Configurando o Cisco VPN 3000 Concentrator com Microsoft RADIUS

Índice

Introdução

O servidor de autenticação de Internet do microsoft (IAS) e o sistema comercial de Internet de Microsoft (MCI 2.0) estão atualmente disponíveis. O server do Microsoft RADIUS é conveniente porque usa o diretório ativo no Primary Domain Controller para sua base de dados de usuário. Você já não precisa de manter um base de dados separado. Igualmente apoia 40-bit e criptografia do 128-bit para conexões de VPN do Point-to-Point Tunneling Protocol (PPTP). Refira a Lista de Verificação do Microsoft: Configurando IAS para o tratamento por imagens e a documentação de acesso de VPN para mais informação.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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

Instale e configurar o servidor Radius no Windows 2000 e no Windows 2003

Instale o servidor Radius

Se você não tem o servidor Radius (IAS) instalado já, execute estas etapas a fim instalar. Se você já tem o servidor Radius instalado, continue às etapas de configuração.

1. Introduza o compact disc de Windows Server e comece o programa de instalação.
2. O clique **instala componentes auxiliares**, e clica-os então **adiciona/remove componentes do Windows**.
3. Nos componentes, os **serviços de rede do** clique (mas não selecione nem cancele a caixa de verificação), e clicam então **detalhes**.
4. Verifique o **Internet Authentication Service** e clique a **APROVAÇÃO**.
5. Clique em Next.

Configurar o Servidor do Microsoft Windows 2000 com IAS

Termine estas etapas a fim configurar o servidor Radius (IAS) e começar o serviço a fim fazê-lo disponível para autenticar usuários no concentrador VPN.

1. Escolha o **iniciar > programas > ferramentas administrativas > o Internet Authentication Service**.
2. Clicar com o botão direito o **Internet Authentication Service**, e clique **propriedades do** submenu que aparece.
3. Vá à aba do RAIO a fim examinar os ajustes para portas.Se suas portas do User Datagram Protocol (UDP) da contabilidade da autenticação RADIUS e do RAIO diferem dos valores padrão fornecidos (1812 e 1645 para a autenticação, 1813 e 1646 para explicar) na autenticação e na contabilidade, datilografe suas configurações de porta. Clique a **APROVAÇÃO** quando você é terminado.**Nota:** Não mude as portas padrão. Separe as portas usando vírgulas para usar ajustes da porta múltipla para pedidos da autenticação ou explicar.
4. Clicar com o botão direito **clientes** e escolha o **cliente novo** a fim adicionar o concentrador VPN como um cliente do Authentication, Authorization, and Accounting (AAA) ao servidor Radius (IAS).**Nota:** Se a Redundância é configurada entre dois concentradores do Cisco VPN 3000, o Cisco VPN 3000 Concentrator alternativo deve igualmente ser adicionado ao servidor Radius como um cliente RADIUS.
5. Dê entrada com um nome amigável e selecione-o como o **raio do protocolo**.
6. Defina o concentrador VPN com um endereço IP de Um ou Mais Servidores Cisco ICM NT ou um nome de DNS na próxima janela.
7. Escolha **Cisco de** Client-Vendor scrollbar.
8. Incorpore um segredo compartilhado.**Nota:** Você deve recordar o segredo *exato* que você

usa. Você precisa esta informação a fim configurar o concentrador VPN.

