

由於ESN協商導致的安全訪問IPsec隧道與Versa網路路由器連線問題

目錄

問題

在使用Versa-Network Router作為邊緣裝置在分支機構部署Cisco Secure Access期間，儘管兩個IPsec隧道都顯示正常，但還是遇到了連線問題。T

具體症狀包括：

- 分支機構無法連線到Cisco Secure Access
- 通過靜態路由的Internet訪問不起作用
- 觀察到單向加密流量（僅出站到安全訪問）
- 路由器統計資訊，顯示正在傳送的出站資料包，但沒有收到入站資料包
- 在SD-WAN路由器和安全訪問之間雙向工作的失效對等體檢測
- 用於正確匹配出站流量的安全引數索引(SPI)值
- 通道擺動（重置）未解決連線問題
- 資料包捕獲和螢幕截圖證實了缺少入站流量
- 將隧道密碼從CBC更改為GCM未解決問題

調查顯示由於校驗和錯誤，流量未能在思科端解密，該錯誤追蹤到Versa路由器協商ESN（擴展序列號）功能。

環境

- 思科安全訪問部署

- Versa — 作為邊緣裝置的網路路由器
- IP-Identity隧道配置
- 嘗試使用CBC和GCM密碼的IPsec隧道配置

解析

解決方法涉及在Versa路由器上禁用擴展序列號(ESN)協商，以防止校驗和錯誤，這些錯誤導致思科安全訪問前端上的解密失敗。

解決步驟

步驟 1:確定根本原因

調查確定Versa路由器正在協商ESN（擴展序列號），從而導致思科安全訪問前端接收校驗和錯誤，並且無法解密ESN構建的資料包。

步驟 2:在Versa路由器上禁用ESN

聯絡Versa網路支援或路由器管理員禁用Versa路由器配置上的ESN檢查和協商。這解決了導致ESN協商不當的已知Versa錯誤。

步驟 3:驗證連線

禁用ESN協商後，確認已建立雙向通訊流，並恢復從分支機構到安全訪問和Internet的完全連線。

步驟 4:監控流量

驗證路由器上的入站和出站資料包統計資訊是否顯示兩個方向的正确通訊流，確認單向通訊問題的成功解決。

原因

根本原因確定為已知的Versa網路錯誤(Versa支援錯誤ID:122437 - ESN不得由VOS交涉，其中Versa路由器在IPsec通道建立期間錯誤地交涉延伸序號(ESN)功能。此ESN協商會導致Cisco Secure Access頭端接收帶有校驗和錯誤的資料包，從而阻止正确解密，並導致單向流量。Versa路由器成功傳送出站資料包，但由於ESN相關的解密失敗，無法正确處理返回流量。

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）。