SLF- en SQLF-beveiligingsgebeurtenissen configureren in Secure Analytics

Inhoud

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.

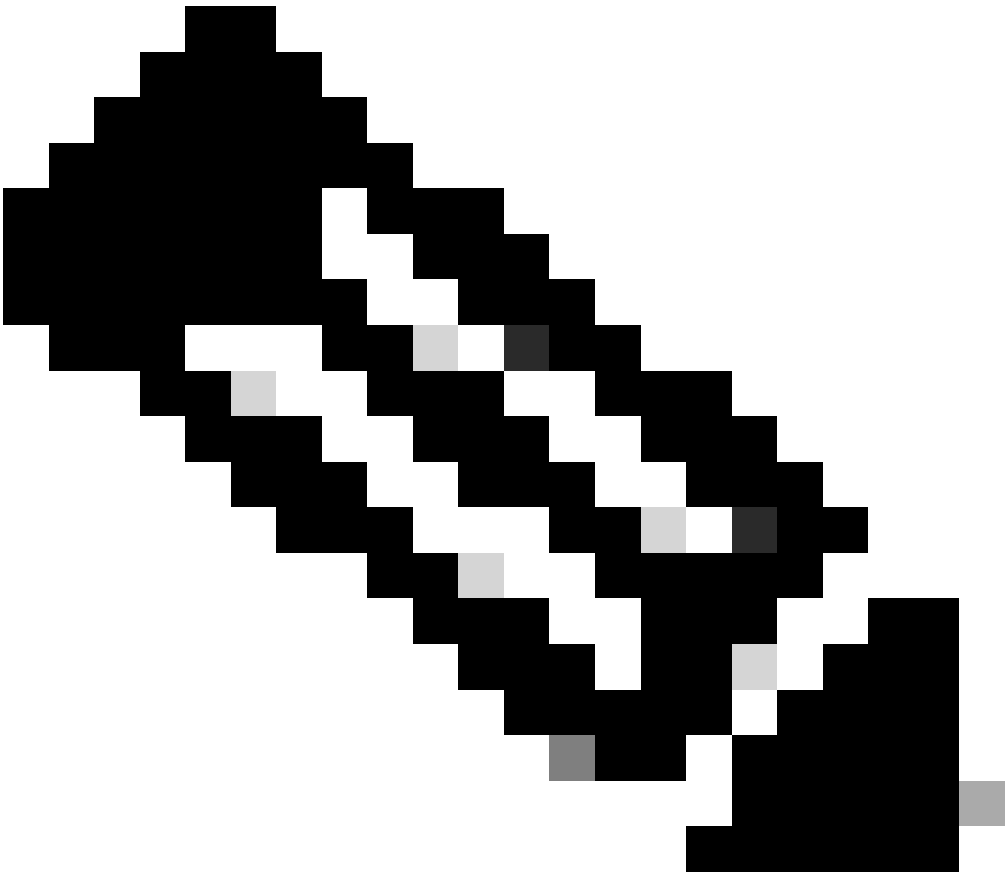
Houd er rekening mee dat u uw laptop gedurende 3 dagen via een geheime VPN op uw pc thuis aansluit, maar dat de pc thuis en de laptop normaal gesproken geen lange stroomverbindingen hebben. De Flow Collector detecteert deze afwijking en activeert een beveiligingsgebeurtenis, afhankelijk van de hoeveelheid 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.

