在安全分析中配置SLF和SQLF安全事件

目录

简介

本文档介绍可用于调整可疑长流(SLF)和可疑安静长流(SQLF)安全事件的两个参数。

背景信息

可疑长流事件是由Secure Analytics生成的特定类型的安全事件，旨在检测主机之间比正常会话更长的会话。可疑长流事件有两种不同的类型；可疑的Long Flow和可疑的Quiet Long Flow。

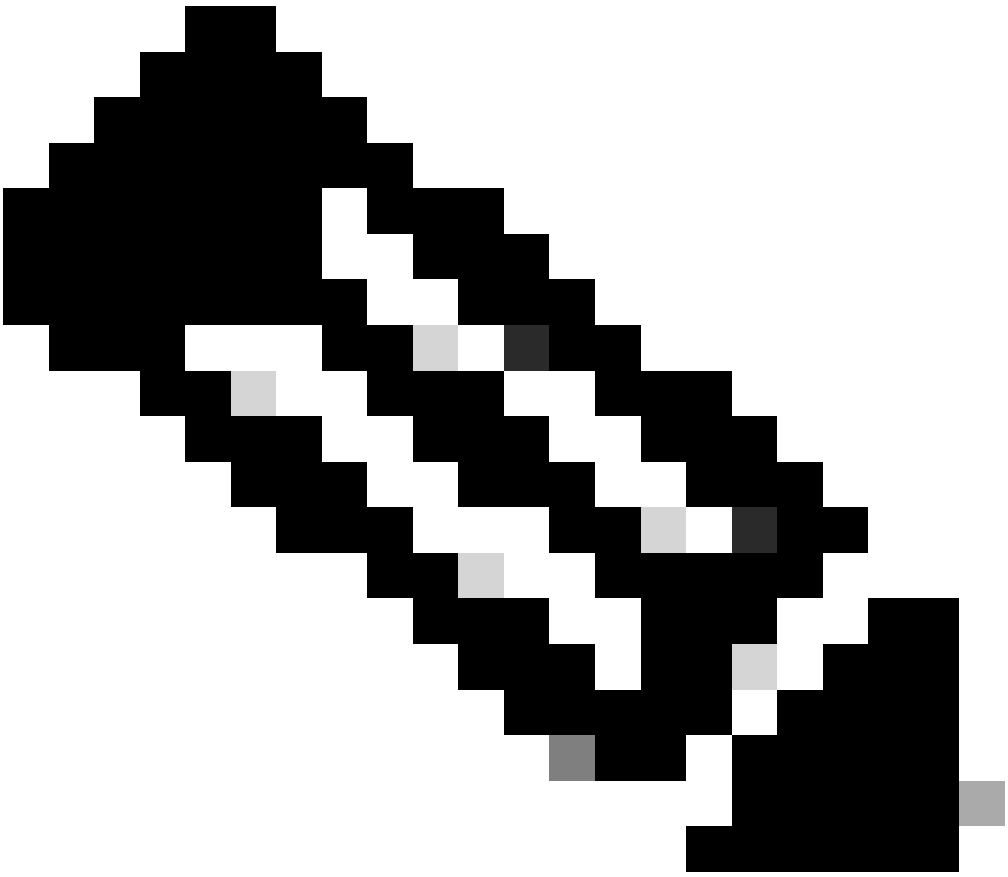
假设您通过隐式VPN将笔记本电脑连接到家庭PC长达3天，但家庭PC和笔记本电脑通常都不会进行长流连接。流量收集器检测到此异常，并根据通过的流量和流量的持续时间触发安全事件。这些事件旨在识别长时间运行的流和传递最小流量的长时间运行的流。

