对安全访问的SWG SAML身份验证Cookie替代问题进行故障排除

目录

问题

当应用执行跨域重定向或从多个相关域获取资源时，通过Cisco安全访问访问Web应用的用户会遇到身份验证失败。问题表现为：

- Web应用程序在SAML身份验证后无法正确初始化。
- 对跨域资源的请求（CORS错误）被默认拒绝规则阻止。
- 活动日志，显示归因于网络或隧道身份而不是经过身份验证的用户身份的请求。
- 浏览器控制台中出现重定向请求的CORS策略错误。
- 使用IP代理时，应用程序在物理计算机上正常工作，但在使用Cookie代理的Citrix虚拟桌面环境中失败。

当在虚拟环境中使用cookie替代身份验证时，问题会特别出现，在跨域资源读取期间，重定向的请求会丢失用户到cookie的映射。

环境

- 配置了SAML身份验证的思科安全访问
- 为Citrix虚拟桌面环境启用Cookie替代身份验证
- 用于物理计算机的IP代理身份验证
- 执行跨域重定向的Web应用（Web开发人员工具控制台日志中的CORS错误）
- 同时具有物理和虚拟桌面基础设施的混合环境

分辨率

通过对受影响的网络范围实施IP代理旁路，从而在跨域重定向期间允许正确的用户身份属性，从而解决了此问题。

步骤 1：导航到IP代理配置

访问Cisco Secure Access控制面板并导航到Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogate。

步骤 2：启用内部网络旁路

将受影响的网络范围添加到内部网络旁路配置。这使系统能够维护来自这些网络的请求的用户身份属性。

步骤 3：测试应用程序访问

实施IP代理后，测试受影响的应用程序，以验证：

- 跨域资源请求正确归属于用户身份
- 应用程序成功初始化，无CORS错误
- 活动日志显示所有请求的用户身份，而不是基于网络或隧道的身份

步骤 5：监控活动报告

使用Monitor > Activity Search验证请求现在是否正确归属于经过身份验证的用户，而不是显示为基于网络或隧道的身份。

原因

出现此行为的原因是在虚拟化环境中结合Cookie代理的SAML身份验证的性质。当Web应用执行跨域重定向或从多个相关域获取资源时，重定向的请求可能不会以思科安全访问可以关联回经过身份验证的用户会话的方式传送替代Cookie。

出现根本原因的原因如下：

- Cookie替代依赖于浏览器通过重定向的cookie传播。
- 跨域安全策略(CORS)可以在307/重定向场景期间删除cookie。
- 浏览器安全措施可防止在不同域之间共享cookie。
- 虚拟桌面环境处理cookie传播的方式与物理机不同。

一旦用户到cookie的映射丢失，安全访问无法将请求解析为经过身份验证的用户，导致请求仅归属于注册网络/作为源的不同身份，随后被默认拒绝规则阻止。

相关内容

- 思科技术支持和下载

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）。