침입 정책

다음 주제에서는 침입 정책 및 밀접하게 연관된 NAP(네트워크 분석 정책)에 대해 설명합니다. 침입 정책에는 위협에 대한 트래픽을 확인하고 공격으로 표시되는 트래픽을 차단하는 규칙이 포함됩니다. 네트워크 분석 정책은 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비하는 트래픽 전처리를 제어합니다.

전처리 및 침입 검사는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검사하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다.

침입 및 네트워크 분석 정책 정보

네트워크 분석 및 침입 정책은 침입 위협을 탐지 및 방지하기 위해 함께 작동합니다.

- NAP(네트워크 분석 정책)는 트래픽을 디코딩하고 전처리하는 방법을 제어합니다. 이 정책의 목적은 향후 평가를 위함이며, 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽의 경우 유효합니다.
- 침입 정책은 침입 및 전처리 규칙(침입 규칙으로 총칭함)을 사용하여 패턴 기반의 공격에 대한 디코딩된 패킷을 검사합니다. 규칙은 위협 트래픽을 방지(삭제)하고 이벤트를 생성하거나, 단순히 이를 탐지(알림)만 하고 이벤트를 생성할 수 있습니다.

시스템이 트래픽을 분석하기 때문에, 네트워크 분석 디코딩 및 전처리 단계는 침입 방지 단계보다 이전에 또는 별도로 발생합니다. 네트워크 분석 및 침입 정책은 폭넓고 심층적인 패킷 검사를 제공합니

다. 이 둘을 함께 사용하면 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성을 위협할 수 있는 네트워크 트래픽을 탐지하고 알리고 방지할 수 있습니다.

시스템 정의 네트워크 분석 및 침입 정책

시스템에는 상호 보완하고 함께 작동하는 동일한 이름의 네트워크 분석 및 침입 정책 쌍이 여러 개 포함되어 있습니다. 예를 들어, "Balanced Security and Connectivity(보안과 연결의 균형 유지)"라는 이름으로 NAP 및 침입 정책이 모두 있으며 이 두 정책은 함께 사용해야 합니다. 시스템 제공 정책은 Cisco Talos Intelligence Group(Talos)에서 구성합니다. Talos에서는 이러한 정책에 대해 침입 및 전처리기 규칙 상태를 설정하고 전처리기 및 다른 고급 설정에 대한 초기 구성을 제공합니다.

새로운 취약성이 알려지면 Talos에서 침입 규칙 업데이트를 릴리스합니다. 이 규칙 업데이트는 모든 시스템 제공 네트워크 분석 또는 침입 정책을 수정할 수 있고 새롭게 업데이트된 침입 규칙 및 전처리기 규칙, 기존 규칙을 위한 수정된 상태, 그리고 수정된 기본 정책 설정을 제공할 수 있습니다. 규칙 업데이트는 또한 시스템 제공 정책에서 규칙을 삭제할 수 있고, 새로운 규칙 카테고리를 제공할 수 있으며, 기본 변수 집합을 수정할 수 있습니다.

규칙 데이터베이스를 수동으로 업데이트하거나 정기 업데이트 일정을 구성할 수 있습니다. 업데이트를 적용하려면 업데이트를 구축해야 합니다. 시스템 데이터베이스 업데이트에 대한 자세한 내용은 시스템 데이터베이스 업데이트를 참조하십시오.

시스템 제공 정책은 다음과 같습니다.

Balanced Security and Connectivity(보안과 연결의 균형 유지**)** 네트워크 분석 및 침입 정책

이 정책은 속도 및 탐지 모두에 구축됩니다. 두 정책을 함께 사용하는 것은 대부분의 네트워크 및 구축 유형에 대해 좋은 시작점이 됩니다. 시스템에서는 Balanced Security and Connectivity(보안과 연결의 균형 유지) 네트워크 분석 정책을 기본값으로 사용합니다.

Connectivity Over Security(연결이 보안에 우선함**)** 네트워크 분석 및 침입 정책

이러한 정책은 연결(모든 리소스에 접근할 수 있는 기능)이 네트워크 인프라 보안보다 우선하는 네트워크에 구축됩니다. 침입 정책은 Security Over Connectivity(보안이 연결에 우선함)에서 활성화된 것보다 훨씬 더 적은 규칙을 활성화합니다. 트래픽을 차단하는 가장 중요한 규칙만 사용 설정됩니다.

Security Over Connectivity(보안이 연결에 우선함**)** 네트워크 분석 및 침입 정책

이러한 정책은 네트워크 인프라 보안이 사용자 편의보다 우선하는 네트워크에 구축됩니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다.

Maximum Detection(최대 탐지**)** 네트워크 분석 및 침입 정책

이러한 정책은 Security over Connectivity(연결보다 보안 우선) 정책에서보다 네트워크 인프라 보안이 강조되는 네트워크에 구축되며, 운영에 더 큰 영향을 미칠 수 있습니다. 예를 들어 이 침입 정책에서는 악성코드, 익스플로잇 킷, 오래된 일반적인 취약점, 통제되지 않은 알려진 익스플로잇 등 다수의 위협 범주에서 규칙을 활성화합니다.

검사 모드: 방지 및 탐지

기본적으로 모든 침입 정책은 Prevention(차단) 모드에서 작동하여 IPS(침입 방지 시스템)를 구현합니다. Prevention(차단) 검사 모드에서 연결이 트래픽을 삭제하는 작업을 수행하는 침입 규칙과 일치하는 경우 연결이 능동적으로 차단됩니다.

대신 네트워크에서 침입 정책의 영향을 테스트하려는 경우, 모드를 IDS(침입 탐지 시스템)를 구현하는 모드를 Detection(탐지)로 변경할 수 있습니다. 이 검사 모드에서 삭제 규칙은 일치하는 연결에 대한 알림을 받는 알림 규칙처럼 처리되지만, 작업 결과는 Would Have Blocked(차단되었을 수 있음)가 되고 연결은 실제로 차단되지 않습니다.

침입 정책에 따라 검사 모드를 변경하면 차단 및 탐지를 혼합하여 사용할 수 있습니다.

Snort 3 네트워크 분석 정책(NAP)에도 검사 모드가 있습니다. 침입 정책과 달리 NAP 정책은 전역 정책이므로 모든 NAP 처리를 방지 또는 탐지 모드에서 실행해야 합니다. 침입 정책에 사용하는 것과 동일한 모드를 사용해야 합니다. 방지 및 탐지 정책이 혼합된 경우 가장 제한적인 침입 정책과 일치하도록 Prevention(방지)을 선택합니다.

침입 및 전처리기 규칙

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.

시스템에는 Cisco Talos Intelligence Group(Talos)가 생성한 다음 유형의 규칙이 포함됩니다.

- 침입 규칙(공유 개체 규칙 및 표준 텍스트 규칙으로 세분화됨)
- 전처리기 규칙(네트워크 분석 정책에서 전처리기 및 패킷 디코더 탐지 옵션과 관련된 규칙). 대부분의 전처리기 규칙은 기본적으로 비활성화되어 있습니다.

다음 주제에서는 침입 규칙에 대해 자세히 설명합니다.

침입 규칙 특성

침입 정책을 확인하면 위협을 식별하는 데 사용할 수 있는 모든 침입 규칙 목록이 표시됩니다.

각 정책에 대한 규칙 목록은 동일합니다. 차이점은 각 규칙에 대해 구성된 작업에 있습니다. 30,000개 이상의 규칙이 있으므로, 목록을 스크롤하는 데 시간이 걸립니다. 목록을 스크롤하면 규칙이 표시됩니다.

다음은 각 규칙을 정의하는 특성입니다.

> (서명 설명)

왼쪽 열의 > 버튼을 클릭하여 서명 설명을 엽니다. 설명은 트래픽을 규칙과 일치시키기 위해 Snort 검사 엔진에서 사용하는 실제 코드입니다. 코드에 대한 설명은 이 문서의 범위를 벗어나지만 *Management Center* 컨피그레이션 가이드에는 자세히 설명되어 있습니다. http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html에서 해당하는 소프트웨어 버전의 문서를 선택하십시오. 침입 규칙 수정에 대한 정보를 찾아봅니다.

서명에는 특정 항목에 대한 변수가 포함됩니다. 자세한 내용은 기본 침입 변수 집합, 4 페이지를 참고하십시오.

GID

생성기 식별자(ID). 이 번호는 어떤 시스템 구성 요소가 규칙을 평가하고 이벤트를 생성하는지 나타냅니다. 1은 표준 텍스트 침입 규칙을 나타내고, 3은 공유 개체 침입 규칙을 나타냅니다. (이러한 규칙 유형의 차이점은 device manager 사용자에게 크게 중요하지 않습니다.) 이러한 규칙은 침입 정책을 구성할 때 관심을 가져야 할 주요 규칙입니다. 기타 GID에 대한 자세한 내용은 생성기 식별자, 5 페이지를 참조하십시오.

SID

SID(Snort 식별자)는 서명 ID라고도 합니다. 1000000보다 낮은 Snort ID는 Cisco Talos Intelligence Group(Talos)에서 생성했습니다.

Action(작업)

선택한 침입 정책에 있는 이 규칙의 상태입니다. 규칙마다 "(Default(기본값))"가 작업에 추가되며, 이는 이 정책에 있는 규칙의 기본 작업입니다. 기본 설정으로 규칙을 되돌리려면 이 작업을 선택합니다. 가능한 작업은 다음과 같습니다.

- **Alert(알림)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
- **Drop(삭제)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하고 연결도 삭제합니다.
- **Disabled(비활성화됨)** — 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.

Status(상태)

Snort 2 규칙의 경우 상태는 별도의 열에 표시됩니다. 규칙에 대한 기본 작업을 변경할 경우, 이 열에 "Overridden(재정의됨)"이 표시됩니다. 그렇지 않을 경우, 열이 비어 있습니다.

Snort 3 규칙의 경우 "Overridden(재정의됨)" 상태를 변경했으면 Action 특성의 맨 아래에 표시됩니다.

Message(메시지)

이는 규칙의 이름이며, 해당 규칙으로 트리거된 이벤트에도 표시됩니다. 메시지는 일반적으로 서명이 일치하는 위협을 식별합니다. 각 위협에 대한 자세한 내용은 인터넷을 검색하여 참조할 수 있습니다.

기본 침입 변수 집합

침입 규칙 서명에는 특정 항목에 대한 변수가 포함됩니다. 아래에는 변수의 기본값이 나와 있으며, $HOME_NET 및 $EXTERNAL_NET이 가장 일반적으로 사용되는 변수입니다. 프로토콜은 포트 번호와 별도로 지정되므로, 포트 변수는 번호로만 존재합니다.

