Cisco Secure Firewall 통합 개요 가이드

최종 변경: 2024년 12월 16일

소개

이 가이드에서는 Secure Firewall Threat Defense (이전 명칭: Firepower Threat Defense) 디바이스를 이벤트 분석을 위해 다음과 같은 각 툴과 통합하기 위한 지침을 제공합니다.

- Cisco XDR
- Cisco Event Streamer
- Splunk
- IBM QRadar
- Cisco Security Analytics and Logging(온프레미스 및 SaaS)

이벤트 분석 툴 및 필요한 통합 유형에 따라 Secure Firewall Management Center (이전의 Firepower Management Center) 또는 Secure Firewall Device Manager (이전의 Firepower Device Manager)-매니지드 Threat Defense 디바이스를 사용하여 통합을 수행할 수 있습니다. 이 가이드에는 해당되는 경우 Management Center 또는 device manager에서 관리하는 Threat Defense 디바이스를 통합하는 지침이 포함되어 있습니다.

Note 2024년 7월 31일부터 Cisco SecureX는 단계적으로 중단되며 더 이상 사용할 수 없습니다. Cisco SecureX 액세스는 더 이상 Cisco Secure Firewall 제품 구매와 함께 제공되지 않습니다. 단종 날짜 이후에는 사용자에 대해 Cisco SecureX를 프로비저닝할 수 없습니다. 또한 모든 기존 Cisco SecureX 환경이 비활성화되고 모든 기능을 사용할 수 없게 됩니다. 자세한 내용은 Cisco SecureX의 단종 알림을 참조하십시오.

활용 사례

이 섹션에는 일반적인 사용 사례와 통합을 수행하는 데 사용되는 툴이 나와 있습니다.

활용 사례	해결책	지원되는 최소 **Threat Defense** 릴리스	추가 정보
여러 원격 분석 소스에서 가시성을 통합하고 탐지의 상호 연관성을 파악하고, 가장 큰 위험에 따라 위협의 우선순위를 정하고, 보안 분석가가 긴급한 주의가 필요한 사항에 대해 신속하고 효과적인 조치를 취할 수 있도록 하려는 것입니다.	Cisco XDR	6.4	Cisco XDR와 통합
관리 센터에서 호스트, 검색, 상관관계, 컴플라이언스 화이트리스트, 침입, 사용자 활동, 파일, 멀웨어 및 연결 데이터를 스트리밍하려고 합니다.	Cisco Event Streamer(eStreamer)	6.0	Cisco Event Streamer와의 통합
Splunk를 사용하여 Management Center로부터 받은 위협 및 트래픽 데이터를 저장하고 이 데이터를 사용하여 위협을 발견하고 조사하려고 합니다.	Splunk용 Cisco Secure Firewall(이전 Firepower) 앱	6.0	Splunk와의 통합
QRadar의 여러 보안 제품이 주는 인사이트를 제공하여 네트워크에 대한 위협을 분석하고 억제하고자 합니다.	IBM QRadar용 Cisco Firepower 앱	6.0	IBM QRadar와의 통합
온프레미스 방화벽 이벤트 데이터 스토리지 용량을 늘리고, 이 데이터를 더 오랫동안 보존하고, 이벤트 데이터를 Secure Network Analytics 어플라이언스로 내보내려고 합니다.	Cisco Security Analytics and Logging(온프레미스)	6.4	Cisco Security Analytics and Logging과의 통합(온프레미스), on page 8
온프레미스 스토리지가 제공할 수 있는 것보다 더 많은 스토리지가 필요하기 때문에 Cisco Secure Cloud Analytics(이전의 Stealthwatch Cloud)로 Firewall 이벤트를 전송하여 저장하고, 선택적으로 Cisco Secure Cloud Analytics를 사용하여 보안 분석에 Firewall 이벤트 데이터를 사용할 수 있게 하려고 합니다.	Cisco Security Analytics and Logging(SaaS)	6.4	Cisco Security Analytics and Logging과의 통합(SaaS), on page 10

Cisco XDR와 통합

Cisco Extended Detection and Response(Cisco XDR)는 여러 텔레메트리 소스에서 탐지된 위협을 상호 연결하여 가시성을 통합하는 클라우드 기반 솔루션 으로, 보안 팀이 가장 정교한 위협을 탐지하고 우선 순위를 정하고 이에 대응합니다. 이 솔루션은 위험을 기반으로 인시던트의 우선 순위를 지정하여 위협 탐지 및 대응 기능을 향상하며, 보안 분석가가 시급한 주의가 필요한 사항에 대해 신속하고 효과적인 조치를 취할 수 있도록 합니다.

이 통합은 지원되는 이벤트를 Threat Defense 디바이스에서 분석을 위해 Cisco XDR로 전송합니다.

참고 Cisco XDR는 별도 라이선스 제품입니다. Cisco Secure Firewall 제품에 필요한 라이선스 외에 추가 구독이 필요합니다. 자세한 정보는 Cisco XDR 라이선스를 참고하십시오.

통합 유형

두 가지 통합 방법을 사용하여 Threat Defense 디바이스를 Cisco XDR와 통합할 수 있습니다.

