排除安全访问漫游模块"；云服务不可用"；或"；未受保护的"；状态故障

目录

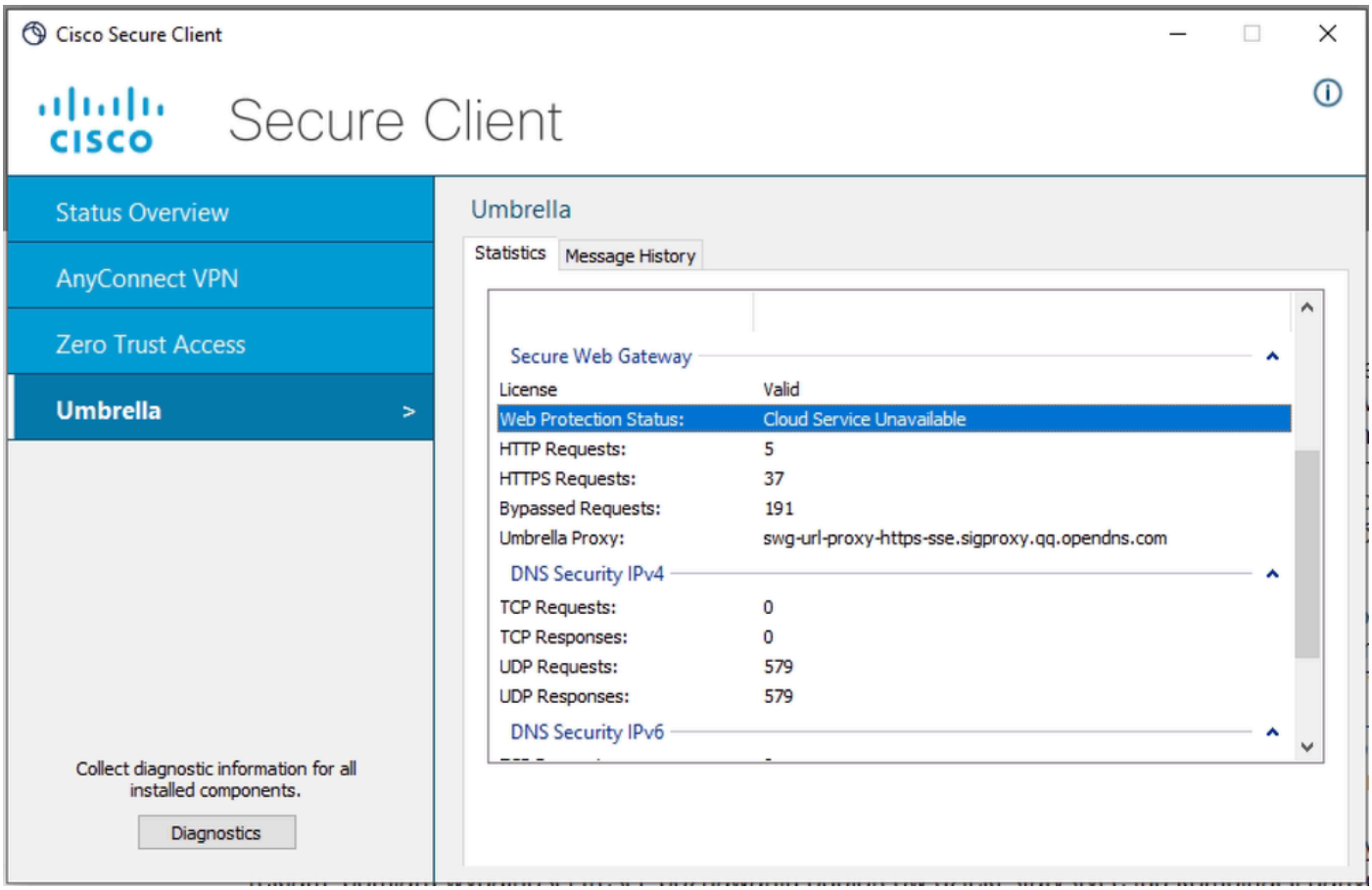
简介

本文档介绍一种调查安全客户端漫游模块中“云服务不可用”或“未受保护”状态的根本原因的方法。

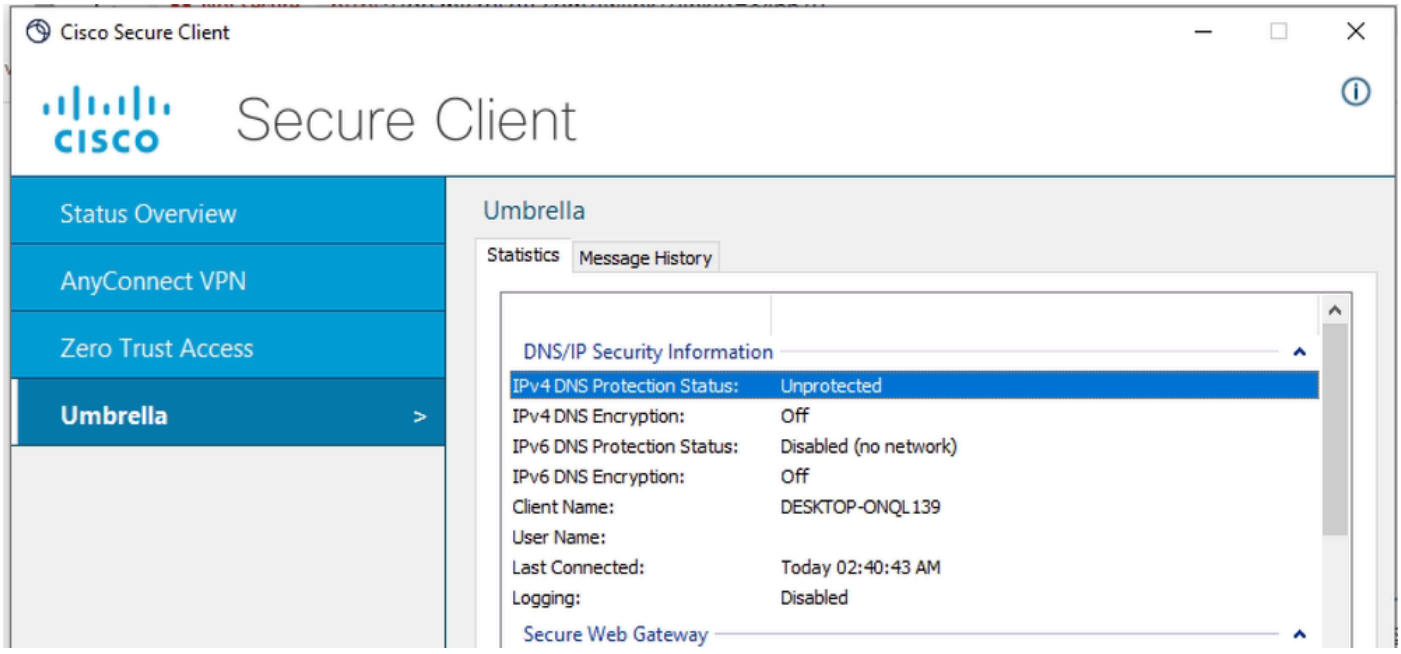
问题

当用户启动安全客户端的漫游模块并希望使用DNS和/或Web保护时，安全客户端用户界面中会出现错误状态：