- $DNS_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $EXTERNAL_NET = 임의의 IP 주소

- $FILE_DATA_PORTS = $HTTP_PORTS, 143, 110
- $FTP_PORTS = 21, 2100, 3535
- $GTP_PORTS = 3386, 2123, 2152
- $HOME_NET = 임의의 IP 주소
- $HTTP_PORTS = 144개의 포트 번호가 지정됨: 36, 80-90, 311, 383, 443, 555, 591, 593, 631, 666, 801, 808, 818, 901, 972, 1158, 1212, 1220, 1414, 1422, 1533, 1741, 1830, 1942, 2231, 2301, 2381, 2578, 2809, 2980, 3029, 3037, 3057, 3128, 3443, 3507, 3702, 4000, 4343, 4848, 5000, 5117, 5222, 5250, 5450, 5600, 5814, 6080, 6173, 6767, 6988, 7000, 7001, 7005, 7071, 7080, 7144, 7145, 7510, 7770, 7777-7779, 8000, 8001, 8008, 8014, 8015, 8020, 8028, 8040, 8060, 8080-8082, 8085, 8088, 8118, 8123, 8161, 8180-8182, 8222, 8243, 8280, 8300, 8333, 8344, 8400, 8443, 8500, 8509, 8787, 8800, 8888, 8899, 8983, 9000, 9002, 9060, 9080, 9090, 9091, 9111, 9290, 9443, 9447, 9710, 9788, 9999, 10000, 11371, 12601, 13014, 15489, 19980, 23472, 29991, 33300, 34412, 34443, 34444, 40007, 41080, 44449, 50000, 50002, 51423, 53331, 55252, 55555, 56712
- $HTTP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $ORACLE_PORTS = 임의로 지정됨
- $SHELLCODE_PORTS = 180
- $SIP_PORTS = 5060, 5061, 5600
- $SIP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SMTP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SNMP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SQL_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SSH_PORTS = 22
- $SSH_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $TELNET_SERVERS = $HOME_NET(임의의 IP 주소 의미)

생성기 식별자

GID(생성기 식별자)는 침입 규칙을 평가하고 이벤트를 생성하는 하위 시스템을 식별합니다. 표준 텍스트 침입 규칙에는 생성기 ID 1이 있으며 공유 개체 침입 규칙에는 생성기 ID 3이 있습니다. 또한, 다양한 전처리기에 대한 여러 가지 규칙 집합이 있습니다. 다음 표에서는 GID에 대해 설명합니다.

표 ***1:*** 생성기 ***ID***

ID	**Component(**구성 요소**)**
1	표준 텍스트 규칙

ID	Component(구성 요소)
2	태그가 지정된 패킷 (태그가 지정된 세션에서 패킷을 생성하는 태그 생성기에 대한 규칙)
3	공유 개체 규칙
102	HTTP 디코더
105	Back Orifice 탐지기
106	RPC 디코더
116	패킷 디코더
119, 120	HTTP 검사 전처리기 (GID 120 규칙은 서버별 HTTP 트래픽과 관련이 있음)
122	포트스캔 탐지기
123	IP 조각 모음기
124	SMTP 디코더 (SMTP 동사를 대상으로 익스플로잇)
125	FTP 디코더
126	텔넷 디코더
128	SSH 전처리기
129	스트림 전처리기
131	DNS 전처리기
133	DCE/RPC 전처리기
134	규칙 레이턴시, 패킷 레이턴시 (규칙 레이턴시가 침입 규칙의 그룹을 일시 중지(SID 1)하거나 다시 활성화(SID 2)하는 경우 또는 패킷 레이턴시 임계값이 초과되어 시스템이 패킷 검사를 중지하는 경우(SID 3), 이러한 규칙에 대한 이벤트가 생성됨)
135	속도 기반 공격 탐지기 (네트워크의 호스트에 대한 과도한 연결)
137	SSL 전처리기
138, 139	민감한 데이터 전처리기

ID	Component(구성 요소)
140	SIP 전처리기
141	IMAP 전처리기
142	POP 전처리기
143	GTP 전처리기
144	Modbus 전처리기
145	DNP3 전처리기

네트워크 분석 정책

네트워크 분석 정책은 트래픽 전처리를 제어합니다. 전처리기는 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비합니다. 네트워크 분석 관련 전처리는 보안 인텔리전스 삭제 및 SSL 암호 해독 후, 그리고 액세스 제어 및 침입/파일 검사 전에 발생합니다.

기본적으로 시스템에서는 Balanced Security and Connectivity(보안과 연결의 균형 유지) 네트워크 분석 정책을 사용하여 액세스 제어 정책에 의해 처리된 모든 트래픽을 전처리합니다. 그러나 액세스 제어 규칙에 대해 침입 정책을 구성하는 경우 시스템에서는 적용된 가장 적극적인 침입 정책과 일치하는 네트워크 분석 정책을 사용합니다. 예를 들어 액세스 제어 규칙에서 Security over Connectivity(보안이 연결에 우선함) 및 Balanced(보안과 연결의 균형 유지) 정책을 모두 사용하는 경우 시스템에서는 모든 트래픽에 대해 Security over Connectivity(보안이 연결에 우선함) NAP를 사용합니다. Snort 3 맞춤형 침입 정책의 경우 이러한 할당은 침입 정책에 할당된 기본 템플릿 정책에 따라 수행됩니다.

Snort 3을 사용하는 경우 정책을 명시적으로 선택하고 선택적으로 설정을 사용자 지정할 수 있습니다. 침입 정책을 직접 사용하거나 사용자 지정 침입 정책의 기본 정책으로 사용하는 경우 디바이스를 통과하는 대부분의 트래픽에 사용하는 침입 정책과 일치하는 이름의 정책을 선택하는 것이 좋습니다. 그런 다음 검사 모드를 변경하거나 네트워크의 트래픽을 고려하여 특정 검사기 또는 바인더 설정을 조정할 수 있습니다.

또한 침입 정책에서 전처리기 규칙을 활성화했는지 여부도 고려하십시오. 전처리기가 필요한 규칙을 활성화하는 경우 NAP에서 해당 검사기를 활성화해야 합니다. 각 검사기에 대해 검사한 포트(바인더)를 포함하여 검사기의 속성을 조정하여 네트워크에 대한 검사기 동작을 사용자 지정할 수도 있습니다.

참고 Snort 2를 사용하는 경우 시스템은 액세스 제어 규칙에서 적용하는 가장 제한적인 침입 정책과 동일한 이름의 NAP 정책을 사용하며, 검사기 또는 바인더 설정을 편집할 수 없습니다.

침입 정책을 위한 라이선스 요건

액세스 제어 규칙에 침입 정책을 적용하려면 위협라이선스를 활성화해야 합니다. 라이선스 구성에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화를 참조하십시오.

네트워크 분석 정책의 경우 추가 라이선스가 필요하지 않습니다.

액세스 제어 규칙에서 침입 정책 적용

침입 정책을 네트워크 트래픽에 적용하려면 트래픽을 허용하는 액세스 제어 규칙 내에서 정책을 선택하고 침입 정책을 직접 할당하지는 마십시오.

서로 다른 침입 정책을 할당하여 보호 중인 네트워크의 상대적인 위험도를 기반으로 다양한 침입 보호 기능을 제공할 수 있습니다. 예를 들어, 내부 네트워크와 외부 네트워크 간의 트래픽에 대해서는 더 엄격한 Security over Connectivity(연결보다 보안 우선) 정책을 사용하는 반면, 내부 네트워크 간의 트래픽에 대해서는 덜 엄격한 Connectivity over Security(연결이 보안에 우선함) 정책을 적용할 수 있습니다.

모든 네트워크에 대해 동일한 정책을 사용하여 컨피그레이션을 간소화할 수도 있습니다. 예를 들어, Balanced Security and Connectivity(보안과 연결의 균형 유지) 정책은 연결에 지나치게 영향을 미치지 않고 우수한 보호 기능을 제공하도록 설계되었습니다.

프로시저

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

단계 **2** 트래픽을 허용하도록 새 규칙을 생성하거나 기존 규칙을 수정합니다.

기본 작업이 허용인 경우, 기본 작업에서 침입 정책을 지정할 수도 있습니다.

트래픽을 신뢰하거나 차단하는 규칙에는 침입 정책을 적용할 수 없습니다.

단계 **3** **Intrusion Policy(**침입 정책**)** 탭을 클릭합니다.

단계 **4** **Intrusion Policy(**침입 정책**)** > **On(**켜기**)**을 선택하고 일치하는 트래픽에서 사용할 침입 검사 정책을 선택합니다.

Snort 2와 Snort 3 간 전환

Snort는 제품에 대한 기본 검사 엔진입니다. Snort 버전을 자유롭게 전환할 수는 있지만, Snort 2.0의 일부 침입 규칙은 Snort 3.0에는 없을 수 있으며 그 반대의 경우도 마찬가지입니다. 이러한 규칙 중 하나에 대한 규칙 동작을 변경한 경우에는 해당 변경 사항이 유지되지 않습니다. 해당 변경 사항은 Snort 3으로 전환했다가 다시 Snort 2로 전환하거나 Snort 3으로 다시 전환하는 경우에는 유지되지 않습니다. 두 버전에 모두 있는 규칙의 규칙 동작에 대한 변경 사항은 유지됩니다. Snort 3과 Snort 2의 규칙

간 매핑은 일대일 또는 일대 다수가 될 수 있으므로 변경 사항을 가장 효과적으로 유지할 수 있습니다.

Snort 버전을 변경하는 경우 시스템에서는 자동 구축을 수행하여 변경을 구현합니다. 작업 목록에서 진행률을 확인할 수 있습니다. 작업은 'Snort 버전 변경' 및 '자동 구축-Snort 버전 전환'입니다. 새 버전을 시작할 수 있도록 Snort를 중지해야 하므로 일시적인 트래픽 손실이 발생합니다.

참고 Snort 버전을 전환하려고 하는데 스위치에 장애가 발생하면 취소할 수 없는 변경 사항을 보류하게 되며, 이후의 전환 시도는 허용되지 않습니다. 이 경우 API Explorer에서 사용할 수 있는 ToggleInspectionEngine API를 사용하여 스위치를 완료해야 합니다. bypassPendingChangeValidation 특성을 TRUE로 설정해야 합니다.

시작하기 전에

현재 어떤 Snort 버전이 활성화되어 있는지 확인하려면 이 절차를 사용하거나 **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다. 테이블 위의 **Snort Version(Snort** 버전**)** 라인을 찾습니다. 현재 버전은 전체 버전 번호의 첫 번째 번호입니다. 예를 들어 2.9.17-95는 Snort 2 버전입니다.

디바이스가 에어 갭(air-gapped) 네트워크에 있는 경우 전환하기 전에 새 버전의 최신 규칙 패키지를 수동으로 업로드하는 것이 좋습니다.

2.0으로 다운그레이드하는 경우, 생성한 맞춤형 침입 정책이 맞춤형 정책에 사용된 기본 정책으로 변환됩니다. 가능한 한 규칙 작업 재정의가 유지됩니다. 둘 이상의 맞춤형 정책이 동일한 기본 정책을 사용하는 경우, 대부분의 액세스 제어 정책에 사용되는 맞춤형 정책의 재정의는 유지되며 다른 맞춤형 정책의 재정의는 손실됩니다. 이러한 "중복" 정책을 사용하는 액세스 제어 규칙은 이제 가장 많이 사용되는 맞춤형 정책에서 생성된 기본 정책을 사용합니다. 모든 맞춤형 정책이 삭제됩니다. 나중에 가져올 수 있도록 맞춤형 정책을 유지하려는 경우 Snort 3으로 다시 전환한 후 threat defense API를 사용하여 컨피그레이션을 내보냅니다.

