Cliente VPN FAQ

Índice

Introdução

Este documento responde a perguntas frequentes sobre o Cisco VPN Client.

Nota: As convenções de nomenclatura para os diversos clientes VPN são:

- Cisco Secure VPN Client versões 1.0 a 1.1a somente
- Cisco VPN 3000 Client versões 2.x somente
- Cisco VPN Client 3.x e posteriores somente

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

Download do Software do VPN Client

Q. Onde posso eu transferir o software Cisco VPN Client?

A. Você deve entrar e possuir um contrato de serviço válido a fim alcançar o software Cisco VPN Client. O software Cisco VPN Client pode ser transferido da página do software da transferência de Cisco (clientes registrados somente). **Se você não tem um contrato de serviço válido associado com seu perfil do cisco.com, você não pode entrar e transferir o software do cliente VPN.**

A fim obter um contrato de serviço válido, você pode:

- Entre em contato com sua Equipe de Conta da Cisco se possuir um contrato de compra direta.
- Entre em contato com um parceiro ou revendedor da Cisco para adquirir um contato de

serviço.
- Use o Profile Manager (somente clientes registrados) para atualizar seu perfil do Cisco.com e solicitar a associação a um contrato de prestação de serviços.

Q. A área da transferência do Cisco VPN Client parece estar vazia. Por quê?

A. Ao chegar na área de cliente VPN do Centro de Softwares (somente clientes registrados) certifique-se de selecionar a área de downloads para o sistema operacional desejado no centro da página.

Q. Como posso eu desabilitar a característica do firewall stateful durante a instalação do Cisco VPN Client?

A. **Para versões do cliente VPN mais antigas que o 5.0:**

Consulte a seção Alterações na Documentação das Release Notes do VPN Client Rel 4.7 para aprender sobre os dois tópicos "Utilização do MSI para Instalar o Cliente VPN para Windows sem o Firewall Stateful" e "Utilização do InstallShield para Instalar o cliente VPN para Windows sem o Firewall Stateful".

Para versões do cliente VPN mais recentes que o 5.0:

Começando com a liberação de Cisco VPN Client 5.0.3.0560, uma bandeira da instalação MSI foi adicionada para evitar a instalação da guilda em arquivos do Firewall:

```
msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1
```

Refira contornear a instalação de arquivos do Firewall quando o firewall stateful não é seção exigida para obter mais informações sobre deste.

Q. Como eu desinstalo ou promovo o Cisco VPN Client?

A. Refira a remoção de uma versão do cliente VPN instalada com o instalador MSI para obter informações sobre de como desinstalar manualmente (InstallShield) e promover então a Versão Cliente VPN Cisco 3.5 e mais atrasado para o Windows 2000 e o Windows XP.

O Cisco VPN Client para o software do Windows 2000 e do Windows XP pode firmemente transferir atualizações e novas versões automaticamente através de um túnel de um VPN 3000 concentrator ou do outro servidor de VPN que possam fornecer notificações. O pré-requisito mínimo para isso é que os usuários remotos devem ter o VPN Client for Windows 4.6 ou posterior instalado em seus PC para usar o recurso de atualização automática.

Com esse recurso, chamado de autoupdate, os usuários não precisam desinstalar uma versão antiga do software, reinicializar, instalar a nova versão e, em seguida, reinicializar novamente. Em vez disso, um administrador disponibiliza as atualizações e os perfis em um servidor de Web e quando um usuário remoto inicia o Cliente VPN, o software detecta que um download está disponível e pega automaticamente. Para obter mais informação, consulte Como Gerenciar autoupdates e Como Funciona a Atualização Automática.

Para obter informações sobre como configurar uma atualização do cliente em um Mecanismo de Segurança Cisco ASA Series 5500 Adaptive usando o ASDM, consulte Configuração de

Atualização do Software do Cliente Usando o ASDM.

Q. Eu quero personalizar os clientes VPN para o Vista. Eu sei que, na nova versão do cliente VPN para o Vista, não há mais um arquivo como oem.mst. Como podemos personalizar as novas versões de clientes VPN (5.x), ou onde posso encontrar esse arquivo?

A. O arquivo MST é fornecido já não com o cliente VPN, mas você pode transferi-lo da página do software da transferência (clientes registrados somente):

Nome do arquivo: Leia-me e MST para a instalação na versão internacional do Windows.

Sistema operacional

Q. A Cisco fornece um cliente VPN para o Windows Vista?

A. O Cisco VPN Client novo 5.0.07 da liberação apoia Windows Vista em x86 (de 32 bits) e em x64. Consulte 5.0.07.0240 Release Notes para obter mais informações.

Nota: O Cisco VPN Client oferece suporte somente na instalação nova do Windows Vista, o que significa o upgrade de qualquer sistema operacional Windows para o Windows Vista não é suportada com o software de cliente VPN. Você deve instalar o Windows Vista a partir do zero e, em seguida, instalar o software Vista VPN Client.

Nota: Se você não possuir um contrato de serviço válido associado ao seu perfil do Cisco.com, você não poderá iniciar sessão e baixar o software do VPN Client. Consulte Baixar Software do VPN Client para obter mais informações.