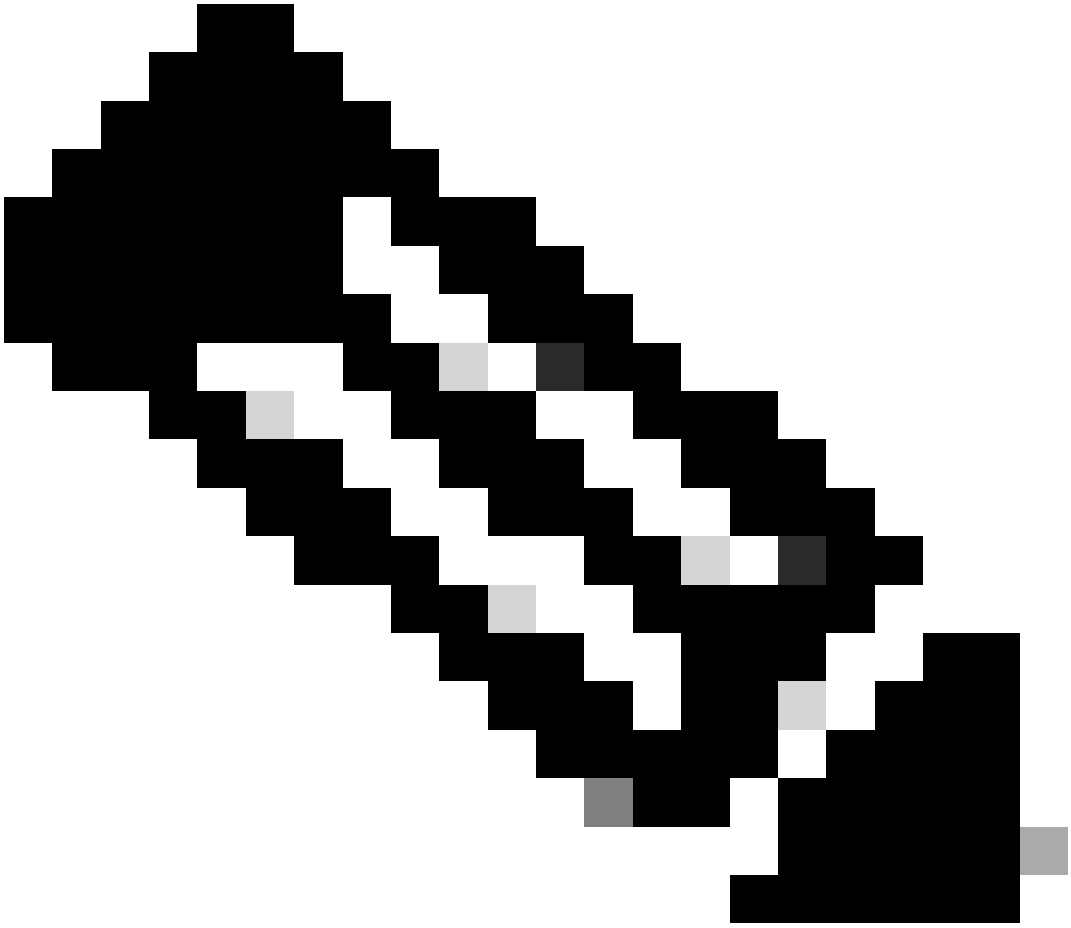
U kunt deze instellingen afstemmen via de pagina Configureren > Stroomverzamelaars > Geavanceerd in de WebUI van het beheertoestel.

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



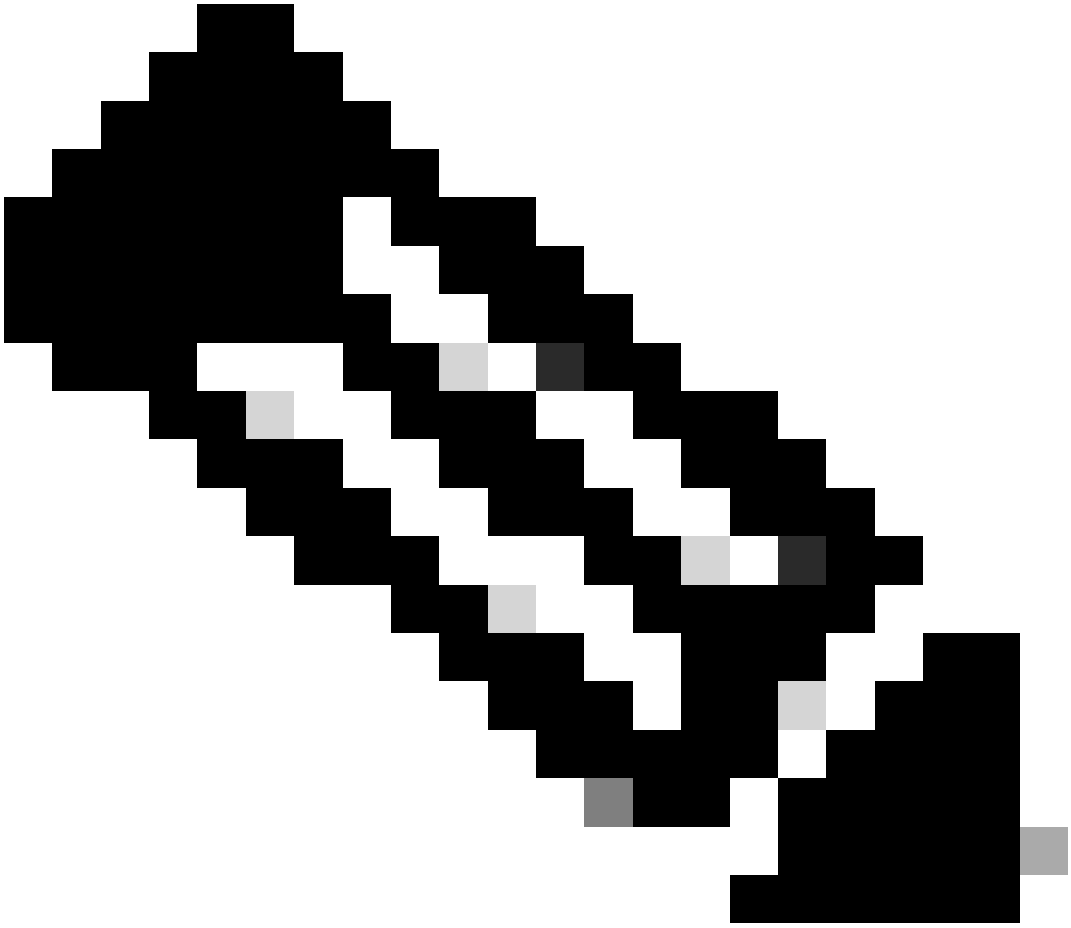
Opmerking: Met deze configuratieoptie in de webUI wordt de parameter long_flow_duration ingesteld in het configuratiebestand flow collectors lc_threshold.txt.

