Cisco Security Analytics and Logging

정보 Security Analytics and Logging

Security Analytics and Logging(SAL)은 확장 가능한 Cisco 방화벽 로깅 및 상관관계 분석을 제공하는 중앙 로그 관리 및 고급 위협 탐지 서비스입니다. 중앙 로깅은 가시성을 제공하고, 중단을 비롯한 네트워크 액세스 문제를 해결하고, 디바이스 및 전체 네트워크 상태 모니터링을 활성화하는 데 도움이 됩니다. 분석은 지능형 위협에 대한 탐지를 제공합니다.

SAL 서비스는 다음 두 가지 방법으로 사용할 수 있습니다.

- Security Analytics and Logging(SaaS) — Secure Cloud Analytics(이전의 Stealthwatch Cloud)를 사용하여 이벤트를 저장하고 보안 분석용 데이터를 제공하는 호스팅된 SaaS(Software as a Service)입니다. 이 서비스는 Security Analytics 및 Logging 클라우드 데이터 저장소를 방화벽 클라우드 관리자, Cisco Defense Orchestrator(CDO)에 연결합니다.

  이 설명서에서는 이 방법을 SAL(SaaS)라고도 합니다.

- Security Analytics and Logging(보안 애널리틱스) — Secure Network Analytics(이전의 Stealthwatch) 어플라이언스에서 실행되어 고객의 프레미스에 이벤트 로그를 저장하는 서비스입니다. 이 서비스는 Security Analytics and Logging(보안 애널리틱스) 데이터를 온프레미스 관리자, Secure Firewall Management Center에 연결합니다.

  이 설명서에서는 이 방법을 SAL(온프레미스)라고도 합니다.

Security Analytics and Logging에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html을 참조하십시오.

SAL 원격 이벤트 스토리지 및 모니터링 옵션 비교

SAL 통합에서는 management center 및 CDO의 외부에 이벤트 데이터를 저장하는 유사한 옵션을 보여 줍니다.

	SAL(온프레미스)	**SAL(SaaS)**
이 솔루션을 선택 하는 이유	온프레미스 방화벽 이벤트 데이터 스토리지 용량을 늘리고, 이 데이터를 더 오랫동안 보존하고, 이벤트 데이터를 Secure Network Analytics 어플라이언스로 내보내려고 합니다.	스토리지를 위해 방화벽 이벤트를 전송하고, 필요에 따라 Secure Cloud Analytics를 사용하여 보안 분석에 방화벽 이벤트 데이터를 제공할 수 있습니다.
라이선싱	방화벽 뒤에서 스토리지 시스템을 구매, 라이선싱, 설정합니다. 자세한 내용은 라이선싱: SAL(온프레미스), 3 페이지 항목을 참조하십시오.	라이선스 및 데이터 스토리지 요금제를 구매하고 Cisco 클라우드로 데이터를 전송합니다. 자세한 내용은 라이선싱: SAL(SaaS), 9 페이지 항목을 참조하십시오.
지원되는 이벤트 유형	• 연결 • 파일 및 악성코드 • 침입 • LINA • 보안 인텔리전스	• 연결 • 파일 및 악성코드 • 침입 • 보안 인텔리전스
지원되는 이벤트 전송 방법	시스템 로그 및 직접 통합을 모두 지원합니다.	시스템 로그 및 직접 통합을 모두 지원합니다.
이벤트 보기	• Secure Network Analytics Manager에서 이벤트를 확인합니다. • management center 이벤트 뷰어에서 교차 실행하여 Secure Network Analytics Manager의 이벤트를 확인합니다. • 관리 센터에 원격으로 저장된 연결 및 보안 인텔리전스 이벤트를 봅니다.	라이선스에 따라 CDO 또는 Secure Network Analytics Manager의 이벤트를 확인합니다. management center 이벤트 뷰어에서 교차 실행합니다.

정보 SAL(온프레미스)

더 긴 보존 기간에 스토리지를 늘리기 위해 방화벽 이벤트 데이터를 저장하도록 SAL(온프레미스)을 구성할 수 있습니다. Secure Network Analytics 어플라이언스를 배포하고 방화벽 구축과 통합하면 이벤트 데이터를 Secure Network Analytics 어플라이언스로 내보낼 수 있습니다.

