Solucionar problemas de módulo de roaming de acceso seguro "servicio en la nube no disponible" o "no protegido" estado

Contenido

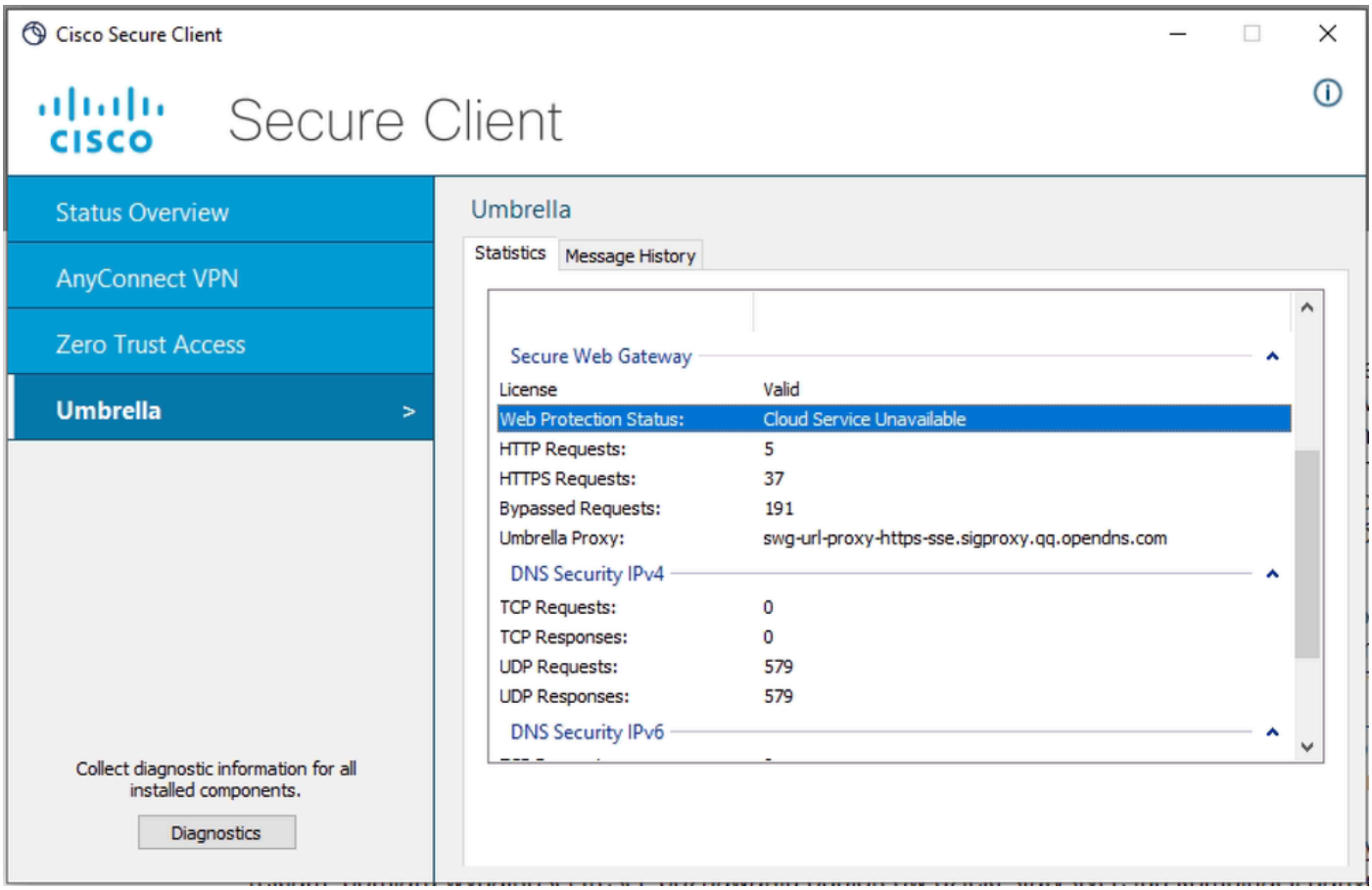
Introducción

Este documento describe una manera de investigar la causa raíz del estado "Servicio en la nube no disponible" o "Desprotegido" en el módulo de roaming de Secure Client.

