具有IdleTimeout錯誤的企業防火牆後安全訪問間歇性斷開連線

目錄

- 問題
- 環境
- 解析
  - 步驟 1:實施MX TTL緩衝區配置
  - 步驟 2:配置所需的域排除
  - 步驟 3:驗證埠和協定允許範圍
  - 步驟 4:監控和驗證解決方案
- 原因
- 相關內容

問題

當終端連線到企業網路時，思科安全訪問客戶端會經歷間歇性斷開和立即重新連線。斷開連線是隨機發生的，客戶端大約在5秒後自動重新連線。當網際網路流量通過零信任訪問(ZTA)從位於Cisco FirePower和Meraki MX裝置後的終端代理到安全訪問時，會觀察到此行為。

Windows事件日誌捕獲這些斷開連線事件期間的特定「idleTimeout」錯誤。當使用者從家庭Internet連線進行連線時，不會出現斷開連線模式，這表明該問題與公司網路基礎設施特別相關。

該症狀會造成業務中斷，以便為公司網路環境中操作的使用者提供安全的遠端訪問連線，而遠端使用者仍然不受此連線問題的影響。

環境

- 思科安全訪問 — 優勢部署
- Cisco Secure Internet Access(SIA)客戶端軟體
- 採用Cisco FirePower安全裝置的企業網路基礎設施
- 網路路徑中的Meraki MX安全裝置
- 將網際網路流量代理到安全訪問的零信任訪問(ZTA)配置
- 具有事件日誌記錄功能的Windows終結點
- 混合連線方案：公司網路（受影響）和家庭internet連線（不受影響）

解析

解決方案涉及在Meraki MX裝置上實施配置更改，並確保安全訪問整合的適當域排除和埠許可。

步驟 1:實施MX TTL緩衝區配置

在Meraki MX裝置上配置MX TTL緩衝區，以解決導致間歇性斷開問題的DNS TTL快取行為。此配置更改解決了DNS解析快取和Secure Access客戶端連線期望之間的定時衝突。

步驟 2:配置所需的域排除

確保正確將這些域從偵聽中排除，並新增到Cisco FirePower和Meraki MX裝置上的非解密清單中：

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- 策略配置中標識的其他安全訪問服務域

步驟 3:驗證埠和協定允許範圍

配置企業防火牆基礎設施，以允許通過FirePower和Meraki MX裝置使用所需的安全接入埠和協定。確保正確處理流向安全訪問服務端點的埠443的流量，而不會受到可能導致超時條件的安全檢查的干擾。

步驟 4:監控和驗證解決方案

實施MX TTL緩衝區配置後，請連續幾天監控Secure Access客戶端的行為，以確認間歇性斷開和重新連線模式已停止。

原因

間歇性斷開是由企業網路基礎設施和安全訪問服務預期之間的DNS TTL（生存時間）快取行為衝突引起的。思科工程分析顯示，DNS TTL值會因解析程式快取行為而變化，而交替的IP地址則因安全訪問服務架構中的負載平衡機制而變化。

當企業網路裝置（Cisco FirePower和Meraki MX）處理安全訪問終端的DNS響應時，快取和TTL處理會生成計時不匹配，從而導致「idleTimeout」條件。此計時衝突導致Secure Access客戶端將連線解釋為空閒並啟動斷開連線/重新連線循環。

此問題特定於企業網路環境，因為家庭網際網路連線通常未實施可干擾Secure Access客戶端連線狀態管理的同級DNS快取和流量檢查。

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）。