

SLF- en SQLF-beveiligingsgebeurtenissen configureren in Secure Analytics

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Afstemming/configuratie](#)

[Oplossing](#)

Inleiding

Dit document beschrijft twee parameters die kunnen worden gebruikt om de verdachte lange stroom (SLF) en verdachte rustige lange stroom (SQLF) beveiligingsgebeurtenissen af te stemmen.

Achtergrondinformatie

Een Suspect Long Flow-gebeurtenis is een specifiek type beveiligingsevenement dat wordt gegenereerd door Secure Analytics en is ontworpen om langer dan normale gesprekken tussen hosts te detecteren. Er zijn twee verschillende soorten van de verdachte lange stroom gebeurtenis; verdachte lange stroom en verdachte stille lange stroom.

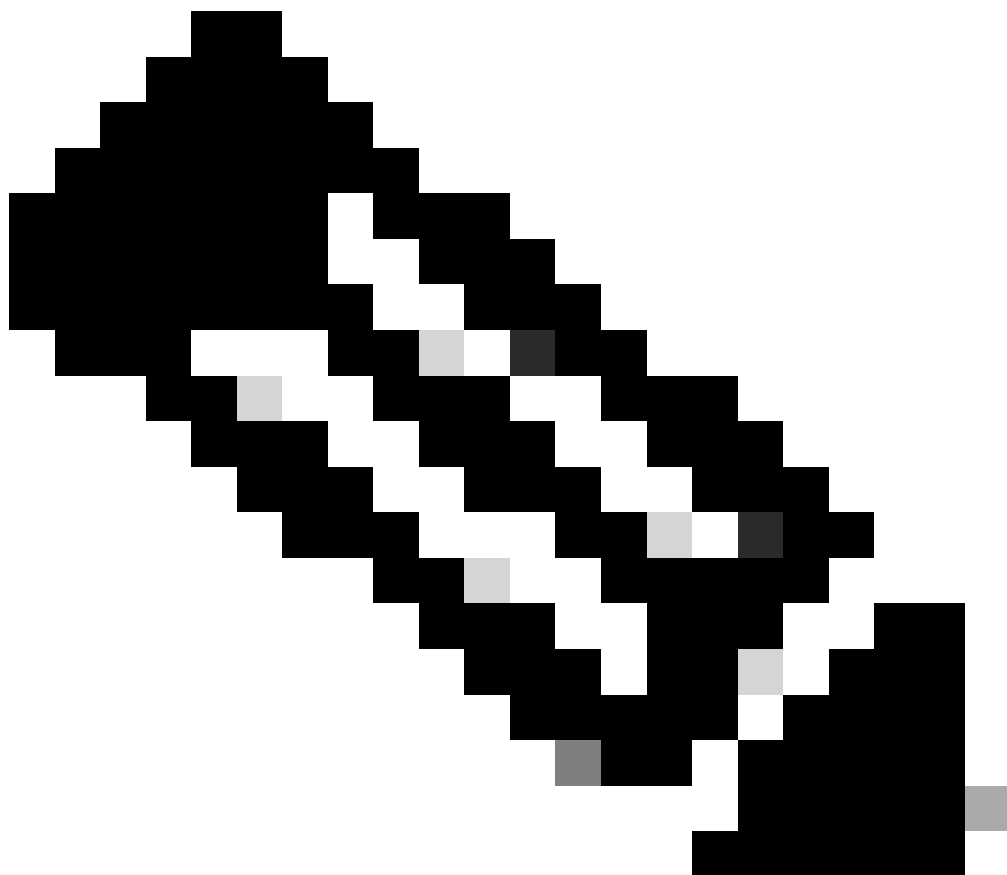
Houd er rekening mee dat u uw laptop gedurende 3 dagen via een geheime VPN op uw pc thuis aansluit, maar dat de pc thuis en de laptop normaal gesproken geen lange stroomverbindingen hebben. De Flow Collector detecteert deze afwijking en activeert een beveiligingsgebeurtenis, afhankelijk van de hoeveelheid verkeer die wordt doorgegeven en de duur van de stroom. Deze gebeurtenissen zijn bedoeld om langlopende stromen en langlopende stromen te identificeren die minimaal verkeer passeren.