- 직접 통합: Management Center에서 지원됨
- 시스템 로그 통합: Management Center 및 device manager에서 지원됨

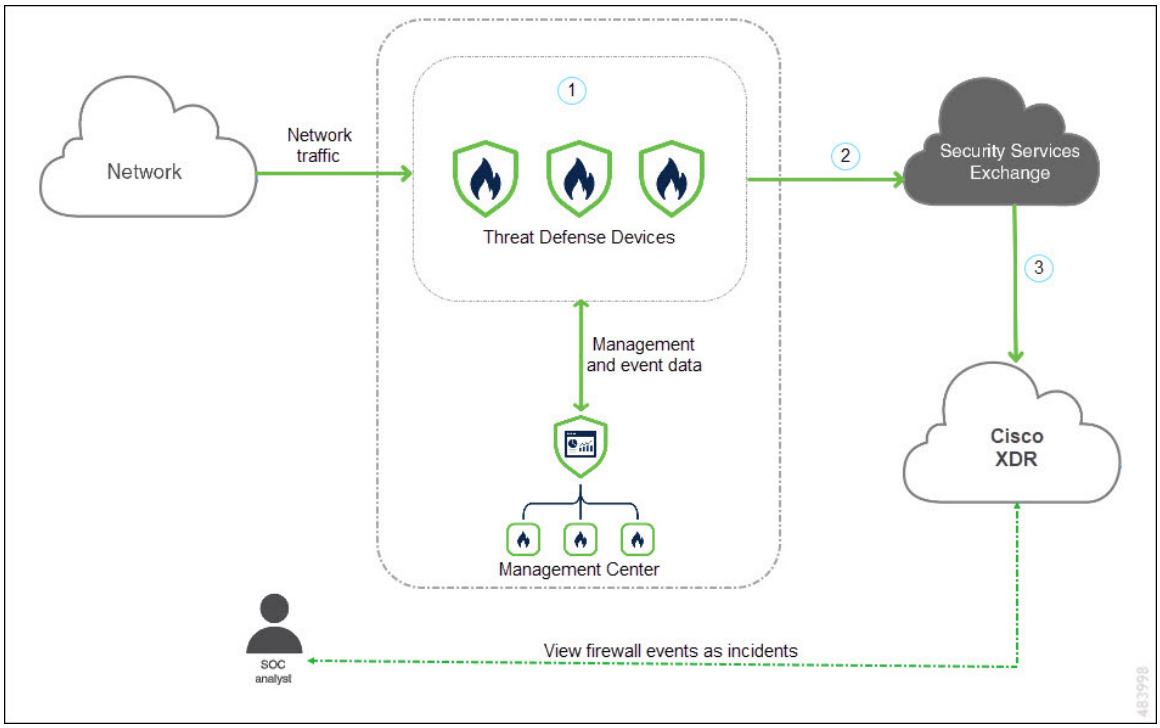
직접 통합

지원되는 이벤트를 Cisco Security Cloud의 보안 서비스 익스체인지로 직접 전송하도록 매니지드 Threat Defense 디바이스를 구성할 수 있습니다.

- 통합을 수행하는 데 지원되는 Secure Firewall 사용자 역할: 관리자.
- 지원되는 최소 Threat Defense 버전: 북미 클라우드의 경우 6.4, 유럽, APJC, 인도 및 호주 클라우드의 경우 6.5.
- 지원되는 최소 Management Center 버전: 7.0.2~7.0.x 및 7.2.0 이상.

참고 이미 SecureX 구독을 사용하여 Cisco Security Cloud로 이벤트를 전송하고 있었다면 계속해서 Cisco XDR로 이벤트를 전송할 수 있습니다. 하지만 이제 CDO 계정을 사용하여 클라우드 테넌시에 Management Center를 등록하는 경우 CDO 계정에 Cisco XDR로 이벤트를 전달할 수 있는 Security Analytics and Logging 라이선스가 있어야 합니다.

다음 다이어그램은 직접 통합의 작동 방식을 보여줍니다.



