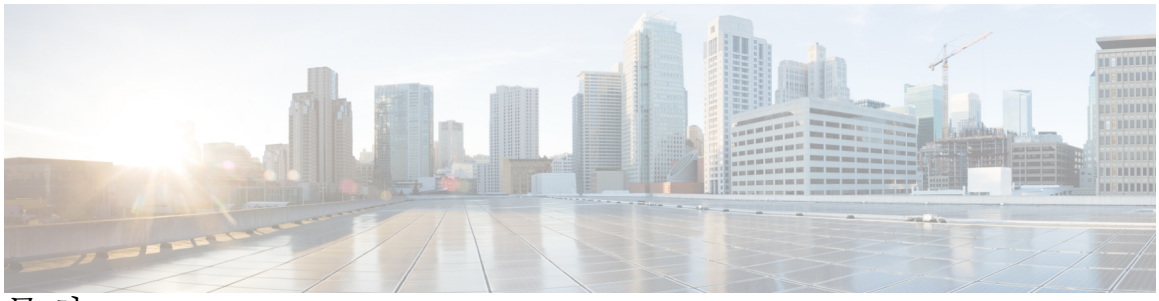
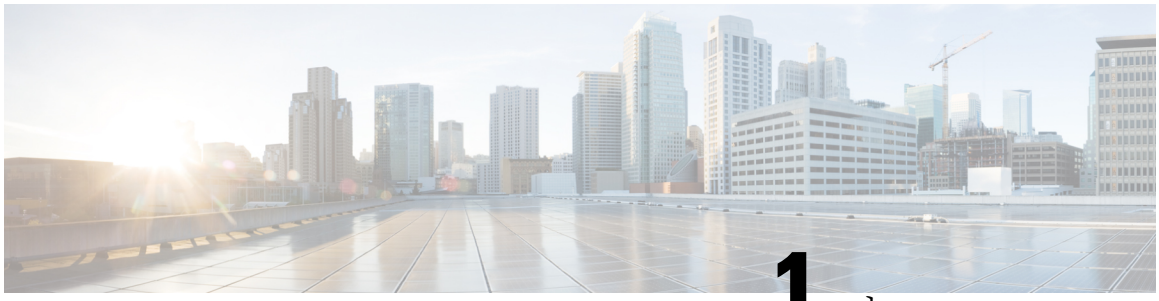
Cisco Secure Firewall Management Center Snort 3 구성 가이드, 버전 7.6

최종 변경: 2024년 12월 23일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

네트워크 분석 및 침입 정책 개요

Snort 검사 엔진은 Secure Firewall Threat Defense(이전 명칭: Firepower Threat Defense) 디바이스의 필수 요소입니다. 이 장에서는 Snort 3 및 네트워크 분석 정책과 침입 정책에 대해 간략히 설명합니다. 또한 시스템에서 제공하는 사용자 지정 네트워크 분석 및 침입 정책에 대한 인사이트도 제공합니다.

네트워크 분석 및 침입 정책 정보

네트워크 분석 및 침입 정책은 침입 탐지 및 방지 기능의 일부로 함께 작동합니다.

- 침입 탐지란 용어는 일반적으로 네트워크 트래픽에서 잠재적인 침입을 수동적으로 모니터링 및 분석하고 보안 분석을 위한 공격 데이터를 저장하는 프로세스를 말합니다. 'IDS'라고 하기도 합니다.
- 침입 방지란 용어에는 침입 탐지의 개념이 포함되지만, 악성 트래픽이 네트워크를 통과할 때 이를 차단 또는 변경하는 기능이 추가됩니다. 'IPS'라고 하기도 합니다.

침입 방지 구축에서 시스템이 패킷을 검토할 때:

- 네트워크 분석 정책은 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽을 향후에 평가할 수 있도록 트래픽을 해독하고 전처리하는 방법을 제어합니다.
- 침입 정책은 침입 및 전처리 규칙(집합적으로 침입 규칙이라고도 함)을 사용하여 패턴 기반의 공격에 대한 디코딩된 패킷을 검사합니다. 침입 정책은 변수 집합과 페어링되는데, 이를 통해 네트워크 환경을 올바르게 반영하는 지정된 값을 사용할 수 있습니다.

