Conexão VPN do Cisco Secure Client Redefinida pelo Peer com Interferência de Descriptografia SSL/TLS Zscaler

Contents

Problema

Um usuário enfrenta falhas de conexão VPN ao tentar estabelecer uma conexão usando o Cisco Secure Client.

Ambiente

- Tecnologia: Cisco Secure Access - Acesso remoto seguro ao cliente (VPN, postura, recurso privado)
- Linha de produtos: SECACCS
- Sistema operacional: macOS (com base nos caminhos do arquivo de log mostrando /Users/admin/workspace/secure-client-macos_Raccoon_MR15/)
- Software de terceiros: Zscaler instalado no sistema cliente
- Protocolo VPN: CSTP (Cisco SSL Tunnel Protocol)
- Versão TLS: TLS 1.3 com codificação TLS_AES_256_GCM_SHA384

Resolução

A resolução envolve a identificação e a resolução do conflito entre o Cisco Secure Client e a funcionalidade de descriptografia SSL/TLS da Zscaler.

Passo 1: Análise e diagnóstico de registros

Capture e analise os registros do Cisco Secure Client DART para identificar o padrão de falha de conexão. Os registros mostrarão o estabelecimento bem-sucedido de uma sessão TLS, seguido por uma reinicialização imediata da conexão.

Principais indicadores de diagnóstico nos registros:

- Estabelecimento de conexão TLS 1.3 com codificação TLS_AES_256_GCM_SHA384
- O cálculo de MTU e a negociação de HTTP continuam normalmente
- Conexão redefinida por erro de mesmo nível (Código de retorno: 54) durante a operação de leitura do soquete

A sessão TLS 1.3 é estabelecida com êxito usando a codificação TLS_AES_256_GCM_SHA384, mas imediatamente após o estabelecimento da sessão, um pacote de redefinição é enviado, o que encerra a conexão, resultando no encerramento do túnel VPN. O erro específico observado nos logs mostra "Connection reset by peer" (Conexão redefinida pelo peer) com código de retorno 54 (0x00000036) durante a operação de leitura do soquete.

A seguinte sequência de erros ocorre durante tentativas de conexão:

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

Passo 2: Identificação de software de terceiros

Investigue a presença de software de segurança de terceiros que possa estar executando inspeção ou descriptografia SSL/TLS no sistema cliente. Nesse caso, Zscaler foi identificado como o aplicativo que interfere.

Passo 3: Resolução de conflitos de descriptografia SSL/TLS

Resolva o conflito entre o tráfego do Cisco Secure Client VPN e a funcionalidade de descriptografia SSL/TLS do Zscaler. O tráfego VPN parece estar passando por descriptografia SSL/TLS por Zscaler, o que interfere no estabelecimento do túnel VPN e causa a redefinição da

conexão.

As possíveis abordagens de resolução incluem:

- Configurar o Zscaler para excluir o tráfego de VPN do Cisco Secure Client da inspeção de SSL/TLS
- Crie regras de desvio em Zscaler para os pontos de extremidade do servidor VPN
- Desabilite temporariamente o Zscaler durante o teste de conexão VPN para confirmar o conflito
- Coordenar-se com a equipe de segurança de rede para estabelecer exclusões apropriadas

Causa

A causa raiz desse problema é um conflito entre o tráfego do Cisco Secure Client VPN e a funcionalidade de descriptografia SSL/TLS da Zscaler. Quando o Zscaler tenta descriptografar ou inspecionar o tráfego TLS da VPN, ele interfere no processo de estabelecimento de túnel seguro. Essa interferência se manifesta como uma redefinição de conexão imediatamente após o estabelecimento da sessão TLS, impedindo que o túnel VPN conclua sua fase de negociação. A temporização do pacote de reinicialização (que ocorre logo após o estabelecimento bem-sucedido do TLS, mas antes da conclusão do túnel) é característica da interferência de inspeção SSL/TLS dos dispositivos de segurança ou software.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.