Dica: O Cisco AnyConnect VPN Client está agora disponível para os sistemas operacionais Windows, o que inclui o Vista de 32 e de 64 bits. O cliente do AnyConnect oferece suporte a SSL e DTLS. Não apoia o IPsec neste tempo. Além disso, o AnyConnect está disponível somente para uso com um Cisco Adaptive Security Appliance versão 8.0(2) ou mais recente. O cliente também pode ser usado no modo weblaunch com os IOS Appliances que executam a versão 12.4(15)T. Não há suporte ao VPN 3000.

O Cisco AnyConnect VPN Client e ASA 8.0 podem ser obtidos no Centro de Software (somente clientes registrados). Consulte as Release Notes do Cisco AnyConnect VPN Clientpara obter mais informações sobre o AnyConnect Client. Consulte as Release Notes dos Cisco ASA 5500 Series Adaptive Security Appliances para obter mais informações sobre o ASA 8.0.

Nota: Se você não possuir um contrato de serviço válido associado ao seu perfil do Cisco.com, você não poderá iniciar sessão e baixar o software do AnyConnect VPN Client ou do ASA. Consulte Baixar Software do VPN Client para obter mais informações.

Q. Como eu configuro uma conexão PPTP a partir de um PC com Microsoft Windows?

A. A configuração depende da versão do Microsoft Windows que você usa. Entre em contato com a Microsoft para obter informações específicas. Seguem instruções de configuração para algumas das versões do Windows mais comuns:

Windows 95

1. Instale o Msdun13.exe.
2. Escolha **Programs > Accessories > Dial Up Networking**.
3. Crie uma nova conexão chamada “PPTP.”
4. Selecione o **VPN Adapter** como dispositivo da conexão.
5. Insira o endereço IP da interface pública do switch e clique em **Finish**.
6. Volte para a conexão que você acabou de criar, clique com o botão direito, e escolha **Properties**.
7. Em Allowed Network Protocols, pelo menos, desmarque **netbeui**.
8. Configure as **Advanced Options**. Mantenha as configurações padrão para permitir que o switch e o cliente negociem automaticamente o método de autenticação.Habilite **Require Encrypted Password** para forçar a autenticação Challenge Handshake Authentication Protocol (CHAP).Habilite **Require Encrypted Password** e **Require Data Encryption** para forçar a autenticação MS-CHAP.

Windows 98

1. Conclua estas etapas para instalar o recurso PPTP: Escolha **Start > Settings > Control Panel > Add New Hardware**, e clique em **Next**.Clique em **Select from List**, escolha **Network Adapter**, e clique em **Next**.Escolha **Microsoft** no painel esquerdo e **Microsoft VPN Adapter** no painel direito.
2. Conclua estas etapas para configurar o recurso PPTP: Escolha **Start > Programs > Accessories > Communications > Dial Up Networking**.Clique em **Make new connection**, e escolha **Microsoft VPN Adapter** em Select a device. O endereço IP do servidor VPN = ponto final do túnel 3000.
3. Conclua estas etapas para alterar o PC para permitir também o Password Authentication Protocol (PAP): **Nota:** A autenticação padrão do Windows 98 é usar a criptografia de senha (CHAP ou MS-CHAP).Escolha **Properties > Server types**.Desmarque Require encrypted password. Você pode configurar a criptografia de dados (MPPE ou sem MPPE) nessa área.

Windows 2000

1. Escolha **Start > Programs > Accessories > Communications > Network and Dialup connections**.
2. Clique em **Make new connection** e, em seguida, em **Next**.
3. Escolha **Connect to a private network through the Internet and Dial a connection prior** (não selecione essa opção se tiver um LAN), e clique em **Next**.
4. Insira o nome de host ou o endereço IP do ponto final do túnel (3000).
5. Se precisar alterar o tipo da senha, escolha **Properties > Security for the connection > Advanced**. O padrão é MS-CHAP e MS-CHAP v2 (não CHAP ou PAP). Você pode configurar a criptografia de dados (MPPE ou não MPPE) nessa área.

Windows NT

Consulte Instalação, Configuração e Utilização do PPTP com Clientes e Servidores Microsoft.

Q. Quais versões de sistemas operacionais suportam o Cisco VPN Client?

A. O suporte a sistemas operacionais adicionais é acrescentado constantemente para o cliente VPN. Consulte Requisitos do sistema nas release notes do VPN Client 5.0.07 para determinar

isso, ou consulte Hardware e Clientes VPN da Cisco que Oferecem Suporte a IPsec/PPTP/L2TP.

Notas:

- O cliente VPN inclui suporte para estações de trabalho dual-processor e dual-core para Windows XP e Windows Vista.
- A liberação de cliente VPN 4.8.00.440 de Windows era a versão final que apoiou oficialmente o sistema operacional de Windows 98.
- O Windows VPN Client Release 4.6.04.0043 foi a versão final que oficialmente ofereceu suporte ao sistema operacional Windows NT.
- O Cisco VPN Client ver 5.0.07 oferece suporte ao Windows Vista e ao Windows 7 nas edições x86 (de 32 bits) e x64 (64-bit).
- O Cisco VPN Client oferece suporte apenas ao Windows XP de 32 bits, mas o Windows XP de 64 bits não é suportado.**Nota:** O suporte ao Windows Vista de 32 bits estava disponível em todas as releases 5.x. O Cisco VPN client version 5.0.07 adicionou o suporte a 64 bits.