调整/配置

主要有2个流量收集器配置参数负责控制这两个事件的行为。

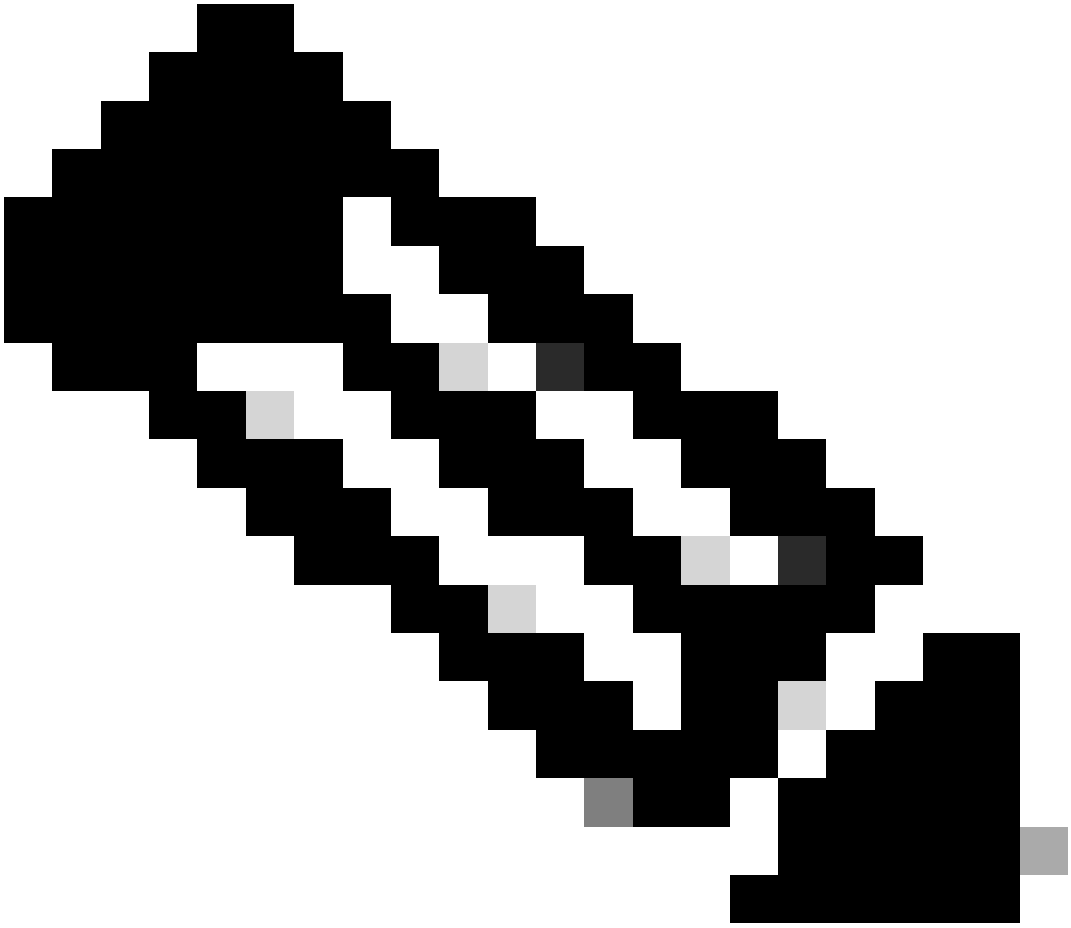
可以通过访问Manager设备的WebUI中的配置>流量收集器>高级页面来调整这些设置。

- 将流限定为长持续时间的设置所需的秒数控制可疑长流事件的行为。



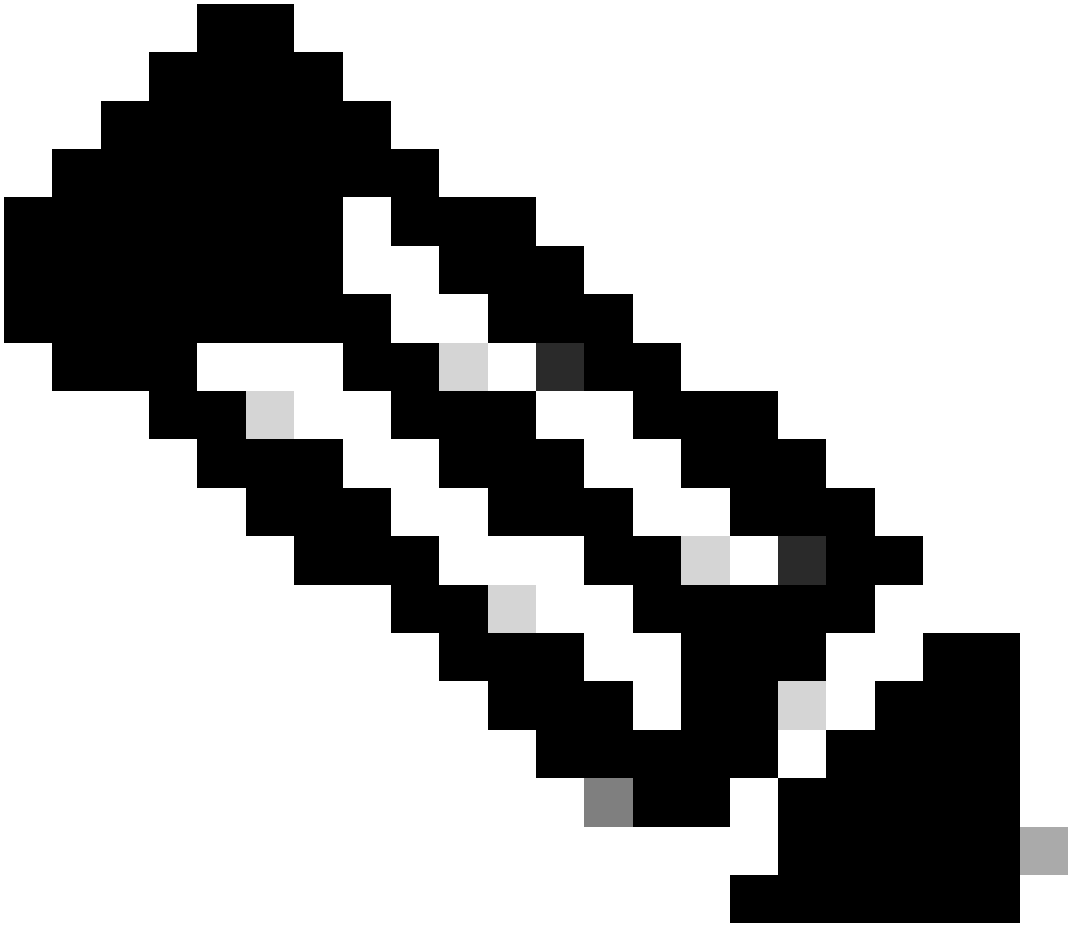
注意：WebUI中的此配置选项设置流收集器lc_thresholds.txt配置文件中的long_flow_duration参数。

