

# AnyConnect VPN登入因終端狀態條件（包括Cortex）而被拒絕

## 目錄

---

---

## 問題

多個使用者間歇性地無法連線到安全客戶端遠端訪問(RAVPN)並收到錯誤消息「AnyConnect VPN Login denied」。您的環境不符合管理員定義的訪問條件。" 此問題同時影響MacBooks和Surface筆記型電腦，使用者通常需要多次嘗試連線或系統重新啟動才能建立成功連線。連線失敗似乎與終端狀態驗證條件有關，具體包括macOS版本要求和Cortex XDR狀態驗證。

## 環境

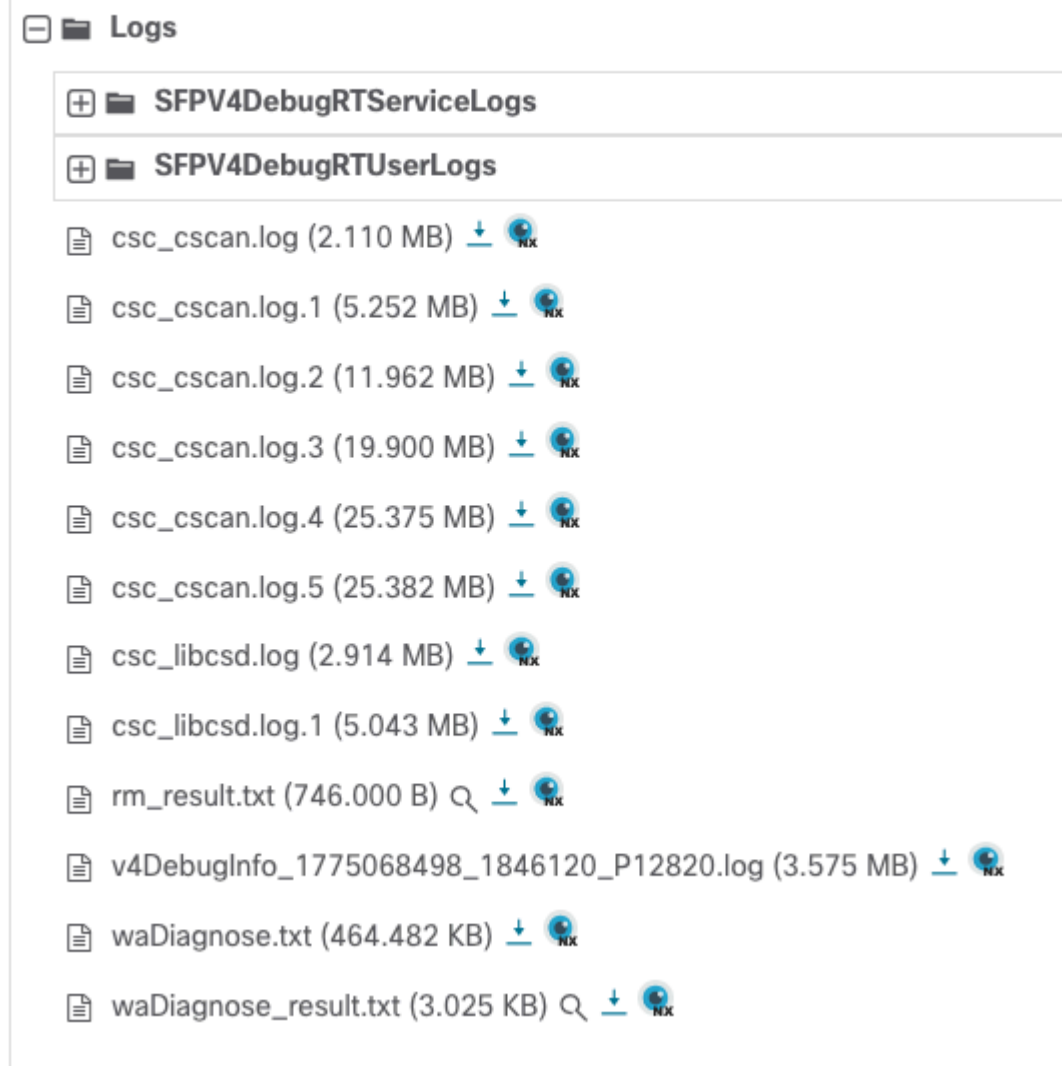
- 安全客戶端遠端訪問(RAVPN)部署，安全狀態評估
- 包括MacBooks和Surface筆記型電腦在內的混合終端環境
- 終端安全評估要求：運行Cortex XDR的MacOS版本26.2或更高版本
- 實施裝置訪問策略(DAP)的安全訪問解決方案

