

Configure SLF and SQLF Security Events in Secure Analytics

Contents

[Introduction](#)

[Background Information](#)

[Tuning/Configuration](#)

[Solution](#)

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.

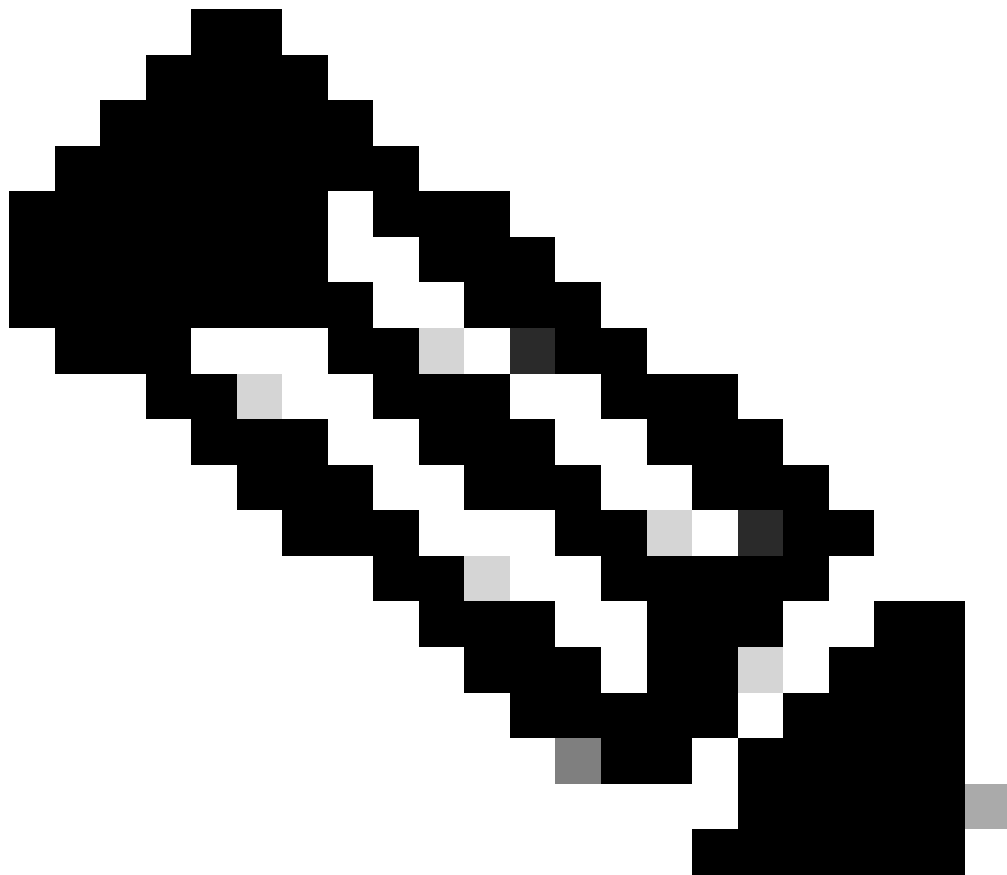
Consider that you connect your laptop to your home PC via a covert VPN for 3 days, but neither the home PC nor the laptop normally carry on long flow connections. The Flow Collector detects this abnormality and triggers a security event depending on the amount of traffic passed and the duration of the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

