Configurar eventos de segurança SLF e SQLF no Secure Analytics

Contents

Introdução

Este documento descreve dois parâmetros que podem ser usados para ajustar os eventos de segurança de fluxo longo suspeito (SLF) e de fluxo longo de silêncio suspeito (SQLF).

Informações de Apoio

Um evento Suspeito de Fluxo Longo é um tipo específico de evento de segurança gerado pelo Secure Analytics que é projetado para detectar conversas mais longas que as normais entre hosts. Existem dois tipos diferentes de evento Suspeito de Fluxo Longo; Suspeito de fluxo longo e Suspeito de fluxo longo silencioso.

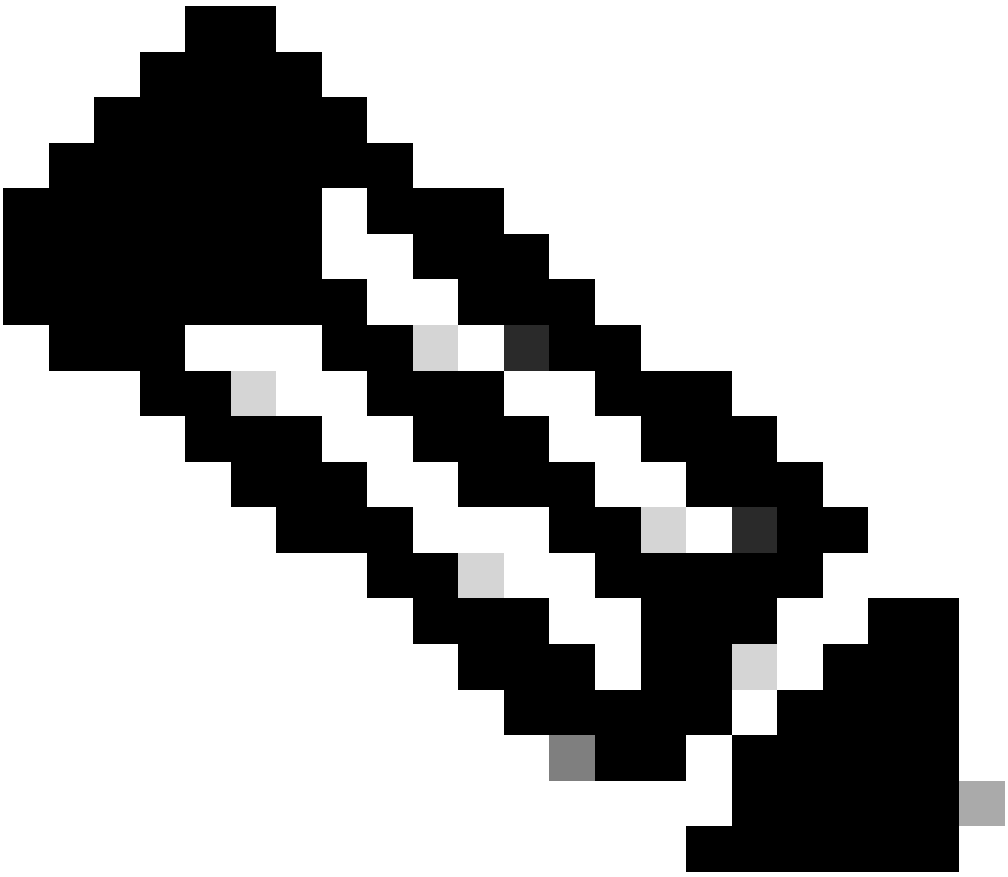
Considere que você conecte seu notebook ao seu PC residencial através de uma VPN secreta por 3 dias, mas nem o PC residencial nem o notebook normalmente têm conexões de fluxo longo. O coletor de fluxo detecta essa anormalidade e aciona um evento de segurança, dependendo da quantidade de tráfego passada e da duração do fluxo. Esses eventos destinam-se a identificar fluxos de longa duração e fluxos de longa duração que estão passando pelo tráfego mínimo.

Ajuste/Configuração

Há principalmente 2 parâmetros de configuração do coletor de fluxo que são responsáveis por controlar o comportamento desses dois eventos.

