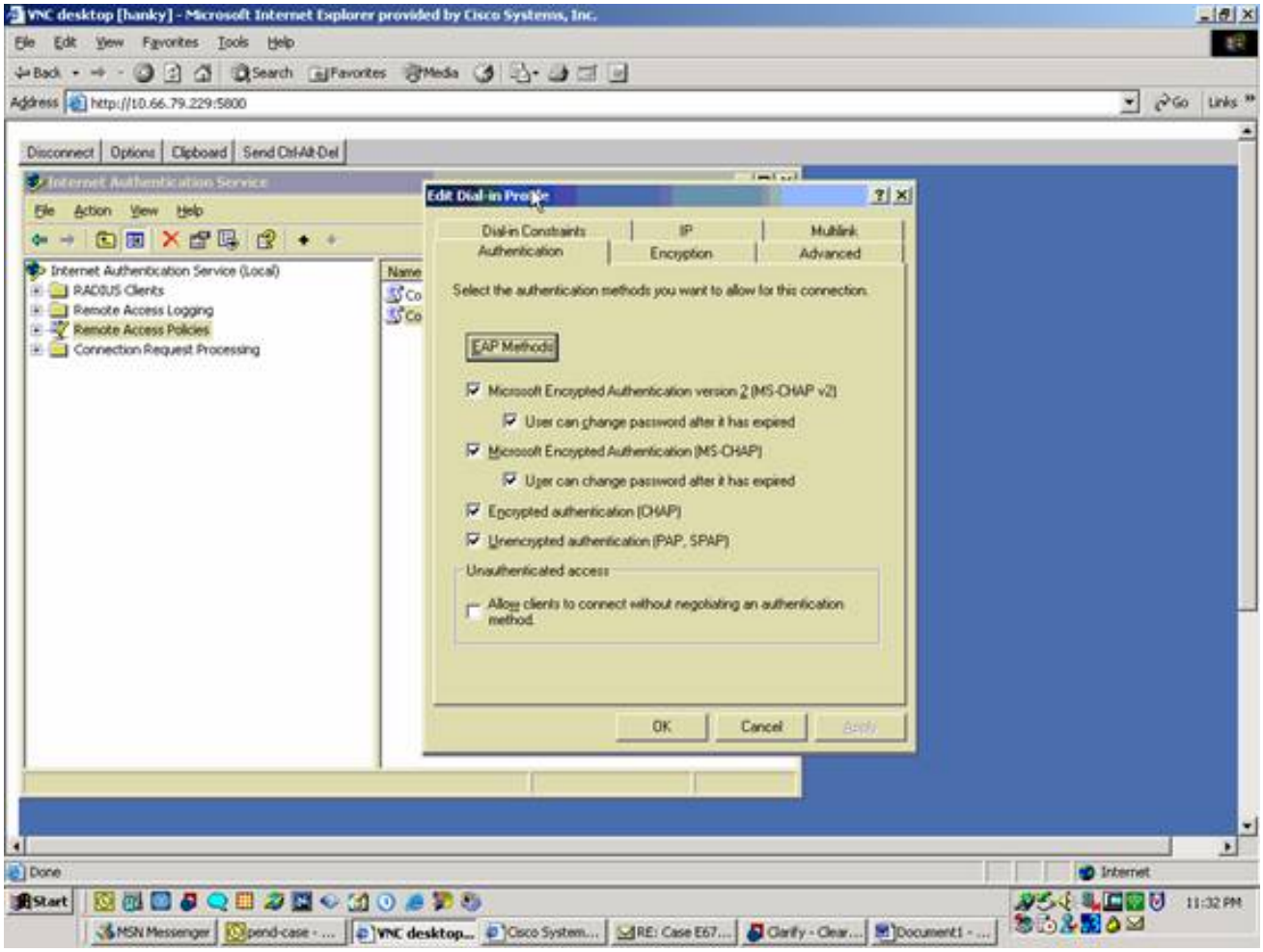
19. Clique em **Apply** e **OK** para concluir a ação. Você pode fechar a janela Gerenciamento do console e salvar a sessão, se desejar.Os usuários que você modificou agora podem acessar o VPN Concentrator com o VPN Client. Lembre-se de que o servidor IAS autentica apenas as informações do usuário. O VPN Concentrator ainda faz a autenticação de grupo.

