규칙을 사용하여 침입 정책 조정

다음 주제에서는 규칙을 사용하여 침입 정책을 조정하는 방법을 설명합니다.

침입 규칙 조정 기본 사항

침입 정책의 Rules(규칙) 페이지를 사용하여 공유 개체 규칙, 표준 텍스트 규칙, 전처리기 규칙의 규칙 상태 및 기타 설정을 구성할 수 있습니다.

규칙 상태를 Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)으로 설정하여 규칙을 활성화합니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 이벤트를 생성합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다. 인라인 구축에서 Drop and Generate Events(이벤트 삭제 및 생성)으로 설정된 규칙이 일치하는 트래픽에 대해 이벤트를 생성하거나 해당 트래픽을 삭제하도록 침입 정책을 설정할 수도 있습니다. 수동 배포에서, Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙은 일치 트래픽에만 이벤트를 생성합니다.

하위 집합을 표시하도록 규칙을 필터링하면 규칙 상태 또는 규칙 설정을 변경하고자 하는 정확한 규칙 집합을 선택할 수 있습니다.

침입 규칙 또는 규칙 인수에 비활성화된 전처리기가 필요한 경우, 네트워크 분석 정책의 웹 인터페이스에서 전처리기가 비활성화 상태로 남아 있더라도 시스템은 자동으로 전처리기를 현재 구성으로 사용합니다.

침입 규칙 유형

침입 규칙은 시스템이 네트워크에서 취약점을 익스플로잇하려는 시도를 탐지하는 데 사용하는 키워드와 인수의 지정된 집합입니다. 시스템에서 네트워크 트래픽을 분석하면서 각 규칙에 지정된 조건과 패킷을 비교하고 데이터 패킷이 규칙에 지정된 모든 조건을 충족하는 경우 규칙을 트리거합니다.

침입 정책에는 다음이 포함됩니다.

- 침입 규칙(공유 개체 규칙 및 표준 텍스트 규칙으로 세분화됨)
- 패킷 디코더의 탐지 옵션 또는 시스템에 포함된 전처리기 중 하나와 연결된 전처리기 규칙

다음 표에는 이러한 규칙 유형의 속성이 요약되어 있습니다.

표 *1:* 침입 규칙 유형

유형	**GID(generator ID)**	**Snort ID SID**	소스	복사 가능 여부	편집 가능 여부
공유 객체 규칙	3	1000000 미만	Talos 인텔리전스 그룹	예	제한적
표준 텍스트 규칙	1 (전역 도메인 또는 레거시 GID)	1000000 미만	Talos	예	제한적
	1000 - 2000 (하위 도메인)	1000000 이상	사용자가 생성하거나 가져옴	예	예
전처리기 규칙	디코더 또는 전처리기별	1000000 미만	Talos	아니요	아니요
		1000000 이상	옵션 구성 중 시스템에서 생성	아니요	아니요

Talos에서 생성한 규칙의 변경 사항은 저장할 수 없지만 맞춤형 규칙으로 수정된 규칙의 복사본은 저장할 수 있습니다. 규칙 또는 규칙 헤더 정보(예: 소스 및 대상 포트와 IP 주소)에 사용되는 변수 중 하나를 수정할 수 있습니다. 다중 도메인 구축에서 Talos에 의해 생성된 규칙은 전역 도메인에 속합니다. 하위 도메인의 관리자는 규칙의 로컬 복사본을 저장한 다음 편집할 수 있습니다.

Talos은 생성하는 규칙마다 각 기본 침입 정책에서 기본 규칙 상태를 할당합니다. 대부분의 전처리기 규칙은 기본적으로 비활성화되어 있으며, 시스템에서 전처리기 규칙을 위한 이벤트를 생성하고 인라인 구축에서 문제가 되는 패킷을 삭제하도록 하려면 활성화해야 합니다.

침입 규칙 라이선스 요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

침입 규칙 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 정책의 침입 규칙 보기

침입 정책에서 규칙이 표시되는 방법을 조정할 수 있으며, 여러 기준으로 규칙을 정렬할 수 있습니다. 또한 규칙 설정, 규칙 문서 및 기타 규칙 사양을 보려면 특정 규칙에 대한 세부사항을 표시할 수 있습니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 규칙을 보면서 다음을 수행할 수 있습니다.

- 침입 정책에서 규칙 필터 설정, 15 페이지에 설명된 대로 규칙을 필터링합니다.
- 정렬하려는 열의 상단에서 제목을 클릭하여 규칙을 정렬합니다.
- 침입 규칙 세부 사항 보기, 5 페이지에 설명된 대로 침입 규칙의 세부 정보를 봅니다.
- **Policy(**정책**)** 드롭다운 목록에서 레이어를 선택하여 다른 정책 레이어의 규칙을 봅니다.

침입 규칙 페이지 열

침입 규칙 페이지는 메뉴 바와 열 헤더에서 동일한 아이콘을 사용합니다. 예를 들어, Rule State(규칙 상태) 메뉴는 규칙 목록의 Rule State(규칙 상태) 열과 동일한 **Generate Events(**이벤트 생성**)**를 사용합니다.

표 *2:* 규칙 페이지 열

제목	설명
GID	규칙의 GID(Generator ID)를 나타내는 정수.
SID	Snort ID(SID)를 나타내는 정수로, 규칙의 고유한 식별자 역할을 합니다. 맞춤형 규칙의 경우, SID는 1000000 이상입니다.
메시지	규칙 이름으로도 작동하는 이 규칙에서 생성된 이벤트에 포함된 메시지.
이벤트 생성	규칙의 규칙 상태: • 이벤트 삭제 및 생성 • 이벤트 생성 • **Disabled** 비활성화된 규칙의 아이콘은 트래픽 삭제 없이 이벤트를 생성하도록 설정된 규칙의 아이콘이 흐리게 표시된 버전입니다. 또한 규칙의 규칙 상태 아이콘을 클릭하면 규칙 상태를 변경할 수 있습니다.
Cisco 권장 규칙 상태	Cisco가 권장하는 규칙의 규칙 상태
이벤트 필터	규칙에 적용된 이벤트 임계값 및 이벤트 삭제를 포함하는 이벤트 필터.
동적 상태	특정 속도 이상이 발생한 경우 효과를 나타내는 규칙을 위한 동적 상태 규칙.
Error(오류**)** ( )	규칙에 구성된 알림(현재는 SNMP 알림만 해당됨)
Comment(코멘트**)** ( )	규칙에 추가된 코멘트.

또한 레이어 드롭다운 목록을 사용하여 침입 정책의 다른 레이어에 대한 Rules(규칙) 페이지로 전환할 수 있습니다. 정책에 레이어를 추가하지 않는 한, 드롭다운 목록에 나열되는 수정 가능한 보기는

정책 Rules(규칙) 페이지 및 정책 레이어에 대한 Rules(규칙) 페이지(원래 이름은 My Changes)뿐입니다. 이 두 보기 중 하나에서 변경하는 것은 다른 보기에서 변경하는 것과 동일합니다. 드롭다운 목록에는 읽기 전용 기본 정책을 위한 Rules(규칙) 페이지도 나열됩니다.

침입 규칙 세부 사항

Rule Detail(규칙 세부 사항) 보기에서 규칙 문서, Cisco 권장 사항 및 규칙 오버헤드를 볼 수 있습니다. 또한 규칙 특정 기능을 보고 추가할 수 있습니다.

