

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

## Contenido

---

[Introducción](#)

[Problema](#)

[El estado de protección de DNS no está protegido](#)

[El estado de la protección web es Servicio en la nube no disponible](#)

[Solución](#)

[Información Relacionada](#)

---

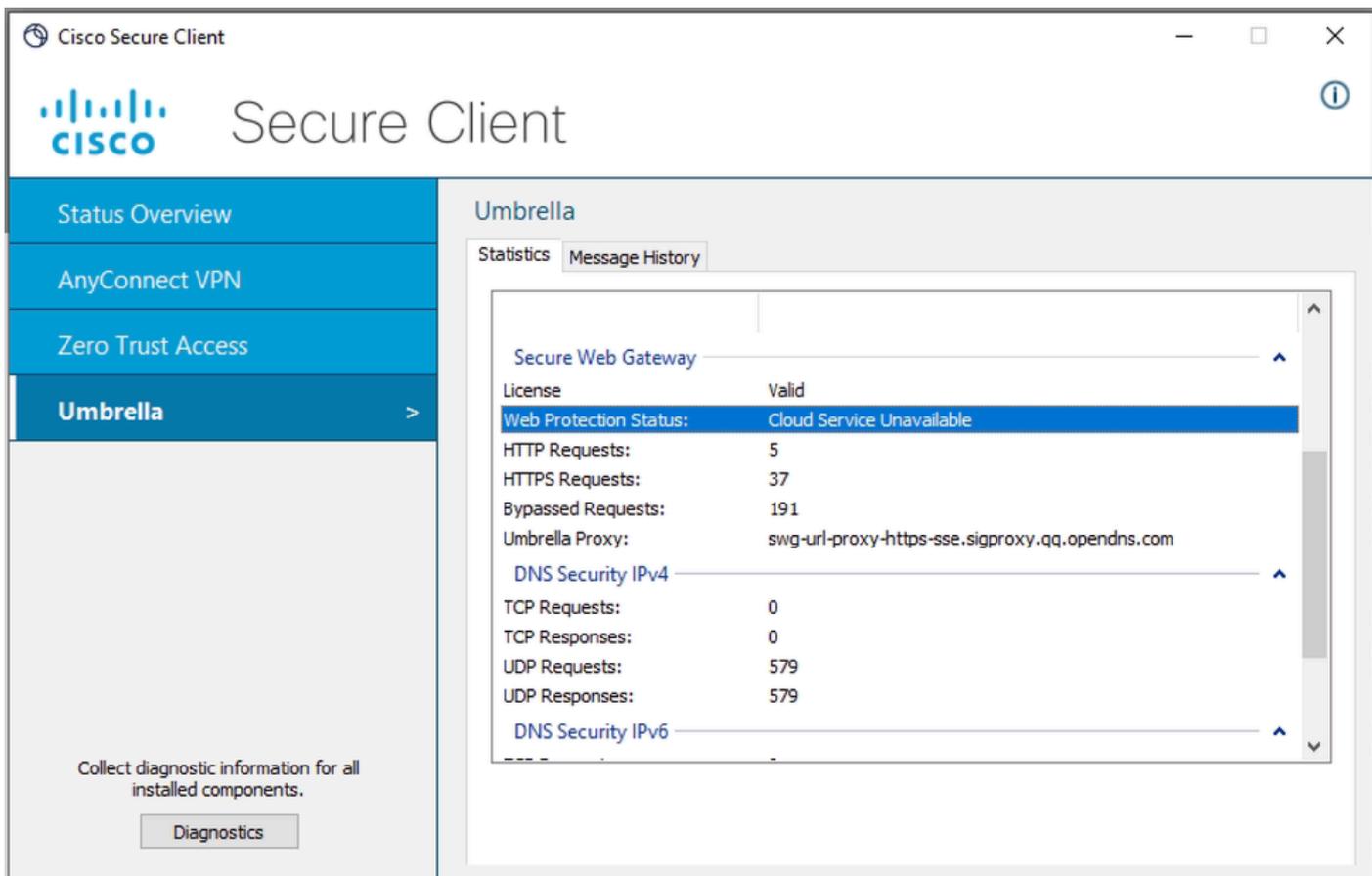
## Introducción

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.