또한 2.0으로 다운그레이드하면 NAP 사용자 지정이 제거되고, 시스템은 액세스 제어 규칙에 사용되는 침입 정책에 따라 가장 적합한 NAP를 사용하도록 전환됩니다.

활성 인증의 호스트 이름 리디렉션에도 Snort 3이 필요하며, Snort 2로 전환하면 제거됩니다.

보류 중인 변경 사항을 구축해야 Snort 버전을 전환할 수 있습니다.

프로시저

단계 **1** 디바이스를 선택한 다음 Updates(업데이트) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

Intrusion Rule(침입 규칙**)** 그룹을 확인합니다. 현재 Snort 버전이 표시됩니다.

단계 **2** **Intrusion Rule(**침입 규칙**)** 그룹에서 **Upgrade to Snort 3.0(Snort 3.0**으로 업그레이드**)** 또는 **Downgrade to Snort 2.0(Snort 2.0**으로 다운그레이드**)**을 클릭하여 Snort 버전을 변경할 수 있습니다.

단계 **3** 작업을 확인하라는 프롬프트가 표시되면 최신 침입 규칙 패키지를 가져오는 옵션을 선택한 다음 **Yes(**예**)**를 클릭합니다.

최신 규칙 패키지를 받는 것이 좋습니다. 시스템은 액티브 Snort 버전용 패키지만 다운로드하므로 전환하려는 Snort 버전용 최신 패키지가 설치되어 있지 않을 가능성이 높습니다.

버전 전환 작업이 완료될 때까지 기다려야 침입 정책을 수정할 수 있습니다.

침입 이벤트를 위한 **Syslog** 구성

침입 정책에 외부 syslog 서버를 구성하여 침입 이벤트를 syslog 서버에 전송할 수 있습니다. 서버에 침입 이벤트를 전송하려면 침입 정책에서 syslog 서버를 구성해야 합니다. 액세스 규칙에서 syslog 서버를 구성하면 syslog 서버에 연결 이벤트만 전송되고 침입 이벤트는 전송되지 않습니다.

여러 시스템 로그 서버를 선택하면 각 서버로 이벤트가 전송됩니다.

침입 이벤트의 메시지 ID는 430001입니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하여 syslog를 구성합니다.

단계 **3** **Send Intrusion Events To(**다음으로 침입 이벤트 전송**)** 아래의 **+** 버튼을 클릭하고 시스템 로그 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(**새 시스템 로그 서버 생성**)**를 클릭하여 개체를 생성합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

네트워크 분석 정책 구성**(Snort 3)**

네트워크 분석 정책(NAP)은 디바이스에서 허용되는 모든 연결에 적용됩니다. NAP는 활성화된 검사기 및 검사기에서 사용하는 속성의 값을 결정합니다. 바인더는 다양한 검사기와 연결해야 할 포트 및 프로토콜을 결정합니다.

액세스 제어 규칙에서 적용하는 침입 정책에 따라 NAP를 조정합니다.

- 액세스 제어 규칙에서 단일 침입 정책을 사용하는 경우 동일한 이름의 NAP를 선택합니다. 그런 다음 침입 정책의 설정을 기반으로 검사기와 속성을 조정합니다. 예를 들어 CIP와 같은 특정 검사기에 대해 침입 규칙을 활성화하는 경우, NAP에서 해당 검사기를 활성화해야 합니다.
- 여러 침입 정책을 사용하는 경우 가장 엄격한 침입 정책과 일치하는 NAP를 선택합니다.
- 사용자 지정 침입 정책을 사용하는 경우 사용자 지정 침입 정책에 대한 기본 침입 정책을 기반으로 NAP를 선택합니다.

- 검사기 또는 바인더를 사용자 지정할 필요가 없는 경우, 침입 정책 사용을 기반으로 가장 적합한 NAP를 자동으로 선택하도록 시스템을 구성하는 것이 좋습니다. 이것이 기본 옵션입니다.

시작하기 전에

이를 방지하지 않는 한 시스템은 LSP 업데이트를 정기적으로 검사 규칙에 다운로드합니다. 이러한 업데이트는 검사기와 속성을 추가 또는 제거하고, 속성의 기본 설정을 변경할 수 있습니다. 제거된 검사기를 재정의한 경우, 이러한 재정의가 유지되며 검사기가 더 이상 지원되지 않는다는 경고가 표시됩니다. 이 경우 검사기를 삭제하고 NAP가 완전히 유효한지 확인하기 위해 플래그가 지정된 다른 조정을 수행합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

표 위에 표시된 Snort 버전이 3.x인지 확인합니다.

단계 **2** **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭합니다.

단계 **3** **Default Network Analysis Policy(**기본 네트워크 분석 정책**)**에서 다음 중 하나를 선택합니다.

- **Auto(**자동**)** - 액세스 제어 규칙에 적용된 가장 많이 사용되는 침입 정책(또는 사용자 지정 규칙의 기본 정책)과 일치하는 NAP를 자동으로 선택합니다. 침입 정책을 적용하지 않으면 Balanced Security and Connectivity NAP(균형 잡힌 보안 및 연결성 NAP)가 사용됩니다. NAP는 Prevention(방지) 모드에서 실행되며 침입 또는 바인더 설정을 사용자 지정할 수 없습니다. 이 절차의 나머지 부분은 자동 모드에서 실행할 때 적용되지 않습니다.
- **Custom(**사용자 지정**)** - 사용해야 할 NAP를 명시적으로 선택합니다. 다른 정책을 선택하려면 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다. 그런 다음 검사 모드를 선택하고 다음 단계에서 설명하는 것과 같이 검사기 및 바인더 설정을 사용자 지정할 수 있습니다.

단계 **4** Edit Network Analysis Policy(네트워크 분석 정책 편집) 대화 상자에서 정책을 선택하고 해당 설정을 구성합니다.

a) **Network Analysis Policy(**네트워크 분석 정책**)**에서 허용되는 모든 연결에 전역으로 적용해야 하는 정책을 선택합니다.

b) **Inspection Mode(**검사 모드**)**를 선택합니다.

검사 모드에 따라 규정 미준수 트래픽을 처리하는 방법이 결정됩니다. 최적의 결과를 얻으려면 침입 정책에서 사용하는 것과 동일한 검사 모드를 사용하십시오.

- **Prevention(**방지**)** - 정책의 설정에 따라 모든 디코더, 정규화 또는 프로토콜 변칙을 차단합니다. SSL 암호 해독 정책을 활성화하거나 액세스 제어 정책 설정에서 **TLS Server Identity Discovery(TLS** 서버 **ID** 검색**)** 옵션을 활성화하는 경우 이 옵션을 사용해야 합니다.
- **Detection(**탐지**)** - 디코더, 정규화 또는 프로토콜 변칙에 대한 알림만 제공합니다. 어떤 트래픽도 차단하지 않습니다.

c) (선택 사항). 검사기 및 바인더에 대한 재정의를 구성하고 관리합니다.

- 재정의를 편집하려면 검사기 및 바인더 재정의 구성, 12 페이지 항목을 참조하십시오.
- 스키마 또는 재정의를 다운로드하려면 재정의 및 스키마 다운로드, 14 페이지 항목을 참조하십시오.
- 재정의를 업로드하려면 재정의 업로드, 15 페이지 항목을 참조하십시오.
- 모든 재정의를 재설정하려면 NAP 파일 위의 **Reset Inspector / Binder Overrides(**검사기/바인더 재정의 재설정**)** 링크를 클릭합니다. 재설정을 확인하라는 메시지가 나타납니다. 명령 이름에 표시된 대로 삭제는 검사기 또는 바인더로 제한됩니다. 예를 들어, 모든 바인더 재정의를 삭제해도 검사기 재정의는 변경되지 않습니다.
- 선택한 검사기의 모든 변경 사항을 취소하려면 **Reset *Inspector* to Defaults(**검사기를 기본값으로 재설정**)**를 클릭합니다.
- 재정의가 있는 검사기만 볼 수 있도록 보기를 필터링하려면 **Show Only Overrides(**재정의만 표시**)**를 클릭합니다. **Show All Inspectors(**모든 검사기 표시**)**를 클릭하여 필터를 제거합니다.

d) **OK(**확인**)**를 클릭합니다.

검사기 및 바인더 재정의 구성

기본 NAP를 선택하면 해당 베이스라인 정책에 포함된 관리자 설정을 선택하게 됩니다. 대부분의 경우에는 적절한 설정입니다.

하지만 선택한 NAP의 설정을 재정의할 수 있습니다. 예를 들어 개별 검사기를 활성화 또는 비활성화하거나 속성 또는 바인더에 대한 값을 변경할 수 있습니다.

다음 절차에서는 재정의를 직접 구성하는 방법을 설명합니다. 또는 스키마를 다운로드하고 오프라인에서 변경한 다음 재정의를 업로드할 수 있습니다. 다른 디바이스에서 다운로드한 재정의를 업로드할 수도 있습니다.

시작하기 전에

각 검사기, 바인더 및 속성에 대한 설명은 이 문서의 범위를 벗어납니다. 예시를 포함한 세부 정보는 https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/snort3-inspectors/snort-3-inspector-reference.html에서 *Snort 3* 검사기 참조에서 확인하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택한 다음 **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하고, NAP 설정에 대해 **Custom(**맞춤형**)**을 선택한 다음 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다.

단계 **2** 변경할 설정이 포함된 탭을 클릭합니다.

- **Inspector(**검사기**)** - 검사기는 FTP와 같은 특정 유형의 트래픽에서 프로토콜 변칙을 검사합니다.

- **Binders(**바인더**)** - 바인더 검사기는 트래픽을 검사하기 위해 서비스 검사기를 사용해야 하는 시기를 결정합니다. 바인딩 검사기의 구성에는 포트, 호스트, CIDR 및 네트워크 분석 정책의 다른 검사기가 트래픽을 검사해야 하는 시기를 정의하는 서비스가 포함됩니다.

단계 **3** 필요에 따라 설정을 편집합니다.

- 다음을 사용하여 JSON 편집기에서 보기를 제어합니다.
  - JSON 파일의 전체 텍스트 검색을 수행하려면 **Filter(**필터**)** 편집 상자를 사용합니다.
  - JSON 파일의 모든 폴더를 열려면 **Expand All Fields(**모든 필드 확장**)(**  **)** 버튼을 클릭합니다.
  - JSON 파일의 모든 폴더를 닫으려면 **Collapse All Fields(**모든 필드 축소**)(**  **)** 버튼을 클릭합니다.
  - 최근 변경 사항을 취소하려면 **Undo Last Action(**마지막 작업 실행 취소**)(**  **)** 버튼을 클릭합니다
  - 마지막으로 되돌린 변경 사항을 다시 적용하려면 **Redo(**다시 실행**)(**  **)** 버튼을 클릭합니다.
  - 작업 메뉴, 오류 플래그 및 편집을 안내하는 기타 기능이 포함된 JSON 파일의 형식이 지정된 보기를 보려면 **Tree(**트리**)**를 선택합니다.
  - 원시 JSON 파일을 보려면 **Code(**코드**)**를 선택합니다.
- 트리 보기에서 **Menu(**메뉴**)(****)** 버튼을 클릭하여 파일의 내용을 조작합니다 다음 작업을 수행할 수 있습니다.
  - 속성을 삽입합니다. 편집기를 사용하여 적절한 데이터 유형을 결정하도록 하려면 Auto(자동)를 사용합니다. 그렇지 않으면 배열, 개체 또는 문자열을 추가합니다. 유효하지 않은 속성을 추가하는 경우 시스템은 검사기 또는 바인더를 해결해야 하는 문제가 있는 것으로 표시합니다.
  - 속성을 추가합니다. 이 작업은 삽입과 동일하지만 섹션 끝에 속성을 배치합니다.
  - 선택한 속성을 복제합니다.
  - 선택한 속성을 제거(삭제)합니다. 속성을 편집할 때 팝업 메시지에 삭제 명령이 제공될 수도 있습니다.
- 현재 비활성화된 검사기를 활성화하거나 부울 속성의 설정을 변경하려면 속성 값 앞에 있는 확인란을 클릭합니다. 예를 들어, 검사기를 활성화하려면 **enabled : false** 속성을 다음과 같이 변경합니다.

