

Guia de solução de problemas do cliente AnyConnect VPN - Problemas comuns

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Processo de Troubleshooting](#)

[Problemas de Instalação e do Adaptador Virtual](#)

[Desconexão ou Incapacidade de Estabelecer a Conexão Inicial](#)

[Problemas com a Passagem de Tráfego](#)

[Problemas de Quedas do AnyConnect](#)

[Problemas de Fragmentação/Passagem de Tráfego](#)

[Desinstalar Automaticamente](#)

[Problema ao preencher o cluster FQDN](#)

[Configuração de lista do servidor de backup](#)

[AnyConnect: Problema de Banco de Dados de Drivers Corrompido](#)

[Reparo](#)

[Falha no reparo](#)

[Análise o Banco de Dados](#)

[Mensagens de erro](#)

[Erro: Unable to Update the Session Management Database](#)

[Solução 1](#)

[Solução 2](#)

[Erro: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register"](#)

[Solução](#)

[Erro: "Um erro foi recebido do gateway seguro em resposta à solicitação de negociação de VPN. Entre em contato com o administrador da rede"](#)

[Solução](#)

[Erro: Não foi possível estabelecer a sessão. O limite de 2 sessões foi atingido.](#)

[Solução 1](#)

[Solução 2](#)

[Erro: O AnyConnect não está habilitado no servidor VPN ao tentar conectar o anyconnect ao ASA](#)

[Solução](#)

[Erro:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x que transmitem o pacotes maiores 1220 \(ponto inicial 1206\)](#)

[Solução](#)

[Erro: O gateway seguro rejeitou a solicitação de conexão ou reconexão à vpn do agente.](#)

[Solução](#)

[Erro: "Não foi possível atualizar o banco de dados de gerenciamento de sessão"](#)

[Solução](#)

[Erro: "O driver de cliente VPN encontrou um erro"](#)

Solução

Erro: "Não foi possível processar a resposta de xxx.xxx.xxx.xxx"

Solução

Erro: "Login negado, mecanismo de conexão não autorizado; entre em contato com o administrador"

Solução

Erro: "Pacote do Anyconnect indisponível ou corrompido. Entre em contato com o administrador do sistema"

Solução

Erro: "O pacote do AnyConnect no gateway seguro não pode ser localizado"

Solução

Erro: "A VPN segura via desktop remoto não é compatível"

Solução

Erro: "O certificado do servidor recebido ou sua cadeia não está em conformidade com o FIPS. Não será estabelecida uma conexão de VPN"

Solução

Erro: "Falha na validação do certificado"

Solução

Erro: "O serviço do agente da VPN encontrou um problema e precisa ser fechado. Lamentamos o inconveniente"

Solução

Erro: "Este pacote de instalação não pode ser aberto. Verifique se o pacote existe"

Solução

Erro: "Erro ao aplicar transformações. Verifique se os caminhos de transformação especificados são válidos."

Solução

Erro: "O driver de cliente VPN encontrou um erro"

Solução

Erro: "Uma reconexão de VPN resultou na definição de configuração diferente. A configuração de rede VPN está sendo reinicializada. Aplicações que utilizam a rede privada podem precisar ser restauradas."

Solução

Erro do AnyConnect ao fazer login

Solução

A configuração de proxy do IE não é restaurada após a desconexão do AnyConnect no Windows 7

Solução

Erro: O AnyConnect Essentials não pode ser habilitado até que todas essas sessões sejam encerradas.

Solução

Erro: A guia de Conexão na opção de Internet do Internet Explorer é oculta depois de ficar conectada ao cliente AnyConnect.

Solução

Erro: Alguns usuários estão recebendo mensagem de erro de falha de login enquanto outros são capazes de se conectar através da VPN do AnyConnect

Solução

Erro: O certificado que você está visualizando não coincide com o nome do site que você está

[tentando visualizar.](#)

[Solução](#)

[Não foi possível iniciar o AnyConnect do CSD Vault em uma máquina com Windows 7](#)

[Solução](#)

[O perfil do AnyConnect não é replicado para o modo de espera após o failover](#)

[Solução](#)

[O AnyConnect cliente trava se o Internet Explorer estiver off-line](#)

[Solução](#)

[Mensagem de Erro: TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER](#)

[Solução](#)

[Mensagem de Erro: "A tentativa de conexão falhou devido à entrada de host inválido"](#)

[Solução](#)

[Erro: "Verifique se os certificados do servidor podem passar o modo rigoroso se você configurar a VPN sempre ativa"](#)

[Solução](#)

[Erro: "Ocorreu um erro interno nos Serviços HTTP do Microsoft Windows"](#)

[Solução](#)

[Erro: "O transporte SSL recebeu uma falha de canal seguro. Pode ser resultado de uma configuração de criptografia não suportada no Secure Gateway."](#)

[Solução](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve um cenário de solução de problemas que se aplica a aplicativos que não funcionam através do Cisco AnyConnect VPN Client.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações contidas neste documento têm como base um dispositivo Cisco Adaptive Security (ASA) que executa a versão 8.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Processo de Troubleshooting

Este cenário de troubleshooting típico destina-se a aplicações que não funcionam através do Cisco AnyConnect VPN Client para usuários finais com computadores baseados no Microsoft

Windows. Estas seções abordam e fornecem soluções para os problemas:

- [Problemas de Instalação e do Adaptador Virtual](#)
- [Desconexão ou Incapacidade de Estabelecer a Conexão Inicial](#)
- [Problemas com a Passagem de Tráfego](#)
- [Problemas de Quedas do AnyConnect](#)
- [Problemas de Fragmentação/Passagem de Tráfego](#)

Problemas de Instalação e do Adaptador Virtual

Conclua estes passos:

1. Obtenha o arquivo do log do dispositivo:

Windows XP/Windows 2000:

```
\Windows\setupapi.log
```

Windows Vista:

Note: É necessário tornar as pastas ocultas visíveis para que seja possível ver estes arquivos.

```
\Windows\Inf\setupapi.app.log  
\Windows\Inf\setupapi.dev.log
```

Se você vir erros no arquivo de log **setupapi**, poderá aumentar a verbosidade para 0x2000FFFF.

