Configure SLF and SQLF Security Events in Secure Analytics

Contents

Introduction

This document describes two parameters that can be used to tune the suspect long flow (SLF) and suspect quiet long flow (SQLF) security events.

Background Information

A Suspect Long Flow event is a specific type of security event generated by Secure Analytics which is designed to detect longer than normal conversations between hosts. There are two different types of the Suspect Long Flow event; Suspect Long Flow and Suspect Quiet Long Flow.

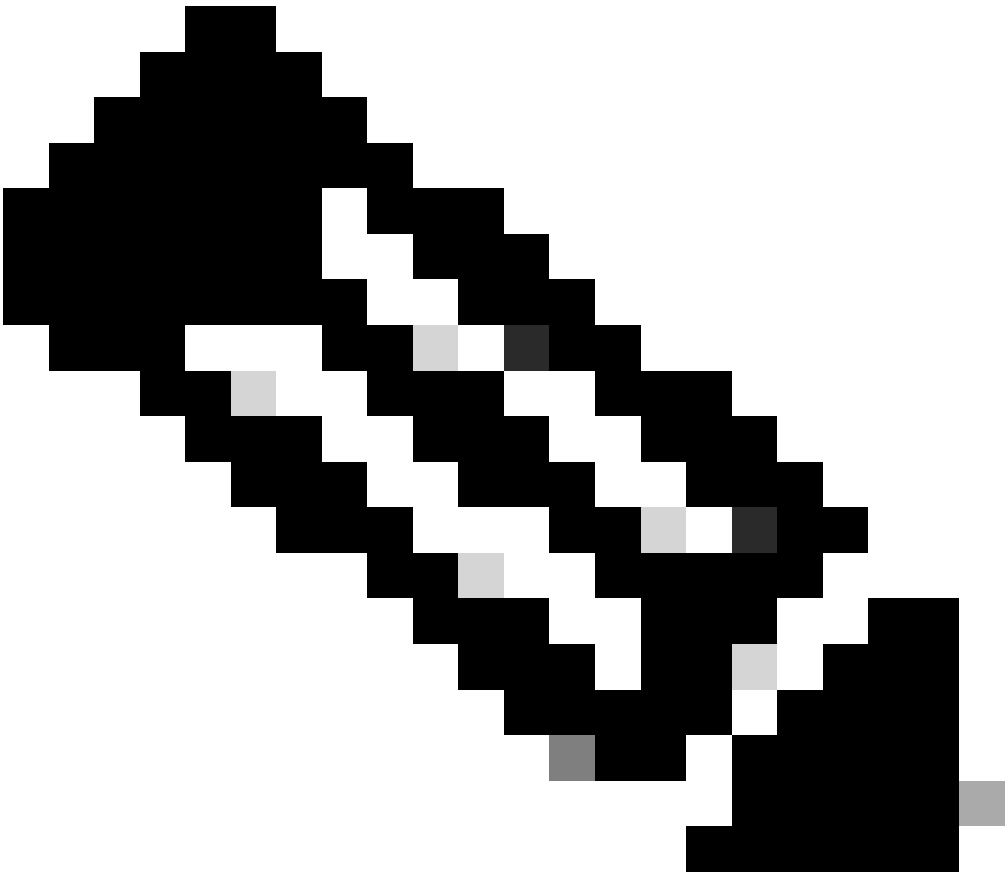
Consider that you connect your laptop to your home PC via a covert VPN for 3 days, but neither the home PC nor the laptop normally carry on long flow connections. The Flow Collector detects this abnormality and triggers a security event depending on the amount of traffic passed and the duration of the flow. These events are intended to identify long running flows and long running flows that are passing minimal traffic.

Tuning/Configuration

There are primarily 2 flow collector configuration parameters which are responsible for controlling the behavior of these two events.

