Configuración de eventos de seguridad SLF y SQLF en Secure Analytics

Contenido

Introducción

Este documento describe dos parámetros que se pueden utilizar para ajustar los eventos de seguridad de flujo largo sospechoso (SLF) y flujo largo silencioso sospechoso (SQLF).

Antecedentes

Un evento de flujo largo sospechoso es un tipo específico de evento de seguridad generado por Secure Analytics que está diseñado para detectar conversaciones más largas de lo normal entre hosts. Existen dos tipos diferentes del evento Sospect Long Flow; Sospechoso de flujo largo y Sospechoso de flujo largo silencioso.

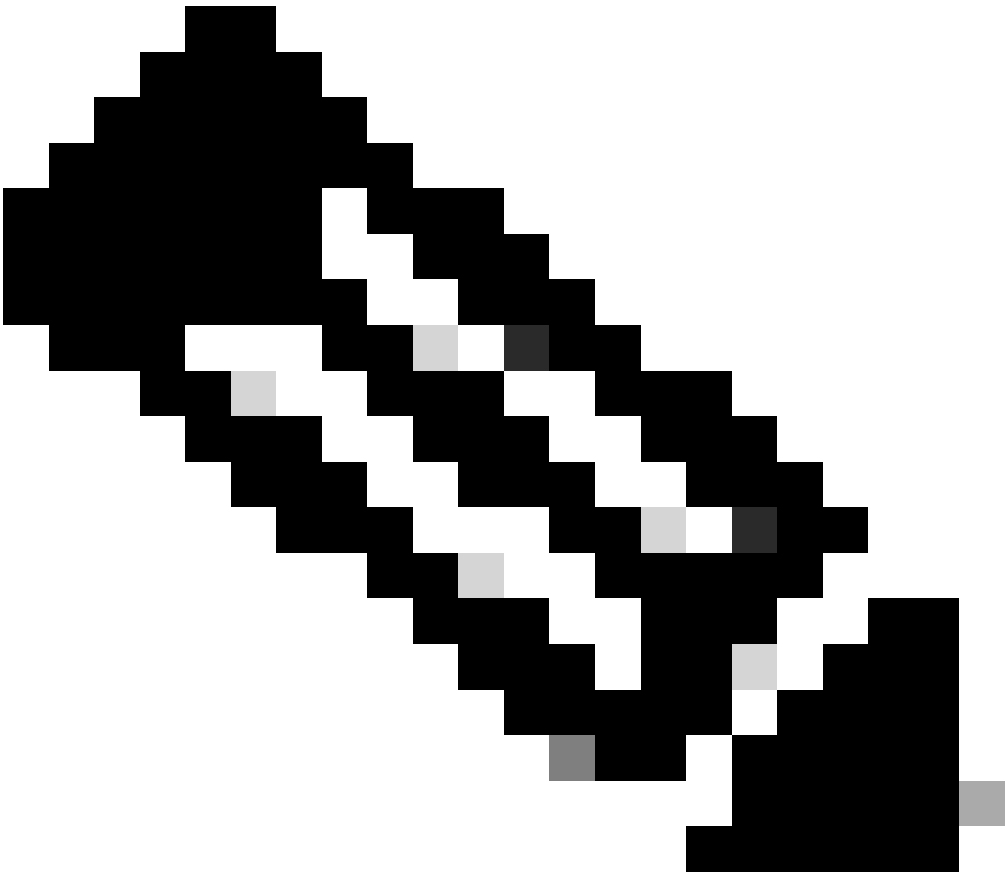
Tenga en cuenta que conecta el portátil al PC doméstico a través de una VPN encubierta durante 3 días, pero ni el PC doméstico ni el portátil suelen llevar conexiones de flujo largo. Flow Collector detecta esta anomalía y activa un evento de seguridad en función de la cantidad de tráfico transferido y la duración del flujo. Estos eventos están pensados para identificar los flujos de larga duración y los flujos de larga duración que pasan un tráfico mínimo.

Ajuste/Configuración

Hay principalmente 2 parámetros de configuración del colector de flujo que son responsables de controlar el comportamiento de estos dos eventos.