이를 통해 다음과 같은 기능이 제공됩니다.

- Secure Network Analytics 어플라이언스에 이벤트를 저장합니다.
- 관리 센터에서 이러한 이벤트를 보려면 이 원격 데이터 소스를 지정합니다.
- 이벤트 뷰어를 사용하여 Secure Network Analytics Manager(이전 Stealthwatch Management Console) 웹 앱 UI에서 이벤트 데이터를 검토합니다.
- 관리 센터 UI에서 이벤트 뷰어로 크로스 실행하여 크로스 실행한 정보에 대한 추가 컨텍스트를 확인합니다.

라이선싱: SAL(온프레미스)

SAL(온프레미스)을 사용하려면 Logging and Troubleshooting(기록 및 문제 해결) 스마트 라이선스를 얻어야 합니다. 매일 방화벽 구축에서 Secure Network Analytics 어플라이언스로 시스템 로그 데이터를 전송하는 동안 예상되는 데이터의 양에 따라 라이선스를 얻을 수 있습니다.

Secure Network Analytics 어플라이언스 라이선스에 대한 자세한 내용은 Secure Network Analytics 스마트 소프트웨어 라이선싱 가이드를 참조하십시오.

SAL(온프레미스) 라이선싱 옵션에 대한 자세한 내용은 Cisco Security Analytics and Logging 주문 가이드를 참조하십시오.

참고 라이선스 계산을 위해 데이터의 양은 가장 가까운 전체 GB로 보고됩니다. 예를 들어 하루에 4.9GB를 전송하는 경우 4GB로 보고됩니다.

CDO 매니지드 Threat Defense 디바이스에 대해 SAL(온프레미스) 관리

Secure Firewall Threat Defense(이전 Firepower Threat Defense) 버전 7.2부터는 CDO 매니지드 threat defense 디바이스에서 생성된 정규화된 이벤트를 management center로 전송하도록 선택할 수 있습니다. 는 이러한 이벤트에 대한 데이터 분석을 수신하고 표시합니다.management center 이벤트 데이터를 수신하고 표시하는 management center을 분석 전용 관리 센터라고도 합니다.

디바이스가 SAL(온프레미스)을(를) 사용하여 Secure Network Analytics Manager에 연결 이벤트를 전송하도록 활성화된 경우, 관리 센터 이벤트 뷰어 및 상황 탐색기에서 원격으로 저장된 이벤트를 확인

하고 작업을 수행하고 보고서를 생성할 때 해당 이벤트를 포함할 수 있습니다. Secure Network Analytics 어플라이언스를 구축하고 방화벽 구축과 통합하면 이벤트 데이터를 Secure Network Analytics 어플라이언스로 내보낼 수 있습니다. 이렇게 하면 관리 센터 UI에서 이벤트를 보고 관리할 수 있습니다. Management Center 인터페이스에서 Secure Network Analytics Manager를 교차 실행하여 이벤트 데이터를 보고 관리할 수도 있습니다.

관리 센터는 다음과 같은 CDO 매니지드 threat defense 디바이스에 대한 이벤트 분석을 수신하고 표시할 수 있습니다.

- CDO에 온보딩된 신규 또는 기존 threat defense 디바이스

  threat defense 디바이스를 CDO에 온보딩하는 방법에 대한 자세한 내용은 디바이스를 클라우드 사용 Firewall Management Center에 온보딩하기 위한 사전 요건 섹션을 참조하십시오.

  워크플로우는 다음과 같습니다.

  1. CDO에 threat defense 디바이스를 온보딩합니다.

     디바이스를 클라우드 사용 Firewall Management Center에 온보딩하기 위한 사전 요건에 설명된 온보딩 방법을 사용하여 threat defense 디바이스를 온보딩합니다. 온보딩 프로세스에는 정책 할당 및 적절한 라이선스 선택이 포함됩니다.

  2. 해당 관리 센터에서 이 threat defense 디바이스를 등록합니다.