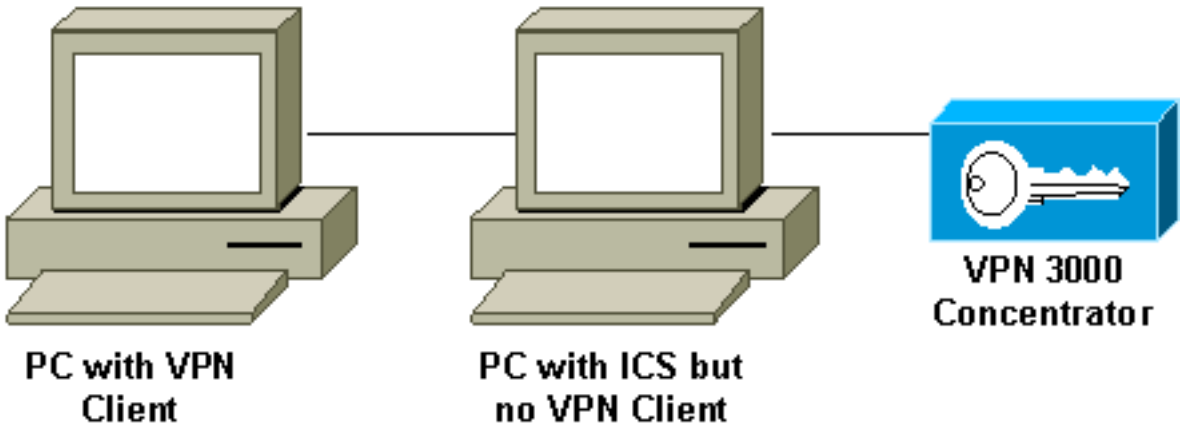
Q. Eu preciso ser um administrador nos computadores Windows NT/2000 para carregar o cliente VPN?

A. Sim, é necessário ter privilégios de administrador para instalar o cliente VPN no Windows NT e no Windows 2000, pois esses sistemas operacionais exigem esses privilégios para vincularem os drivers de rede existentes ou instalarem novos drivers de rede. O software de cliente VPN é um software de rede. Você deve ter privilégios do administrado instalá-lo.

Q. O Cisco VPN Client pode funcionar com o Microsoft Internet Connection Sharing (ICS) instalado na mesma máquina?

A. Não, Cisco VPN 3000 Client não é compatível com Microsoft ICS na mesma máquina. Você deve desinstalar o ICS antes de instalar o cliente VPN. Consulte Desabilitação do ICS na Preparação para Instalar ou Fazer o Upgrade para o Cisco VPN Client 3.5.x no Microsoft Windows XP para obter mais informações.

Embora ter o cliente VPN e o ICS no mesmo PC não funcione, esta disposição funciona.



Q. Meu cliente VPN parece se conectar apenas a determinados endereços. Eu uso o Windows XP. O que devo fazer?

A. Verifique se o firewall interno do Windows XP está desabilitado.

Q. O Cisco VPN Client é compatível com o firewall stateful do Windows XP?

A. Este problema foi resolvido. Consulte o bug da Cisco ID CSCdx15865 (somente clientes registrados) no Bug Toolkit para obter detalhes.

Q. Quando eu instalo o cliente VPN no Windows XP e no Windows 2000, a interface multiusuário é desabilitada?

A. A instalação desabilita a tela de boas vindas e a troca rápida de usuários. Consulte o bug da Cisco ID CSCdu24073 (somente clientes registrados) no Bug Toolkit para obter detalhes.

Q. Como posso fazer com que o cliente VPN para Linux vá para o segundo plano após a execução? Se iniciar uma conexão como vpnclient connect foo, eu consigo entrar masso shell retorna.

A. Após o registro, insira:

- **^Z**
- **bg**

Q. Quando eu instalo o Cisco VPN Client no Windows XP Home Edition, a barra de tarefas some. Como faço para desfazer isso?

A. Escolha **Control Panel > Network Connections > Remove Network Bridge** para ajustar essa configuração.

Q. Quando eu tento instalar o Linux VPN Client no RedHat 8.0, recebo um erro que diz que o módulo não pode ser carregado porque o módulo foi compilado com o GCC 2 e o kernel foi compilado com GCC 3.2. O que devo fazer?

A. Isso ocorre porque a nova versão do RedHat tem uma versão mais nova do compilador GCC (3.2+), o que provoca a falha do Cisco VPN Client atual. Esse problema foi corrigido e está disponível em Cisco VPN 3.6.2a. Consulte o bug da Cisco ID CSCdx15865 (somente clientes registrados) no Bug Toolkit para obter detalhes ou baixe o software do Centro de Software de VPN (somente clientes registrados).

Q. Por que o software desabilita a Fast User Switching quando eu instalo o VPN client 3.1 no Windows XP?

A. A Microsoft desabilita automaticamente Fast User Switching no Windows XP quando uma biblioteca GINA.dll é especificada no registro. O Cliente de VPN Cisco instala a dll CSgina para implementar o recurso "Start Before Login" (Iniciar Antes do Login). Se precisar usar a Troca Rápida de Usuários, desabilite o recurso "Iniciar Antes do Login". Os usuários registrados podem obter mais informações no bug da Cisco ID CSCdu24073 (somente clientes registrados) no Bug Toolkit.