Configurar o Microsoft Windows 2003 Server com IAS

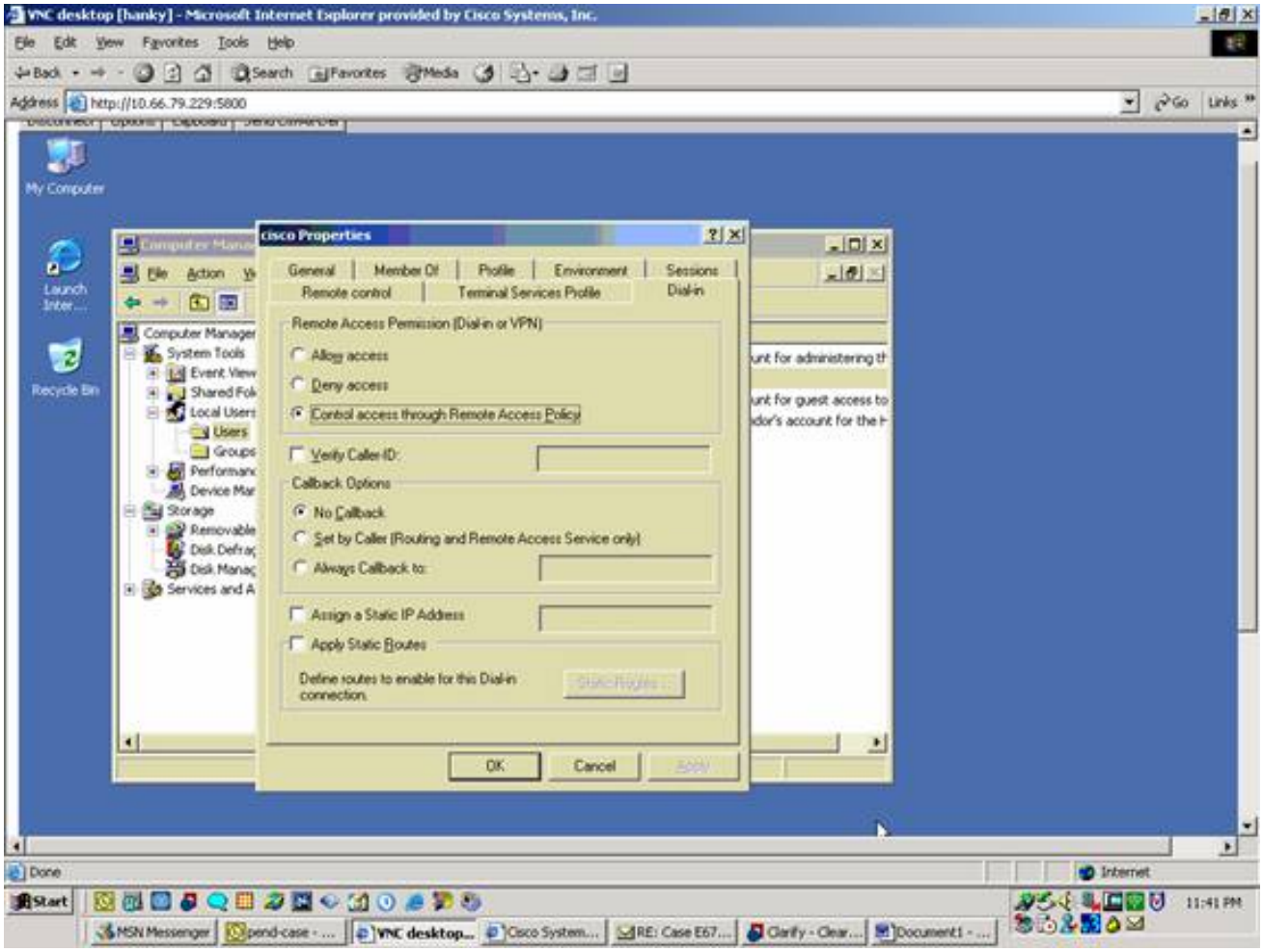
Conclua estes passos para configurar o servidor Microsoft Windows 2003 com IAS.

Observação: estas etapas presumem que o IAS já está instalado na máquina local. Caso contrário, adicione-o através do **Painel de controle > Adicionar ou remover programas**.