표 *3:* 규칙 세부사항

항목	설명
요약	규칙 요약. 규칙 기반 이벤트의 경우, 규칙 문서에 요약 정보가 포함되어 있으면 이 행이 나타납니다.
규칙 상태	해당 규칙에 대한 현재 규칙 상태. 규칙 상태가 설정된 레이어를 나타내기도 합니다.
Cisco 권장 사항	Cisco 권장 사항이 생성된 경우, 권장 규칙 상태를 나타내는 아이콘(침입 규칙 페이지 열, 4 페이지 참조). 권장 사항이 규칙 활성화인 경우, 시스템은 권장 사항을 트리거한 네트워크 자산 또는 구성도 표시합니다.
규칙 오버헤드	시스템 성능에 대한 규칙의 잠재적 영향력 및 규칙이 오탐을 생성할 가능성. 취약성에 매핑되지 않는 한 로컬 규칙에는 할당된 오버헤드가 없습니다.
임계값	현재 이 규칙에 설정된 임계값이자 해당 규칙에 대해 임계값을 추가하는 기능
삭제	현재 이 규칙에 설정된 삭제 설정이자 해당 규칙에 대해 삭제를 추가하는 기능
동적 상태	현재 이 규칙에 설정된 등급 기반 규칙 상태 및 해당 규칙의 동적 규칙 상태를 추가하는 기능.
알림	이 규칙에 설정된 SNMP 알림 및 해당 규칙에 대한 알림을 추가하는 기능.
코멘트	이 규칙에 추가된 코멘트이자 해당 규칙에 대해 코멘트를 추가하는 기능
설명서	Talos 인텔리전스 그룹가 제공한 현재 규칙의 규칙 문서. 원하는 경우, 더 구체적인 규칙 세부 사항을 보려면 **Rule Documentation(**규칙 문서**)**을 클릭합니다.

침입 규칙 세부 사항 보기

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색 창에서 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 규칙 세부 사항을 보려는 규칙을 클릭한 다음 페이지 하단에서 **Show Details(**세부 정보 표시**)**를 클릭합니다.
침입 규칙 세부 사항, 5 페이지에 설명된 대로 규칙 세부 사항이 표시됩니다.

단계 **5** 규칙 세부 사항에서 다음을 구성할 수 있습니다.

- 알림 - 침입 규칙에 대한 SNMP 알림 설정, 8 페이지 참조.
- 코멘트 - 침입 규칙에 설명 추가, 9 페이지 참조.
- 동적 규칙 상태 - 규칙 세부 사항 페이지에서 동적 규칙 상태 설정, 7 페이지 참조.
- 임계값 - 침입 규칙에 대한 임계값 설정, 6 페이지 참조.
- 억제 - 침입 규칙에 대한 삭제 설정, 7 페이지 참조.

침입 규칙에 대한 임계값 설정

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 단일 임계값을 설정할 수 있습니다. 임계값을 추가하여 규칙에 대한 기존 임계값을 덮어씁니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 이를 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워 둡니다.

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Thresholds(**임계값**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Type(**유형**)** 드롭다운 목록에서 설정하려는 임계값 유형을 선택합니다.

- **Limit(**제한**)**를 선택하여 기간당 지정된 이벤트 인스턴스 수로 알림을 제한합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold(**임계값**)**를 선택합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both(**모두**)**를 선택합니다.

단계 **3** 이벤트 인스턴스를 소스 IP 주소로 추적할지 대상 IP 주소로 추적할지 나타내려면 **Track By(**추적 기준**)** 드롭다운 목록에서 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택합니다.

단계 **4** 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(**카운트**)** 필드에 입력합니다.

단계 **5** 이벤트 인스턴스를 추적할 기간(초 단위)을 지정하는 숫자를 **Seconds(**초**)** 필드에 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 이벤트 필터 개수가 표시됩니다.

침입 규칙에 대한 삭제 설정

침입 규칙에서 규칙에 하나 이상의 억제를 설정할 수 있습니다.

유효하지 않은 값을 입력하면 **Revert(**되돌리기**)**가 이 필드에 나타난다는 점에 유의하십시오. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Suppressions(**억제**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Suppression Type(**억제 유형**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 선택한 규칙에 대한 이벤트를 완전히 억제하려면 **Rule(**규칙**)**을 선택합니다.
- 지정된 소스 IP 주소에서 시작되는 패킷에 의해 생성된 이벤트를 억제하려면 **Source(**소스**)**를 선택합니다.
- 지정된 대상 IP 주소로 이동하는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination(**대상**)**을 선택합니다.

단계 **3** 억제 유형으로 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택한 경우, **Network(**네트워크**)** 필드에 IP 주소, 주소 블록 또는 이러한 항목의 조합으로 구성된 쉼표로 구분된 목록을 입력합니다.

침입 정책이 액세스 제어 정책의 기본 작업과 연결된 경우 기본 작업 변수 집합의 네트워크 변수를 지정하거나 나열할 수도 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

팁 시스템은 억제된 규칙 옆의 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 필터 위의 숫자는 이벤트 필터의 수를 나타냅니다.

규칙 세부 사항 페이지에서 동적 규칙 상태 설정

규칙에 하나 이상의 동적 규칙 상태를 설정할 수 있습니다. 나열된 첫 번째 동적 규칙 상태의 우선 순위가 가장 높습니다. 2개의 동적 규칙 상태가 충돌하면 첫 번째 상태의 작업이 수행됩니다.

동적 규칙 상태는 정책에 따라 다릅니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 이를 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워 둡니다.

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Dynamic State(**동적 상태**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Track By(**추적 기준**)** 드롭다운 목록에서 옵션을 선택해 규칙 일치를 추적할 방법을 나타냅니다.

- 특정 소스 또는 소스 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Source(**소스**)**를 선택합니다.
- 특정 대상 또는 대상 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Destination(**대상**)**을 선택합니다.
- 해당 규칙의 모든 일치를 추적하려면 **Rule(**규칙**)**을 선택합니다.

단계 **3** **Track By(**추적 기준**)**를 **Source(**소스**)** 또는 **Destination(**대상**)**으로 설정하는 경우, **Network (**네트워크**)** 필드에 추적하려는 각 호스트의 IP 주소를 입력합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 공격 속도를 설정하려면 **Rate(**속도**)** 옆에 기간당 규칙 일치 수를 지정합니다.

- 임계값으로 사용할 규칙 일치의 수를 **Count(**카운트**)** 필드에서 지정합니다.
- **Seconds(**초**)** 필드에서 공격을 추적할 기간을 구성하는 시간(초)을 지정합니다.

단계 **5** **New State(**새로운 상태**)** 드롭다운 목록에서 조건이 충족되면 취할 새로운 작업을 선택합니다.

단계 **6** **Timeout(**시간 제한**)** 필드에 값을 입력합니다.

시간 제한이 발생한 후, 규칙은 원래 상태로 돌아갑니다. 새로운 작업이 시간 초과되는 것을 방지하려면 `0`을 입력합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Dynamic State(동적 상태) 열의 규칙 옆에 동적 상태()를 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가한 경우, 필터 위의 숫자는 필터 수를 나타냅니다.

침입 규칙에 대한 **SNMP** 알림 설정

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 SNMP 알림을 설정할 수 있습니다.

프로시저

침입 규칙의 세부 사항에서 **Alerts(**알림**)** 옆에 있는 **Add SNMP Alert(SNMP** 알림추가**)**를 클릭합니다.

팁 시스템은 Alerting(알림) 열의 규칙 옆에 알림 아이콘(**Error(**오류**)** ())을 표시합니다. 규칙에 여러 알림을 추가하는 경우 알림 개수가 표시됩니다.

침입 규칙에 설명 추가

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Comments(**코멘트**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Comments(**코멘트**)** 필드에 규칙 코멘트를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Comments(코멘트) 열의 규칙 옆에 **Comment(**코멘트**)** ( )를 표시합니다. 규칙에 여러 코멘트를 추가하는 경우, 코멘트 위의 숫자는 코멘트 수를 나타냅니다.

단계 **4** 규칙 코멘트를 삭제하려면 규칙 코멘트 섹션에서 **Delete(**삭제**)**를 클릭합니다. 커밋되지 않은 침입 정책 변경 사항과 함께 코멘트가 캐시된 경우에만 코멘트를 삭제할 수 있습니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

침입 정책의 침입 규칙 필터

Rules(규칙) 페이지에 표시된 규칙을 단일 기준 또는 여러 기준의 조합으로 필터링할 수 있습니다.

