



Snort 3 침입 정책 시작하기

이 장에서는 침입 탐지 및 방지를 위한 Snort 3 침입 정책 및 액세스 제어 규칙 구성 관리 정보를 제공합니다.

- 침입 정책 개요, 1 페이지
- 네트워크 분석 및 침입 정책 사전 요건, 2 페이지
- 사용자 지정 Snort 3 침입 정책 생성, 2 페이지
- Snort 3 침입 정책 편집, 3 페이지
- 침입 정책의 기본 정책 변경, 8 페이지
- 침입 정책 관리, 9 페이지
- 침입 방지를 수행하는 액세스 제어 규칙 설정, 9 페이지

침입 정책 개요

침입 정책은 트래픽에서 보안 위반을 검사하고 인라인 구축에서 악성 트래픽을 차단 또는 변경할 수 있는 침입 탐지 및 방지 구성의 정의된 집합입니다. 침입 정책은 액세스 제어 정책에 따라 호출되며, 트래픽이 목적지에 허가되기 전 시스템의 마지막 방어선입니다.

각 침입 정책의 핵심에는 침입 규칙이 있습니다. 활성화된 규칙은 시스템이 규칙과 일치하는 트래픽의 침입 이벤트를 생성하도록 하거나 선택적으로 차단하도록 합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다.

시스템은 Cisco Talos(Talos Intelligent Group)의 경험을 활용할 수 있는 여러 기본 침입 정책을 제공합니다. Talos는 이 정책에 대해 침입 및 검사기 규칙 상태(활성화 또는 비활성화)를 설정할 뿐 아니라 다른 고급 설정의 초기 구성을 제공합니다.



팁 시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다.

사용자 지정 침입 정책을 생성하는 경우, 다음을 수행할 수 있습니다.

- 규칙 활성화/비활성화 및 고유의 규칙 작성과 추가를 통해 탐지 기능을 조정할 수 있습니다.
- Secure Firewall 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결합니다.

침입 정책은 일치하는 패킷을 삭제하고 침입 이벤트를 생성할 수 있습니다. 침입 또는 전처리기 삭제 규칙을 구성하려면 해당 상태를 Block(차단)으로 설정합니다.

침입 정책을 조정할 경우, 특히 규칙을 활성화하고 추가할 경우, 일부 침입 규칙에서는 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 합니다. 침입 정책이 패킷을 검토하기 전에, 패킷은 네트워크 분석 정책 내 구성에 따라 전처리됩니다. 검사기를 비활성화한 경우, 검사기가 네트워크 분석 정책 웹 사용자 인터페이스에서 비활성화된 상태로 남아 있다고 해도 시스템은 자동으로 검사기를 현재의 설정으로 사용합니다.



주의 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다.

사용자 지정 침입 정책을 구성한 후, 하나 이상의 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 침입 정책을 연결함으로써 액세스 제어 구성의 일부로 사용할 수 있습니다. 이는 트래픽이 최종 목적지로 전달되기 전에 허용되는 특정 트래픽을 검토하기 위해 시스템이 침입 정책을 강제로 사용하도록 합니다. 침입 정책과 페어링된 변수 집합을 통해 홈 네트워크 및 외부 네트워크와 사용자 네트워크의 서버를 적절하게 반영할 수 있습니다.

기본적으로 시스템은 암호화된 페이로드의 침입 검사를 비활성화합니다. 이는 암호화 연결이 침입 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

추가 지원 및 정보는 [Snort 3 침입 정책 개요](#) 비디오를 참조하십시오.

네트워크 분석 및 침입 정책 사전 요건

Snort 검사기 엔진이 침입 및 악성코드 분석을 위해 트래픽을 처리하도록 허용하려면 Threat Defense 디바이스에 대해 활성화된 IPS 라이선스가 있어야 합니다.

네트워크 분석, 침입 정책을 관리하고 마이그레이션 작업을 수행하려면 관리자 사용자여야 합니다.

사용자 지정 Snort 3 침입 정책 생성

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

단계 2 Create Policy(정책 생성)를 클릭합니다.

단계 3 고유한 Name(이름)을 입력하고, 필요한 경우 Description(설명)을 입력합니다.

단계 4 Inspection Mode(검사 모드)를 선택합니다.