云服务不可用，无法获得Web保护状态



Unprotected for DNS Protection状态



这些错误的原因是，由于网络连接问题，漫游模块无法联系其云服务。

如果受影响的客户端PC过去没有出现此问题，则意味着很可能该PC连接的网络受到限制，并且不符合SSE文档中列出的要求

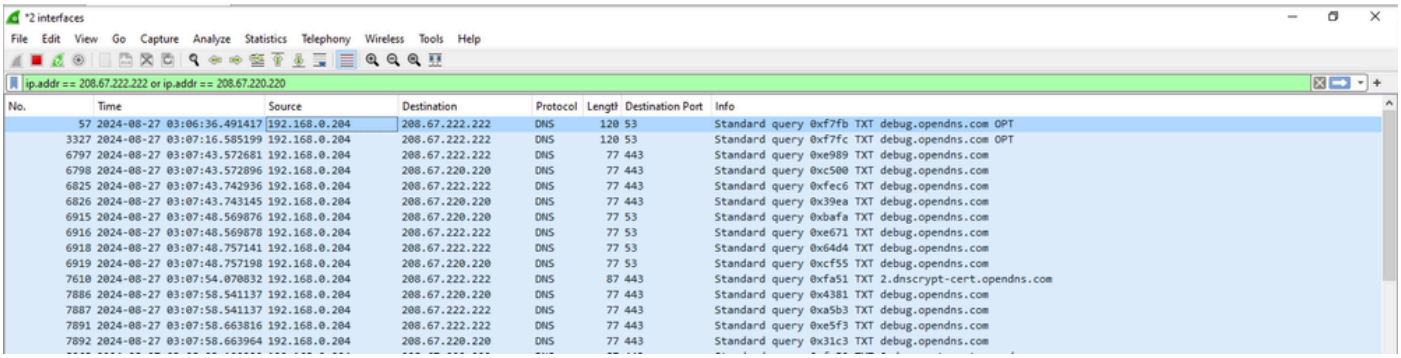
DNS保护状态为“未保护”