2. Obtenha o arquivo de log do instalador MSI:

Se esta for uma instalação de implantação via Web inicial, este log estará localizado no diretório temporário de cada usuário.

Windows XP/Windows 2000:

```
\Documents and Settings\  

```

Windows Vista:

```
\Users\
```

Se este for um upgrade automático, este log estará no diretório temporário do sistema:

```
\Windows\Temp
```

O nome de arquivo está no formato: **anyconnect-win-x.x.xxxx-k9-install-yyyyyyyyyyyyyy.log**. Obtenha o arquivo mais recente para a versão do cliente que você deseja instalar. x.xxxx muda com base na versão, como 2.0.0343, e yyyyyyyyyyyyyyy representa a data e a hora da instalação.

3. Obtenha o arquivo de informação de sistema do PC:

Desde um Prompt de Comandos/DOS, digite:

Windows XP/Windows 2000:

```
winmsd /nfo c:\msinfo.nfo
```

Windows Vista:

```
msinfo32 /nfo c:\msinfo.nfo
```

Note: Depois de digitar esse prompt, aguarde. A conclusão do arquivo poderá levar entre dois e cinco minutos.

Obtenha um dump do arquivo systeminfo de um prompt de comando:

Windows XP e Windows Vista:

```
systeminfo c:\sysinfo.txt
```

Consulte o [AnyConnect: Problema de Banco de Dados de Drivers Corrompido para depurar o problema.](#)

Desconexão ou Incapacidade de Estabelecer a Conexão Inicial

Se você tiver problemas de conexão com o cliente AnyConnect, como desconexões ou a incapacidade de estabelecer uma conexão inicial, obtenha estes arquivos:

- O arquivo de configuração do ASA para determinar se alguma coisa na configuração está causando a falha de conexão:

No console do ASA, digite `write net x.x.x.x:ASA-Config.txt` onde `x.x.x.x` é o endereço IP de um servidor TFTP na rede.

OU

No console do ASA, digite `show running-config`. Deixe a configuração completa na tela, depois recorte e cole em um editor de texto e salve.

- Os logs de eventos do ASA:

Para ativar o logon no ASA para eventos de autenticação, WebVPN, Secure Sockets Layer (SSL) e SSL VPN Client (SVC), emita estes comandos na CLI:

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

Crie uma sessão do AnyConnect e verifique se a falha pode ser reproduzida. Capture a saída de log do console para um editor de texto e salve.

Para desabilitar o log, execute o comando `no logging enable`.

- O log do Cisco AnyConnect VPN Client do Windows Event Viewer PC cliente:

Escolha **Start > Run**.

Insira:

```
eventvwr.msc /s
```

Clique com o botão direito do mouse no log **Cisco AnyConnect VPN Client** e selecione **Salvar o arquivo de log como AnyConnect.evt**.

Note: Salve-o sempre como **formato de arquivo .evt**.

Se o usuário não puder se conectar com o AnyConnect VPN Client, o problema pode estar relacionado a uma sessão do Remote Desktop Protocol (RDP) estabelecida ou Switching de usuário rápido habilitada no computador do cliente. O usuário pode ver as configurações de perfil do AnyConnect determinarem um único usuário local, mas vários usuários locais estão conectados no momento no computador. *Uma mensagem de erro VPN connection will not be established no PC cliente.* Para resolver esse problema, desconecte qualquer sessão RDP estabelecida e desative o Switch de usuário rápido. Esse comportamento é controlado pelo atributo [Imposição de Logon do Windows](#) no perfil do cliente, no entanto, atualmente não há nenhuma configuração que permita que um usuário estabeleça uma conexão VPN enquanto vários usuários estão conectados simultaneamente na mesma máquina. Solicitação de aprimoramento [CSCsx15061](#) foi arquivado para endereçar este recurso.

Note: Verifique se a porta 443 não está bloqueada para que o cliente AnyConnect possa se conectar ao ASA.

Quando um usuário não consegue conectar o AnyConnect VPN Client ao ASA, o problema pode ser causado por uma incompatibilidade entre a versão do AnyConnect Client e a versão de imagem de software ASA. Neste caso, o usuário recebe esta mensagem de erro: *o instalador não foi capaz de iniciar o cliente do Cisco VPN; o acesso clientless não está disponível.*

Para resolver esse problema, atualize a versão do cliente AnyConnect para ser compatível com a imagem do software ASA.

Quando você se conectar pela primeira vez ao AnyConnect, o script de login não será executado. Se você se desconectar e fizer login novamente, o script de login funciona muito bem. Este é o comportamento esperado.

Ao conectar o AnyConnect VPN Client para ASA, você poderá receber este erro: *usuário não autorizado para acessar o AnyConnect Client. Entre em contato com o administrador.*

Esse erro é visto quando a imagem do AnyConnect está ausente do ASA. Uma vez que a imagem é carregada para o ASA, o AnyConnect pode se conectar sem problemas ao ASA.

Esse erro pode ser resolvido ao desativar o Datagram Transport Layer Security (DTLS). Acesse **Configuração > VPN de acesso remoto > Acesso de rede (cliente) > Perfis de conexão do AnyConnect** e **desmarque a caixa de seleção Habilitar DTLS**. Essa ação desativa o DTLS.

