Solucionar problemas do Secure Access Roaming Module "Cloud Service Unavailable" ou "Unprotected" Status

Contents

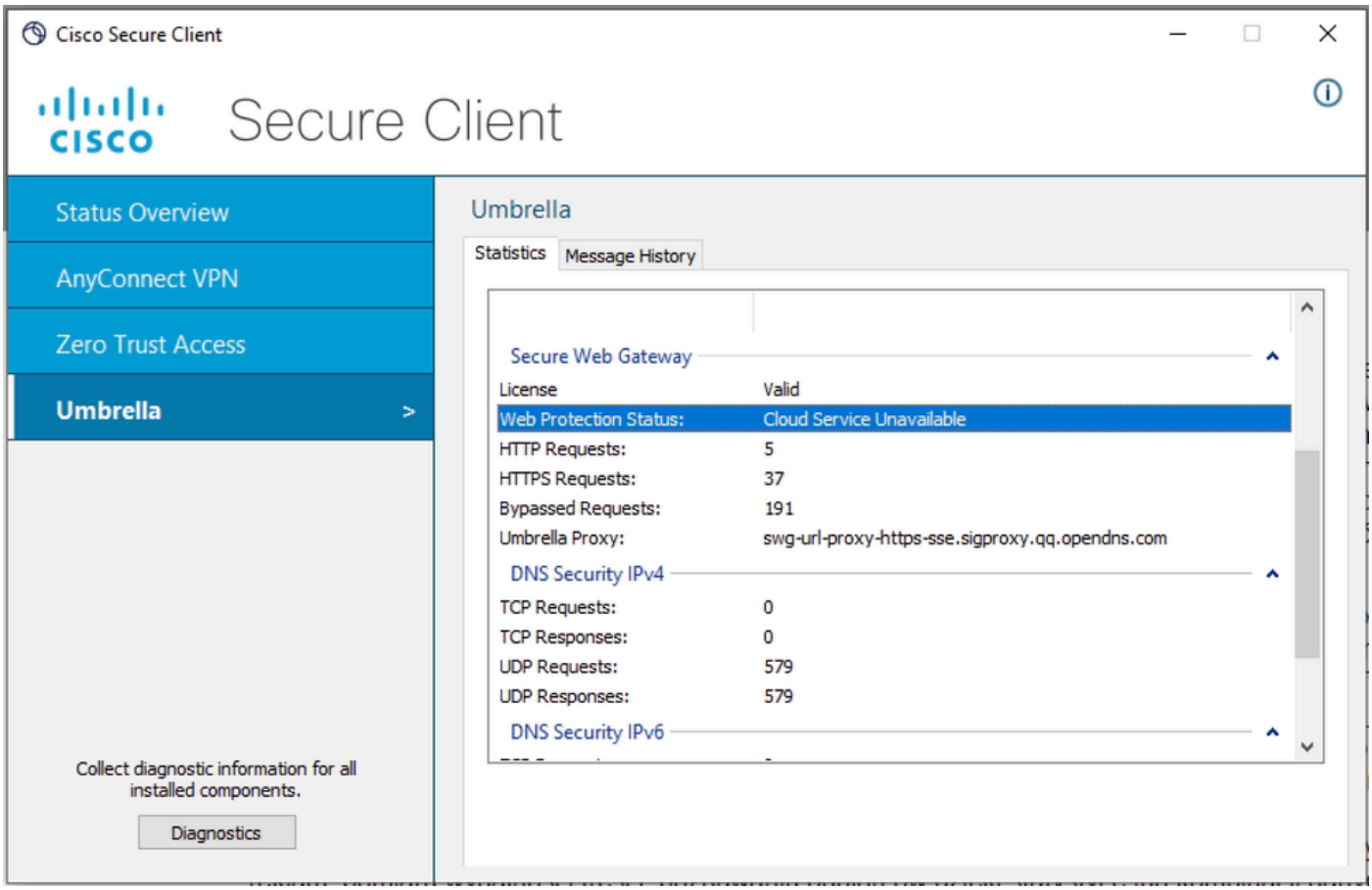
Introdução

Este documento descreve uma forma de investigar a causa raiz do status "Serviço em nuvem indisponível" ou "Desprotegido" no Módulo de roaming do cliente seguro.

