思科安全存取流量控制組態和使用者端同步

目錄

問題

檢視思科安全訪問流量控制配置時，VPN配置檔案設定和XML檔案不顯示為流量控制配置的目標IP地址或域。這會造成一些混亂，包括Secure Access客戶端如何確定用於指導決策的流量目標，以及在管理門戶中進行的配置更改如何同步到客戶端。

具體來說，管理員注意到，通過VPN配置檔案管理介面配置流量控制設定時，對應的VPN配置檔案XML檔案不包含應受流量控制約束的目標地址或域的可見條目。

環境

- 思科安全存取解決方案
- 啟用了流量控制的VPN配置檔案配置
- 安全訪問客戶端部署

解析

Cisco Secure Access中的流量控制通過動態規則交付機制運行，而不是VPN配置檔案XML中的靜態條目。以下說明此程式的工作原理以及如何驗證配置：

流量控制規則傳遞過程

流量控制規則不儲存在管理員可以檢視的VPN配置檔案XML檔案中。相反，這些規則在VPN連線建立期間從安全訪問前端動態推送到客戶端。該過程的工作方式如下：

1. 建立VPN連線時，安全接入前端會將當前的流量引導（拆分隧道）規則推送到連線的客戶端
2. 客戶端接收這些規則並將它們直接寫入本地客戶端路由表
3. 流量控制決策基於客戶端路由表中的條目作出，而不是通過VPN配置檔案XML中可見的資訊作出

配置更改同步

在管理門戶中對流量控制設定所做的更改遵循特定同步模式：

- 在管理門戶中進行的配置更改在活動VPN會話期間不會生效
- 在下一次VPN連線建立時應用新的流量控制規則
- 要驗證流量控制配置更改後的行為，必須斷開並重新連線VPN連線

驗證步驟

要驗證Traffic Steering配置更改：

1. 對安全訪問管理門戶中的Traffic Steering設定進行所需的更改
2. 斷開客戶端上的現有VPN連線
3. 重新連線VPN以接收更新的流量控制規則
4. 檢查客戶端路由表以驗證是否已應用新規則

原因

VPN配置檔案XML中明顯沒有流量引導目標，這是設計問題。Cisco Secure Access使用動態規則交付系統，在該系統中，流量引導規則在連線時推送到客戶端，並通過路由表條目實施，而不是作為可見的配置元素儲存在配置檔案XML中。此架構支援即時策略更新和集中控制，同時保持安全性和效能。

相關內容

- ASA拆分隧道配置指南
- 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）。