규칙 필터 키워드를 사용하면 규칙 설정(예: 규칙 상태 또는 이벤트 필터)을 적용할 규칙을 쉽게 찾을 수 있습니다. 키워드로 필터링하고 동시에 Rules(규칙) 페이지 필터 패널에서 원하는 인수를 선택하여 키워드에 대한 인수를 선택할 수 있습니다.

침입 규칙 필터 참고 사항

구성한 필터가 Filter(필터) 텍스트 상자에 표시됩니다. 필터 패널에서 키워드 및 키워드 인수를 클릭하여 필터를 구성할 수 있습니다. 여러 키워드를 선택하면 시스템에서 AND 논리로 키워드를 통합하여 복합 검색 필터를 생성합니다. 예를 들어 **Category(**카테고리**)** 아래에서 **preprocessor(**전처리기**)**를 선택한 다음 **Rule Content(**규칙 콘텐츠**)** > **GID**를 선택하고 `116`을 입력하면 `Category: “preprocessor” GID:”116”` 필터가 생성됩니다. 이 필터는 전처리기 규칙이고 GID가 116인 규칙을 모두 검색합니다.

Category(카테고리), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Platform Specific(플랫폼 특징), Preprocessor(전처리기) 및 Priority(우선 순위) 필터 그룹을 통해 키워드를 위한 1개 이상의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어 **Category(**카테고리**)**에서 **os-linux** 및 **os-windows**를 선택하면 `Category:"os-windows,os-linux"` 필터를 생성할 수 있습니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리에 속하는 모든 규칙을 검색합니다.

필터 패널을 표시하려면 표시 아이콘을 클릭합니다.

필터 패널을 숨기려면, 숨기기 아이콘을 클릭합니다.

침입 정책 규칙 필터 구성 가이드라인

대부분의 경우, 필터를 작성할 때 침입 정책의 Rules(규칙) 페이지 왼쪽에 있는 필터 패널을 사용하여 원하는 키워드/인수를 선택할 수 있습니다.

Rule(규칙) 필터는 필터 패널의 규칙 필터 그룹으로 그룹화됩니다. 많은 규칙 필터 그룹에 하위 기준이 포함되어 있어서 원하는 특정 규칙을 손쉽게 찾을 수 있습니다. 일부 규칙 필터에는 개별 규칙으로 드릴다운하기 위해 확장할 수 있는 여러 레벨이 있습니다.

필터 패널의 항목은 때로는 필터 유형 그룹, 때로는 키워드, 그리고 때로는 키워드에 대한 인수를 나타냅니다. 다음에 유의하십시오.

- 키워드(Rule Configuration(규칙 구성), Rule Content(규칙 콘텐츠), Platform Specific(플랫폼별) 및 Priority(우선순위)가 아닌 필터 유형 그룹 제목을 선택하면 확장되어 사용 가능한 키워드가 나열됩니다.

  기준 목록의 노드를 클릭하여 키워드를 선택하면 팝업 창이 나타나는데, 여기에서 필터링할 인수를 제공합니다.

  해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

  예를 들어 필터 패널에서 **Rule Configuration(**규칙 구성**)** > **Recommendation(**권장 사항**)** 아래에 있는 **Drop and Generate Events(**이벤트 삭제 및 생성**)**를 클릭하는 경우, 필터 텍스트 상자에 `Recommendation: "Drop and Generate Events"`가 추가됩니다. 그런 다음 **Rule Configuration(**규칙 구성**)** > **Recommendation(**권장 사항**)** 아래에 있는 **Generate Events(**이벤트 생성**)**를 클릭하는 경우, 필터가 `Recommendation:"Generate Events"`로 변경됩니다.

- 키워드(Category(카테고리), Classifications(분류), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Priority(우선 순위) 및 Rule Update(규칙 업데이트))인 필터 유형 그룹 제목을 선택하면 사용 가능한 인수가 나열됩니다.

  이 그룹 유형에서 항목을 선택하면 항목이 적용하는 인수와 키워드가 필터에 즉시 추가됩니다. 키워드가 필터에 이미 있는 경우, 그룹에 해당하는 키워드에 대한 기존 인수를 교체합니다.

  예를 들어 필터 패널에서 **Category(**카테고리**)** 아래의 **os Linux**를 클릭할 경우, 필터 텍스트 상자에 `Categoy:"os-linux"`가 추가됩니다. 그런 다음 **Category(**카테고리**)** 아래에서 **os-windows**를 클릭하면 필터가 `Category:"os-windows"`로 변경됩니다.

- Rule Content(규칙 콘텐츠) 아래의 참조는 키워드이며, 그 아래에 나열된 참조 ID 유형도 마찬가지입니다. 참조 키워드를 선택하면 팝업 창이 나타납니다. 여기서 인수를 제공하면 기존 필터에 키워드가 추가됩니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우, 새로 제공하는 인수가 기존 인수를 교체합니다.

  예를 들어, 필터 패널에서 **Rule Content(**규칙 내용**)** > **Reference(**참조**)** > **CVE ID**를 클릭하면 팝업 창에 CVE ID를 입력하라는 메시지가 표시됩니다. `2007`을 입력한 경우, 다음 `CVE: “2007”`이 필터 텍스트 상자에 추가됩니다. 예를 들어 필터 패널에서 **Rule Content(**규칙 내용**)** > **Reference(**참조**)**를 클릭하면 팝업 창에 참조를 입력하라는 메시지가 표시됩니다. `2007`을 입력한 경우, `Reference:”2007”`이 필터 텍스트 상자에 추가됩니다.

- 서로 다른 그룹에서 규칙 필터 키워드를 선택하면 각 필터 키워드가 필터에 추가되며 기존 키워드는 유지됩니다(동일한 키워드의 새 값으로 덮어쓰지 않는 한).

  예를 들어 필터 패널에서 **Category(**카테고리**)** 아래의 **os Linux**를 클릭할 경우, 필터 텍스트 상자에 `Categoy:"os-linux"`가 추가됩니다. **Microsoft Vulnerabilities(Microsoft** 취약성**)** 아래의 **MS00-006**을 클릭할 경우, 필터는 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`으로 변경됩니다.

- 여러 키워드를 선택하면 시스템에서 AND 논리로 키워드를 통합하여 복합 검색 필터를 생성합니다. 예를 들어 **Category(**카테고리**)** 아래에서 **preprocessor(**전처리기**)**를 선택한 다음 **Rule Content(**규칙 콘텐츠**)** > **GID**를 선택하고 `116`을 입력하면 `Category: “preprocessor” GID:”116”` 필터가 생성됩니다. 이 필터는 전처리기 규칙이고 GID가 116인 규칙을 모두 검색합니다.

- Category(카테고리), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Platform Specific(플랫폼 특징) 및 Priority(우선 순위) 필터 그룹을 통해 키워드를 위한 하나 이상의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어 **Category(**카테고리**)**에서 **os-linux** 및 **os-windows**를 선택하면 `Category:"os-windows,app-detect"` 필터를 생성할 수 있습니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리에 속하는 모든 규칙을 검색합니다.

둘 이상의 필터 키워드/인수 쌍으로 동일한 규칙을 검색할 수 있습니다. 예를 들어, 규칙이 **dos** 카테고리에서 필터링될 경우, 그리고 **High(**높은**)** 우선 순위로 필터링할 경우 DOS Cisco 시도 규칙(SID 1545)이 나타납니다.

참고 Talos 인텔리전스 그룹는 규칙 업데이트 메커니즘을 사용하여 규칙 필터를 추가 및 제거할 수 있습니다.

Rules(규칙) 페이지에 있는 규칙은 공유 개체 규칙(generator ID 3) 또는 표준 텍스트 규칙(generator ID 1, Global domain or legacy GID; 1000 - 2000, descendant domains)일 수 있습니다. 다음 표는 다양한 규칙 필터에 대해 설명합니다.