Q. Faz o suporte ao cliente do IPSec VPN o começo antes da característica do fazer logon (SBL) em Windows 7?

A. A característica SBL não é apoiada em clientes do IPSec VPN em Windows7. É apoiada com o cliente VPN de AnyConnect.

Mensagens de erro

Q. Quando eu instalo o Cisco VPN Client 4.x, eu recebo esta mensagem de erro: **Advertindo 201: The necessary VPN sub-system is not available. Você não pode conectar ao servidor de VPN remoto**

A. Este problema pode ser causado pelos pacotes de firewall instalados em seu computador do VPN Client. Para evitar essa mensagem de erro, certifique-se de que nenhum programa de firewall ou antivírus esteja instalado ou em execução em seu PC no momento da instalação.

Q. Eu fiz upgrade para o Mac OS X 10.3 (conhecido como "Panther"), mas agora meu Cisco VPN Client 4.x exibe estas mensagens de erro: **A conexão do VPN seguro terminou localmente pela razão do cliente: Incapaz de contactar o gateway de segurança**

A. Você deve adicionar UseLegacyIKEPort=0 ao perfil (arquivo .pcf) encontrado no diretório /etc/CiscoSystemsVPNClient/Profiles/ para o Cisco VPN Client 4.x funcionar com o Mac OS X 10.3 ("Panther").

Q. Quando eu tento desinstalar o cliente VPN, eu recebo esta mensagem de erro: **Error msg (mensagem de erro): não encontram o arquivo de desinstação…** O que essa mensagem de erro significa e como posso concluir com sucesso a desinstalação?

A. Verifique o Control Panel de rede para garantir que o Deterministic NDIS Extender (DNE) não foi instalado. Escolha também **Microsoft > Current Version > Uninstall** para verificar o arquivo de desinstalação. Remova o arquivo **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5}** e repita a desinstalação.

Q. Não consigo instalar o cliente VPN no Windows 2000 Professional. Eu recebo este erro: **Um arquivo de suporte de instalação não podia ser instalado.** Falha catastrófica. O que devo fazer?

A. Remova a chave **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall**. Em seguida, reinicialize seu computador e reinstale o cliente VPN.

Nota: Para encontrar a chave correta para o software Cisco VPN Client no caminho HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<key *to be determined*>, vá para HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\ e clique em **VPN Client**. Na janela à direita, veja o Uninstall Path (caminho de desinstalação) sob a coluna Name (nome). A coluna dos dados correspondentes indica o valor chave do cliente VPN. Anote essa chave, vá para HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\, selecione a chave determinada, e a exclua.

Consulte Troubleshooting de Erros de Inicialização e também o bug da Cisco ID CSCdv15391 (somente clientes registrados) no Bug Toolkit para obter mais informações.

Q. Quando eu tento instalar o Linux VPN Client no RedHat 8.0, recebo um erro que diz que o módulo não pode ser carregado porque o módulo foi compilado com o GCC 2 e o kernel foi compilado com GCC 3.2. O que devo fazer?

A. Isso ocorre porque a nova release do RedHat tem uma versão mais recente do compilador GCC (3.2+), o que provoca a falha do Cisco VPN Client atual. Esse problema foi corrigido e está disponível em Cisco VPN 3.6.2a. Consulte o bug da Cisco ID CSCdx15865 (somente clientes registrados) no Bug Toolkit para obter detalhes ou baixe o software do Centro de Software de VPN (somente clientes registrados).

Q. Eu recebo uma mensagem de erro "peer no longer responding" quando meu VPN Client 3.5 para Linux tenta estabelecer uma conexão IPSec para um PIX ou para um VPN 3000 Concentrator. O que devo fazer?

A. O sintoma desse problema é que o cliente Linux parece tentar conectar, mas nunca obtém uma resposta do dispositivo de gateway.

O sistema operacional Linux possui um firewall interno (ipchains) que bloqueia a porta UDP 500, a porta UDP 1000 e os pacotes ESP. Como o firewall é habilitado por padrão, você tem que desabilitar o firewall ou abrir as portas para a comunicação IPsec para ambas as conexões de entrada e saída para corrigir o problema.

Q. Eu recebo um erro de extensão de kernel quando eu tento executar Cisco VPN 5000 5.2.2 Client no Mac OS X 10.3. O que devo fazer?

A. Conforme indicado nas release notes do produto, o Cisco VPN 5000 Client é suportado até a versão 10.1.x e, portanto, não é suportado na versão 10.3. É possível fazer com que o cliente VPN funcione quando você retorna as permissões em dois dos arquivos instalados depois de executar o script de instalação. Aqui está um exemplo:

Nota: Essa configuração *não* é suportada pela Cisco.

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. Não consigo instalar a nova versão do Cisco VPN Client. Quando eu instalo, eu recebo uma destas mensagens de erro: "Error DNEinst execution error while installing DNE, return code -2146500093" ou "InstallDNE Error: DNEinst execution error while installing DNE, returncode -2147024891." Esse problema ocorre quando eu instalo o Deterministic Network Enhancer.

