FireSIGHT System과 eStreamer Client(SIEM) 간의 문제 해결

목차

소개

Event Streamer(eStreamer)를 사용하면 FireSIGHT 시스템에서 사용자 정의 개발 클라이언트 애플리케이션으로 여러 종류의 이벤트 데이터를 스트리밍할 수 있습니다. 클라이언트 애플리케이션을 생성한 후 이를 eStreamer 서버(예: FireSIGHT Management Center)에 연결하고 eStreamer 서비스를 시작하고 데이터 교환을 시작할 수 있습니다. eStreamer 통합에는 사용자 정의 프로그래밍이 필요하지만 어플라이언스에서 특정 데이터를 요청할 수 있습니다. 이 문서에서는 eStreamer 클라이언트가 통신하는 방법과 클라이언트 문제를 해결하는 방법에 대해 설명합니다.

eStreamer 클라이언트와 서버 간의 통신 방법

클라이언트와 eStreamer 서비스 간에는 다음과 같은 네 가지 주요 커뮤니케이션 단계가 있습니다.

1단계: 클라이언트가 eStreamer 서버와의 연결을 설정합니다.

먼저 클라이언트가 eStreamer 서버와의 연결을 설정하고 양쪽 당사자가 연결을 인증합니다. 클라이언트가 eStreamer에서 데이터를 요청하려면 먼저 클라이언트가 eStreamer 서비스와의 SSL 지원 TCP 연결을 시작해야 합니다. 클라이언트가 연결을 시작하면 eStreamer 서버가 응답하고 클라이언트와 SSL 핸드셰이크를 시작합니다. eStreamer 서버는 SSL 핸드셰이크의 일부로 클라이언트의 인증 인증서를 요청하고 인증서가 유효한지 확인합니다.

SSL 세션이 설정되면 eStreamer 서버는 인증서의 추가 연결 후 검증을 수행합니다. 연결 후 검증이 완료되면 eStreamer 서버는 클라이언트로부터 데이터 요청을 기다립니다.

2단계: 클라이언트가 eStreamer 서비스에서 데이터를 요청합니다.

이 단계에서는 클라이언트가 eStreamer 서비스에 데이터를 요청하고 스트리밍할 데이터 유형을 지정합니다. 단일 이벤트 요청 메시지는 이벤트 메타데이터를 포함하여 사용 가능한 이벤트 데이터의 임의의 조합을 지정할 수 있다. 단일 호스트 프로필 요청은 단일 호스트 또는 여러 호스트를 지정할 수 있습니다. 이벤트 데이터 및 콜론을 요청하기 위해 두 가지 요청 모드를 사용할 수 있습니다.

- **이벤트 스트림 요청:** 클라이언트는 요청된 이벤트 유형 및 각 유형의 버전을 지정하는 요청 플래그가 포함된 메시지를 전송하고 eStreamer 서버는 요청된 데이터를 스트리밍하여 응답합니다.
- **확장 요청:** 클라이언트는 이벤트 스트림 요청과 동일한 메시지 형식의 요청을 제출하지만 확장 요청에 대한 플래그를 설정합니다. 그러면 클라이언트와 eStreamer 서버 간의 메시지 상호 작용이 시작되고, 이를 통해 클라이언트는 추가 정보 및 이벤트 스트림 요청을 통해 사용할 수 없는 버전 조합을 요청합니다.

3단계: eStreamer에서 요청된 데이터 스트림 설정

이 단계에서 eStreamer는 요청된 데이터 스트림을 클라이언트에 설정합니다. 비활성 기간 동안 eStreamer는 정기적으로 null 메시지를 클라이언트로 전송하여 연결을 열어 둡니다. 클라이언트 또는 중간 호스트로부터 오류 메시지를 받으면 연결을 닫습니다.

4단계: 연결이 종료됩니다.

eStreamer 서버는 다음과 같은 이유로 클라이언트 연결을 닫을 수도 있습니다.

- 메시지를 보낼 때마다 오류가 발생합니다. 여기에는 비활성 기간 동안 전송되는 이벤트 데이터 메시지와 null 킵얼라이브 메시지 eStreamer가 모두 포함됩니다.
- 클라이언트 요청을 처리하는 동안 오류가 발생했습니다.
- 클라이언트 인증이 실패합니다(오류 메시지가 전송되지 않음).
- eStreamer 서비스를 종료하고 있습니다(오류 메시지가 전송되지 않음).