표 *4:* 규칙 필터 그룹

필터 그룹	설명	다중 인수 지원 여부	제목	목록 내 항목
규칙 컨피그레이션	규칙의 구성에 따라 규칙을 찾습니다.	아니요	그룹화	키워드
규칙 콘텐츠	규칙의 내용에 따라 규칙을 찾습니다.	아니요	그룹화	키워드
카테고리	규칙 편집기에 사용되는 규칙 카테고리에 따라 규칙을 찾습니다. 로컬 규칙은 로컬 하위 그룹에 나타납니다.	예	키워드	인수
분류	규칙에 의해 생성된 이벤트의 패킷 표시에 나타나는 공격 분류에 따라 규칙을 찾습니다.	아니요	키워드	인수

필터 그룹	설명	다중 인수 지원 여부	제목	목록 내 항목
Microsoft 취약성	Microsoft 게시판 번호에 따라 규칙을 찾습니다.	예	키워드	인수
Microsoft 웜	Microsoft Windows 호스트에 영향을 미치는 특정 웜에 따라 규칙을 찾습니다.	예	키워드	인수
플랫폼별	특정 운영 체제 버전에 대한 연관성에 따라 규칙을 찾습니다. 규칙 하나가 둘 이상의 운영 체제 또는 둘 이상의 운영 체제 버전에 영향을 미칠 수 있습니다. 예를 들어, SID 2260을 활성화하면 Mac OS X, IBM AIX 및 기타 운영 체제의 모든 버전에 영향을 줍니다.	예	키워드	인수 하위 목록의 항목 중 하나를 선택한 경우, 인수에 수정자가 추가됩니다.
전처리기	개별 전처리기에 대한 규칙을 찾습니다. 전처리기가 활성화되었을 때 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 전처리기 옵션에 연결된 전처리기 규칙을 활성화해야 합니다.	예	그룹화	하위 그룹화
우선순위	높음, 중간, 낮음 우선순위에 따라 규칙을 찾습니다. 규칙에 할당된 분류가 우선순위를 결정합니다. 이 그룹은 규칙 카테고리로 심화 그룹화됩니다. 로컬 규칙(즉, 사용자가 가져오거나 생성하는 규칙)은 우선순위 그룹에 나타나지 않습니다.	예	키워드	인수 하위 목록의 항목 중 하나를 선택한 경우, 인수에 수정자가 추가됩니다.
규칙 업데이트	특정 규칙 업데이트를 통해 추가 또는 수정된 규칙을 찾습니다. 각 규칙 업데이트에 대해 모든 규칙을 보거나, 가져온 규칙만 보거나, 업데이트에 의해 변경된 기존 규칙만 볼 수 있습니다.	아니요	키워드	인수

침입 규칙 설정 필터

Rules(규칙) 페이지에 나열되는 규칙을 여러 규칙 컨피그레이션 설정으로 필터링할 수 있습니다. 예를 들어 규칙 상태가 권장 규칙 상태에 일치하지 않는 규칙 집합을 보려는 경우, **Does not match recommendation(**권장 규칙 상태에 일치하지 않음**)**을 선택하여 규칙 상태를 필터링할 수 있습니다.

기준 목록의 노드를 클릭하여 키워드를 선택하면 필터링할 인수를 입력할 수 있습니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

예를 들어 필터 패널에서 **Rule Configuration(**규칙 구성**)** > **Recommendation(**권장 사항**)** 아래에 있는 **Drop and Generate Events(**이벤트 삭제 및 생성**)**를 클릭하는 경우, 필터 텍스트 상자에 `Recommendation: "Drop and Generate Events"`가 추가됩니다. 그런 다음 **Rule Configuration(**규칙 구성**)** >

Recommendation(권장 사항**)** 아래에 있는 **Generate Events(**이벤트 생성**)**를 클릭하는 경우, 필터가 `Recommendation:"Generate Events"`로 변경됩니다.

침입 규칙 콘텐츠 필터

Rules(규칙) 페이지에 나열되는 규칙을 여러 규칙 콘텐츠 항목별로 필터링할 수 있습니다. 예를 들어, 규칙의 SID를 검색하여 규칙을 빠르게 검색할 수 있습니다. 또한 특정 목적지 포트로 가는 트래픽을 검사하는 모든 규칙을 찾을 수 있습니다.

기준 목록의 노드를 클릭하여 키워드를 선택하면 필터링할 인수를 입력할 수 있습니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

예를 들어 필터 패널의 **Rule Content(**규칙 콘텐츠**)**에서 **SID**를 클릭하면 SID를 입력하라는 팝업 창이 나타납니다. `1045`를 입력하면 `SID:"1045"`가 필터 텍스트 상자에 추가됩니다. 그런 다음 **SID**를 다시 클릭하여 SID 필터를 `1044`로 변경하면 필터가 `SID:"1044"`로 바뀝니다.

표 ***5:*** 규칙 콘텐츠 필터

이 필터는**...**	다음과 같은 규칙을 찾습니다**.**
메시지	메시지 필드에 제공된 문자열을 포함합니다.
SID	지정된 SID가 있습니다.
GID	지정된 GID가 있습니다.
참조	참조 필드에 제공된 문자열을 포함합니다. 특정 참조 유형과 제공된 문자열을 기준으로 필터링할 수도 있습니다.
조치	`Alerts(알림)` 또는 `pass(통과)`로 시작합니다.
프로토콜	선택한 프로토콜을 포함합니다.
방향	표시된 방향 설정이 규칙에 포함되어 있는지 여부에 기반합니다.
소스 IP	규칙에서 소스 IP 주소 지정에 특정 주소나 변수를 사용합니다. 유효한 IP 주소, CIDR 블록/접두사 길이로 필터링하거나 `$HOME_NET` 또는 `$EXTERNAL_NET` 같은 변수를 사용하여 필터링할 수 있습니다.
대상 IP	규칙에서 소스 IP 주소 지정에 특정 주소나 변수를 사용합니다. 유효한 IP 주소, CIDR 블록/접두사 길이로 필터링하거나 `$HOME_NET` 또는 `$EXTERNAL_NET` 같은 변수를 사용하여 필터링할 수 있습니다.
소스 포트	지정된 소스 포트를 포함합니다. 포트 값은 1과 65535 사이의 정수이거나 포트 변수여야 합니다.
대상 포트	지정된 대상 포트를 포함합니다. 포트 값은 1과 65535 사이의 정수이거나 포트 변수여야 합니다.
규칙 오버헤드	선택한 규칙 오버 헤드가 있습니다.

이 필터는...	다음과 같은 규칙을 찾습니다.
메타데이터	일치하는 키 값 쌍을 포함하는 메타데이터가 있습니다. 예를 들어, HTTP 애플리케이션 프로토콜과 관련된 메타데이터로 규칙을 찾으려면 `metadata:"service http"`를 입력합니다.

침입 규칙 카테고리

Firepower System은 규칙이 탐지하는 트래픽 유형에 따라 카테고리에 규칙을 배치합니다. Rules(규칙) 페이지에서 규칙 카테고리로 필터링하여, 한 카테고리의 모든 규칙에 대해 규칙 속성을 설정할 수 있습니다. 예를 들어 네트워크에 Linux 호스트가 없는 경우, **os-linux** 카테고리로 필터링한 다음 표시되는 모든 규칙을 비활성화하여 전체 **os-linux** 카테고리를 비활성화할 수 있습니다.

마우스 포인터를 카테고리 이름 위로 이동하면 해당 카테고리의 규칙 수가 표시됩니다.

참고 Talos 인텔리전스 그룹는 규칙 업데이트 메커니즘을 사용하여 카테고리를 추가 및 제거할 수 있습니다.