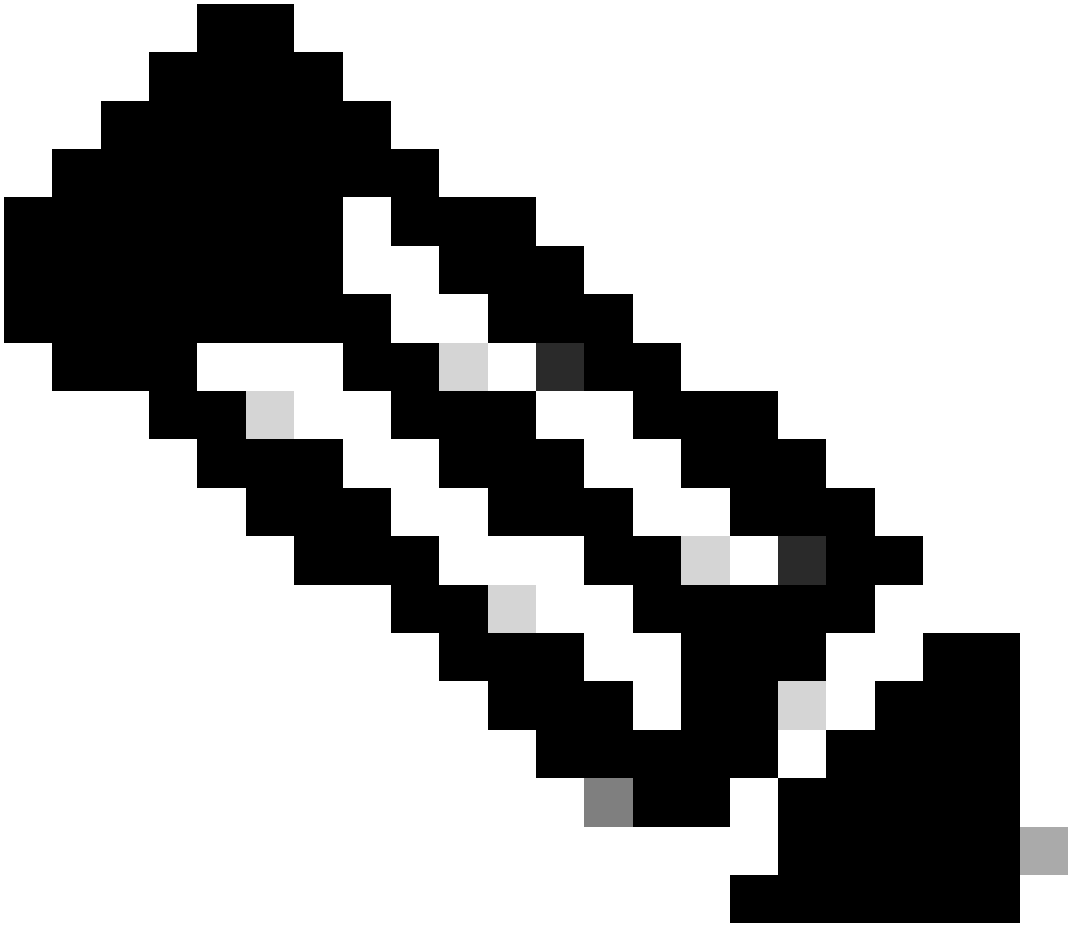
Essas configurações podem ser ajustadas acessando a página Configurar > Flow Collectors > Avançado na WebUI do dispositivo gerenciador.

- Os segundos necessários para qualificar um fluxo como uma configuração de longa duração controlam o comportamento do evento de fluxo longo suspeito.