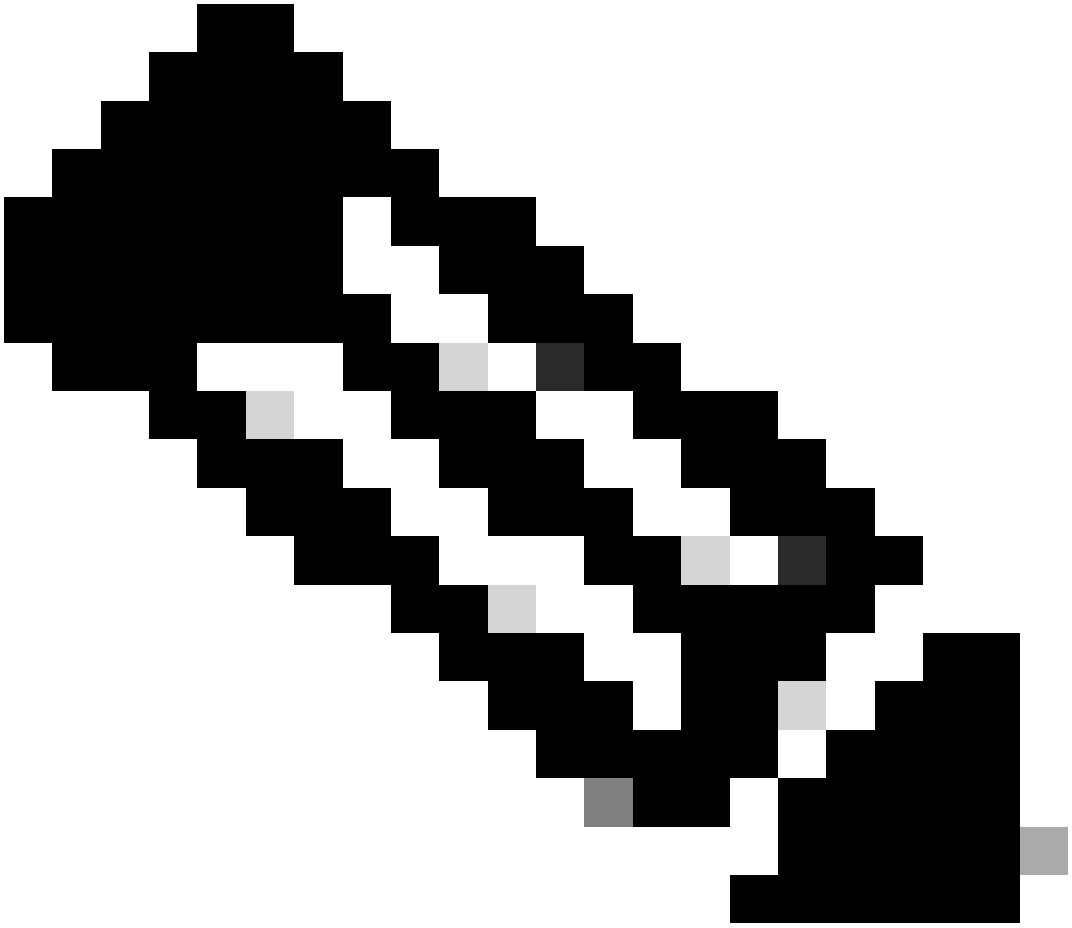
Estos ajustes se pueden ajustar accediendo a la página Configure > Flow Collectors > Advanced en la interfaz de usuario web del dispositivo de administración.

- Los segundos necesarios para calificar un flujo como configuración de larga duración controlan el comportamiento del evento de flujo largo sospechoso.