네트워크 분석과 침입 정책 모두 상위 액세스 제어 정책에 의해 호출되지만 그 시점은 다릅니다. 시스템이 트래픽을 분석하기 때문에, 네트워크 분석(디코딩 및 전처리) 단계는 침입 방지(추가 전처리 및 침입 규칙) 단계보다 이전에 또는 별도로 발생합니다. 네트워크 분석 및 침입 정책은 폭넓고 심층적인 패킷 검사를 제공합니다. 이 둘을 함께 사용하면 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성을 위협할 수 있는 네트워크 트래픽을 탐지하고 알리고 방지할 수 있습니다.

시스템에서는 상호 보완하고 함께 작동하는 비슷한 이름의 여러 네트워크 분석 및 침입 정책(예: Balanced Security and Connectivity)을 제공합니다. 시스템이 제공하는 정책을 사용하면 Cisco Talos Intelligence Group(Talos)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 검사기 규칙 상태뿐 아니라 검사기의 초기 구성과 기타 고급 설정을 제공합니다.

또한 사용자 지정 네트워크 분석 및 침입 정책을 만들 수 있습니다. 사용자 지정 정책의 설정을 조정하여 가장 중요하다고 생각되는 방식으로 트래픽을 검사할 수 있으며, 따라서 매니지드 디바이스의 성능과 디바이스가 생성하는 이벤트에 효과적으로 대응하는 능력 모두를 향상시킬 수 있습니다.

웹 인터페이스에서 유사한 정책 편집기를 사용하여 네트워크 분석 및 침입 정책을 생성, 수정, 저장 및 관리합니다. 정책 유형 중 하나를 수정할 때 탐색 패널이 웹 인터페이스의 왼쪽에 표시되며, 오른쪽에는 다양한 구성 페이지가 표시됩니다.

추가 지원 및 정보는 다음 비디오를 참조하십시오.

- Snort 3 요약 개요
- Snort 3 확장 개요

Snort 검사 엔진

Snort 검사 엔진은 Secure Firewall Threat Defense (이전 명칭: Firepower Threat Defense) 디바이스의 필수 요소입니다. 검사 엔진은 트래픽을 실시간으로 분석하여 심층 패킷 검사를 제공합니다. 네트워크 분석 및 침입 정책은 Snort 검사 엔진의 기능을 활용하여 침입을 탐지하고 보호합니다.

Snort 3

Snort 3는 Snort 검사 엔진의 최신 버전으로 이전 버전의 Snort와 비교하여 크게 개선되었습니다. Snort의 이전 버전은 Snort 2입니다. Snort 3는 더 효율적이며 더 우수한 성능과 확장성을 제공합니다.

Snort 3는 Snort 2에 비해 동일한 리소스로 더 많은 트래픽을 검사하도록 아키텍처가 재설계되었습니다. Snort 3를 사용하면 트래픽 파서를 간단하고 유연하게 삽입할 수 있습니다. 또한 Snort 3의 새로운 규칙 명령문을 통해 규칙을 더 쉽게 작성하고 해당하는 공유 개체 규칙을 볼 수 있습니다.

이 밖에 Snort 3의 중요한 변경 사항은 다음과 같습니다.

- 여러 Snort 인스턴스를 사용하는 Snort 2와 달리 Snort 3는 여러 스레드를 단일 Snort 인스턴스와 연결합니다. 이렇게 하면 메모리가 줄어들고 Snort 다시 로드 시간이 개선되며 더 많은 침입 규칙과 더 큰 네트워크 맵이 지원됩니다. Snort 스레드의 수는 플랫폼에 따라 다르며 각 플랫폼의 Snort 2 인스턴스 수와 동일합니다. 사용량은 거의 투명합니다.