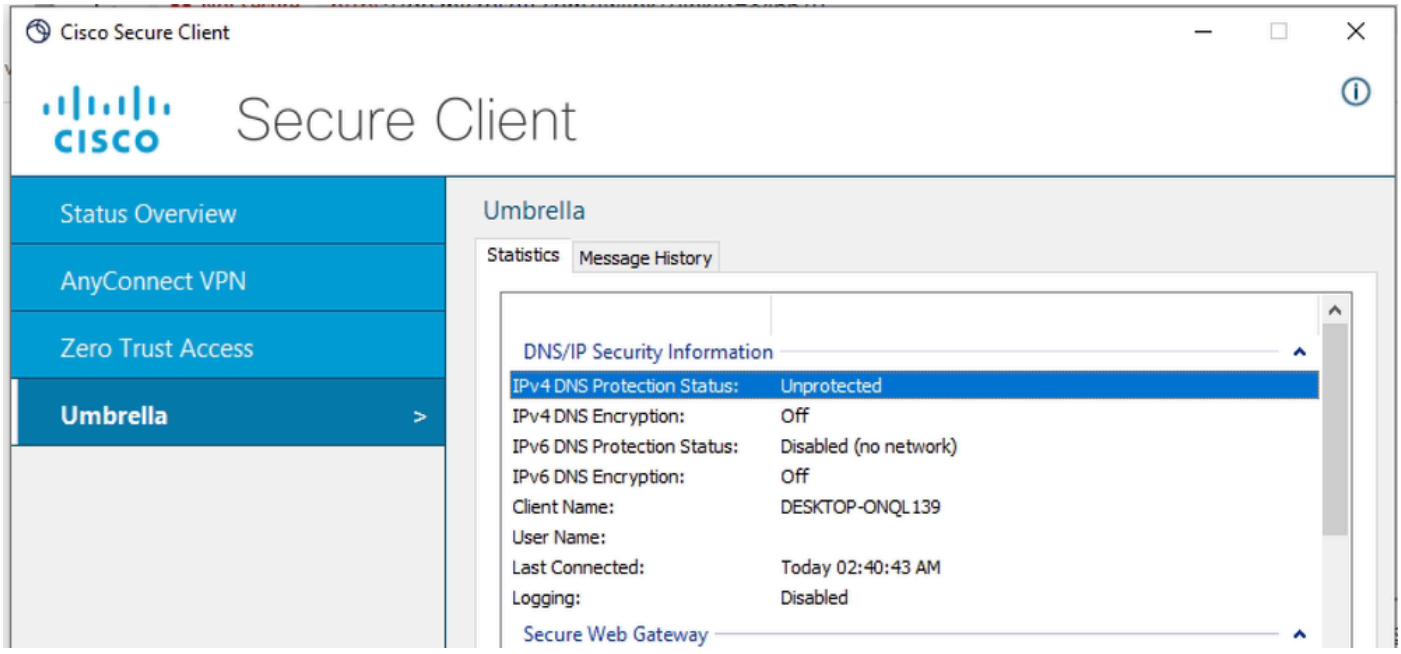
Problema

Quando um usuário inicia o módulo de roaming do cliente seguro e espera usar a proteção DNS e/ou Web, os estados errados podem ser vistos na interface de usuário do cliente seguro:

Serviço em nuvem indisponível para status de proteção da Web



Desprotegido para Status de Proteção DNS



A razão por trás desses erros é que o módulo de roaming não pode entrar em contato com seus serviços de nuvem devido a problemas de conectividade de rede.

