# O acesso à Internet falha quando o Secure Client Umbrella SWG Agent Service está ativo

## Contents

## Problema

Quando o serviço Cisco Secure Client - Umbrella SWG Agent está sendo executado em um notebook Dell com Windows, os usuários não conseguem acessar nenhum site. Quando o serviço Umbrella SWG Agent é interrompido, o acesso normal à Web é restaurado. O problema ocorre com o Cisco Secure Client versão 5.1.14.145, que inclui os módulos AnyConnect VPN e Umbrella. O arquivo OrgInfo.json está presente no diretório esperado e o certificado da CA raiz do Cisco Secure Access está instalado no armazenamento de certificado raiz confiável.

## Ambiente

- Produto: Cisco Secure Client (módulos AnyConnect VPN e Umbrella)
- Versão de software: 5.1.14.145
- Sistema operacional: Windows (notebook Dell)
- Serviço Umbrella SWG Agent ativado/desativado
- OrgInfo.json presente em `%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`
- CA raiz de acesso seguro da Cisco instalada no armazenamento de autoridades de certificação raiz confiáveis
- Segurança DNS/Web habilitada no painel de controle de Acesso Seguro
- Perfil de segurança atribuído com descriptografia ativada

## Resolução

O problema foi resolvido com a identificação e a correção de uma falha de sincronização de NTP (Network Time Protocol) no dispositivo cliente. A incapacidade de sincronizar o tempo impediu a comunicação segura exigida pelo Agente Umbrella SWG para proxy do tráfego da Web, resultando em pacotes de redefinição de TCP (RST) e perda de acesso à Web. Depois que a sincronização de NTP foi restaurada, o acesso à Web funcionou normalmente com o Agente SWG ativo.

Siga este fluxo de trabalho abrangente de solução de problemas.

### Etapa 1: Verificar a configuração e os pré-requisitos

- Verifique se `OrgInfo.json` está localizado em `%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`.

- Confirme se a CA raiz de acesso seguro da Cisco está presente no armazenamento de autoridades de certificação raiz confiáveis.
- Verifique se a Segurança DNS/Web está habilitada no painel de controle do Secure Access.
- Verifique se o Perfil de segurança atribuído tem a Descriptografia ativada.

### Etapa 2: Capturar e analisar o tráfego de rede

Obtenha uma captura de pacotes do tráfego do cliente direcionado ao proxy SWG para identificar comportamentos anormais, como pacotes inesperados de redefinição de TCP.

Descrição da captura de pacotes mostrando o problema:

```
The packet capture revealed that TCP reset (RST) packets were being sent to the client, disrupting the
```

### Etapa 4: Validar as regras de firewall do perímetro

- Inspecione as regras de firewall de perímetro para garantir que o tráfego de e para servidores SWG seja permitido na interface de entrada.

### Etapa 5: Execute o diagnóstico do sistema e do protocolo

Execute este comando no cliente para verificar se há erros de sincronização de NTP:

```
curl ipinfo.io
```

Descrição do resultado de diagnóstico:

```
The output indicated NTP timing was out of sync on the client device.
```

## Causa

A causa raiz foi uma falha na sincronização NTP (Network Time Protocol) no dispositivo cliente. Esse problema de temporização impediu a comunicação segura entre o cliente e o serviço proxy Umbrella SWG, resultando em pacotes de redefinição de TCP e perda de acesso à Web quando o serviço SWG Agent estava ativo. Resolver o problema de sincronização de NTP restaurou a operação adequada do agente Umbrella SWG, permitindo que o tráfego da Web seja encaminhado por proxy com segurança.

## 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.