- Threat Defense 별 Snort 버전 - Snort 검사 엔진은 Threat Defense 에 고유하며, Secure Firewall Management Center(이전 명칭: Firepower Management Center)에는 고유하지 않습니다. Management Center에서는 여러 Threat Defense 를 관리할 수 있으며, 각각 Snort 버전 Snort 2 및 Snort 3를 사용합니다. Management Center의 침입 정책은 고유하지만, 시스템은 디바이스의 선택한 검사 엔진에 따라 침입 방지를 위해 Snort 2 또는 Snort 3 버전의 침입 정책을 적용합니다. 디바이스의 검사 엔진에 대한 자세한 내용은 Snort 3 검사 엔진, 21 페이지의 내용을 참조하십시오.
- 디코더 규칙 - 패킷 디코더 규칙은 기본 침입 정책에서만 실행됩니다. 시스템은 다른 정책에서 활성화한 디코더 규칙을 무시합니다.
- 공유 개체 규칙 - Snort 3에서는 일부 공유 개체(SO) 침입 규칙(GID(제너레이터 ID)가 3인 규칙)을 지원하지는 않습니다. 지원되지 않는 활성화된 공유 개체 규칙은 트리거되지 않습니다.
- 보안 인텔리전스를 위한 멀티 레이어 검사 - Snort 2는 멀티 레이어 트래픽에서 2개의 레이어를 검사합니다. Snort 3는 레이어에 관계없이 가장 안쪽 IP 주소를 탐지합니다.
- 플랫폼 지원 - Snort 3는 Threat Defense 7.0 이상이 필요합니다. ASA FirePOWER 또는 NGIPSv에서는 지원되지 않습니다.
- 매니지드 디바이스 - 7.0 버전의 Management Center는 버전 6.4, 6.5, 6.6, 6.7 및 7.0 Snort 2 Threat Defense 와 버전 7.0 Snort 3 Threat Defense 를 동시에 지원할 수 있습니다.
- Snort 버전 전환 시 트래픽 중단 - Snort 버전을 전환하면 트래픽 검사가 중단되고 구축 중에 일부 패킷이 삭제될 수 있습니다.
- 일관된 정책 - 매니지드 Threat Defense 에 활성화된 기본 Snort 엔진 버전에 관계없이 Management Center에 구성된 액세스 제어 정책, 침입 정책 및 네트워크 분석 정책은 정책 적용 시 원활하게 작동합니다. Management Center 7.0 이상 버전의 모든 침입 정책에는 Snort 2 버전과 Snort 3 버전의 두 가지 버전이 있습니다. 침입 정책은 일관적입니다. 즉, 두 가지 버전의 정책(Snort 2 버전 및 Snort 3 버전)이 있더라도 공통 이름, 기본 정책 및 검사 모드를 사용한다는 점에서 일관됩니다. 침입 정책의 Snort 2 버전과 Snort 3 버전은 규칙 설정 측면에서 다를 수 있습니다. 그러나 침입 정책이 디바이스에 적용되면 시스템은 디바이스에서 활성화된 Snort 버전을 자동으로 식별하여 해당 버전에 대해 구성된 규칙 설정을 적용합니다.
- LSP(Lightweight Security Package) - Snort 3 차세대 침입 규칙 및 구성 업데이트를 위해 SRU(Snort 규칙 업데이트)를 교체합니다. 업데이트를 다운로드하면 Snort 3 LSP 및 Snort 2 SRU가 모두 다운로드됩니다.

  Management Center 및 Threat Defense 7.0 이상 버전에서 LSP 업데이트는 새로운 침입 규칙과 업데이트된 침입 규칙 및 검사기 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. Management Center를 6.7 이하 버전에서 7.0 버전으로 업그레이드하면 LSP와 SRU가 모두 지원됩니다. 또한 LSP 업데이트는 시스템 제공 규칙을 삭제하고, 새로운 규칙 범주와 기본 변수를 제공하며, 기본 변수 값을 변경할 수 있습니다. LSP 업데이트에 대한 자세한 내용은 최신 버전의 *Firepower Management Center* 구성 가이드에 있는 침입 규칙 업데이트 항목을 참조하십시오.
- Snort 2와 Snort 3 규칙 및 사전 설정 매핑 - Snort 2와 Snort 3 규칙은 매핑되며, 이 매핑은 시스템에서 제공됩니다. 그러나 이는 일대일 매핑이 아닙니다. 시스템에서 제공하는 침입 기반 정책은 Snort 2 및 Snort 3에 대해 미리 구성되어 있으며, 규칙 세트가 다르더라도 동일한 침입 방지 기능을 제공합니다. Snort 2 및 Snort 3에 대한 시스템 제공 기본 정책은 동일한 침입 방지 설정에 대해

서로 매핑됩니다. 자세한 내용은 Snort 2 및 Snort 3 기본 정책 매핑 보기, 26 페이지를 참조하십시오.

