採用TLS/DTLS和IPsec(IKEv2)雙配置的Cisco安全訪問RAVPN協定行為

目錄

問題

當在主協定設定為IPsec(IKEv2)的Cisco安全接入RAVPN中同時啟用TLS/DTLS和IPsec(IKEv2)協定時，嘗試從阻止IPsec流量（UDP埠500/4500）的網路建立VPN連線時，會出現連線故障。安全客戶端預設使用客戶端UI下拉選單中的IPsec選項，並且在IPsec連線失敗時不會自動故障切換到TLS/DTLS，從而導致連線錯誤和無法從受限網路環境中建立RAVPN連線。

環境

- 含雙通訊協定組態的Cisco安全存取RAVPN
- TLS/DTLS和IPsec(IKEv2)協定均已啟用
- 配置為IPsec(IKEv2)的主協定設定
- 包含單獨的IPsec和TLS選項的「使用協定選擇的安全客戶端」下拉選單
- 在UDP埠500和4500上阻止IPsec流量的網路環境

解析

所觀察到的行為是預期的，並且是設計好的。當兩個協定都啟用並且主協定遇到連線問題時，Cisco Secure Access RAVPN不會執行從IPsec(IKEv2)到TLS/DTLS的自動協定故障切換。

需要手動選擇協定

從阻止IPsec流量的網路進行連線時，使用者必須在安全客戶端中手動選擇適當的協定：

步驟 1:開啟Secure Client應用程式

步驟 2:在客戶端介面中找到「協定選擇」下拉選單

步驟 3:手動將選擇從IPsec選項更改為TLS選項

步驟 4:使用TLS/DTLS協定啟動VPN連線

通訊協定行為說明

Cisco Secure Access RAVPN中的Primary protocol設定確定安全客戶端中顯示的預設協定，但不啟用自動故障切換功能。同時啟用TLS/DTLS和IPsec(IKEv2)時：

- 安全客戶端在下拉選單中顯示單獨的協定選項
- 客戶端預設為主協定設定（本例中為IPsec）
- 根據網路連線條件，協定之間不會進行自動交換
- 使用者必須根據其網路環境手動選擇適當的協定

原因

Cisco Secure Access RAVPN設計時沒有自動協定故障切換功能。當同時啟用TLS/DTLS和IPsec(IKEv2)協定時，系統需要通過安全客戶端介面手動選擇協定。Primary protocol設定僅確定客戶端下拉選單中的預設選擇，並且當主協定遇到連線問題時不會實現自動交換邏輯。

相關內容

- 思科安全存取檔案
- 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）。