Se esse problema não foi visto no PC cliente afetado no passado, isso significa que muito provavelmente a rede à qual o PC está conectado é restrita e não atende aos requisitos descritos na Documentação do SSE

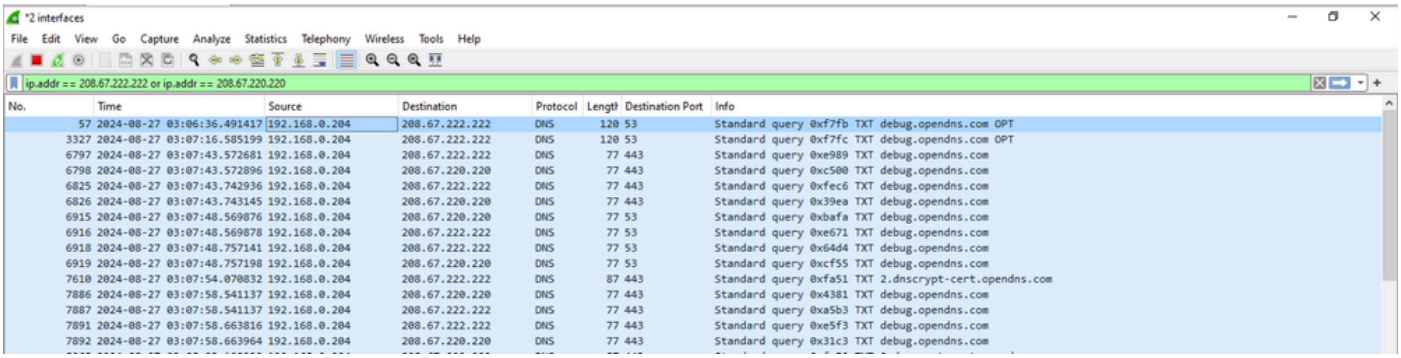
O status de proteção DNS está desprotegido

Quando você vir o estado DNS desprotegido, provavelmente o módulo de roaming não terá conectividade upstream com servidores OpenDNS (208.67.222.222 e 208.67.220.220).
Você veria o arquivo de log no arquivo cscumbrellaplugin.txt, que faz parte do pacote DART.

```
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:43 [8880] [DEBUG] < 13> Dns Protection IPv6 State Machine: rejected all candidate reso
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:53 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: rejected all candidate reso
```

Para verificar e confirmar novamente os problemas de conectividade, você pode coletar a captura do Wireshark na interface física de saída do PC (WiFi ou Ethernet) e usar o filtro de exibição para procurar apenas o tráfego destinado aos resolvedores do OpenDNS:

```
ip.addr == 208.67.222.222 or ip.addr == 208.67.220.220
```



Como você vê no snippet do Wireshark, é claro que o cliente continua retransmitindo consultas TXT DNS destinadas a 208.67.222.222 e 208.67.220.220 nas portas UDP 443 e 53, mas não recebe nenhuma resposta.

Pode haver vários motivos por trás de tal comportamento, muito provavelmente o dispositivo de firewall de perímetro está bloqueando o tráfego de DNS de saída para servidores OpenDNS ou permitindo apenas o tráfego para servidores DNS específicos.

O status da proteção da Web é Serviço em nuvem indisponível

Quando você vir o estado de proteção da Web Serviço Indisponível, provavelmente o Módulo de roaming não terá conectividade upstream com os servidores do Gateway da Web Seguro.

Se o PC não tiver conectividade IP com servidores SWG, você verá o arquivo de log no

Umbrella.txt, que faz parte do pacote DART.

```
Date : 08/27/2024
Time : 06:41:22
Type : Warning
Source : csc_swgagent

Description : WARN | Thread 27cc | TCP handshake to SWG Proxy URL was not successful. Since fail open p
```