- Snort 2 및 Snort 3 규칙 재정의 동기화 - Threat Defense 를 7.0으로 업그레이드하는 경우 Threat Defense 의 검사 엔진을 Snort 3 버전으로 업그레이드할 수 있습니다. Management Center에서는 Talos에서 제공하는 매핑을 사용하여 침입 정책 내 Snort 2 버전의 기존 규칙에 있는 모든 재정의를 해당 Snort 3 규칙으로 매핑합니다. 그러나 업그레이드 후에 추가 재정의가 수행되거나 버전 7.0의 새 Threat Defense 를 설치한 경우 수동으로 동기화해야 합니다. 자세한 내용은 Snort 2 규칙과 Snort 3 동기화 , 26 페이지를 참고하십시오.
- 사용자 지정 침입 규칙 - Snort 3에서 사용자 지정 침입 규칙을 생성할 수 있습니다. 또한 Snort 2에 대해 존재하는 사용자 지정 침입 규칙을 Snort 3로 가져올 수 있습니다. 자세한 내용은 Snort 3의 사용자 지정 규칙, 47 페이지를 참고하십시오.
- 규칙 그룹 - Management Center에서는 모든 Snort 3 규칙을 규칙 그룹으로 그룹화합니다. 규칙의 논리적 그룹인 규칙 그룹을 사용하면 간편한 관리 인터페이스를 통해 규칙 액세스 가능성과 규칙 탐색을 개선하고 규칙 그룹의 보안 수준을 보다 효과적으로 제어할 수 있습니다.

  Management Center 7.3.0부터는 여러 레벨의 규칙 그룹에 대한 규칙 탐색이 지원되어 보다 유연하고 논리적으로 규칙을 그룹화할 수 있습니다. MITER 프레임워크가 추가되어 MITER 프레임워크를 사용하여 규칙을 탐색할 수 있습니다. MITRE는 규칙 그룹의 또 다른 범주이며 Talos 규칙 그룹의 일부입니다.

참고 MITRE에 대한 자세한 내용은 https://attack.mitre.org를 참조하십시오.

  규칙은 여러 MITRE ATT&CK 규칙 그룹, 규칙 범주 규칙 그룹, 여러 "자산 유형" 규칙 그룹, 악성 코드 캠페인 등과 같은 다양한 규칙 그룹의 일부일 수 있습니다. 사용 가능한 규칙 그룹이 침입 정책 편집기에 나열되며 정책을 개선하도록 선택될 수 있습니다.

  이 다단계 계층 구조를 사용하면 마지막 요소인 "리프 규칙 그룹"까지 이동할 수 있습니다. 이러한 규칙 그룹은 특정 유형의 취약성, 유사한 대상 시스템 또는 유사한 위협 범주 등 서로 관련된 규칙 집합을 포함합니다. 규칙 그룹에는 4개의 보안 레벨이 연결되어 있습니다. 보안 레벨을 변경하거나 규칙 그룹을 추가 또는 제거할 수 있으며, 네트워크에 표시된 트래픽과 일치하는 규칙에 대한 규칙 작업을 변경할 수 있습니다. 이는 보안, 성능 및 오탐 방지 사이의 균형을 유지하기 위해 수행됩니다.

  Snort 3 침입 정책을 편집하려면 Snort 3 침입 정책 편집, 35 페이지의 내용을 참조하십시오.

  침입 이벤트에서의 규칙 그룹 보고에 대해서는 규칙 그룹 보고, 40 페이지의 내용을 참조하십시오.

- Snort 2 엔진과 Snort 3 엔진 간의 전환—Snort 3를 지원하는 Threat Defense 는 Snort 2도 지원할 수 있습니다. Snort 3에서 Snort 2로 전환하는 것은 효율성 측면에서 권장되지 않습니다. 그러나 전환이 필요한 경우 Snort 3 검사 엔진, 21 페이지의 지침을 따르십시오.