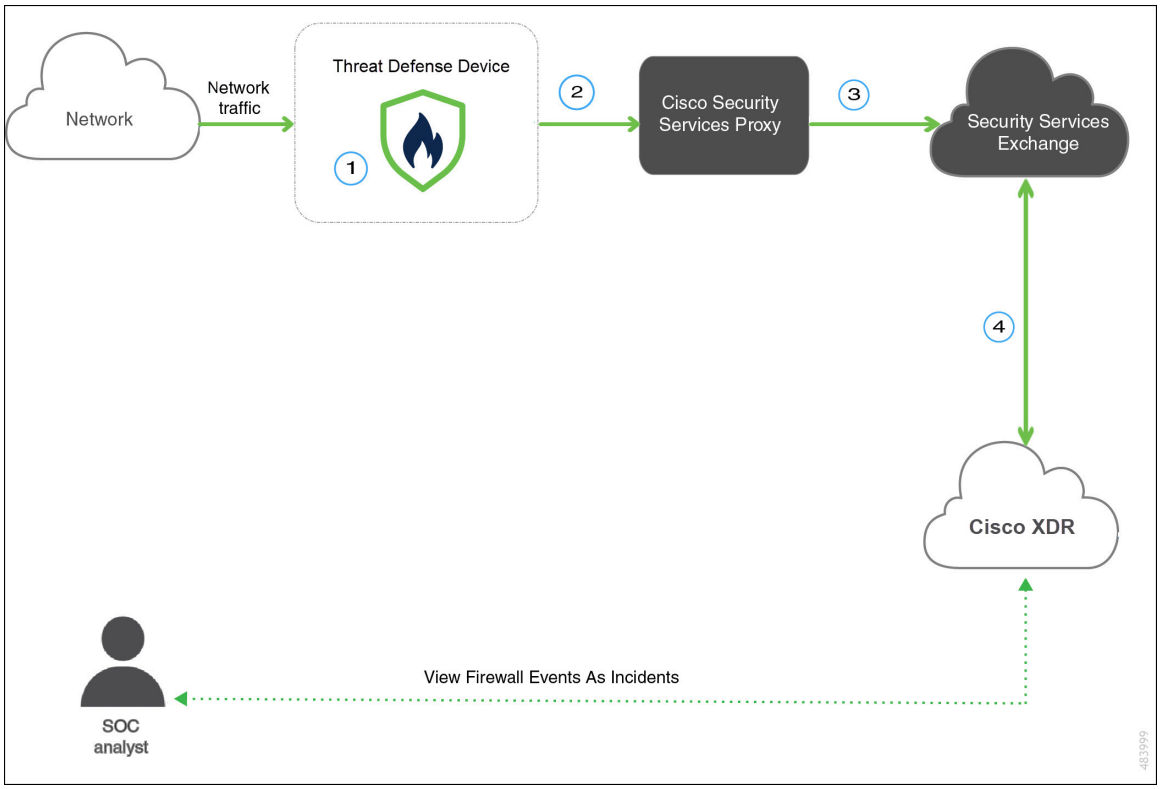
1	Threat Defense 디바이스는 이벤트를 생성합니다.
2	Threat Defense 디바이스는 지원되는 이벤트를 보안 서비스 익스체인지에 전송합니다.
3	Cisco XDR는 보안 서비스 익스체인지에 조사 중인 IP 주소와 관련된 발견을 쿼리하고 보안 분석가에게 추가 정보를 제공합니다. 이벤트는 Cisco XDR에 나타나는 인시던트로 자동 또는 수동 승격됩니다.

시스템 로그 통합

시스템 로그를 사용하여 Firewall 디바이스에서 지원되는 이벤트를 Cisco Cloud로 전송합니다.

- 통합을 수행하는 데 지원되는 Secure Firewall 사용자 역할: 관리자.
- 지원되는 최소 Secure Firewall 릴리스: 모든 클라우드 지역의 경우 6.3.

다음 다이어그램은 시스템 로그 통합이 작동하는 방식을 보여줍니다.



1	Threat Defense 디바이스가 이벤트를 생성합니다.
2	Threat Defense 디바이스는 지원되는 시스템 로그 이벤트를 CSSP(Cisco Security Services Proxy) 서버 로 전송합니다.
3	10분마다 CSSP는 수집된 이벤트를 보안 서비스 익스체인지로 전달합니다.
4	Cisco XDR는 보안 서비스 익스체인지에 조사 중인 IP 주소와 관련된 발견을 쿼리하고 보안 분석가에게 추가 정보를 제공합니다. 이벤트는 Cisco XDR에 나타나는 인시던트로 자동 또는 수동 승격됩니다.

Cisco Event Streamer와의 통합

Cisco Event Streamer(eStreamer라고도 함)를 사용하면 Firewall 시스템 이벤트를 외부 클라이언트 애플리케이션으로 스트리밍할 수 있습니다.

간단하게 설명하자면 eStreamer 서비스는 Firewall에서 요청 클라이언트로 데이터를 스트리밍하기 위한 메커니즘입니다. 서비스는 다음 데이터 카테고리를 스트리밍할 수 있습니다.

- 침입 이벤트 데이터 및 이벤트 추가 데이터
- 상관관계(컴플라이언스) 이벤트 데이터

- 검색 이벤트 데이터
- 사용자 이벤트 데이터
- 이벤트의 메타데이터
- 호스트 정보
- 악성코드 이벤트 데이터

eStreamer는 NGIPSv, Firewall 서비스 Threat Defense Virtual및 Threat Defense에서 지원되지 않습니다. 이러한 디바이스에서 이벤트를 스트리밍하려는 경우 해당 디바이스가 보고하는 관리 센터에 eStreamer를 구성할 수 있습니다.

eStreamer 클라이언트를 생성하여 Firewall 시스템과 통합할 때는 다음의 세 가지 주요 단계를 수행합니다.

1. eStreamer 애플리케이션 프로토콜을 사용하여 Management Center 또는 매니지드 디바이스와 메시지를 교환하는 클라이언트 애플리케이션을 작성합니다. 참조 클라이언트 애플리케이션은 eStreamer SDK에 포함되어 있습니다.
2. 필요한 이벤트 유형을 클라이언트 애플리케이션으로 전송하도록 관리 센터 또는 디바이스를 구성합니다.
3. 클라이언트 애플리케이션을 Management Center 또는 디바이스에 연결하고 데이터 교환을 시작합니다.

통합을 수행하는 데 지원되는 **Firewall** 사용자 역할: 관리자

지원되는 최소 **Firepower** 릴리스: 6.0

Firewall과 Cisco Event Streamer의 통합에 대한 자세한 내용은 Secure Firewall Management Center Event Streamer 통합 가이드를 참조하십시오.