선택한 작업에 따라 침입 규칙이 차단 및 알림(예방 모드) 또는 알림만(탐지 모드)인지 여부가 결정됩니다.

참고 예방 모드를 선택하기 전에 차단 규칙이 알림만 표시할 수 있도록 하여 많은 오탐을 유발하는 규칙을 식별할 수 있습니다.

단계 5 **Base Policy**(기본 정책)를 선택합니다.

시스템에서 제공하는 정책 또는 기존 정책을 기본 정책으로 사용할 수 있습니다.

단계 6 **Save**(저장)를 클릭합니다.

새로운 정책의 설정은 기본 정책의 설정과 같습니다.

다음에 수행할 작업

정책을 사용자 지정하려면 [Snort 3 침입 정책 편집, 3 페이지](#) 항목을 참조하십시오.

Snort 3 침입 정책 편집

Snort 3 정책을 편집하는 동안 모든 변경 사항이 즉시 저장됩니다. 변경 사항을 저장하는 데 추가 작업이 필요하지 않습니다.

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

단계 2 **Intrusion Policies**(침입 정책) 탭이 선택되었는지 확인합니다.

단계 3 구성하려는 침입 정책 옆의 **Snort 3** 버전을 클릭합니다.

단계 4 정책을 수정합니다.

- 모드 변경 - 검사 모드를 변경하려면 **Mode**(모드) 드롭다운을 클릭합니다.


주의 검사 모드는 정책의 Snort 3 버전에 대해서만 변경됩니다. 기존 검사 모드는 Snort 2 버전에서 그대로 유지됩니다. 즉, 정책의 Snort 2 및 Snort 3 버전의 검사 모드가 서로 다릅니다. 이 옵션은 신중하게 사용하는 것이 좋습니다.

- **Prevention**(방지) - 트리거된 차단 규칙은 이벤트(경고)를 생성하고 연결을 삭제합니다.
- **Detection**(탐지) - 트리거된 차단 규칙은 알림을 생성합니다.

탐지를 시작하기 전에 예방을 위해 탐지 모드를 선택할 수 있습니다. 예를 들어, 예방 모드를 선택하기 전에 차단 규칙이 알림만 할 수 있도록 하여 많은 오탐을 유발하는 규칙을 식별할 수 있습니다.

단계 5 침입 정책의 기본 설정을 정의하는 **Base Policy**(기본 정책) 레이어를 클릭합니다.

- 검색 규칙 - 검색 필드를 사용하여 표시를 필터링합니다. **GID**, **SID**, 규칙 메시지 또는 참조 정보를 입력할 수 있습니다. 예를 들어 **GID:1**; **SID:9621**은 1:962 규칙만 표시하고, **SID:9621,9622,9623**은 서로 다른 **SID**의 여러 규칙을 표시합니다. **Search**(검색) 텍스트 상자 내부를 클릭하여 다음 옵션 중 하나를 선택할 수도 있습니다.

- **Action = Alert** 또는 **Action: Block** 필터 적용
 - **Disabled Rules** 필터 적용
 - **Custom/User Defined Rules** 표시
 - **GID, SID** 또는 **GID:SID**로 필터링
 - **CVE**로 필터링
 - **코멘트**로 필터링
- **View filtered rules**(필터링된 규칙 보기) - **Presets**(프리셋)를 클릭하여 알림, 차단, 비활성화 등으로 설정된 규칙을 봅니다.
재정의된 규칙은 규칙 작업이 기본 작업에서 다른 작업으로 변경된 규칙을 나타냅니다. 변경되면 원래 기본 작업으로 다시 변경하더라도 규칙 작업 상태가 재정의됩니다. 그러나 **Rule Action**(규칙 작업) 드롭다운 목록에서 **Revert to default**(기본값으로 되돌리기)를 선택하면 재정의된 상태가 제거됩니다.
Advanced Filters(고급 필터)는 **LSP(Lightweight Security Package)** 릴리스, 침입 분류 및 Microsoft 취약성을 기반으로 하는 필터 옵션을 제공합니다.
 - **View rule documentation**(규칙 문서 보기) - 규칙 ID 또는 **Rule Documentation**(규칙 문서) 아이콘을 클릭하여 규칙에 대한 Talos 문서를 표시합니다.
 - **View a rule message**(규칙 메시지 보기) - 규칙 세부 정보를 보려면 규칙 행의 확장 화살표(>) 아이콘을 클릭합니다.
 - **Add rule comments**(규칙 코멘트 추가) - 규칙에 대한 코멘트를 추가하려면 **Comments**(코멘트) 열 아래의 **Comment**(코멘트)()를 클릭합니다.