클라이언트에서 이벤트를 표시하지 않음

eStreamer 클라이언트 응용 프로그램에 이벤트가 표시되지 않는 경우 아래 단계에 따라 이 문제를 해결하십시오.

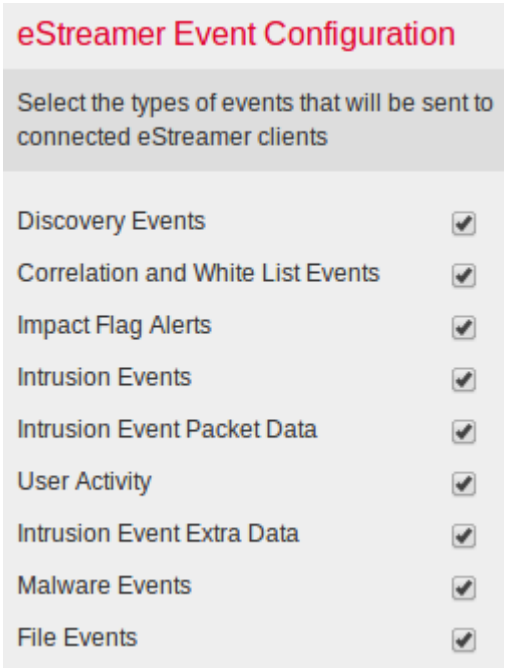
1단계: 구성 확인

eStreamer 서버가 이벤트를 요청하는 클라이언트 애플리케이션에 전송할 수 있는 이벤트 유형을 제어할 수 있습니다. eStreamer에서 전송하는 이벤트 유형을 구성하려면 다음 단계를 수행합니다.

1. **시스템 > 로컬 > 등록으로 이동합니다**.

2. eStreamer 탭을 **클릭합니다**.

3. eStreamer **Event Configuration** 메뉴에서 eStreamer가 요청 클라이언트로 전송할 이벤트 유형 옆의 확인란을 선택합니다.



> **참고:** 클라이언트 애플리케이션이 수신할 이벤트 유형을 요청하는지 확인합니다. 요청 메시지를 eStreamer 서버(FireSIGHT Management Center 또는 관리되는 디바이스)로 보내야 합니다.

4. 저장을 **클릭합니다**.

2단계: 인증서 확인

필요한 인증서가 추가되었는지 확인합니다. eStreamer가 eStreamer 이벤트를 클라이언트로 전송하려면 먼저 eStreamer 컨피그레이션 페이지를 사용하여 eStreamer 서버의 피어 데이터베이스에 클라이언트를 추가해야 합니다. eStreamer 서버에서 생성된 인증 인증서도 클라이언트에 복사해야 합니다.

3단계: 오류 메시지 확인

다음 명령을 사용하여 /var/log/messages에서 명백한 eStreamer 관련 오류를 식별합니다.

```
admin@FireSIGHT:~$ grep -i estreamer /var/log/messages | grep -i error
```

4단계: 연결 확인

서버가 수신 연결을 수락하는지 확인합니다.

```
admin@FireSIGHT:~$ netstat -an | grep 8302
```

출력은 다음과 같아야 합니다. 그렇지 않으면 서비스가 실행되고 있지 않을 수 있습니다.

```
tcp 0 0 <local_ip>:8302 0.0.0.0:* LISTEN
```

5단계: 프로세스 상태 확인

실행 중인 sfstreamer 프로세스가 있는지 확인하려면 다음 명령을 사용하십시오.

```
admin@FireSIGHT:~$ pstree -a | grep -i sfestreamer
```

클라이언트에서 중복 이벤트 표시

클라이언트에 표시되는 중복 이벤트 처리

eStreamer 서버는 전송한 이벤트의 기록을 보관하지 않으므로 클라이언트 응용 프로그램은 중복 이벤트를 확인해야 합니다. 여러 가지 이유로 중복 이벤트가 발생할 수 있습니다. 예를 들어, 새 스트리밍 세션을 시작할 때 클라이언트가 새 세션의 시작점으로 지정한 시간에 여러 개의 메시지가 있을 수 있습니다. 이 중 일부는 이전 세션에서 전송되었지만 일부는 전송되지 않았습니다. eStreamer는 지정된 요청 기준을 충족하는 모든 메시지를 보냅니다. EStreamer 클라이언트 애플리케이션은 결과로 발생하는 모든 중복을 탐지하고 중복 제거하도록 설계되어야 합니다.

