Configure the Flow Collector's Ignore List Feature

Contents

Introduction

This document describes how to configure your SNA flow collector to reject incoming netflow from a particular exporter by using Ignore List.

Background Information

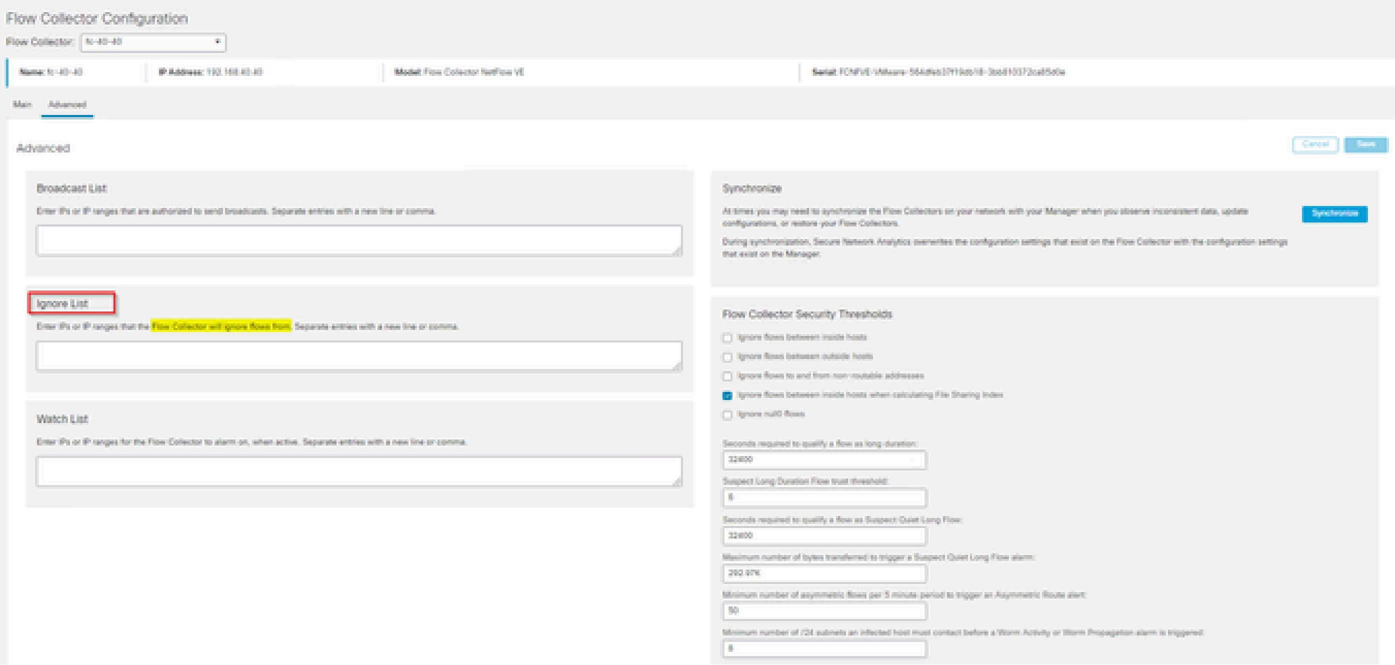
Often times, the question is posed, "Is there any way to tell my SNA flow collector to reject incoming netflow from a particular exporters?"

The answer is yes, this is done through the use of the flow collectors "Ignore List" feature.

Configure

The ignore list feature is flow collector specific. In later version of SNA 7.x, this feature is available inside of the flow collector configuration page on the SNA Manager Web UI.

Use this page to specify an unlimited number of hosts or subnets for which theFlow Collectorcompletelyignorestraffic. If theFlow Collectorsees any traffic attributable to these IP addresses, it excludes that traffic from any graph or table. Be certain that you can trust all traffic traveling to or from the hosts to beignored.Secure Network Analyticsdoes not analyze this traffic nor any that is spoofed to include any of these hosts. If an attack is launched on your network involving one of these hosts/subnets, theFlow Collectorcannot report it.



Flow Collector Configuration

Flow Collector: fc-40-40

Name: fc-40-40 | **IP Address:** 192.168.40.40 | **Model:** Flow Collector NetFlow VE | **Serial:** FCNFVE-VMware-564d9eb37f19db18-3bb810372ca85d0e

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.

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: 6

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

FAQs

What is the Effect of Ignore List on Flows Per Second (FPS) calculations for Smart Licensing?

Answer: Adding host IP addresses or ranges to the ignore list effectively prevents any of these flows from counting against the calculated FPS rate sent up to the SMC and used for Smart License reporting. The flows are NO longer shown/counted in the flow trend graph displayed on the SMC dashboard.

How is the ignore list feature used when processing NVM flow when client is in split tunnel mode?

A customer could configure AnyConnect to send us on-network and off-network traffic (aka split tunnel). The off-network traffic uses the endpoint local IP address which most likely contain overlapping IPs. SNA does not support overlapping IPs, thus is has been suggested to use Ignore list feature to circumvent the split tunnel issue, thereby preserving the benefit of the NVM based flows for detections.

In this use case, we Configure the "Ignore List" to prevent the off-network NVM flows from flow cache → flow_stats, Flow Search, Custom Security Events

1. Add the IP address and Network Mask (e.g add 192.168.1.0/24, 127.0.0.1/24) into the Ignore List
2. Verify the nvm_flows are still populated with the NVM flows
3. Verify that the flow_stats do not have the NVM flows if either src or dst IP is in the Ignore List

Can I use an ignore list to ignore flows from an entire exporter? No, because the ignore list is based on flow data and not exporter data, adding an exporter IP address to the ignore list would effectively ignore flow data where the exporter IP was listed as either the source or the destination of the flow, instead of ignoring all flow records from that particular exporter