9. Clique em Finish.
10. Fazer duplo clique **políticas de acesso remoto** e fazer duplo clique a política que aparece no lado direito do indicador.**Nota:** Depois que você instala IAS, uma política de acesso remoto deve já existir.No Windows 2000, a autorização é concedida com base nas propriedades do discado de uma conta de usuário e de políticas de acesso remoto. As políticas de acesso remoto são um conjunto de condição e as configurações de conexão que dão a administradores de rede mais flexibilidade em tentativas de conexão de autorização. O roteamento do Windows 2000 e Remote Access Service e o Windows 2000 IAS ambas as políticas de acesso remoto do uso para determinar se aceitar ou rejeitar tentativas de conexão. Em ambos os casos, as políticas de acesso remoto são armazenadas localmente. Refira a documentação IAS do Windows 2000 para obter mais informações sobre de como as tentativas de conexão são processadas.
11. Escolha a **permissão de acesso remoto de Grant** e o clique **edita o perfil** a fim configurar propriedades do discado.
12. Selecione o protocolo para usar-se para a autenticação na aba da autenticação. Verifique a **versão 2 da autenticação criptografada de Microsoft** e desmarcar todos Protocolos de autenticação restantes.**Nota:** Os ajustes neste perfil do discado devem combinar os ajustes na configuração e no cliente de discagem de entrada do VPN 3000 concentrator. Neste exemplo MS-CHAPv2 a autenticação sem criptografia de PPTP é usada.
13. **No no encryption da** verificação da aba da criptografia somente.
14. Clique a **APROVAÇÃO** a fim fechar o perfil do discado, a seguir clique a **APROVAÇÃO** a fim fechar o indicador da política de acesso remoto.
15. Clicar com o botão direito o **Internet Authentication Service** e clique o **serviço do começo na** árvore de console.**Nota:** Você pode igualmente usar esta função para parar o serviço.
16. Termine estas etapas a fim alterar os usuários para permitir a conexão.Escolha o **Console > Adicionar/Remover Snap-in**.O clique **adiciona** e escolhe **usuários locais e grupos pressão-em**.Clique em Add.Certifique-se selecionar o **computador local**Clique o **revestimento** e a **APROVAÇÃO**.
17. Expanda o **usuário local e os grupos** e clique a **pasta de usuários no** painel esquerdo. No painel correto, fazer duplo clique o usuário (usuário VPN) que você quer permitir o acesso.
18. Vá ao guia de discagem de entrada e escolha **permitem o acesso** sob a permissão de acesso remoto (discado ou VPN).
19. O clique **aplica-se** e **APROVA-SE** a fim terminar a ação. Você pode fechar a janela de gerenciamento do console e salvar a sessão, se desejado.Os usuários que você alterou podem agora alcançar o concentrador VPN com o cliente VPN. Mantenha na mente que o servidor de IAS autentica somente a informação sobre o usuário. O concentrador VPN ainda faz a autenticação do grupo.

Configurar o server de Microsoft Windows 2003 com IAS

Termine estas etapas a fim configurar o server de Microsoft Windows 2003 com IAS.

Nota: Estas etapas supõem que IAS está instalado já na máquina local. Se não, adicionar isto com o **> Add do Control Panel/remova os programas**.

1. Escolha o **Ferramentas Administrativas > Serviço de Autenticação de Internet** e clicar com o botão direito no **cliente RADIUS** a fim adicionar um cliente RADIUS novo. Depois que você

datilografa a informação cliente, clique a **APROVAÇÃO**.
2. Dê entrada com um nome amigável.
3. Defina o concentrador VPN com um endereço IP de Um ou Mais Servidores Cisco ICM NT ou um nome de DNS na próxima janela.
4. Escolha **Cisco de** Client-Vendor scrollbar.
5. Incorpore um segredo compartilhado.**Nota:** Você deve recordar o segredo *exato* que você usa. Você precisa esta informação a fim configurar o concentrador VPN.
6. **APROVAÇÃO do** clique a terminar.
7. Vá às **políticas de acesso remoto**, clicar com o botão direito em **conexões a outros servidores de acesso**, e escolha **propriedades**.
8. Escolha a **permissão de acesso remoto de Grant** e o clique **edita o perfil** a fim configurar propriedades do discado.
9. Selecione o protocolo para usar-se para a autenticação na aba da autenticação. Verifique a **versão 2 da autenticação criptografada de Microsoft** e desmarcar todos Protocolos de autenticação restantes.**Nota:** Os ajustes neste perfil do discado devem combinar os ajustes na configuração e no cliente de discagem de entrada do VPN 3000 concentrator. Neste exemplo MS-CHAPv2 a autenticação sem criptografia de PPTP é usada.
10. **No no encryption da** verificação da aba da criptografia somente.
11. **APROVAÇÃO do** clique quando você for terminado.
12. Clicar com o botão direito o **Internet Authentication Service** e clique o **serviço do começo na** árvore de console.**Nota:** Você pode igualmente usar esta função a fim parar o serviço.
13. Escolha o **Ferramentas Administrativas > Gerenciamento de Computador > Ferramentas de Sistema > Usuários e Grupos Locais**, clicar com o botão direito em **usuários** e escolha **novos usuários** a fim adicionar um usuário na conta do computador local.
14. Adicionar o usuário com senha Cisco “vpnpassword” e verifique esta informação do perfil.No tab geral, assegure-se de que a opção de senha **Expired** esteja selecionada **nunca** em vez da opção para o usuário deva mudar a senha.No guia de discagem de entrada, escolha a opção para o **acesso Allow** (ou deixe a configuração padrão do acesso do controle com a política de acesso remoto).Clique a **APROVAÇÃO** quando você é terminado.