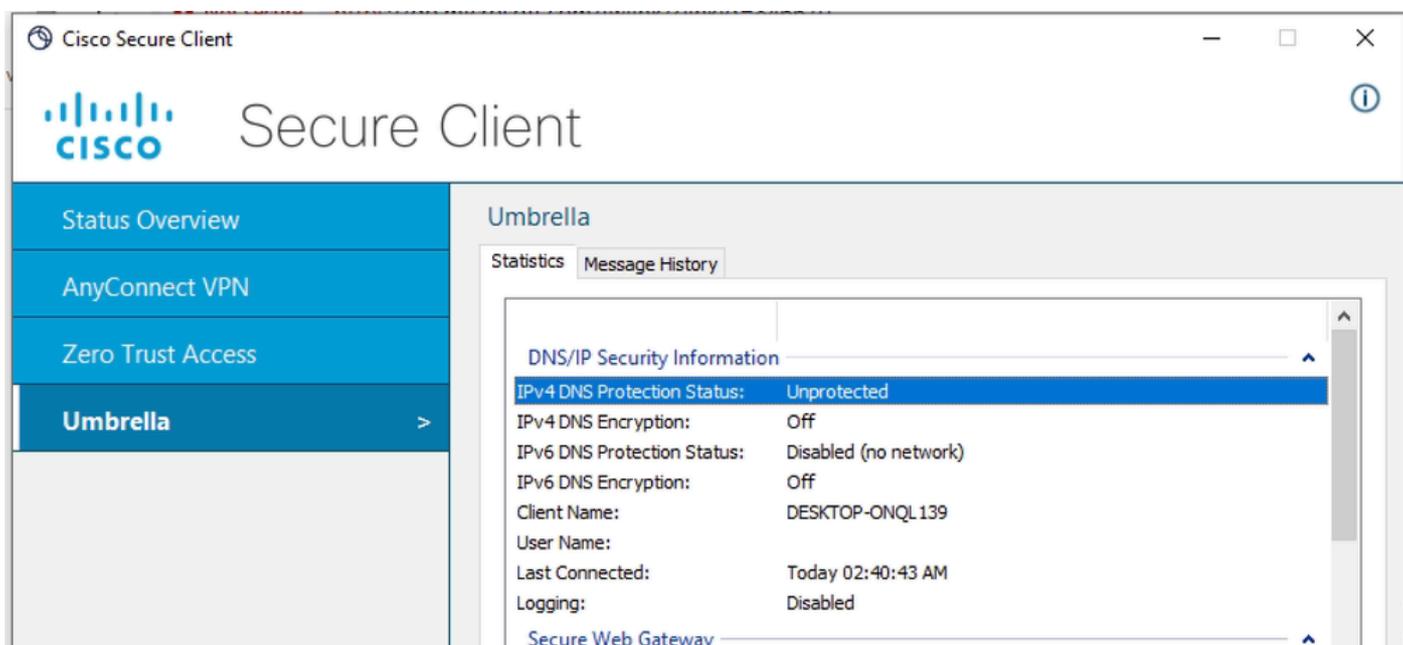
## Problema

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](#)

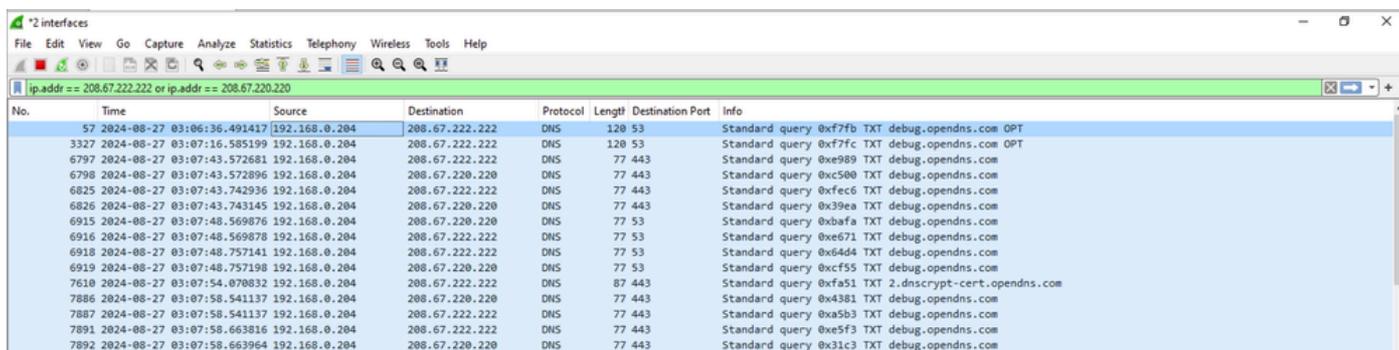
## El estado de protección de DNS no está protegido