Os arquivos dartbundle mostram esta mensagem de erro quando o utilizador é desligado:

```
TUNNELPROTOCOLDPDPMGR_ERROR_NO_DPD_RESPONSE:O gateway seguro não respondeu aos pacotes de Detecção de Peer Dead. Esse erro significa que o canal DTLS foi dividido devido à falha de Dead
```

Peer Detection (DPD). Este erro é resolvido se você ajustar os keepalives DPD e executar estes comandos:

```
webvpn
svc keepalive 30
svc dpd-interval client 80
svc dpd-interval gateway 80
```

Os comandos `svc keepalive` e `svc dpd-interval` são substituídos pelos comandos `anyconnect keepalive` e `anyconnect dpd-interval` respectivamente no ASA versão 8.4(1) e posterior, como mostrado aqui:

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

Problemas com a Passagem de Tráfego

Quando são detectados problemas com o tráfego de passagem para a rede privada com uma sessão do AnyConnect através do ASA, conclua estas etapas de coleta de dados:

1. Obtenha a saída do comando ASA `show vpn-sessiondb detail svc filter name <username> do console`. Se a saída mostrar `O Nome do filtro: XXXXX`, obtenha a saída de `show access-list XXXXX`. Verifique se a lista de acesso XXXXXX não bloqueia o fluxo de tráfego pretendido.
2. Exporte as estatísticas do AnyConnect de **AnyConnect VPN Client > Estatísticas > Detalhes > Exportação (AnyConnect-ExportedStats.txt)**.
3. Verifique o arquivo de configuração do ASA em busca de instruções `nat`. Se a Conversão de endereço de rede (NAT) estiver habilitada, ela deve isentar dados que retornam para o cliente como resultado de NAT. Por exemplo, para isentar os endereços IP do pool AnyConnect da NAT (nat 0), use isto na CLI:

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. Determine se o gateway padrão tunelado precisa ser habilitado para a instalação. O gateway padrão tradicional é o Gateway of Last Resort para o tráfego não descriptado.

Exemplo:

```
!--- Route outside 0 0 is an incorrect statement.
```

```
route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

Por exemplo, se o cliente de VPN precisar acessar um recurso que não está na tabela de roteamento de gateway de VPN, o pacote é encaminhado através do gateway padrão. O gateway de VPN não precisa da tabela de roteamento interno completa para resolver isso. A palavra-chave **em túnel pode ser encapsulada nesse caso**.

5. Verifique se o tráfego do AnyConnect é descartado pela política de inspeção do ASA. Você pode isentar o aplicativo específico que é usado pelo AnyConnect Client se implementar a Modular Policy Framework do Cisco ASA. Por exemplo, você pode isentar o protocolo skinny com esses comandos.

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect skinny
```

Problemas de Quedas do AnyConnect

Conclua estas etapas de coleta de dados:

1. Certifique-se de que o utilitário Microsoft Dr. Watson esteja habilitado. Para fazer isso, escolha Start > Run e execute **Drwtsn32.exe**. Configure-o e clique em OK:

```
Number of Instructions      : 25
Number of Errors To Save  : 25
Crash Dump Type           : Mini
Dump Symbol Table         : Checked
Dump All Thread Contexts  : Checked
Append To Existing Log File : Checked
Visual Notification       : Checked
Create Crash Dump File    : Checked
```

Quando a queda/falha ocorre, obtenha os arquivos .log .dmp de **C:\Documents and Settings\AllUsers\Application Data\Microsoft\Dr Watson**. Se estes arquivos parecem estar em uso, use o **ntbackup.exe**.

2. Obtenha o log do AnyConnect VPN Client do Windows Event Viewer do PC cliente:

Escolha **Start > Run**.

Insira:

```
eventvwr.msc /s
```

Clique com o botão direito do mouse no log **Cisco AnyConnect VPN Client** e selecione **Salvar o arquivo de log como AnyConnect.evt**.

Note: Salve-o sempre como **formato de arquivo .evt**.

Problemas de Fragmentação/Passagem de Tráfego

Alguns aplicativos, como Microsoft Outlook, não funcionam. No entanto, o túnel é capaz de passar outro tipo de tráfego, como pings pequenos.

Isso pode fornecer indícios de um problema de fragmentação na rede. Roteadores de uso doméstico são particularmente deficientes na fragmentação e remontagem de pacotes.

Tente um conjunto de dimensionamento de pings para determinar se ele falha em um determinado tamanho. Por exemplo, ping -l 500, ping -l 1000, ping -l 1500, ping -l 2000.

É recomendável configurar um grupo especial para os usuários que experimentam a fragmentação e definir a Unidade máxima de transição (MTU) de SVC para esse grupo de 1200. Dessa forma, você pode corrigir os usuários que têm esse problema sem afetar a base de usuários mais ampla.

Problema

As conexões TCP param de funcionar quando são conectadas ao AnyConnect.

Solução

Para verificar se o usuário tem um problema de fragmentação, ajuste o MTU para AnyConnect Clients no ASA.

```
ASA(config)#group-policy <name> attributes
webvpn
svc mtu 1200
```

Desinstalar Automaticamente

Problema

O AnyConnect VPN Client é desinstalado depois que termina a conexão. Os logs do cliente mostram que keep installed está desabilitado.

Solução

O AnyConnect é desinstalado mesmo se a opção **manter instalado estiver selecionada no Adaptive Security Device Manager (ASDM)**. Para resolver este problema, configure o comando **svc keep-installer installed** na diretiva de grupo.

Problema ao preencher o cluster FQDN

Problema: O AnyConnect Client será previamente preenchido com o nome do host em vez do Fully Qualified Domain Name (FQDN) do cluster.

Quando você tiver um cluster de balanceamento de carga configurado para VPN SSL e o cliente tentar se conectar ao cluster, a solicitação será redirecionada para o nó do ASA e o cliente conseguirá fazer logon. Depois de algum tempo, quando o cliente tentar se conectar novamente ao cluster, o cluster FQDN não será visto nas entradas de **Conectar-se a**. Em vez disso, é vista a entrada do ASA do nó ao qual o cliente foi redirecionado.

Solução

Isso ocorre porque o AnyConnect Client mantém o nome do host ao qual se conectou por último. Esse comportamento foi observado e um bug foi arquivado. Para obter detalhes completos sobre o bug, consulte a ID da Cisco [CSCsz39019](#). A solução sugerida é atualizar o Cisco AnyConnect para a versão 2.5.

Configuração de lista do servidor de backup

Uma lista de servidor de backup é configurada caso o servidor principal selecionado pelo usuário não seja alcançável. Isso é definido no painel **Servidor de backup no perfil AnyConnect**. Conclua estes passos:

1. Faça download do [Editor de perfil do AnyConnect \(somente clientes registrados\)](#). O nome do arquivo é **AnyConnectProfileEditor2_4_1.jar**.

2. Crie um arquivo XML usando o Editor de perfil do AnyConnect.

Acesse a guia de lista de servidores.

