EVE 위협 신뢰도 점수를 기반으로 트래픽 차단

암호화된 가시성 엔진 정보

TLS(전송 계층 보안) 암호화를 사용하는 클라이언트 애플리케이션 및 프로세스를 식별하는 데 EVE(암호화된 가시성 엔진)를 사용할 수 있습니다. EVE는 암호 해독 없이 암호화된 세션에 대한 가시성을 향상합니다. EVE의 결과에 따라 관리자는 환경 내 트래픽에 대해 정책 작업을 시행할 수 있습니다. EVE를 사용하여 악성코드를 식별하고 중지할 수도 있습니다.

이점

관리자는 EVE의 위협 점수를 활용하고 조정하여 악성 암호화 트래픽을 차단할 수 있습니다. 수신 트래픽이 악성일 가능성이 있는 경우 위협 점수를 기반으로 연결을 차단하도록 EVE를 구성할 수 있습니다.

샘플 비즈니스 시나리오

대규모 기업 네트워크에서는 Snort 3를 기본 침입 탐지 및 방지 시스템으로 사용합니다. 빠르게 진화하는 위협 환경에서 강력한 네트워크 보안 조치의 채택은 꼭 필요하며 중요합니다. 보안 팀은 완전한 MITM(Man-In-the-Middle) 암호 해독을 구현할 필요 없이 EVE를 사용하여 암호화된 트래픽 검사를 강화합니다. EVE 기술은 알려진 악성 프로세스의 핑거프린트를 사용하여 악성코드를 식별하고 중지

합니다. 네트워크 관리자는 설정된 차단 임계값을 기반으로 잠재적으로 악의적인 연결을 차단하도록 EVE의 차단 트래픽 임계값을 구성할 수 있는 유연성이 있어야 합니다.

사전 요구 사항

- Management Center 7.4.0 이상을 실행해야 하며, 매니지드 Threat Defense도 7.4.0 이상이어야 합니다.
- 유효한 IPS(침입 방지 시스템) 라이선스가 있고 Snort 3가 탐지 엔진인지 확인합니다.

고수준 워크플로우

1. EVE는 수신 트래픽을 분석하고 수신 트래픽이 악성코드일 가능성에 대한 판정을 제공합니다.
2. EVE가 특정 신뢰도 레벨의 수신 트래픽을 악성코드로 탐지하면 해당 트래픽을 차단하도록 EVE를 구성할 수 있습니다.
3. 먼저 패킷에서 악성코드 가능성 또는 위협 점수를 확인하며, 위협 점수는 사용자가 설정한 차단 임계값과 비교됩니다.
4. 위협 점수가 구성된 임계값보다 높으면 EVE는 트래픽을 차단합니다.
5. 위협 점수가 구성된 임계값보다 작으면 EVE는 아무런 작업을 수행하지 않습니다.

EVE에서 차단 임계값 구성

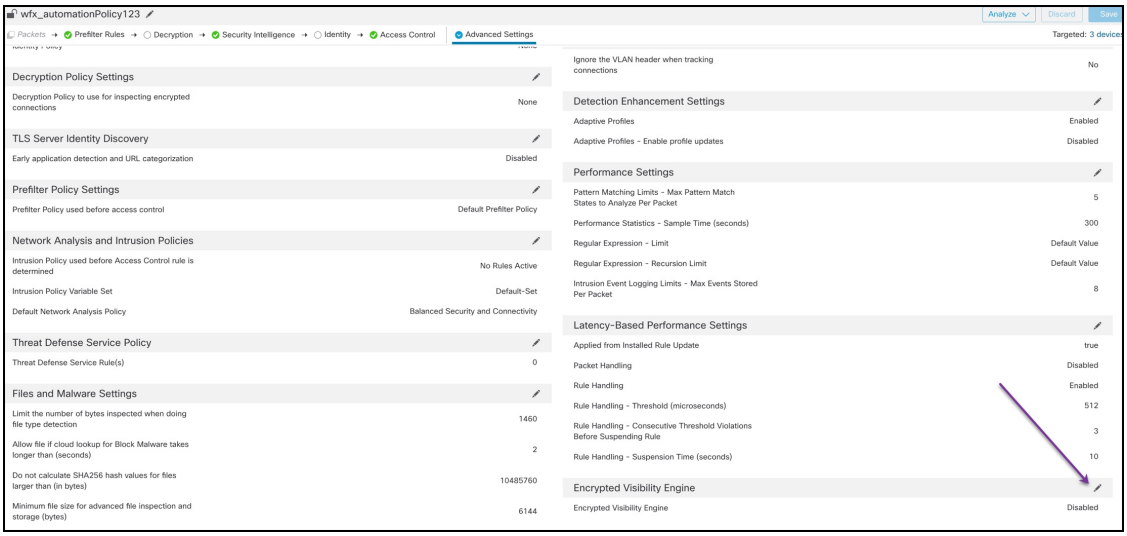
이 절차에서는 EVE 위협 신뢰도 점수 90% 이상을 기준으로 잠재적으로 악의적인 트래픽을 차단하는 방법을 보여줍니다.

