

Secure Analytics에서 SLF 및 SQLF 보안 이벤트 구성

목차

[소개](#)

[배경 정보](#)

[튜닝/컨피그레이션](#)

[솔루션](#)

소개

이 문서에서는 의심스러운 SLF(long flow) 및 의심스러운 SQLF(quiet long flow) 보안 이벤트를 튜닝하는 데 사용할 수 있는 두 가지 매개변수에 대해 설명합니다.

배경 정보

Suspect Long Flow 이벤트는 Secure Analytics에서 생성되는 특정 유형의 보안 이벤트로, 호스트 간의 일반적인 대화보다 긴 시간을 탐지하도록 설계되었습니다. Suspect Long Flow 이벤트에는 두 가지 다른 유형이 있습니다. Suspect Long Flow 및 Suspect Quiet Long Flow.

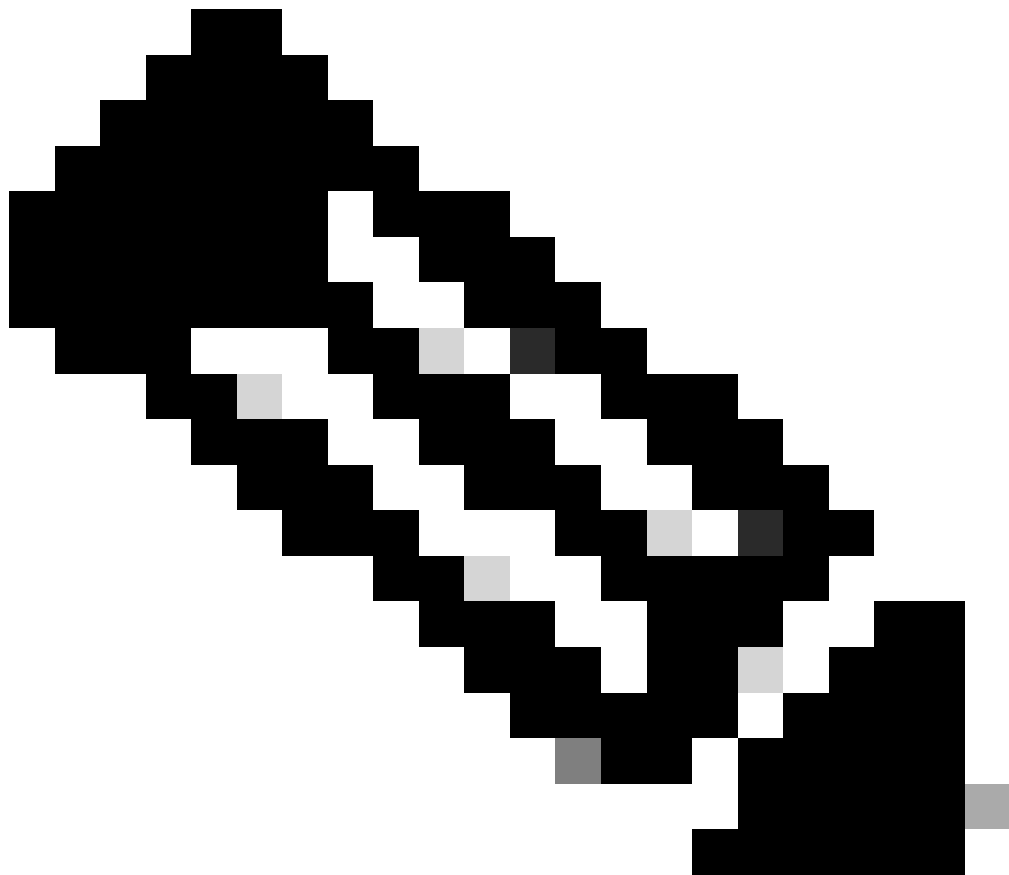
3일 동안 가정용 VPN을 통해 노트북 컴퓨터를 가정용 PC에 연결하지만 가정용 PC와 노트북 컴퓨터는 일반적으로 긴 흐름 연결을 수행하지 않습니다. Flow Collector는 이러한 이상을 탐지하고 전달된 트래픽의 양과 흐름 기간에 따라 보안 이벤트를 트리거합니다. 이러한 이벤트는 긴 실행 흐름과 최소 트래픽을 전달하는 긴 실행 흐름을 식별하기 위한 것입니다.