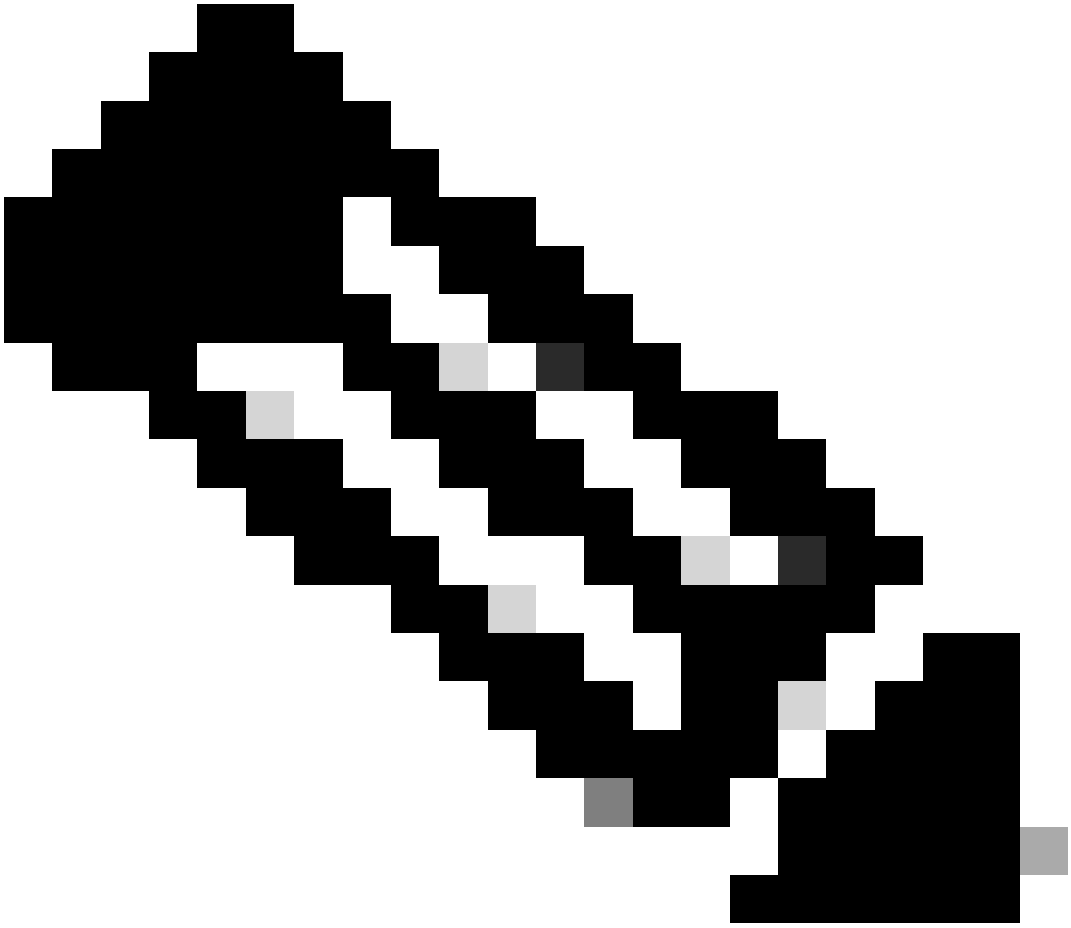
These settings can be tuned by accessing the **Configure > Flow Collectors > Advanced page** in the WebUI of the manager appliance.

- The seconds required to qualify a flow as a long duration setting controls the behavior of the suspect long flow event.