Clique em **Add**.

Digite o servidor principal no campo **Nome de host**.

Inclua o servidor de backup abaixo da lista de servidor de backup no campo **Endereço de host**. Em seguida, clique em **Adicionar**.

3. Quando tiver o arquivo XML, você precisará atribuí-lo para a conexão usada no ASA.

No ASDM, escolha **Configuração > VP de acesso remoto > Acesso de rede (cliente) > Perfis de conexão do AnyConnect**.

Selecione o perfil e clique em **Editar**.

Clique em **Gerenciar na seção de Política de grupo padrão**.

Selecione a diretiva de grupo e clique em **Editar**.

Selecione **Avançado e, em seguida, clique em SSL VPN cliente**.

Clique em **New**. Depois, você precisa inserir um nome para o perfil e atribuir o arquivo XML.

4. Conecte o cliente à sessão para baixar o arquivo XML.

AnyConnect: Problema de Banco de Dados de Drivers Corrompido

Esta entrada no arquivo SetupAPI.log sugere que o sistema de catálogo está corrompido:

W239 driver signing class list " C:\WINDOWS\INF\certclas.inf" was missing or invalid. Error 0xfffffde5: Erro desconhecido., supondo que todas as classes de dispositivos estão sujeitas à política de assinatura de driver.

Você também poderá receber esta mensagem de erro: Erro(3/17): Não é possível iniciar a VA, a configuração compartilhou a fila ou desistiu da fila compartilhada .

Você pode receber este log no cliente: "o driver do VPN Client encontrou um erro".

Reparo

Esse problema é devido à ID de bug da Cisco [CSCsm54689](#). Para resolver este problema, certifique-se de que o roteamento e o Remote Access Service estejam desabilitados antes de iniciar o AnyConnect. Se isso não resolver o problema, conclua estes passos:

1. Abra um prompt de comando como um administrador no PC (prompt elevado no Vista).
2. Execute net stop CryptSvc.
3. Executar:

```
esentutl /p%systemroot%\System32\catroot2\
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. Quando solicitado, escolha **OK para tentar o reparo**.
5. Saia do prompt de comando.
6. Reinicialização.

Falha no reparo

Se o reparo falhar, conclua estes passos:

1. Abra um prompt de comando como um administrador no PC (prompt elevado no Vista).
2. Execute net stop CryptSvc.
3. Renomeie o diretório %WINDIR%\system32\catroot2 to catroot2_old.
4. Saia do prompt de comando.
5. Reinicialização.

Analise o Banco de Dados

Você pode analisar o banco de dados a qualquer momento para determinar se ele é válido.

1. Abra um prompt de comando como um administrador no PC.

2. Executar:

```
esentutl /g%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

Consulte [Integridade do Banco de Dados de Catálogo do Sistema para obter mais informações.](#)

Mensagens de erro

Erro: Unable to Update the Session Management Database

Enquanto a VPN SSL está conectada via navegador da Web, a mensagem de erro Unable to Update the Session Management Database. **é exibida e o log do ASA mostra %ASA-3-211001: Memory allocation Error. O dispositivo de segurança adaptativa falhou ao alocar memória do sistema RAM.**

Solução 1

Esse problema é devido à ID de bug da Cisco [CSCsm51093](#). Para resolver este problema, reinicie o ASA ou faça o upgrade do software do ASA para a versão temporária mencionada no bug. Consulte o bug da Cisco ID [CSCsm51093](#) para obter mais informações.

Solução 2

Este problema também pode ser resolvido se você desabilitar a detecção de ameaças no ASA se a detecção de ameaças for utilizada.

Erro: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register"

Quando você usa o AnyConnect client em notebooks ou computadores, ocorre um erro durante a instalação:

```
"Module C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed  
to register..."
```

Quando esse erro é encontrado, o instalador não pode seguir adiante e o cliente é removido.

Solução

Estas são as soluções possíveis para resolver esse erro:

- O mais recente AnyConnect Client já não é oficialmente compatível com o Microsoft Windows 2000. É um problema de registro com o computador 2000.

- Remova os aplicativos VMware. Uma vez que o AnyConnect é instalado, os aplicativos VMware podem ser adicionados de volta ao PC.
- Adicione o ASA a sites confiáveis.
- Copie esses arquivos da pasta `\ProgramFiles\Cisco\CiscoAnyconnect` para uma nova pasta e execute o prompt de comando `regsvr32 vpnapi.dll`:

`vpnapi.dllvpncommon.dllvpncommoncrypt.dll`

- Crie uma nova imagem do sistema operacional no laptop/PC.

A mensagem de log relacionada para este erro no AnyConnect Client é semelhante a esta:

```
DEBUG: Error 2911: Could not remove the folderC:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
DEBUG: Error 2911: Could not remove the folder C:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
Info 1721. There is a problem with this Windows Installer package. A program required for
this install to complete could not be run. Contact your support personnel or package
vendor. Action: InstallHelper.exe, location: C:\Program Files\Cisco\Cisco AnyConnect VPN
Client\InstallHelper.exe, command: -acl "C:\Documents and Settings\All Users\Application
Data\Cisco\Cisco AnyConnect VPN Client\\" -r
```

Erro: "Um erro foi recebido do gateway seguro em resposta à solicitação de negociação de VPN. Entre em contato com o administrador da rede"

Quando os clientes tentam se conectar à VPN usando o Cisco AnyConnect VPN Client, esse erro é recebido.

Essa mensagem foi recebida do gateway seguro:

"Classe de endereço ilegal" ou "Host ou rede é 0" ou "Outro erro"

Solução

O problema ocorre devido à depleção do pool de IP local do ASA. Como o recurso de pool de VPN está esgotado, a faixa de pool de IP deve ser ampliada.

A ID do bug da Cisco [CSCsl82188 é arquivado para esta questão](#). Esse erro geralmente ocorre quando o pool local para atribuição de endereço está esgotado, ou se uma máscara de sub-rede de 32 bits for usada para o pool de endereços. A solução é expandir o pool de endereços e usar uma máscara de sub-rede de 24 bits para o pool.