Afstemming/configuratie

Er zijn voornamelijk 2 flow collector configuratieparameters die verantwoordelijk zijn voor het beheersen van het gedrag van deze twee gebeurtenissen.

U kunt deze instellingen afstemmen via de pagina Configureren > Stroomverzamelaars > Geavanceerd in de WebUI van het beheertoestel.

- De seconden die nodig zijn om een flow te kwalificeren als een lange duurstelling, bepalen het gedrag van de verdachte lange stroomgebeurtenis.



Opmerking: Met deze configuratieoptie in de webUI wordt de parameter `long_flow_duration` ingesteld in het configuratiebestand `flow collectors lc_threshold.txt`.

-
- De seconden die nodig zijn om een stroom te kwalificeren als verdachte stille lange stroom instelling regelt het gedrag van de verdachte stille lange stroom gebeurtenis.



Opmerking: Met deze configuratieoptie in de webUI wordt de parameter `quiet_long_flow_duration` ingesteld in het configuratiebestand `flow collectors lc_threshold.txt`.

De standaardwaarde voor beide tellers is 32400 seconden (9 uur).



Opmerking: Met betrekking tot het wijzigen van deze tellers, gerelateerde CDET:

Cisco bug ID [CSCwm05128](#)



Waarschuwing: dit heeft alleen invloed op v7.5.1 of eerdere versies.

Dit defect dicteert dat een verdachte stille lange stroom eerst ook een verdachte lange stroom moet zijn. Dit betekent dat als u de seconden die nodig zijn om een stroom te kwalificeren als verdachte stille lange stroom wijzigt in een kortere duur dan de seconden die nodig zijn om een stroom als een lange duurstelling te kwalificeren, onverwachte resultaten waarschijnlijk zijn.

Als u een of beide van deze Geavanceerde instellingen wijzigt, kan dit ertoe leiden dat de detectie van lange stromen mislukt.

Aangezien een stille lange stroom per definitie ook een lange stroom moet zijn, is het logisch dat bij de juiste behandeling van deze twee instellingen de stroom eerst de vereiste lange stroom overschrijdt voordat wordt getest of het een stille lange stroom is.

Als `long_flow_duration` bijvoorbeeld op de standaardwaarde van 9 uur blijft staan en `quiet_long_flow_duration` op een lagere waarde zoals 8 uur is ingesteld, verhoogt de motor geen stille lange duur flow-gebeurtenis totdat de stroom ten minste 9 uur lang is.

Als long_flow_duration op de standaardwaarde van 9 uur blijft staan en quiet_long_flow_duration op 10 uur is ingesteld, schakelt deze configuratie effectief de gebeurtenis quiet long duration flow uit (tenzij de stroom een enkele export is met een duur > quiet_long_flow_duration van 10 uur).

Oplossing

Beide Geavanceerde instellingen moeten op dezelfde gewenste waarde worden ingesteld of de quiet_long_flow_duration moet altijd $\geq$ long_flow_duration zijn.

The screenshot shows the 'Secure Network Analytics' interface for configuring a 'Flow Collector'. The top navigation bar includes a search bar and an 'Admin User' profile. The left sidebar contains navigation links: 'Monitor', 'Investigate', 'Report', 'Configure', and 'Apps'. The 'Configure' section is active, showing the 'Advanced' tab for the 'Flow Collector' named 'fc-60-60' with IP address '192.168.40.40'.

The 'Advanced' configuration area is divided into several sections:

- Broadcast List:** A text input field for entering IP addresses or IP ranges authorized to send broadcasts.
- Ignore List:** A text input field for entering IP addresses or IP ranges that the Flow Collector will ignore flows from.
- Watch List:** A text input field for entering IP addresses or IP ranges for the Flow Collector to alarm on when active.
- Synchronize:** A section with a 'Synchronize' button and explanatory text about synchronizing Flow Collectors with the Manager.
- Flow Collector Security Thresholds:** A section with several checkboxes and input fields:
 - Checkboxes: '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' (checked), and 'Ignore null0 flows'.
 - Input fields for thresholds:
 - 'Seconds required to qualify a flow as long duration': 92400
 - 'Suspect Long Duration Flow trust threshold': 6
 - 'Seconds required to qualify a flow as Suspect Quiet Long Flow': 92400
 - '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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.