     CDO 매니지드 threat defense 디바이스에서 생성된 이벤트를 관리 센터에 표시하려면 관리 센터에서 threat defense 디바이스를 등록해야 합니다. management center에서 이 디바이스를 등록하려면 **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address*}*reg_key*[*nat_id*] CLI로 이동한 다음 **CDO Managed Device(CDO** 매니지드 디바이스**)** 확인란을 사용하여 management center에 디바이스를 추가합니다.

     참고 등록 키 및 NAT ID는 디바이스를 CDO에 온보딩하는 동안 사용되는 것과 고유해야 합니다.

     자세한 내용은 Firepower Management Center 디바이스 구성 가이드의 *Management Center*에 디바이스 추가 및 *CLI*를 사용하여 *Threat Defense* 초기 구성 완료를 참조하십시오.

  3. 관리 센터에서 이벤트를 보거나 구성된 Secure Network Analytics Manager에 대한 교차 실행

     관리 센터 이벤트 뷰어에서 이벤트를 보고 작업합니다. Secure Network Analytics 어플라이언스가 구축되고 방화벽 구축과 통합된 경우 이벤트 데이터를 Secure Network Analytics 어플라이언스로 내보낼 수 있습니다. 이를 통해 관리 센터 UI에서 Secure Network Analytics Manager로 교차 실행하여 이벤트 데이터를 보고 관리할 수 있습니다.

     자세한 내용은 이벤트 및 자산 및 외부 도구를 사용한 이벤트 분석을 참조하십시오.

- 관리 센터의 기존 threat defense 디바이스

  Threat Defense Manager 변경 기능을 사용하여 threat defense 디바이스 관리를 관리 센터에서 CDO로 변경할 수 있습니다. Threat Defense Manager 변경 기능은 threat defense 디바이스 관리를 관리 센터에서 CDO로 변경할 수 있는 기능을 제공합니다. 관리자를 변경하는 동안 이러한 위협 방어

디바이스에 의해 생성된 이벤트 데이터를 관리 센터에 유지하도록 선택할 수 있습니다. 이벤트 데이터를 관리 센터에 유지하도록 선택하면 분석 전용 모드의 threat defense 디바이스 사본이 관리 센터에 보존됩니다.

자세한 내용은 Secure Firewall Threat Defense를 클라우드로 마이그레이션을 참조하십시오.

워크플로우는 다음과 같습니다.

1. CDO에 관리 센터 온보딩

   관리 센터에서 CDO로 기존 threat defense 디바이스를 온보딩하려면 해당 관리 센터를 CDO에 온보딩해야 합니다.

   자세한 내용은 FMC 온보딩을 참조하십시오.

2. 위협 방어 관리 프로세스 변경 완료

   위협 방어 관리 프로세스 변경 중에 디바이스 관리자를 변경하는 동안 이러한 threat defense 디바이스에서 생성된 이벤트 데이터를 관리 센터에 유지하도록 선택할 수 있습니다.

   자세한 내용은 Secure Firewall Threat Defense를 클라우드로 마이그레이션을 참조하십시오.

3. 관리 센터에서 이벤트를 보거나 구성된 Secure Network Analytics 어플라이언스에 대해 교차 실행합니다.

   관리 센터 이벤트 뷰어에서 이벤트를 보고 작업합니다. Secure Network Analytics 어플라이언스가 구축되고 방화벽 구축과 통합된 경우 이벤트 데이터를 Secure Network Analytics 어플라이언스로 내보낼 수 있습니다. 이를 통해 관리 센터 UI에서 Secure Network Analytics Manager로 교차 실행하여 이벤트 데이터를 보고 관리할 수 있습니다.

   자세한 내용은 이벤트 및 자산 및 외부 도구를 사용한 이벤트 분석을 참조하십시오.

SAL(온프레미스) 통합 구성

다음 구축 옵션 중 하나를 사용하여 Secure Network Analytics 어플라이언스에 이벤트를 전송하도록 CDO를 구성할 수 있습니다.