중요 Snort 버전을 자유롭게 전환할 수는 있지만 한 버전의 Snort 버전에서 침입 규칙 변경 사항이 다른 버전에서는 자동으로 업데이트되지 않습니다. 한 버전의 Snort에서 규칙에 대한 규칙 작업을 변경하는 경우 Snort 버전을 전환하기 전에 다른 버전의 변경 사항을 복제하십시오. 시스템에서 제공하는 동기화 옵션은 침입 정책의 Snort 2 버전에 대한 변경 사항을 Snort 3 버전으로 동기화하기만 하며 그 반대로는 동기화하지 않습니다.

Snort 2와 Snort 3 비교

Snort 3는 Snort 2에 비해 동일한 리소스로 더 많은 트래픽을 검사하도록 아키텍처가 재설계되었습니다. Snort 3를 사용하면 트래픽 파서를 간단하고 유연하게 삽입할 수 있습니다. 또한 Snort 3의 새로운 규칙 명령문을 통해 규칙을 더 쉽게 작성하고 해당하는 공유 개체 규칙을 볼 수 있습니다.

아래 테이블에는 검사 엔진 기능 측면에서 Snort 2와 Snort 3 버전 간의 차이점이 나와 있습니다.

기능	**Snort 2**	**Snort 3**
패킷 스레드	프로세스당 한 개	프로세스당 개수 제한 없음
구성 메모리 할당	프로세스 수 * *x*GB	총 *x*GB, 패킷에 더 많은 메모리 사용 가능
구성 다시 로드	더 느림	더 빠름, 한 스레드가 여러 코어에 분산되어 처리될 수 있음
규칙 명령문	일관성이 없고 줄 이스케이프 필요	일관된 시스템이며 임의의 공백이 사용됨
규칙 코멘트	코멘트만 나열	#, #begin 및 #end 표시, C 언어 스타일

추가 참조: Firepower에서 Snort 2와 Snort 3의 차이점.

Management Center 매니지드 Threat Defense를 위한 Snort 3의 기능 제한 사항

다음 테이블에는 Management Center 매니지드 Threat Defense 디바이스에 대해서 Snort 2에서는 지원되나 Snort 3에서는 지원되지 않는 기능이 나와 있습니다.

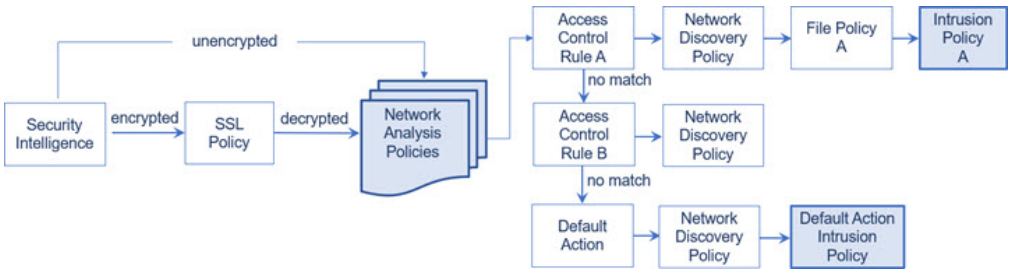
표 *1: Snort 3*의 기능 제한 사항

정책/영역	지원되지 않는 기능
액세스 제어 정책	다음 애플리케이션 설정: • 안전 검색 • YouTube EDU
침입 정책	• 전역 규칙 임계값 • 로깅 구성: • SNMP • Snort 3가 LSP 규칙 업데이트만 지원하므로 SRU 규칙을 업데이트
기타 기능	FQDN 이름을 사용하는 이벤트 로깅

정책이 트래픽에서 침입을 검토하는 방법

시스템이 액세스 제어 배포의 일부로 트래픽을 분석할 때, 네트워크 분석(디코딩 및 전처리) 단계는 침입 방지(침입 규칙 및 고급 설정) 단계보다 이전에 또는 별도로 발생합니다.