Erro: Não foi possível estabelecer a sessão. O limite de 2 sessões foi atingido.

Ao tentar conectar mais de dois clientes com o AnyConnect VPN Client, você recebe a mensagem de erro `Falha de login no Cliente` e uma mensagem de aviso nos logs do ASA que afirma que `Não foi possível estabelecer a sessão. O limite de 2 sessões foi atingido. Eu tenho a licença AnyConnect Essential no ASA, que executa a versão 8.0.4.`

Solução 1

Esse erro ocorre porque a licença do **AnyConnect Essential não é compatível com o ASA versão 8.0.4**. Você precisa atualizar o ASA para a versão 8.2.2 para corrigir o erro.

Note: Independentemente da licença usada, se o limite de sessão for atingido, o usuário receberá a mensagem de erro `falha de login`.

Solução 2

Esse erro também pode ocorrer se o comando `vpn-sessiondb max-anyconnect-premium-or-essentials-limit session-limit` for usado para definir o limite de sessões VPN permitidas. Se o limite de sessão for definido como dois, o usuário não pode estabelecer mais de duas sessões mesmo que a licença instalada permita mais sessões. Defina o limite de sessões para o número de sessões de VPN necessários para evitar esta mensagem de erro.

Erro: O AnyConnect não está habilitado no servidor VPN ao tentar conectar o anyconnect ao ASA

Você recebe a mensagem de erro `Anyconnect não habilitado no servidor VPN` quando tenta conectar o AnyConnect ao ASA.

Solução

Esse erro é resolvido se você habilitar o AnyConnect na interface externa do ASA com ASDM. Para obter mais informações sobre como habilitar o AnyConnect na interface externa, consulte [Configurar VPN SSL Sem Clientes \(WebVPN\) no ASA](#).

Erro:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x que transmitem o pacotes maiores 1220 (ponto inicial 1206)

O `%ASA-6-722036`: A mensagem de erro `Grupo < client-group > Usuário < xxxx > IP < x.x.x.x >` transmitindo pacote grande 1220 (limite de 1206) aparece nos logs do ASA. O que significa esse log e como ele é resolvido?

Solução

Esta mensagem de registro indica que um pacote grande foi enviado ao cliente. A fonte do pacote não está ciente do cliente MTU. Isto pode igualmente ser devido à compressão de dados não-compressíveis. A solução é desativar a compactação de SVC usando o [comando `svc compression none`](#) para resolver o problema.

Erro: O gateway seguro rejeitou a solicitação de conexão ou reconexão à vpn do

agente.

Quando você se conecta ao AnyConnect Client, este erro é recebido: "o gateway seguro rejeitou a solicitação de conexão ou reconexão à vpn do agente. Uma nova conexão exige reautenticação e deve ser iniciada manualmente. Se o problema persistir, entre em contato com o administrador da rede. A seguinte mensagem foi recebida do gateway seguro: nenhum endereço atribuído".

Esse erro também é recebido quando você se conecta ao AnyConnect Client: "o gateway seguro rejeitou a tentativa de conexão. É necessário fazer uma nova tentativa de conexão para o mesmo ou outro gateway seguro, que exige reautenticação. A seguinte mensagem foi recebida do gateway seguro: Host ou rede é 0".

Esse erro também é recebido quando você se conecta ao AnyConnect Client: "o gateway seguro rejeitou a solicitação de conexão ou reconexão à vpn do agente. Uma nova conexão exige reautenticação e deve ser iniciada manualmente. Se o problema persistir, entre em contato com o administrador da rede. A seguinte mensagem foi recebida do gateway seguro: Nenhuma licença".

Solução

O roteador estava sem a configuração do pool depois de recarregar. Você precisa adicionar a configuração em questão de volta ao roteador.

```
Router#show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254  
svc address-pool SSLPOO
```

"O gateway seguro rejeitou a solicitação de conexão ou reconexão à vpn do agente. Uma nova conexão exige reautenticação e deve ser iniciada manualmente. Se o problema persistir, entre em contato com o administrador da rede. A seguinte mensagem foi recebida do gateway seguro: O erro Nenhuma licença" ocorre quando a licença AnyConnect Mobility está ausente. Uma vez que a licença é instalada, o problema é resolvido.

Erro: "Não foi possível atualizar o banco de dados de gerenciamento de sessão"

Quando você tenta autenticar no WebPortal, esta mensagem de erro é recebida: "Não foi possível atualizar o banco de dados de gerenciamento de sessão".

Solução

Este problema está relacionado à alocação de memória no ASA. Esse problema é encontrado principalmente quando a versão do ASA é 8.2.1. Inicialmente, isso exige 512MB de RAM para atingir a funcionalidade completa.

Como uma solução permanente, atualize a memória para 512 MB.

Como solução temporária, tente liberar memória seguindo estas etapas:

1. Desative a detecção de ameaças.
2. Desative a compressão de SVC.
3. Recarregue o ASA.

Erro: "O driver de cliente VPN encontrou um erro"

Esta é uma mensagem de erro que aparece na máquina cliente quando você tenta se conectar a AnyConnect.

Solução

Para resolver esse erro, conclua este procedimento para definir manualmente o agente AnyConnect VPN para Interactive:

1. Clique com o botão direito do mouse em **Meu Computador > Gerenciar > Serviços e Aplicações > Serviços >** e selecione **Cisco AnyConnect VPN Agent**.
2. Clique com o botão direito do mouse em **Propriedades**, em seguida faça logon e selecione **Permitir que o serviço interaja com a área de trabalho**.

Isso define o valor de tipo de registro DWORD para 110 (o padrão é 010) para o HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent.

Note: Se isso for usado, então a preferência será usar a transformação **.MST nesta instância**. Isso ocorre porque se a definição for feita manualmente usando esses métodos, será necessário definir após cada processo de instalação/atualização. Por isso é necessário identificar o aplicativo que causa o problema.

Quando o Routing and Remote Access Service (RRAS) está habilitado no Windows PC, o AnyConnect falha com o o cliente de VPN encontrou um erro. mensagem de erro. Para resolver esse problema, verifique se o roteamento e o RRAS estão desabilitados antes de iniciar o AnyConnect. Consulte a ID de bug da Cisco [CSCsm54689 para obter mais informações](#).