- Secure Network Analytics Manager Only(보안 네트워크 분석 관리자만 해당) - 독립형 관리자를 구축하여 이벤트를 수신하고 저장합니다. 위협 방어 디바이스는 이벤트 데이터를 Network Analytics Manager로 전송합니다. 모든 이벤트 데이터는 Network Analytics Manager에 저장됩니다. 관리 센터 사용자 인터페이스에서 관리자를 교차 실행하여 저장된 이벤트에 대한 자세한 정보를 볼 수 있습니다.
- Secure Network Analytics 데이터 저장소 - 이벤트를 수신할 Cisco Secure Network Analytics Flow Collector, 이벤트를 저장할 Cisco Secure Network Analytics 데이터 저장소(3개의 Cisco Secure Network Analytics Data Nodes 포함) 및 관리자를 구축합니다. 위협 방어 디바이스는 이벤트 데이터를 플로우 컬렉터로 전송하며, 여기서 이벤트는 저장을 위해 데이터 저장소로 전송됩니다. 관리 센터 사용자 인터페이스에서 관리자를 교차 실행하여 저장된 이벤트에 대한 자세한 정보를 볼 수 있습니다.

threat defense 버전 7.2부터는 서로 다른 플로우 컬렉터를 서로 다른 디바이스에 연결하도록 선택할 수 있습니다.

Secure Network Analytics Manager 구성

CDO 매니지드 threat defense디바이스와 SAL(온프레미스)가 통합되도록 Secure Network Analytics Manager 구축을 구성합니다.

시작하기 전에

다음이 필요합니다.

- 프로비저닝된 CDO 테넌트가 있고 다음과 같은 CDO 사용자 역할이 있어야 합니다.
  - Admin(관리자)
  - 슈퍼 관리자
- threat defense 디바이스가 예상대로 작동하고 이벤트를 생성하고 있습니다.
- 현재 시스템 로그를 사용하여 이벤트를 직접 전송하는 것을 지원하는 디바이스 버전에서 Secure Network Analytics Manager에 이벤트를 전송하는 경우, 원격 볼륨에서 이벤트가 중복되지 않도록 해당 디바이스에 대해 시스템 로그를 비활성화합니다(또는 시스템 로그 구성을 포함하지 않는 액세스 제어 정책을 해당 디바이스에 할당).
- 사용자에게 Secure Network Analytics Manager의 호스트 이름이나 IP 주소가 있습니다.

참고 등록 프로세스 중에 Secure Network Analytics Manager에서 로그아웃될 수 있습니다. 구축 마법사를 시작하기 전에 진행 중인 작업을 완료하십시오.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 탐색합니다.

단계 **3** **Firewall Management Center**를 선택하고 **Configuration(**구성**)**을 클릭합니다.

단계 **4** **Integration(**통합**)** > **Security Analytics & Logging(**보안 분석 및 로깅**)**으로 이동합니다.

단계 **5** **Secure Network Analytics Manager** 전용 위젯에서 **Start(**시작**)**을 클릭합니다.

단계 **6** Secure Network Analytics Manager의 호스트 이름 또는 IP 주소와 포트 번호를 입력하고 **Next(**다음**)**를 클릭합니다.

단계 **7** 매니지드 디바이스에 변경 사항을 구축합니다.

이벤트 데이터는 로깅 정책 변경 사항이 등록된 threat defense 디바이스에 구축될 때까지 SAL(온프레미스)에 로깅되지 않습니다.

참고 이러한 구성을 변경해야 하는 경우 마법사를 다시 실행합니다. 구성을 비활성화하거나 마법사를 다시 실행하면 계정 자격 증명을 제외한 모든 설정이 유지됩니다.

관리 센터의 이벤트 뷰어 및 컨텍스트 탐색기에서 이러한 원격으로 저장된 이벤트를 보고 작업할 수 있으며 보고서를 생성할 때 이를 포함할 수 있습니다. 관리센터의 이벤트에서 교차 실행하여 Secure Network Analytics 어플라이언스의 관련 데이터를 볼 수도 있습니다.

자세한 내용은 관리 센터에 대한 온라인 도움말을 참조하십시오.

단계 **8** **OK(**확인**)**를 클릭합니다.