A. Instale o upgrade DNE mais recente do Deterministic Networks.

Q. Eu obtenho estes logs para o Cisco VPN Client quando eu faço uma conexão:

```
208    15:09:08.619  01/17/08  Sev=Debug/7CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209    15:09:08.619  01/17/08  Sev=Warning/2CVPND/0xE3400003
Function RegOpenKey failed with an error code of 0x00000002(WindowsVirtualAdapter:558)

210    15:09:08.619  01/17/08  Sev=Warning/3CVPND/0xE340000C
```

The Client was unable to enable the Virtual Adapter because it could not open the device.

A. É uma mensagem de erro razoavelmente genérica, que normalmente exige a desinstalação manual do cliente. Siga as instruções neste link. Removendo uma versão do cliente VPN instalada com o instalador MSI.

Após desinstalar, certifique-se de reinicializar. Em seguida, reinstale o cliente. Certifique-se de estar conectado como um usuário que tenha direitos de administrador na máquina local.

Q. Quando eu tento conectar o Cisco VPN Client em um Mac OS, eu recebo este Mensagem de Erro: **Erro 51- incapaz a uma comunicação com o subsistema VPN.** Como resolvo esse problema?

A. O problema será resolvido se você reiniciar o serviço após fechar o VPN Client desta forma:

Para parar:

```
sudo kextunload -b com.cisco.nke.ipsec
```

Para iniciar:

```
sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN
```

Verifique também a seguinte execução na mesma máquina onde o cliente VPN está instalado e desabilite o mesmos.

- Qualquer software virtual (como VMWare Fusions, Parallels, crossovers)
- Qualquer software antivírus/de firewall.
- Compatibilidade do cliente VPN com o sistema operacional de 64 bits; consulte as Release Note do Cisco VPN Client.

Q. Eu recebo o erro "Reason 442: failed to enable virtual adapter". Como eu posso solucionar esse erro?

A. O erro Reason 442: failed to enable virtual adapter aparece depois que o Vista informa que foi detectado um endereço IP duplicado. As conexões subsequentes falham com a mesma mensagem, mas o Vista não informa que foi detectado um endereço IP duplicado. Consulte Endereço IP Duplicado Aciona o Erro 442 no Windows Vista para obter mais informações sobre como solucionar esse problema.

Q. Quando eu instalo o Cisco VPN Client, o erro Deterministic Network Enhancer Add Plugin Failed é exibido. Como solucionar esse erro?

A. Instalar o adaptador DNE pode resolver o problema. É melhor usar a versão Installshield para a instalação em vez do MSI.

Q. Eu recebi este erro: **Razão 442: não permitem o adaptador virtual.** Como resolvo esse problema?

A. Este erro aparece após Windows 7 e Windows Vista relata um endereço de IP duplicado detectado. As conexões subsequente falham com a mesma mensagem, mas o OS não relata que o endereço de IP duplicado está detectado. Refira o erro 442 dos disparadores do endereço de IP duplicado em Windows 7 e a vista para obter mais informações sobre de como resolver esta edição.

Q. Quando eu tento lançar o cliente VPN 4.9 para o MAC OS 10.6, eu recebo este erro: `Erro 51: Incapaz de comunicar-se com o subsistema do vpn.` Como resolver esta edição?

A. Esta edição ocorre porque o apoio 64-bit não está disponível com o Cisco VPN Client para a liberação 4.9 do MAC OS. Como uma ação alternativa, você pode carreg no modo de 32 bits do núcleo. Para mais informação, refira a identificação de bug Cisco CSCth11092 (clientes registrados somente) e o Cisco VPN Client para Release Note MAC OSX.

Compatibilidade com Terceiros

Q. O cliente Nortel é compatível com os Cisco VPN 300 Concentrators?

A. No. O cliente Nortel não pode conectar ao Cisco VPN 3000 Concentrator.

Q. Posso ter clientes VPN de outros fornecedores, como o Nortel Contivity VPN Client, instalados simultaneamente com o Cisco VPN Client?

A. No. Sabe-se que ocorrem problemas quando vários clientes VPN são instalados no mesmo PC.

Q. Os Cisco VPN Clients são suportados com VPN Concentrators de terceiros?

A. Não há suporte para Cisco VPN Clients com VPN Concentrators de terceiros.

Autenticação

Q. Como as versões 1.1 e 3.x dos Cisco VPN Clients armazenam internamente os certificados digitais (X.509v3)?

A. O Cisco VPN Client 1.1 tem seu armazenamento próprio de certificados. O Cisco VPN Client 3.x pode armazenar os certificados no armazenamento da Microsoft usando a Common-Application Programming Interface (CAPI) ou no armazenamento próprio da Cisco (Rsa Data Security).

Q. Posso usar um nome de grupo igual ao nome de usuário no VPN concentrator?

A. Não, o nome do grupo e o nome de usuário não podem ser o mesmo. Esse é um problema conhecido, encontrado nas versões 2.5.2 e 3.0 do software e integrado na versão 3.1.2. Consulte o bug da Cisco ID CSCdw29034 (somente clientes registrados) no Bug Toolkit para obter detalhes.

