排除PAC文件的安全访问SWG代理连接问题

目录

问题

用户尝试使用SWG（安全Web网关）代理URL swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com通过思科安全访问访问网站时遇到了连接故障。

具体症状包括：

- Web请求（例如https://www.google.com）失败，浏览器中出现连接错误
- 活动搜索日志中未显示流量
- 从客户端源IP/客户端出口IP到目标终端观察到服务器重置：
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- 问题开始于美国东部标准时间上午9:30
- SWG主机名的DNS解析工作正常
- 通过端口443成功通过Telnet连接到swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.com
- 外部防火墙未阻止与目标IP的连接

数据包捕获分析显示来自代理的TCP RST数据包，表示在代理级别终止连接。

环境

- 技术：思科安全访问(SSE)
- 组件：安全Web网关(SWG)

- SWG代理URL:swg-url-proxy-https-8385532.sseproxy.qq.op endns.com
- 受影响的端口：443 和 80
- 原始NAT IP:20.x.x.x
- 更新的NAT IP:21.x.x.x
- 中的AWS ELB终端，例如：欧盟中部或美国东部地区
- 将浏览器定向到SWG代理的WPAD配置

分辨率

通过更新allow-list配置以包含正确的NAT IP地址解决了此问题。

下面几节中介绍的步骤用于识别和解决问题。

步骤 1：诊断数据收集

收集的数据包捕获和WPAD脚本配置，用于分析流量和代理配置。

除此之外，主要的线索是https://policy.test.sse.cisco.com显示“401 unauthorized”错误。这意味着http连接请求正在访问代理，但代理无法根据用户的OrgID和其他元数据详细信息对用户流量进行身份验证，从而应用策略并允许流量。

步骤 2：流量分析

对数据包捕获的分析显示：

- 从代理发送TCP RST数据包
- 活动搜索日志未显示失败的流量
- 流量中的源IP已更改

步骤 3：NAT IP地址标识

调查发现，NAT公有IP地址已从20.x.x.x更改为21.x.x.x。已更改的IP已作为注册网络添加到用户CSA UI中，在CSA门户中注册正确的IP后，SWG流量开始用于PAC文件部署。

步骤 4：允许列表配置更新

已更新允许列表/防火墙规则，以允许来自新NAT IP地址21.x.x.x的流量。

步骤 5：确认

使用新的NAT IP地址更新允许列表后，正常的安全访问流量会恢复，Web请求开始通过SWG代理正常运行。

原因

根本原因是用户NAT公有IP地址从20.x.x.x更改为21.x.x.x。安全访问SWG代理配置为仅允许来自原始IP地址的流量，从而导致流量从新IP地址到达时连接重置。除此之外，主要线索是https://policy.test.sse.cisco.com显示“401 unauthorized”错误，该错误表示http连接请求正在访问代理，这同样由PCAP确认，但代理无法根据用户流量的OrgID和其他元数据详细信息来验证用户流量，从而应用策略并允许流量。这导致代理终止与TCP RST数据包的连接，从而阻止处理成功的Web请求。

在注册网络下的用户CSA UI中添加了新的NATed IP，以解决SWG PAC文件的Web流量问题。

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）。