침입 규칙 필터 구성 요소

필터 패널에서 필터를 클릭할 때 제공되는 특수 키워드 및 해당 인수를 변경하려면 필터를 수정할 수 있습니다. Rules(규칙) 페이지의 사용자 지정 필터 규칙은 규칙 편집기에서 사용되는 것처럼 기능하지만 필터 패널을 통해 필터를 선택할 때 표시되는 구문을 사용하여 Rules(규칙) 페이지 필터에 제공된 모든 키워드를 사용할 수 있습니다. 나중에 사용할 키워드를 결정하려면 필터 패널 오른쪽에서 적절한 인수를 클릭합니다. 필터 텍스트 상자에 필터 키워드와 인수 구문이 나타납니다. 키워드에 대한 쉼표로 구분된 여러 인수는 Category(카테고리) 및 Priority(우선 순위) 필터 유형에만 지원된다는 점을 기억하십시오.

키워드와 인수, 문자 문자열, 따옴표의 리터럴 문자 문자열을 사용할 수 있으며 여러 필터 조건을 공백으로 구분할 수 있습니다. 필터에는 정규 표현식, 와일드카드 문자 또는 부정 문자(!), 보다 큼 기호(>), 보다 작음 기호(<)와 같은 특별 연산자를 포함할 수 없습니다. 키워드 없이, 키워드의 첫 글자 대문자 없이 또는 인수 앞뒤의 따옴표 없이 검색할 용어를 입력하면 검색은 문자열 검색으로 처리되며, 지정된 용어가 카테고리, 메시지 및 SID 필드에서 검색됩니다.

`gid` 및 `sid` 키워드를 제외한, 모든 인수 및 문자열은 부분 문자열로 처리됩니다. `gid` 및 `sid`의 인수는 정확히 일치하는 것만 반환합니다.

각 규칙 필터의 형식에는 하나 이상의 키워드를 포함할 수 있습니다.

keyword:"*argument*"

키워드가 침입 규칙 필터 그룹의 키워드 중 하나이고 인수가 큰 따옴표로 둘러싸여 있으며 특정 필드 또는 키워드 관련 필드에서 검색할 단일 대소문자 구분 영숫자 문자열인 경우입니다. 키워드의 첫 글자는 대문자로 입력해야 합니다.

gid 및 sid를 제외한 모든 키워드에 대한 인수는 부분 문자열로 처리됩니다. 예를 들어, 인수 123은 "12345", "41235", "45123" 등을 반환합니다. gid 및 sid의 인수는 정확하게 일치하는 경우에만 반환됩니다. 예를 들어, sid:3080은 SID 3080만 반환합니다.

각 규칙 필터는 또한 하나 이상의 영숫자 문자 문자열을 포함할 수 있습니다. 문자열은 규칙 Message(메시지) 필드, Snort ID(SID) 및 생성자 ID(GID)를 검색합니다. 예를 들어, 문자열 123은 규칙 메시지에서 문자열 "Lotus123", "123mania" 등을 반환하며, 또한 SID 6123, SID 12375 등을 반환합니다. 하나 이상의 문자열로 필터링하여 부분 SID를 검색할 수 있습니다.

모든 문자열은 대소문자를 구분하지 않으며 부분 문자열로 처리됩니다. 예를 들어, 문자열 ADMIN, admin 또는 Admin은 모두 "admin", "CFADMIN", "Administrator" 등을 반환합니다.

정확히 일치하는 항목을 반환하기 위해 인용구에서 문자열을 묶을 수 있습니다. 예를 들어, 인용구 내 문자열 "overflow attempt"는 정확한 문자열만 반환하지만, 인용구가 없는 두 개의 문자열 overflow 및 attempt로 구성된 필터는 "overflow attempt", "overflow multipacket attempt", "overflow with evasion attempt" 등을 반환합니다.

키워드, 문자열 또는 둘 다로 이루어진 스페이스로 구분된 문자열의 조합을 입력하여 필터링 결과를 좁힐 수 있습니다. 결과는 필터링 조건과 일치하는 모든 규칙을 포함합니다.

순서에 상관없이 여러 필터 상태를 입력할 수 있습니다. 예를 들어, 다음 필터 각각은 동일한 규칙을 반환합니다.

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

침입 규칙 필터 사용

침입 정책의 Rules(규칙) 페이지 왼쪽에 있는 필터 패널에서 사전 정의된 필터 키워드를 선택할 수 있습니다. 필터를 선택하면 페이지에 모든 일치하는 규칙이 표시되거나 일치하는 규칙이 없음이 표시됩니다.

추가로 제한하려면 필터에 키워드를 추가할 수 있습니다. 입력한 모든 필터는 전체 규칙 데이터베이스를 검색하고 일치하는 규칙을 모두 반환합니다. 페이지가 계속 이전 검색 결과를 표시하고 있는데 필터를 입력하는 경우, 페이지는 이를 지우고 새 필터의 결과로 돌아갑니다.

필터를 선택할 때 제공된 동일한 키워드 및 인수 구문을 사용하여 필터를 입력할 수도 있고, 선택한 후 필터에서 인수 값을 수정할 수도 있습니다. 키워드 없이, 키워드의 첫 글자 대문자 없이 또는 인수 앞뒤의 따옴표 없이 검색할 용어를 입력하면 검색은 문자열 검색으로 처리되며, 지정된 용어가 카테고리, 메시지 및 SID 필드에서 검색됩니다.

침입 정책에서 규칙 필터 설정

규칙의 하위 집합을 표시하려면 Rule(규칙) 페이지에서 규칙을 필터링할 수 있습니다. 그런 다음 컨텍스트 메뉴에서 사용 가능한 기능 선택을 포함하여 원하는 페이지 기능을 사용할 수 있습니다. 이 기능은 예를 들어 특정 카테고리의 모든 규칙에 대해 임계값을 설정하고자 할 때 유용할 수 있습니다.

필터링된 목록이나 필터링되지 않은 목록의 규칙과 같은 기능을 사용할 수 있습니다. 예를 들어 필터링된 목록 또는 필터링되지 않은 목록에서 규칙에 새 규칙 상태를 적용할 수 있습니다.

모든 키워드, 키워드 인수 및 문자열은 대소문자를 구분하지 않습니다. 필터에 이미 있는 키워드에 대한 인수를 클릭하면 기존 인수가 교체됩니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 다음 방법을 개별적으로 사용하거나 조합하여 필터를 구성합니다.

- **Filter(**필터**)** 텍스트 상자에 값을 입력하고 Enter를 누릅니다.
- 미리 정의된 키워드를 확장합니다. 예를 들어 **Rule Configuration(**규칙 구성**)**을 클릭합니다.
- 키워드를 클릭하고 메시지가 표시되면 인수 값을 지정합니다. 예를 들면 다음과 같습니다.
  - **Rule Configuration(**규칙 구성**)** 아래에서 **Rule State(**규칙 상태**)**를 클릭하고 드롭다운 목록에서 `Generate Events(`이벤트 생성`)`를 클릭한 다음 **OK(**확인**)**를 클릭합니다.
  - **Rule Configuration(**규칙 구성**)** 아래에서 **Comment(**코멘트**)**를 클릭하고 필터링할 코멘트 텍스트 문자열을 입력한 다음 **OK(**확인**)**를 클릭할 수 있습니다.
  - **Category(**카테고리**)**에서 시스템이 인수 값으로 사용하는 **app-detect**를 클릭할 수 있습니다.
- 키워드를 확장하고 인수 값을 클릭합니다. 예를 들어 **Rule State(**규칙 상태**)**를 확장하고 **Generate Events(**이벤트 생성**)**를 클릭합니다.

침입 규칙 상태

침입 규칙 상태를 통해 개별 침입 정책 내에서 규칙을 활성화하거나 비활성화할 수 있을 뿐 아니라 모니터링된 조건이 규칙을 트리거하는 경우, 시스템이 수행하는 작업을 지정할 수도 있습니다.