Q. As placas full-challenge, como a Defender, são aceita no Cisco VPN Client para PIX?

A. Não, não há suporte a placas desse tipo.

Versão do Software do VPN Client

Q. O que aconteceu com a opção "Set MTU Utility" que havia nas versões 2.5.2 e anteriores do Cisco VPN Client?

A. O Cisco VPN Client agora ajusta o tamanho da Unidade Máxima de Transmissão (MTU). A opção Set MTU Utility do grupo não é mais uma etapa de instalação obrigatória. A opção Set MTU é usada principalmente para diagnosticar problemas de conectividade. O caminho para selecionar a opção SetMTU para uma máquina de Windows é **Start > Programs > Cisco Systems VPN Client > SetMTU**. Para obter mais informações sobre a opção SetMTU e a configuração desta opção em outros sistemas operacionais, consulte Alteração do tamanho do MTU com a opção SetMTU.

Q. Quais são os idiomas suportados nas versões de interface gráfica do usuário do Cisco VPN Client posteriores à 4.0?

A. Os idiomas suportados nas versões de interface gráfica do usuário do Cisco VPN Client posteriores à 4.0 são canadense, francês e japonês.

Q. Quais firewalls pessoais são compatíveis com o Cisco VPN Client?

A. Para fornecer um nível mais alto de segurança, o cliente VPN pode aplicar a operação de um firewall suportado ou receber uma política de stateful firewall para o tráfego da Internet.

Atualmente, o VPN Client 5.0 suporta os seguintes firewalls pessoais:

- BlackIce Defender
- Cisco Security Agent
- Sygate Personal Firewall
- Sygate Personal Firewall Pro
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

A partir da versão 3.1, um novo recurso foi adicionado ao VPN 3000 Concentrator para detectar quais softwares de firewall pessoal os usuários remotos instalaram e impedir que os usuários se conectem na ausência do software apropriado. Escolha **Configuration > User Management > Groups > Client FW**, e clique na guia do grupo para o qual você vai configurar esse recurso

Para obter mais informações sobre a aplicação da política de firewall em uma máquina Cisco VPN Client, consulte Cenários de Configuração de Firewall.

Q. Existem problemas de conectividade ao utilizar o Cisco VPN Client 3.x com o AOL 7.0?

A. O Cisco VPN Client não funciona com AOL 7.0 sem o uso de tunelamento dividido. Consulte o bug da Cisco ID CSCdx04842 (somente clientes registrados) no Bug Toolkit para obter detalhes.

Configuração de Software do VPN Client

Q. Por que o Cisco VPN Client desconecta após 30 minutos? Posso estender esse período de tempo?

A. Se não houver atividades de comunicação em uma conexão do usuário durante esse período de 30 minutos, o sistema terminará a conexão. A configuração de timeout de ociosidade padrão é 30 minutos, com um valor mínimo permitido de 1 minuto e um máximo de 2.147.483.647 minutos (mais de 4.000 anos).

Escolha **Configuration > User Management > Groups** e escolha o nome do grupo apropriado para modificar a configuração de timeout de ociosidade. Escolha **Modify Group**, clique na guia **HW Client** e insira o valor desejado no campo User Idle Timeout. Insira **0** para desabilitar o timeout e permitir um período ocioso ilimitado.

Q. O Cisco VPN Client pode ser implementado com todos os parâmetros pré-configurados?

A. Se o arquivo vpnclient.ini está empacotado com o software de cliente VPN quando ele é instalado, ele configurará automaticamente o cliente VPN durante a instalação. Você também pode distribuir os arquivos de perfil (um arquivo .pcf para cada entrada de conexão) como perfis de conexão pré-configurados para a configuração automática. Para distribuir cópias pré-configuradas do software de cliente VPN aos usuários para a instalação, conclua estas etapas:

1. Copie os arquivos do software de cliente VPN do CD-ROM de distribuição em cada diretório em que você criou um arquivos vpnclient.ini (global) e separe os perfis de conexão para cada conjunto de usuários.**Nota:** Para a plataforma Mac OS X, os arquivos pré-configurados são colocados nas pastas Perfis e Recursos antes do cliente VPN ser instalado. O arquivo vpnclient.ini é colocado no diretório do instalador. Você deve colocar os arquivos personalizados vpnclient.ini no diretório VPN Client Installer no mesmo nível que as pastas Perfis e Recursos. Veja o Capítulo 2 do Guia do Usuário do Cliente VPN para Mac OS X para obter mais informações
2. Prepare e distribua o software empacotado. Distribuição em CD-ROM ou em rede. Certifique-se de que o arquivo vpnclient.ini e os arquivos de perfil estejam no mesmo diretório com todos os arquivos de imagem do CD-ROM. Os usuários podem instalar a partir desse diretório através de uma conexão de rede; ou você pode copiar todos os arquivos para um novo CD-ROM de distribuição; ou você pode criar um arquivo zip self-extracting que contenha todos os arquivos desse diretório, e os usuários baixam e, em seguida, instalam o software.
3. Forneça aos usuários quaisquer outras informações e instruções de configuração necessárias. Veja o Capítulo 2 do Guia do Usuário do Cliente VPN para sua plataforma.