- 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.



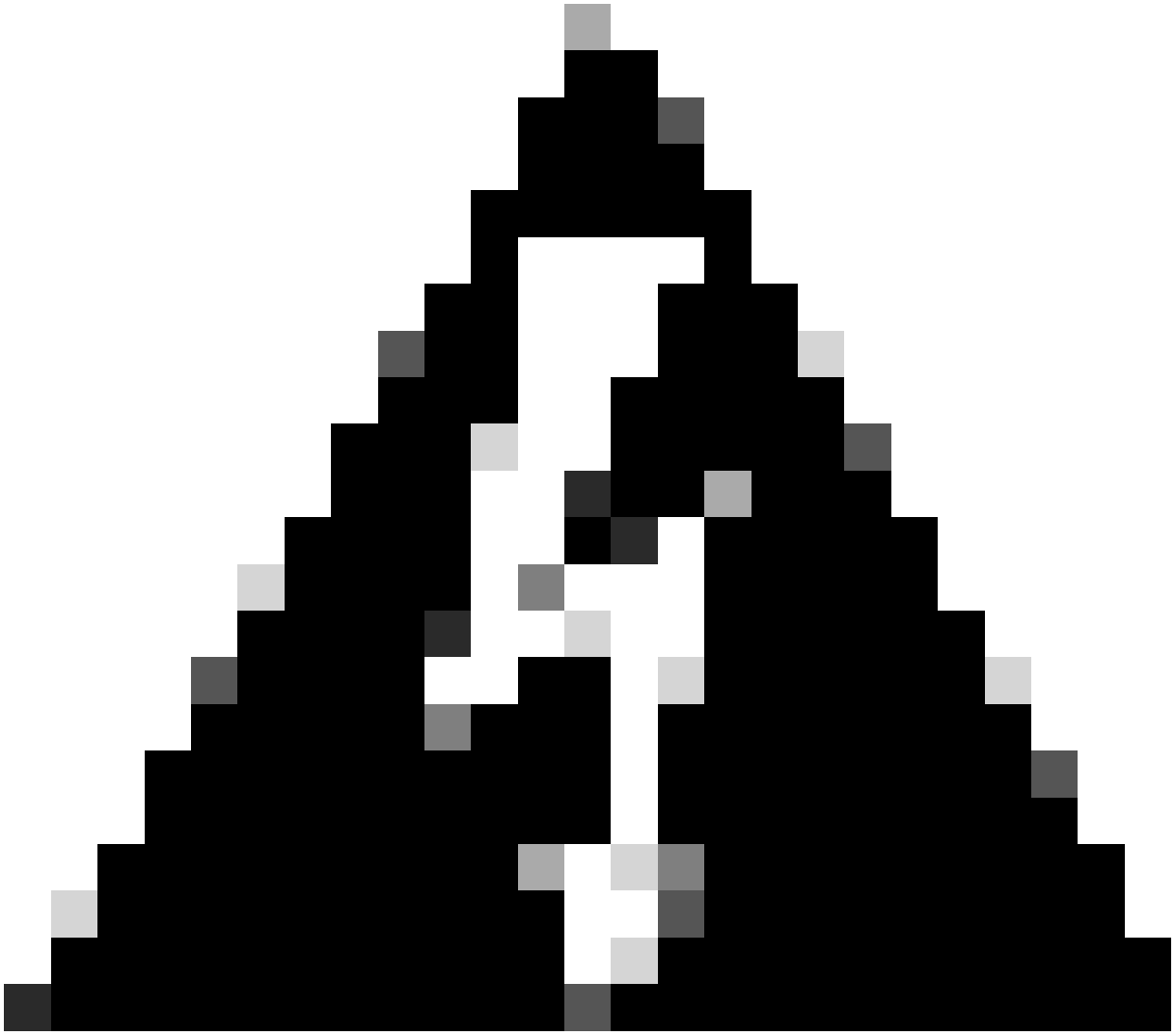
Opmerking: Met deze configuratieoptie in de webUI wordt de parameter quiet_long_flow_duration ingesteld in het configuratiebestand flow collectors lc_threshold.txt.