Splunk와의 통합

Splunk용 Cisco Secure Firewall(f.k.a. Firepower) 앱은 버전 6.0 이상을 실행하는 Management Center에서 Splunk로 전송된 보안 및 네트워크 이벤트 정보를 제공합니다. Management Center의 위협 및 트래픽 데이터를 사용하여 위협을 발견하고 조사할 수 있습니다. Splunk는Management Center보다 훨씬 더 많은 데이터를 저장할 수 있으므로 네트워크의 활동에 대한 가시성을 높일 수 있습니다.

이 앱은 Splunk용 Cisco Firepower eNcore 앱(https://splunkbase.splunk.com/app/3663/)의 후속 앱입니다. 원한다면 두 앱을 동시에 실행할 수 있습니다.

통합을 수행하는 데 지원되는 **Firewall** 사용자 역할: 관리자

지원되는 최소 **Firepower** 릴리스: 6.0

지원되는 Splunk 버전 및 기타 호환성 정보는 다음과 같습니다. https://splunkbase.splunk.com/app/4388/
.

이 앱을 사용하려면 Firewall 이벤트 데이터가 Splunk에 있어야 합니다. Firewall 데이터를 Splunk로 가져오려면 Splunk용 Cisco Secure eStreamer 클라이언트 애드온(이전의 Splunk용 Cisco eStreamer eNcore 애드온)을 사용하십시오. 이 TA(Technical Add-On)는 https://splunkbase.splunk.com/app/3662/에서 사용할 수 있습니다.

이 TA에 대한 설명서는 https://www.cisco.com/c/en/us/support/security/defense-center/products-programming-reference-guides-list.html에서 제공됩니다.

Splunk용 Cisco Secure Firewall(f.k.a. Firepower) 앱에 대한 자세한 내용은 Splunk용 Cisco Secure Firewall(f.k.a. Firepower) 앱 사용자 가이드를 참조하십시오.

IBM QRadar와의 통합

Cisco Firepower App for IBM QRadar를 사용하면 QRadar의 여러 보안 제품이 주는 인사이트를 제공하여 네트워크에 대한 위협을 분석하고 억제할 수 있습니다.

QRadar SIEM(보안 정보 및 이벤트 관리) 툴은 변칙 탐지, 인시던트 포렌식 및 취약성 관리를 제공합니다.

앱을 설정한 후 QRadar 콘솔에서 Firewall 시스템의 이벤트 데이터를 그래픽 형식으로 볼 수 있습니다.

통합을 수행하는 데 지원되는 **Firewall** 사용자 역할: 관리자

지원되는 최소 **Firepower** 릴리스: 6.0

IBM QRadar용 Cisco Firepower 앱에 대한 자세한 내용은 IBM QRadar용 Cisco Firepower 앱 통합 가이드를 참조하십시오.

Cisco Security Analytics and Logging과의 통합

Cisco Security Analytics and Logging(CSAL)은 다양한 Cisco 디바이스의 로그를 집계하고 네트워크 활동에 대한 직관적인 보기를 제공함으로써 의사 결정을 간소화합니다. Security Analytics and Logging은 사용자의 재량에 따라 확장할 수 있으므로 방화벽 및 기타 네트워킹 디바이스에서 발견된 잠재적 위협에 대해 더 오래 보존 및 분석하고 경고할 수도 있습니다.

Firewall는 온프레미스 및 SaaS(Security as a Service)의 두 가지 방법을 사용하여 CSAL과 통합할 수 있습니다.

Cisco Security Analytics and Logging 원격 이벤트 스토리지의 옵션 비교

온프레미스	**SaaS**
방화벽 뒤에서 스토리지 시스템을 구매, 라이선싱, 설정합니다.	라이선스 및 데이터 스토리지 요금제를 구매하고 Cisco 클라우드로 데이터를 전송합니다.

온프레미스	SaaS
지원되는 이벤트 유형: • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드 • LINA	지원되는 이벤트 유형: • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드
시스템 로그 및 직접 통합을 모두 지원합니다.	시스템 로그 및 직접 통합을 모두 지원합니다.
• Secure Network Analytics Manager에서 모든 이벤트 확인합니다. • Management Center 이벤트 뷰어에서 교차 실행하여 Secure Network Analytics Manager의 이벤트를 확인합니다. • Management Center에서 원격으로 저장된 연결 및 보안 인텔리전스 이벤트 보기	라이선스에 따라 CDO 또는 Secure Network Analytics의 이벤트를 확인합니다. Management Center 이벤트 뷰어에서 교차 실행합니다.

자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드 또는 온라인 도움말의 데이터 스토리지 장에 있는 링크를 참조하십시오.

Cisco Security Analytics and Logging과의 통합(온프레미스)

Cisco Security Analytics and Logging(온프레미스)을 사용하여 방화벽 이벤트 데이터를 저장하여 보존 기간을 늘리고 저장 공간을 늘릴 수 있습니다.. Cisco Secure Network Analytics(이전 Stealthwatch) 어플라이언스를 구축하고 방화벽 구축과 통합하면 Secure Network Analytics 어플라이언스로 이벤트 데이터를 내보낼 수 있습니다.

