遠端訪問VPN的iOS上思科安全客戶端的DNS日誌記錄和裝置註冊行為

目錄

問題

當使用iOS上的思科安全客戶端(iPad)通過Microsoft Entra ID使用SAML身份驗證與思科安全訪問建立遠端訪問VPN時，即使正確生成防火牆和網路日誌，VPN連線成功後也不會在安全訪問中顯示DNS日誌。此外，建立VPN連線後，iPad不會顯示在Secure Access控制面板中的漫遊裝置>流動裝置下。

觀察到的具體症狀包括：

- 遠端訪問日誌在Secure Access中顯示成功的「連線」事件
- 生成防火牆和Web日誌並顯示經過SAML身份驗證的使用者身份
- 安全訪問日誌記錄中完全沒有DNS日誌
- iPad裝置資訊未填充在安全訪問漫遊裝置部分
- 所有流量通過VPN隧道（未配置分割隧道）

環境

- 執行iOS 26.2的iPad
- 思科安全使用者端
- 身份提供程式：Microsoft Entra ID
- 安全聯結器：未安裝
- 配置了SSO身份驗證的Cisco安全訪問
- SAML身份驗證實施

- 將DNS模式配置為預設模式的VPN配置檔案
- 未配置拆分隧道（所有通過VPN路由的流量）
- 用於配置檔案分發的流動裝置管理(MDM)

解析

所觀察到的行為對於所記錄的配置是預期的。iOS上的Cisco Secure Client充當VPN客戶端（AnyConnect等效功能），預設情況下不包括RSM等效功能。安全聯結器是iOS上與RSM等效的元件，是終端身份填充和Umbrella式DNS控制所必需的。

瞭解架構

缺少DNS日誌和裝置註冊的原因如下：

- 僅思科安全客戶端提供VPN連線，但缺少DNS可視性所需的終端代理功能
- 安全訪問中的DNS控制和裝置註冊需要安全聯結器（相當於Windows上的RSM）
- 如果沒有安全聯結器，DNS查詢由VPN獲取的DNS伺服器處理，無法檢視Umbrella/Secure Access

通過流量導向的DNS日誌記錄解決方案

要在不安裝安全聯結器的情況下啟用DNS日誌記錄，請配置流量引導以將DNS查詢定向到Umbrella DNS伺服器：

步驟 1:在安全訪問中配置流量控制

導覽至Traffic Steering > Add > Add a source，然後指定DNS伺服器IP作為源。

步驟 2:將DNS流量定向到Umbrella伺服器

配置VPN配置檔案以使用Umbrella DNS伺服器（208.67.222.222和208.67.220.220），以確保DNS查詢對安全訪問可見。

步驟 3:驗證DNS日誌記錄

實施流量控制配置後，DNS日誌應該在VPN會話的安全訪問控制面板中可見。

VPN配置檔案DNS模式設定

VPN配置檔案中的「DNS模式」設定與此配置中沒有DNS日誌無關。無論此設定如何，RAVPN（遠端訪問VPN）會話都使用通過VPN獲取的DNS伺服器，而日誌的可見性取決於DNS流量是否定向到受監控的DNS基礎設施。

安全聯結器安裝選項

在iOS上安裝安全聯結器將啟用：

- 安全訪問中的DNS日誌記錄可見性
- 增強的端點身份和裝置註冊功能
- Umbrella式DNS控制和保護

安全聯結器可與Secure Client結合使用，但需要適當的流量排除和設計注意事項來防止兩個元件之間的衝突。

原因

根本原因是架構性的：iOS上的Cisco Secure Client提供VPN連線，但不包括Secure Access中的DNS可視性和裝置註冊所需的終端代理功能。此功能需要安全聯結器安裝或流量控制配置，以通過受監控的基礎設施來引導DNS查詢。如果沒有這些元件，DNS查詢將繞過安全訪問監控，並且裝置標識資訊不會填充在漫遊裝置部分。

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）。