- 문자열 또는 숫자 속성의 값을 변경하려면 속성을 클릭하고 필요에 따라 값을 편집합니다. 항목이 필드의 규칙을 위반할 경우, 오류 메시지에서 불일치를 설명합니다. 예를 들어, 범위를 벗어난 값을 입력하는 경우 숫자 값에 유효한 값 범위가 표시됩니다.

- 재정의 재설정:
  - **Reset Inspector/Binder Overrides(**검사기/바인더 재정의 재설정**)**를 클릭하여 모든 검사기 또는 바인더에 대한 모든 변경 사항을 제거하고 기본값으로 되돌립니다. 명령 이름에 표시된 대로 삭제는 검사기 또는 바인더로 제한됩니다. 예를 들어, 모든 바인더 재정의를 삭제해도 검사기 재정의는 변경되지 않습니다.
  - **Reset *Inspector* to Defaults(**검사기를 기본값으로 재설정**)**를 클릭하여 선택한 검사기의 모든 변경 사항만 되돌립니다.
- 재정의가 있는 검사기만 볼 수 있도록 보기를 필터링하려면 **Show Only Overrides(**재정의만 표시**)**를 클릭합니다. **Show All Inspectors(**모든 검사기 표시**)**를 클릭하여 필터를 제거합니다.
- 검사기가 더 이상 지원되지 않으면 검사기는 메시지와 함께 플래그가 지정됩니다. 메시지에서 **Delete Inspector(**검사기 삭제**)** 링크를 클릭하여 검사기를 제거합니다.

단계 **4** 완료되면**OK(**확인**)**를 클릭합니다.

재정의 및 스키마 다운로드

NAP 스키마를 다운로드하거나 정책에 대해 구성한 재정의를 다운로드할 수 있습니다.

기본 NAP를 변경할 때마다 이전 설정으로 돌아가려면 재정의를 다운로드하는 것이 좋습니다. 또한 한 디바이스에서 JSON 편집기를 사용하여 모든 디바이스에서 사용할 재정의를 구현하고, 재정의를 다운로드한 다음 해당 재정의 파일을 다른 디바이스에 업로드할 수 있습니다.

오프라인으로 파일을 편집한 다음 이 디바이스 또는 여러 디바이스에 재정의를 업로드하려는 경우 스키마를 다운로드하면 유용합니다. 변경 사항만 재정의로 간주되도록 하려면 전체 파일을 업로드하는 대신 변경해야 하는 섹션만 복사/붙여넣기해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택한 다음 **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하고, NAP 설정에 대해 **Custom(**맞춤형**)**을 선택한 다음 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 현재 선택한 NAP의 스키마를 다운로드하려면 기어 아이콘(⚙)을 클릭하고 **Download(**다운로드**)** > **Policy Schema(**정책 스키마**)**를 선택합니다
- 현재 편집 세션 이전에 있었던 것처럼 저장된 재정의 세트를 다운로드하려면 기어 아이콘(⚙)을 클릭하고 **Download(**다운로드**)** > **Last Saved Overrides(**마지막으로 저장된 재정의**)**를 선택합니다. 파일에는 재정의된 속성과 해당 속성에 포함된 개체가 있습니다.

- 현재 편집 세션에서 생성한 재정의를 다운로드하려면 기어 아이콘(⚙)을 클릭하고 **Download(**다운로드**)** > **Current Unsaved Overrides(**현재 저장되지 않은 재정의**)**를 선택합니다. 파일에는 재정의된 속성과 해당 속성에 포함된 개체가 있습니다.

재정의 업로드

임베디드 JSON 편집기를 사용하여 속성을 편집하는 대신 NAP 정책 스키마를 다운로드하고 파일을 오프라인에서 편집한 다음 파일을 업로드할 수 있습니다. 그러면 업로드된 파일에 구성된 모든 재정의가 선택한 NAP에 적용됩니다.

다른 디바이스에서 재정의를 구성한 후 다운로드한 파일을 업로드할 수도 있습니다.

재정의를 업로드하면 동일한 파일을 여러 디바이스에 업로드하고 동일한 재정의를 쉽게 적용할 수 있습니다.

시작하기 전에

네트워크 분석 정책에서 검사기 구성을 재정의하려면 필요한 변경 사항만 업로드해야 합니다. 전체 구성을 업로드해서는 안 됩니다. 이렇게 하면 재정의가 고정되어 이후에 LSP 업데이트의 일부로 포함되는 기본값 또는 구성 변경 사항이 적용되지 않습니다. 업로드한 재정의는 변경하려는 속성에만 집중해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택한 다음 **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하고, NAP 설정에 대해 **Custom(**맞춤형**)**을 선택한 다음 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다.

단계 **2** 기어 아이콘(⚙)을 클릭하고 **Upload(**업로드**)** > **Overrides(**재정의**)**를 선택합니다.

단계 **3** (선택 사항). **Download(**다운로드**)** 링크 중 하나를 클릭하여 기존 재정의 사본을 저장합니다.

마지막으로 저장한 재정의(현재 편집 세션 전에 수행한 재정의) 또는 현재 저장되지 않은 재정의(현재 편집 세션 중에 수행한 재정의)를 다운로드할 수 있습니다.

단계 **4** Confirm Upload Overrides(업로드 재정의 확인) 대화 상자에서 **Yes(**예**)**를 클릭하여 계속할 것임을 확인합니다.

단계 **5** **Browse(**찾아보기**)**를 클릭하거나 드래그 앤 드롭하여 재정의가 포함된 JSON 파일을 선택하고 **OK(**확인**)**를 클릭합니다.

침입 정책 관리(Snort 3)

Snort 3를 검사 엔진으로 사용하는 경우 고유한 침입 정책을 생성하여 원하는 대로 맞춤화할 수 있습니다. 시스템은 동일한 이름의 Cisco Talos Intelligence Group(Talos) 정의된 정책을 기반으로 하는 사전 정의된 정책과 함께 제공됩니다. 이러한 정책을 수정할 수는 있지만, 기본 Talos 정책을 기반으로 고유한 정책을 생성하고 규칙 작업을 조정해야 하는 경우 변경하는 것이 좋습니다.

이러한 사전 정의된 각 정책에는 동일한 침입 규칙(서명이라고도 함) 목록이 포함되지만, 각 규칙에 수행되는 조치가 다릅니다. 예를 들어 어떤 규칙은 어떤 정책에서는 활성화되지만, 다른 정책에서는 비활성화될 수 있습니다.

특정 규칙이 차단하지 말아야 할 트래픽을 차단하여 오탐(False Positive)이 지나치게 많이 발생하고 있다는 사실을 알게 될 경우, 보안이 더 낮은 침입 정책으로 전환하지 않고도 규칙을 비활성화할 수 있습니다. 또는 트래픽을 삭제하지 않고 일치 항목에 대해 알리도록 규칙을 변경할 수 있습니다.

이와 반대로, 특정 공격을 차단해야 하지만 선택한 침입 정책에서 관련 규칙이 비활성화된 경우, 보안이 더 높은 정책으로 변경하지 않고도 규칙을 활성화할 수 있습니다.

침입 관련 대시보드 및 이벤트 뷰어(두 가지 모두 **Monitoring(**모니터링**)** 페이지에서 제공)를 사용하여 침입 규칙이 트래픽에 어떤 영향을 미치는지 평가하십시오. 침입 이벤트와 침입 데이터는 알리거나 삭제하도록 설정된 침입 규칙과 일치하는 트래픽에 대해서만 표시됩니다. 즉, 비활성화된 규칙은 평가되지 않습니다.

참고 Snort 2로 전환하면 맞춤형 정책을 생성할 수 없으며, 침입 정책이 약간 다르게 사용됩니다. 이 항목 대신 침입 정책 관리(Snort 2), 29 페이지를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

표 위에 표시된 Snort 버전이 3.x인지 확인합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Search/Filter(**검색/필터**)** 상자를 사용하여 정책을 찾습니다. 이름으로만 검색할 수 있습니다.
- 기어 아이콘()을 클릭하여 시스템 로그 서버에 로깅을 활성화합니다. 침입 이벤트를 위한 Syslog 구성, 10 페이지의 내용을 참조하십시오.
- 기어 아이콘()을 클릭하여 네트워크 분석 정책(NAP)을 구성합니다. 네트워크 분석 정책 구성(Snort 3), 10 페이지의 내용을 참조하십시오.
- 새 정책을 생성하려면 +를 클릭합니다. 맞춤형 침입 정책 구성(Snort 3), 17 페이지의 내용을 참조하십시오.

- 정책에서 속성과 규칙을 확인하고 수정하려면 수정 아이콘()을 클릭합니다. 침입 정책 속성 보기 또는 수정(Snort 3), 18 페이지의 내용을 참조하십시오.
- 정책을 삭제하려면 삭제 아이콘()을 클릭합니다.

맞춤형 침입 정책 구성(Snort 3)

사전 정의된 정책이 요구 사항에 맞지 않을 경우 새 침입 정책을 생성하여 규칙 동작을 맞춤설정할 수 있습니다. 일반적으로, 이러한 정책을 변경하는 대신 미리 정의된 정책을 기반으로 맞춤형 정책을 생성하는 것이 좋습니다. 그러면 맞춤화로 필요한 결과를 얻지 못하는 경우에 Cisco Talos 정의 정책 중 하나를 쉽게 구현할 수 있습니다.

프로시저

단계 **1** **Policies**(정책) > **Intrusion**(침입)을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 정책을 생성하려면 **+**를 클릭합니다.
- 기존 정책을 편집하려면, 정책에 대한 편집 아이콘()을 클릭합니다. 정책 상세정보가 표시되면 페이지 상단의 정책 속성 섹션에서 **Edit**(수정) 링크를 클릭합니다.

단계 **3** 정책의 **Name**(이름)을 입력하고 필요한 경우 설명을 입력합니다.

단계 **4** 정책을 위한 **Inspection Mode**(검사 모드) 구성

- **Prevention**(차단) - 침입 규칙 작업이 항상 적용됩니다. 삭제 규칙과 일치하는 연결이 차단됩니다.
- **Detection**(탐지) - 침입 규칙에서 알림만 생성합니다. 삭제 규칙과 일치하는 연결을 통해 알림 메시지가 생성되지만 연결은 차단되지 않습니다.

