

ChromeOS SWG Web保护不起作用，活动搜索中不会连续显示任何Web日志

目录

问题

尽管似乎已为组织启用安全网络网关(SWG)保护，但是未为ChromeOS用户生成Web日志。受影响的ChromeOS终端仅显示DNS级保护，在“活动搜索”界面中看不到任何SWG/Web日志记录活动。用户遇到完全没有网络流量日志的情况，而SWG保护状态表明它已启用。

在调查期间，诊断日志显示[HTTP 407 \(需要代理身份验证\) 错误响应导致终端 http://407.checkumbrella.com](#)重复同步失败。ChromeOS客户端/扩展无法正确通过代理服务进行身份验证，导致无法正确激活SWG保护并随后生成网络日志。

环境

- 思科安全访问
- 具有思科安全访问客户端/扩展的ChromeOS终端
- 用于ChromeOS管理的Google管理控制台

分辨率

通过为包含受影响的ChromeOS用户的Google Admin Organization Unit(OU)启用基本身份验证方案，并执行策略重新加载以激活SWG保护，问题得以解决。

步骤 1：日志收集和分析

已收集的HAR捕获（查看网络和控制台日志）以确定同步失败的根本原因。在尝试与思科安全访问服务同步时，日志显示反复的身份验证失败。

步骤 2：为Google管理员OU启用基本身份验证

在Google Admin控制台中，导航到包含受影响的ChromeOS用户的组织单位，并启用基本身份验证方案。这允许ChromeOS客户端/扩展正确通过思科安全访问代理服务进行身份验证。

步骤 3：策略重新加载和验证

启用基本身份验证后，在受影响的ChromeOS设备上执行策略重新加载。通过检查保护状态，验证SWG保护是否变为活动状态。SWG保护现在必须显示为活动状态，而不是仅显示DNS级保护。

步骤 4：验证

测试受影响的ChromeOS用户的Web浏览活动，并确认现在正在生成Web日志并在“活动搜索”界面中显示。日志必须显示适当的网络流量检查和通过SWG服务进行日志记录。

原因

ChromeOS客户端/扩展已禁用包含受影响用户的Google管理员组织单元的基本身份验证方案。如果未启用基本身份验证，ChromeOS设备将无法使用思科安全访问代理服务进行正确身份验证，从而在尝试同步期间导致HTTP 407（需要代理身份验证）错误。这阻止了SWG保护正常激活，导致设备回退到仅DNS保护并阻止生成网络日志。

相关内容

- [排除故障并收集思科安全访问的基本信息](#)
- [思科安全访问Chromebook客户端](#)

- [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）。