통합을 수행하는 데 지원되는 **Firewall** 사용자 역할: 관리자, 분석가, 보안 분석가

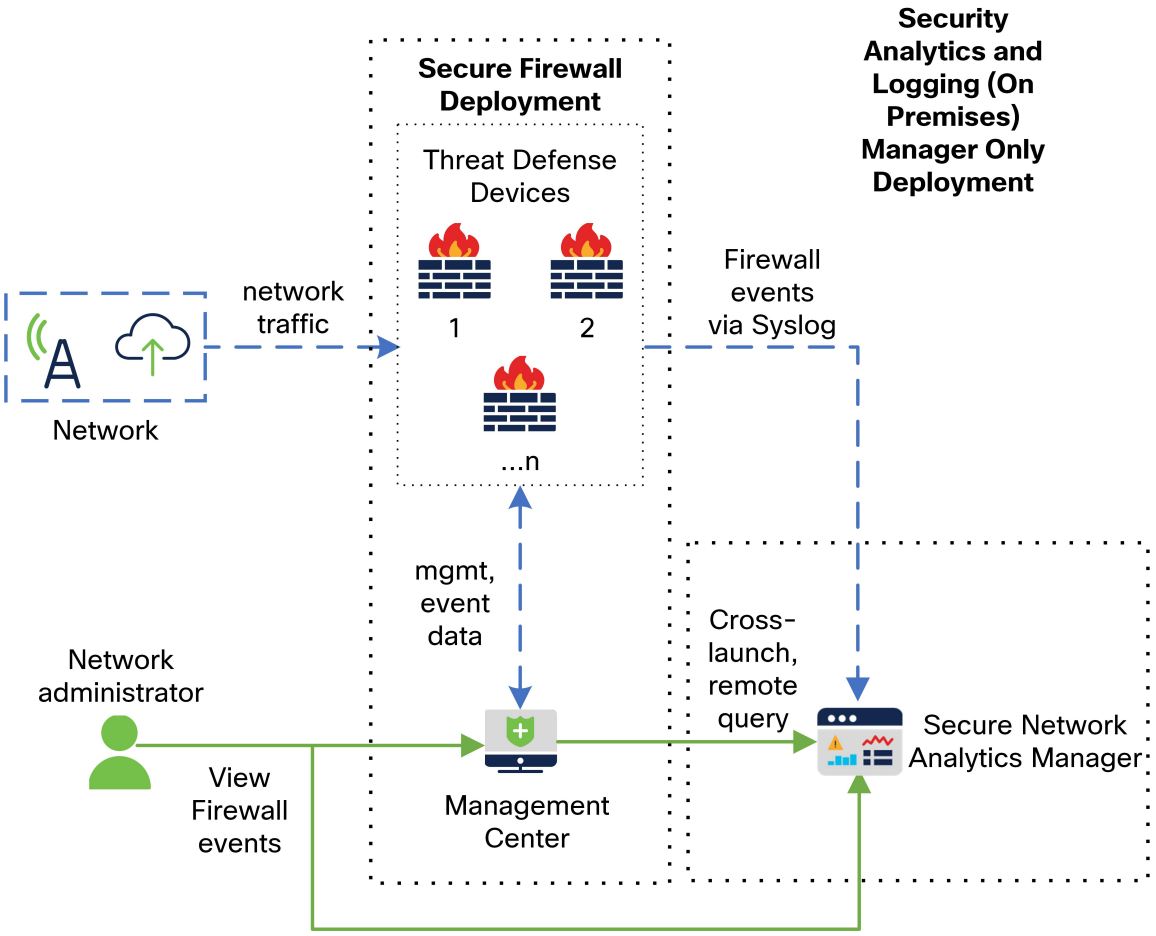
지원되는 최소 **Secure Firewall** 릴리스: 6.4

구축 유형

관리자 전용 구축

이벤트를 수신 및 저장하고 이벤트를 검토하고 쿼리할 수 있는 독립형 관리자를 구축합니다.

다음 다이어그램에서 관리자가 있는 관리자 전용 구축의 예를 참조하십시오.