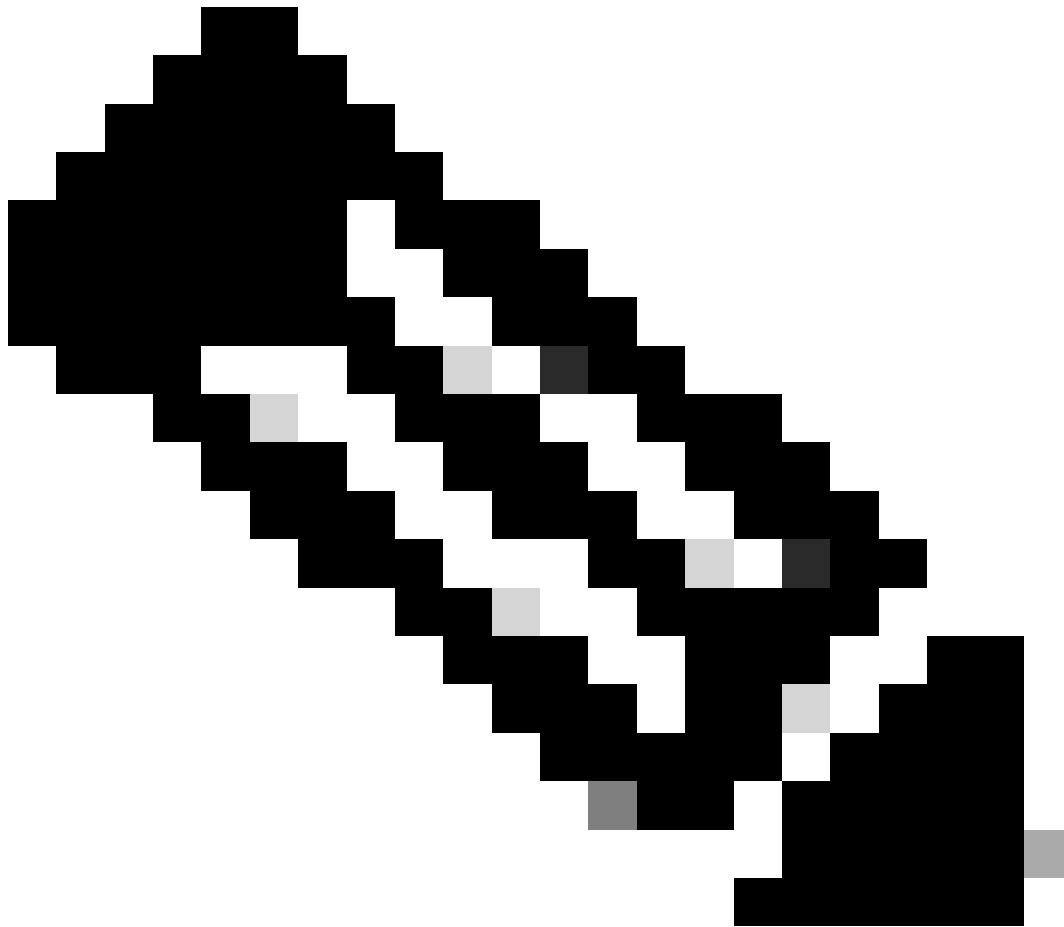
These settings can be tuned by accessing the **Configure > Flow Collectors > Advanced page** in the WebUI of the manager appliance.

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



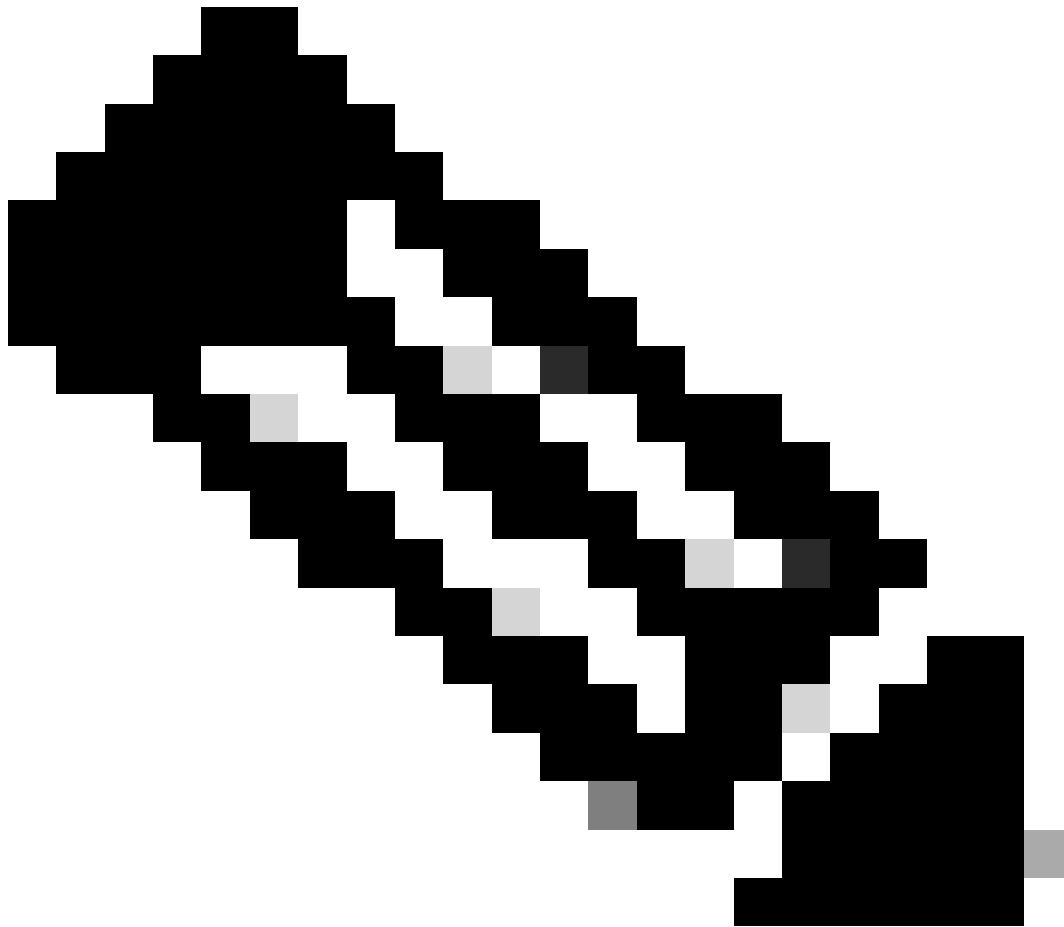
Note: This configuration option in the webUI sets the `long_flow_duration` parameter in the flow collectors `lc_thresholds.txt` configuration file.

