침입 이벤트 로깅 글로벌 제한

다음 주제에서는 침입 이벤트 로깅을 전역 제한하는 방법을 설명합니다.

전역 규칙 임계값 기본 사항

전역 규칙 임계값은 침입 정책에 의한 이벤트 로깅에 대해 제한을 설정합니다. 모든 트래픽에 해당되는 글로벌 규칙 임계값을 설정하여 정책이 지정된 기간당 특정 소스 또는 대상의 이벤트를 로깅하고 표시하는 빈도를 제한할 수 있습니다. 또한, 정책에서 공유 객체 규칙, 표준 텍스트 규칙 또는 전처리기 규칙당 임계값도 설정할 수 있습니다. 글로벌 임계값을 설정하면 해당 임계값은 정책 내에서 특정 임계값을 재정의하지 않는 각 규칙에 적용됩니다. 임계값을 사용하면 이벤트 수가 너무 많아서 혼란스러워지는 상황을 피할 수 있습니다.

각 침입 정책은 모든 침입 규칙 및 전처리기 규칙에 기본적으로 적용되는 기본 글로벌 규칙 임계값을 포함합니다. 이 기본 임계값은 대상에 방문하는 트래픽의 이벤트 수를 60초당 하나로 제한합니다.

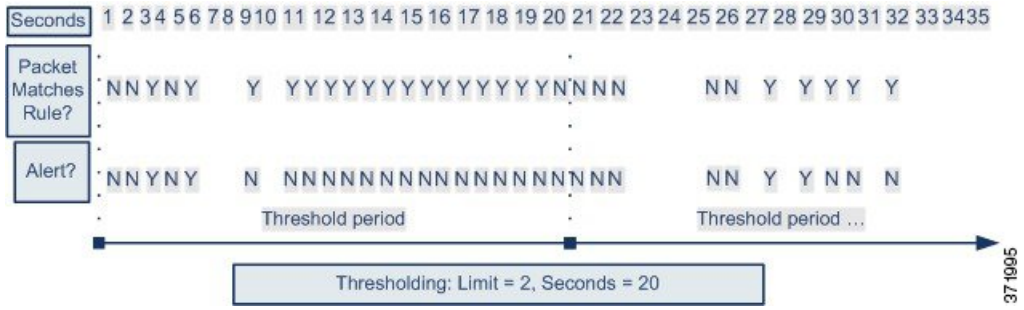
다음 작업을 수행할 수 있습니다.

- 전역 임계값을 변경합니다.
- 전역 임계값을 비활성화합니다.
- 특정 규칙의 개별 임계값을 설정하여 전역 임계값을 재정의합니다.

  예를 들어 전역 제한 임계값은 60초당 이벤트 5회이지만, SID 1315에 대해서는 60초당 이벤트 10회의 특정 임계값을 설정할 수 있습니다. 다른 모든 규칙은 60초당 생성되는 이벤트가 5회를 넘지 않지만 SID 1315의 경우, 시스템은 60초당 이벤트를 최대 10회 생성합니다.

팁 다중 CPU를 가진 매니지드 디바이스에서 전역 또는 개별 임계값은 예상보다 많은 수의 이벤트를 야기할 수 있습니다.

다음 다이어그램은 전역 규칙 임계값 설정의 작동 방식을 보여줍니다. 이 예에서는 공격이 특정 규칙에 대해 진행 중입니다. 전역 제한 임계값은 각 규칙의 이벤트 생성을 20초당 2회로 제한하도록 설정되어 있습니다. 기간은 1초에 시작하여 21초에 끝납니다. 기간이 끝나면 주기가 다시 시작되고 다음 두 규칙 일치가 이벤트를 생성하며, 시스템은 해당 기간 중에 더 이상 이벤트를 생성하지 않습니다.



전역 규칙 임계값 옵션

기본 임계값은 각 규칙에 대한 이벤트 생성을 동일한 대상으로 향하는 트래픽에서 매 60초당 하나의 이벤트로 제한합니다. 전역 규칙 임계값 설정 옵션의 기본값은 다음과 같습니다.

- **Type(**유형**)** — 제한
- **Track By(**추적 방법**)** — 대상
- **Count(**카운트**)** — 1
- **Seconds(**초**)** — 60

이러한 기본값은 다음과 같이 수정할 수 있습니다.

표 *1:* 임계값 설정 유형

옵션	설명
Limit(제한)	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(count 인수로 지정)에 대한 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Limit(**제한**)**로, **Count(**카운트**)**는 `10`으로, 그리고 **Seconds(**초**)**는 `60`으로 설정하고 14개의 패킷이 규칙을 트리거하는 경우, 시스템은 동일한 시간(분) 내 발생한 첫 10개의 패킷을 표시한 후 규칙의 이벤트 로깅을 중단합니다.