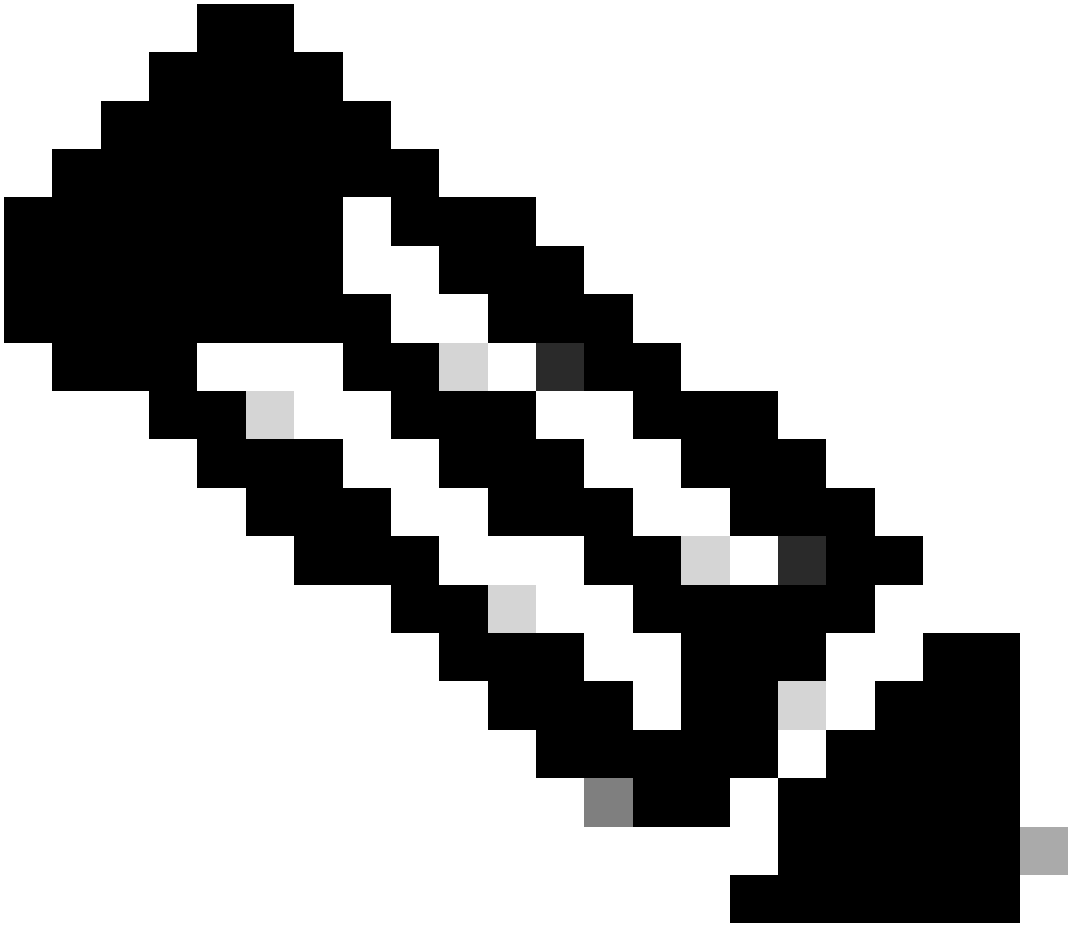
Note: This configuration option in the webUI sets the long_flow_duration parameter in the flow collectors lc_thresholds.txt configuration file.

- The seconds required to qualify a flow as suspect quiet long flow setting controls the behavior of the Suspect Quiet Long Flow event.