단계 6 Group Overrides(그룹 재정의) - 규칙 그룹의 모든 범주를 나열하는 **Group Overrides**(그룹 재정의) 레이어를 클릭합니다. **Description**(설명), **Overrides**(재정의), **Enabled Groups**(활성화된 그룹) 등이 있는 최상위 규칙 그룹이 표시됩니다. 상위 규칙 그룹은 업데이트할 수 없으며 읽기 전용입니다. 리프 규칙 그룹만 업데이트할 수 있습니다. 각 규칙 그룹에서 마지막 리프 그룹까지 이동할 수 있습니다. 각 그룹에서 규칙 그룹을 재정의, 포함 및 제외할 수 있습니다. 리프 규칙 그룹에서 다음을 수행할 수 있습니다.

- **Search rule groups**(규칙 그룹 검색) - 검색 필드를 사용하여 키워드를 입력하고 규칙 그룹을 검색합니다.
- 왼쪽 패널에서 프리셋 필터 옵션을 선택하여 규칙 그룹을 검색할 수 있습니다.
 - **All**(모두) - 모든 규칙 그룹을 표시합니다.
 - **Excluded**(제외됨) - 제외된 그룹을 표시합니다.
 - **Included**(포함) - 포함된 그룹을 표시합니다.
 - **Overridden**(재정의됨) - 재정의된 규칙 그룹 구성을 표시합니다.
- **Set the security level for a rule group**(규칙 그룹의 보안 레벨 설정) - 왼쪽 창에서 필요한 규칙 그룹으로 이동하여 클릭합니다. 규칙 그룹의 **Security Level**(보안 레벨) 옆에 있는 **Edit**(편집)을 클릭하여 시스템 정의 규칙 설정에 따라 보안 수준을 높이거나 낮춥니다.

Edit Security Level(보안 레벨 편집) 대화 상자에는 **Revert to Default**(기본값으로 되돌리기)를 클릭하는 옵션이 있으며, 클릭하면 변경 사항을 되돌립니다.

management center는 구성된 보안 레벨에 대해 규칙 그룹의 규칙에 대한 작업을 자동으로 변경합니다. **Rule Overrides**(규칙 재정의) 레이어에서 보안 레벨을 변경할 때마다 **Presets**(프리셋)에서 **Block Rules**(차단 규칙) 및 **Disabled Rules**(비활성화 규칙)의 수를 확인합니다.

- 보안 레벨을 대량으로 변경하여 특정 규칙 범주에 있는 모든 규칙 그룹의 보안 레벨을 변경할 수 있습니다. 대량 보안 레벨은 둘 이상의 규칙 그룹이 있는 규칙 그룹에 적용됩니다. 규칙 그룹을 대량 업데이트한 후에도 규칙 그룹과 연결된 규칙 그룹의 보안 레벨은 계속 업데이트할 수 있습니다.

규칙 그룹 내에서 혼합 보안 레벨이 있을 수 있습니다. 혼합은 하위 그룹에 상위 규칙 그룹 내에서 혼합 보안 레벨이 포함되어 있음을 나타냅니다.

- **Include or exclude rule groups**(규칙 그룹 포함 또는 제외) - 표시되는 규칙 그룹은 시스템에서 제공하는 기본 침입 정책과 연결된 기본 규칙 그룹입니다. 침입 정책에서 규칙 그룹을 포함하거나 제외할 수 있습니다. 제외된 규칙 그룹은 침입 정책에서 제거되며 해당 규칙은 트래픽에 적용되지 않습니다. management center의 사용자 지정 규칙 업로드에 대한 자세한 내용은 **규칙 그룹에 사용자 지정 규칙 추가**를 참조하십시오.

규칙 그룹을 제외하려면 다음과 같이 합니다.

1. **Rule Groups**(규칙 그룹) 창을 탐색하여 제외할 규칙 그룹을 선택합니다.
2. 오른쪽 창에서 **Exclude**(제외) 하이퍼링크를 클릭합니다.
3. **Exclude**(제외)를 클릭합니다.

