對未對安全Web網關流量應用的SAML標識進行故障排除

目錄

簡介

本文檔介紹如何對未應用於分段Web網關流量的SAML標識進行故障排除。

SAML標識未應用於任何Web流量

如果未對任何Web流量應用SAML標識，請參閱Umbrella文檔以確保設定已正確完成。必須完成這些配置專案。

- 在「Deployments > SAML Configuration」中配置並測試了IdP設置
- 在「Deployments > Web Users and Groups」中調配的使用者/組的列表
- 必須在相關策略*的「Policies > Web Policies」中啟用SAML。
- 必須在「策略> Web策略」中的相關策略中啟用HTTPS解密

在Web策略中啟用SAML

必須在適用於相關網路或隧道標識的策略中啟用SAML和HTTPS解密。這些功能在識別使用者之前應用，因此重要策略是應用於「連線方法」的策略。

SAML策略必須按以下方式排序：

1. 高優先順序 — 策略適用於使用者/組。此策略決定已驗證使用者的內容/安全設定。
2. LOWER Priority — 策略應用於網路/隧道。此策略啟用了SAML並觸發初始身份驗證。

SAML標識未應用於特定網路流量

IP代理（預設行為）

為了提高使用者標識的一致性，建議啟用新的IP代理功能。此功能對所有新Umbrella SAML客戶自

動啟用，但需要為現有Umbrella客戶手動啟用。

IP代理使用Internal IP > Username資訊的快取，這意味著可以將SAML標識應用於所有型別的請求：即使非Web瀏覽器流量、不支援cookie的流量以及不受SSL解密約束的流量。

IP代理可以極大地提高使用者標識的一致性，減輕管理負擔。

請注意，IP代理具有以下要求:

- 必須使用Umbrella網路隧道或代理鏈部署和X-Forwarded-For報頭來提供內部IP可視性。 這與Umbrella的託管PAC檔案無關
- IP代理不能在共用IP地址場景中使用（終端伺服器、快速使用者交換）
- 必須在瀏覽器中啟用Cookie。 初始身份驗證步驟仍然需要Cookie。

Cookie代理（禁用IP代理）

禁用IP代理後，使用者身份將僅適用於來自受支援的Web瀏覽器的請求，並且Web瀏覽器必須支援cookie。 SWG要求瀏覽器支援每個請求的Cookie，以便在Cookie中跟蹤使用者的會話。遺憾的是，這意味著在這種模式下，不應期望每個Web請求與使用者關聯。

在這些情況下SAML不適用，而是使用分配給網路/隧道標識的預設策略：

- 非Web瀏覽器流量
- 禁用cookie 或IE Enhanced Security Configuration的網路瀏覽器
- 不支援cookie的OCSP/證書吊銷檢查
- 不支援Cookie的個人Web請求。在某些情況下，由於網站的內容安全策略，會阻止個人請求Cookie。 此限制適用於許多常用的內容交付網路。
- 使用SAML旁路清單從SAML繞過目標域/類別時
- 當使用Umbrella Selective Decryption 清單從HTTPS解密繞過目標域/類別時。

由於這些限制，必須在相關網路/隧道策略中配置適當的最低訪問級別。預設策略必須允許關鍵業務應用程式/域/類別和內容交付網路。

或者，使用IP Surrogates系統提高相容性。

SAML旁路

在極少數情況下需要例外。 當SWG對請求進行SAML身份驗證但應用程式或網站無法支援時，這是必要的。 在以下情況下會發生這種情況：

- 非瀏覽器應用使用類似Web瀏覽器的使用者代理
- 指令碼無法處理cookie測試執行的HTTP重定向
- 瀏覽會話中的第一個請求是POST請求(例如，單一登入URL)，無法正確重定向至SAML

SAML Bypass List是在仍保持安全性（檔案檢查）的情況下從驗證中排除域的最佳方式。

- SAML Bypass List例外必須應用於影響用於連線的網路/隧道的正確策略
- SAML Bypass List不會自動允許流量。 相關策略中的類別或目標清單仍必須允許域。

SAML旁路 — 注意事項

新增熱門網站和「首頁」的排除項時，必須考慮對SAML的影響。當瀏覽會話中的第一個請求是對HTML頁面的GET請求時，SAML效果最佳。 例如： http://www.myhomepage.tld。 此請求被重定向以進行SAML身份驗證，後續請求採用IP代理或cookie的相同身份。

繞過SAML的首頁可能會觸發一個問題，其中SAML系統看到的第一個請求是針對背景內容。例如，http://homepage-content.tld/script.js。這是一個問題，因為在瀏覽器載入嵌入內容（如JS檔案）時，無法將SAML重定向到SAML登入頁。 這表示頁面呈現或操作不正確，直到使用者轉到其他站點來觸發登入。

在考慮熱門網站和首頁時，請考慮以下選擇：

- 除非必要，否則請勿將首頁和常用網站從SAML或HTTPS解密中排除
- 如果排除首頁，則必須排除該站點使用的所有域（包括背景內容）以避免SAML不相容

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）。