튜닝/컨피그레이션

이러한 두 이벤트의 동작을 제어하는 2개의 플로우 컬렉터 컨피그레이션 매개변수가 주로 있습니다.

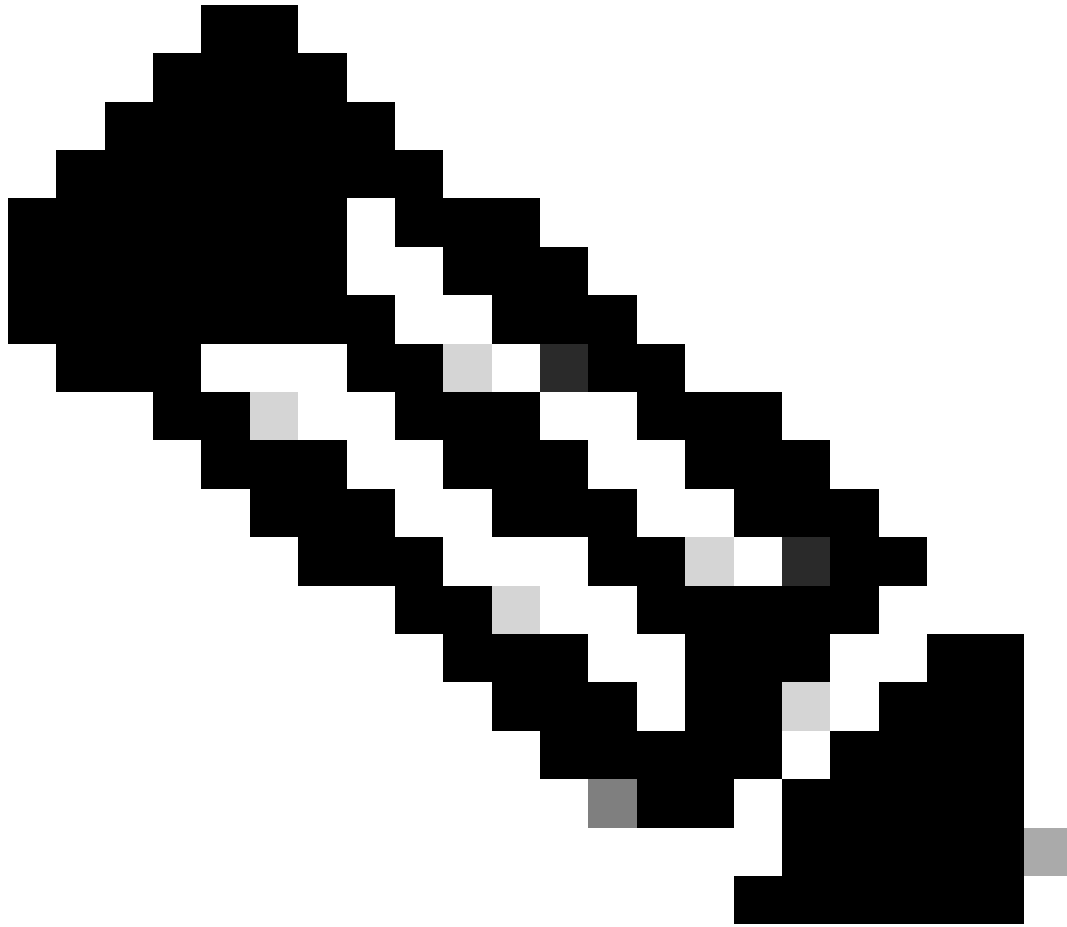
이러한 설정은 관리자 어플라이언스의 WebUI에서 Configure > Flow Collectors > Advanced 페이지에 액세스하여 조정할 수 있습니다.