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 2 편집하려는 액세스 제어 정책 옆에 있는 **Edit(**편집**)**(✎)을 클릭합니다.

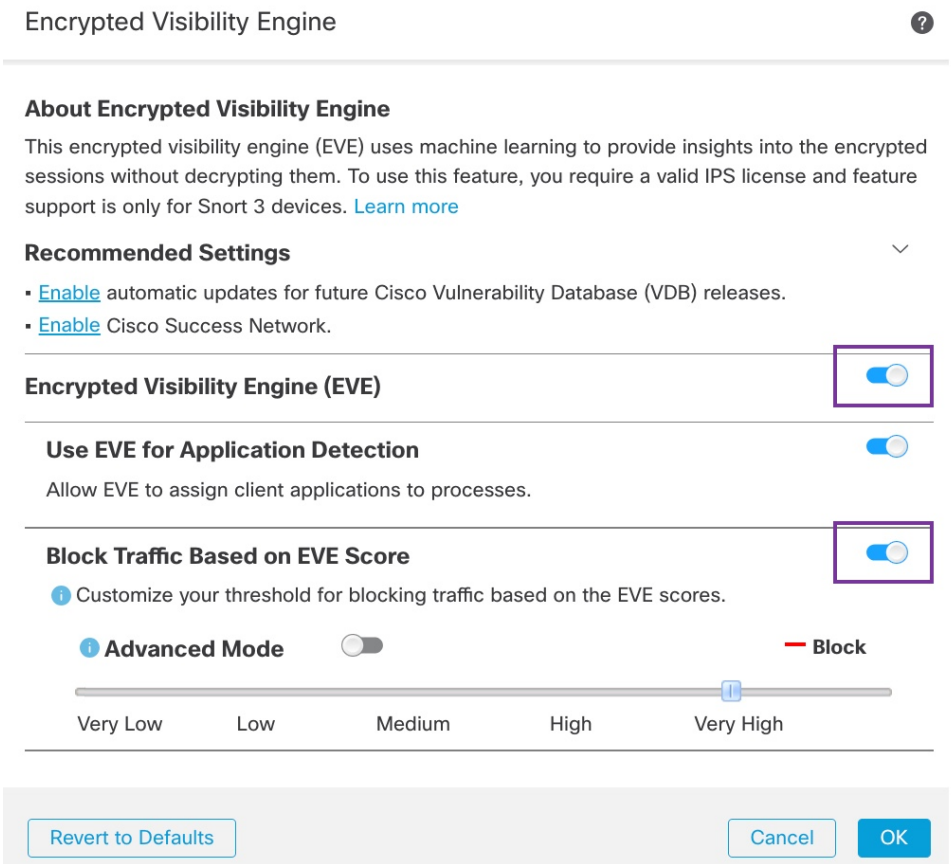
단계 3 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 4 **Encrypted Visibility Engine(**암호화된 가시성 엔진**)** 옆에 있는 **Edit(**편집**)**(✎)을 클릭합니다.