## 解析

1:收集DART。

2:導航到Secure Firewall Posture資料夾並下載csc\_scan.log:

Secure Firewall Posture



inline\_image\_0.png

3:查詢以下日誌：

[2026年3月27日星期五 13:53:10.419]調試：Json in as {"input":{"method":1000,"signature":}}

[2026年3月27日星期五 13:53:10.420]錯誤：Opwat返回錯誤：-22並轉換為：6

[2026年3月27日星期五 13:53:10.420]錯誤：在條件中失敗：opSuccess != status

[2026年3月27日星期五 13:53:10.420]調試：Opwat Return status is access denied

[2026年3月27日星期五 13:53:10.420]調試：使用服務檢查防惡意軟體的rtp狀態。

[2026年3月27日星期五 13:53:10.420]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:10.420]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:10.420]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:10.420]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:15.060]錯誤：正在接收響應。

[2026年3月27日週五 13:53:15.060]調試：無法執行am檢查rtp。<<<<-----

[2026年3月27日週五 13:53:15.060]資訊：返回的RTP狀態失敗

[2026年3月27日週五 13:53:15.060]資訊：Opswat退貨定義日期為1

[2026年3月27日週五 13:53:15.060]調試：使用服務獲取反惡意軟體的定義日期。

[2026年3月27日星期五 13:53:15.060]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:15.060]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:15.060]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:15.060]追蹤軌跡：TCP/IP狀態Ipv4(1),Ipv6(1)

[2026年3月27日星期五 13:53:20.079]錯誤：正在接收響應。

[2026年3月27日週五 13:53:20.079]調試：無法執行反惡意軟體定義日期操作<<<<<<—

[2026年3月27日週五 13:53:20.079]調試：發現反惡意軟體==>()(Cortex XDR(Mac))(9.1.0)() (失敗)。

[2026年3月27日週五 13:53:20.084]調試：匹配失敗：進程名稱為「ciscod」和「cscan」

[2026年3月27日週五 13:53:20.084]調試：edr internet連線檢查狀態(1)



附註：基於此，這似乎是Cortex對我們流程的限制，或者對網際網路接入的限制，以及我們

---

---

所能檢查的Cortex是否沒有干擾該流程的其他事情。它可能正在阻止安全防火牆狀態，因為掃描可能被視為惡意軟體。

---

## 防惡意軟體排除清單

思科安全使用者端(CSC)：所有模組 — 系統

1. Windows:C:\Program Files (x86)\Cisco\Cisco Secure Client\\*
2. macOS:/opt/cisco/secureclient/\*
3. Linux:/opt/cisco/secureclient/\*

思科安全使用者端(CSC)：所有模組 — 使用者

1. Windows: %localappdata%\Cisco\Cisco Secure Client\\*
2. macOS: ~/.cisco/secureclient/\*
3. Linux: ~/.cisco/secureclient/\*

## 原因

此問題由終端狀態評估過程中的間歇性故障導致，具體與macOS版本要求和Cortex XDR狀態驗證相關。狀態評估系統無法持續檢測或驗證所需安全條件（macOS 26.2或更高版本和Cortex XDR運行狀態），導致即使端點滿足指定標準也會拒絕連線。這會導致使用者需要多次嘗試連線或系統重新啟動才能成功進行狀態評估和VPN連線。

## 相關內容

- [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）。