- 흐름을 long duration 설정으로 정규화하는 데 필요한 시간(초)은 의심되는 long flow 이벤트의 동작을 제어합니다.



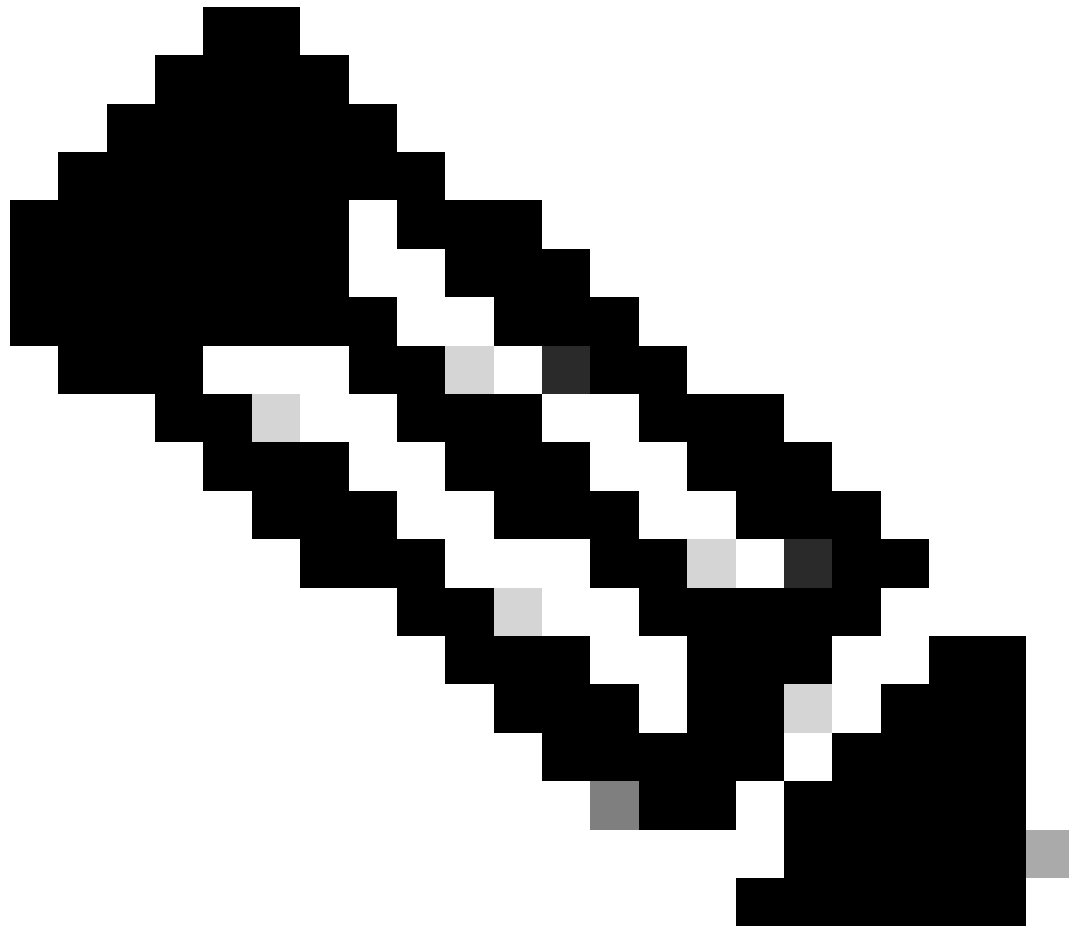
참고: webUI의 이 컨피그레이션 옵션은 flow collectors lc_thresholds.txt 컨피그레이션 파일에서 long_flow_duration 매개변수를 설정합니다.