-
- 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 `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 \geq `long_flow_duration`.

The screenshot shows the Cisco Secure Network Analytics interface for configuring a Flow Collector. The top navigation bar includes the Cisco logo, the product name "Secure Network Analytics", and a search bar. The left sidebar contains navigation links: "Configure", "Monitor", "Investigate", "Report", and "Apps". The main content area is titled "Flow Collector" and shows details for a specific collector named "fc-60-60". The "Advanced" tab is selected, displaying three lists on the left: "Broadcast List", "Ignore List", and "Watch List", each with a text input field for IP addresses or ranges. On the right, the "Synchronize" section has a "Synchronize" button. Below it, the "Flow Collector Security Thresholds" section contains several checkboxes and input fields. The input fields for "Seconds required to qualify a flow as long duration" (32400), "Seconds required to qualify a flow as Suspect Quiet Long Flow" (32400), "Maximum number of bytes transferred to trigger a Suspect Quiet Long Flow alarm" (292.97K), "Minimum number of asymmetric flows per 5 minute period to trigger an Asymmetric Route alert" (50), and "Minimum number of /24 subnets an infected host must contact before a Worm Activity or Worm Propagation alarm is triggered" (8) are highlighted with red and yellow boxes.

Flow Collector

Name: fc-60-60 IP Address: 192.168.40.40 Model: Flow Collector NetFlow VE Serial: FCNFE-v/VMware-564d9b37119b18-3bb810372ca85d0e

Main Advanced

Advanced

Broadcast List

Enter IPs or IP ranges that are authorized to send broadcasts. Separate entries with a new line or comma.

Ignore List

Enter IPs or IP ranges that the Flow Collector will ignore flows from. Separate entries with a new line or comma.

Watch List

Enter IPs or IP ranges for the Flow Collector to alarm on, when active. Separate entries with a new line or comma.

Synchronize

At times you may need to synchronize the Flow Collectors on your network with your Manager when you observe inconsistent data, update configurations, or restore your Flow Collectors.

During synchronization, Secure Network Analytics overwrites the configuration settings that exist on the Flow Collector with the configuration settings that exist on the Manager.

Synchronize

Flow Collector Security Thresholds

☐ Ignore flows between inside hosts

☐ Ignore flows between outside hosts

☐ Ignore flows to and from non-routable addresses

☒ Ignore flows between inside hosts when calculating File Sharing Index

☐ Ignore null0 flows

Seconds required to qualify a flow as long duration:

32400

Suspect Long Duration Flow trust threshold:

5

Seconds required to qualify a flow as Suspect Quiet Long Flow:

32400

Maximum number of bytes transferred to trigger a Suspect Quiet Long Flow alarm:

292.97K

Minimum number of asymmetric flows per 5 minute period to trigger an Asymmetric Route alert:

50

Minimum number of /24 subnets an infected host must contact before a Worm Activity or Worm Propagation alarm is triggered:

8