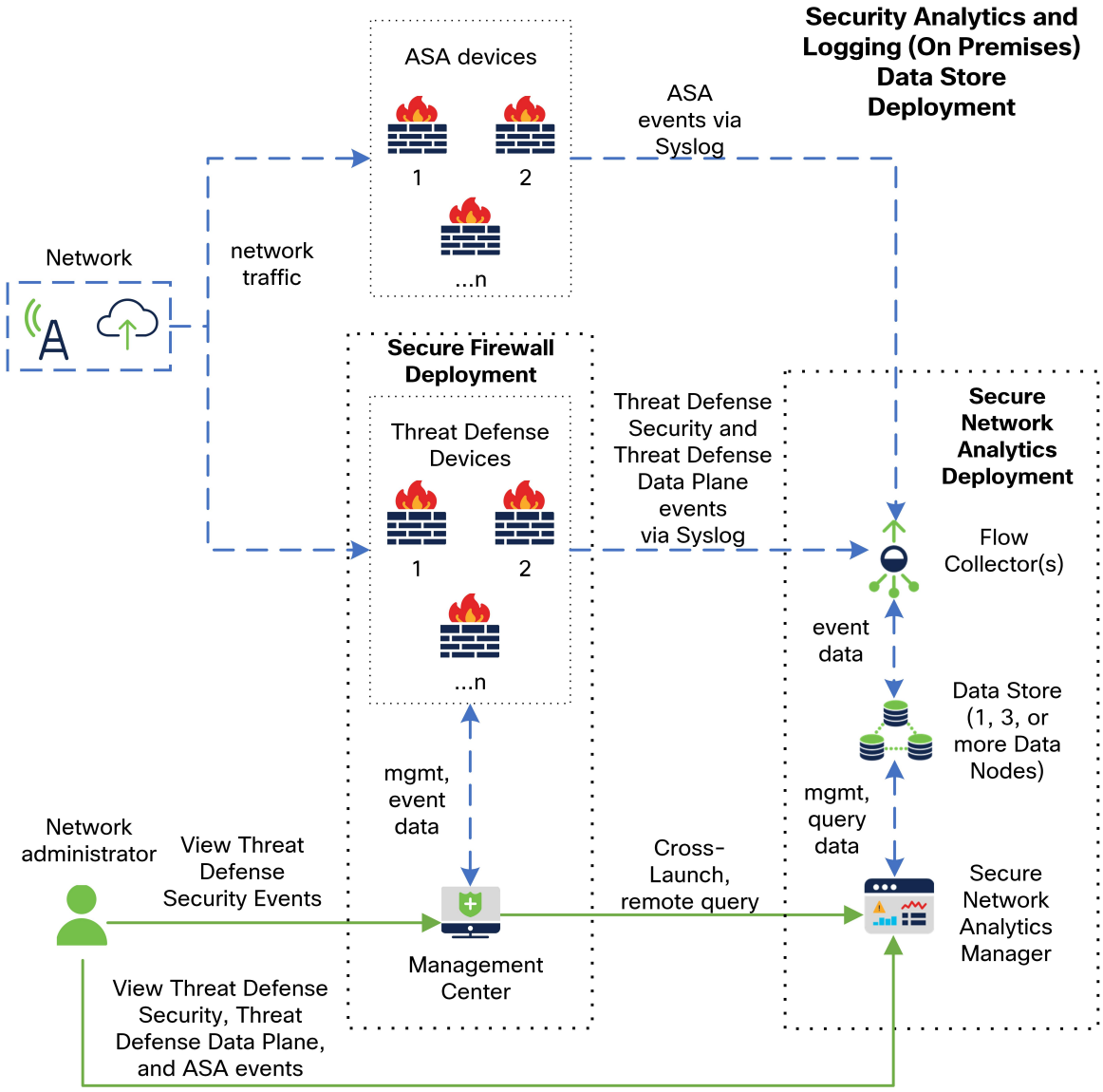
이 구축에서 Threat Defense 디바이스는 방화벽 이벤트를 관리자에게 전송하고, 관리자는 이러한 이벤트를 저장합니다. 사용자는 Management Center UI에서 관리자에 교차 실행하여 저장된 이벤트에 대한 세부 정보를 볼 수 있습니다. 추가로 Management Center에서 이벤트의 원격 쿼리를 수행할 수 있습니다.

Note 관리자 전용 구축은 Secure Network Analytics 어플라이언스 버전 7.5.1 이상에서 지원되지 않습니다. 자세한 내용은 Cisco Security Analytics and Logging 설명서를 참조하십시오.

데이터 저장소 구축

이벤트를 수신할 Cisco Secure Network Analytics 플로우 컬렉터, 이벤트를 저장할 Cisco Secure Network Analytics 데이터 저장소(3개의 Cisco Secure Network Analytics 데이터 노드 포함), 이벤트를 검토하고 쿼리할 수 있는 관리자를 구축합니다.

다음 다이어그램에서 관리자, 데이터 노드 3개, 플로우 컬렉터가 있는 데이터 저장소 구축의 예를 참조하십시오.



이 구축에서 Threat Defense 및 ASA 디바이스는 방화벽 이벤트를 플로우 컬렉터로 전송합니다. 플로우 컬렉터는 데이터 저장소(데이터 노드 3개)로 이벤트를 전송하여 저장합니다. 사용자는 Management Center UI에서 관리자에 교차 실행하여 저장된 이벤트에 대한 세부 정보를 볼 수 있습니다. 추가로 Management Center에서 이벤트의 원격 쿼리를 수행할 수 있습니다.

방화벽을 SAL(온프레미스)과 통합하는 방법에 대한 자세한 내용은 Cisco Security Analytics and Logging (온프레미스): 방화벽 이벤트 통합 가이드를 참조하십시오.

Cisco Security Analytics and Logging과의 통합(SaaS)

Firewall 이벤트를 저장하는 데 추가 공간이 필요한 경우 Cisco Security Analytics and Logging(SaaS)을 사용하여 저장용으로 Firewall 이벤트를 Cisco Secure Cloud Analytics(이전의 Stealthwatch Cloud)에 전

송하고, 필요한 경우 Firewall 이벤트 데이터로 만들기 위해 선택적으로 Cisco Secure Cloud Analytics를 사용한 보안 애널리틱스에 사용할 수 있습니다.

이 통합은 Management Center에서 관리하는 Threat Defense 디바이스와 관련이 있습니다. 이 통합은 Firewall 소프트웨어를 실행하지 않는 디바이스, device manager에서 관리하는 디바이스 또는 Management Center에서 관리하는 Threat Defense가 아닌 디바이스에서는 지원되지 않습니다.