- 将流限定为可疑安静长流设置所需的秒数控制可疑安静长流事件的行为。



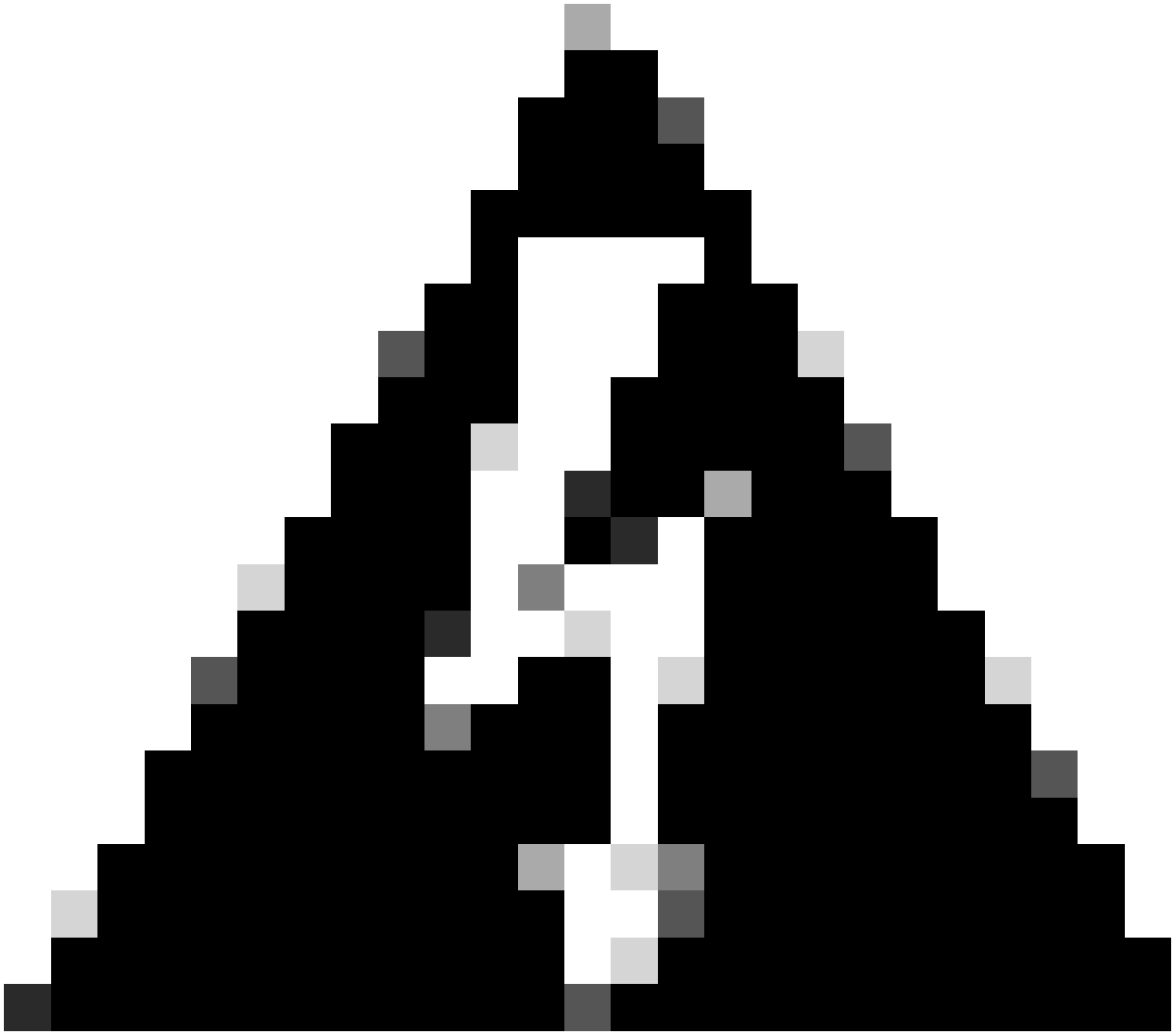
注意：WebUI中的此配置选项设置流收集器lc_thresholds.txt配置文件中的quiet_long_flow_duration参数。