Talos 인텔리전스 그룹는 각 기본 정책에서 각 침입 및 전처리기 규칙의 기본 상태를 설정합니다. 예를 들어, 규칙은 Security Over Connectivity(연결성에 우선하는 보안) 기본 정책에서 활성화되며 Connectivity Over Security(보안에 우선하는 연결성) 기본 정책에서는 비활성화됩니다. Talos에서는 때때로 규칙 업데이트를 사용하여 기본 정책에 있는 하나 이상의 규칙의 기본 상태를 변경합니다. 규칙 업데이트가 기반 정책을 업데이트하도록 허용하면, 정책을 생성하기 위해 사용한 기본 정책(또는 기반으로 하는 기본 정책)에서 기본 상태가 변경될 때 정책에 있는 규칙의 기본 상태를 변경하는 것도 허용됩니다. 그러나 규칙 상태를 변경한 경우 규칙 업데이트가 변경 사항을 재정의하지 않습니다.

침입 규칙을 생성하면 침입 정책은 정책 생성에 사용되는 기본 정책에 있는 규칙의 기본 상태를 상속합니다.

침입 규칙 상태 옵션

침입 정책에서 규칙의 상태를 다음 값으로 설정할 수 있습니다.

이벤트 생성

시스템이 일치하는 트래픽을 찾으면 특정 침입 시도를 탐지하고 침입 이벤트를 생성하도록 하려는 경우에 설정합니다. 악의적인 패킷이 네트워크를 이동하여 규칙을 트리거하면 규칙이 목적지로 전송되고 시스템이 침입 이벤트를 생성합니다. 악의적인 패킷이 대상에 도달하지만 이벤트 로깅을 통해 알림이 전송됩니다.

이벤트 삭제 및 생성

시스템이 일치하는 트래픽을 찾으면 특정 침입 이벤트를 탐지하고, 공격을 포함하는 패킷을 삭제하고, 침입 이벤트를 생성하도록 하려는 경우에 설정합니다. 악성 패킷은 대상에 도달하지 못하며 이벤트 로깅을 통해 알림이 전송됩니다.

디바이스 인라인 인터페이스 집합이 탭 모드인 구축을 포함한 패시브 구축. 시스템에서 패킷을 삭제하려면 침입 정책에서 **Drop when Inline(**인라인 시 삭제**)**를 활성화(기본 설정)하고 디바이스 인라인으로 구축해야 합니다.

Disable(비활성화**)**

시스템이 일치하는 트래픽을 평가하지 않도록 하려면 설정합니다.

참고 **Generate Events(**이벤트 생성**)** 또는 **Drop and Generate Events(**이벤트 삭제 및 생성**)** 옵션을 선택하면 규칙이 활성화됩니다. **Disable(**비활성화**)**를 선택하면 규칙이 비활성화됩니다.

Cisco는 침입 정책 내 침입 규칙을 모두 활성화하지 않을 것을 강력히 권장합니다. 모든 규칙이 활성화될 경우 관리되는 디바이스의 성능이 저하될 수 있습니다. 대신 네트워크 환경과 가능한 한 일치하도록 규칙 설정을 조정하십시오.

침입 규칙 상태 설정

침입 규칙 상태는 정책별로 다릅니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

팁 이 페이지에는 활성화된 총 규칙 수, Generate Events(이벤트 생성)로 설정된 활성화된 총 규칙 수, Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 총 수가 표시됩니다. 또한 수동 배포에서는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙만 이벤트를 생성한다는 점에 유의하십시오.

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 규칙 상태를 설정할 규칙을 선택합니다.

단계 **5** 다음 중 하나를 선택합니다.

- **Rule State(**규칙 상태**)** > **Generate Events(**이벤트 생성**)**
- **Rule State(**규칙 상태**)** > **Drop and Generate Events(**이벤트 삭제 및 생성**)**
- **Rule State(**규칙 상태**)** > **Disable(**비활성화**)**

단계 **6** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

침입 정책의 침입 이벤트 알림 필터

침입 이벤트의 중요성은 발생 빈도 또는 소스/대상 IP 주소를 기준으로 결정될 수 있습니다. 어떤 경우에는 특정 횟수가 발생할 때까지 이벤트에 대해 신경 쓰지 않아도 됩니다. 예를 들어, 어떤 사용자가 서버에 로그인을 시도하는 경우 특정 횟수만큼 실패할 때까지는 염려하지 않아도 됩니다. 다른 경우에는 소수의 발생 상황만 확인해도 광범위한 문제의 존재 여부를 파악할 수 있습니다. 예를 들어 웹 서버에 대해 DoS 공격이 시작된 경우, 상황을 해결해야 하는지를 파악하려면 침입 이벤트의 발생 상황을 몇 번만 확인해보면 됩니다. 동일한 이벤트를 수백 번 확인하면 시스템에 부담을 줄 뿐입니다.

침입 이벤트 임계값

지정된 기간 내 이벤트 생성 횟수를 기반으로 시스템이 침입 이벤트를 로깅 및 표시하는 횟수를 제한하도록 침입 정책당 개별 규칙에 대한 임계값을 설정할 수 있습니다. 이를 통해 많은 수의 동일한 이벤트로 인해 마비되는 것을 방지할 수 있습니다. 공유 개체 규칙, 표준 텍스트 규칙 또는 전처리기 규칙별 임계값을 설정할 수 있습니다.

침입 이벤트 임계값 설정

임계값을 설정하려면 먼저 임계값 설정 유형을 지정합니다.

표 *6:* 임계값 설정 옵션

옵션	설명
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 10으로, 그리고 **Seconds(**초**)**는 60으로 설정하고 14개의 패킷이 규칙을 트리거하는 경우, 시스템은 동일한 시간(분) 내 발생한 첫 10개의 패킷을 표시한 후 규칙의 이벤트 로깅을 중단합니다.
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. 카운터가 33초에 0으로 재설정되어 있기 때문에 시스템은 다른 이벤트를 로깅합니다.
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, 다음과 같이 이벤트가 계산됩니다. • 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).

다음으로 이벤트 임계값이 소스 IP 주소별로 계산되는지 대상 IP 주소별로 계산되는지 결정하는 추적을 지정합니다.

표 *7:* 임계값 설정 ***IP*** 옵션

옵션	설명
소스	소스 IP 주소당 이벤트 인스턴스 수를 계산합니다.
대상	대상 IP 주소당 인스턴스 이벤트 수를 계산합니다.

마지막으로, 임계값을 정의하는 기간 및 인스턴스 수를 지정합니다.

표 *8:* 임계값 설정 인스턴스/시간 옵션

옵션	설명
개수	임계값 충족에 필요한 추적 IP 주소당 지정된 기간의 이벤트 인스턴스 수.

옵션	설명
시간(초)	카운트가 재설정되기 전에 경과된 시간(초). 임계값 유형을 **limit(**제한**)**로, 추적을 **Source IP(**소스 **IP)**로, **count(**카운트**)**를 `10`으로, 그리고 **seconds(**초**)**를 `10`으로 설정한 경우, 시스템은 주어진 소스 포트에서 10초 안에 발생한 첫 10개의 이벤트를 로깅하고 표시합니다. 첫 10초 안에 7개의 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.

침입 이벤트 임계값 설정을 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 삭제와 조합하여 사용할 수도 있습니다.

팁 침입 이벤트의 패킷 보기 내에서 임계값을 추가할 수도 있습니다.

관련 항목

detection_filter 키워드

침입 이벤트 임계값 추가 및 수정

침입 정책에서 하나 이상의 특정 규칙의 임계값을 설정할 수 있습니다. 별도로 또는 동시에 기존 임계값 설정을 수정할 수도 있습니다. 각각에 대해 단일 임계값을 설정할 수 있습니다. 임계값을 추가하여 규칙에 대한 기존 임계값을 덮어씁니다.

또한 침입 정책에 연결된 모든 규칙 및 전처리기 생성 이벤트에 기본적으로 적용되는 전역 임계값을 수정할 수 있습니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없으면 필드를 비워 둡니다.