단계 **5** 정책의 **Base Template**(기본 템플릿)을 선택합니다.

기본 템플릿은 Cisco Talos에서 제공합니다. 각각에 대한 정보 아이콘을 클릭하면 정책에 대한 추가 정보를 확인할 수 있습니다. 새 규칙 패키지가 설치되면 정책 이름이 변경될 수 있으며 새 정책이 표시됩니다.

- **Maximum Detection**(최대 탐지) **(Cisco Talos)** — 이 정책은 오로지 보안에 중점을 둡니다. 네트워크 연결 및 처리량을 보장하지 않으며 오탐이 발생할 수 있습니다. 이 정책은 강력한 보안이 필요한 영역에만 사용해야 하며, 알림을 조사하여 유효성을 확인할 보안 모니터를 마련해야 합니다.

- **Security Over Connectivity(**보안이 연결에 우선함**) (Cisco Talos)** — 이 정책은 가급적 네트워크 연결 및 처리량 대신 보안에 중점을 둡니다. 트래픽을 더 자세히 검사하고 더 많은 규칙을 평가하지만 합당한 수준 내에서 오탐이 발생하고 레이턴시가 증가합니다.
- **Balanced Security and Connectivity(**보안과 연결의 균형 유지**) (Cisco Talos)** — (기본값) 이 정책은 네트워크 연결 및 처리량과 보안 요구 사항의 사이에서 절묘한 균형을 유지하려 합니다. 이 정책은 연결성보다 보안 우선 정책만큼 엄격하지는 않지만 정상적인 트래픽을 가급적 방해하지 않으면서 사용자의 안전을 유지하려 합니다.
- **Connectivity Over Security(**연결이 보안에 우선함**) (Cisco Talos)** — 이 정책은 가급적 보안 대신 네트워크 연결성 및 처리량에 중점을 둡니다. 트래픽을 자세히 검사하지 않으며 평가하는 규칙도 더 적습니다.
- **No Rules Active(**활성 규칙 없음**) (Cisco Talos)** — 이 정책은 일반적인 전 처리기 설정을 지정하는 기본 정책이지만 규칙 또는 기본 제공 알림을 활성화하지 않습니다. 적용하려는 정책만 활성화되도록 하려면 이 정책을 기본으로 사용합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

침입 정책 목록으로 돌아갑니다. 이제 새 정책을 보고 필요에 따라 규칙 작업을 조정할 수 있습니다.

침입 정책 속성 보기 또는 수정(Snort 3)

Intrusion Policy(침입 정책) 페이지에는 사전 정의된 정책과 사용자 정의 정책을 포함하는 정책 목록과 해당 설명이 표시됩니다. 정책을 수정하려면 먼저 정책의 속성을 확인해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

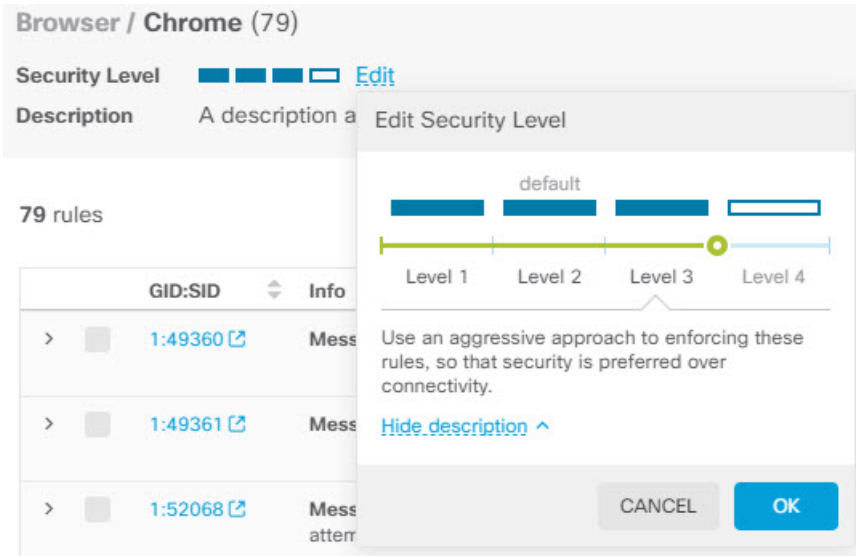
단계 **2** 정책의 편집 아이콘()을 클릭합니다.

정책에는 다음 섹션이 포함되어 있습니다.

- **Policy Name(**정책 이름**)** 드롭다운 목록
  - 드롭다운 목록에서 다른 정책을 선택하여 쉽게 전환하거나 뒤로 버튼()을 클릭하여 정책 목록으로 돌아갈 수 있습니다.
  - 정책 이름() 옆에 있는 삭제 아이콘을 클릭하여 이 정책을 삭제할 수 있습니다.
- **General properties(**일반 속성**)** 이 섹션에서는 침입 모드, 기본 정책 및 설명을 보여줍니다. **Edit(**수정**)**를 클릭하여 이러한 속성 또는 정책 이름을 변경합니다.
- 규칙 그룹 목차. 이 목록에는 정책에 액티브 규칙이 있는 모든 규칙 그룹이 표시됩니다. 그룹에는 더 큰 상위 그룹 내에서 규칙의 하위 세트를 구성하는 하위 그룹을 포함한 상위 그룹을 가진

계층 구조가 있습니다. 각 그룹은 규칙의 논리적 모음이며 지정된 규칙이 둘 이상의 그룹에 표시될 수 있습니다.

- 현재 정책에 액티브 규칙이 없는 그룹을 추가하려면 + > **Add Existing Rule Group**(기존 규칙 그룹 추가)을 클릭하여 그룹을 선택합니다. 침입 정책에서 규칙 그룹 추가 또는 제거(Snort 3), 20 페이지의 내용을 참조하십시오.
- 그룹의 보안 레벨을 변경하려면 목록에서 하위 그룹을 선택합니다. 규칙 목록이 아래에 나열된 그룹의 규칙과 함께 맨 위에 보안 레벨을 표시하도록 변경됩니다. 보안 레벨 옆에 있는 **Edit**(수정) 링크를 클릭하여 새 레벨을 선택합니다. 수정할 때는 **View Description**(설명 보기)을 클릭하여 각 보안 레벨에 대한 정보를 가져옵니다. 레벨을 변경하면 액티브 상태인 규칙이 변경될 수 있으며, 보다 많은 액티브 규칙 및 삭제 작업을 가진 보다 많은 규칙을 사용하는 경향이 있는 안전한 레벨을 사용하여 지정된 규칙에 대한 작업도 변경될 수 있습니다. **OK**(확인)를 클릭하여 변경을 확인합니다. (보안 수준은 맞춤형 규칙 그룹에 적용되지 않습니다.)



- 그룹의 모든 규칙을 제거하려면 목록에서 하위 그룹을 선택합니다. 그 다음 그룹 이름의 맨 오른쪽에 있는 **Exclude**(제외) 링크를 클릭하고 그룹을 제외할 것임을 확인합니다. 그룹을 제외하면 그룹의 모든 규칙이 간단히 비활성화됩니다. 그룹은 삭제되지 않습니다.

  그러나 활성화된 다른 그룹과 공유하는 규칙이 그룹에 포함된 경우 공유 규칙은 여전히 액티브 상태인 그룹에서 적용한 모든 작업을 유지합니다. 모든 경우, 그룹 구성원 자격에 관계없이 개별 규칙에 대해 가장 적극적인 설정을 유지합니다.
- 맞춤형 규칙의 새 맞춤형 규칙 그룹을 추가하려면 + > **Upload Custom Rules**(맞춤형 규칙 업로드)를 클릭합니다. 자세한 내용은 맞춤형 침입 규칙 업로드, 25 페이지 섹션을 참조해 주십시오.
- 맞춤형 규칙 그룹의 이름 또는 설명을 변경하려면 **Edit**(편집)를 클릭합니다.
- 맞춤형 규칙 그룹을 삭제하려면 **Delete**(삭제)를 클릭합니다. 자세한 내용은 맞춤형 침입 규칙 및 규칙 그룹 관리, 24 페이지를 참고하십시오.

- 맞춤형 규칙 그룹에 새 맞춤형 규칙을 추가하려면 규칙 테이블 위에 있는 +를 클릭합니다. 개별 맞춤형 침입 규칙 설정, 28 페이지의 내용을 참조하십시오.
- 맞춤형 규칙에 대한 그룹 멤버십을 편집, 복제, 삭제 또는 관리하려면 규칙 오른쪽에 마우스를 두고 해당 버튼 또는 명령을 클릭합니다. 자세한 내용은 개별 맞춤형 침입 규칙 설정, 28 페이지를 참고하십시오.

- **List of rules(**규칙 목록**)**. 전체 텍스트 검색을 사용하여 규칙을 찾으려면 검색 필드를 이용하십시오. GID 또는 SID의 조합에서 검색할 필터링 항목을 선택하거나 (추가한) 사용자 정의 규칙만 표시하거나,작업이 재정의된 규칙만 표시하거나, 해당 작업(비활성, 알림, 삭제)을 기준으로 간단히 규칙을 표시할 수도 있습니다. 규칙은 느리게 로드되므로 필터링되지 않은 전체 목록을 스크롤하려면 시간이 조금 걸립니다. 목록을 필터링할 때 새로 고침 버튼을 클릭하여 필터링된 보기를 다시 로드합니다.
  - 규칙에 대한 작업을 변경하려면 해당 규칙에 대한 **Action(**작업**)** 셀을 클릭하고 새 작업, 즉 **Alert(**알림**)** 전용, 일치하는 트래픽 **Block(**차단**)** 또는 규칙 **Disable(**비활성화**)**을 선택합니다. 각 규칙에 대한 기본 작업이 표시됩니다.
  - 한 번에 두 개 이상의 규칙에 대한 작업을 변경하려면 변경할 규칙의 왼쪽 열에 있는 체크박스를 클릭한 다음 규칙 테이블 위의 **Action(**작업**)** 드롭다운 목록에서 새 작업을 선택합니다. GID:SID 헤더의 체크 박스를 클릭하여 목록의 모든 규칙을 선택합니다. 한 번에 최대 5,000개의 규칙을 변경할 수 있습니다.
  - 맞춤형 규칙 그룹 내에서 규칙을 업데이트하려면 **Upload Rule File(**규칙 파일 업로드**)**을 클릭합니다. 자세한 내용은 맞춤형 침입 규칙 업로드, 25 페이지를 참고하십시오.
  - 규칙에 대한 자세한 정보를 얻으려면 **GID:SID** 셀의 링크를 클릭합니다. 링크를 클릭하면 Snort.org로 이동됩니다.
  - 나열된 규칙을 변경하려면 규칙 그룹 목차에서 상위 그룹이 아닌 하위 그룹을 클릭하면 됩니다. 규칙 그룹 목록의 맨 위에 있는 **ALL RULES(**모든 규칙**)**를 클릭하여 모든 규칙 목록으로 돌아갈 수 있습니다.
  - 정렬 순서를 변경하려면 열의 테이블 헤더를 클릭합니다. 규칙의 기본 정렬은 재정의된 규칙, 삭제 규칙, 알림 규칙 순입니다.
  - 침입 규칙(LSP) 업데이트의 변경 사항을 확인하려면 필터 필드에서 **LSP Update(LSP** 업데이트**)**를 선택한 다음 변경 사항을 확인하려는 업데이트를 선택하고, 모든 변경 사항을 볼지 아니면 규칙에 대한 추가 또는 변경 사항만 표시할지를 지정합니다.