데이터 중복 요청 관리

여러 플래그 또는 여러 확장 요청으로 동일한 데이터의 여러 버전을 요청하는 경우 가장 높은 버전이 사용됩니다. 예를 들어 eStreamer가 검색 이벤트 버전 1 및 6에 대한 플래그 요청과 버전 3에 대한 확장 요청을 수신하면 버전 6을 전송합니다.

클라이언트에서 잘못된 Snort 규칙 ID(SID)를 표시합니다.

이는 일반적으로 규칙을 시스템으로 가져오면 SID가 내부적으로 다시 매핑되는 SID 충돌로 인해 발생합니다.

다시 매핑된 SID가 아니라 입력한 SID를 사용하려면 확장 헤더를 *활성화해야 합니다*. 비트 23은 확장 이벤트 헤더를 요청합니다. 이 필드를 0으로 설정하면 레코드 유형 및 레코드 길이만 포함하는 표준 이벤트 헤더와 함께 이벤트가 전송됩니다.

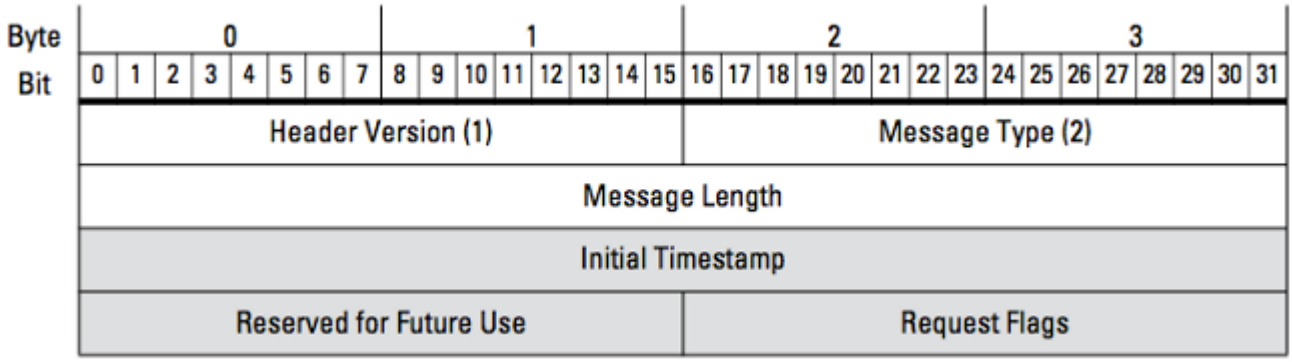


그림: 다이어그램은 eStreamer에서 데이터를 요청하는 데 사용되는 메시지 형식을 보여줍니다. 요청 메시지 형식에 해당하는 필드는 회색으로 강조 표시됩니다.

