排除PAC檔案的安全訪問SWG代理連線故障

目錄

問題

使用者嘗試使用SWG（安全Web網關）代理URL swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com通過Cisco Secure Access訪問網站時遇到連線失敗。

具體症狀包括：

- Web請求(例如https://www.google.com)失敗，在瀏覽器中出現連線錯誤
- 活動搜尋日誌中未顯示流量
- 從客戶端源IP/客戶端輸出IP到目標終端觀察到伺服器重置：
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- 問題大約在CEST上午9:30開始
- SWG主機名的DNS解析工作正常
- 在埠443上成功通過Telnet連線到swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com
- 外部防火牆沒有阻止與目標IP的連線

封包擷取分析顯示來自代理的TCP RST封包，表示在代理層級終止連線。

環境

- 技術：思科安全存取(SSE)
- 元件：安全Web閘道(SWG)

- SWG代理URL:swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- 受影響的埠：443和80
- 原始NAT IP:20.x.x.x
- 更新的NAT IP:21.x.x.x
- AWS ELB端點入門，例如：歐盟中部或美國東部地區
- 將瀏覽器定向到SWG代理的WPAD配置

解析

通過更新allow-list配置以包括正確的NAT IP地址解決了此問題。

接下來幾節中介紹的步驟用於識別和解決問題。

步驟 1:診斷資料收集

收集的資料包捕獲和WPAD指令碼配置以分析流量和代理配置。

除此之外，主要的線索是https://policy.test.sse.cisco.com，顯示有「401 unauthorized」錯誤。這意味著http連線請求正在進入proxy，但proxy無法根據使用者流量的OrgID和其他後設資料詳細資訊來驗證使用者流量以應用策略並允許流量。

步驟 2:流量分析

對資料包捕獲的分析顯示：

- 正在從代理傳送TCP RST資料包
- 活動搜尋日誌未顯示失敗的流量
- 流量中的源IP已更改

步驟 3:NAT IP位址識別

調查發現NAT公有IP地址已從20.x.x.x更改為21.x.x.x。已更改的IP已作為註冊網路新增到使用者CSA UI中，在CSA門戶中註冊正確的IP後，SWG流量開始用於PAC檔案部署。

步驟 4:允許清單配置更新

已更新允許清單/防火牆規則以允許來自新NAT IP地址21.x.x.x的流量。

步驟 5:驗證

在用新的NAT IP地址更新允許清單後，正常的安全訪問流量被恢復，Web請求開始通過SWG代理正常運行。

原因

根本原因是使用者NAT公有IP地址從20.x.x.x更改為21.x.x.x。安全存取SWG代理設定為僅允許來自原始IP位址的流量，這會導致流量從新IP位址到達時連線重設。除此之外，主要線索是https://policy.test.sse.cisco.com顯示「401未授權」錯誤，即http連線請求正對Proxy命中，這同樣由PCAP確認，但Proxy無法根據使用者流量的OrgID和其他後設資料詳細資訊來驗證使用者流量，從而應用策略並允許流量。這導致代理終止與TCP RST資料包的連線，從而阻止處理成功的Web請求。

在註冊網路下的使用者CSA UI中新增了新的NATed IP，以解決SWG PAC檔案的Web流量問題。

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）。