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
```



The screenshot shows the Wireshark interface with a capture filter applied: `ip.addr == 208.67.222.222 or ip.addr == 208.67.220.220`. The packet list pane displays several DNS standard query packets (TXT) sent to the OpenDNS servers. The packets are as follows:

No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
57	2024-08-27 03:06:36.491417	192.168.0.204	208.67.222.222	DNS	120	53	Standard query 0xf7fb TXT debug.opendns.com OPT
3327	2024-08-27 03:07:16.585199	192.168.0.204	208.67.222.222	DNS	120	53	Standard query 0xf7fc TXT debug.opendns.com OPT
6797	2024-08-27 03:07:43.572681	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xe989 TXT debug.opendns.com
6798	2024-08-27 03:07:43.572896	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0xc500 TXT debug.opendns.com
6825	2024-08-27 03:07:43.743296	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xfec6 TXT debug.opendns.com
6826	2024-08-27 03:07:43.743145	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x39ea TXT debug.opendns.com
6915	2024-08-27 03:07:48.569876	192.168.0.204	208.67.220.220	DNS	77	53	Standard query 0xbafa TXT debug.opendns.com
6916	2024-08-27 03:07:48.569878	192.168.0.204	208.67.222.222	DNS	77	53	Standard query 0xe671 TXT debug.opendns.com
6918	2024-08-27 03:07:48.757141	192.168.0.204	208.67.222.222	DNS	77	53	Standard query 0x64d4 TXT debug.opendns.com
6919	2024-08-27 03:07:48.757198	192.168.0.204	208.67.220.220	DNS	77	53	Standard query 0xc555 TXT debug.opendns.com
7610	2024-08-27 03:07:54.870832	192.168.0.204	208.67.222.222	DNS	87	443	Standard query 0xfa51 TXT 2.dnscrypt-cert.opendns.com
7886	2024-08-27 03:07:58.541137	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x4381 TXT debug.opendns.com
7887	2024-08-27 03:07:58.541137	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xa5b3 TXT debug.opendns.com
7891	2024-08-27 03:07:58.663816	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xe5f3 TXT debug.opendns.com
7892	2024-08-27 03:07:58.663964	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x31c3 TXT debug.opendns.com

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
```