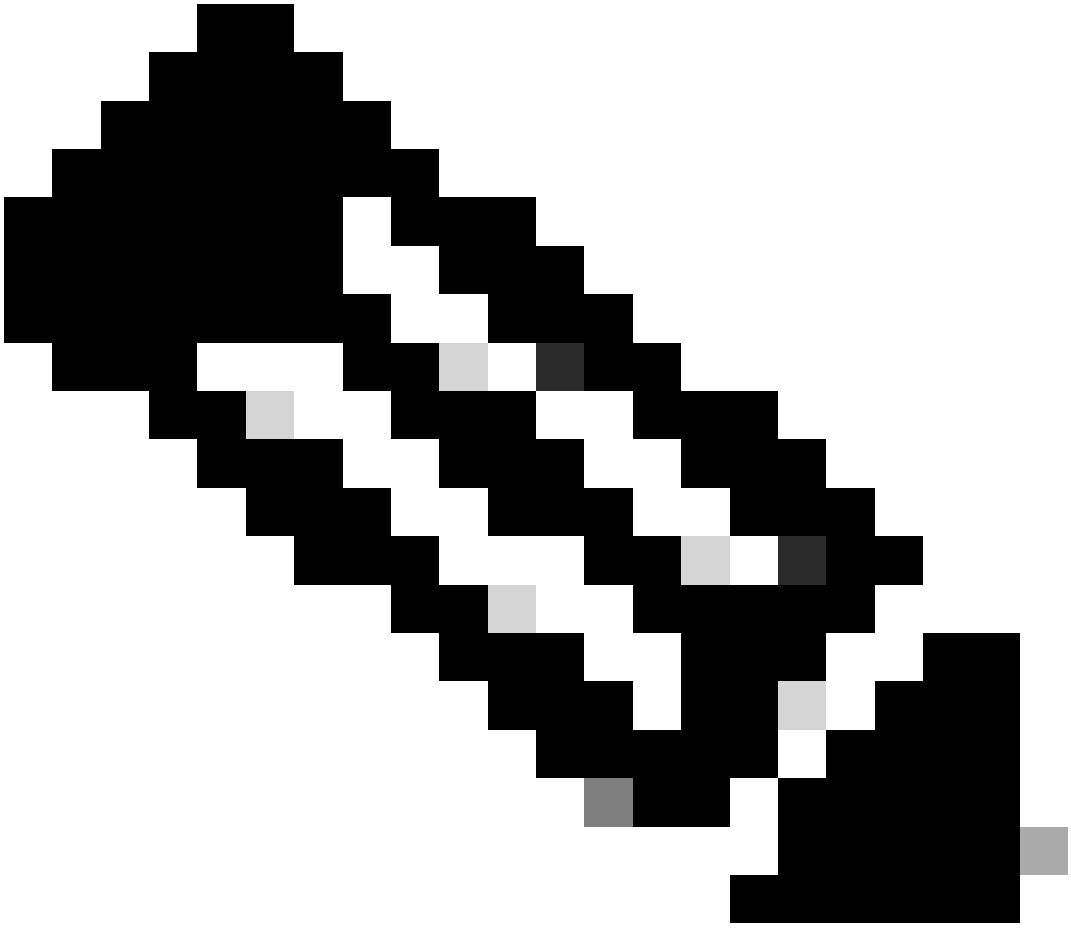
Nota: Esta opción de configuración de la interfaz de usuario Web define el parámetro long_flow_duration en el archivo de configuración lc_threshold.txt de los recopiladores de flujo.

- Los segundos necesarios para calificar un flujo como flujo largo silencioso sospechoso controlan el comportamiento del evento Flujo largo silencioso sospechoso.