1. Escolha **Administrative Tools > Internet Authentication Service** e clique com o botão direito do mouse em **RADIUS Client** para adicionar um novo cliente RADIUS. Depois de digitar as informações do cliente, clique em **OK**.
2. Digite um nome amigável.
3. Defina o VPN Concentrator com um endereço IP ou nome DNS na próxima janela.
4. Escolha **Cisco** na barra de rolagem Client-Vendor.
5. Insira um segredo compartilhado.**Observação:** você deve se lembrar do segredo *exato* que usa. Você precisa dessas informações para configurar o VPN Concentrator.
6. Clique em **OK** para concluir.
7. Vá para **Políticas de acesso remoto**, clique com o botão direito do mouse em **Conexões a outros servidores de acesso** e escolha **Propriedades**.
8. Escolha **Conceder permissão de acesso remoto** e clique em **Editar perfil** para configurar as propriedades de discagem de entrada.
9. Selecione o protocolo a ser usado para autenticação na guia Autenticação. Verifique a **Microsoft Encrypted Authentication versão 2** e desmarque todos os outros protocolos de autenticação.**Observação:** as configurações neste perfil de discagem devem corresponder às configurações na configuração do VPN 3000 Concentrator e no cliente de discagem de entrada. Neste exemplo, é usada a autenticação MS-CHAPv2 sem criptografia PPTP.
10. Na guia Encryption (Criptografia), marque **No Encryption** only (**Nenhuma criptografia** apenas).
11. Clique em **OK** quando terminar.



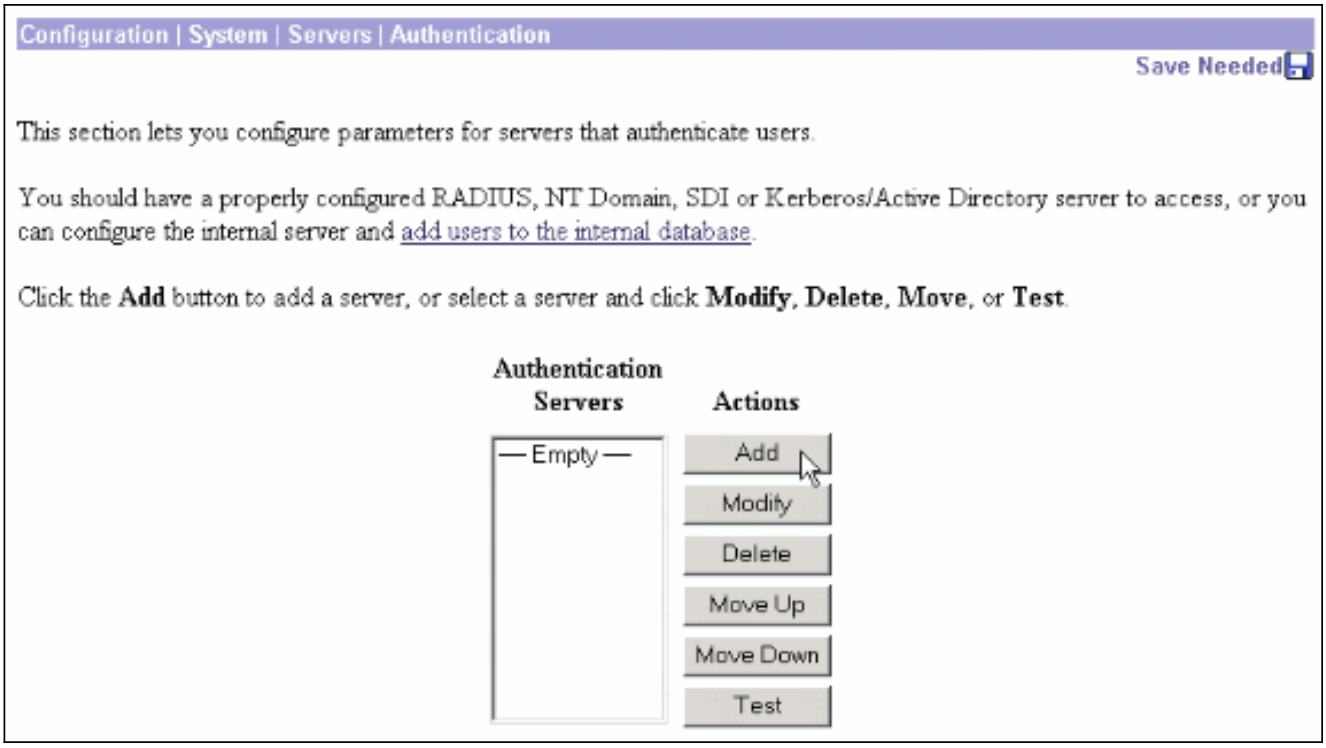
12. Clique com o botão direito do mouse em **Internet Authentication Service** e clique em **Start Service** na árvore do console.**Observação:** você também pode usar esta função para interromper o serviço.
13. Escolha **Administrative Tools > Computer Management > System Tools > Local Users and Groups**, clique com o botão direito do mouse em **Users** e escolha **New Users** para adicionar um usuário à conta do computador local.
14. Adicione o usuário com a senha "vpnpassword" da Cisco e verifique essas informações de perfil.Na guia Geral, certifique-se de que a opção **Senha nunca expirada** esteja selecionada, em vez da opção Usuário deve alterar a senha.Na guia Discar, escolha a opção **Permitir acesso** (ou deixe a configuração padrão de Controle de acesso por meio da Diretiva de acesso remoto).Clique em **OK** quando terminar.