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

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색 창에서 **Policy Information(**정책 정보**)** 바로 아래의 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 임계값을 설정할 규칙을 찾습니다.

단계 **5** **Event Filtering(**이벤트 필터링**)** > **Threshold(**임계값**)**를 선택합니다.

단계 **6** **Type(**유형**)** 드롭다운 목록에서 임계값 유형을 선택합니다.

단계 **7** **Track By(**추적 기준**)** 드롭다운 목록에서 이벤트 인스턴스를 **Source(**소스**)** IP 주소로 추적할지 **Destination(**대상**)** IP 주소로 추적할지 선택합니다.

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

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

단계 **10** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우, 필터 위의 숫자는 이벤트 필터의 수를 나타냅니다.

단계 **11** 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 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

전역 규칙 임계값 기본 사항

침입 이벤트 임계값 보기 및 삭제

규칙의 기존 임계값 설정을 보거나 삭제하고자 할 수 있습니다. 임계값에 대해 구성된 설정을 표시하여 시스템에 적절한지 확인하려면 Rules Details(규칙 세부 사항) 보기를 사용할 수 있습니다. 적절하지 않은 경우 새 임계값을 추가하여 기존 값을 덮어쓸 수 있습니다.

또한 침입 정책이 로깅한 모든 규칙 및 전처리기 생성 이벤트에 기본적으로 적용되는 전역 임계값을 수정할 수 있습니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색 창에서 **Policy Information(**정책 정보**)** 바로 아래의 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 보거나 삭제할 구성된 임계값이 있는 규칙을 선택합니다.

단계 **5** 선택한 각 규칙에 대한 임계값을 제거하려면 **Event Filtering(**이벤트 필터링**)** > **Remove Thresholds(**임계값 제거**)**를 선택합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** 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 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

전역 규칙 임계값 기본 사항

침입 정책 삭제 구성

특정 IP 주소 또는 특정 범위의 IP 주소가 특정 규칙 또는 전처리기를 트리거하면 침입 이벤트 알림을 삭제할 수 있습니다. 이렇게 하면 오탐을 없애는 데 도움이 됩니다. 예를 들어 특정 익스플로잇처럼 보이는 패킷을 전송하는 메일 서버가 있는 경우, 메일 서버에 의해 이벤트가 트리거될 때 해당 이벤트에 대한 이벤트 알림을 억제할 수 있습니다. 규칙은 모든 패킷에 대해 트리거되지만, 기준에 맞는 공격에 대한 이벤트만 표시됩니다.

침입 정책 삭제 유형

침입 이벤트 억제를 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 임계값 설정과 조합하여 사용할 수도 있습니다.

팁 침입 이벤트의 패킷 보기 내에서 억제를 추가할 수도 있습니다. 침입 규칙 편집기 페이지(**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**) 및 침입 이벤트 페이지(이벤트가 침입 규칙에 의해 트리거된 경우)에서 마우스 오른쪽 버튼을 클릭하면 나타나는 컨텍스트 메뉴를 사용하여 억제 설정에 액세스할 수도 있습니다.

관련 항목

detection_filter 키워드

침입 규칙에 대한 침입 이벤트 삭제

침입 정책에서 규칙에 대한 침입 이벤트 알림을 억제할 수 있습니다. 규칙에 대한 알림이 삭제되면, 규칙은 트리거되지만 이벤트는 생성되지 않습니다. 규칙에 하나 이상의 삭제를 설정할 수 있습니다. 나열된 첫 번째 삭제가 가장 높은 우선 순위를 갖습니다. 2개의 억제가 충돌하면 첫 번째 억제의 작업이 수행됩니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 이를 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 억제 조건을 구성할 하나 이상의 규칙을 선택합니다.

단계 **5** **Event Filtering(**이벤트 필터링**)** > **Suppression(**억제**)**을 선택합니다.

단계 **6** **Suppression Type(**억제 유형**)**을 선택합니다.

단계 **7** 억제 유형으로 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택한 경우, **Network(**네트워크**)** 필드에 소스 또는 대상 IP 주소로 지정할 IP 주소, 주소 블록 또는 변수를 입력하거나 이러한 항목의 조합을 포함하는 쉼표로 구분된 목록을 입력합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

팁 시스템은 억제된 규칙 옆의 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우, 필터 위의 숫자는 이벤트 필터의 수를 나타냅니다.

단계 **9** 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 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

삭제 조건 보기 및 삭제

기존 삭제 조건을 보거나 삭제하려고 할 수 있습니다. 예를 들어, 메일 서버는 일반적으로 익스플로잇처럼 보이는 패킷을 전송하므로 메일 서버 IP 주소에서 시작되는 패킷에 대한 이벤트 알림을 억제할 수 있습니다. 그리고 해당 메일 서버를 폐쇄하고 다른 호스트에 IP 주소를 다시 할당할 경우, 해당 소스 IP 주소에 대한 삭제 조건을 삭제해야 합니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 억제를 보거나 삭제할 규칙을 선택합니다.

단계 **5** 다음 옵션을 이용할 수 있습니다.

- 규칙에 대한 모든 억제를 제거하려면 **Event Filtering(**이벤트 필터링**)** > **Remove Suppressions(**억제 제거**)**를 선택합니다.
- 특정 억제 설정을 제거하려면 규칙을 클릭한 다음 **Show details(**세부 정보 보기**)**를 클릭합니다. 삭제 설정을 확장하고 제거할 삭제 설정 옆에 있는 **Delete(**삭제**)**를 클릭합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** 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 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

동적 침입 규칙 상태

속도 기반 공격은 네트워크 또는 호스트에 과도한 트래픽을 전송하여 네트워크 또는 호스트를 마비시켜 느려지게 하거나 적법한 요청을 거부하도록 시도하는 것입니다. 속도 기반 차단을 사용하여 특정 규칙에 대한 과도한 규칙 일치에 대응하여 규칙 작업을 변경할 수 있습니다.

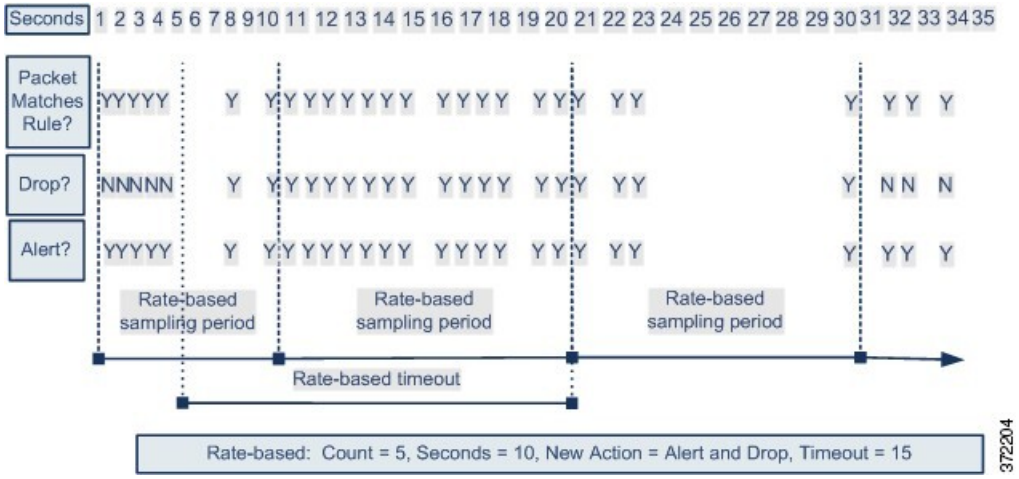
지정된 기간에 규칙에 대해 너무 많은 일치가 발생할 때 이를 탐지하는 속도 기반 필터를 포함하도록 침입 정책을 구성할 수 있습니다. 인라인으로 구축된 매니지드 디바이스에서 이 기능을 사용하여 지정된 시간 동안 속도 기반 공격을 차단한 후 규칙 일치를 통해 이벤트만 생성하고 트래픽을 삭제하지는 않는 규칙 상태로 돌아갈 수 있습니다.