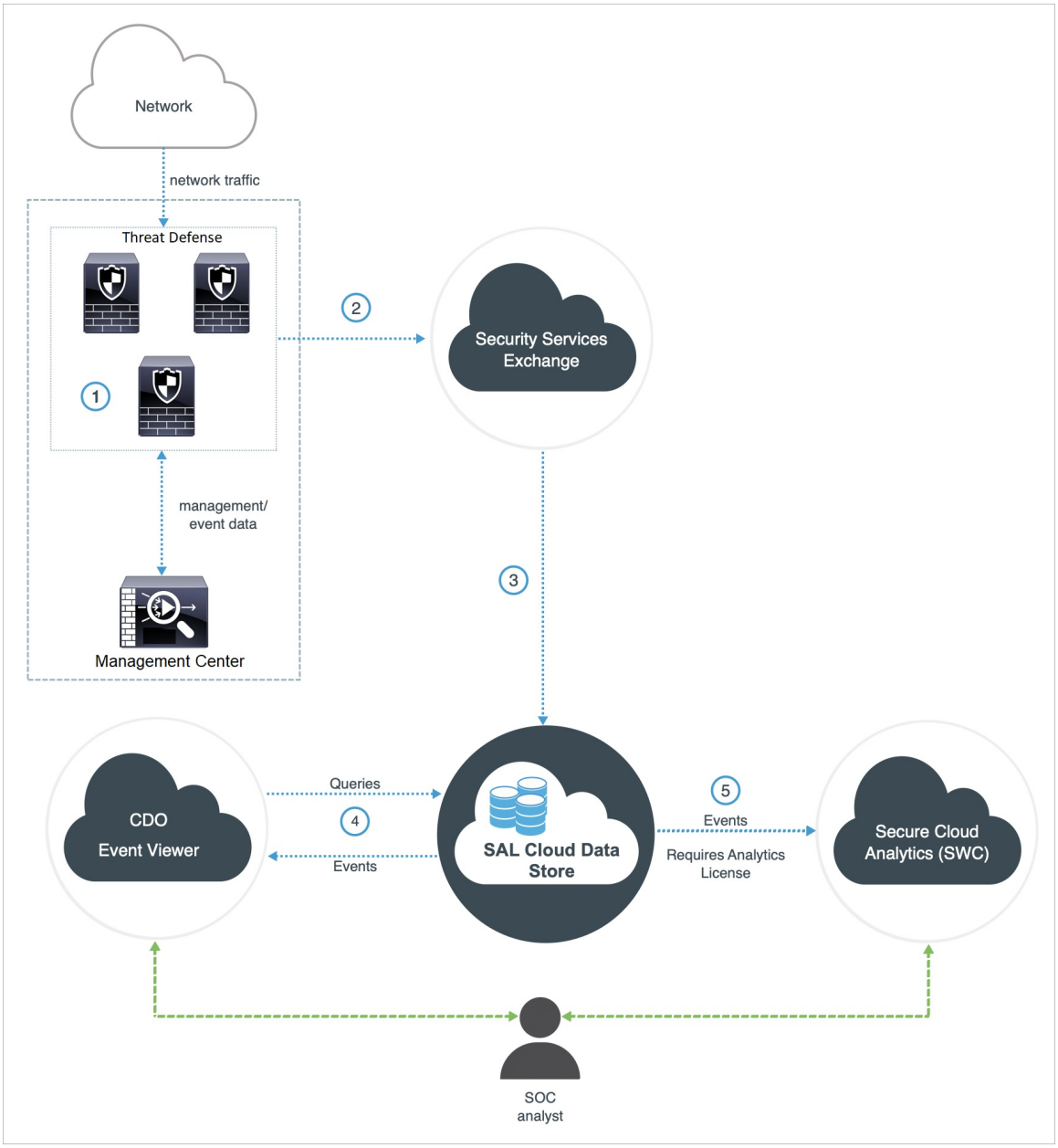
통합 유형

직접 통합

통합을 수행하는 데 지원되는 **Firewall** 사용자 역할: 관리자, 액세스 관리자, 네트워크 관리자, 보안 승인자

지원되는 최소 **Firepower** 릴리스: 6.4

다음 다이어그램은 직접 통합의 작동 방식을 보여줍니다.



1	Threat Defense 디바이스는 이벤트를 생성합니다.
2	Threat Defense 디바이스는 지원되는 이벤트를 보안 서비스 익스체인지로 전달하며, 이는 Cisco 클라우드 보안 제품에서 사용할 클라우드-클라우드 및 프레미스-클라우드 식별, 인증 및 데이터 스토리지를 처리하는 안전한 중개 클라우드 서비스입니다.

