配置IP范围和防火墙以实现安全访问Webhook集成

问题

第三方集成成功加载到思科安全访问(SSE)控制面板中，但是基于Webhook的安全事件未在本地的HTTP连接器上接收以进行SIEM集成。组织需要明确思科SSE源IP范围（包括特定区域的IP），以正确配置防火墙规则并启用webhook事件交付。

环境

- 产品:思科安全访问(SSE)
- 技术：解决方案支持 — 安全访问报告和日志记录
- 集成类型：基于Webhook的第三方集成
- 目标连接器：本地HTTP连接器服务器

分辨率

要解决Cisco安全访问集成的Webhook传输问题，请配置防火墙规则以允许从指定SSE源IP范围到内部部署连接器的入站HTTPS流量。

思科SSE源IP范围

将防火墙配置为允许来自以下思科SSE源IP范围的入站HTTPS连接：

```
146.112.161.0/24
146.112.163.0/24
146.112.165.0/24
146.112.167.0/24
```

防火墙配置步骤

步骤 1：验证第三方集成状态

在SSE控制面板中导航至Admin（管理）> Third Party Integrations（第三方集成），并确认已为您的组织正确加载集成。

步骤 2：配置防火墙规则

创建防火墙规则以允许从SSE源IP范围到内部部署连接器服务器的入站HTTPS流量（端口443）。确保将规则同时应用于网络防火墙和互联网与连接器服务器之间的任何中间防火墙。

步骤 3：验证Webhook事件交付

实施防火墙更改后，监控您的本地HTTP连接器，以确认正在从Cisco SSE接收Webhook事件。

地区IP信息

思科SSE仅使用来自欧盟和美国地区的共享IP范围。所提供的IP范围包括两个区域部署，无论您的组织位于哪个主要区域，都必须进行配置。

原因

来自思科安全访问的Webhook事件被防火墙规则阻止，这些防火墙规则不允许从SSE源IP地址到本地HTTP连接器服务器的入站HTTPS连接。当SSE控制面板显示成功集成加载时，实际的Webhook交付需要特定的防火墙配置，以允许来自思科基础设施的流量到达用户连接器终端。

相关内容

- 思科安全访问文档
- 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）。