两个计数器的默认值为32400 秒（9小时）。



注意：关于更改这些计数器，相关CDET:

Cisco Bug ID CSCwm05128



警告：这仅影响v7.5.1或早期版本。

此缺陷规定可疑静默长流必须首先也是可疑长流。这意味着，如果将将验证流为可疑的静默长流所需的秒数更改为短于验证流为长持续时间设置所需的秒数，则可能会出现意外的结果。

如果更改其中一项或两项高级设置，则可能导致长流检测失败。

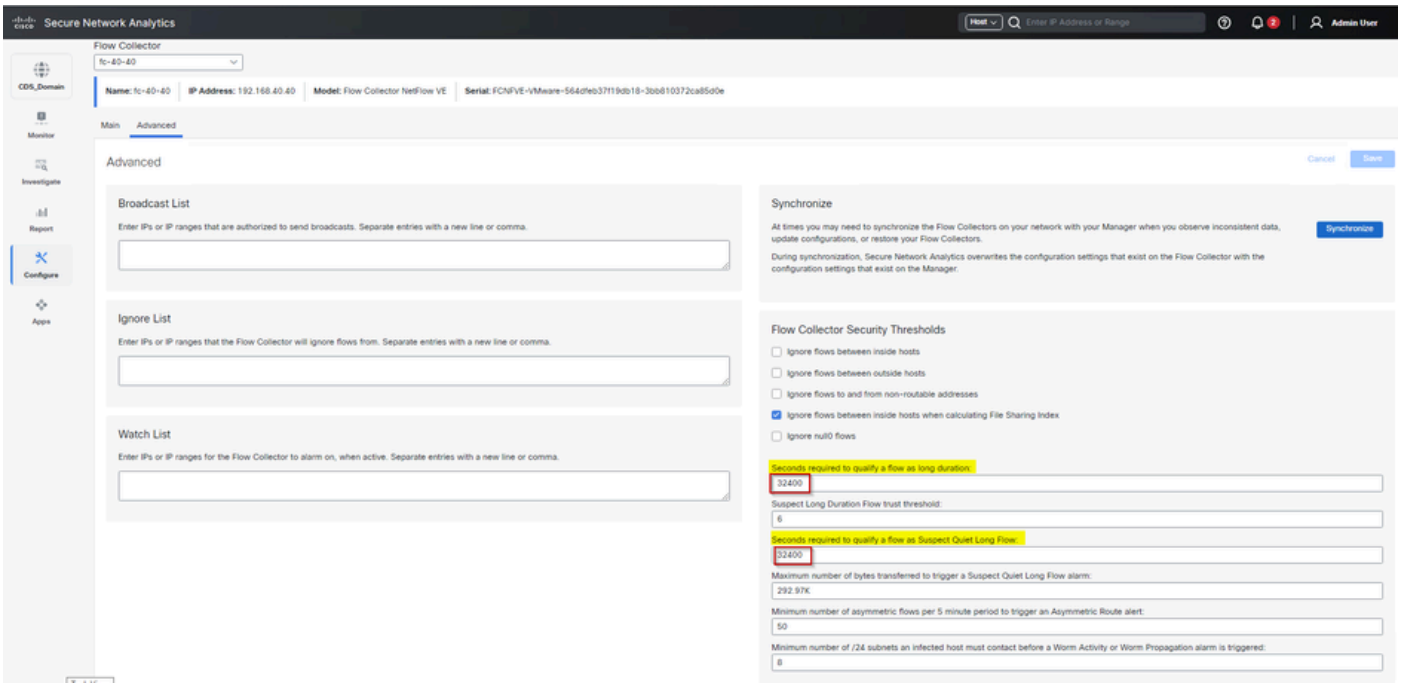
由于静默长流在定义上也必须是一个长流，正确处理这两个设置时的逻辑是首先使流超过长流要求，然后再测试它是静默长流。

例如，如果long_flow_duration保留为默认值9小时，而quiet_long_flow_duration设置为较低值（例如8小时），则在流至少达到9小时之前，引擎不会引发无声长持续时间流事件。

或者，如果long_flow_duration的默认值是9小时，而quiet_long_flow_duration设置为10小时，则此配置将有效禁用静默持续时间长流事件（除非流是持续时间大于quiet_long_flow_duration 10小时的单个导出）。

解决方案

这两个高级设置需要设置为相同的所需值，或者quiet_long_flow_duration必须始终为>= long_flow_duration。



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）。