침입 정책에서 규칙 그룹 추가 또는 제거(Snort 3)

침입 규칙은 로컬 그룹에서 구성됩니다. 그룹에는 계층 구조가 있으며 관련 하위 그룹을 포함하는 상위 그룹이 있습니다. 규칙 자체는 하위 그룹에만 나타납니다. 상위 그룹은 단순한 조직 구조입니다. 지정된 규칙은 둘 이상의 그룹에 나타날 수 있습니다.

생성하는 모든 맞춤형 규칙 그룹은 User Defined Groups 폴더에 있습니다. 맞춤형 규칙 그룹에는 계층 구조가 없습니다.

침입 정책에 규칙을 추가하거나 제거하는 가장 쉬운 방법은 그룹을 추가하거나 제거하는 것입니다. 그룹의 규칙은 논리적으로 관련되어 있으므로 지정된 그룹 내의 모든 규칙은 아니더라도 대부분을 사용해야 할 가능성이 높습니다.

다음 절차에서는 그룹을 추가하고 그룹의 보안 레벨을 변경하는 방법에 대해 설명합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 변경할 정책의 편집 아이콘()을 클릭합니다.

단계 **3** (그룹 추가) 그룹이 규칙 그룹 목록에 표시되지 않으면 + > **Add Existing Rule Group(**기존 규칙 그룹 추가**)**을 클릭하고 다음을 수행합니다.

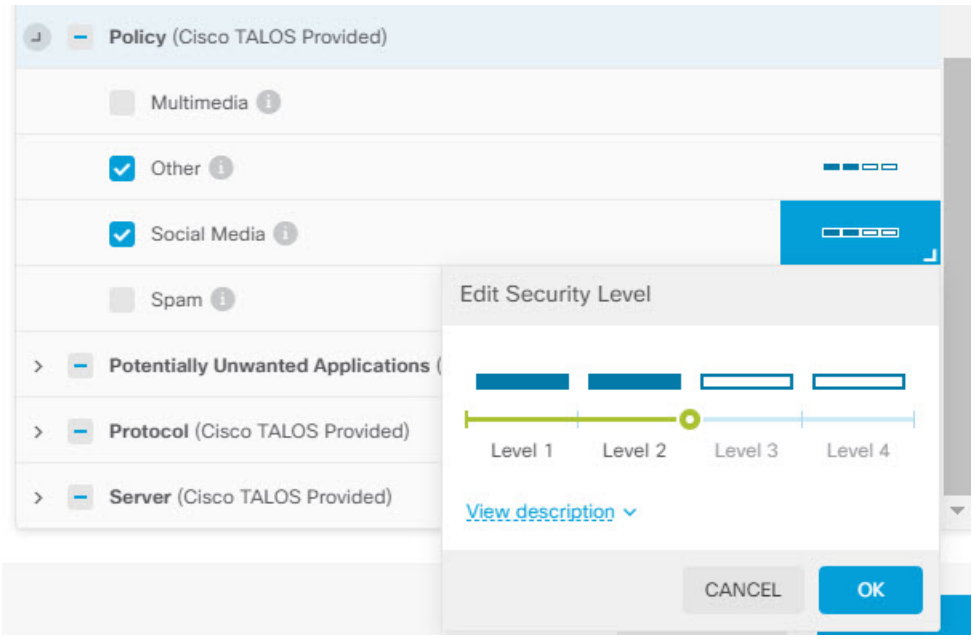
a) 하위 그룹을 찾습니다.

- 상위 그룹 이름 옆의 확인 표시는 상위 그룹의 모든 하위 그룹이 이미 선택되었음을 나타냅니다.
- 상위 그룹 이름 옆의 빼기 표시는 하나 이상의 하위 그룹에 이 정책에 대해 활성화된 규칙이 없음을 나타냅니다. 이들은 추가할 수 있는 그룹입니다.
- 하위 그룹 이름 옆의 확인 표시는 그룹이 이미 선택되었음을 나타냅니다.

b) 추가할 그룹을 선택합니다(즉, 체크 박스 선택).

c) (선택 사항으로, 맞춤형 규칙 그룹에 적용되지 않습니다.) 각 그룹에는 맞춤형 정책에 사용되는 기본 정책에 따라 기본 보안 레벨이 있습니다. 변경하려면 보안 레벨 아이콘을 클릭하여 새 레벨을 선택한 후 **OK(**확인**)**를 클릭합니다.

레벨 1은 보안보다 연결을 강조하는 가장 덜 안전한 상태이며, 레벨 4는 최대한의 보안을 제공하는 가장 적극적인 보안 상태입니다. **View Description(**설명 보기**)**을 클릭하여 각 레벨에 대한 설명을 선택하여 볼 수 있습니다.



d) 모든 변경 사항을 적용할 때까지 그룹을 계속 선택하거나 선택을 취소합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **4** (그룹 제거) 그룹 내의 모든 규칙을 비활성화하려는 경우 다음 방법 중 하나를 사용할 수 있습니다.

- 그룹을 선택한 다음, 규칙 목록 위의 그룹 이름 맨 오른쪽에 있는 **Exclude(**제외**)** 링크를 클릭합니다.
- 그룹을 추가하는 방법을 사용합니다. 대신 원치 않는 그룹을 선택 취소하고(즉, 체크 박스 선택을 취소) **OK(**확인**)**를 클릭합니다.
- 맞춤형 규칙 그룹을 삭제하여 시스템 및 이를 사용하는 모든 침입 정책에서 완전히 제거할 수 있습니다. 그룹을 선택한 다음 **Delete(**삭제**)**를 클릭합니다.

침입 규칙 작업 변경(Snort 3)

각 침입 정책의 규칙은 동일합니다. 차이점은 각 규칙에 수행되는 작업이 정책마다 다를 수 있다는 점입니다.

규칙 작업을 변경하면 오탐이 지나치게 많이 발생하는 규칙을 비활성화하거나, 규칙에서 일치하는 트래픽을 알리거나 삭제할지 여부를 변경할 수 있습니다. 또한 비활성화된 규칙을 활성화하여 일치하는 트래픽을 알리거나 삭제할 수 있습니다.

규칙 작업을 변경하는 가장 쉬운 방법은 규칙 그룹의 보안 레벨을 변경하는 것입니다. 그룹의 보안 레벨을 변경하면 그룹 내 규칙의 작업이 변경됩니다. 즉, 선택한 보안 상태에 따라 일부 규칙이 활성화(또는 비활성화)되거나 작업이 알림과 삭제 간에 변경될 수 있습니다. 그러나 필요한 경우 개별 규칙 작업을 변경할 수 있습니다.

참고 지정된 규칙에 대한 기본 작업은 선택된 그룹 및 심각도 전체를 기반으로 합니다. 그룹의 심각도를 변경하거나 그룹을 제외하면 규칙에 대한 기본 작업이 변경될 수 있습니다.

시작하기 전에

맞춤형 규칙 그룹에는 보안 레벨이 없습니다. 보안 레벨 기술을 사용하여 맞춤형 규칙에 대한 규칙 작업을 변경할 수 없습니다.

프로시저

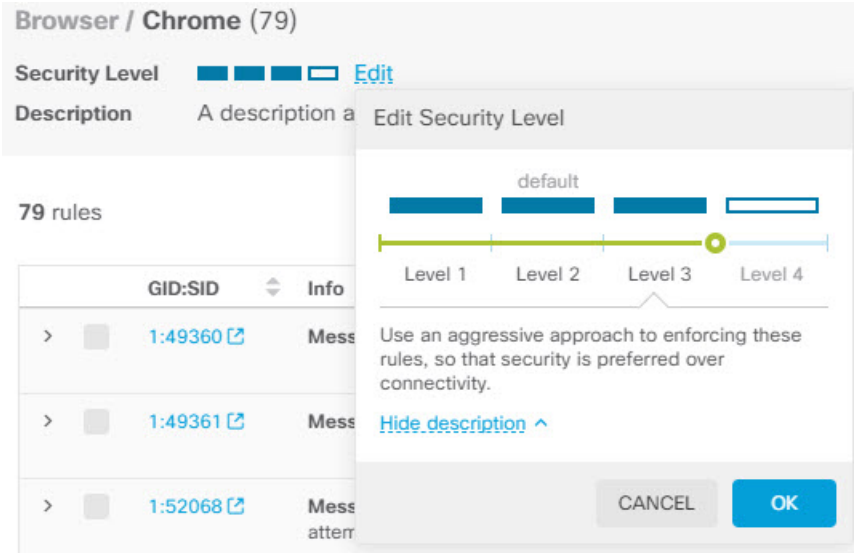
단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 변경하려는 규칙 작업이 있는 정책의 보기 아이콘( )을 클릭합니다.

단계 **3** (권장 방법) 규칙 그룹의 보안 레벨을 변경합니다.

a) 규칙 그룹 목록에서 하위 규칙 그룹을 클릭합니다.

b) 규칙 목록 위에서 그룹의 보안 레벨 옆에 있는 **Edit(**수정**)**를 클릭합니다.



참고 그룹의 모든 규칙을 비활성화하려면 **Edit(**수정**)**를 클릭하지 마십시오. 대신 **Exclude(**제외**)**를 클릭하여 그룹을 제외할 것임을 확인합니다. 그룹은 삭제되지 않으며 해당 규칙은 단순히 비활성화됩니다. 나머지 단계를 건너 뜁니다.

c) 그룹의 새 레벨을 선택합니다. **View Description(**설명 보기**)**을 클릭하여 각 레벨에 대한 설명을 선택하여 볼 수 있습니다.

레벨 1은 보안보다 연결을 강조하는 가장 덜 안전한 상태이며, 레벨 4는 최대한의 보안을 제공하는 가장 적극적인 보안 상태입니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **4** (수동 방법) 하나 이상의 규칙에 대한 작업을 변경합니다.

a) 변경하려는 작업이 있는 규칙을 찾습니다.

Search/Filter(검색/필터**)** 상자를 사용하여 규칙 정보 내의 문자열을 검색합니다. GID 또는 SID의 조합에서 검색할 필터링 항목을 선택하거나 해당 작업(비활성, 알림, 삭제)을 기준으로 간단히 규칙을 표시할 수도 있습니다. 규칙은 느리게 로드되므로 필터링되지 않은 전체 목록을 스크롤하려면 시간이 조금 걸립니다. 목록을 필터링할 때 새로 고침 버튼을 클릭하여 필터링된 보기를 다시 로드합니다.

문제 해결 작업을 수행 중인 경우, 이벤트 또는 Cisco Technical Support를 통해 SID(Snort 식별자) 및 GID(생성기 식별자)를 제공받는 것이 가장 좋습니다. 그러면 규칙을 정확하게 검색할 수 있습니다.

b) 작업을 변경하려면 다음 중 하나를 수행합니다.