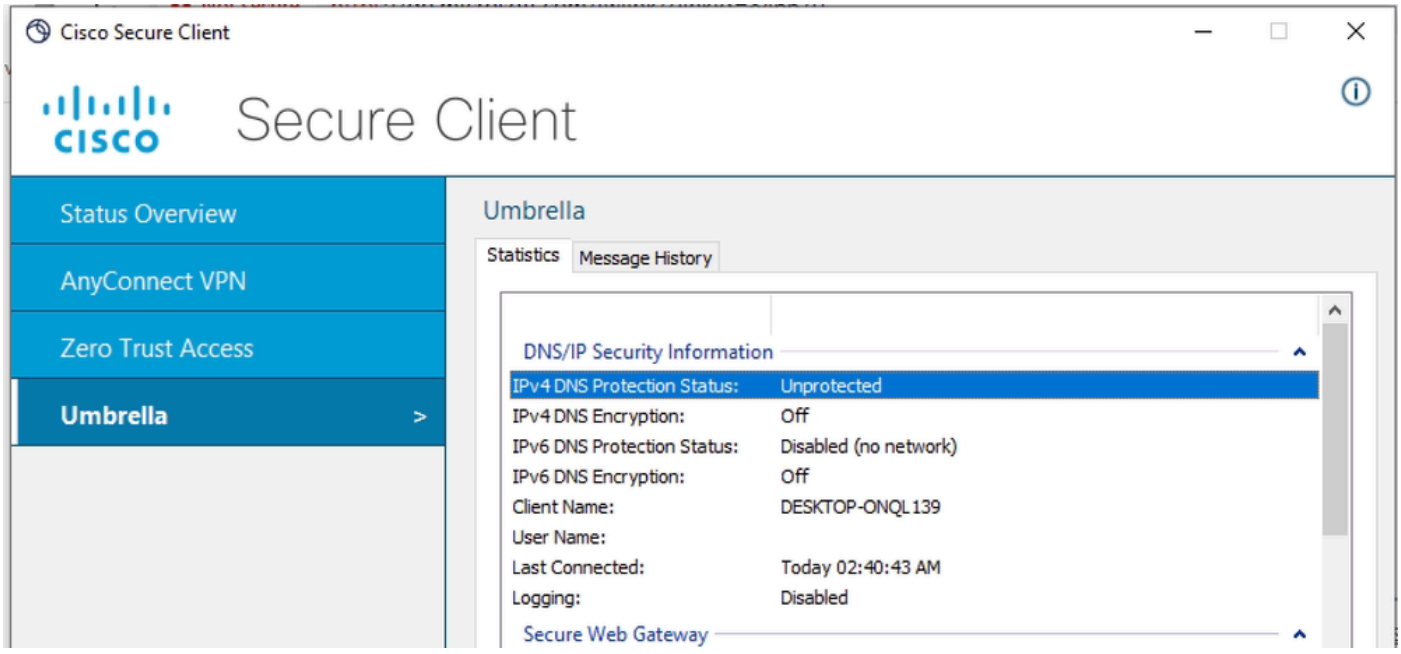
Problema

Cuando un usuario inicia el Módulo Roaming de Secure Client y espera utilizar la protección DNS y/o Web, se pueden ver estados erróneos en la Interfaz de usuario de Secure Client:

Servicio en la nube no disponible para estado de protección web



No protegido para el estado de protección DNS



El motivo de estos errores es que el módulo de roaming no puede ponerse en contacto con sus servicios en la nube debido a problemas de conectividad de red.

Si este problema no se vio en el equipo cliente afectado en el pasado, significa que lo más probable es que la red a la que el equipo está conectado esté restringida y no cumpla con los requisitos descritos en la Documentación de SSE

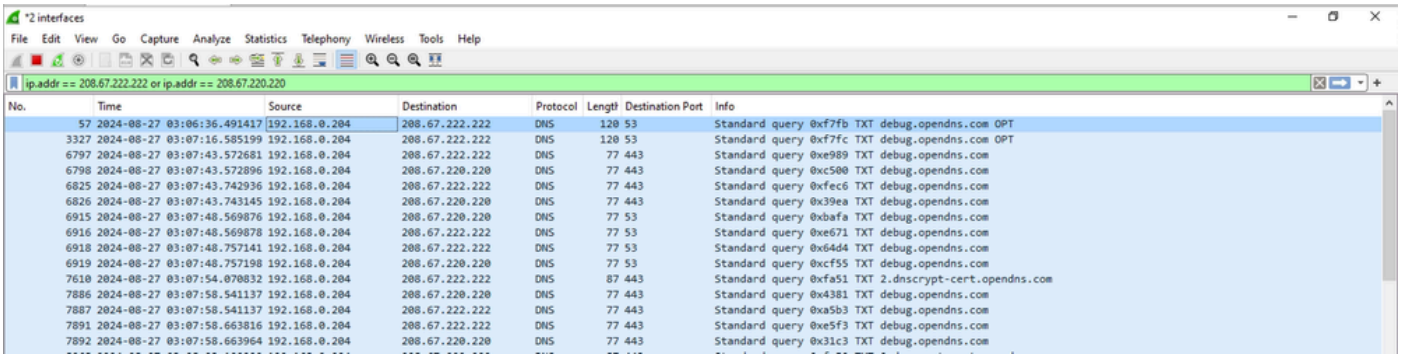
El estado de protección de DNS no está protegido

