

由於Codex應用程式DNS風暴，安全客戶端Umbrella模組變為非活動狀態

目錄

問題

MacOS上的多個使用者會體驗Cisco Secure Client Umbrella漫遊模組間歇性地轉換到非活動（失效開放）狀態。在這些期間，包括終端啟動的nslookup命令在內的DNS請求無法到達網路層，從而影響使用者解析域和訪問基於網際網路的資源的能力。

此問題在Umbrella日誌中反複出現探測失敗，顯示以下消息：

```
Transparent probe failed
Encrypted probe failed
Switching to basic probe
DNS probe failed by timeout - going open
```

分析表明，當Umbrella處於非活動狀態時，Acsock驅動程式在同一故障視窗內崩潰。當使用者主動使用Codex和AI Assistant應用程式時，在向CODEX傳送命令後立即向chatgpt.com進行大量連線嘗試時，最常發現此問題。

環境

- 思科安全客戶端版本5.1.13、5.1.16、5.1.17
- macOS（觀察到多個版本）
- 已啟用Umbrella漫遊模組
- 已啟用ZTNA/安全網路存取(SIA)模組
- Codex應用程式正在使用

- 從不同網路 (家庭、辦公室、不同ISP) 工作的使用者

解析

通過實施域旁路配置來防止DNS請求重複來解決此問題。驗證了下一節中介紹的方法。

主要解決方案：域繞過

- 步驟 1:將chatgpt.com新增到Cisco Secure Access配置的旁路清單中。這可防止安全客戶端複製Codex應用程式生成的DNS請求，從而消除導致驅動程式不穩定的DNS風暴。
- 步驟 2:驗證旁路配置。測試Codex功能，以確認在旁路就緒後，問題不再出現。

備選解決方案：Codex配置解決方法

應用GitHub問題中引用的代碼配置更改，以減少應用程式生成的DNS請求量。

<https://github.com/openai/codex/issues/21218>

使用的高級故障排除步驟

已執行這些診斷步驟以確定根本原因。

1. — 啟用詳細套接字記錄：

```
sudo /opt/cisco/secureclient/kdf/bin/acsocketool -sdf 0x830801F2
```

2. — 重現問題並在出現故障後立即收集DART捆綁包。

3. — 禁用詳細日誌記錄：

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -cdf
```

4. — 為SWG啟用最大調試日誌記錄。建立包含內容的SWGConfigOverride.json檔案：

```
{"logLevel": "1"}
```

儲存到/opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json。

5. — 為DNS啟用RSM跟蹤日誌。建立包含內容的force_log_level.plist檔案：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>logLevel</key>
<string>trace</string>
</dict>
</plist>
```

儲存到/opt/cisco/secureclient/umbrella/data。

原因

核心問題與Codex應用行為有關，該行為會生成大量的DNS請求。如果未繞過chatgpt.com，則這些請求會被Cisco Secure Client有效複製，從而產生一個DNS風暴，導致CPU使用率高和快取記憶體核心驅動程式不穩定。

出現此問題的原因如下：

- Codex在操作期間生成大量到chatgpt.com的DNS查詢。
- 如果沒有旁路配置，安全客戶端將攔截並複製這些請求。
- 大量重複的DNS請求會導致套接字驅動程式崩潰。
- 驅動程式不穩定會導致Umbrella探測器故障和轉換到失效開放狀態。

當繞過chatgpt.com或應用了Codex解決方法時，不會發生這種重複，問題不再出現。此問題同時影響僅Umbrella和ZTNA SIA配置，表明問題出在流量處理機制而非特定模組內。

相關內容

- [安全訪問漫遊模組故障排除](#)
- [排除故障並收集基本資訊](#)
- [思科技術支援與下載](#)

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）。

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）。