소개

개요

이 가이드에서는 더 긴 보존 기간에 스토리지를 늘리기 위해 방화벽 이벤트 데이터를 저장하도록 Cisco Security Analytics 및 로깅(온프레미스) 구성을 하는 방법을 설명합니다. Cisco Secure Network Analytics(이전 Stealthwatch) 어플라이언스를 구축하고 방화벽 구축과 통합하면 Secure Network Analytics 어플라이언스로 이벤트 데이터를 내보낼 수 있습니다.

다음을 할 수 있습니다.

- Secure Firewall Management Center에 이벤트를 저장하고 Secure Network Analytics 구축에 이벤트를 저장합니다.
- management center에서 이러한 이벤트를 보려면 이 원격 데이터 소스를 지정합니다.
- 이벤트 뷰어를 사용하여 Cisco Secure Network Analytics Manager(이전 Stealthwatch Management Console) 웹 애플리케이션 UI에서 이벤트 데이터를 검토합니다.
- management center UI에서 이벤트 뷰어로 크로스 실행하여 크로스 실행한 정보에 대한 추가 컨텍스트를 확인합니다.

참고 온프레미스가 아니라 Cisco 클라우드에 방화벽 이벤트 데이터를 저장하려는 경우 Cisco SaaS(Security Analytics and Logging) 설명서에서 자세한 내용을 참조하십시오.

개념 및 아키텍처

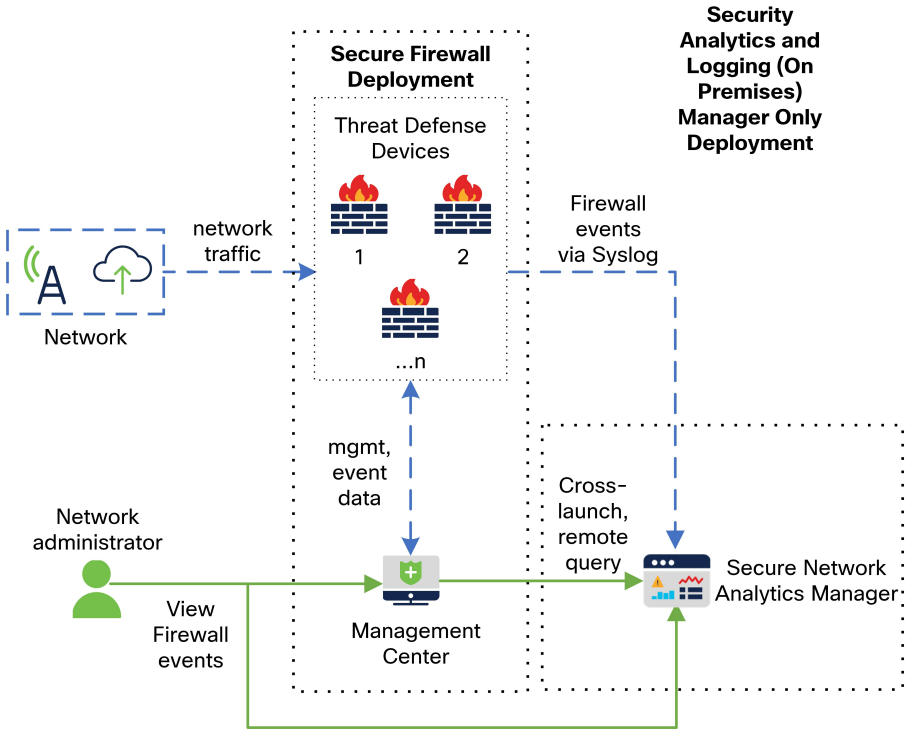
Security Analytics and Logging(온프레미스)구축에서 어플라이언스를 사용Secure Network Analytics하여 다른 Cisco 제품 구축의 데이터를 저장할 수 있습니다. 보안 방화벽 구축의 경우 management center에서 관리하는 Secure Firewall Threat Defense 디바이스에서 보안 이벤트 및 데이터 플레인 이벤트를 관리자에 내보내 해당 정보를 저장할 수 있습니다.

Secure Network Analytics 구축에는 두 가지 옵션이 있습니다.

- 관리자 전용 - 이벤트를 수신 및 저장하는 독립형 관리자 구축, 이벤트의 검토 및 쿼리 가능
- 데이터 저장소 - 이벤트를 수신할 Cisco Secure Network Analytics 플로우 컬렉터(최대 5개), 이벤트를 저장할 Cisco Secure Network Analytics 데이터 노드 1~3개 이상(3개 세트)을 포함하는 Cisco Secure Network Analytics 데이터 저장소 구축 이벤트를 검토하고 쿼리할 수 있는 관리자

