非瀏覽器Web流量的安全訪問SSO身份驗證行為

目錄

問題

在通過IPsec連線實施思科安全訪問(CSA)時，需要澄清安全配置檔案中的SSO身份驗證行為。具體來說，當站點通過IPsec隧道連線時，會出現以下問題：哪種型別的出站Internet流量會觸發SSO身份驗證？

主要關注點是瞭解SSO身份驗證是否僅應用於通過TCP埠80和443進行的基於瀏覽器的Web訪問，或者它是否還擴展到非瀏覽器應用程式和裝置（如印表機或生成網路流量的非Windows終端）。對於來自所連線站點的不同型別的Web流量，何時會發生身份驗證提示和重定向到身份提供者(IdP)的行為，需要加以澄清。

環境

- 思科安全存取(CSA)部署
- 站點和CSA之間的IPsec隧道連線
- 配置了SSO身份驗證的安全配置檔案
- 包含印表機和非Windows終端等各種裝置的混合環境
- 已啟用HTTPS檢查
- 已配置SAML整合

解析

Cisco Secure Access中的SSO身份驗證行為專門設計為僅針對基於瀏覽器的網路流量。系統執行複雜的檢查過程以確定Web請求是否必須接受SSO身份驗證。

SSO身份驗證過程

將Web請求重定向到身份提供程式(IdP)之前，思科安全訪問使用HTTPS檢查來確定請求是否來自支援cookie的瀏覽器。此檢查過程是區分基於瀏覽器的Web流量和非瀏覽器Web流量的關鍵機制。

流量分類

基於瀏覽器的流量（接受SSO身份驗證）

- 來自支援cookie的瀏覽器的Web請求
- 來自瀏覽器應用程式的TCP埠80和443上的HTTP/HTTPS流量
- 通過HTTPS檢查cookie/瀏覽器檢測的流量

非瀏覽器流量（不受SSO身份驗證約束）

- 來自印表機和其他網路裝置的網路流量
- 不支援cookie或未被識別為瀏覽器的應用程式
- 生成未通過瀏覽器檢測的網路流量的非Windows終端
- 未通過HTTPS檢查瀏覽器驗證的任何Web流量

SSO身份驗證的前提條件

要使SSO身份驗證在環境中正常工作，必須滿足幾個先決條件：

- 工作SAML配置必須到位。
- 使用XFF的代理網路和/或沒有NAT的隧道（IP代理需要內部專用IP的可見性）。

- 必須啟用HTTPS檢查。
- 瀏覽器會話必須維護cookie（建議不要在會話結束時刪除cookie或不識別）。
- 跨位置的非重疊IP地址，如果存在重疊，則進行適當的站點分離。

原因

此行為是思科安全訪問中的設計行為。SSO身份驗證機制專門設計為通過Web瀏覽器進行互動式使用者會話的目標，同時允許自動系統和非互動式裝置訪問Web資源而不中斷身份驗證。此設計可防止對無法處理身份驗證重定向或基於cookie的會話的自動化流程、裝置管理介面和應用程式的中斷。

相關內容

- 配置SAML整合 — 為SAML啟用IP代理
- 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）。