針對漫遊客戶端SWG流量使用Duo IdP的Cisco安全訪問SSO身份驗證

目錄

問題

當嘗試對源自漫遊客戶端的安全訪問SWG（安全Web網關）流量使用Duo IdP的SSO身份驗證時，不會提示使用者進行Duo SSO身份驗證，並且使用者身份不會填充在Secure Access控制面板中。雖然網路流量與已啟用身份驗證的預期SWG規則匹配，並且流量已解密，但身份驗證流不會啟動漫遊客戶端流量，從而阻止使用者級別的Web活動標識。

具體來說，觀察到以下行為：

- SWG日誌記錄和活動顯示流量與預定的SWG規則匹配，目標流量已解密
- 日誌和Secure Access活動檢視僅顯示PC身份和網路身份；未發現Duo/SAML身份驗證質詢、SSO重定向或互動式提示
- 策略條目僅顯示漫遊和源資訊；在AD加入之前不存在任何使用者標識
- 當測試虛擬機器在故障排除期間加入Active Directory時，使用者身份在Secure Access Activity Search中變得可見，但Duo/SAML互動提示仍未出現

環境

- 具有SWG功能的思科安全訪問
- 安全客戶端版本5.1.13.177
- 為SSO身份驗證配置的Duo IdP
- 組織訂閱：安全訪問基礎
- 重新驗證Web代理間隔設定為Daily
- 在測試期間未使用PAC檔案或VPN
- 使用漫遊電腦配置的測試環境

解析

經過全面的分析和測試，確定由於產品設計限制，對於安全訪問漫遊客戶端流量不支援使用SAML的SSO身份驗證。為確認此限制，執行了以下故障排除步驟：

步驟 1:即時故障排除和行為複製

測試確認已正確執行SWG策略匹配和SSL解密，但未針對漫遊客戶端流量啟動身份驗證流程（互動式SAML/Duo SSO重定向和質詢）。

步驟 2:規則和源修改

在重新嘗試期間，SWG規則源已從漫遊電腦名稱更改為特定使用者身份。已重新啟動安全客戶端服務，並觀察到策略傳播。這些修改未解決身份驗證流問題。

步驟 3:Active Directory加入測試

測試虛擬機器已加入Active Directory以確定對使用者身份可見性的影響。雖然這使得使用者身份在Secure Access Activity Search中可見，但Duo/SAML互動提示仍未出現，確認此問題僅與使用者身份可見性有關。

步驟 4:DART捆綁包分析

收集並分析一個DART捆綁包。分析確認了SWG策略應用，但顯示漫遊客戶端流量沒有身份驗證流啟動，支援此行為是設計行為的結論。

步驟 5:Duo IdP配置驗證

已成功執行並完成對Duo IdP後設資料和配置的獨立測試，確認Duo配置本身不是問題的根源。

步驟 6:內部驗證

作為產品設計限制，對於安全訪問漫遊客戶端流量不支援使用SAML的SSO身份驗證。

結論:在安裝程式中未找到配置錯誤。缺乏互動式SSO提示的原因在於明確的產品支援限制，而不是可修復的配置問題。

原因

此問題是由產品設計限制引起的，其中Secure Access漫遊客戶端流量不支援使用SAML（包括Duo IdP整合）的SSO身份驗證。這是目前安全存取平台架構的固有限制，與組態問題或軟體錯誤無關。

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）。