-
- 폴로우를 Suspect Quiet Long Flow 설정으로 정규화하는 데 필요한 초 단위로 Suspect Quiet Long Flow 이벤트의 동작을 제어합니다.



참고: webUI의 이 컨피그레이션 옵션은 flow collectors lc_thresholds.txt 컨피그레이션 파일에서 quiet_long_flow_duration 매개변수를 설정합니다.

두 카운터의 기본값은 32400초(9시간)입니다.



참고: 이러한 카운터 변경과 관련된 CDET:

Cisco 버그 ID [CSCwm05128](#)



경고: 이는 v7.5.1 또는 이전 버전에만 적용됩니다.

이 결함은 의심스러운 조용한 긴 흐름이 먼저 의심스러운 긴 흐름이어야 함을 지시합니다. 즉, 폴로우를 Suspect Quiet Long Flow로 지정하는 데 필요한 초를 Long Duration 설정으로 지정하는 데 필요한 초보다 짧은 기간으로 변경하면 예기치 않은 결과가 발생할 수 있습니다.

이러한 고급 설정 중 하나 또는 둘 다를 변경할 경우 긴 흐름을 탐지하지 못할 수 있습니다.

정의에 따른 Quiet Long Flow도 Long Flow여야 하므로 이 두 설정을 적절하게 처리하는 논리는 Quiet Long Flow임을 테스트하기 전에 먼저 흐름이 Long Flow 요구 사항을 초과하도록 하는 것입니다.

예를 들어 long_flow_duration을 기본값인 9시간으로 유지하고 quiet_long_flow_duration을 8시간과 같은 더 낮은 값으로 설정하면 흐름이 9시간 이상 길어질 때까지 엔진은 자동 장기 흐름 이벤트를 발생시키지 않습니다.

또는 long_flow_duration이 기본값 9시간으로 유지되고 quiet_long_flow_duration이 10시간으로 설정된 경우, 이 컨피그레이션에서는 quiet_long_flow_duration이 10시간 이상인 단일 내보내기가 아

닌 한 quiet long duration 흐름 이벤트를 효과적으로 비활성화합니다.

솔루션

이러한 고급 설정은 모두 원하는 동일 한 값으로 설정 해야 합니다 또는 quiet_long_flow_duration은 항상 $\geq$ long_flow_duration으로 해야 합니다.

The screenshot displays the Cisco Secure Network Analytics interface for configuring a Flow Collector. The top navigation bar includes the Cisco logo, 'Secure Network Analytics', a search bar, and user information for 'Admin User'. The left sidebar contains navigation links: 'Configure', 'Monitor', 'Investigate', 'Report', and 'Apps'. The main content area is titled 'Flow Collector' and shows details for a specific collector: 'Name: fc-40-40', 'IP Address: 192.168.40.40', 'Model: Flow Collector NetFlow VE', and 'Serial: FCNFE-vMware-564de037119db18-3bb810372ca85d0e'. The 'Advanced' tab is selected, showing four sections: 'Broadcast List', 'Ignore List', 'Watch List', and 'Synchronize'. The 'Synchronize' section has a 'Synchronize' button. The 'Flow Collector Security Thresholds' section contains several checkboxes and input fields. The 'Seconds required to qualify a flow as long duration' is set to 32400. The 'Seconds required to qualify a flow as Suspect Quiet Long Flow' is also set to 32400. Other thresholds include 'Suspect Long Duration Flow trust threshold' (5), '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), and 'Minimum number of /24 subnets an infected host must contact before a Worm Activity or Worm Propagation alarm is triggered' (8).

Flow Collector

Name: fc-40-40 IP Address: 192.168.40.40 Model: Flow Collector NetFlow VE Serial: FCNFE-vMware-564de037119db18-3bb810372ca85d0e

Main Advanced

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.

Synchronize

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:

5

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.