웹 사용자 인터페이스를 사용하여 패킷 데이터 (PCAP 파일) 다운로드

목차

소개

웹 사용자 인터페이스를 사용하여 Snort 규칙을 트리거한 패킷을 다운로드할 수 있습니다. 이 문서에서는 Sourcefire FireSIGHT Management System의 웹 사용자 인터페이스를 사용하여 PCAP 파일(패킷 캡처 데이터)을 다운로드하는 단계를 제공합니다.

사전 요구 사항

요구 사항

Cisco에서는 Sourcefire FirePOWER 디바이스 및 가상 디바이스 모델에 대한 지식을 습득할 것을 권장합니다.

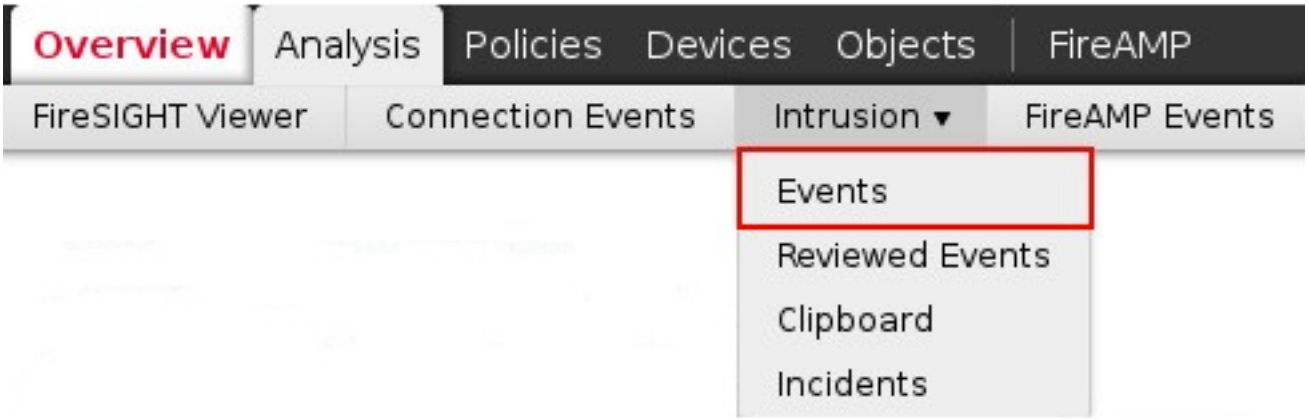
사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 5.2 이상을 실행하는 Defense Center라고도 하는 Sourcefire FireSIGHT Management Center를 기반으로 합니다.

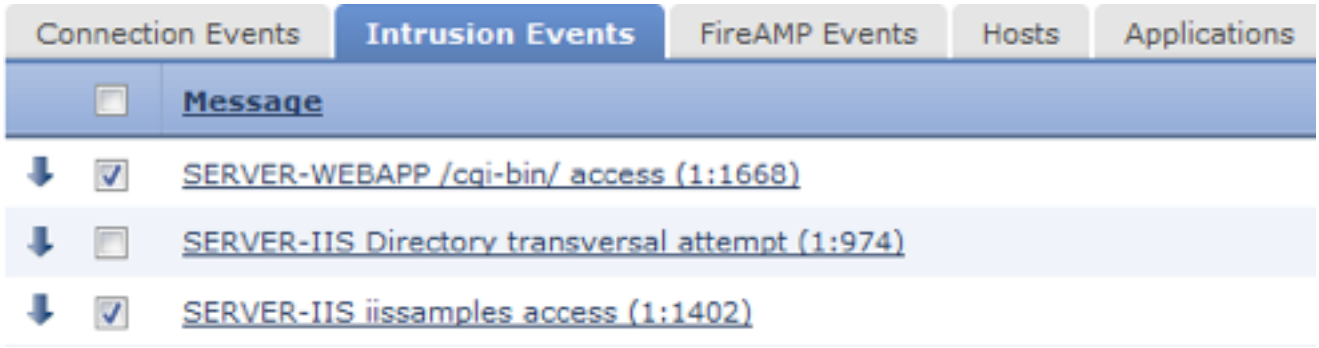
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

PCAP 파일 다운로드 단계

1단계: Sourcefire Defense Center 또는 Management Center에 로그인하고 다음과 같이 Intrusion Events 페이지로 이동합니다.



2단계:확인란을 사용하여 패킷 캡처 데이터(PCAP 파일)를 다운로드할 이벤트를 선택합니다.



3단계:페이지 아래쪽으로 스크롤하여 다음 중 하나를 수행합니다.

- 선택한 침입 이벤트를 트리거한 패킷을 다운로드하려면 Download Packet을 클릭합니다.
- 현재 제한된 보기에서 침입 이벤트를 트리거한 모든 패킷을 다운로드하려면 Download All Packets를 클릭합니다.

참고:다운로드한 패킷은 PCAP로 저장됩니다. 패킷 캡처를 분석하려면 PCAP 파일을 읽을 수 있는 소프트웨어를 다운로드하여 설치해야 합니다.

4단계:메시지가 표시되면 PCAP 파일을 하드 드라이브에 저장합니다.