對安全訪問漫遊模組"；雲服務不可用"；或"；未受保護狀態"；進行故障排除

目錄

[簡介](#)

[問題](#)

- [DNS保護狀態為「未受保護」](#)
- [Web保護狀態為「雲服務不可用」](#)

[解決方案](#)

[相關資訊](#)

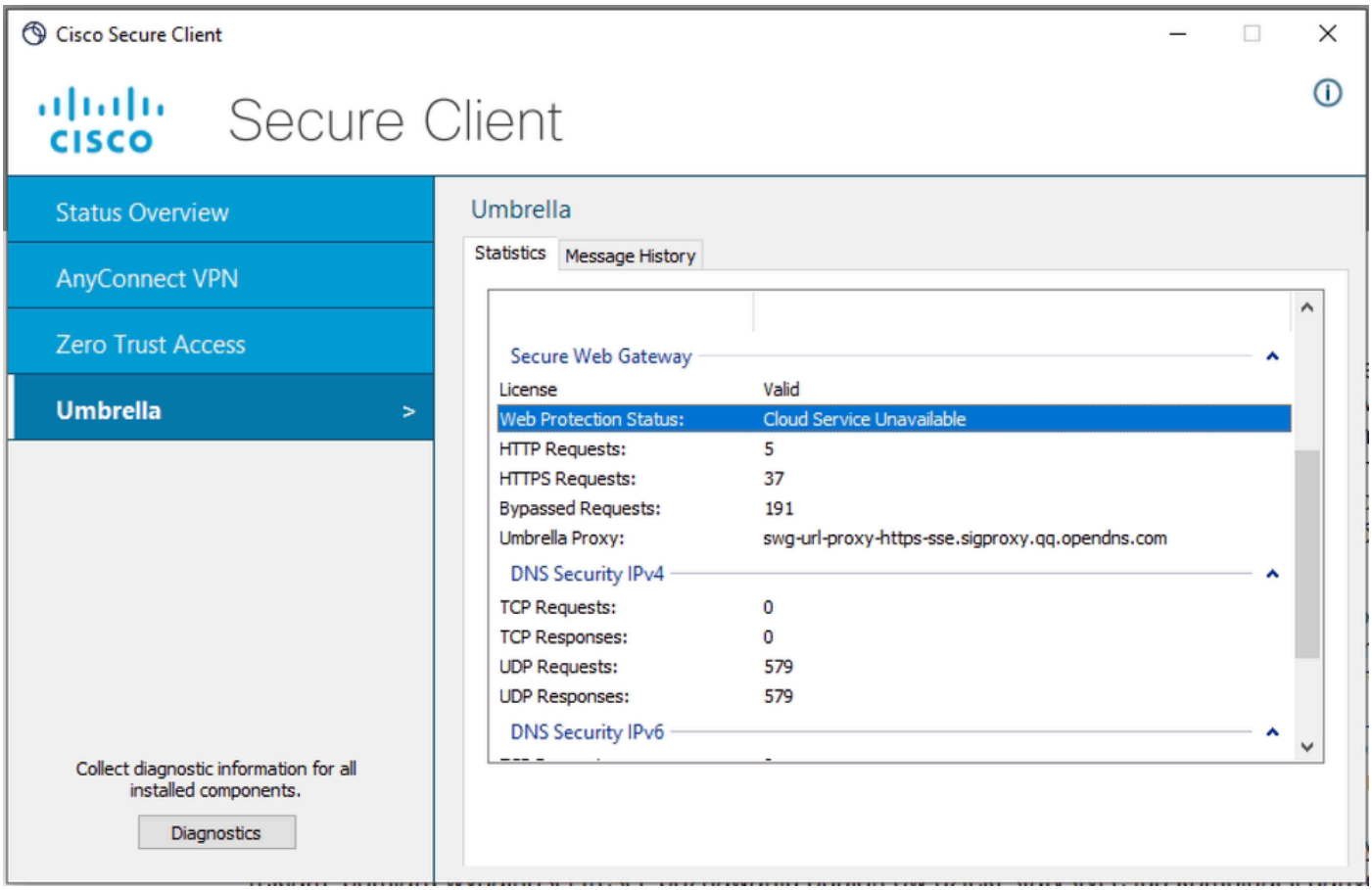
簡介

本文描述一種檢查安全客戶端漫遊模組中「雲服務不可用」或「未受保護」狀態的根本原因的方法。

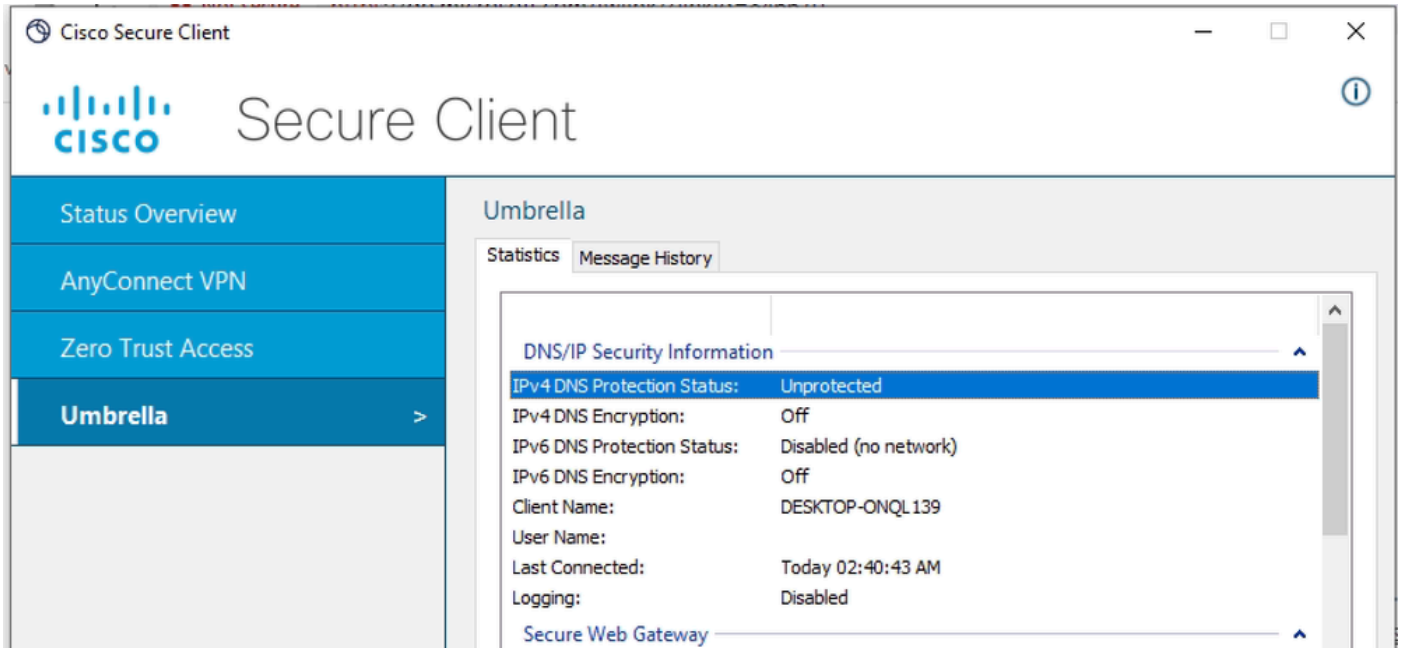
問題

當使用者啟動安全客戶端的漫遊模組並期望使用DNS和/或Web保護時，安全客戶端使用者介面中會顯示錯誤狀態：

雲服務無法用於Web保護狀態



未受保護的DNS保護狀態



這些錯誤的原因是由於網路連線問題導致漫遊模組無法聯絡其雲服務。

如果受影響的客戶端PC過去從未出現過此問題，則意味著與PC連線的網路很可能受到限制，並且不符合SSE文檔中列出的要求