다음 다이어그램은 인라인, 침입 방지 및 AMP for Networks 구축에서 트래픽 분석의 순서를 간소화된 형식으로 보여줍니다. 또한 액세스 제어 정책이 다른 정책을 호출하여 트래픽을 검토하는 방법 및 그러한 정책이 호출되는 순서를 보여줍니다. 네트워크 분석 및 침입 정책 선택 단계는 강조 표시됩니다.



인라인 구축(즉, 관련 설정을 라우팅, 스위칭 또는 투명한 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 디바이스에 구축하는 경우)의 경우, 시스템은 예시된 프로세스의 거의 모든 단계에서 추가 검사 없이 트래픽을 차단할 수 있습니다. 보안 인텔리전스, SSL 정책, 네트워크 분석 정책, 파일 정책 및 침입 정책은 모두 트래픽을 삭제 또는 수정할 수 있습니다. 수동으로 패킷을 검사하는 네트워크 검색 정책만으로는 트래픽의 흐름에 영향을 줄 수 없습니다.

마찬가지로 프로세스의 각 단계에서 패킷은 시스템이 이벤트를 생성하도록 할 수 있습니다. 침입 및 프리프로세서 이벤트(침입 이벤트로 총칭)는 패킷 또는 패킷의 내용에 보안 위험이 있음을 나타내는 것입니다.

팁 다이어그램에는 SSL 검사 설정에서 암호화 트래픽의 통과를 허용하는 경우 또는 SSL 검사를 설정하지 않은 경우, 액세스 제어 규칙이 암호화 트래픽을 처리한다는 점이 반영되어 있지 않습니다. 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

단일 연결의 경우, 다이어그램에 나타난 것처럼 시스템은 액세스 제어 규칙에 앞서 네트워크 분석 정책을 선택하지만, 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후에 발생한다는 점에 유의하십시오. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방식에 영향을 주지 않습니다.

복호화, 정규화 및 전처리: 네트워크 분석 정책

프로토콜 차이가 패턴 일치를 불가능하게 할 수 있으므로 디코딩과 전처리가 없으면 시스템은 침입 탐지를 위해 트래픽을 제대로 평가할 수 없습니다. 네트워크 분석 정책은 이러한 트래픽 처리 작업을 제어합니다.

- 보안 인텔리전스에 의해 트래픽이 필터링된 후
- 암호화된 트래픽이 선택적인 SSL 정책에 의해 해독된 후
- 트래픽을 파일 또는 침입 정책으로 검사할 수 있기 전

네트워크 분석 정책은 처리 단계에서 패킷을 제어합니다. 먼저 시스템이 첫 세 개 TCP/IP 레이어를 통해 패킷을 디코딩한 다음, 프로토콜 이상 징후를 표준화하고, 전처리하며, 계속해서 탐지합니다.

- 패킷 디코더는 패킷 헤더 및 페이로드를 검사기에서 쉽게 사용할 수 있는 형식으로, 그리고 추후 침입 규칙에서 쉽게 사용할 수 있는 형식으로 변환합니다. TCP/IP 스택의 각 레이어는 데이터 링크 레이어로 시작하여 계속해서 네트워크 및 전송 레이어를 통해 차례로 디코딩됩니다. 패킷 디코더는 또한 패킷 헤더의 다양하고 변칙적인 작업을 탐지합니다.
- 인라인 배포에서, 인라인 표준화 전처리기는 공격자가 탐지를 우회하는 가능성을 최소화하기 위해 트래픽을 새로 포맷합니다(표준화합니다). 이는 다른 검사기 및 침입 규칙에 따라 패킷이 검사될 수 있도록 준비하고, 시스템이 처리하는 패킷이 사용자 네트워크 호스트에서 수신된 패킷과 동일한지 확인할 수 있도록 지원합니다.
- 다양한 네트워크 및 전송 레이어 검사기는 IP 프래그먼트를 이용한 공격을 탐지하고, 체크섬 검증을 수행하며, TCP와 UDP 세션 전처리를 수행합니다.

  일부 고급 전송 및 네트워크 검사기 설정은 액세스 제어 정책의 대상 디바이스에서 처리된 모든 트래픽에 전역으로 적용된다는 점에 유의하십시오. 이러한 설정은 네트워크 분석 정책보다는 액세스 제어 정책에서 구성합니다.