当您看到不受保护的DNS状态时，漫游模块很可能没有到OpenDNS服务器(208.67.222.222和208.67.220.220)的上行连接。
您会看到cscumbrellaplugin.txt文件中的日志，该文件是DART捆绑包的一部分。

```
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
```

为了仔细检查并确认连接问题，您可以在PC的出口物理接口（WiFi或以太网）上收集wireshark捕获，并使用显示过滤器仅查找发往OpenDNS解析器的流量：

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



如您在Wireshark的代码片断中所见，很显然，客户端在UDP端口443和53上不断重新传输发往208.67.222.222和208.67.220.220的DNS TXT查询，但是没有收到任何响应。

这种行为背后可能有多种原因，最有可能的是外围防火墙设备阻止了通往OpenDNS服务器的出口DNS流量，或者只允许流向特定DNS服务器的流量。

Web保护状态为“云服务不可用”

当您看到“服务不可用”Web保护状态时，漫游模块很可能不具有到安全Web网关服务器的上游连接。

如果PC与SWG服务器没有IP连接，您将看到Umbrella.txt文件中的日志，该文件是DART捆绑包的一部分。

```
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
```

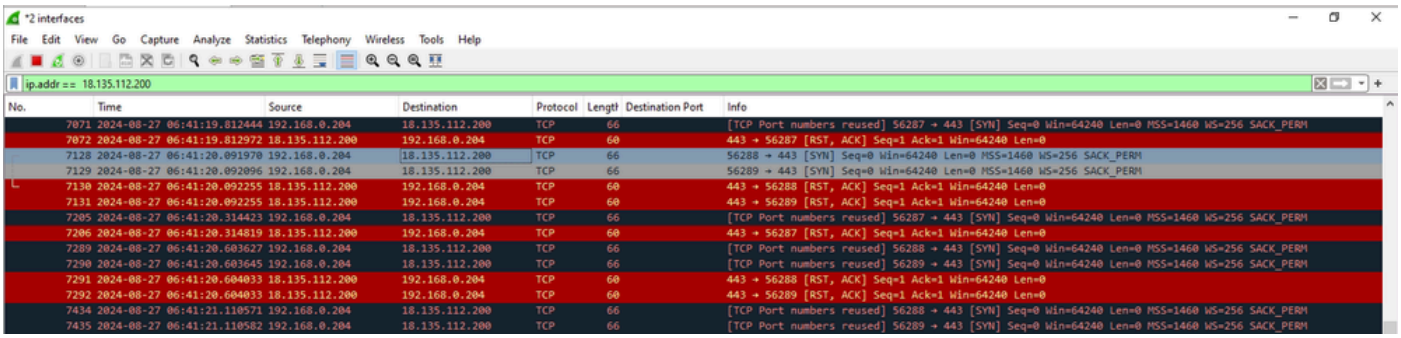
为了进一步调查，请收集数据包捕获来证明PC与SWG服务器没有连接。
在terminal中发出命令以获取SWG IP地址：

