

O Secure Client Umbrella Module torna-se inativo devido à tempestade de DNS do Codex Application

Contents

Problema

Vários usuários no macOS experimentam o módulo de roaming do Cisco Secure Client Umbrella em transição intermitente para um estado inativo (fail-open). Durante esses períodos, as solicitações de DNS, incluindo os comandos nslookup iniciados pelo terminal, não conseguem acessar a camada de rede, afetando a capacidade dos usuários de resolver domínios e acessar recursos baseados na Internet.

O problema se manifesta com repetidas falhas de teste nos logs do Umbrella, mostrando mensagens como:

```
Transparent probe failed  
Encrypted probe failed  
Switching to basic probe  
DNS probe failed by timeout - going open
```

A análise revelou que o driver de estoque trava durante a mesma janela de falha quando o Umbrella se torna inativo. O problema é observado com mais frequência enquanto os usuários estão usando ativamente os aplicativos Codex e AI Assistant, com um alto volume de tentativas de conexão para chatgpt.com imediatamente após os comandos enviados ao CODEX.

Ambiente

- Cisco Secure Client versões 5.1.13, 5.1.16, 5.1.17
- macOS (várias versões observadas)

- Módulo Umbrella Roaming habilitado
- Módulo ZTNA/Secure Internet Access (SIA) habilitado
- Aplicativo do Codex em uso
- Usuários que trabalham em várias redes (residenciais, escritórios, diferentes ISPs)

Resolução

O problema foi resolvido com a implementação de configurações de desvio de domínio para evitar a duplicação de solicitações de DNS. As abordagens descritas nas próximas seções foram validadas.

Resolução primária: Ignorar Domínio

- Passo 1: Adicione chatgpt.com à lista de desvio na configuração do Cisco Secure Access. Isso evita que o Secure Client duplique as solicitações de DNS geradas pelo aplicativo Codex, eliminando a tempestade de DNS que causa instabilidade no driver.
- Passo 2: Verifique a configuração de desvio. Teste a funcionalidade do Codex para confirmar se o problema não se reproduz mais com o bypass no lugar.

Resolução alternativa: Solução de configuração do Codex

Aplice as alterações de configuração do Codex referenciadas no problema do GitHub para reduzir o volume de solicitações de DNS geradas pelo aplicativo.

<https://github.com/openai/codex/issues/21218>

Etapas Avançadas de Solução de Problemas Usadas

Essas etapas de diagnóstico foram executadas para identificar a causa raiz.

1.- Habilitar registro de estoque detalhado:

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -sdf 0x830801F2
```

2.- Reproduza o problema e colete o pacote DART imediatamente após a falha.

3.- Desativar registro extenso:

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -cdf
```

4.- Ative o registro de depuração máximo para o SWG. Criar arquivo SWGConfigOverride.json com conteúdo:

```
{"logLevel": "1"}
```

Salve em /opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json.

5.- Habilite os logs de rastreamento do RSM para DNS. Criar arquivo force_log_level.plist com conteúdo:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>logLevel</key>
<string>trace</string>
</dict>
</plist>
```

Salve em /opt/cisco/secureclient/umbrella/data.

Causa

A questão central está relacionada ao comportamento do aplicativo Codex, que gera um volume

muito alto de solicitações de DNS. Quando chatgpt.com não é ignorado, essas solicitações são efetivamente duplicadas pelo Cisco Secure Client, criando uma tempestade de DNS que leva ao alto uso da CPU e instabilidade do driver do kernel de estoque.

O problema ocorre porque:

- O Codex gera várias consultas DNS para chatgpt.com durante a operação.
- Sem ignorar a configuração, o Secure Client intercepta e duplica essas solicitações.
- O alto volume de solicitações de DNS duplicadas faz com que o driver de armazenamento falhe.
- A instabilidade do driver resulta em falhas de sonda Umbrella e transição para o estado fail-open.

Quando chatgpt.com é ignorado ou a solução alternativa do Codex é aplicada, essa duplicação não ocorre e o problema não se reproduz mais. O problema afeta as configurações SIA Umbrella e ZTNA, indicando que o problema está dentro do mecanismo de tratamento de tráfego em vez de em um módulo específico.

Conteúdo relacionado

- [Solucionar problemas do módulo de roaming de acesso seguro](#)
- [Solucionar problemas e coletar informações básicas](#)
- [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.

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.