Configurar o Cisco VPN 3000 Concentrator para a autenticação RADIUS

Termine estas etapas a fim configurar o Cisco VPN 3000 Concentrator para a autenticação RADIUS.

1. Conecte ao concentrador VPN com seu navegador da Web, e escolha o **configuração > sistema > servidores > autenticação do** menu de frame esquerdo.
2. O clique **adiciona** e configura estes ajustes.Tipo de servidor = RAIOAuthentication Server = endereço IP ou nome do host de seu servidor Radius (IAS)Porta de servidor = 0 (0=default=1645)Segredo de servidor = mesmos que em etapa 8 na seção Configure o servidor Radius
3. O clique **adiciona** a fim adicionar as mudanças à configuração running.
4. O clique **adiciona**, escolhe o **servidor interno** para o tipo de servidor, e o clique **aplica-se**.Você precisa este mais tarde a fim configurar um grupo IPSec (você precisa somente o tipo de servidor = o servidor interno).

5. Configurar o concentrador VPN para usuários PPTP ou para usuários de cliente VPN.**PPTP**Termine estas etapas a fim configurar para usuários PPTP.Escolha o **configuration > user management > o grupo base**, e clique a aba **PPTP/L2TP**.Escolha o **MSCHAPv2** e desmarcar outros Protocolos de autenticação na seção dos protocolos de autenticação de PPTP.O clique **aplica-se na** parte inferior da página a fim adicionar as mudanças à configuração running.Agora em que os usuários PPTP conectam, são autenticados pelo servidor Radius (IAS).**Cliente de VPN**Termine estas etapas a fim configurar para usuários de cliente VPN.Escolha o **configuration > user management > os grupos** e o clique **adiciona** a fim adicionar um grupo novo.Datilografe um nome do grupo (por exemplo, IPsecUsers) e uma senha.Esta senha é usada como a chave pré-compartilhada para a negociação do túnel.Vá à aba do IPsec e ajuste a autenticação ao **RAIO**.Isto permite que os clientes de IPSec sejam autenticados através do servidor de autenticação RADIUS.O clique **adiciona na** parte inferior da página a fim adicionar as mudanças à configuração running.Agora em que os clientes de IPSec conectam e usam o grupo que você configurou, são autenticados pelo servidor Radius.

Verificar

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

Troubleshooting

A autenticação WebVPN falha

Estas seções fornecem a informação que você pode se usar para pesquisar defeitos sua configuração.

- Problema: Os usuários WebVPN não podem autenticar contra o servidor Radius mas podem autenticar com sucesso com o base de dados local do concentrador VPN. Recebem erros tais como o “início de uma sessão falhado” e a esta mensagem.Causa: Estes tipos dos problemas acontecem frequentemente quando todo o base de dados a não ser o base de dados interno do concentrador é usado. Os usuários WebVPN batem o grupo base quando primeiramente conectam ao concentrador e devem usar o método de autenticação padrão. Frequentemente este método é ajustado ao base de dados interno do concentrador e não sido um RAIO configurado ou o outro server.Solução: Quando um usuário WebVPN autentica, o concentrador verifica a lista de server definida no **configuração > sistema > servidores > autenticação** e usa superior. Certifique-se mover o server que você quer usuários WebVPN autenticar com à parte superior desta lista. Por exemplo, se o RAIO for o método de autenticação, você precisa de mover o servidor Radius para a parte superior da lista para empurrar-lhe a autenticação para.**Nota:** Apenas porque os usuários WebVPN batem inicialmente o grupo base não significa que estão limitados ao grupo base. Os grupos adicionais WebVPN podem ser configurados no concentrador, e os usuários podem ser-lhes atribuídos pelo servidor Radius com a população do atributo 25 com **OU=groupname**. Refira o travamento de usuários em um VPN 3000 concentrator group usando um servidor Radius para mais explicação detalhada.

A autenticação de usuário falha contra o diretório ativo

No servidor ative directory, na aba da conta das propriedades de usuário do usuário de falha, você pode ver esta caixa de verificação:

O [x] não exige a PRE-autenticação

Se esta caixa de verificação é desmarcada, **verifique-a**, e tente-a autenticar outra vez com este usuário.

Informações Relacionadas

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociação IPsec/Protocolos IKE
- Página de suporte dos radius (serviço de usuário de discagem de autenticação remota)
- Remote Authentication Dial-In User Service (RADIUS)
- Suporte Técnico e Documentação - Cisco Systems