安全訪問中MX75網路隧道的安全客戶端身份可視性問題

目錄

問題

當具有安全客戶端的終端部署在連線到安全接入的MX75網路隧道之後時，漫遊客戶端和使用者身份在系統中無法正確可見。觀察到以下特定行為：

- 當端點落後於MX75時，配置為通過網路隧道連線優先使用安全客戶端的回退設定無法按預期運行
- 基於域的流量引導規則不適用，因為流量僅歸屬於網路隧道標識而不是漫遊客戶端
- 「活動搜尋」顯示不完整的源位置資訊，僅顯示網路隧道標識，同時忽略使用者和漫遊客戶端標識
- 基於身份的流量引導規則（例如基於Active Directory使用者或漫遊客戶端身份的規則）無法應用於通過MX75隧道的流量

此行為可阻止通過網路隧道基礎設施連線的端點正確身份隔離和策略應用。

環境

- 思科安全訪問部署
- MX75裝置，通過網路隧道配置實現安全訪問
- 在所有端點上安裝的安全客戶端代理
- 在漫遊客戶端上禁用回退設定，以通過網路隧道連線優先使用安全客戶端
- 為基於域的路由配置的流量控制規則
- 為Active Directory使用者和漫遊客戶端配置的基於身份的策略

解析

通過使用註冊網路方法實施替代配置，而不是依賴通過MX75網路隧道的漫遊身份可視性，解決了此問題。

因應措施實施

步驟 1:使用註冊網路配置RSM（漫遊安全模組）

將現有網路隧道配置替換為RSM部署與註冊網路設定相結合。此配置允許正確的身份屬性和策略應用。

步驟 2:驗證身份可視性

實施註冊網路配置後，請驗證：

- 使用者身份在Activity Search中正確顯示
- 漫遊客戶端標識可見且屬性正確
- 基於使用者和客戶端身份功能的流量引導規則（如預期）

步驟 3:測試流量控制功能

確認基於域的流量控制規則和基於身份的策略正確應用於新配置。

替代方法

對於不需要通過專用網路進行身份隔離的環境，請考慮實施RSM - Internet配置。此方法將RSM流量直接傳送到網際網路，而不是通過私有網路隧道傳送，這樣可以在保持安全控制的同時提供適當的身份可視性。

技術分析

在故障排除期間，使用policy.test.sse.cisco.com收集診斷輸出，以演示終端位於MX75隧道後面時的身份屬性行為。分析確認，雖然通過網路隧道路由漫遊身份在技術上是可行的，但是對於此特定部署方案，這不是推薦或支援的操作流程。

原因

根本原因與安全訪問在流量通過網路隧道基礎設施時如何處理身份屬性有關。當終端通過MX75網路隧道連線時，系統將所有流量都歸屬於隧道標識，而不是保留各個漫遊客戶端和使用者標識。此行為是為網路隧道連線設計的，但會與個人身份可視性和策略應用的要求衝突。

雖然通過網路隧道路由漫遊身份在技術上可行，但由於上述身份屬性限制，不建議或不支援將此配置作為標準操作流程。

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）。