具有Zscaler SSL/TLS解密干擾的對等方重置Cisco安全客戶端VPN連線

目錄

問題

使用者嘗試使用Cisco Secure Client建立連線時遇到VPN連線失敗。

環境

- 技術：思科安全訪問 — 安全客戶端遠端訪問（VPN、安全狀態、專用資源）
- 產品系列：SEACACS
- 作業系統：macOS（基於顯示/Users/admin/workspace/secure-client-macos_Raccoon_MR15/）的日誌檔案路徑
- 第三方軟體：客戶端系統上安裝的Zscaler
- VPN協定：CSTP（思科SSL隧道協定）
- TLS版本：帶密碼TLS_AES_256_GCM_SHA384的TLS 1.3

解析

解決方案涉及識別和解決Cisco安全客戶端和Zscaler的SSL/TLS解密功能之間的衝突。

步驟 1:日誌分析和診斷

捕獲和分析Cisco安全客戶端DART日誌，確定連線故障模式。日誌將顯示成功的TLS會話建立，然後立即重置連線。

日誌中的主要診斷指標：

- 使用密碼TLS_AES_256_GCM_SHA384建立TLS 1.3連線
- MTU計算和HTTP協商正常進行
- 對等體錯誤導致連線重置(返回代碼：54)在套接字讀取操作期間

TLS 1.3會話使用密碼TLS_AES_256_GCM_SHA384成功建立，但會話建立後會立即傳送重置資料包，該資料包將終止連線，導致VPN隧道關閉。在套接字讀取操作期間，日誌中觀察到的特定錯誤顯示返回代碼為54(0x00000036)的「對等連線重置」。

在連線嘗試期間發生以下錯誤序列：

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

步驟 2:第三方軟體識別

調查是否存在可能會在客戶端系統上執行SSL/TLS檢查或解密的第三方安全軟體。在這種情況下，Zscaler被確定為干擾應用。

步驟 3:SSL/TLS解密衝突解決方案

解決Cisco安全客戶端VPN流量與Zscaler的SSL/TLS解密功能之間的衝突。Zscaler似乎正在對VPN流量進行SSL/TLS解密，這將干擾VPN隧道的建立並導致連線重置。

可能的解決方法包括：

- 將Zscaler配置為從SSL/TLS檢查中排除Cisco安全客戶端VPN流量
- 在Zscaler中為VPN伺服器終端建立旁路規則
- 在VPN連線測試期間臨時禁用Zscaler以確認衝突

- 與網路安全團隊協調，確定適當的排除項

原因

此問題的根本原因是思科安全客戶端VPN流量與Zscaler的SSL/TLS解密功能之間的衝突。Zscaler嘗試解密或檢查VPN的TLS流量時，會干擾安全隧道建立過程。這種干擾在TLS會話建立後立即表現為連線重置，從而阻止VPN隧道完成其協商階段。重置資料包的定時（在成功建立TLS之後但隧道完成之前）是來自安全裝置或軟體的SSL/TLS檢查干擾的特徵。

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）。