Q. Parece que o Cisco VPN Client tem um conflito com minha placa de rede. Como devo solucionar esse problema?

A. Assegure-se de executar os drivers mais recentes na placa de rede. Isso é sempre recomendado. Se possível, teste para ver se o problema é específico do sistema operacional, hardware do PC e de outras placas NIC.

Q. Como automatizo a conexão do Cisco VPN Client a partir do Dial-Up Networking?

A. Escolha **Options > Properties > Connections** e faça o Cisco VPN Client selecionar uma entrada da agenda telefônica do Dial-UP Networking para automatizar totalmente a discagem na conexão VPN.

Q. Como eu configuro o Cisco VPN 3000 Concentrator para notificar usuários remotos para a atualização do cliente VPN?

A. Você pode notificar os usuários do cliente VPN quando é hora de atualizar o software de Cliente VPN em seus sistemas remotos. Consulte Notificação de Usuários Remotos sobre uma Atualização de Cliente para uma abordagem passo a passo. Certifique-se de digitar as informações de release como "(Rel)", conforme mostrado no passo 7 do processo.

Q. O que pode causar um atraso antes do Cisco VPN Client ser aberto, especificamente quando a opção "Start Before Logon" está habilitada?

A. O Cisco VPN Client está no *modo fall back*. Isso contribui para o atraso. No modo fallback, o Cliente VPN executa de forma diferente de quando inicia antes da sessão estar em uso. Ao operar no modo fallback, o cliente VPN não verifica se os serviços necessários do Windows foram iniciados. Como consequência, a conexão VPN poderá falhar se for iniciada muito rápido. Desinstale o Cisco VPN Client e remova os aplicativos causadores para permitir a inicialização sem estar no modo "fall back". Em seguida, reinstale o Cisco VPN Client. Para obter mais informações sobre o modo fallback, consulte Iniciar antes do Logon.

Consulte os bugs da Cisco IDs CSCdt88922 (somente clientes registrados) e CSCdt55739 (somente clientes registrados) no Bug Toolkit para obter mais informações.

Q. Eu preciso compreender a diferença entre o ipsecdialer.exe e o vpngui.exe. Por que o vpngui.exe está instalado na INICIALIZAÇÃO do meu Windows XP, mas eu ainda preciso iniciar manualmente o ipsecdialer para acessar os recursos da minha empresa? E (independentemente do tamanho) esses programas parecem acionar a mesma coisa: um logon VPN na rede da minha empresa.

A. O ipsecdialer.exe era o mecanismo de inicialização original para o Cisco VPN Client version 3.x. Quando a GUI foi alterada nas versões 4.x, um novo executável chamado vpngui.exe foi criado. O arquivo ipsecdialer.exe teve o nome aproveitado para fins de compatibilidade com as versões anteriores e apenas inicia o vpngui.exe. Essa é a razão pela qual você percebeu a diferença no tamanho do arquivo.

Então, quando você muda da versão 4.x para versão 3.x do Cisco VPN Client, você precisa do arquivo ipsecdialer.exe para a inicialização.

Q. Posso remover com segurança o ícone de inicialização da VPN? Por que ele é

necessário?

A. O Cisco VPN Client na pasta de inicialização oferece suporte ao recurso "Iniciar Antes do Logon". Se você não usa o recurso, ele não precisa estar na pasta de inicialização.

Q. Por que "user_logon" é adicionado, e não o atalho do ipsecdialer.exe? Qual é a finalidade do "início de sessão do usuário"?

A. O recurso "Iniciar Antes do Logon" necessita do "user_logon", mas uma inicialização normal do Cisco VPN Client pelo usuário não precisa.

Problemas de NAT/PAT

Q. Meu problema é que apenas um cliente VPN (releases 3.3 e anteriores) está conseguindo se conectar por meio de um dispositivo de Tradução de Endereço de Porta (PAT). O que posso fazer para eliminar o problema?

A. Houve um bug em várias implementações de Conversão de Endereço de Rede (NAT)/PAT que fazer com que as portas com menos de 1024 não sejam convertidas. No Cisco VPN Client 3.1, mesmo com a transparência de NAT habilitada, a sessão do Internet Security Association and Key Management Protocol (ISAKMP) usa a porta UDP 512. O primeiro cliente VPN atravessa o dispositivo PAT e mantém a porta de origem 512 na parte externa. Quando o segundo cliente VPN conecta, a porta 512 já está em uso. A tentativa falha.

Existem três possíveis soluções alternativas.

- Corrija o dispositivo PAT.
- Faça upgrade dos clientes VPN para a versão 3.4 e use o encapsulamento de TCP.
- Instale um VPN 3002 para substituir todos os clientes VPN.

Q. É possível conectar dois laptops com o Cisco VPN Client do mesmo local?

A. Dois clientes podem conectar ao mesmo head end a partir do mesmo local desde que os clientes não estejam ambos atrás de um dispositivo que executa o PAT, como um roteador/firewall SOHO. Muitos dispositivos PAT podem mapear UMA conexão de VPN para um cliente atrás dele, mas não dois. Para permitir que dois clientes VPN se conectem do mesmo local por trás de um dispositivo PAT, habilite algum tipo de encapsulamento, como NAT-T, IPSec over UDP ou IPSec over TCP no head end. Geralmente, o NAT-T ou outro encapsulamento deve ser habilitado se QUALQUER dispositivo NAT estiver entre o cliente e o head end.