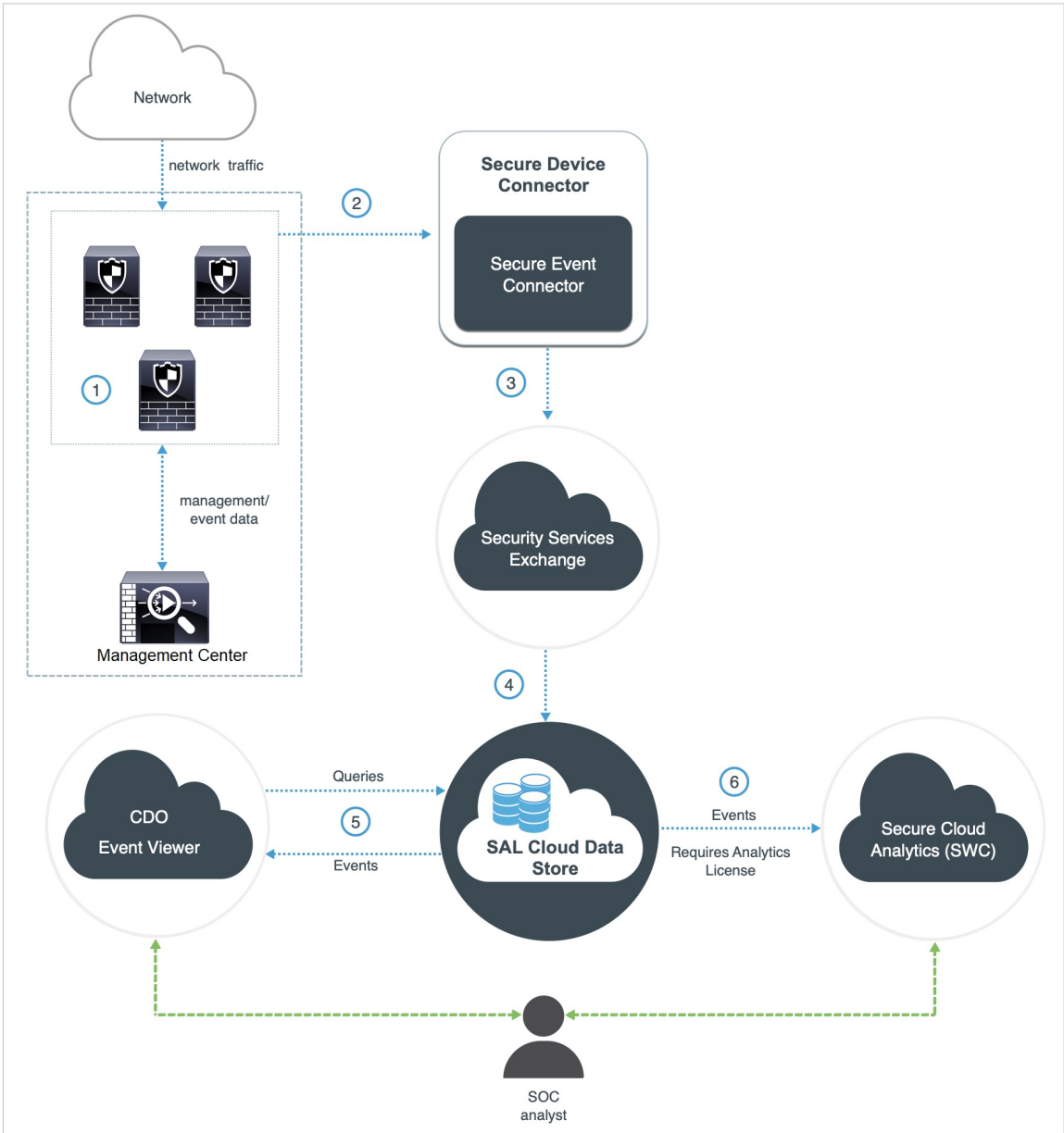
3	보안 서비스 익스체인지는 이벤트를 Cisco Security Analytics and Logging(SAL) 클라우드 데이터 저장소로 전달합니다.
4	CDO 이벤트 뷰어는 SAL 클라우드 데이터 저장소에서 이벤트를 쿼리하고 SOC 분석가에게 추가 컨텍스트를 제공합니다.
5	(분석 라이선스가 있는 경우에만 해당) Cisco Secure Cloud Analytics(이전 명칭 SWC)는 SAL 클라우드 데이터 저장소에서 이벤트를 수신하고, SOC 분석가가 제품의 애널리틱스 기능에 액세스할 수 있도록 합니다.

시스템 로그 통합

통합을 수행하는 데 지원되는 **Firewall** 사용자 역할: 관리자, 액세스 관리자, 네트워크 관리자, 보안 승인자

지원되는 최소 **Firepower** 릴리스: 7.0

다음 다이어그램은 시스템 로그 통합의 작동 방식을 보여줍니다.



1	Threat Defense 디바이스는 이벤트를 생성합니다.
2	Threat Defense 디바이스는 지원되는 이벤트를 네트워크 의 가상 머신에 설치된 SEC(Secure Event Connector)에 시스템 로그 메시지로 전송합니다.

3	SEC는 이벤트를 보안 서비스 익스체인지로 전달하며, 이는 Cisco 클라우드 보안 제품에서 사용할 클라우드-클라우드 및 프레미스-클라우드 식별, 인증 및 데이터 스토리지를 처리하는 안전한 중개 클라우드 서비스입니다.
4	보안 서비스 익스체인지는 이벤트를 Cisco Security Analytics and Logging(SAL) 클라우드 데이터 저장소로 전달합니다.
5	CDO 이벤트 뷰어는 SAL 클라우드 데이터 저장소에서 이벤트를 쿼리하고 SOC 분석가에게 추가 컨텍스트를 제공합니다.
6	(분석 라이선스가 있는 경우에만 해당) Cisco Secure Cloud Analytics(이전 명칭 SWC)는 SAL 클라우드 데이터 저장소에서 이벤트를 수신하고, SOC 분석가가 제품의 애널리틱스 기능에 액세스할 수 있도록 합니다.

Firewall을 CSAL(SaaS)과 통합하는 방법에 대한 자세한 내용은 Cisco Secure Firewall Management Center 및 Cisco Security Analytics and Logging(SaaS) 통합 가이드를 참조하십시오.