针对采用SAML身份验证和基于PAC的流量转发的共享计算机环境的安全网络网关(SWG)中的每用户识别和策略实施挑战

目录

问题

在使用具有SAML身份验证的安全访问以及基于PAC或分支到Internet流量转发的Cisco安全Web网关(SWG)部署中，只有登录到共享计算机的第一位用户才被正确识别为进行Web流量和策略实施。切换用户时，即使禁用了IP代理选项并使用了PAC文件，后续的Web流量仍继续归属于初始用户。DNS查询通过Umbrella虚拟设备反映正确的活动用户，但Web和防火墙日志会持续将活动映射到前一用户。请求用于确定SWG是否支持每用户识别和策略实施，以及共享计算机环境以确保正确的用户映射。

环境

- 用于DNS解析的虚拟设备。
- 用户身份的SAML身份验证。
- 流量转发与PAC和没有PAC文件的混合。
- 启用IP代理选项，为Cookie代理绕过特定子网和主机。
- 内部设备；无远程终端或用户。

分辨率

通过用户教育和配置指南解决了此问题，并牢记以下几点：

- 对PAC文件使用Cookie替代标识。流量可以路由进入或离开网络隧道。
- 使用没有PAC文件的Cookie替代标识，但流量必须通过网络隧道路由。
- 要实施Cookie替代的访问策略必须在安全配置文件中启用SAML身份验证。
- Cookie替代流量仅用于基于浏览器的流量。需要使用单独的规则来标识来自计算机的非Cookie流量（例如，Teams或Webex流量），并将源标识用作网络。
- SWG模块不能使用，Cookie代理才能正常工作。
- 当还启用IP代理时，必须在旁路列表（用户和组 — 配置管理 — 高级设置）中添加要使用cookie代理的专用IP地址/子网。
- Cookie替代的旁路列表也匹配较短的前缀。例如，如果添加10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
- Cookie替代支持用户从计算机进行切换，而无需注销以保留多个身份。

许多故障排除工作都是策略测试和活动搜索。

原因

在共享计算机环境中，用户标识不正确的根本原因主要是由于用户教育。

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）。