단계 **5** **Encrypted Visibility Engine(**암호화된 가시성 엔진**)** 페이지에서 **EVE(**암호화된 가시성 엔진**)** 토글 버튼을 활성화합니다.

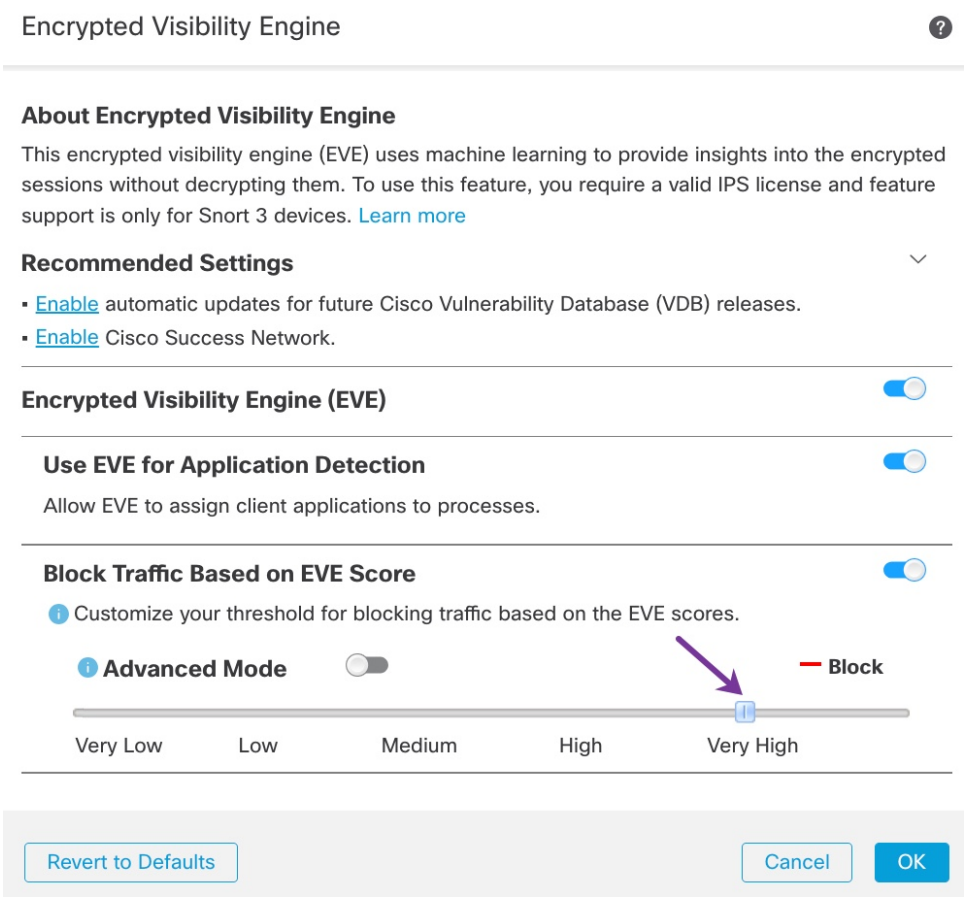
단계 **6** **Block Traffic Based on EVE Score(EVE** 점수 기반 트래픽 차단**)** 토글 버튼을 활성화합니다. 잠재적인 위협인 모든 수신 트래픽은 기본적으로 차단됩니다.



참고 기본적으로 악성코드가 차단되는 임계값은 99%이며, 이는 다음을 의미합니다.

- EVE가 99% 이상의 신뢰도로 트래픽이 악성코드임을 탐지하면 EVE는 트래픽을 차단합니다.
- EVE가 트래픽을 99% 미만의 신뢰도로 악성코드로 탐지하는 경우, EVE는 작업을 수행하지 않습니다.