속도 기반 공격 방지는 비정상적 트래픽 패턴을 식별하고 해당 트래픽이 정당한 요청에 미치는 영향을 최소화하려 시도합니다. 특정 대상 IP 주소로 이동하거나 특정 소스 IP 주소에서 오는 트래픽에서의 과도한 규칙 일치를 식별할 수 있습니다. 탐지된 모든 트래픽에서 특정 규칙에 대해 발생하는 과도한 일치에 대응할 수도 있습니다.

규칙과 일치하는 모든 패킷을 삭제하지는 않을 것이지만 지정된 시간에 특정 일치 속도가 발생하면 규칙과 일치하는 패킷을 삭제하려는 경우, 규칙을 Drop and Generate Events(이벤트 삭제 및 생성) 상태로 설정하지 않을 수 있습니다. 동적 규칙 상태를 사용하면 규칙에 대한 작업에서 변경을 트리거하는 속도, 속도가 충족될 때 작업에서 변경해야 할 내용, 새 작업의 지속 시간 등을 구성할 수 있습니다.

다음 다이어그램은 공격자가 호스트에 액세스하기 위해 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지가 구성된 규칙을 트리거합니다. 속도 기반 설정은 10초 범위 안에 규칙 일치가 다섯 번 발생하면 규칙 속성을 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 새로운 규칙 속성은 15초 후 시간 초과됩니다.

시간이 초과되더라도 패킷은 이어지는 속도 기반 샘플링 기간 내에 여전히 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 Generate Events(이벤트 생성)로 돌아갑니다.



동적 침입 규칙 상태 설정

침입 정책에서 침입 또는 전처리기 규칙에 대해 속도 기반 필터를 구성할 수 있습니다. 속도 기반 필터에는 다음과 같은 3개의 구성 요소가 포함되어 있습니다.

- 특정 초 이내 규칙 일치의 계수로 구성한 규칙 일치 비율
- 속도를 초과할 경우 다음 3개의 사용 가능한 작업과 함께 취할 새로운 작업: Generate Events(이벤트 생성), Drop and Generate Events(이벤트 삭제 및 생성), Disable(비활성화)
- 시간 제한 값으로 설정한 작업 기간

시작한 경우, 속도가 해당 기간 동안 구성된 속도까지 떨어지더라도 시간 제한에 도달할 때까지 새로운 작업이 발생한다는 점에 유의하십시오. 시간 제한에 도달하면, 속도가 임계값 아래로 떨어진 경우, 규칙 작업은 규칙에 처음 설정된 작업으로 돌아갑니다.

인라인 구축에서 속도 기반 공격 차단을 구성하여 일시적으로 또는 영구적으로 공격을 차단할 수 있습니다. 속도 기반 구성 없이 Generate Events(이벤트 생성)로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙에 대한 패킷을 삭제하지 않습니다. 하지만 속도 기반 기준이 구성되어 있는 규칙이

공격 트래픽과 일치하는 경우, 해당 규칙이 처음에는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있지 않더라도 속도 작업은 속도 작업이 활성화된 기간 동안 패킷이 삭제되도록 할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나 비활성화된 규칙에 일치하는 트래픽을 삭제할 수 없습니다.

동일한 규칙에서 다중 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 나열된 첫 번째 필터의 우선 순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌하면 첫 번째 속도 기반 필터의 작업이 수행됩니다.

규칙 페이지에서 동적 규칙 상태 설정

규칙에 하나 이상의 동적 규칙 상태를 설정할 수 있습니다. 나열된 첫 번째 동적 규칙 상태의 우선 순위가 가장 높습니다. 2개의 동적 규칙 상태가 충돌하면 첫 번째 상태의 작업이 수행됩니다.

동적 규칙 상태는 정책에 따라 다릅니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없으면 필드를 지웁니다.

참고 동적 규칙 상태는 비활성화된 규칙을 활성화하거나, 비활성화된 규칙과 일치하는 트래픽을 삭제할 수 없습니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색 창에서 **Policy Information(**정책 정보**)** 바로 아래의 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 동적 규칙 상태를 추가할 규칙을 선택합니다.

단계 **5** **Dynamic State(**동적 상태**)** > **Add Rate-Based Rule State(**속도 기반 규칙 상태 추가**)**를 선택합니다.

단계 **6** **Track By(**추적 기준**)** 드롭다운 목록에서 값을 선택합니다.

단계 **7** **Track By**를 **Source** 또는 **Destination**으로 설정하는 경우 추적하려는 각 호스트의 주소를 **Network** 필드에 입력합니다. 단일 IP 주소, 주소 블록, 변수 또는 이들 조합으로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **8** 공격 속도를 설정하려면 **Rate(**속도**)** 옆에 기간당 규칙 일치 수를 지정합니다.

- **Count(**카운트**)** 필드에 값을 입력합니다.
- **Seconds(**초**)** 필드에 값을 입력합니다.

단계 **9** **New State(**새로운 상태**)** 드롭다운 목록에서 조건이 충족되면 수행할 새로운 작업을 지정합니다.

단계 **10** **Timeout(**시간 제한**)** 필드에 값을 입력합니다.

시간 제한이 발생한 후, 규칙은 원래 상태로 돌아갑니다. 새 작업의 시간 초과를 금지하려면 0을 지정하거나 **Timeout** 필드를 비워둡니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Dynamic State(동적 상태) 열의 규칙 옆에 **Dynamic State(**동적 상태**)**를 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가한 경우, 필터 위의 숫자는 필터 수를 나타냅니다.

팁 규칙 집합에 대한 모든 동적 규칙 설정을 삭제하려면 Rules(규칙) 페이지에서 규칙을 선택한 후 **Dynamic State(**동적 상태**)** > **Remove Rate-Based States(**속도 기반 상태 제거**)**를 선택합니다. 규칙을 선택하고 **Show details(**세부 정보 보기**)**를 클릭한 후 제거할 속도 기반 필터 옆에 있는 **Delete(**삭제**)**를 클릭하여 규칙의 규칙 세부 정보에서 개별 속도 기반 규칙 상태 필터를 삭제할 수도 있습니다.

단계 **12** 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 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

침입 규칙 설명 추가

침입 정책에서 규칙에 코멘트를 추가할 수 있습니다. 이렇게 추가되는 코멘트는 해당 정책에 한정됩니다. 즉, 한 침입 정책에서 규칙에 추가하는 코멘트는 다른 침입 정책에서는 표시되지 않습니다. 추가하는 코멘트는 해당 침입 정책 Rules(규칙) 페이지의 Rule Details(규칙 세부 사항) 보기에서 볼 수 있습니다.

코멘트가 포함된 침입 정책 변경 사항을 커밋한 후에는 또한 규칙 Edit(수정) 페이지에서 **Rule Comment(**규칙 코멘트**)**를 클릭하여 코멘트를 볼 수 있습니다.

프로시저

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

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

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 코멘트를 추가하고자 하는 규칙을 선택합니다.

단계 **5** **Comments(**코멘트**)** > **Add Rule Comment(**규칙 코멘트 추가**)**를 선택합니다.

단계 **6** **Comments(**코멘트**)** 필드에 규칙 코멘트를 입력합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Comments(코멘트) 열의 규칙 옆에 **Comment(**코멘트**)** ( )를 표시합니다. 규칙에 여러 코멘트를 추가하는 경우, 코멘트 위의 숫자는 코멘트 수를 나타냅니다.

단계 **8** 원하는 경우, 코멘트 옆의 **Delete(**삭제**)**를 클릭하여 규칙 코멘트를 삭제합니다.

커밋되지 않은 침입 정책 변경 사항과 함께 코멘트가 캐시된 경우에만 코멘트를 삭제할 수 있습니다. 침입 정책 변경 사항이 커밋되면 규칙 코멘트는 영구적입니다.

단계 **9** 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 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.