Umbrella SWG的SAML旁路現在可用

目錄

簡介

本檔案將說明Umbrella安全Web閘道(SWG)的SAML略過可用性。

概觀

現在可以通過域或IP地址繞過SAML使用者身份質詢。

使用SAML獲取使用者身份有時可能會導致與特定型別的Web請求不相容。例如，非瀏覽器應用程式或IoT（物聯網）裝置流量可能無法正確響應SAML身份質詢。當無法獲得使用者標識時，請求會被阻止。如果已知無法正確響應SAML質詢的原因是不相容問題，可以新增SAML旁路來防止將來發生SAML質詢。

對目標繞過SAML意味著使用者身份無法與基於使用者的策略匹配。其他標識型別（如網路或隧道）用於匹配Web策略以及基於策略結果允許或阻止的請求。

現在可以使用名為「SAML Bypass」的新目標清單型別。通過編輯SAML設定，可以將目標清單新增到規則集。

有關配置SAML旁路的更多資訊，請參閱Umbrella文檔 —

1. 新增SAML繞過目標清單 — https://docs.umbrella.com/umbrella-user-guide/docs/add-a-saml-bypass-destination-list
2. 將規則集新增到Web策略 — https://docs.umbrella.com/umbrella-user-guide/docs/add-a-rules-based-policy

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）。