啟用安全訪問Web安全的Azure VPN客戶端連線失敗

目錄

問題

從Umbrella遷移到SSE並使用新分配的SIA許可證啟用網路安全後，啟用網路安全時，無法為使用者建立Azure VPN客戶端連線。Azure VPN客戶端連線問題會影響所有客戶端，阻止它們連線到VPN。從客戶端電腦解除安裝Cisco Secure Access Client時，VPN連線將恢復，這表示安全訪問客戶端正在阻止與Azure VPN服務的連線。

禁用Web Security或解除安裝Cisco Secure Access Client會還原VPN連線，但在需要網路安全保護時，這會影響使用者通過Azure VPN對資源的訪問。

環境

- 啟用網路安全的Cisco Secure Access（前身為SIA）
- Azure VPN客戶端
- 從Umbrella遷移到SSE已完成
- 新分配的SIA許可證

解析

解決方法涉及將Azure VPN網關公共IP地址新增到SSE/SWG異常清單，以防止阻止VPN連線的流量攔截。

步驟 1:確定Azure VPN網關IP地址

確定Azure VPN網關的公共IP地址。

步驟 2:將基於IP的例外新增到SSE/SWG

1. — 將Azure虛擬網關公共IP地址新增到Cisco Secure Access環境中的SSE/SWG異常清單中。

2. — 登入到Cisco Secure Access Dashboard — 點選Connect - End user Connectivity - Internet Security - Add exception。這將阻止安全Web網關攔截和檢查發往Azure VPN網關的流量。

步驟 3:測試VPN連線

應用基於IP的異常後，測試Azure VPN連線以驗證客戶端是否可以在啟用網路安全的情況下成功建立VPN連線。

步驟 4:擴展測試

將基於IP的異常的測試擴展到整個環境中的其他使用者，以確保功能一致，然後再考慮解決完成。

原因

之所以會出現此問題，是因為安全Web閘道(SWG)例外機制需要網域的DNS查詢來建立網域到IP的快取專案。當Azure VPN客戶端直接連線到IP地址而不對VPN URL執行DNS查詢時，SWG模組無法將域對映到IP地址。因此，SWG會繼續檢查並攔截到IP地址的流量，從而阻止VPN連線的建立。

資料包捕獲分析顯示VPN URL沒有DNS查詢，Azure網關IP沒有可見的SWG偵聽流量，確認SWG正在阻止連線，原因是其快取中缺少正確的域到IP對映。

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）。