Cuando vea el estado de DNS desprotegido, lo más probable es que el módulo de roaming no tenga conectividad ascendente con los servidores OpenDNS (208.67.222.222 y 208.67.220.220). Verá el archivo de inicio de sesión cscumbrellaplugin.txt, que forma parte del paquete 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 y confirmar los problemas de conectividad, puede recopilar la captura de Wireshark en la interfaz física de salida del PC (WiFi o Ethernet) y utilizar el filtro de visualización para buscar solamente el tráfico destinado a los resolvers OpenDNS:

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



Como puede ver en el fragmento de Wireshark, está claro que el cliente sigue retransmitiendo consultas DNS TXT destinadas a 208.67.222.222 y 208.67.220.220 en los puertos UDP 443 y 53, pero no recibe ninguna respuesta.

Puede haber múltiples razones detrás de tal comportamiento, muy probablemente el dispositivo de firewall perimetral esté bloqueando el tráfico DNS de salida a los servidores OpenDNS, o solamente permitiendo el tráfico a un servidor DNS específico.

El estado de la protección web es Servicio en la nube no disponible

Cuando vea el estado de protección Web Servicio no disponible, lo más probable es que el módulo de roaming no tenga conectividad ascendente con los servidores de gateway web seguro.

Si el PC no tiene conectividad IP con los servidores SWG, verá el archivo de registro Umbrella.txt,

que forma parte del paquete 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
```

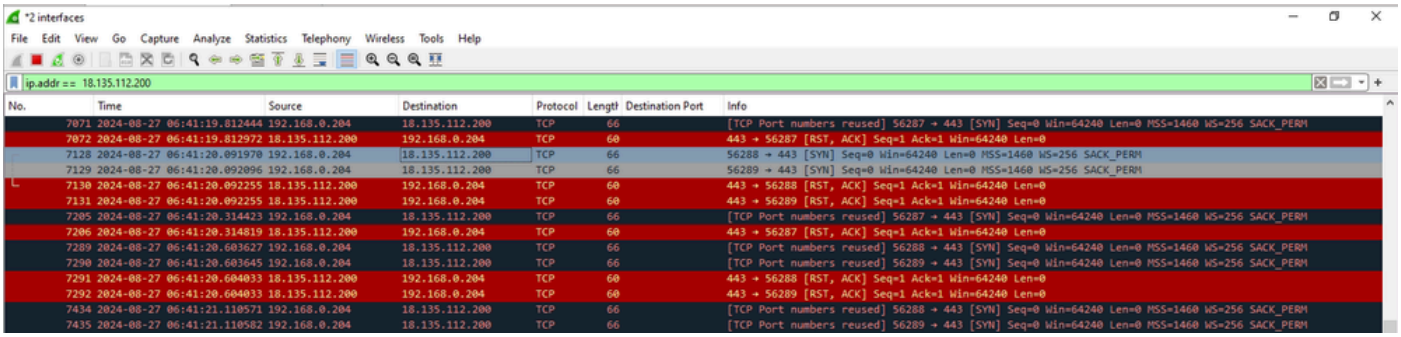
Para investigar más a fondo, recopile la captura de paquetes para probar que la PC no tiene conectividad con el servidor SWG.
Ejecute el comando en el terminal para obtener la dirección IP de SWG:

<#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
```