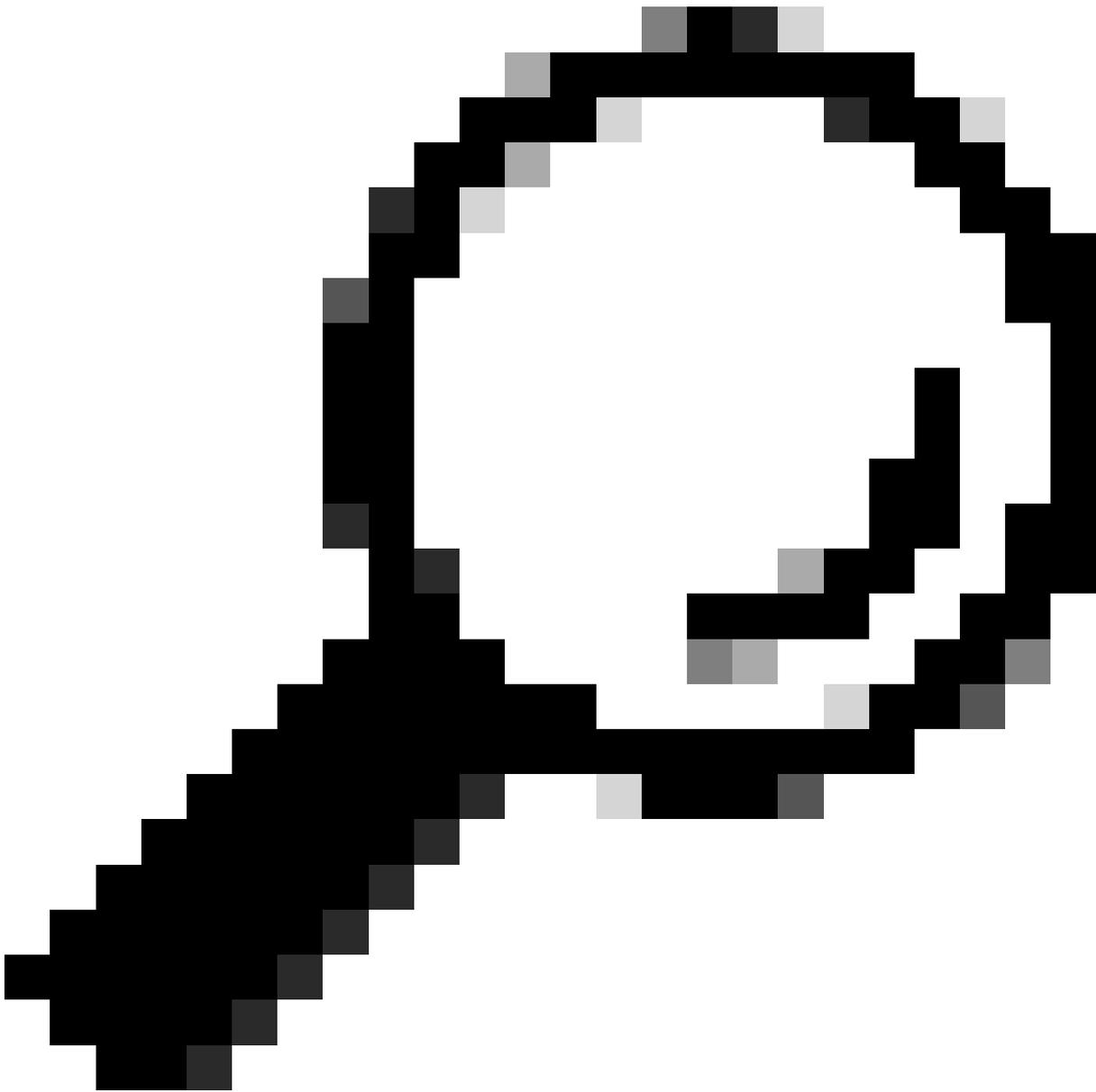
The image shows a Wireshark packet capture window with the filter 'ip.addr == 18.135.112.200'. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
7071	2024-08-27 06:41:19.812444	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56287 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7072	2024-08-27 06:41:19.812972	18.135.112.200	192.168.0.204	TCP	60		443 → 56287 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7128	2024-08-27 06:41:20.091970	192.168.0.204	18.135.112.200	TCP	66		56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7129	2024-08-27 06:41:20.092096	192.168.0.204	18.135.112.200	TCP	66		56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7130	2024-08-27 06:41:20.092255	18.135.112.200	192.168.0.204	TCP	60		443 → 56288 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7131	2024-08-27 06:41:20.092255	18.135.112.200	192.168.0.204	TCP	60		443 → 56289 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7205	2024-08-27 06:41:20.314423	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56287 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7206	2024-08-27 06:41:20.314819	18.135.112.200	192.168.0.204	TCP	60		443 → 56287 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7289	2024-08-27 06:41:20.603627	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7290	2024-08-27 06:41:20.603545	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7291	2024-08-27 06:41:20.604033	18.135.112.200	192.168.0.204	TCP	60		443 → 56288 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7292	2024-08-27 06:41:20.604033	18.135.112.200	192.168.0.204	TCP	60		443 → 56289 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7434	2024-08-27 06:41:21.110571	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7435	2024-08-27 06:41:21.110582	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

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 (hotspot, 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).