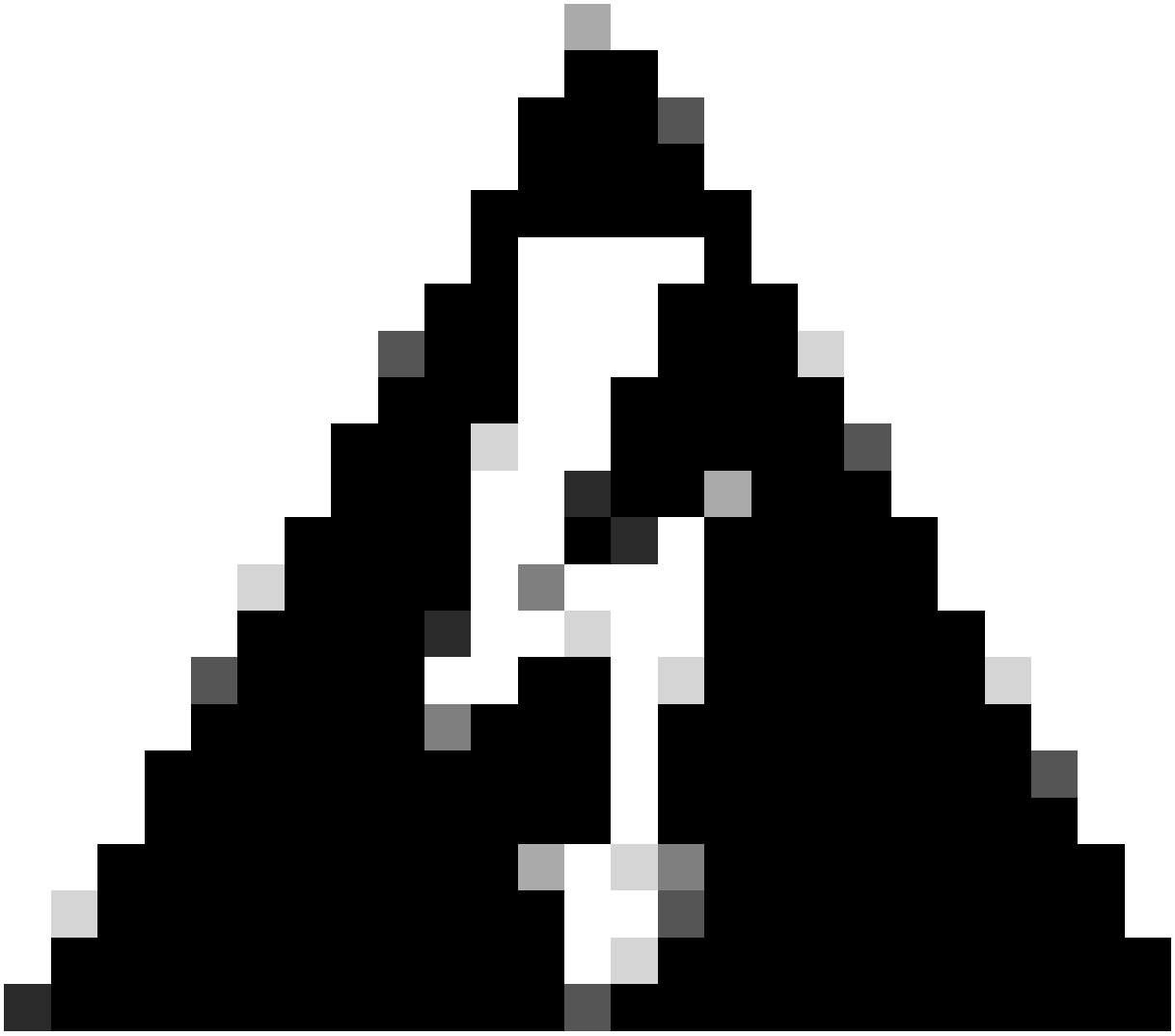
Nota: Esta opción de configuración de la interfaz de usuario Web define el parámetro quiet_long_flow_duration en el archivo de configuración lc_threshold.txt de los recopiladores de flujo.

El valor predeterminado para ambos contadores es 32400 segundos (9 horas).



Nota: Con respecto al cambio de estos contadores, el CDET relacionado:

ID de bug de Cisco CSCwm05128



Advertencia: Esto sólo afecta a la versión 7.5.1 o versiones anteriores.

Este defecto dicta que un flujo largo y silencioso sospechoso primero debe ser también un flujo largo sospechoso. Esto significa que si cambia los segundos requeridos para calificar un flujo como flujo largo silencioso sospechoso a una duración más corta que los segundos requeridos para calificar un flujo como configuración de larga duración, entonces es probable que se produzcan resultados inesperados.

Si modifica uno o ambos de estos parámetros avanzados, puede provocar un error en la detección de flujos largos.

Dado que un flujo largo silencioso por definición también debe ser un flujo largo, la lógica en el manejo adecuado de estas dos configuraciones es primero hacer que el flujo exceda el requisito de flujo largo antes de probar que es un flujo largo silencioso.