업로드된 사용자 지정 규칙 또는 이전에 제외된 규칙 그룹에 새 규칙 그룹 또는 여러 규칙 그룹을 포함하려면 다음을 수행합니다.

1. 규칙 그룹 필터 드롭다운 목록 옆에 있는 **Add**(추가) (+)를 클릭합니다.
2. 해당 규칙 그룹 옆의 체크 박스를 선택하여 추가할 모든 규칙 그룹을 선택합니다.
3. **Save**(저장)를 클릭합니다.

- 리프 규칙 그룹의 경우 **Override**(재정의) 열 헤더 아래의 아이콘을 클릭하여 침입 규칙에 대한 기본 정책 및 그룹 재정의로 인해 할당될 수 있는 재정의된 규칙 작업의 순서를 설명하는 규칙 작업 추적을 확인합니다. 기본 정책 구성 또는 사용자 그룹 재정의에서 규칙 작업을 가져올 수 있습니다. 사용자 그룹 재정의가 둘 사이의 우선순위를 지정합니다. 우선순위는 규칙 그룹에 할당된 최종 재정의 작업을 나타냅니다.
- 규칙 그룹의 일부인 규칙 요약을 보려면 **Rule Count**(규칙 수) 열 헤더 아래에 있는 규칙 카운트(숫자)를 클릭합니다.

단계 7 권장 사항 - Cisco 권장 규칙을 생성 및 적용하려면 **Recommendations**(권장 사항) 레이어를 클릭합니다. 권장 사항은 호스트 데이터베이스를 사용하여 알려진 취약성을 기반으로 규칙을 활성화하거나 비활성화합니다.

단계 8 Rule Overrides(규칙 재정의) - **Rule Overrides**(규칙 재정의) 레이어를 클릭하여 알림, 차단, 비활성화, 재정의, 재작성, 통과, 삭제 또는 거부로 설정된 규칙을 보려면 프리셋을 선택합니다.

- **Set By**(설정 기준) 열에는 상태별(Base Policy(기본 정책))로 설정된 기본값 또는 **Group Overrides**(그룹 재정의), **Rule Overrides**(규칙 재정의) 또는 **Recommendations**(권장 사항)별로 수정된 규칙 상태가 표시됩니다. 왼쪽 창에

있는 **All Rules**(모든 규칙)의 **Set By**(설정 기준) 열에는 우선순위 순서에 따라 재정의 작업을 추적한 규칙 작업이 표시됩니다. 규칙 작업의 우선순위 순서는 **Rule Override**(규칙 재정의) > **Recommendations**(권장 사항) > **Group Override**(그룹 재정의) > **Base Policy**(기본 정책)입니다.

- **Rule Action**(규칙 작업) 수정 - 규칙 작업을 수정하려면 다음 중 하나를 선택합니다.
 - 대량 편집 - 하나 이상의 규칙을 선택한 다음 **Rule Action**(규칙 작업) 드롭다운 목록에서 필요한 작업을 선택하고 **Save**(저장)를 클릭합니다.

참고 대량 규칙 작업 변경은 처음 500개 규칙에 대해서만 지원됩니다.
 - 단일 규칙 편집 - **Rule Action**(규칙 작업) 열의 드롭다운 목록에서 규칙에 대한 작업을 선택합니다.

규칙 작업은 다음과 같습니다.

- **Block**(차단) - 이벤트를 생성하고, 현재 일치하는 패킷과 이 연결의 모든 후속 패킷을 차단합니다.
- **Alert**(알림) - 일치하는 패킷에 대한 이벤트만 생성하며, 패킷 또는 연결을 삭제하지 않습니다.
- **Disabled**(비활성화됨) - 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.
- **Revert to default**(기본값으로 되돌리기) - 시스템 기본 작업으로 되돌립니다.
- **Pass**(통과) - 이벤트가 생성되지 않으며, 후속 Snort 규칙에 따른 추가 평가 없이 패킷을 전달할 수 있습니다.

참고 Pass(통과) 작업은 시스템 제공 규칙이 아닌 사용자 지정 규칙에만 사용할 수 있습니다.
- **Drop**(삭제) - 이벤트를 생성하고, 일치하는 패킷을 삭제하며, 이 연결에서 추가 트래픽을 차단하지 않습니다.
- **Reject**(거부) - 소스 및 대상 호스트에 대한 TCP 프로토콜인 경우 이벤트를 생성하고, 일치하는 패킷을 삭제하며, 이 연결의 추가 트래픽을 차단하고, TCP 재설정을 전송합니다.