Secure Network Analytics 데이터 저장소 구성

CDO에서 관리하는 threat defense 디바이스와 SAL(온프레미스)를 통합하도록 Secure Network Analytics 데이터 저장소 구축을 구성합니다.

시작하기 전에

다음이 필요합니다.

- 프로비저닝된 CDO 테넌트가 있고 다음과 같은 CDO 사용자 역할이 있어야 합니다.
  - Admin(관리자)
  - 슈퍼 관리자
- threat defense 디바이스가 예상대로 작동하고 이벤트를 생성하고 있습니다.
- 현재 시스템 로그를 사용하여 이벤트를 직접 전송하는 것을 지원하는 디바이스 버전에서 Secure Network Analytics appliance에 이벤트를 전송하는 경우, 원격 볼륨에서 이벤트가 중복되지 않도록 해당 디바이스에 대해 시스템 로그를 비활성화합니다(또는 시스템 로그 구성을 포함하지 않는 액세스 제어 정책을 해당 디바이스에 할당).
- 다음 정보를 수집합니다.
  - Secure Network Analytics Manager의 호스트 이름이나 IP 주소.
  - 플로우 컬렉터의 IP 주소.

참고 등록 프로세스 중에 Secure Network Analytics Manager에서 로그아웃될 수 있습니다. 구축 마법사를 시작하기 전에 진행 중인 작업을 완료하십시오.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 탐색합니다.

단계 **3** **Firewall Management Center**를 선택하고 **Configuration(**구성**)**을 클릭합니다.

단계 **4** **Integration(**통합**)** > **Security Analytics & Logging(**보안 분석 및 로깅**)**으로 이동합니다.

단계 **5** **Secure Network Analytics** 데이터 저장소 위젯에서 **Start(**시작**)**를 클릭합니다.

단계 **6** 플로우 컬렉터의 호스트 이름 또는 IP 주소와 포트 번호를 입력합니다.

플로우 컬렉터를 더 추가하려면 **+Add another Flow Collector(+** 다른 플로우 컬렉터 추가**)**를 클릭합니다.

단계 **7** 둘 이상의 플로우 컬렉터를 구성한 경우 다른 플로우 컬렉터와 관리 디바이스를 연결합니다.

참고 기본적으로 모든 관리 디바이스는 기본 플로우 컬렉터에 할당됩니다.

a) 디바이스 할당을 클릭합니다.
b) 할당할 매니지드 디바이스를 선택합니다.
c) 디바이스 재할당 드롭다운 목록에서 플로우 컬렉터를 선택합니다.

관리 디바이스가 플로우 컬렉터에 이벤트 데이터를 전송하지 않도록 하려면 해당 디바이스를 선택하고, 디바이스 재할당 드롭다운 목록에서 플로우 컬렉터에 로깅하지 않음을 선택합니다.

원하는 플로우 컬렉터 위로 마우스를 이동하고 **Set default(**기본값 설정**)**을 클릭하여 기본 플로우 컬렉터를 변경할 수 있습니다.

d) **Apply Changes(**변경 사항 적용**)**를 클릭합니다.
e) **Next(**다음**)**를 클릭합니다.

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** 등록된 매니지드 디바이스에 변경 사항을 구축합니다.

이벤트 데이터는 로깅 정책 변경 사항이 등록된 threat defense 디바이스에 구축될 때까지 SAL(온프레미스)에 로깅되지 않습니다.

참고 이러한 구성을 변경해야 하는 경우 마법사를 다시 실행합니다. 구성을 비활성화하거나 마법사를 다시 실행하면 계정 자격 증명을 제외한 모든 설정이 유지됩니다.

관리 센터의 이벤트 뷰어 및 컨텍스트 탐색기에서 이러한 원격으로 저장된 이벤트를 보고 작업할 수 있으며 보고서를 생성할 때 이를 포함할 수 있습니다. 관리센터의 이벤트에서 교차 실행하여 Secure Network Analytics Manager의 관련 데이터를 볼 수도 있습니다.

자세한 내용은 관리 센터에 대한 온라인 도움말을 참조하십시오.