Diversos

Q. Quando me conecto à rede do escritório usando um laptop e depois o levo para casa, tenho problemas para me conectar ao VPN 3000 Concentrator em casa. Qual é o problema?

A. O laptop pode estar retendo as informações de roteamento da conexão de LAN. Consulte VPN Clients com Problemas de Roteamento Microsoft para obter informações sobre como resolver

esse problema.

Q. Como posso saber se um cliente VPN está conectado ao VPN Concentrator?

A. Verifique a chave do Registro chamada HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. Se um túnel estiver ativo, o valor será 1. Se não houver túnel, o valor será 0.

Q. Tenho problemas com a conexão do NetMeeting a partir de um PC por trás de um VPN Concentrator para um cliente VPN, mas a conexão funciona quando executo a partir do PC para um cliente VPN por trás de um VPN Concentrator. Como posso resolver isso?

A. Siga os passos apropriados relacionados aqui para controlar as configurações de conexão:

- Na unidade principal do PC, escolha **Program Files > Cisco Systems > VPN Client > Profiles**. Clique com o botão direito o perfil que você usa, e escolha **Abrir com** para abrir o perfil em um editor de texto (por exemplo, o Bloco de notas). (Ao escolher o programa que deseja usar, certifique-se de desmarcar a caixa que diz **Always use this program to open these files**.) Encontre o parâmetro do perfil para ForcekeepAlives e altere o valor de 0 para **1**. Em seguida, salve o perfil.ou
- Para o cliente VPN, escolha **Options > Properties > General** e insira um valor para "Peer response timeout", conforme mostrado nesta janela de exemplo. Você pode especificar uma sensibilidade de timeout entre 30 a 480 segundos.ou
- Para o VPN concentrator, escolha **Configuration > User Management > Groups > modify group** . Na guia IPsec, escolha a opção para IKE Keepalives, conforme mostrado nesta janela de exemplo.

O intervalo de Dead Peer Detection (DPD) varia em função da configuração de sensibilidade. Uma vez que uma resposta não é recebida, ele entra em um modo mais agressivo e envia pacotes a cada cinco segundos até que o limite da resposta do peer seja atingido. Quando isso ocorrer, a conexão será desfeita. Você pode desabilitar os keepalives, mas, se sua conexão for realmente desfeita, você precisará esperar o intervalo. A Cisco recomenda que você defina um valor de sensibilidade muito baixo inicialmente.

Q. O Cisco VPN Client suporta autenticação dupla?

A. Não A autenticação dupla não é suportada no Cisco VPN Client.

Q. Como eu posso configurar o Cisco VPN Client para conectar no modo principal, em vez do modo agressivo?

A. Você deve usar assinaturas digitais (certificados) para permitir que o Cisco VPN Client conecte no modo principal. Há 2 métodos para realizar isso:

1. Obtenha certificados CA do fornecedor de certificados de terceiros (por exemplo, o VeriSign ou Entrust) para o roteador e para todos os Cisco VPN Clients. Registre os certificados de identidade do mesmo servidor CA e use assinaturas digitais como uma maneira de autenticação entre o Cisco VPN Client e o roteador. Para obter mais informações sobre essa

configuração, consulte Configuração de IPSec entre Cisco IOS Routers e Cisco VPN Client Usando Certificados do Entrust.

2. A segunda opção é configurar o roteador como o servidor CA, juntamente com o head end ao acesso remoto VPN. Instalar os certificados (e todo o resto) permanecerá como descrito no link anterior, exceto que o roteador se comportará como um servidor CA. Para obter mais informações, consulte VPN LAN-to-LAN Dinâmico entre Cisco IOS Routers Utilizando IOS CA no Exemplo de Configuração do Hub.

Q. Como eu transformo em somente leitura os parâmetros obrigatórios no arquivo de acesso ao cliente VPN?

A. Adicione um ponto de exclamação (!) à parte inicial de cada parâmetro no arquivo .pcf para cada usuário para tornar o parâmetro somente leitura.

Os valores para os parâmetros que começam com um ponto de exclamação (!) não podem ser mudados pelo usuário no cliente VPN. Os campos para esses valores na interface gráfica do usuário aparecerão escurecidos (somente leitura).

Esta é uma configuração de exemplo:

Arquivo .pcf Original

```
[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1

GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C85
              1ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice
```

Arquivo .pcf Alterado

```
[main]

!Description=connection to TechPubs server

!Host=10.10.99.30

AuthType=1
```

```
!GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C
          851ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

!Username=alice
```

Nesse exemplo, o usuário é incapaz de alterar os valores de *Description*, *Host*, *GroupName*, e *Username*.

Q. É possível limitar/restringe o acesso para os clientes VPN baseados em endereços MAC?

A. No. Não é possível limitar/restringe o acesso para os clientes VPN baseados em endereços MAC.

Informações Relacionadas

- Página de suporte ao Cisco VPN 3000 Client
- Página de Suporte do Cisco VPN Client
- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Suporte Técnico e Documentação - Cisco Systems