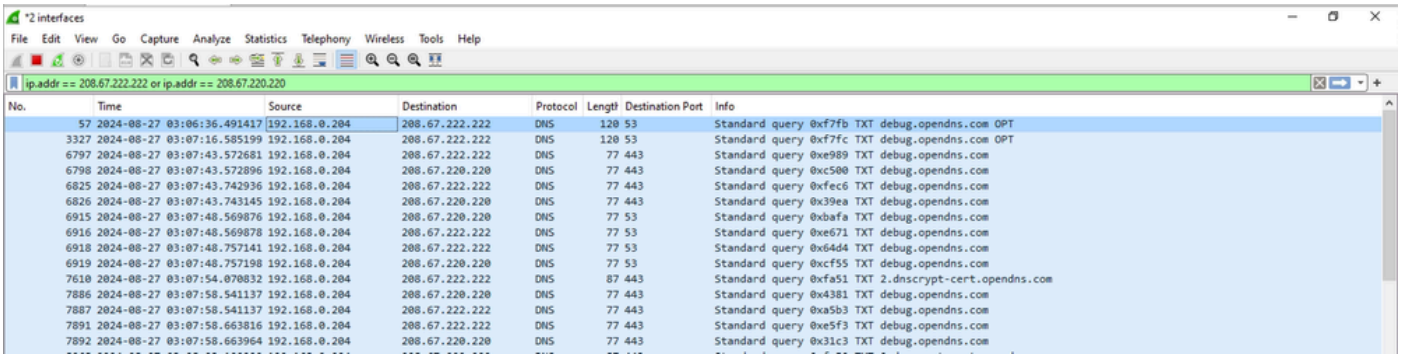
DNS保護狀態為「未受保護」

當您看到未受保護的DNS狀態時，很可能是漫遊模組沒有到OpenDNS伺服器(208.67.222.222和208.67.220.220)的上行連線。
您將在DART捆綁包中的csccumbrellaplugin.txt檔案中看到日誌。

```
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
```

為了再次檢查並確認連線問題，您可以在PC的出口物理介面（WiFi或乙太網）上收集wireshark捕獲，並使用顯示過濾器僅查詢發往OpenDNS解析器的流量：

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