Behavior of reject in different firewall modes and IP address or source or destination in relation to Client or Server(클라이언트 또는 서버와 관련된 여러 방화벽 모드 및 IP 주소 또는 소스나 대상에서의 거부 동작): Snort는 라우팅, 인라인 및 브리지 인터페이스의 경우 클라이언트와 서버 모두에 RST 패킷을 전송합니다. Snort는 두 개의 RST 패킷을 전송합니다. 클라이언트 방향의 RST 패킷은 소스가 서버 IP로, 대상이 클라이언트 IP로 설정됩니다. 서버 방향의 RST 패킷에서는 소스가 클라이언트 IP로 설정되고 대상이 서버 IP로 설정됩니다.
- **Rewrite**(재작성) - 이벤트를 생성하고 규칙의 교체 옵션에 따라 패킷 내용을 덮어씁니다.

IPS 규칙 작업 로깅에 대해서는 [규칙 작업 로깅, 7 페이지](#)의 내용을 참조하십시오.

React(대응) 규칙이 있는 경우 알림 작업으로 변환됩니다.

단계 9 Summary(요약) 레이어를 클릭하면 정책에 대한 현재 변경 사항을 전체적으로 볼 수 있습니다. 정책 요약 페이지에는 다음 정보가 포함되어 있습니다.

- 정책의 규칙 배포(활성 규칙, 비활성화된 규칙 등).
- 정책을 내보내고 침입 정책 보고서를 생성하는 옵션.

- 기본 정책 세부 정보.
- 권장 사항 생성 옵션.
- 재정의한 그룹의 목록을 표시하는 그룹 재정의.
- 사용자가 재정의한 규칙의 목록을 표시하는 규칙 재정의.
- **Summary**(요약) 레이어에서 ? 아이콘을 클릭하여 Snort 계층화 개념을 설명하는 Snort 도움말 가이드 팝업 창을 엽니다.

기본 정책을 변경하려면 [침입 정책의 기본 정책 변경, 8 페이지](#) 항목을 참조하십시오.

참고 **Objects(개체) > Intrusion Rules(침입 규칙)**로 이동하고 **Snort 3 All Rules(Snort 3의 모든 규칙)** 탭을 클릭한 다음, 모든 침입 규칙 그룹을 통과할 수 있습니다. 상위 규칙 그룹에는 연결된 하위 그룹과 규칙 수가 나열됩니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. [구성 변경 사항 구축](#)를 참고하십시오.

규칙 그룹 보고

규칙 그룹은 생성된 침입 이벤트에 반영되며, MITRE 전술 및 기술도 호출됩니다. MITRE 전술 및 기술에 대한 열과 침입 이벤트에 대한 비 MITRE 규칙 그룹에 대한 열이 있습니다. 침입 이벤트에 액세스하려면 management center에서 **Analysis(분석) > Intrusions(침입) > Events(이벤트)**로 이동하고 **Table View of Events(이벤트의 테이블 보기)** 탭을 클릭합니다. **Unified Events(통합 이벤트)** 뷰어에서 침입 이벤트 필드를 볼 수도 있습니다. **Analysis(분석)** 탭에서 **Unified Events(통합 이벤트)**를 클릭합니다.

Intrusion Events(침입 이벤트) 페이지에서 규칙 그룹 보고를 위해 다음 필드가 추가됩니다. 언급된 열을 명시적으로 활성화해야 합니다.

- MITRE ATT&CK
- 규칙 그룹

이러한 필드에 대한 자세한 내용은 *Cisco Secure Firewall Management Center* 관리 가이드, 7.3의 침입 이벤트 필드 섹션을 참조하십시오.

규칙 작업 로깅

Management Center 7.2.0부터는 **Intrusion Events(침입 이벤트)** 페이지에서 **Inline Result(인라인 결과)** 열의 이벤트가 규칙에 적용된 IPS 작업과 동일한 이름을 표시하므로, 규칙과 일치하는 트래픽에 적용된 작업을 볼 수 있습니다.