<#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
```

为了仔细检查并确认连接问题，您可以在PC的出口物理接口（WiFi或以太网）上收集wireshark捕获，并使用显示过滤器仅查找发往SWG服务器的流量（使用上一步获得的IP地址）

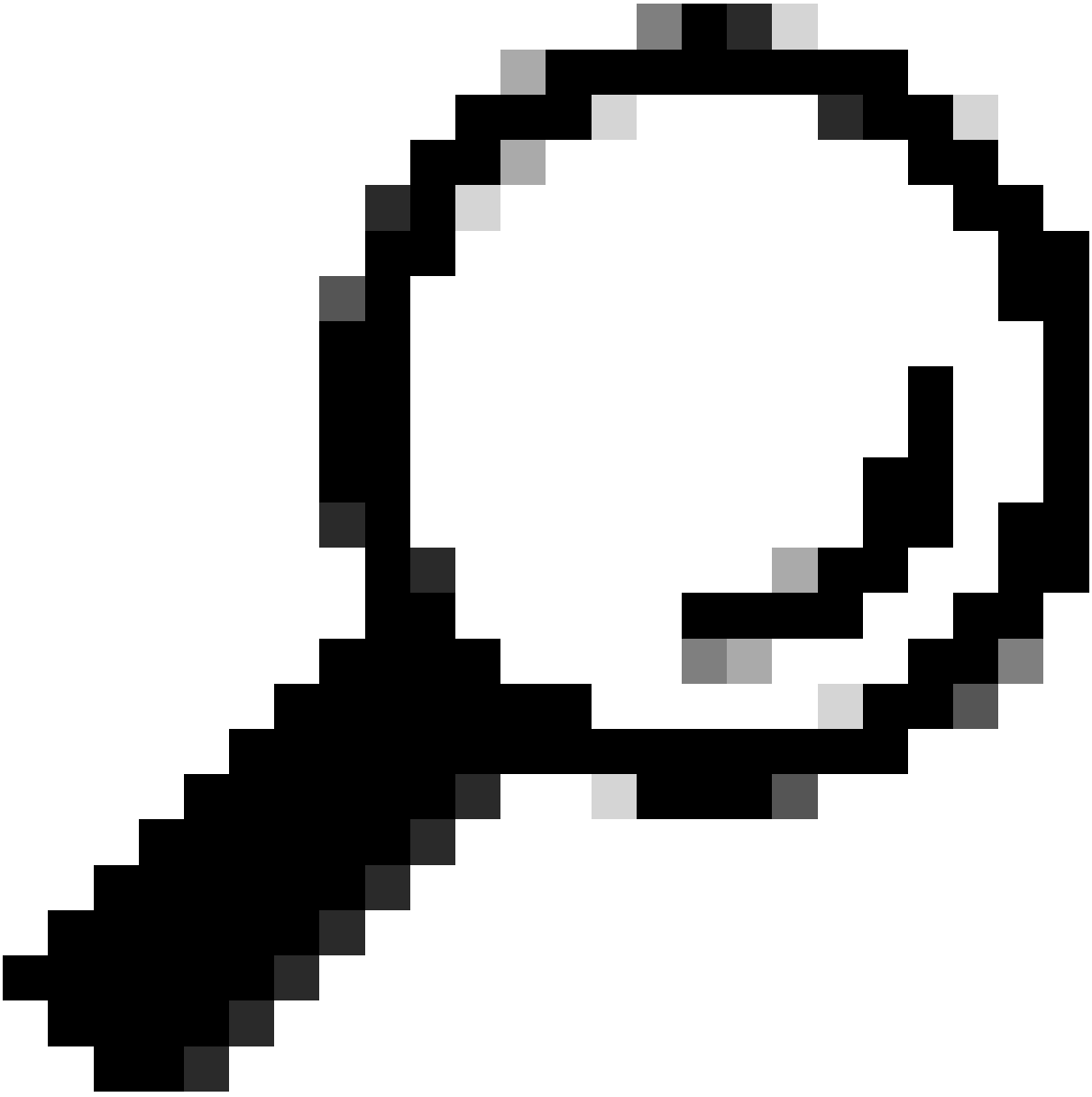
```
ip.addr == 18.135.112.200
```



正如您在Wireshark的代码片断中所看到的，客户端显然是不断重新传输发往18.135.112.200的TCP

SYN数据包，但接收TCP RST作为响应。

在此特定实验场景中，边界防火墙阻止了发往SWG IP地址的流量。
在现实生活中，您只能看到TCP SYN重新传输，而无法看到TCP RST。



提示：如果客户端无法访问SWG服务器，则默认情况下会进入失效开放状态，其中Web流量通过直接互联网访问（WiFi或以太网）离开。Web保护未应用于失效开放模式。

解决方案

为了快速确定底层网络导致的问题，用户可以连接到没有任何边界防火墙的任何其他开放网络（热站、家庭WiFi）。

要修复所述的连接错误，请确保PC具有如SSE文档中所述的不受限制的上行连接。

DNS保护状态问题：

- 208.67.222.222 TCP/UDP端口53
- 208.67.220.220 TCP/UDP端口53

对于Web保护状态问题，请确保边界防火墙上允许流向入口IP地址的流量- SSE文档

入口IP地址的特定范围取决于您的位置。

相关信息

- 安全访问用户指南
- 如何从Cisco安全客户端收集DART捆绑包
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。