- 다양한 애플리케이션 레이어 프로토콜 디코더는 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화합니다. 애플리케이션 레이어 프로토콜 인코딩을 정규화함으로써 시스템에서는 데이터가 다르게 표현된 패킷에 동일한 콘텐츠 관련 침입 규칙을 효과적으로 적용하고 의미 있는 결과를 얻을 수 있습니다.
- Modbus, DNP3, CIP 및 s7commplus SCADA 검사기는 트래픽 변칙을 탐지하고 침입 규칙에 데이터를 제공합니다. Supervisory Control(감시 제어) 및 Data Acquisition(데이터 획득. SCADA) 프로토콜은 제조, 생산, 정수 처리, 배전, 공항 및 배송 시스템 등과 같은 산업, 인프라 및 설비의 데이터를 모니터링하고, 제어하며, 획득합니다.
- 여러 검사기가 Back Orifice, 포트 스캔, SYN 플러드 및 기타 속도 기반 공격과 같은 특정 위협을 탐지할 수 있는 기능을 제공합니다.

  침입 정책에서 ASCII 텍스트의 신용카드 번호 및 주민등록번호/사회보장번호 같은 민감한 데이터를 탐지하는 민감한 데이터 검사기를 구성할 수 있습니다.

새로 만든 액세스 제어 정책에서 하나의 기본 네트워크 분석 정책은 동일한 상위 액세스 제어 정책에 의해 호출된 모든 침입 정책에 대한 모든 트래픽에 대해 전처리를 제어합니다. 먼저, 시스템은 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책을 기본값으로 사용하지만, 기타 시스템이 제공하는 네트워크 분석 정책 또는 사용자 지정 네트워크 분석 정책으로 변경할 수 있습니다. 더 복잡한 구축에서 고급 사용자는 일치하는 트래픽을 전처리하는 다양한 맞춤형 네트워크 분석 정책을 할당하여 특정 보안 영역, 네트워크, VLAN에 트래픽 전처리 옵션을 맞출 수 있습니다.

참고 규칙 동작이 **Trust(**신뢰**)**인 액세스 제어 정책과 기록 옵션이 비활성화된 상태에서 작업이 **Fastpath(**단축 경로**)**인 프리필터 규칙의 경우, 플로우 종료 이벤트가 시스템에서 여전히 생성됩니다. 이벤트는 Management Center 이벤트 페이지에 표시되지 않습니다.

액세스 제어 규칙: 침입 정책 선택

초기 전처리 후, (있는 경우) 액세스 제어 규칙이 트래픽을 평가합니다. 대부분의 경우 패킷과 일치하는 첫 번째 액세스 제어 규칙이 트래픽을 처리하는 규칙입니다. 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용할 수 있습니다.

액세스 제어 규칙을 통해 트래픽을 허용할 경우, 시스템은 트래픽에서 데이터 검색, 악성코드, 금지 파일 및 침입을 순서대로 검사할 수 있습니다. 액세스 제어 규칙과 일치하지 않는 트래픽은 검색 데이터와 침입을 검사할 수 있는 액세스 제어 정책의 기본 작업에 의해 처리됩니다.

참고 어느 네트워크 분석 정책이 패킷을 전처리하는지에 상관없이 모든 패킷은 구성된 액세스 제어 규칙에 일치되며 따라서 하향식 순서로 침입 정책에 의한 잠재적 검사의 대상이 됩니다.

정책이 트래픽에서 침입을 검토하는 방법, 6 페이지의 다이어그램은 다음과 같이 인라인, 침입 방지 및 AMP for Networks 구축에서 디바이스를 통한 트래픽 플로우를 보여줍니다.