Erro: "Não foi possível processar a resposta de xxx.xxx.xxx.xxx"

Falha ao conectar clientes AnyConnect a um Cisco ASA. O erro na janela do AnyConnect é "Não é possível processar a resposta de xxx.xxx.xxx.xxx".

Solução

Para resolver esse erro, tente estas soluções:

- Remova o WebVPN do ASA e reative-o.<
- Alterar o número da porta para 444 das 443 atuais e reabilitá-la em 443.

Para obter mais informações sobre como habilitar a WebVPN e alterar a porta para WebVPN, consulte esta [Solução](#).

Erro: "Login negado, mecanismo de conexão não autorizado; entre em contato com

o administrador"

Falha ao conectar clientes AnyConnect a um Cisco ASA. O erro na janela do AnyConnect é "Login negado; mecanismo de conexão não autorizado; entre em contato com o administrador".

Solução

Esta mensagem de erro ocorre principalmente devido a problemas de configuração impróprios ou a uma configuração incompleta. Verifique a configuração e certifique-se de que ela segue o exigido para resolver o problema.

<

Erro: "Pacote do Anyconnect indisponível ou corrompido. Entre em contato com o administrador do sistema"

Esse erro ocorre quando você tenta iniciar o software AnyConnect em um cliente Macintosh para se conectar a um ASA.

Solução

Para resolver esse problema, execute estas etapas:

1. Carregar o pacote Macintosh AnyConnect para o flash do ASA.
2. Modifique a configuração da WebVPN para especificar o pacote AnyConnect usado.

```
webvpn
svc image disk0:/anyconnect-macosx-i386-2.3.2016-k9.pkg 2
svc image disk0:/anyconnect-macosx-powerpc-2.3.2016-k9.pkg 3
```

O comando `svc image` é substituído pelo comando `anyconnect image` no ASA versão 8.4(1) e posterior, conforme mostrado aqui:

```
hostname(config)#webvpn

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-win-3.0.0527-k9.pkg 1

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

Erro: "O pacote do AnyConnect no gateway seguro não pode ser localizado"

Esse erro é causado na máquina Linux do usuário quando ele tenta se conectar ao ASA, iniciando o AnyConnect. Aqui está o erro completo:

"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."

Solução

Para resolver essa mensagem de erro, verifique se o sistema operacional (SO) que é usado na máquina do cliente é compatível com o AnyConnect Client.

Se o SO for compatível, verifique se o pacote AnyConnect é especificado na configuração da WebVPN ou não. Consulte a seção [Pacote do Anyconnect indisponível ou corrompido deste documento para obter mais informações.](#)

Erro: "A VPN segura via desktop remoto não é compatível"

Os usuários não conseguem acessar remotamente a área de trabalho. A mensagem de erro **A VPN segura através de desktop remoto não é compatível** aparece.

Solução

Esse problema é devido a estas IDs de bugs da Cisco: [CSCsu22088](#) e [CSCso42825](#). Se você atualizar o AnyConnect VPN Client, ele pode resolver o problema. Consulte esses bugs para obter mais informações.

Erro: "O certificado do servidor recebido ou sua cadeia não está em conformidade com o FIPS. Não será estabelecida uma conexão de VPN"

Quando você tentar conectar-se por VPN ao ASA 5505, aparece a mensagem **o certificado do servidor recebido ou sua cadeia não está em conformidade com o FIPS. Aparece a mensagem Não será estabelecida uma conexão VPN.**

Solução

Para resolver esse erro, você deve desabilitar o Federal Information Processing Standards (FIPS) no arquivo **AnyConnect Local Policy**. Este arquivo normalmente pode ser encontrado em `C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml`. Se este arquivo não for encontrado neste caminho, localize o arquivo em um diretório diferente com um caminho como `C:\Documents and Settings\All Users\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml`. Uma vez que você localizar o arquivo xml, faça alterações nele, como mostrado aqui:

Altere a frase:

```
<FipsMode>true</FipsMode>
```

Para:

```
<FipsMode>>false</FipsMode>
```

E reinicie o computador. Os usuários devem ter permissão administrativa para alterar esse arquivo.

Erro: "Falha na validação do certificado"

Os usuários não conseguem iniciar o AnyConnect e recebem o erro **Falha de validação de certificado**.

Solução

A autenticação de certificado funciona de forma diferente com o AnyConnect se comparado ao cliente IPsec. Para que a autenticação de certificado funcione, você deve importar o certificado de cliente para o navegador e alterar o perfil de conexão para usar a autenticação de certificado. Você também precisará habilitar este comando no ASA para permitir que certificados de cliente SSL sejam usados na interface externa:

```
ssl certificate-authentication interface outside port 443
```

Erro: "O serviço do agente da VPN encontrou um problema e precisa ser fechado. Lamentamos o inconveniente"

Quando o AnyConnect versão 2.4.0202 é instalado em um PC com Windows XP, ele para na atualização de arquivos de localização, e uma mensagem de erro mostra que o **vpnagent.exe** falhou.

Solução

Esse comportamento é registrado na ID de bug da Cisco [CSCsq49102](#). A solução sugerida é desabilitar o cliente Citrix.

Erro: "Este pacote de instalação não pode ser aberto. Verifique se o pacote existe"

Quando o AnyConnect é baixado, esta mensagem de erro é recebida:

"Entre em contato com o administrador do sistema. O instalador apresentou o seguinte erro: Este pacote de instalação não pode ser aberto. Verifique se o pacote existe e se você pode acessá-lo, ou entre em contato com o fornecedor do aplicativo para verificar se este é um pacote válido do Windows Installer."

Solução

Conclua estes passos para corrigir o problema:

1. Remova qualquer software antivírus.
2. Desative o firewall do Windows.
3. Se nem o passo 1 nem o 2 ajudar, formate a máquina e instale.
4. Se o problema persistir, abra um [chamado no TAC](#).

Erro: "Erro ao aplicar transformações. Verifique se os caminhos de transformação especificados são válidos."

Essa mensagem de erro é recebida durante o download automático do AnyConnect do ASA:

"Contact your system administrator. The installer failed with the following error:
Error applying transforms. Verify that the specified transform paths are valid."

Esta é a mensagem de erro recebida ao conectar-se com o AnyConnect para MacOS:

"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."

Solução

Use uma destas soluções para resolver esse problema:

1. A causa raiz desse erro pode ser devido a um arquivo de conversão de MST corrompido (por exemplo, importado). Siga estas etapas para corrigir esse problema:

Remova a tabela de conversão de MST.

Configure a imagem do AnyConnect para MacOS no ASA.

2. No ASDM, siga o caminho **Acesso de rede (cliente) > AnyConnect Custom > Instala e exclua o arquivo do pacote do AnyConnect**. Verifique se o pacote permanece em **Acesso à rede (cliente) > Avançado > VPN SSL > Configuração do cliente**.

Se nenhuma dessas soluções resolver o problema, entre em contato com o [Suporte técnico da Cisco](#).

Erro: "O driver de cliente VPN encontrou um erro"

Esse erro é recebido:

The VPN client driver has encountered an error when connecting through Cisco AnyConnect Client.

Solução

Esse problema pode ser resolvido quando você desinstalar o AnyConnect Client e remover o software antivírus. Depois disso, reinstale o AnyConnect Client. Se essa resolução não funcionar, reformate o PC para corrigir esse problema.

Erro: "Uma reconexão de VPN resultou na definição de configuração diferente. A configuração de rede VPN está sendo reinicializada. Aplicações que utilizam a rede privada podem precisar ser restauradas."

Este erro é recebido quando você tenta iniciar o AnyConnect:

"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."

Solução

Para resolver esse erro:

```
group-policy <Name> attributes
webvpn
svc mtu 1200
```

O comando **svc mtu** é substituído pelo comando **anyconnect mtu** no ASA versão 8.4(1) e posterior, conforme mostrado aqui:

```
hostname(config)#group-policy
```

```
hostname(config-group-policy)#webvpn
```

```
hostname(config-group-webvpn)#anyconnect mtu 500
```

Erro do AnyConnect ao fazer login

Problema

O AnyConnect recebe este erro quando se conecta ao cliente:

```
The VPN connection is not allowed via a local proxy. This can be changed
through AnyConnect profile settings.
```

Solução

O problema pode ser resolvido se você fizer essas alterações no perfil do AnyConnect:

Adicione esta linha ao perfil do AnyConnect:

```
<ProxySettings>IgnoreProxy</ProxySettings><
AllowLocalProxyConnections>
false</AllowLocalProxyConnections>
```

A configuração de proxy do IE não é restaurada após a desconexão do AnyConnect no Windows 7

Problema

No Windows 7, se a configuração do proxy do IE estiver configurada para **Detectar automaticamente as configurações**, e o AnyConnect aplicar uma nova configuração de proxy, a configuração de proxy do IE não será restaurada de volta para **Detectar configurações automaticamente** depois que o usuário encerra a sessão do AnyConnect. Isso causa problemas de LAN para usuários que precisam de suas configurações de proxy definidas para **Detectar automaticamente as configurações**.

Solução

Esse comportamento é registrado na ID de bug da Cisco [CSCtj51376](#). A solução sugerida é atualizar para [AnyConnect 3.0](#).

Erro: O AnyConnect Essentials não pode ser habilitado até que todas essas sessões sejam encerradas.

Esta mensagem de erro é recebida no Cisco ASDM quando você tenta ativar a licença AnyConnect Essentials:

```
There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.
```

Solução

Esse é o comportamento normal do ASA. O AnyConnect Essentials é um cliente de VPN SSL licenciado separadamente. Ele é totalmente configurado no ASA e oferece os recursos completos do AnyConnect, com as seguintes exceções:

- Nenhum Cisco Secure Desktop (CSD) (incluindo HostScan/Vault/Cache Cleaner)
- Nenhuma VPN SSL clientless
- Suporte móvel opcional para Windows

Essa licença não pode ser usada em paralelo com a licença VPN SSL premium. Quando você precisar usar uma licença, desabilite a outra.

Erro: A guia de Conexão na opção de Internet do Internet Explorer é oculta depois de ficar conectada ao cliente AnyConnect.

A guia conexão na Opção de Internet do Internet Explorer é ocultada depois que você se conecta ao cliente do AnyConnect.

Solução

Isso acontece devido ao recurso msie-proxy lockdown. Se você ativar esse recurso, ele oculta a guia Conexões no Microsoft Internet Explorer durante todo o tempo de uma sessão de VPN do AnyConnect. Se você desativar o recurso, ele deixará a exibição da guia conexões inalterada.

Erro: Alguns usuários estão recebendo mensagem de erro de falha de login enquanto outros são capazes de se conectar através da VPN do AnyConnect

Alguns usuários recebem a mensagem de erro de falha de login enquanto outros podem se conectar com êxito através da VPN do AnyConnect.

Solução

Esse problema pode ser resolvido se você se certificar de que a caixa de seleção **não exigir pré-autenticação** está marcada para os usuários.

Erro: O certificado que você está visualizando não coincide com o nome do site que você está tentando visualizar.

Durante a atualização de perfil do AnyConnect, é mostrado um erro que diz que o certificado é inválido. Isso ocorre somente com o Windows e na fase de atualização de perfil. A mensagem de erro é mostrada aqui:

```
The certificate you are viewing does not match with the name of the site you are trying to view.
```

Solução

Isso pode ser resolvido se você modificar a lista de servidores do perfil AnyConnect para utilizar o FQDN do certificado.

Esta é uma amostra do perfil XML:

