使用SSE NATaaS出口IP时，Web应用防火墙阻止访问地域限制的网站

目录

问题

尝试通过思科安全访问(SSE)访问特定网站会导致阻止消息“对不起，您被阻止了”。

使用常规家庭Wi-Fi连接时，可以访问该站点。怀疑原因是远程网站仅允许从特定IP地址范围进行访问，而SSE出口IP似乎不在允许的范围内。

技术调查显示，网站的Web应用程序防火墙(Cloudflare)阻止了整个安全访问NATaaS出口IP范围，而不考虑国家/地区。此问题可重复出现，在使用SSE出口IP时始终出现。

环境

- 技术：采用统一策略（互联网策略、私有策略、DLP策略、RBI、安全配置文件）的思科安全访问(SSE)
- 访问路径：SSE的任何数据中心
- 地理限制网站
- 安全控制：目标网站上的Web应用防火墙(Cloudflare)
- 从远程网络（SSE出口IP）到本地网络（家庭Wi-Fi）的互联网访问
- 问题发生时安全访问部署没有任何更改
- 观察到的错误消息：“对不起，您已被阻止”

分辨率

要解决远程站点阻止Cisco安全访问NATaaS出口IP而引起的访问问题，建议使用此工作流。这些步骤可确保采用系统化的方法来识别阻止的性质，并探索可能的变通方法或解决方案。

第1步：确认错误消息并阻止行为

通过SSE访问站点时，请注意以下消息：

```
sorry you have been blocked
```

第2步：验证来自不同网络的网站可访问性

从以下网址访问该网站：

- 任何SSE数据中心（受阻）
- 常规家庭Wi-Fi连接（可访问）

第3步：确定负责阻止的安全控制

技术观察：Cloudflare Web应用防火墙(WAF)阻止了整个安全访问NATaaS出口IP范围。

第4步：确认最终用户使用的访问路径

确定用于将流量发送到安全访问的方法：

- 漫游安全模块
- RAVPN隧道
- 站点到站点VPN隧道
- PAC部署

第5步：探索旁路或允许列表选项

检查以下选项是否可用：

- 与目标网站管理员建立业务关系或联系，请求允许SSE出口IP列表。
- 本文档中列出了SSE出口IP:
- 可以使用不同出口IP的备用访问路径未被WAF阻止。
- 从SSE代理绕过有问题的网站（具体步骤取决于用于将流量发送到安全访问的方法）

第6步：记录观察结果和后续步骤

记录以下观察结果：

错误消息

访问路径和相应结果

与远程站点管理员通信（如果允许列出）。

原因

此问题的根本原因是目标网站的Web应用程序防火墙(Cloudflare)正在主动阻止思科安全访问(SSE)NATaaS出口IP范围。此阻止不限于非以色列IP或地理位置过滤。相反，它针对与思科安全访问关联的整个已知出口IP范围，很可能是远程网站上的策略或安全配置问题。因此，无论其实际来源国家或最终用户位置如何，源自这些IP的任何流量都会被拒绝。

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）。