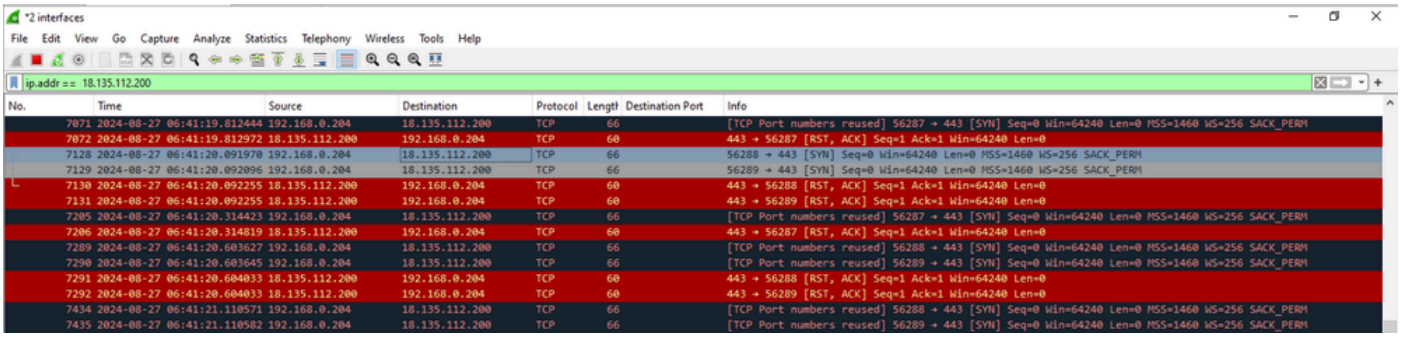
Para investigar mais, colete a captura de pacotes para provar que o PC não tem conectividade com o servidor SWG.
Emita o comando no terminal para obter o endereço IP do SWG:

<#root>

```
C:\Users\admin>

nslookup swg-url-proxy-https-sse.sigproxy.qq.opendns.com


Server: ad.lab.local
Address: 192.168.0.65

Non-authoritative answer:
Name: k8s-sigproxy-sigproxy-c8f482b42a-ddf1929ae349b3e5.elb.eu-west-2.amazonaws.com
Address:

18.135.112.200


Aliases: swg-url-proxy-https-sse.sigproxy.qq.opendns.com
swg-proxy_eu-west-2_1_1n.sigproxy.aws.umbrella.com
```