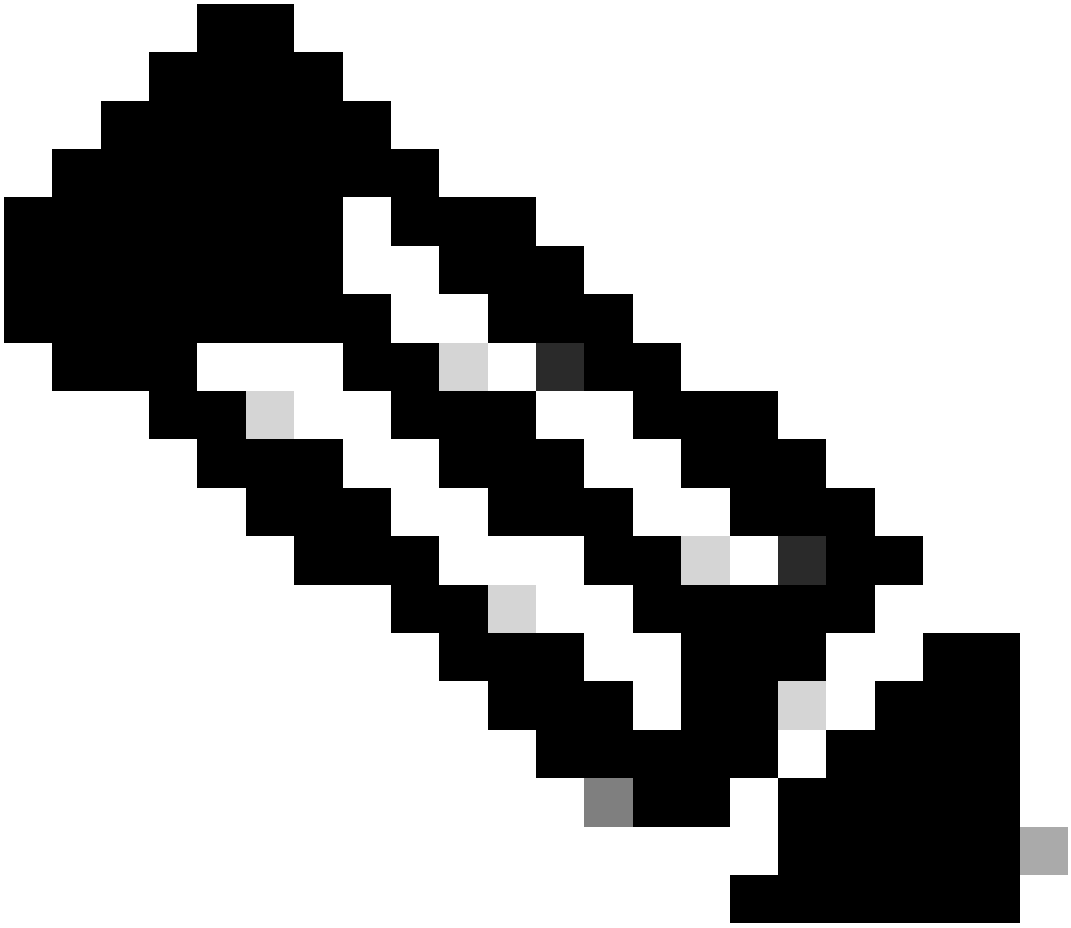
Note: Esta opção de configuração na webUI define o parâmetro long_flow_duration no arquivo de configuração lc_thresholds.txt dos coletores de fluxo.

- Os segundos necessários para qualificar um fluxo como configuração de fluxo longo silencioso suspeito controlam o comportamento do evento de fluxo longo silencioso suspeito.