관리자 전용

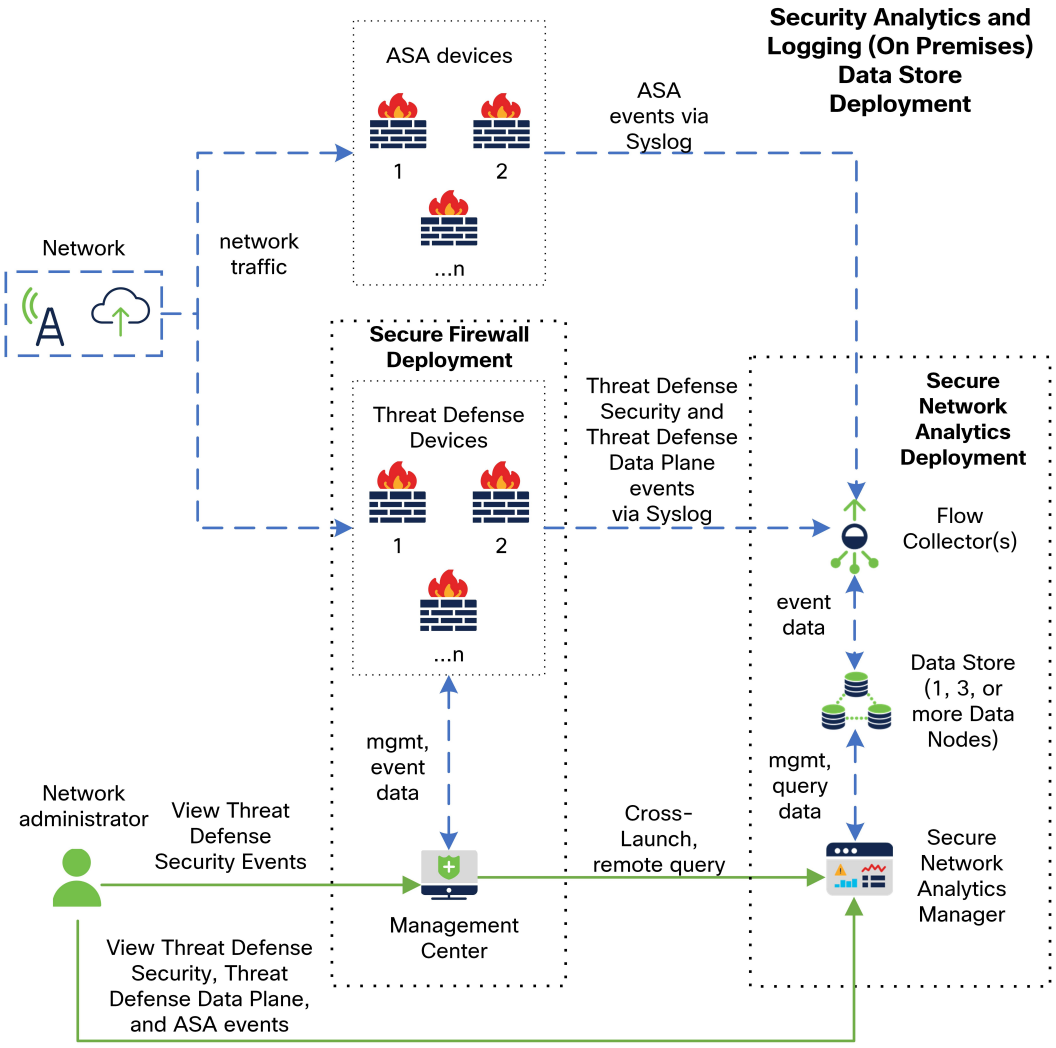
다음 다이어그램에서 관리자 전용 구축의 예를 참조하십시오.



이 구축에서 threat defense 디바이스는 관리자(으)로 보안 방화벽 이벤트를 전송하고, 관리자는 이러한 이벤트를 저장합니다. 사용자는 management center UI에서 관리자에 교차 실행하여 저장된 이벤트에 대한 세부 정보를 볼 수 있습니다. 또한 management center에서 이벤트를 원격으로 쿼리할 수 있습니다.

데이터 저장소

다음 다이어그램에서 관리자, 데이터 노드 및 플로우 컬렉터가 있는 데이터 저장소 구축의 예를 참조하십시오.



이 구축에서 threat defense 및 보안 방화벽 ASA 디바이스는 플로우 컬렉터로 방화벽 이벤트를 전송합니다. 플로우 컬렉터는 데이터 저장소로 이벤트를 전송하여 저장합니다. 사용자는 management center UI에서 관리자에 교차 실행하여 저장된 이벤트에 대한 세부 정보를 볼 수 있습니다. 또한 management center에서 이벤트를 원격으로 쿼리할 수 있습니다.

지원되는 이벤트 유형

- Threat Defense 보안 이벤트
  - 연결
  - 침입
  - 파일 및 악성코드
- Threat Defense 데이터 플레인 이벤트(데이터 저장소 구축만 해당)

- ASA 이벤트(데이터 저장소 구축만 해당)