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 duurinstelling 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.

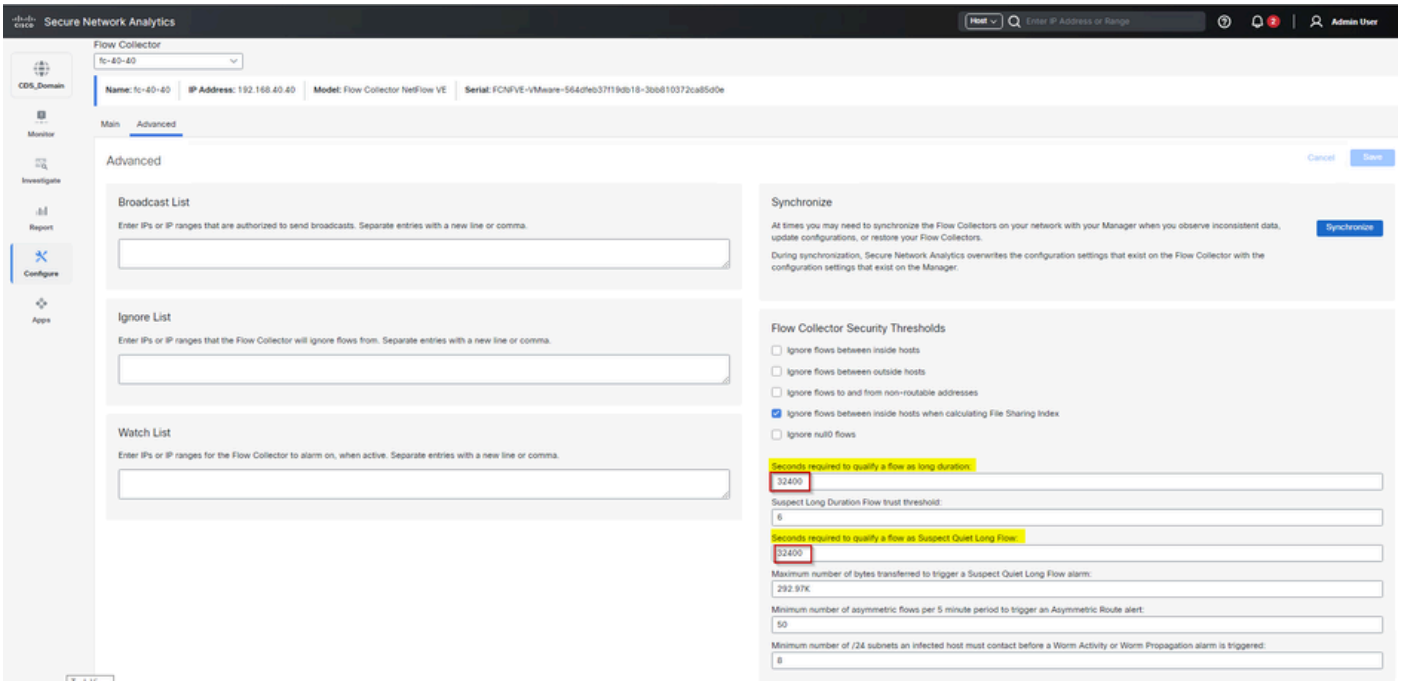
Aangezien een stille lange stroom per definitie ook een lange stroom moet zijn, is het logisch dat bij de juiste behandeling van deze twee instellingen de stroom eerst de vereiste lange stroom overschrijdt voordat wordt getest of het een stille lange stroom is.

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 >= long_flow_duration zijn.



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.