- 한 번에 하나의 규칙 변경 — 규칙의 **Action(**작업**)** 열을 클릭하고 필요한 작업을 선택합니다.
  - **Alert(**알림**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
  - **Drop(**삭제**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하고 연결도 삭제합니다.
  - **Disabled(**비활성화됨**)** — 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.
- 한 번에 여러 규칙 변경 — 변경하려는 규칙의 체크 박스를 클릭한 다음, 테이블 위의 **Bulk(**대량**)** 드롭다운을 클릭하여 원하는 작업을 선택합니다. GID:SID 헤더의 체크 박스를 클릭하여 목록의 모든 규칙을 선택합니다. 한 번에 최대 5,000개의 규칙을 변경할 수 있습니다.

맞춤형 침입 규칙 및 규칙 그룹 관리

시스템에는 Cisco Talos Intelligence Group(Talos)에서 정의한 수천 개의 침입 규칙이 제공됩니다. 추가 공격에 대해 알고 있는 경우 맞춤형 침입 규칙을 생성 및 업로드하여 해당 공격을 차단하고 알림을 보내거나 삭제할 수 있습니다. 규칙을 한 번에 하나씩 생성, 편집 및 삭제할 수도 있습니다.

업로드된 규칙의 경우 텍스트 편집기를 사용하여 오프라인으로 규칙을 생성합니다. 업로드하는 각 텍스트 파일에 맞춤형 규칙 그룹을 포함하는 것이 좋습니다. 그런 다음 규칙에 변경 사항을 쉽게 업로드하고, 새 규칙을 맞춤형 규칙 그룹에 병합하거나, 규칙을 편집된 새 복사본으로 교체할 수 있습니다.

이러한 규칙을 생성하는 방법을 설명하는 것은 이 문서의 범위를 벗어납니다. Snort 2 규칙을 Snort 3 형식으로 변환하는 방법을 포함하여 Snort에 대한 침입 규칙을 작성하는 방법에 대한 자세한 내용은 https://snort.org/documents 가이드를 참조하십시오. https://snort.org/documents/rules-writers-guide-to-snort-3-rules의 규칙 작성자를 위한 *Snort 3* 규칙 작성 소개를 예로 들 수 있습니다.

시작하기 전에

맞춤형 침입 규칙 업로드, 25 페이지에서 설명하는 것과 같이 맞춤형 규칙을 업로드하는 프로세스 도중 또는 개별 규칙을 생성하거나 규칙 구성원 자격을 관리할 때 맞춤형 규칙 그룹을 생성합니다. 그룹을 생성한 후에는 그룹 및 그룹의 콘텐츠를 관리할 수 있습니다.

맞춤형 그룹은 그룹을 생성할 때 편집한 정책뿐만 아니라 모든 침입 정책에 사용할 수 있습니다. 따라서 그룹에 대한 변경 사항은 모든 정책에 적용됩니다. 예를 들어, 맞춤형 규칙 그룹을 삭제하면 모든 정책에서 삭제되며 더 이상 사용할 수 없습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 정책의 편집 아이콘( )을 클릭합니다.

기본 제공 정책 중 하나가 아닌 맞춤형 침입 정책에 사용자 지정 규칙을 추가하는 것이 좋습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 그룹을 생성하려면 + > **Upload Custom Rules(**맞춤형 규칙 업로드**)**를 클릭합니다. 맞춤형 침입 규칙 업로드, 25 페이지의 내용을 참조하십시오.
- 그룹의 이름 또는 설명을 편집하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 이후 **Edit(**편집**)**를 클릭하고 변경합니다.
- 정책에서 그룹 및 그룹의 규칙을 제외하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 이후 **Exclude(**제외**)**를 클릭하여 그룹을 제거할 수 있습니다.
- 시스템과 그룹을 사용하는 모든 정책에서 그룹을 삭제하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 그런 다음 **Delete(**삭제**)**를 클릭합니다. 규칙이 삭제된 그룹에만 있는 경우 시스템에서도 삭제됩니다. 하지만 삭제하지 않은 다른 맞춤형 규칙 그룹에도 규칙이 있는 경우 규칙은 해당 그룹에서 그대로 유지됩니다.
- 그룹에서 규칙을 대량으로 교체하거나 업데이트하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 그런 다음 그룹의 규칙 테이블 위에 있는 Action(작업) 드롭다운 목록에서 **Upload Rule File(**규칙 파일 업로드**)**을 클릭합니다. 해당 프로세스는 맞춤형 침입 규칙 업로드, 25 페이지에서 설명한 것과 동일합니다.
- 개별 규칙과 그룹에 대한 규칙 할당을 생성 및 관리하려면 개별 맞춤형 침입 규칙 설정, 28 페이지의 내용을 참조하십시오.

맞춤형 침입 규칙 업로드

현재 다른 규칙에서 처리하지 않는 공격에 대해 알고 있는 경우 맞춤형 침입 규칙을 생성 및 업로드하여 해당 공격을 차단하고 알림을 보내거나 삭제할 수 있습니다. 가져온 규칙의 작업은 알림 또는 삭제여야 하며, 규칙의 기본 작업은 가져온 파일의 작업에 의해 정의됩니다. 가져온 후에는 규칙 작업을 변경하고 필요한 경우 규칙을 비활성화할 수 있습니다.

이러한 규칙은 오프라인으로 생성해야 합니다. device manager에서는 단순히 규칙 파일을 업로드하는 것이며, 규칙을 직접 설정하지 않습니다. 규칙 파일은 텍스트 파일이어야 합니다. 줄바꿈을 사용하여 읽을 수 있도록 규칙의 형식을 지정하거나 한 줄에 규칙을 배치할 수 있으며, 빈 줄이 허용됩니다. 규칙 형식은 snort.org에서 설명합니다.

