使用安全客戶端的基於客戶端的ZTNA流量引導問題

目錄

問題

當通過FQDN或直接IP地址訪問時，基於客戶端的零信任網路訪問(ZTNA)無法提供對內部應用程式的訪問，而相同的應用程式仍可通過VPN連線訪問。

觀察到的具體症狀包括：

- 當VPN斷開連線時，安全客戶端ZTNA無法通過FQDN或直接IP訪問內部應用程式。
- 基於瀏覽器的ZTNA訪問對相同應用功能正確。
- 當VPN關閉時，活動日誌中未顯示ZTNA事件，這表明客戶端流量未通過ZTNA路徑路由。
- 已驗證專用應用定義是否將VPN可路由資源與正確的IP/埠/FQDN配置相匹配。
- 已確認ZTNA策略與測試使用者和組分配相匹配。

此問題專門隔離於安全客戶端ZTNA流量引導或實施機制，因為基於瀏覽器的ZTNA會驗證後端發佈和執行是否正常運行。

環境

- 技術：安全存取 — 零信任網路存取(ZTNA)
- 元件:基於客戶端的ZTNA、狀態、註冊、私有資源訪問
- 具有共存VPN配置檔案的安全客戶端
- 可通過FQDN和直接IP定址訪問專用應用程式
- 基於瀏覽器的ZTNA功能確認工作正常

- 在最特定匹配實施模式下配置的策略實施

解析

解決方案涉及對ZTA配置檔案的配置調整和策略驗證。下面幾節中介紹的步驟用於恢復基於客戶端的ZTNA功能。

步驟 1:向ZTA配置檔案中新增專用資源

專用資源已新增到ZTA配置檔案配置中。更改後，阻止的事件開始顯示在活動日誌和螢幕截圖中，這表示客戶端流量現在正通過ZTNA路徑正確路由。

步驟 2:策略驗證和測試

新增了一個臨時的「permit any」規則來驗證流量。當此規則處於活動狀態時，基於客戶端的ZTNA訪問正常運行，確認流量引導機制正在工作，但策略實施需要調整。

步驟 3:策略細化

臨時的permit-any規則被刪除，並且特定訪問策略被驗證。使用平台的最特定匹配實施模式，確認可以使用名為Private Resources_Cyril的訪問策略訪問私有資源。

步驟 4:組態驗證

使用者確認基於客戶端的ZTNA訪問在配置更改後開始持續工作。無需進行其他策略修改或系統更改即可解決問題。

原因

根本原因是ZTA配置檔案中的專用資源配置不完整。如果沒有在ZTA配置檔案中定義正確的私有資源，客戶端流量將不會通過ZTNA實施路徑引導，導致其回退到本地路由機制。這導致流量完全繞過ZTNA策略，這解釋了為什麼在VPN斷開連線時，活動日誌中不會出現ZTNA事件。

此問題特定於基於客戶端的ZTNA流量控制配置，而基於瀏覽器的ZTNA繼續發揮作用，因為它使用已正確配置的不同流量處理機制。

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）。