适用于Umbrella SWG的SAML旁路现已可用

目录

简介

本文档介绍适用于Umbrella安全Web网关(SWG)的SAML旁路可用性。

概述

现在可以通过域或IP地址绕过SAML用户身份质询。

使用SAML获取用户身份有时会导致与特定类型的Web请求不兼容。例如，非浏览器应用或IoT（物联网）设备流量可能无法正确响应SAML身份质询。当无法获取用户身份时，请求会被阻止。如果已知无法正确响应SAML质询的原因是不兼容问题，可以添加SAML旁路来防止将来发生SAML质询。

绕过目标的SAML意味着用户身份无法与基于用户的策略匹配。其他身份类型（如网络或隧道）用于匹配Web策略以及根据策略结果允许或阻止的请求。

名为“SAML Bypass”的新目标列表类型现在可用。通过编辑SAML设置，可以将目标列表添加到规则集。

有关配置SAML旁路的详细信息，请参阅Umbrella文档 —

1. 添加SAML旁路目标列表 — https://docs.umbrella.com/umbrella-user-guide/docs/add-a-saml-bypass-destination-list
2. 将规则集添加到Web策略 — https://docs.umbrella.com/umbrella-user-guide/docs/add-a-rules-based-policy

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。