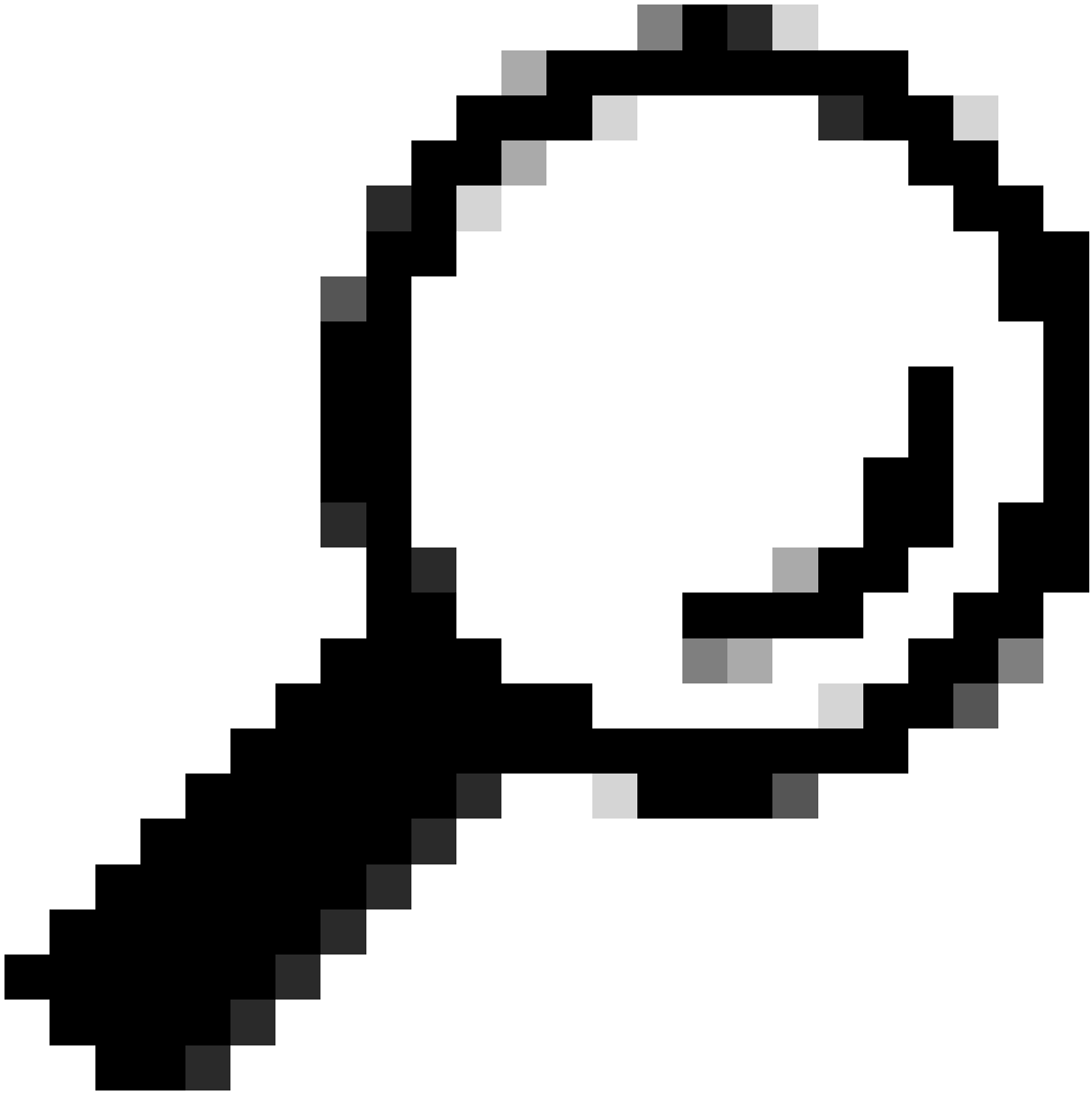
Para verificar e confirmar novamente os problemas de conectividade, você pode coletar a captura do Wireshark na interface física de saída do PC (WiFi ou Ethernet) e usar o filtro de exibição para procurar apenas o tráfego destinado ao servidor SWG (use o endereço IP obtido na etapa anterior)

```
ip.addr == 18.135.112.200
```



Como você vê no snippet do Wireshark, é claro que o cliente continua retransmitindo pacotes TCP SYN destinados a 18.135.112.200, mas recebe TCP RST como resposta.

Neste cenário de laboratório específico, o firewall de perímetro estava bloqueando o tráfego para o endereço IP do SWG.
No cenário real, você pode ver apenas retransmissões TCP SYN, não TCP RST.



Dica: se o cliente não puder acessar os servidores SWG, ele, por padrão, entrará no estado fail open, onde o tráfego da Web está saindo através do Direct Internet Access (WiFi ou Ethernet). A proteção da Web não é aplicada no modo de falha/abertura.

Solução

Para identificar rapidamente se a rede subjacente está causando problemas, o usuário pode se conectar a qualquer outra rede aberta (hotstop, WiFi residencial) que não tenha nenhum firewall de perímetro.

Para corrigir o erro de conexão descrito, certifique-se de que o PC tenha conectividade upstream irrestrita, conforme descrito na Documentação do SSE.

Problemas de Status de Proteção DNS:

- 208.67.222.222 porta TCP/UDP 53
- 208.67.220.220 Porta TCP/UDP 53

Para problemas de Status de proteção da Web, certifique-se de que o tráfego para Endereços IP de entrada seja permitido no firewall de perímetro - Documentação SSE

O intervalo específico de endereços IP de entrada depende da sua localização.

Informações Relacionadas

- Guia do usuário do Secure Access
- Como coletar o pacote DART do Cisco Secure Client
- Suporte Técnico e Documentação - Cisco Systems

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.