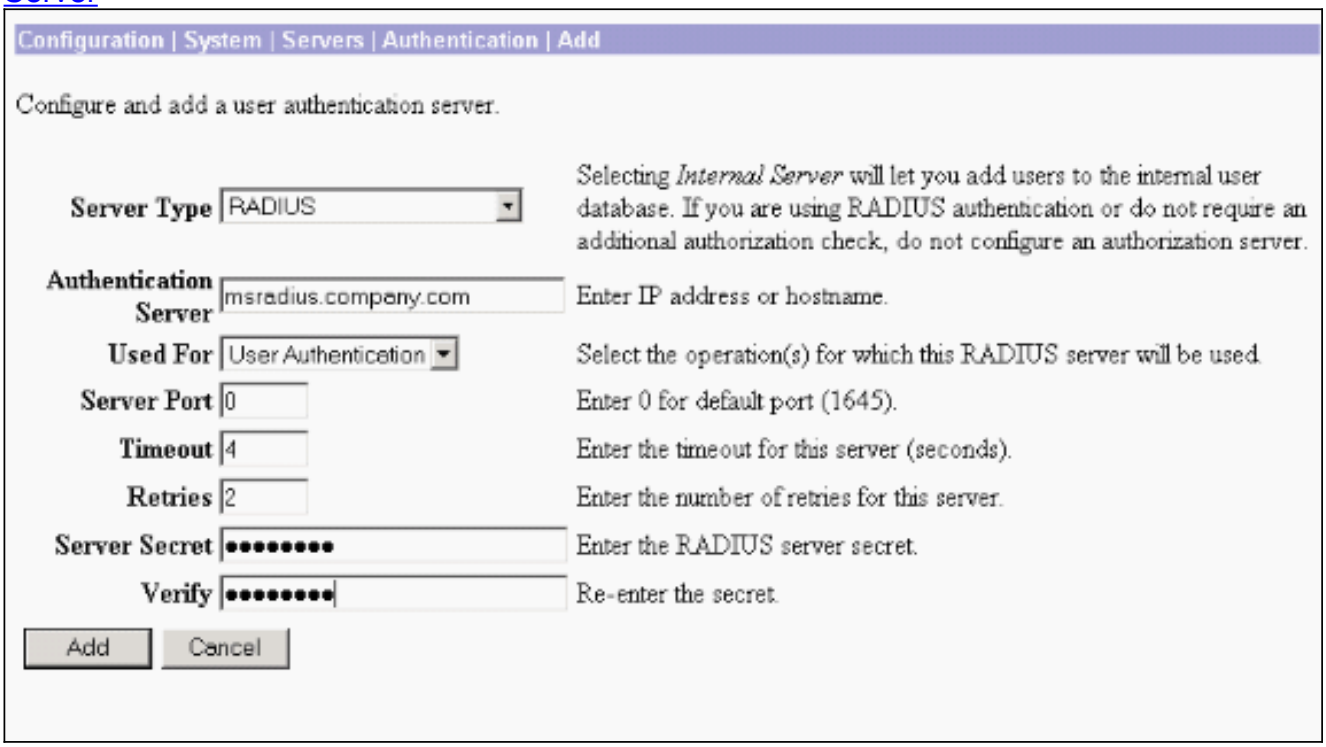
Configurar o Cisco VPN 3000 Concentrator para autenticação RADIUS

Conclua estes passos para configurar o Cisco VPN 3000 Concentrator para autenticação RADIUS.

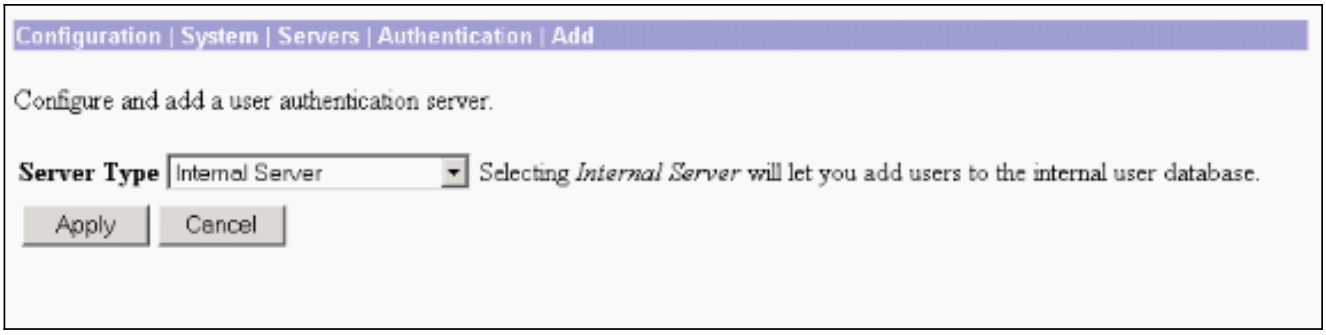
1. Conecte-se ao VPN Concentrator com seu navegador da Web e escolha **Configuration > System > Servers > Authentication** no menu do quadro esquerdo.