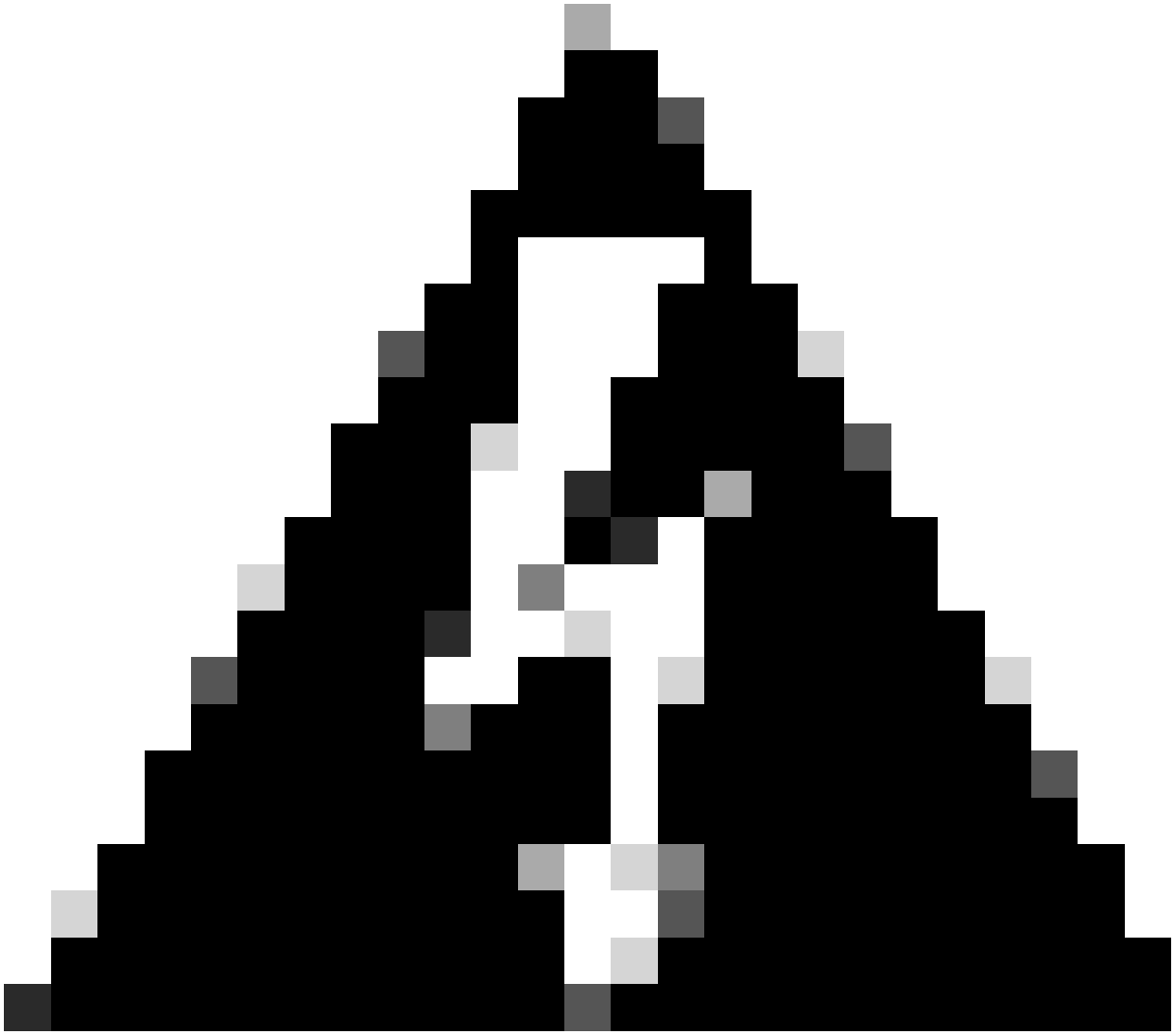
Note: This configuration option in the webUI sets the quiet_long_flow_duration parameter in the flow collectors lc_thresholds.txt configuration file.

The default value for both the counters is **32400 seconds** (9 hours).



Note: In regards to Changing these counters, related CDET:

Cisco bug ID CSCwm05128



Warning: This only affects v7.5.1 or previous versions.

This defect dictates that a suspect quiet long flow must first also be a suspect long flow. This means that if you change the seconds required to qualify a flow as suspect quiet long flow to a duration shorter than the seconds required to qualify a flow as a long duration setting then unexpected results are likely.

If you alter one or both of these Advanced Settings, it can cause the detection of long flows to fail.

Since a Quiet Long Flow by definition must also be a Long Flow, the logic in the proper handling of these two settings is to first have the flow exceed the long flow requirement before testing for it being a quiet long flow.

For example, if long_flow_duration is left at the default value of 9 hours and quiet_long_flow_duration is set to a lower value such as 8 hours, the engine does not raise a quiet long duration flow event until the flow is at least 9 hours long.

Alternatively, if long_flow_duration is left at the default value of 9 hours and
and quiet_long_flow_duration is set to 10 hours, this configuration effectively disables the quiet long duration flow event (unless the flow is a single export having a duration > quiet_long_flow_duration duration of 10 hours.

Solution

Both of these Advanced Settings need to be set to the same desired value or the quiet_long_flow_duration must always be >= long_flow_duration.