當流量通過ASA時，使用TCP的IPsec失敗

目錄

簡介

使用IPsec over TCP連線到VPN頭端的Cisco VPN客戶端可能會連線到頭端，但連線在一段時間後會失敗。本文說明如何切換到IPsec over UDP或原生ESP IPsec封裝以解決問題。

開始之前

需求

為了解決此特定問題，必須配置Cisco VPN客戶端以使用IPsec over TCP連線到VPN頭端裝置。在大多數情況下，網路管理員會配置ASA以通過TCP埠10000接受Cisco VPN客戶端連線。

採用元件

本檔案中的資訊是根據Cisco VPN Client。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題

當VPN客戶端配置為IPsec over TCP(cTCP)時，如果收到重複的TCP ACK請求VPN客戶端重新傳輸資料，VPN客戶端軟體將不會響應。如果VPN客戶端和ASA頭端之間的某個位置發生資料包丟失，則可能會生成重複的ACK。在Internet上，間歇性資料包丟失是一個相當常見的現實。但是，由於VPN端點未使用TCP協定（請回憶一下，它們正在使用cTCP），因此端點將繼續傳輸並且連線將繼續。

在此案例中，如果有其他裝置（例如防火牆）以狀態追蹤TCP連線，則會出現問題。由於cTCP協定

沒有完全實現TCP客戶端，並且伺服器重複的ACK沒有收到響應，這可能導致與此網路流串聯的其他裝置丟棄TCP流量。網路中必須發生資料包丟失，這會導致TCP資料段丟失，從而觸發問題。

這不是錯誤，而是網路上丟包和cTCP不是真實TCP的副作用的結果。cTCP會嘗試模擬TCP通訊協定，方法是將IPsec封包封裝在TCP標頭中，但這正是通訊協定的範圍。

當網路管理員實施帶有IPS的ASA或在ASA上執行某種應用檢測（導致防火牆充當連線的完整TCP代理）時，通常會發生此問題。如果資料包丟失，ASA將代表cTCP伺服器或客戶端確認丟失的資料，但VPN客戶端永遠不會響應。由於ASA從未收到它期望的資料，因此通訊無法繼續。因此，連線失敗。

解決方案

為了解決此問題，請執行以下任一操作：

- 從IPsec over TCP切換為IPsec over UDP，或使用ESP協定的本機封裝。
- 切換到AnyConnect客戶端進行VPN終止，該客戶端使用完全實現的TCP協定棧。
- 將ASA配置為對這些特定IPsec/TCP流應用tcp-state-bypass。這實際上會禁用對匹配tcp狀態略過策略的連線的所有安全檢查，但允許連線工作，直到可以實施此清單中的另一個解析。如需詳細資訊，請參閱TCP狀態略過准則和限制。
- 確定資料包丟失的來源，並採取糾正措施以防止IPsec/TCP資料包在網路上丟失。這通常是不可能的，或者非常困難，因為問題的觸發因素通常是Internet上的資料包丟失，並且無法阻止丟包。

相關資訊

- 技術支援與文件 - Cisco Systems