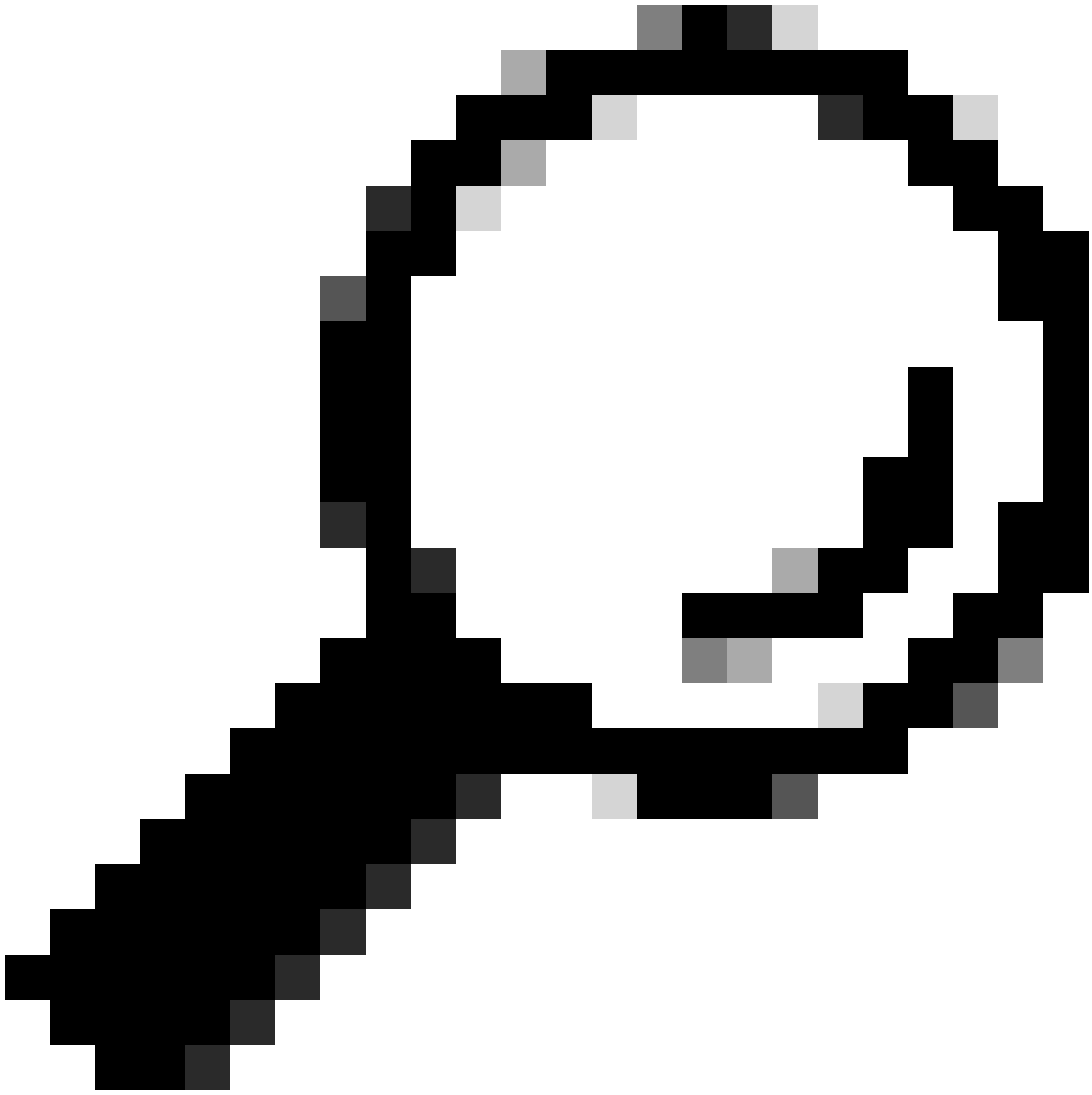
Para verificar y confirmar los problemas de conectividad, puede recopilar la captura de Wireshark en la interfaz física de salida del PC (WiFi o Ethernet) y utilizar el filtro de visualización para buscar solo el tráfico destinado al servidor SWG (utilice la dirección IP obtenida en el paso anterior)

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



Como puede ver en el fragmento de Wireshark, está claro que el cliente sigue retransmitiendo paquetes SYN TCP destinados a 18.135.112.200, pero recibe TCP RST como respuesta.

En esta situación de laboratorio específica, el firewall perimetral bloqueaba el tráfico a la dirección IP de SWG.
En situaciones reales, puede ver solamente retransmisiones TCP SYN, no TCP RST.



Sugerencia: si el cliente no puede alcanzar los servidores SWG, de forma predeterminada entrará en el estado de fallo-apertura cuando el tráfico web salga a través del acceso directo a Internet (WiFi o Ethernet). La protección web no se aplica en el modo fallo-apertura.

Solución

Para identificar rápidamente que la red subyacente está causando problemas, el usuario puede conectarse a cualquier otra red abierta (hotstop, WiFi doméstica) que no tenga ningún firewall perimetral.

Para corregir el error de conexión descrito, asegúrese de que la PC tenga conectividad ascendente sin restricciones, como se describe en la Documentación de SSE.

Problemas de estado de protección DNS:

- 208.67.222.222 Puerto TCP/UDP 53
- 208.67.220.220 Puerto TCP/UDP 53

Para los problemas de estado de protección web, asegúrese de que el tráfico a las direcciones IP de entrada esté permitido en el firewall perimetral - Documentación de SSE

El intervalo específico de direcciones IP de entrada depende de su ubicación.

Información Relacionada

- Guía del usuario de Secure Access
- Cómo recopilar el paquete DART de Cisco Secure Client
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).