정보 SAL(SaaS)

SAL(SaaS)를 사용하면 모든 위협 방어 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트를 캡처하고, CDO의 한 곳에서 볼 수 있습니다. 이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다.

추가 라이선싱을 사용하면 이러한 이벤트를 캡처한 후 CDO에서 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다. Secure Cloud Analytics는 이벤트 및 네트워크 플로우 데이터에 대한 행동 분석을 수행하여 네트워크의 상태를 추적하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

라이선싱: SAL(SaaS)

SAL(SaaS) 라이센스를 사용하면 CDO 테넌트를 사용하여 두 제품 모두에 대한 별도의 라이센스를 보유하지 않고 방화벽 로그와 분석용 Cisco Secure Cloud Analytics 인스턴스를 볼 수 있습니다.

SAL(SaaS) 라이선싱 옵션에 대한 자세한 내용은 Cisco Security Analytics and Logging 주문 가이드를 참조하십시오.

SAL(SaaS) 통합 구성

이 통합을 구축하려면 시스템 로그 또는 직접 연결을 사용하여 SAL(SaaS)에서 이벤트 데이터 스토리지를 설정해야 합니다.

- 시스템 로그를 사용하여 SAL(SaaS)로 이벤트 전송, 10 페이지
- 직접 연결을 사용하여 SAL(SaaS)에 이벤트 전송, 13 페이지

SAL(SaaS) 통합 요구사항

요구 사항 유형	요건
Cisco Secure Firewall Threat Defense	• CDO 관리 독립형 위협 방어 디바이스, 버전 7.2 이상. • 시스템 로그: 위협 방어 버전 6.4 이상을 사용하여 이벤트를 전송 • 이벤트를 직접 전송하려면 위협 방어 버전 7.2 • 방화벽 시스템을 구축하고 이벤트를 성공적으로 생성해야 합니다.
지역 클라우드	• 이벤트를 전송할 지역 클라우드를 결정합니다. • 이벤트는 다른 지역 클라우드에서 보거나 이동할 수 없습니다. • SecureX 또는 Cisco SecureX 위협 방어와 통합하기 위해 클라우드에 이벤트를 전송하기 위해 직접 연결을 사용하는 경우 이 통합에 대해 동일한 지역 CDO 클라우드를 사용해야 합니다. • 이벤트를 직접 전송하는 경우 CDO에서 지정하는 지역 클라우드가 CDO 테넌트의 지역과 일치해야 합니다.
데이터 요금제	• Cisco Cloud가 매일 위협 방어 디바이스로부터 받는 이벤트 수를 반영하는 데이터 계획을 구입해야 합니다. 이를 "일일 수집 속도"라고 합니다. • 데이터 스토리지 요구 사항을 예측하려면 로깅 볼륨 에스티메이터 툴을 사용합니다.
어카운트	이 통합을 위한 라이센스를 구매하면 통합을 지원하기 위한 CDO 테넌트 계정이 제공됩니다.

시스템 로그를 사용하여 SAL(SaaS)로 이벤트 전송

이 절차에서는 CDO에서 관리하는 디바이스에서 보안 이벤트(연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트)에 대한 시스템 로그 메시지를 전송하기 위한 모범 사례 설정을 설명합니다.

시작하기 전에

- 보안 이벤트를 생성하도록 정책을 구성하고 표시될 것으로 예상되는 이벤트가 Analysis(분석) 메뉴의 해당 테이블에 나타나는지 확인합니다.
- 시스템 로그 서버 IP 주소, 포트 및 프로토콜(UDP 또는 TCP)을 수집합니다.

CDO 브라우저 창의 오른쪽 상단에 있는 사용자 메뉴에서 **Secure Connector(**보안 커넥터**)**를 선택하여 필요한 정보를 확인합니다.

- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 탐색합니다.

단계 **3** **Firewall Management Center**를 선택하고 **Configuration(**구성**)**을 클릭합니다.