옵션	설명
Threshold(임계값)	지정된 기간 중 지정된 패킷 수(count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅하고 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅하면 시간에 대한 카운터가 다시 시작됩니다. 예를 들어, 유형은 **Threshold(**임계값**)**로, **Count(**카운트**)**는 10으로, 그리고 **Seconds(**초**)**는 60으로 설정하면 규칙은 33초에 10번 트리거됩니다. 시스템은 하나의 이벤트를 생성한 다음, Seconds(초) Count(카운트) 카운터를 0으로 재설정합니다. 그런 다음 규칙은 다음 25초 안에 다시 10번 트리거됩니다. 33초에 카운터가 0으로 재설정되므로 시스템은 또 다른 이벤트를 로깅합니다.
Both(모두)	지정된 수(카운트)의 패킷이 규칙을 트리거한 후 특정 시기 동안 한 번에 하나의 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Both(**모두**)**로, **Count(**카운트**)**는 2로, 그리고 **Seconds(**초**)**는 10으로 설정하면, 다음 이벤트가 결과를 카운트합니다. • 규칙이 10초 안에 한 번 트리거되는 경우, 시스템은 어떤 이벤트도 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초 안에 두 번 트리거되는 경우, 시스템은 하나의 이벤트를 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

Track By(추적 기준**)** 옵션은 이벤트 인스턴스 카운트가 소스 IP 주소별로 계산되는지 대상 IP 주소별로 계산되는지 결정합니다.

다음과 같이 임계값을 정의하는 인스턴스 수와 기간도 지정할 수 있습니다.

표 ***2:*** 임계값 설정 인스턴스/시간 옵션

옵션	설명
Count	**Limit(**제한**)** 임계값의 경우, 임계값 충족에 필요한 IP 주소 또는 주소 범위 추적별로 지정된 기간별 이벤트 인스턴스의 수. **Threshold(**임계값**)** 임계값의 경우, 임계값으로 사용할 규칙 일치의 수.

옵션	설명
Seconds	**Limit** 임계값의 경우, 공격이 추적되는 기간을 구성하는 초 단위의 시간. **Threshold** 임계값의 경우, 카운트가 재설정되기까지 경과하는 초 단위의 시간. 임계값 유형을 **Limit(**제한**)**로, 추적을 **Source(**소스**)**로, **Count(**카운트**)**를 10으로, 그리고 **Seconds(**초**)**를 10으로 설정한 경우, 시스템은 주어진 소스 포트에서 10초 안에 발생한 첫 10개의 이벤트를 로깅하고 표시합니다. 첫 10초 안에 일곱 개의 이벤트만 발생한 경우, 시스템은 이를 모두 로깅하고 표시하며, 첫 10초 안에 40개의 이벤트가 발생한 경우, 시스템은 10개를 로깅하고 표시한 후, 10초의 시간이 경과한 시점에서 다시 카운팅을 시작합니다.

관련 항목

전역 임계값 구성, 5 페이지
침입 이벤트 임계값

전역 임계값에 대한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

전역 임계값 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

전역 임계값 구성

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Intrusion Rule Thresholds(**침입 규칙 임계값**)**에서 **Global Rule Thresholding(**전역 규칙 임계값 설정**)**이 비활성화된 경우, **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Global Rule Thresholding(**전역 규칙 임계값**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Type(**유형**)**을 사용하여 **Seconds(**초**)** 필드에서 지정하는 시간 동안 적용할 임계값 유형을 지정합니다.

단계 **7** **Track By(**추적 기준**)**을 사용하여 추적 방법을 지정합니다.

단계 **8** **Count(**카운트**)** 필드에 값을 입력합니다.

단계 **9** **Seconds(**초**)** 필드에 값을 입력합니다.

단계 **10** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

전역 규칙 임계값 옵션, 2 페이지
레이어에서 침입 규칙 구성
충돌 및 변경: 네트워크 분석 및 침입 정책

전역 임계값 비활성화

임계값 설정을 모든 규칙에 기본적으로 적용하지 않고 특정 규칙에 대한 이벤트 임계값을 설정하려는 경우, 최상위 정책 레이어에서 전역 임계값 설정을 비활성화할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Intrusion Rule Thresholds(**침입 규칙 임계값**)** 아래 **Global Rule Thresholding(**전역 규칙 임계값 설정**)** 옆에서 **Disabled(**비활성화**)**를 클릭합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책
레이어에서 침입 규칙 구성