예를 들어 세 가지 규칙의 업로드 파일은 다음과 같이 표시될 수 있습니다.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
   gid:1;
   sid:1000002;
   rev:1;
)
```

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 정책의 편집 아이콘( )을 클릭합니다.

기본 제공 정책 중 하나가 아닌 맞춤형 침입 정책에 사용자 지정 규칙을 추가하는 것이 좋습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 그룹 목록 위에서 **+** > **Upload Custom Rules(**맞춤형 규칙 업로드**)**를 클릭합니다.
- 이미 생성한 맞춤형 규칙 그룹에 규칙을 업로드하는 경우 맞춤형 규칙 그룹을 선택하고 그룹의 규칙 테이블 위에 있는 **Action(**작업**)** 드롭다운 목록 옆에서 **Upload Rule File(**규칙 파일 업로드**)**을 클릭할 수 있습니다.

단계 **4** **Browse(**찾아보기**)**를 클릭하고 맞춤형 규칙 파일을 선택하거나 파일을 Upload File(파일 업로드) 대화 상자에 끌어다 놓습니다.

업로드가 완료될 때까지 기다립니다.

단계 **5** 충돌을 처리할 방법을 선택합니다.

추가하는 규칙이 시스템에 이미 있는 규칙과 동일한 경우 충돌이 발생합니다. 이전에 업로드한 것과 동일한 규칙 또는 수정된 버전의 규칙을 업로드하는 경우에만 충돌이 발생합니다.

다음 옵션 중 하나를 선택합니다.

참고 **Merge(**병합**)**와 **Replace(**바꾸기**)**는 기본적으로 동일합니다. 기존 규칙을 변경하려면 업로드한 규칙의 개정 번호가 이전에 업로드한 규칙보다 높아야 합니다. 유일한 차이점은 업로드 파일에 대상 맞춤형 규칙 그룹에 있는 규칙이 없는 경우 **Replace(**바꾸기**)** 옵션은 규칙 그룹에서 해당 규칙을 삭제한다는 것입니다. **Merge(**병합**)** 옵션은 이러한 "없는" 규칙을 그대로 둡니다.

- **Merge(**병합**)** - 업로드된 파일에서 변경된 규칙이 선택한 그룹에도 있는 경우 업로드한 파일의 규칙이 개정 번호가 높다면 변경 사항이 병합됩니다. 변경되지 않은 규칙 또는 업로드에 해당 규칙이 없는 그룹의 규칙은 변경되지 않습니다. 업로드 시 모든 새 규칙이 추가됩니다. 이것이 기본 옵션입니다.
- **Replace(**바꾸기**)** - 업로드한 파일의 규칙이 개정 번호가 더 높은 경우 선택한 그룹의 규칙을 바꿉니다. 업로드된 파일에 없는 기존 규칙은 그룹에서 삭제됩니다. 업로드된 버전의 개정 번호가 같거나 낮은 기존 규칙은 변경되지 않습니다. 업로드 시 모든 새 규칙이 추가됩니다.

단계 **6** **+**를 클릭하고 업로드된 규칙에 대한 맞춤형 규칙 그룹을 선택합니다.

사용하고자 하는 맞춤형 규칙 그룹이 없는 경우 **Create New Group(**새 그룹 생성**)**을 클릭하여 바로 생성합니다. 새 그룹에는 이름과 설명(필요한 경우)이 필요합니다. 이후 새 그룹을 선택할 수 있습니다.

규칙을 바꾸는 경우 단일 그룹만 선택할 수 있습니다. 병합하는 경우 여러 그룹을 선택할 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

파일이 업로드되고 새 그룹에 배치됩니다. 업로드된 규칙 수와 업데이트, 삭제 또는 무시된 규칙 수에 대한 요약이 표시됩니다.

파일에 오류가 있으면 업로드가 실패합니다. 오류에 대한 자세한 정보를 보려면 **Download Error File(**다운로드 오류 파일**)** 링크를 클릭할 수 있습니다.

이 침입 정책에서 그룹이 자동으로 활성화됩니다. 그룹 및 새 규칙을 다른 정책에 추가할 수는 있지만 그룹 및 규칙은 다른 정책에서 자동으로 활성화되지 않습니다. 다른 정책에 그룹을 추가하는 방법

에 대한 자세한 내용은 침입 정책에서 규칙 그룹 추가 또는 제거(Snort 3), 20 페이지의 내용을 참고하십시오.

개별 맞춤형 침입 규칙 설정

맞춤형 침입 규칙은 대량 파일 업로드 대신 한 번에 하나씩 설정할 수 있습니다. 이 방법은 규칙을 빠르게 조정해야 하거나 한 번에 몇 개의 규칙만 만들거나 수정해야 하는 경우에 유용합니다.

침입 규칙을 설정할 때는 다음 사항에 유의하십시오.

- 모든 맞춤형 규칙의 GID는 1이어야 합니다.
- 규칙의 SID는 시스템의 모든 규칙에서 고유해야 합니다. 또한 1,000,000 이상이어야 합니다.
- 규칙을 편집하는 경우 규칙 버전을 변경해야 합니다. 일반적으로 버전 번호는 1 단위로 증가합니다.
- 고유한 버전의 규칙을 생성하기 위해 Cisco Talos Intelligence Group(Talos) 규칙을 복제할 수는 있지만 복제본의 SID를 고유하게 변경해야 합니다.

시스템에서 규칙의 형식이 올바른지 확인하기 위해 유효성 검사를 수행하며, 문제에 대한 오류 메시지가 표시됩니다. 하지만 규칙이 적절한지 여부는 시스템에서 확인할 수 없습니다.

Snort 2 규칙을 Snort 3 형식으로 변환하는 방법을 포함하여 Snort에 대한 침입 규칙을 작성하는 방법에 대한 자세한 내용은 https://snort.org/documents 가이드를 참조하십시오. https://snort.org/documents/rules-writers-guide-to-snort-3-rules의 규칙 작성자를 위한 *Snort 3* 규칙 작성 소개를 예로 들 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 정책의 편집 아이콘()을 클릭합니다.

기본 제공 정책 중 하나가 아닌 맞춤형 침입 정책에 사용자 지정 규칙을 추가하는 것이 좋습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 침입 규칙을 추가하려면 규칙 테이블 위에 있는 **Add Intrusion Rule(**침입 규칙 추가**)** 버튼(+)을 클릭합니다. 규칙을 추가할 때 새 규칙을 포함할 하나 이상의 맞춤형 규칙 그룹을 선택해야 합니다. 필요한 경우 규칙을 추가하면서 새 그룹을 생성할 수 있습니다.
- 기존 규칙을 복제하고 편집하여 규칙을 추가하려면 규칙의 오른쪽 끝에 마우스를 두고 Duplicate(복제) () 버튼을 클릭합니다. 마우스를 올려둔 경우에만 버튼이 표시됩니다. 맞춤형 규칙의 경우 **Duplicate(**복제**)** 명령은 추가 옵션(**...**) 버튼에 있습니다.

- 맞춤형 규칙을 편집하려면 맞춤형 규칙 그룹에서 규칙을 찾고 편집( ) 버튼을 클릭합니다. 편집한 사항은 규칙이 있는 모든 그룹에 적용됩니다. 변경 시 규칙 버전 번호를 1 이상으로 늘려야 합니다.
- 맞춤형 규칙을 삭제하려면 해당 규칙의 삭제( ) 버튼을 클릭합니다. 규칙이 포함된 모든 규칙 그룹에서 규칙이 삭제됩니다. 그룹에서 규칙을 제거하려는 경우 규칙을 삭제하는 대신 **Manage Group Assignments(**그룹 할당 관리**)** 옵션을 사용합니다.
- 규칙을 포함하는 그룹을 변경하려면 추가 옵션**(...)** 버튼을 클릭하고 **Manage Group Assignment(**그룹 할당 관리**)**를 선택합니다. 그런 다음 그룹을 추가하거나 제거할 수 있습니다. 변경 사항은 그룹 구성원 자격에만 영향을 미치며, 규칙을 변경하거나 삭제하지 않습니다.

단계 **4** 새 규칙 및 그룹의 경우 정책에 규칙을 추가합니다.

새 규칙을 생성하거나 기존 규칙을 편집할 때 새 그룹을 생성하면 해당 그룹이 정책에 자동으로 추가되지 않으며 규칙이 자동으로 활성화되지도 않습니다. 편집 중인 정책에 그룹을 추가하라는 메시지가 표시됩니다. 규칙을 추가하거나 편집하는 동안 그룹을 추가하지 않는 경우 다음 프로세스를 사용하여 나중에 그룹을 추가할 수 있습니다.

a) 그룹 콘텐츠 테이블에서 **+** > **Add Existing Rule Group(**기존 규칙 그룹 추가**)**을 클릭합니다.
b) User Defined Groups 폴더에서 그룹을 찾고 선택한 다음 **OK(**확인**)**를 클릭합니다.
c) 콘텐츠 테이블에서 그룹을 선택하고 새 규칙이 그룹에 있으며 원하는 작업이 있는지 확인합니다.

침입 정책 관리(Snort 2)

사전 정의된 침입 정책을 적용할 수 있습니다. 이러한 각 정책에는 동일한 침입 규칙(서명이라고도 함) 목록이 포함되지만, 각 규칙에 시행되는 조치가 다릅니다. 예를 들어 어떤 규칙은 한 정책에서 활성 상태이지만, 다른 정책에서는 비활성 상태일 수 있습니다.

특정 규칙이 차단하지 말아야 할 트래픽을 차단하여 오탐(False Positive)이 지나치게 많이 발생하고 있다는 사실을 알게 될 경우, 보안이 더 낮은 침입 정책으로 전환하지 않고도 규칙을 비활성화할 수 있습니다. 또는 트래픽을 삭제하지 않고 일치 항목에 대해 알리도록 규칙을 변경할 수 있습니다.

이와 반대로, 특정 공격을 차단해야 하지만 선택한 침입 정책에서 관련 규칙이 비활성화된 경우, 보안이 더 높은 정책으로 변경하지 않고도 규칙을 활성화할 수 있습니다.

침입 관련 대시보드 및 이벤트 뷰어(두 가지 모두 **Monitoring(**모니터링**)** 페이지에서 제공)를 사용하여 침입 규칙이 트래픽에 어떤 영향을 미치는지 평가하십시오. 침입 이벤트와 침입 데이터는 알리거나 삭제하도록 설정된 침입 규칙과 일치하는 트래픽에 대해서만 표시됩니다. 즉, 비활성화된 규칙은 평가되지 않습니다.

다음 주제에서는 침입 정책 및 규칙 조정에 대해 자세히 설명합니다.

침입 정책을 위한 검사 모드 구성(Snort 2)

기본적으로 모든 침입 정책은 Prevention(차단) 모드에서 작동하여 IPS(침입 방지 시스템)를 구현합니다. Prevention(차단) 검사 모드에서 연결이 트래픽을 삭제하는 작업을 수행하는 침입 규칙과 일치하는 경우 연결이 능동적으로 차단됩니다.

대신 네트워크에서 침입 정책의 영향을 테스트하려는 경우, 모드를 IDS(침입 탐지 시스템)를 구현하는 모드를 Detection(탐지)로 변경할 수 있습니다. 이 검사 모드에서 삭제 규칙은 일치하는 연결에 대한 알림을 받는 알림 규칙처럼 처리되지만, 작업 결과는 Would Have Blocked(차단되었을 수 있음)가 되고 연결은 실제로 차단되지 않습니다.

침입 정책에 따라 검사 모드를 변경하면 차단 및 탐지를 혼합하여 사용할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 검사 모드를 변경할 침입 정책의 탭을 클릭합니다.

Inspection Mode(검사 모드**)**는 규칙 테이블 위에 표시됩니다.

단계 **3** 검사 모드 옆의 **Edit(**수정**)** 링크를 클릭하고 정책에 대한 모드를 변경한 다음 **OK (**확인**)**를 클릭합니다.

옵션은 다음과 같습니다.

- **Prevention(**차단**)** - 침입 규칙 작업이 항상 적용됩니다. 삭제 규칙과 일치하는 연결이 차단됩니다.
- **Detection(**탐지**)** - 침입 규칙에서 알림만 생성합니다. 삭제 규칙과 일치하는 연결을 통해 알림 메시지가 생성되지만 연결은 차단되지 않습니다.

침입 규칙 작업 변경(Snort 2)

각각의 사전 정의된 침입 정책에는 동일한 규칙이 있습니다. 차이점은 각 규칙에 수행되는 작업이 정책마다 다를 수 있다는 점입니다.

규칙 작업을 변경하면 오탐이 지나치게 많이 발생하는 규칙을 비활성화하거나, 규칙에서 일치하는 트래픽을 알리거나 삭제할지 여부를 변경할 수 있습니다. 또한 비활성화된 규칙을 활성화하여 일치하는 트래픽을 알리거나 삭제할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 변경하려는 규칙 작업이 있는 침입 정책의 탭을 클릭합니다.

사전 정의된 정책:

- Connectivity over Security(연결이 보안에 우선함)
- Balanced Security and Connectivity(균형 잡힌 보안 및 연결성)
- Security over Connectivity(보안이 연결에 우선함)
- Maximum Detection(최대 탐지)

단계 **3** 변경하려는 작업이 있는 규칙을 찾습니다.

규칙은 재정의된 규칙이 먼저 나열되고 재정의된 규칙의 그룹 내에 작업별로 정렬됩니다. 그렇지 않은 경우, 규칙은 GID별로 정렬된 다음 SID별로 정렬됩니다.

검색 상자를 사용하여 변경하려는 규칙을 찾습니다. 문제 해결 작업을 수행 중인 경우, 이벤트 또는 Cisco Technical Support를 통해 SID(Snort 식별자) 및 GID(생성기 식별자)를 제공받는 것이 가장 좋습니다.

각 규칙의 요소에 대한 자세한 내용은 침입 규칙 특성, 3 페이지의 내용을 참조하십시오.

목록을 검색하려면 다음을 수행합니다.

a) **Search(**검색**)** 상자를 클릭하여 검색 특성 대화 상자를 엽니다.
b) 생성기 ID(**GID**), Snort ID(**SID**) 또는 규칙 **Action(**작업**)**을 조합하여 입력하고 **Search(**검색**)**를 클릭합니다.

   예를 들어 **Action = Drop(**작업 = 삭제**)**을 선택하여 일치하는 연결을 삭제하는 정책 내의 모든 규칙을 볼 수 있습니다. 검색 상자 옆의 텍스트는 기준과 일치하는 규칙의 수를 나타내며, 이는 예를 들어 “8937 of 9416 rules found(9416개의 규칙 중 8937개 검색됨)”와 같이 표시됩니다.

   검색 기준을 지우려면 검색 상자에서 해당 기준의 x를 클릭합니다.

단계 **4** 규칙의 **Action(**작업**)** 열을 클릭하고 필요한 작업을 선택합니다.

- **Alert(**알림**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
- **Drop(**삭제**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하고 연결도 삭제합니다.
- **Disabled(**비활성화됨**)** — 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.

규칙의 기본 작업은 작업에 추가되는 "(Default)(기본값)"으로 표시됩니다. 기본값을 변경하면 상태 열에 해당 규칙이 "Overridden(재정의됨)"으로 표시됩니다.

침입 정책 모니터링

침입 정책 통계는 **Monitoring(**모니터링**)** 페이지의 **Attackers(**공격자**)** 및 **Targets(**대상**)** 대시보드에서 확인할 수 있습니다. 이러한 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 침입 정책을 적용해야 합니다. 트래픽 및 시스템 대시보드 모니터링의 내용을 참조하십시오.

침입 이벤트를 보려면 **Monitoring(**모니터링**)** > **Events(**이벤트**)**를 선택한 다음 **Intrusion(**침입**)** 탭을 클릭합니다. 이벤트에 마우스를 올려놓고 **View Details(**세부사항 보기**)** 링크를 클릭하면 더 자세한 정보를 얻을 수 있습니다. 세부 사항 페이지에서 **View IPS Rule(IPS** 규칙 보기**)**을 클릭하면 관련 침입 정책의 규칙으로 이동하여 규칙 작업을 변경할 수 있습니다. 이렇게 하면 작업을 삭제에서 알림으로 변경하여 규칙으로 인해 양호한 연결이 너무 많이 차단되는 오탐의 영향을 줄일 수 있습니다. 이와 반대로 규칙에 대한 공격 트래픽이 많이 표시되는 경우에는 알림 규칙을 삭제 규칙으로 변경할 수 있습니다.

침입 정책에 대한 syslog 서버를 컨피그레이션하는 경우, 침입 이벤트의 메시지 ID는 430001입니다.

침입 정책의 예시

사용 사례 장에는 침입 정책을 구현하는 다음의 예시가 포함되어 있습니다.

- 위협을 차단하는 방법
- 네트워크에서 트래픽을 능동적으로 모니터링하는 방법