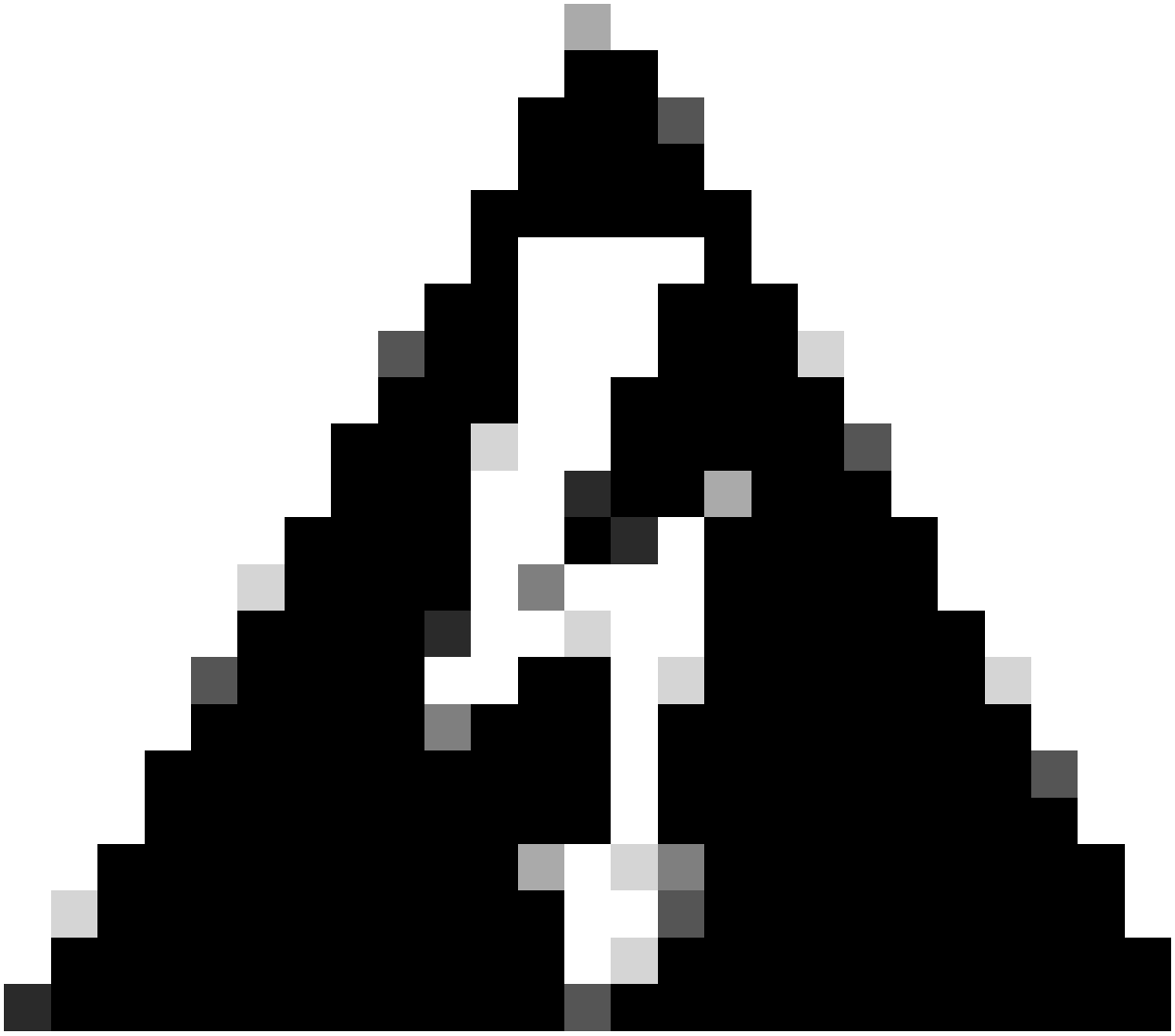
Note: Esta opção de configuração na webUI define o parâmetro quiet_long_flow_duration no arquivo de configuração lc_threshold.txt dos coletores de fluxo.

O valor padrão para ambos os contadores é 32400 segundos (9 horas).



Note: No que diz respeito à alteração desses contadores, o CDET relacionado:

ID de bug da Cisco CSCwm05128



aviso: Isso afeta apenas a v7.5.1 ou versões anteriores.

Esse defeito determina que um fluxo longo silencioso suspeito deve primeiro ser também um fluxo longo suspeito. Isso significa que, se você alterar os segundos necessários para qualificar um fluxo como fluxo longo silencioso suspeito para uma duração menor do que os segundos necessários para qualificar um fluxo como uma configuração de longa duração, resultados inesperados são prováveis.

Se você alterar uma ou ambas as Configurações avançadas, a detecção de fluxos longos poderá falhar.

Como um fluxo longo silencioso por definição também deve ser um fluxo longo, a lógica no tratamento adequado dessas duas configurações é primeiro fazer com que o fluxo exceda o requisito de fluxo longo antes de testar se ele é um fluxo longo silencioso.