IPS 작업의 경우 다음 테이블은 **Intrusion Events(침입 이벤트)** 페이지의 **Inline Result(인라인 결과)** 열과 **Unified Events(통합 이벤트)** 페이지의 **Intrusion Event Type(침입 이벤트 유형)**에 대한 **Action(작업)** 열에 표시되는 이벤트를 보여줍니다.

| Snort 3에 대한 IPS 작업 | 인라인 결과 - Management Center 7.1.0 이하 | 인라인 결과 -Management Center 7.2.0 이상 |
|--------------------|-------------------------------------|------------------------------------|
| 알림 | 통과 | 알림 |
| 차단 | 삭제됨/삭제되었을 수 있음/부분 삭제됨 | 차단/차단 예정/부분 차단 |
| 드롭 | 삭제됨/삭제되었을 수 있음 | 삭제/삭제 예정 |
| 거부 | 삭제됨/삭제되었을 수 있음 | 거부/거부 예정 |
| 재작성 | 허용 | 재작성 |



중요

- "Replace(대체)" 옵션이 없는 규칙의 경우, **Rewrite(재작성)** 작업은 **Would Rewrite(재작성 예정)**로 표시됩니다.
- "Replace(대체)" 옵션이 지정되었지만, IPS 정책이 Detection(탐지) 모드에 있거나 디바이스가 Inline-TAP/Passive(인라인-TAP/패시브) 모드에 있는 경우, **Rewrite(재작성)** 작업은 **Would Rewrite(재작성 예정)**로 표시됩니다.



참고


이전 버전과의 호환성(Threat Defense 7.1.0 디바이스를 관리하는 Management Center 7.2.0)의 경우, 언급된 이벤트는 이벤트에 대한 **Pass(통과)**가 **Alert(알림)**으로 표시되는 IPS 알림 작업에만 적용됩니다. 다른 모든 작업의 경우, Management Center 7.1.0에 대한 이벤트가 적용됩니다.

침입 정책의 기본 정책 변경

다른 시스템 제공 정책 또는 맞춤형 정책을 기본 정책으로 선택할 수 있습니다.

최대 다섯 개의 사용자 지정 정책을 묶을 수 있는데, 다섯 중 넷은 이전에 만들어진 다른 넷 중 하나를 기본 정책으로 사용하는 것이며, 다섯 번째는 반드시 시스템이 제공하는 정책을 기본 정책으로 사용해야 합니다.

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

단계 2 구성하려는 침입 정책 옆에 있는 **Edit(편집)**()을 클릭합니다.

단계 3 **Base Policy(기본 정책)** 드롭다운 목록에서 정책을 선택합니다.

단계 4 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. [구성 변경 사항 구축](#)를 참고하십시오.

침입 정책 관리



Intrusion Policy(침입 정책) 페이지(**Policies**(정책) > **Intrusion**(침입))에서 다음 정보와 함께 현재의 사용자 지정 침입 정책을 볼 수 있습니다.

- 침입 정책을 사용하여 트래픽을 검사하는 액세스 제어 정책 및 디바이스 수
- 다중 도메인 구축에서 정책이 생성된 도메인

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.

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

단계 2 침입 정책을 관리합니다.

- 생성 - **Create Policy**(정책 생성)를 클릭합니다([사용자 지정 Snort 3 침입 정책 생성, 2 페이지 참조](#)).
- 삭제 - 삭제하려는 정책 옆에 있는 삭제()를 클릭합니다. 다른 사용자가 정책 변경 사항을 저장하지 않은 경우, 시스템은 확인하라는 메시지를 표시하고 사용자에게 알립니다. **OK**(확인)를 클릭하여 확인합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 침입 정책 세부 정보 수정 - 수정하려는 정책 옆에 있는 수정()을 클릭합니다. 침입 정책의 **Name**(이름), **Inspection Mode**(검사 모드) 및 **Base Policy**(기본 정책)를 수정할 수 있습니다.
- 침입 정책 설정 수정 - **Snort 3 Version**(Snort 3 버전)을 클릭합니다([Snort 3 침입 정책 편집, 3 페이지 참조](#)).
- 내보내기 - 다른 management center에서 가져오기 위해 침입 정책을 내보내려는 경우 **Export**(내보내기)를 클릭합니다(최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 구성 내보내기 주제 참조).
- 구축 - **Deploy**(구축) > **Deployment**(구축)를 선택합니다([구성 변경 사항 구축 참조](#)).
- 보고서 - **Report**(보고서)를 클릭합니다(최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 현재 정책 보고서 생성 주제 참조). 각 정책 버전에 대해 하나씩 wo 보고서를 생성합니다.