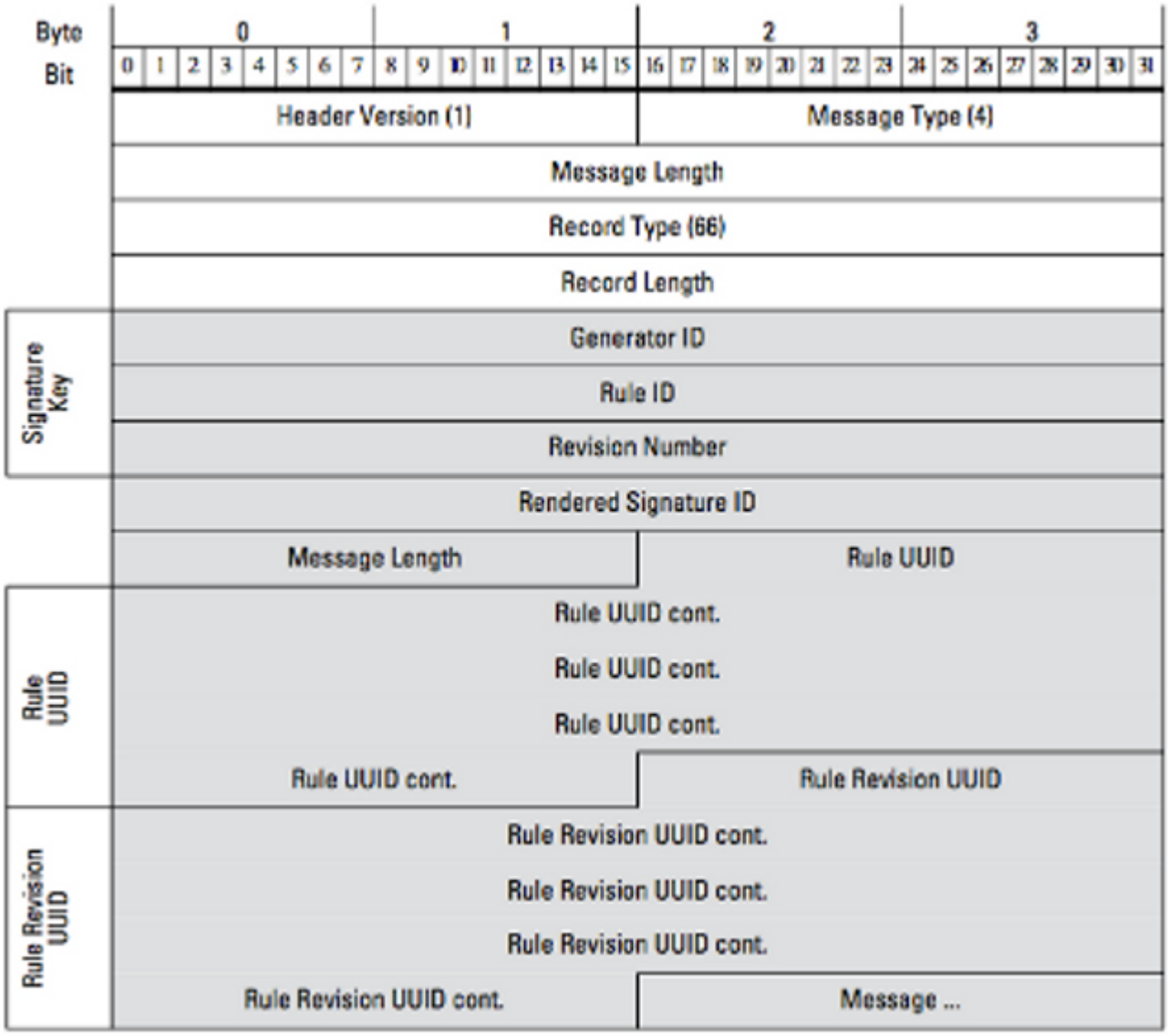


*그림: 이 다이어그램은 규칙 메시지 레코드 내에서 전송되는 이벤트에 대한 규칙 메시지 정보의 형식을 보여줍니다. RuleID(현재 사용 중)와 Rendered **Signature ID**(예상 번호)가 표시됩니다.*

팁: 각 비트 및 메시지에 대한 자세한 설명을 찾으려면 eStreamer 통합 *가이드를 참조하십시오*.

추가 문제 해결 데이터 수집 및 분석

ssl_test.pl 스크립트를 사용하여 테스트

*Event Streamer SDK(Software Development Kit)*에 제공된 ssl_test.pl *스크립트를 활용하여* 문제를 식별합니다. SDK는 지원 사이트의 zip 파일로 제공됩니다. 스크립트에 대한 지침은 zip 파일에 포함된 README.txt를 참조하십시오.

패킷 캡처(PCAP)

eStreamer 서버의 관리 인터페이스에서 패킷을 캡처하고 분석합니다. 네트워크 어딘가에서 트래픽이 차단되거나 거부되지 않았는지 확인합니다.

문제 해결 파일 생성

위의 문제 해결 단계를 완료했지만 여전히 문제를 확인할 수 없는 경우 FireSIGHT Management Center에서 문제 해결 파일을 생성하십시오. 추가 분석을 위해 모든 추가 문제 해결 데이터를 Cisco 기술 지원에 제공합니다.

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.