단계 **4** 위협 방어 디바이스에 대한 시스템 로그 설정을 구성합니다.

a) **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**로 이동하여 위협 방어 디바이스와 연결된 플랫폼 설정 정책을 편집합니다.

b) 왼쪽 탐색 창에서 **Syslog(**시스템 로그**)**를 클릭하고 다음과 같이 시스템 로그 설정을 구성합니다.

클릭합니다**.**	다음을 수행하려면
로깅 설정	로깅을 활성화하고 FTP 서버 설정 및 플래시 사용량을 지정합니다.
로그 대상	특정 대상에 대한 로깅을 활성화하고 메시지 심각도 수준, 이벤트 클래스 또는 사용자 지정 이벤트 목록에 대한 필터링을 지정합니다.
이메일 설정	이메일로 전송되는 시스템 로그 메시지의 소스 주소로 사용할 이메일 주소를 지정합니다.
이벤트 목록	이벤트 클래스, 심각도 레벨 및 이벤트 ID를 포함하는 사용자 지정 이벤트 목록을 정의합니다.
속도 제한	구성된 모든 대상에 전송되는 메시지의 양을 지정하고 속도 제한을 할당할 메시지 심각도 레벨을 정의합니다.
Syslog 설정	로깅 기능을 지정하고 타임스탬프 추가를 활성화하며, 다른 설정을 활성화하여 서버를 시스템 로그 대상으로 설정합니다.
Syslog 서버	로깅 대상으로 지정된 시스템 로그 서버의 IP 주소, 사용된 프로토콜, 형식 및 보안 영역을 지정합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **5** 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 구성합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동하여 위협 방어 디바이스와 연결된 액세스 제어 정책을 편집합니다.

b) **Logging(**로깅**)** 탭을 클릭하고 다음과 같이 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 구성합니다.

클릭합니다**.**	다음을 수행하려면
특정 시스템 로그 알림을 사용해 전송	기존의 미리 정의된 기존 경고 목록에서 시스템 로그 경고를 선택하거나 이름, 로깅 호스트, 포트, 기능 및 심각도를 지정하여 경고를 추가합니다.
디바이스에 구축된 **FTD** 플랫폼 설정 정책에 구성된 시스템 로그 설정을 사용합니다**.**	플랫폼 설정에서 구성하여 시스템 로그 구성을 통합하고 액세스 제어 정책에서 설정을 재사용합니다. 선택한 심각도는 모든 연결 및 침입 이벤트에 적용됩니다. 기본 심각도는 ALERT입니다.
IPS 이벤트에 대한 **Syslog** 메시지 보내기	이벤트를 시스템 로그 메시지로 전송합니다. 재정의하지 않는 한 위에 설정된 기본값이 사용됩니다.
파일 및 악성코드 이벤트에 대한 **Syslog** 메시지 전송	파일 및 악성코드 이벤트를 시스템 로그 메시지로 보냅니다. 재정의하지 않는 한 위에 설정된 기본값이 사용됩니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **6** 액세스 제어 정책에 대한 보안 인텔리전스 이벤트에 대한 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Security Intelligence(**보안 인텔리전스**)** 탭을 클릭합니다.

b) 다음 각 위치에서 **Logging(**로깅**)** 아이콘을 클릭하고 연결 및 시스템 로그 서버의 시작과 끝을 활성화합니다.

- **DNS Policy(DNS** 정책**)** 옆.
- **Block List(**차단 목록**)** 상자에서 **Networks(**네트워크**)** 및 **URL**에 대해.

c) **Save(**저장**)**를 클릭합니다.

단계 **7** 액세스 제어 정책에서 각 규칙에 대해 syslog 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Rules(**규칙**)** 탭을 클릭합니다.

b) 편집할 규칙을 클릭합니다.

c) 규칙에서 **Logging(**로깅**)** 탭을 클릭합니다.

d) 연결의 시작 및 끝을 모두 활성화합니다.

e) 파일 이벤트를 로깅할 경우 **Log Files(**로그 파일**)**를 선택합니다.

f) **Syslog Server(**시스템 로그 서버**)**를 활성화합니다.

g) 규칙이 "**Using default syslog configuration in Access Control Logging(**세스 제어 기록에서 기본 시스템 로그 컨피그레이션 사용**)**"인지 확인합니다.
h) **Save(**저장**)**를 클릭합니다.
i) 정책의 각 규칙에 대해 반복합니다.