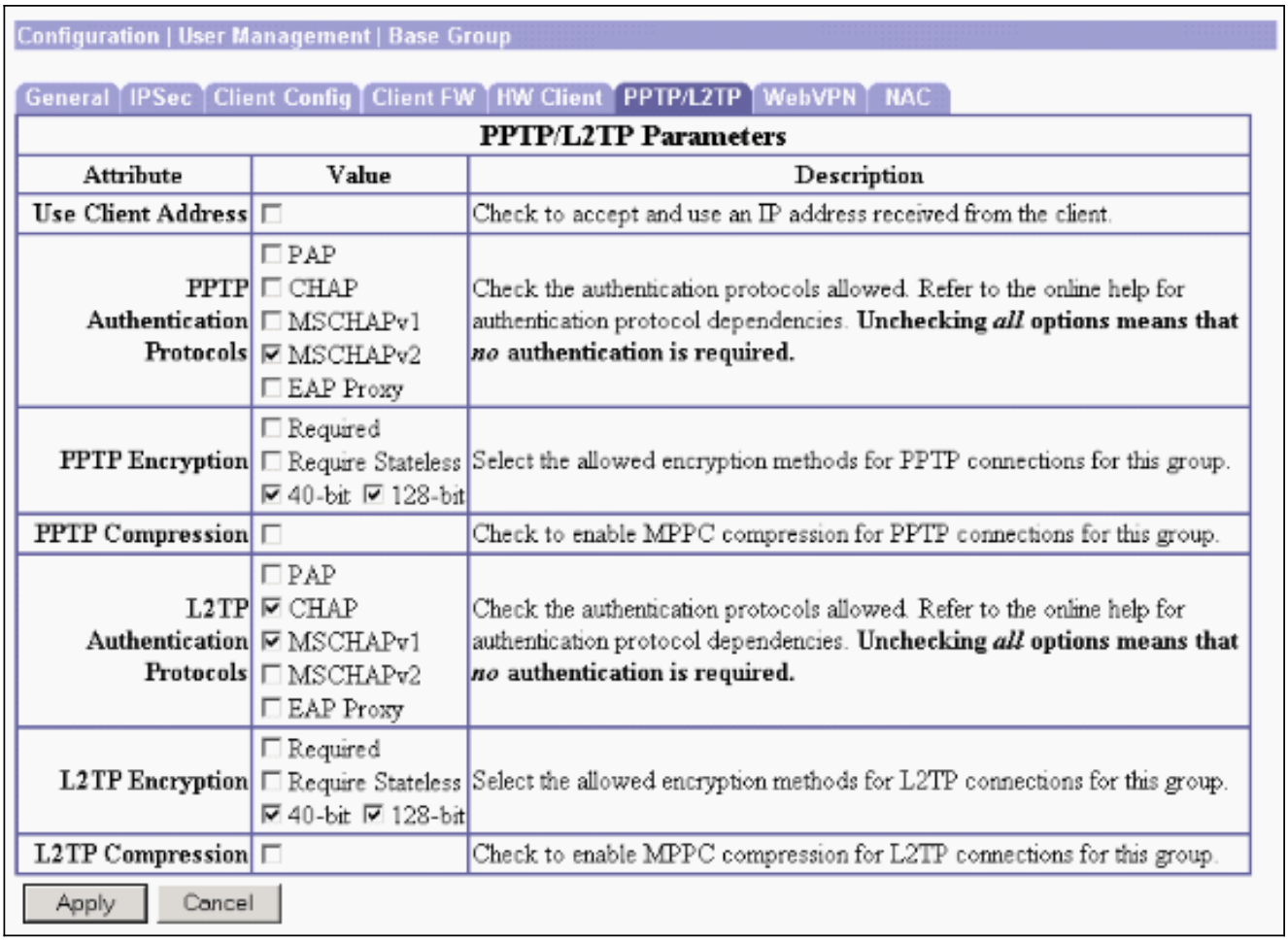
2. Clique em **Adicionar** e defina essas configurações.Tipo de servidor = RADIUSServidor de autenticação = Endereço IP ou nome de host do servidor RADIUS (IAS)Porta do Servidor = 0 (0=padrão=1645)Server Secret = o mesmo da etapa 8 na seção [Configure the RADIUS Server]