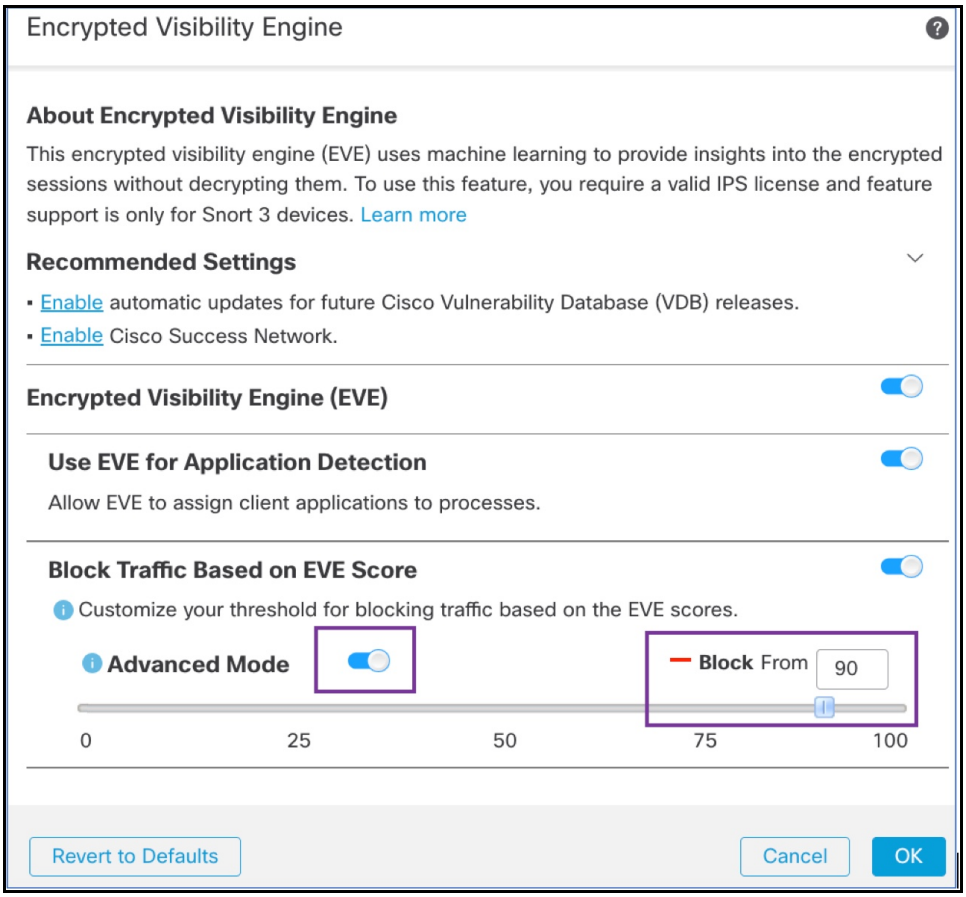
단계 **7** 슬라이더를 사용하여 EVE 위협 신뢰도를 기반으로 차단 임계값을 조정합니다. 범위는 **Very Low(**매우 낮음**)**에서 **Very High(**매우 높음**)**까지입니다. 이 예에서는 슬라이더가 **Very High(**매우 높음**)**로 설정되어 있습니다.



단계 **8** 더 세부적인 제어를 위해 **Advanced Mode(**고급 모드**)** 토글 버튼을 활성화합니다. 이제 트래픽 차단에 대한 특정 EVE 위협 신뢰도 점수를 할당할 수 있습니다. 기본 임계값은 99%입니다.

단계 **9** 이 예에서는 차단 임계값을 **90%**로 변경합니다.

주의 최적의 성능을 보장하기 위해 차단 임계값을 50% 미만으로 설정하지 않는 것이 좋습니다.