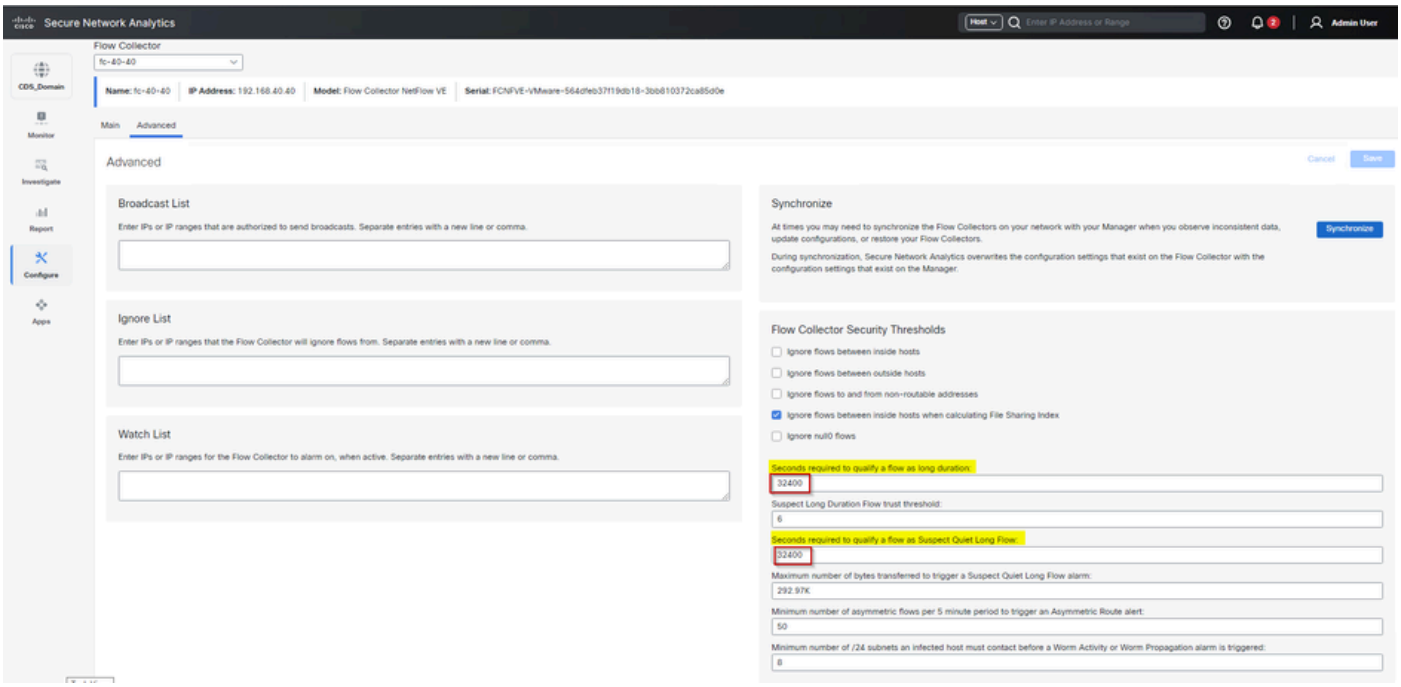
Por exemplo, se long_flow_duration for deixado no valor padrão de 9 horas e quiet_long_flow_duration for definido como um valor mais baixo, como 8 horas, o mecanismo não

gerará um evento de fluxo de longa duração silencioso até que o fluxo tenha pelo menos 9 horas de duração.

Como alternativa, se long_flow_duration for deixado no valor padrão de 9 horas e quiet_long_flow_duration for definido como 10 horas, essa configuração efetivamente desativará o evento de fluxo de longa duração silenciosa (a menos que o fluxo seja uma única exportação com uma duração > quiet_long_flow_duration de 10 horas.

Solução

Essas duas configurações avançadas precisam ser definidas com o mesmo valor desejado ou quiet_long_flow_duration deve ser sempre >= long_flow_duration.



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.