配置流量收集器的忽略列表功能

目录

简介

本文档介绍如何配置SNA流量收集器，以通过使用“忽略列表”拒绝来自特定导出器的传入netflow。

背景信息

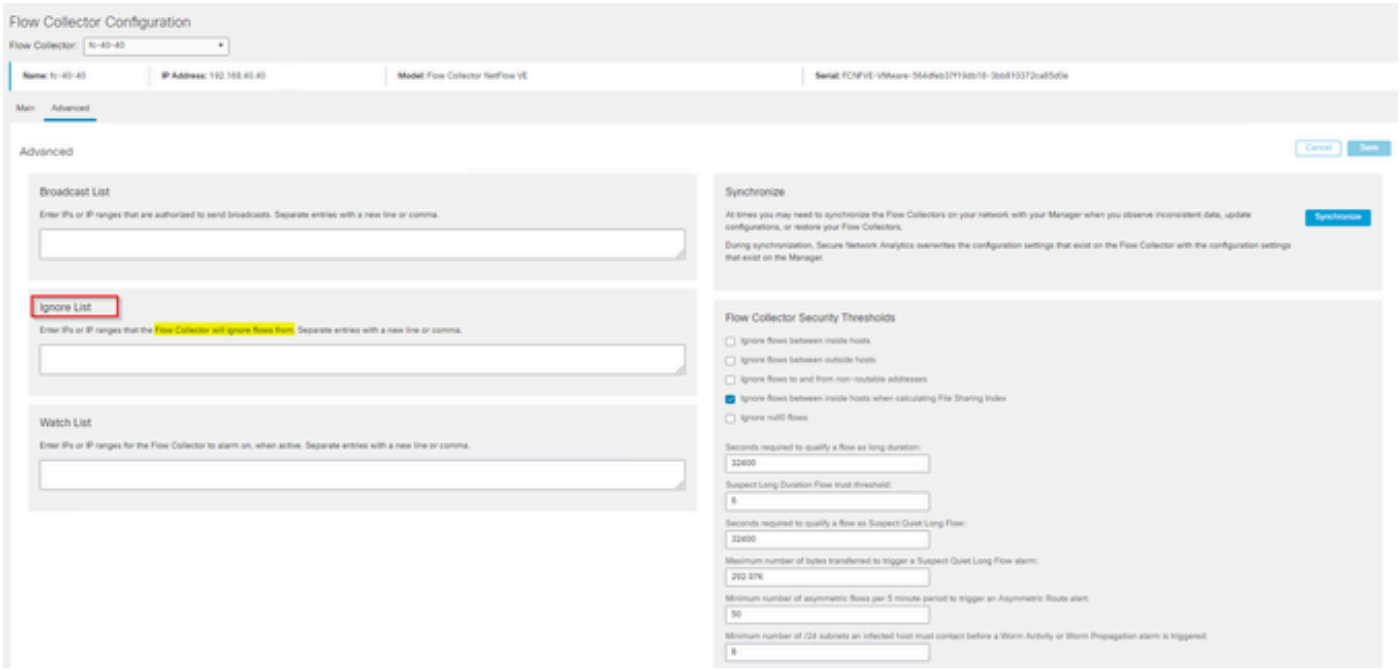
通常，会提出这样的问题：“是否有任何方法指示我的SNA流量收集器拒绝来自特定导出器的传入的netflow？”

答案是肯定的，这是通过使用流量收集器“忽略列表”功能完成的。

配置

忽略列表功能特定于流量收集器。 在SNA 7.x的更高版本中，此功能在SNA Manager Web UI上的流量收集器配置页面中提供。

使用此页可指定流收集器为其分配的Flow Collectorcompletelyignorestraffic的主机或子网数量不限。 如果Flow收集器看到属于这些IP地址的任何流量，则会从任何图形或表中排除该流量。 请确保您可以信任所有进出主机的流量被忽略。Secure Network Analytics不会分析此流量，也不会分析任何被伪装为包含这些主机的流量。如果网络上发起的攻击涉及这些主机/子网之一，则流收集器无法报告。



常见问题解答

忽略列表对智能许可的每秒流量(FPS)计算有何影响？

回答：将主机IP地址或范围添加到忽略列表可有效防止任何这些流量根据计算出的发送到SMC并用于智能许可证报告的FPS速率进行计数。 在SMC控制面板上显示的流趋势图中，不再显示/计算流。

当客户端处于分割隧道模式时，处理NVM流时如何使用忽略列表功能？

客户可以配置AnyConnect向我们发送网内和网外流量（也称为拆分隧道）。 网外流量使用终端本地IP地址，该地址很可能包含重叠的IP。SNA不支持重叠IP，因此建议使用Ignore list功能来避免分割隧道问题，从而保留基于NVM的流的检测优势。

在本使用案例中，我们配置“忽略列表”以防止网络外的NVM流从流缓存→ flow_stats、流搜索、自定义安全事件

1. 将IP地址和网络掩码(例如，添加192.168.1.0/24、127.0.0.1/24)添加到忽略列表中
2. 验证nvm_flows是否仍填充有NVM流
3. 如果src或dst IP在Ignore List中，请验证flow_stats没有NVM流

是否可以使用忽略列表忽略来自整个导出器的流？否则，因为忽略列表基于流数据而不是导出器数据，所以将导出器IP地址添加到忽略列表将会有效地忽略流数据，其中导出器IP被列为流的源或目标，而不是忽略来自该特定导出器的所有流记录

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）。