침입 방지를 수행하는 액세스 제어 규칙 설정

액세스 제어 정책에는 침입 정책과 관련된 여러 액세스 제어 규칙이 포함될 수 있습니다. 모든 Allow or Interactive Block(허용 또는 인터랙티브 차단) 액세스 제어 규칙에 대해 침입 검사를 구성할 수 있습니다.

니다. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크상에 있는 다양한 유형의 트래픽에 대해 다양한 침입 검사 프로파일과 맞춰볼 수 있습니다.

시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 변수 집합을 사용합니다. 집합의 변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책 내 변수를 사용하여 규칙 삭제 및 동적 규칙 상태의 IP 주소를 나타낼 수 있습니다.



팁 시스템에서 제공한 침입 정책을 사용하더라도 Cisco는 네트워크 환경을 정확하게 반영할 수 있도록 시스템의 침입 변수를 구성할 것을 강력히 권장합니다. 최소한 기본값 집합의 기본 변수라도 수정하시기 바랍니다.

시스템이 제공하는 침입 정책 및 사용자 정의 침입 정책의 이해

Cisco는 시스템에서 여러 침입 정책을 제공합니다. 시스템이 제공하는 침입 정책을 사용하여 Cisco Talos(Talos Intelligence Group)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 전처리 규칙 상태를 설정할 뿐만 아니라 고급 설정의 초기 구성을 제공합니다. 사용자는 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다. 맞춤형 정책을 구축하면 사용자 환경에서 시스템의 성능을 개선할 수 있으며, 사용자 네트워크에서 발생하는 악의적인 트래픽 및 정책 위반을 집중적으로 확인할 수 있습니다.

연결 및 침입 이벤트 로깅

액세스 제어 규칙에 의해 호출된 침입 정책이 침입을 탐지하고 침입 이벤트를 생성할 경우, 해당 이벤트는 Management Center에 저장됩니다. 시스템은 또한 액세스 제어 규칙의 로깅 구성에 관계없이 침입이 발생한 연결의 종료를 Management Center 데이터베이스에 자동으로 로깅합니다.

액세스 제어 규칙 설정 및 침입 정책

단일한 액세스 제어 정책에서 사용할 수 있는 고유한 침입 정책의 수는 대상 디바이스의 모델에 따라 다르며, 성능이 뛰어난 디바이스일수록 더 많은 정책을 처리할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다. 다양한 침입 정책-변수 집합 쌍을 Allow(허용) 및 Interactive Block(인터랙티브 차단) 규칙(및 기본 작업)에 연결할 수 있지만 대상 디바이스에 구성된 대로 검사를 수행할 수 있는 리소스가 부족한 경우, 액세스 제어 정책을 구축할 수 없습니다.

침입 방지 수행을 위한 액세스 제어 규칙 구성

이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자 여야합니다.

단계 1 액세스 제어 정책 편집기에서 새 규칙을 생성하거나 기존 규칙을 편집합니다. 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 액세스 제어 규칙 구성 요소 주제를 참조하십시오.

단계 2 규칙 작업이 **Allow(허용)**, **Interactive Block(인터랙티브 차단)** 또는 **Interactive Block with reset(인터랙티브 차단 후 초기화)**으로 설정되어 있는지 확인합니다.

단계 3 **Inspection(검사)**을 클릭합니다.

- 단계 4 시스템이 제공하는 정책 또는 사용자 지정 침입 정책을 선택하거나 **None(없음)**을 선택하여 액세스 제어 규칙과 일치하는 트래픽에 대한 침입 검사를 비활성화합니다.
- 단계 5 침입 정책에 관련된 변수 집합을 변경하려면 **Variable Set(변수 집합)** 드롭다운 목록에서 값을 선택합니다.
- 단계 6 **Save(저장)**를 클릭하여 규칙을 저장합니다.
- 단계 7 **Save(저장)**를 클릭하여 정책을 저장합니다.
-

다음에 수행할 작업

구성 변경 사항을 구축합니다. [구성 변경 사항 구축](#)를 참고하십시오.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.