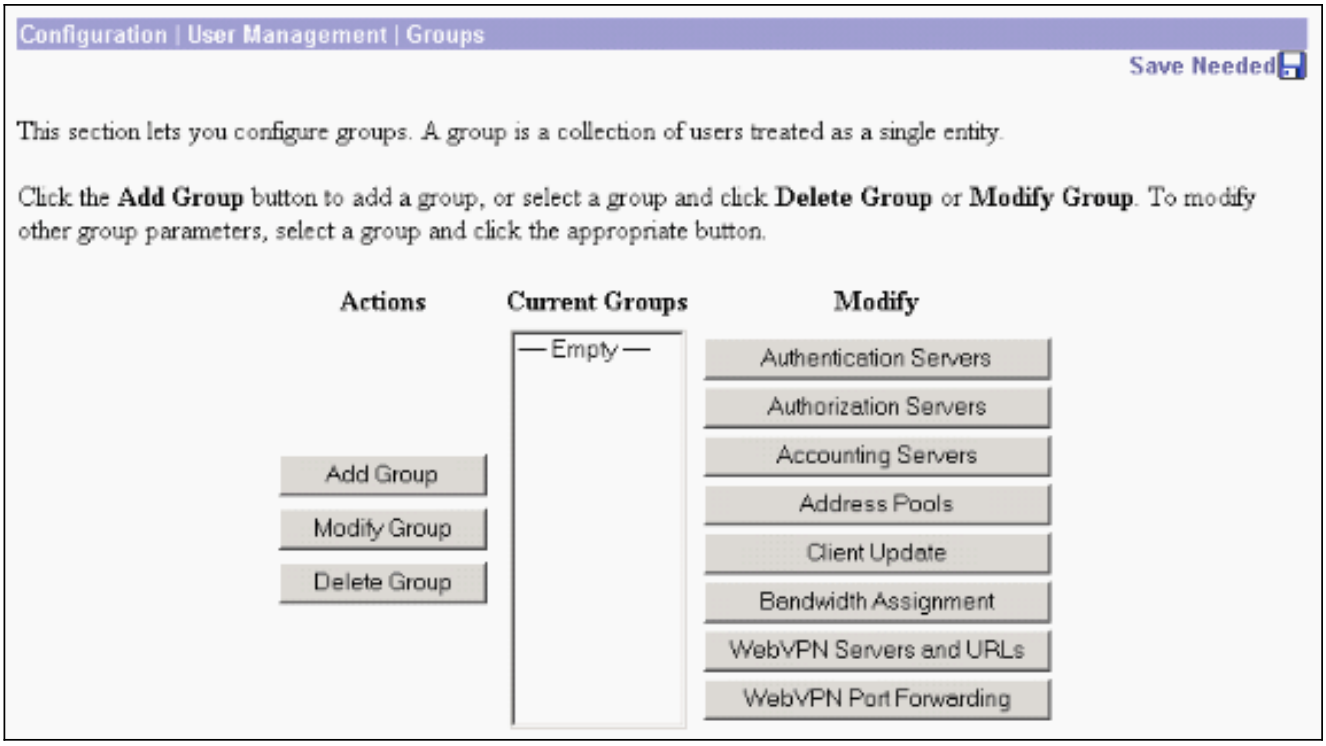
3. Clique em **Adicionar** para adicionar as alterações à configuração atual.
4. Clique em **Adicionar**, escolha **Servidor interno** para Tipo de servidor e clique em **Aplicar**.Você precisará disso mais tarde para configurar um grupo IPsec (somente o tipo de servidor = servidor
interno).