다음에 수행할 작업

변경을 완료한 경우, 매니지드 디바이스에 변경 사항을 구축합니다.

직접 연결을 사용하여 **SAL(SaaS)**에 이벤트 전송

SAL(SaaS)에 이벤트를 직접 전송하도록 클라우드 사용 Firewall Management Center를 구성합니다.

시작하기 전에

- 클라우드 제공 Firewall Management Center에 디바이스를 온보딩하고, 이러한 디바이스에 라이선스를 할당하고, 이벤트를 SAL(SaaS)로 직접 전송하도록 이러한 디바이스를 구성합니다.
- 규칙을 수정하고 **Log at Beginning of Connection(**연결 시작 시 로깅**)** 및 **Log at End of Connection(**연결 종료 시 로깅**)** 옵션을 선택하여 규칙별로 연결 로깅을 활성화합니다.

프로시저

단계 **1** CDO에 로그인합니다.
단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 탐색합니다.
단계 **3** **Firewall Management Center**를 선택하고 오른쪽에 있는 Settings(설정) 창에서 **Cisco Cloud Events(Cisco** 클라우드 이벤트**)**를 선택합니다.
단계 **4** **Configure Cisco Cloud Events(Cisco** 클라우드 이벤트 구성**)** 위젯에서 다음을 수행합니다.

1. **Send Events to the Cisco Cloud(Cisco** 클라우드로 이벤트 전송**)** 슬라이더를 클릭하여 전체 구성을 활성화합니다.
2. 클라우드로 침입 이벤트를 전송하려면 **Send Intrusion Events to the cloud(**클라우드로 침입 이벤트 전송**)** 확인란을 선택합니다.
3. 파일 및 악성코드 이벤트를 클라우드로 전송하려면 **Send File and Malware Events to the cloud(**파일 및 악성코드 이벤트를 클라우드로 전송**)** 확인란을 선택합니다.
4. 연결 이벤트를 클라우드로 보내는 옵션을 선택합니다.
   - 연결 이벤트를 클라우드로 전송하지 않으려면 **None(**없음**)** 라디오 버튼을 클릭합니다.
   - 보안 인텔리전스 이벤트만 클라우드로 전송하려면 **Security Events(**보안 이벤트**)** 라디오 버튼을 클릭합니다.
   - 모든 연결 이벤트를 클라우드로 전송하려면 **All(**모두**)** 라디오 버튼을 클릭합니다.

5. **Save(**저장**)**를 클릭합니다.

CDO에서 이벤트 보기 및 작업

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 분석 > 이벤트 로깅를 선택합니다.

단계 **3** **Historical(**기록**)** 탭을 사용하여 모든 기록 이벤트 데이터를 볼 수 있습니다. 기본적으로 뷰어에는이 탭이 표시됩니다.

단계 **4** 라이브 이벤트를 보려면 **Live(**라이브**)** 탭을 클릭합니다.

이 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 CDO 온라인 도움말을 참조하십시오.

Cisco Secure Cloud Analytics에서 이벤트 보기 및 작업

시작하기 전에

이벤트의 원활한 흐름을 보장하려면 이벤트 뷰어를 사용하기 전에 Stealthwatch Cloud 포털에서 다음을 수행합니다.

- Secure Cloud Analytics가 올바른 CDO 테넌트와 통합되었는지 확인합니다.

  CDO 테넌트를 보려면 **Settings(**설정**)** > **Sensors(**센서**)**를 클릭합니다.

- 모니터링할 서브넷을 Secure Cloud Analytics에 추가합니다.

  서브넷을 추가하려면 **Settings(**설정**)** > **Subnets(**서브넷**)**를 클릭합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택합니다.

Secure Cloud Analytics 포털이 새 브라우저 탭에서 열립니다.

단계 **3** **Investigate(**조사**)** > **Event Viewer(**이벤트 뷰어**)**를 클릭합니다.

자세한 내용은 Secure Cloud Analytics 온라인 도움말을 참조하십시오.