```
<ServerList>
```

```
<HostEntry>
```

```
<HostName>vpn1.ccsd.net</HostName>
```

```
</HostEntry>
```

```
</ServerList>
```

Note: Se houver uma entrada para o endereço IP público do servidor, como `<HostAddress>`, remova-a e mantenha apenas o FQDN do servidor (por exemplo, `<HostName>` mas não `<HostAddress>`).

Não foi possível iniciar o AnyConnect do CSD Vault em uma máquina com Windows 7

Quando o AnyConnect é iniciado no vault do CSD, ele não funciona. Isso ocorre em máquinas com Windows 7.

Solução

Atualmente, isso não é possível porque ele não é compatível.

O perfil do AnyConnect não é replicado para o modo de espera após o failover

O software AnyConnect 3.0 VPN Client com ASA versão 8.4.1 funciona bem. No entanto, após o failover, não há nenhuma replicação para a configuração relativa ao perfil do AnyConnect.

Solução

Esse problema foi observado e registrado sob a ID de bug da Cisco [CSCtn71662](#). A solução temporária é copiar manualmente os arquivos para a unidade em espera.

O AnyConnect cliente trava se o Internet Explorer estiver off-line

Quando isso ocorre, o log de eventos do AnyConnect contém entradas semelhantes a estas:

```
Description : Function:
CAdapterNetworkStateIfc::SetConnectedStateToConnected
File: .\AdapterNetworkStateIfc.cpp
Line: 147
Invoked Function: InternetSetOption
Return Code: 12010 (0x00002EEA)
Description: The length is incorrect for the option type
```

```
Description : Function: CTransportWinHttp::InitTransport
File: .\CTransportWinHttp.cpp
Line: 252
Invoked Function: CConnectedStateIfc::SetConnectedStateToConnected
Return Code: -25362420 (0xFE7D000C)
Description: CADAPTERNETWORKSTATEIFC_ERROR_SET_OPTION
```

Solução

Esse comportamento foi observado e registrado sob a ID de bug da Cisco [CSCtx28970](#). Para resolver esse problema, saia do aplicativo AnyConnect e reinicie-o. As entradas de conexão reapareceram após a reinicialização.

Mensagem de Erro: TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

O AnyConnect Client falha ao se conectar e a mensagem de erro **Não é possível estabelecer uma conexão é recebida**. No log de eventos do AnyConnect, o erro **TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER** é encontrado.

Solução

Isso ocorre quando o headend é configurado para encapsulamento dividido com uma lista muito grande de encapsulamento dividido (aproximadamente 180-200 entradas) e um ou mais atributos do cliente são configurados na política de grupo, como servidor de dns.

Para resolver esse problema, siga estas etapas:

1. Reduza o número de entradas na lista de encapsulamento dividido.
2. Use esta configuração para desabilitar o DTLS:

```
group-policy groupName attributes
webvpn
svc dtls none
```

Para obter mais informações, consulte a ID de bug do Cisco [CSCtc41770](#).

Mensagem de Erro: "A tentativa de conexão falhou devido à entrada de host inválido"

A mensagem de erro **A tentativa de conexão falhou devido à entrada de host inválido é recebida**

enquanto o AnyConnect é autenticado com o uso de um certificado.

Solução

Para resolver esse problema, tente qualquer uma das soluções a seguir:

- Atualize o AnyConnect para a versão 3.0.
- Desabilite o Cisco Secure Desktop em seu computador.

Para obter mais informações, consulte a ID de bug do Cisco [CSCti73316](#).

Erro: "Verifique se os certificados do servidor podem passar o modo rigoroso se você configurar a VPN sempre ativa"

Quando você habilita o recurso de sempre ativo no AnyConnect, a mensagem de erro **verifique se os certificados do servidor podem passar o modo rigoroso, se você configurar a VPN sempre ativa é recebida.**

Solução

Essa mensagem de erro significa que se você quiser usar o recurso Sempre ativo, é preciso configurar um certificado válido de servidor no headend. Sem um certificado de servidor válido, esse recurso não funciona. O modo rígido de certificação é uma opção que você define no arquivo de diretiva local do AnyConnect para garantir que as conexões usem um certificado válido. Se você habilitar esta opção no arquivo de diretiva e se conectar a um certificado falso, a conexão falha.

Erro: "Ocorreu um erro interno nos Serviços HTTP do Microsoft Windows"

Essa Diagnostic AnyConnect Reporting Tool (DART) mostra uma tentativa fracassada:

```
*****
Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1170
Invoked Function: HttpSendRequest
Return Code: 12004 (0x00002EE4)
Description: An internal error occurred in the Microsoft
Windows HTTP Services
*****
Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::connect
File: .\ConnectIfc.cpp
Line: 472
Invoked Function: ConnectIfc::sendRequest
Return Code: -30015443 (0xFE36002D)
```

Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 2999
Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN
Connection attempt failed. Please try again.

Além disso, consulte os logs do visualizador de eventos na máquina com Windows.

Solução

Isso pode ser causado devido a uma conexão Winsock corrompida. Redefina a conexão do prompt de comando usando este comando e reinicie sua máquina windows:

netsh winsock reset

Consulte o artigo [Como determinar e recuperar-se da corrupção do Winsock2 no Windows Server 2003, no Windows XP e no Windows Vista da base de conhecimento para obter mais informações.](#)

Erro: "O transporte SSL recebeu uma falha de canal seguro. Pode ser resultado de uma configuração de criptografia não suportada no Secure Gateway."

Essa Diagnostic AnyConnect Reporting Tool (DART) mostra uma tentativa fracassada:

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::handleRequestError
File: .\CTransportWinHttp.cpp
Line: 854
The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway.

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1199
Invoked Function: CTransportWinHttp::handleRequestError
Return Code: -30015418 (0xFE360046)

Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnuui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 3026
Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015418 (0xFE360046)
Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE
Connection attempt failed. Please try again.

Solução

O Windows 8.1 não suporta RC4 de acordo com a seguinte atualização do KB:

<http://support2.microsoft.com/kb/2868725>

Configure cifras DES/3DES para SSL VPN no ASA usando o comando "ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1" OU edite o arquivo de Registro do Windows na máquina cliente como mencionado abaixo:

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

Informações Relacionadas

- [Dispositivos de segurança adaptáveis Cisco ASA 5500 Series](#)
- [Perguntas frequentes sobre AnyConnect VPN Client](#)
- [Perguntas Frequentes do Cisco Secure Desktop \(CSD\)](#)
- [Cisco AnyConnect VPN Client](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)