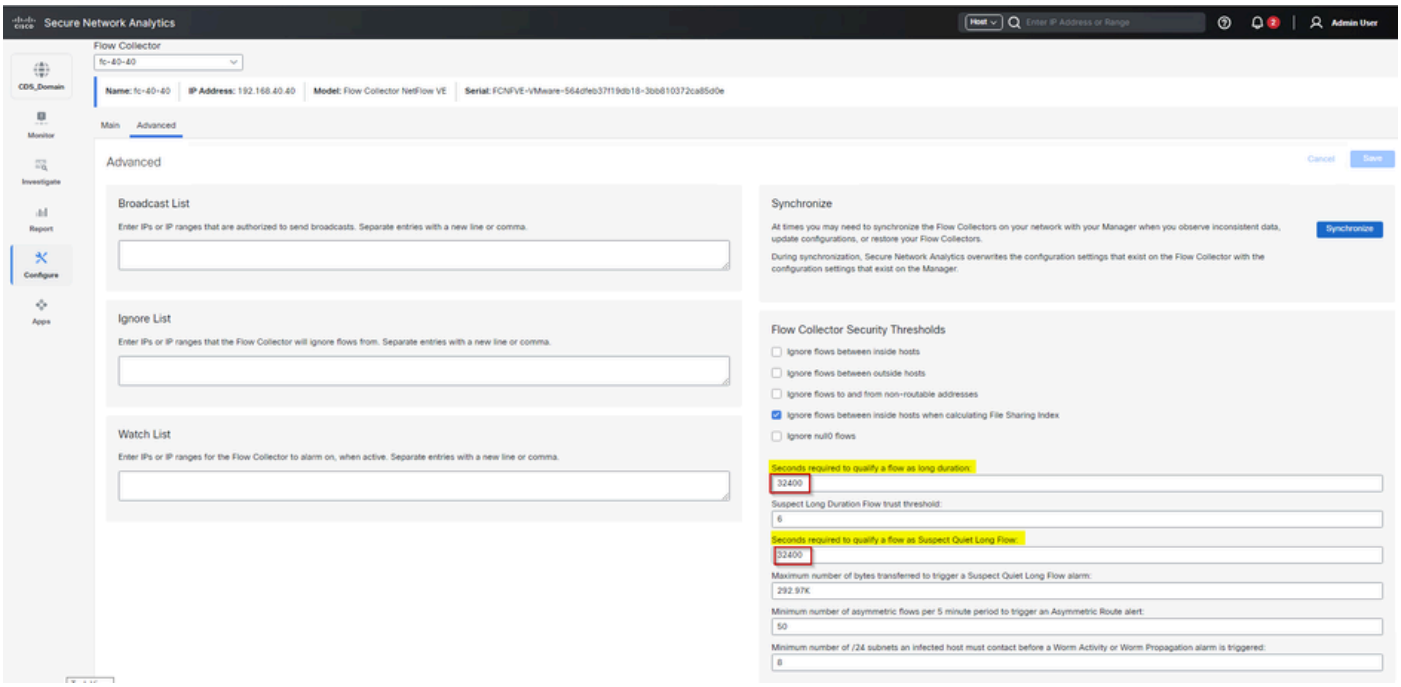
Por ejemplo, si long_flow_duration se deja en el valor predeterminado de 9 horas y quiet_long_flow_duration se establece en un valor inferior, como 8 horas, el motor no provoca un

evento de flujo de larga duración silenciosa hasta que el flujo tenga al menos 9 horas de duración.

Alternativamente, si long_flow_duration se deja en el valor predeterminado de 9 horas y quiet_long_flow_duration se establece en 10 horas, esta configuración inhabilita eficazmente el evento de flujo de larga duración silenciosa (a menos que el flujo sea una exportación única que tenga una duración > quiet_long_flow_duration de 10 horas).

Solución

Ambos valores de configuración avanzados deben establecerse en el mismo valor deseado o quiet_long_flow_duration debe ser siempre >= long_flow_duration.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).