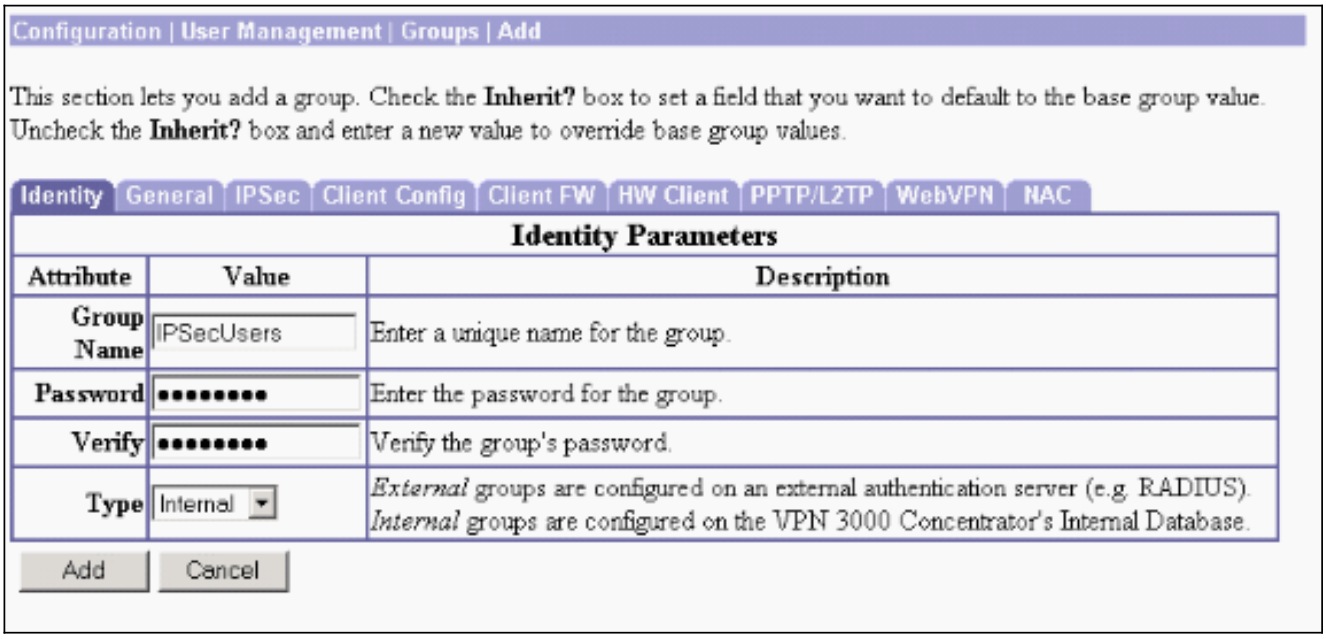
5. Configure o VPN Concentrator para usuários PPTP ou para usuários do VPN Client.**PPTP**Conclua estes passos para configurar usuários PPTP.Escolha **Configuration > User Management > Base Group** e clique na guia **PPTP/L2TP**.Escolha **MSCHAPv2** e desmarque outros protocolos de autenticação na seção Protocolos de autenticação PPTP.



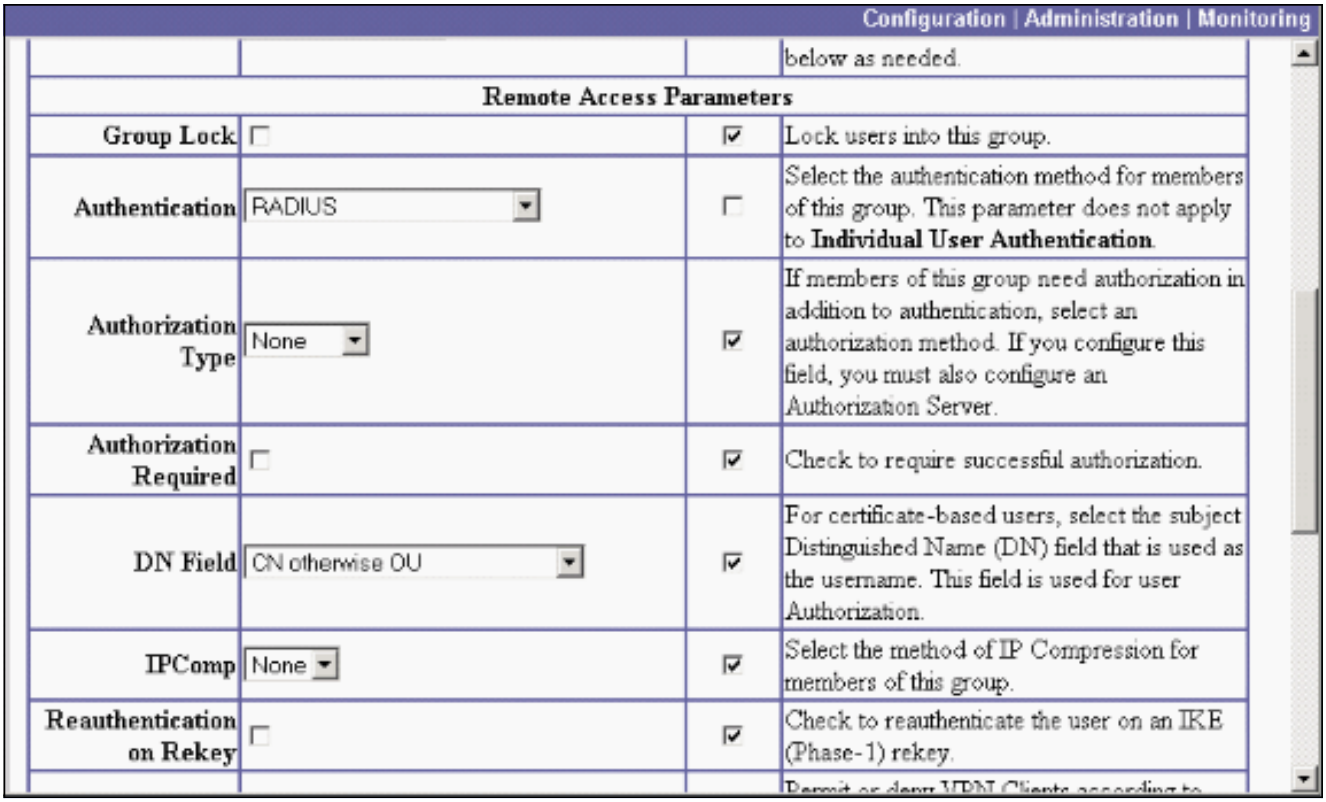
Clique em **Apply** na parte inferior da página para adicionar as alterações à configuração atual.Agora, quando os usuários PPTP se conectam, eles são autenticados pelo servidor RADIUS (IAS).**Cliente de VPN**Conclua estes passos para configurar usuários do VPN Client.Escolha **Configuration > User Management > Groups** e clique em **Add** para adicionar um novo
grupo.