단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

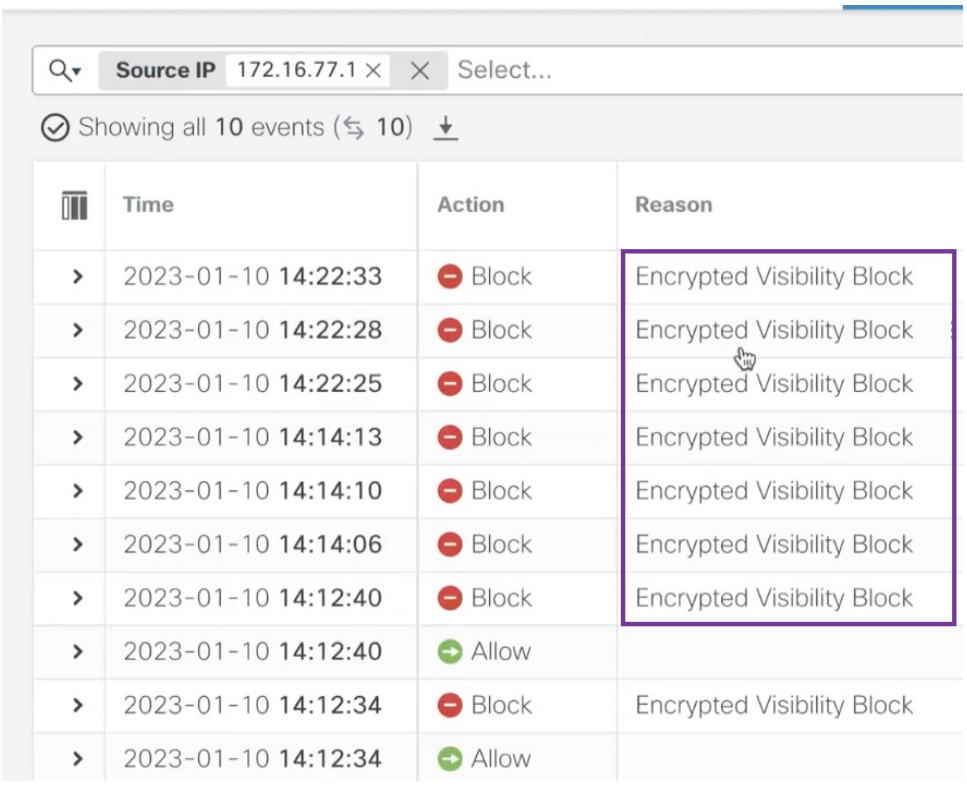
다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

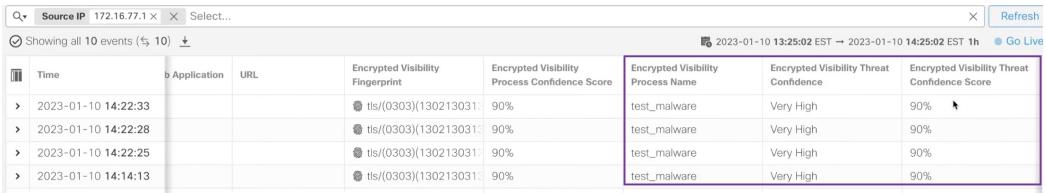
EVE 이벤트 보기

단계 **1** 차단 작업을 확인하려면 **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 선택합니다. **Unified Events(**통합 이벤트**)** 뷰어에서 이벤트를 볼 수도 있습니다.

단계 **2** 트래픽을 차단하도록 EVE를 구성한 경우 **Reason(**사유**)** 필드에 **Encrypted Visibility Block(**암호화된 가시성 차단**)**이 표시됩니다.



단계 **3** 다음은 **Encrypted Visibility Process Name(**암호화된 가시성 프로세스 이름**)**을 **test_malware**로, **Encrypted Visibility Threat Confidence(**암호화된 가시성 위협 신뢰도**)**를 **Very High(**매우 높음**)**로, **Encrypted Visibility Threat Confidence Score(**암호화된 가시성 위협 신뢰도 점수**)**를 **90%**로 설정한 예입니다.



추가 참조 자료

자세한 개념 정보는 이 가이드에 나와 있는 Snort 3의 암호화된 가시성 엔진 장이나 다음 링크의 콘텐츠를 참조하십시오.

암호화된 가시성 엔진