如您在Wireshark的代碼段中所見，很明顯，客戶端會不斷重新傳輸發往UDP埠443和53上的208.67.222.222和208.67.220.220的DNS TXT查詢，但不會收到任何響應。

這種行為背後可能有多種原因，最可能的原因是外圍防火牆裝置阻止了到OpenDNS伺服器的出口DNS流量，或者只允許到特定DNS伺服器的流量。

Web保護狀態為「雲服務不可用」

當您看到「服務不可用」Web保護狀態時，漫遊模組很可能不具有到安全Web網關伺服器的上行連線。

如果PC無法與SWG伺服器建立IP連線，您會看到Umbrella.txt檔案中的日誌，該檔案是DART捆綁包的一部分。

```
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
```

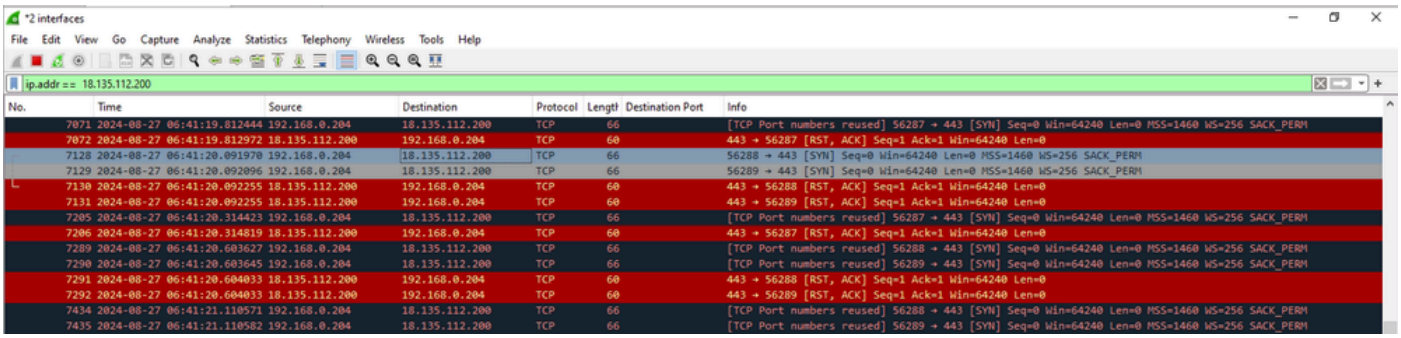
為了進行進一步調查，請收集資料包捕獲資訊，以證明PC無法與SWG伺服器建立連線。
在terminal中發出命令以獲取SWG IP地址：