Digite um nome de grupo (por exemplo, IPsecUsers) e uma senha.



Essa senha é usada como chave pré-compartilhada para a negociação do túnel.Vá até a guia IPSec e defina Authentication como
RADIUS.



Isso permite que os clientes IPsec sejam autenticados através do servidor de autenticação RADIUS.Clique em **Adicionar** na parte inferior da página para adicionar as alterações à configuração atual.Agora, quando os clientes IPsec se conectam e usam o grupo configurado, eles são autenticados pelo servidor RADIUS.

Verificar

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

Troubleshoot

Falha na autenticação WebVPN

Essas seções fornecem informações que você pode usar para solucionar problemas de sua configuração.

- **Problema:** Os usuários do WebVPN não podem se autenticar no servidor RADIUS, mas podem se autenticar com êxito com o banco de dados local do VPN Concentrator. Eles recebem erros como "Falha no login" e esta

mensagem. **Causa:** Esses tipos de problemas frequentemente acontecem quando qualquer banco de dados diferente do banco de dados interno do Concentrador é usado. Os usuários do WebVPN atingem o grupo base quando se conectam ao concentrador pela primeira vez e devem usar o método de autenticação padrão. Frequentemente, esse método é definido para o banco de dados interno do concentrador e não é um RADIUS configurado ou outro servidor.**Solução:** Quando um usuário WebVPN se autentica, o Concentrador verifica a lista de servidores definidos em **Configuração > Sistema > Servidores > Autenticação** e usa o principal. Mova o servidor com o qual deseja que os usuários do WebVPN se autentiquem para o topo desta lista. Por exemplo, se RADIUS deve ser o método de autenticação, você precisa mover o servidor RADIUS para o topo da lista para enviar a autenticação para ele.**Observação:** apenas porque os usuários do WebVPN acessaram inicialmente o grupo base não significa que eles estejam confinados ao grupo base. Grupos WebVPN adicionais podem ser configurados no Concentrador e os usuários podem ser atribuídos a eles pelo servidor RADIUS com a população do atributo 25 com **OU=*groupname***. Consulte Bloqueando Usuários em um Grupo de Concentradores VPN 3000 Usando um Servidor RADIUS para obter uma explicação mais detalhada.

Falha na autenticação do usuário no Ative Diretory

No servidor do Ative Diretory, na guia Conta das Propriedades do usuário com falha, você pode ver esta caixa de seleção:

[x] Não exige pré-autenticação

Se esta caixa de seleção estiver desmarcada, **marque-a** e tente autenticar novamente com este usuário.

Informações Relacionadas

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociação IPsec/Protocolos IKE
- Página de suporte do RADIUS (Remote Authentication Dial-In User Service)
- Remote Authentication Dial-In User Service (RADIUS)
- Suporte Técnico e Documentação - Cisco Systems