針對具有SAML身份驗證和基於PAC的流量轉發的共用電腦環境的安全網路網關(SWG)中的每使用者識別和策略實施挑戰

目錄

問題

在使用具有SAML身份驗證的安全訪問以及基於PAC或分支到Internet流量轉發的Cisco安全Web網關(SWG)部署中，只有登入到共用電腦的第一位使用者才能正確識別網路流量和策略實施。切換使用者後，即使禁用了IP代理選項並使用了PAC檔案，後續的網路流量仍會歸屬於初始使用者。DNS查詢通過Umbrella虛擬裝置反映正確的活動使用者，但Web和防火牆會永久將活動對映到前一使用者。請求是確定SWG是否支援每使用者識別以及共用電腦環境中的策略實施以確保正確的使用者對映。

環境

- 用於DNS解析的虛擬裝置。
- 使用者身份的SAML身份驗證。
- 流量轉發與PAC和沒有PAC檔案的混合。
- 啟用IP代理選項，為cookie代理繞過特定子網和主機。
- 內部裝置；無遠端終端或使用者。

解析

通過使用者教育和配置指南解決了此問題，並牢記以下幾點：

- 對PAC檔案使用Cookie代理標識。流量可以路由進入或離開網路隧道。
- 使用不帶PAC檔案的Cookie代理標識，但流量必須通過網路隧道路由。
- 要實施cookie代理的訪問策略必須在安全配置檔案中啟用SAML身份驗證。
- Cookie替代流量僅用於基於瀏覽器的流量。需要使用單獨的規則來標識來自電腦的非Cookie流量（例如，Teams或Webex流量），並將源標識用作網路。
- SWG模組必須不在使用中，Cookie代理才能正常工作。
- 當還啟用IP代理時，您必須在旁路清單（使用者和組 — 配置管理 — 高級設定）中新增要使用cookie代理的專用IP地址/子網。
- Cookie代理的旁路清單也會匹配較短的字首。例如，如果新增10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
- cookie代理支援使用者從電腦進行切換，而無需註銷以保留多個身份。

許多故障排除工作都是策略測試和活動搜尋。

原因

共用電腦環境中使用者標識不正確的根本原因主要是由於使用者教育。

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）。