<#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
```

為了再次檢查並確認連線問題，您可以在PC的出口物理介面（WiFi或乙太網）上收集wireshark捕獲，並使用顯示過濾器僅查詢發往SWG伺服器的流量（使用上一步中獲取的IP地址）

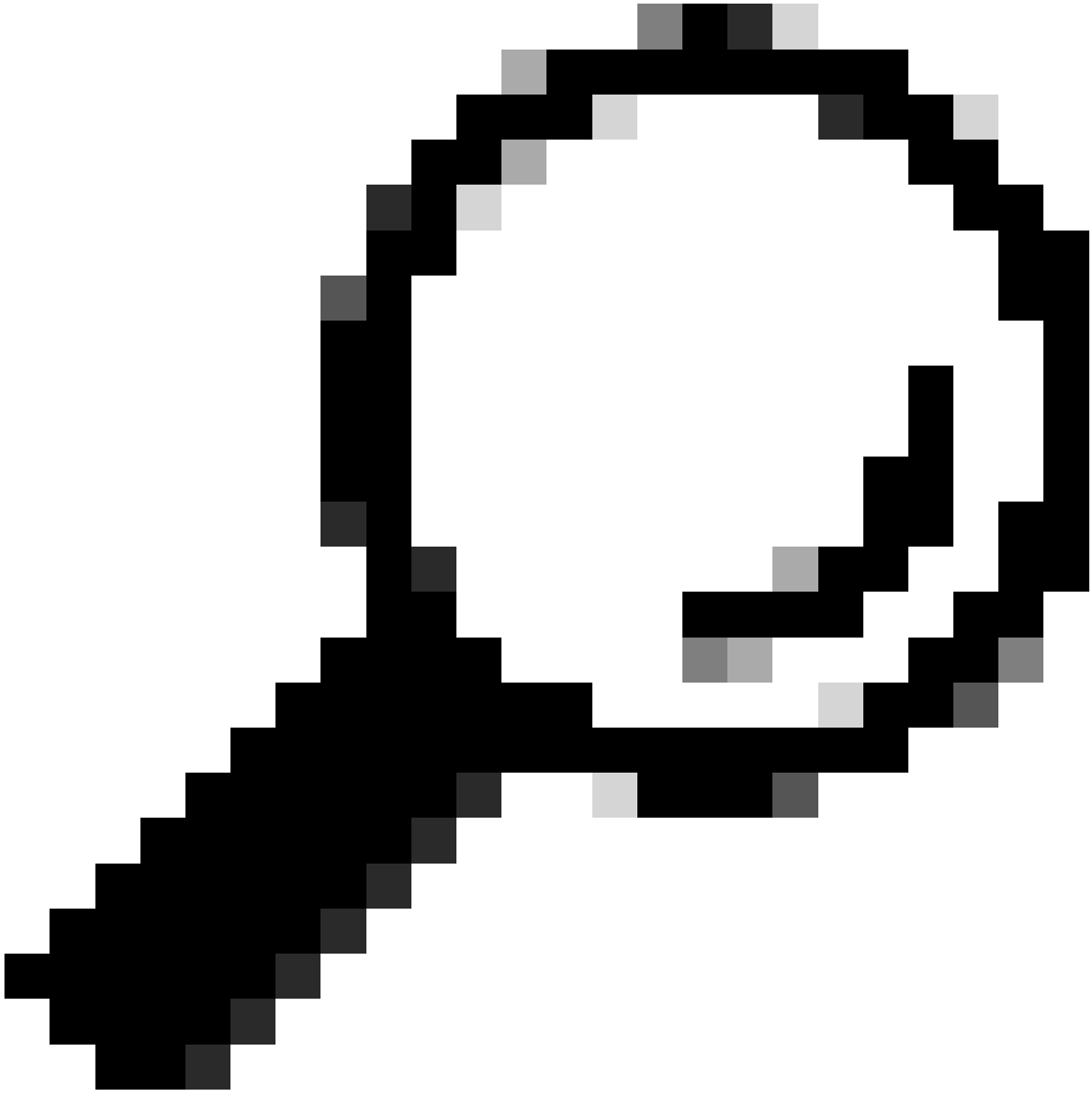
```
ip.addr == 18.135.112.200
```



正如您在來自Wireshark的代碼段中所看到的，客戶端會一直重新傳輸發往18.135.112.200的TCP

SYN資料包，但會接收TCP RST作為響應。

在此特定實驗場景中，邊界防火牆阻止流量到達SWG IP地址。
在現實生活中，您只能看到TCP SYN重新傳輸，而無法看到TCP RST。



提示：如果客戶端無法訪問SWG伺服器，則預設情況下會進入失效開放狀態，在該狀態下，Web流量將透過直接網際網路接入（WiFi或乙太網）離開。Web保護未應用於失效開放模式。

解決方案

為了快速辨識底層網路造成問題，使用者可以連線到沒有任何周邊防火牆的任何其他開放網路（熱站、家庭WiFi）。

要修復描述的連線錯誤，請確保PC具有如SSE文檔中概述的不受限制的上行連線。

DNS保護狀態問題：

- 208.67.222.222 TCP/UDP埠53
- 208.67.220.220 TCP/UDP埠53

對於Web保護狀態問題，請確保周界防火牆上允許流向輸入IP地址的流量- SSE文檔

入口IP地址的特定範圍取決於您的位置。

相關資訊

- Secure Access使用手冊
- 如何從Cisco安全客戶端收集DART捆綁包
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。