

通过安全访问SWG访问应用程序时出现HTTP 429速率限制和连接错误

目录

问题

用户尝试通过Cisco安全访问SWG（安全Web网关）访问应用时，会遇到HTTP 429速率限制错误，例如https://xxxx.com。此问题会影响公司管理的笔记本电脑，并且是在案例打开前大约两周开始出现的。用户在尝试登录时或在身份验证成功后访问某些应用程序功能时会遇到这些错误。

此外，当域添加到安全访问旁路列表时，用户在OTP（一次性密码）输入期间会遇到HTTP 500服务器错误，或者在流量不再通过SWG IP范围(151.186.x.x)时遇到一般连接错误。

应用所有者确认，最近服务器端没有更改速率限制，并且问题似乎与源自Cisco Secure Access SWG出口IP地址的流量有关。

环境

- 支持SWG的思科安全访问（以前称为Cisco Umbrella）
- 采用Cisco SSE（安全服务边缘）客户端的企业管理型笔记本电脑
- 交换机出口IP范围：151.186.x.x
- 数据中心:AWS Singapore(Asia Pacific 1)和AWS US West（俄勒冈）
- 应用:<https://sbstransit.aereacommercial.com>

分辨率

解决方法涉及实施旁路配置并与应用所有者协调以允许列出特定IP地址。

请按照以下步骤操作。

步骤 1：验证当前SWG行为

通过从受影响设备访问此URL检查当前策略和出口IP信息：

<https://policy.test.sse.cisco.com/?host=https://sbstransit.aereacommercial.com>

这显示当前使用的SWG出口IP（通常为151.186.x.x范围），并确认流量正在通过安全访问SWG进行处理。

步骤 2：将域添加到安全访问旁路列表

导航到Cisco Secure Access控制面板中的Internet Settings > Bypass Secure Access，添加有问题的域以绕过DNS和SWG检测：

sbstransit.aereacommercial.com

步骤 3：测试从非公司网络访问

从流量不通过安全接入SWG（151.186.x.x范围）出口的网络测试应用访问。这可以通过个人设备或临时禁用SSE客户端来完成。

通过访问以下网址识别公有ISP IP地址：

<https://whatismyip.com>

步骤 4：与应用所有者协调IP许可列表

向应用程序所有者提供已识别的公有ISP IP地址，并请求在应用程序端允许列出此IP。这有助于验证应用是否正在实施影响安全访问SWG出口IP的基于IP的限制。

步骤 5：检验分辨率

在应用所有者实施IP许可列表后，测试访问行为，确认用户能够成功访问应用，而不会遇到HTTP 429或连接错误。

原因

应用似乎根据源IP地址实施速率限制或访问限制。当多个用户通过Cisco Secure Access SWG访问应用时，所有流量似乎都源自共享SWG出口IP范围(151.186.x.x)。这会导致应用的速率限制机制触发，因为它发现来自单个IP地址或IP范围的请求过多。

公司管理的设备继续通过SSE客户端路由流量，即使连接到个人网络，也会保持触发应用限制的相同出口IP行为，这一事实加剧了这一问题。

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）。