Cisco安全访问SSO身份验证，使用双核IdP实现漫游客户端SWG流量

目录

问题

当尝试对源自漫游客户端的安全访问SWG（安全网络网关）流量使用双点IDp的SSO身份验证时，不会提示用户进行双点SSO身份验证，并且用户身份不会填充在安全访问控制面板中。尽管网络流量与启用了身份验证的预期SWG规则匹配，且流量已解密，但身份验证流不会为漫游客户端流量启动，从而阻止用户级别的网络活动识别。

具体而言，观察到以下行为：

- SWG日志记录和活动显示流量与预期的SWG规则匹配，目标流量已解密
- 日志和“安全访问”活动视图仅显示PC身份和网络身份；未观察到双核/SAML身份验证质询、SSO重定向或交互式提示
- 策略条目仅显示漫游和源信息；在AD加入之前不存在任何用户身份
- 当测试虚拟机在故障排除期间加入Active Directory时，用户身份在Secure Access Activity Search中变得可见，但Duo/SAML交互提示仍未出现

环境

- 具有SWG功能的思科安全访问
- 安全客户端版本5.1.13.177
- 为SSO身份验证配置双IdP
- 组织订用：安全访问基本版
- 重新验证Web代理间隔设置为“每日”
- 测试期间未使用PAC文件或VPN
- 使用漫游计算机配置的测试环境

分辨率

经过综合分析和测试，确定由于产品设计限制，安全访问漫游客户端流量不支持使用SAML的SSO身份验证。为了确认此限制，执行了以下故障排除步骤：

步骤 1：实时故障排除和行为复制

测试确认SWG策略匹配和SSL解密正确，但是没有为漫游客户端流量启动身份验证流程（交互式SAML/Duo SSO重定向和质询）。

步骤 2：规则和源修改

在重试过程中，SWG规则源已从漫游计算机名称更改为特定用户身份。安全客户端服务已重新启动，并观察到策略传播。这些修改未解决身份验证流问题。

步骤 3：Active Directory加入测试

测试虚拟机已加入Active Directory以确定对用户身份可视性的影响。虽然这使得用户身份在安全访问活动搜索中可见，但Duo/SAML交互提示仍未出现，确认此问题仅与用户身份可视性相关。

步骤 4：DART捆绑包分析

收集并分析一个DART套件。分析确认了SWG策略应用，但显示漫游客户端流量没有身份验证流启动，支持此行为是设计行为的结论。

步骤 5：双IdP配置验证

对双核IdP元数据和配置的独立测试已成功执行并完成，确认双核IdP配置本身不是问题的根源。

步骤 6：内部验证

作为产品设计限制，安全访问漫游客户端流量不支持使用SAML的SSO身份验证。

结论:在设置中没有发现配置错误。缺乏交互式SSO提示的原因在于明确的产品支持限制，而不是可修复的配置问题。

原因

该问题由产品设计限制引起，其中对于安全访问漫游客户端流量不支持使用SAML（包括双核IdP集成）的SSO身份验证。这是当前安全访问平台架构的固有限制，与配置问题或软件缺陷无关。

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）。