- Access Control Rule A는 일치하는 트래픽의 진행을 허용합니다. 그런 다음 트래픽은 네트워크 검색 정책에 의해 검색 데이터가, File Policy A에 의해 금지 파일 및 악성코드가 검사된 다음 Intrusion Policy A에 의해 침입이 검사됩니다.
- Access Control Rule B 역시 일치하는 트래픽을 허용합니다. 그러나 이 시나리오에서는 트래픽에서 침입(또는 파일이나 악성코드)이 검사되지 않으므로 규칙과 연결된 침입 또는 파일 정책이 없습니다. 기본적으로 진행을 허용하는 트래픽은 네트워크 검색 정책에 의해 검사되며 이것은 구성할 필요가 없습니다.
- 이 시나리오에서 액세스 제어 정책의 기본 작업은 일치하는 트래픽을 허용하는 것입니다. 다음으로 트래픽은 네트워크 검색 정책으로 그리고 침입 정책의 검사를 받습니다. 침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 때 다른 침입 정책을 사용할 수 있습니다(그러나 반드시 그렇게 해야 할 필요는 없음).

시스템은 차단된 트래픽 또는 신뢰할 수 있는 트래픽은 검사하지 않으므로 다이어그램의 예에는 차단 또는 신뢰 규칙이 포함되어 있지 않습니다.

침입 검사: 침입 정책, 규칙 및 변수 집합

침입 방지는 트래픽이 목적지로 들어가기 전 시스템의 최후의 방어선으로 사용할 수 있습니다. 침입 정책은 보안 위반 확인을 위해 시스템이 인라인 배포에서 트래픽을 검사하는 방식을 제어하며, 악성 트래픽을 차단하거나 변경할 수 있습니다. 침입 정책의 주요 기능은 어느 침입 및 전처리기 규칙이 활성화되는지와 이들이 구성되는 방식을 관리하는 것입니다.

침입 및 검사기 규칙

침입 규칙은 네트워크의 취약성을 이용하려는 시도를 탐지하는 키워드 및 논쟁의 지정된 집합이며, 시스템은 침입 규칙을 사용하여 네트워크 트래픽을 분석하고, 규칙의 기준과 일치하는지를 확인합니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하며, 패킷 데이터가 규칙에 지정된 모든 조건에 일치하는 경우 규칙이 트리거됩니다.

시스템에는 Cisco Talos(Talos Intelligence Group)에서 생성한 다음 유형의 규칙이 포함되어 있습니다.

- 공유 개체 침입 규칙. 이는 컴파일된 것이며 수정할 수 없습니다(소스 및 대상 포트, IP 주소와 같은 규칙 헤더 정보 제외)
- 표준 텍스트 침입 규칙. 이는 규칙의 새 사용자 지정 인스턴스로 저장되며 수정할 수 있습니다.
- 검사기 규칙(네트워크 분석 정책에서 검사기 및 패킷 디코더 탐지 옵션과 관련된 규칙). 검사기 규칙을 복사하거나 수정할 수 없습니다. 대부분의 검사기 규칙은 기본적으로 비활성화되어 있으며, 검사기를 사용하여 이벤트를 생성하고 인라인 구축에서 문제가 되는 패킷을 삭제하려면 활성화해야 합니다.

시스템이 침입 정책에 따라 패킷을 처리할 때, 먼저 규칙 최적화기가 다음과 같은 기준에 근거하여 하위 집합 내 모든 활성화된 규칙을 분류합니다. 전송 레이어, 애플리케이션 프로토콜, 보호된 네트워크로 오가는 방향 등. 다음으로, 침입 규칙 엔진은 각 패킷에 적용하기 위해 적절한 규칙 하위 집합을 선택합니다. 마지막으로 다중 규칙 검색 엔진은 세 가지 검색 유형을 사용하여 트래픽이 규칙과 일치하는지 확인합니다.

- 프로토콜 필드 검색은 애플리케이션 프로토콜 내 특정 필드에서 일치 항목을 검색합니다.
- 일반적인 콘텐츠 검색은 패킷 페이로드의 ASCII 또는 이진 바이트 일치 항목을 검색합니다.
- 패킷 이상 징후 검색은 특정 내용을 포함하기보다는 잘 알려진 프로토콜을 위반하는 패킷 헤더 및 페이로드를 검색합니다.

사용자 지정 침입 정책에서 규칙을 활성화 및 비활성화하고 사용자 고유의 표준 텍스트 규칙을 작성 및 추가하여 탐지를 설정할 수 있습니다. Cisco 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결할 수도 있습니다.

참고 차단 규칙에 대해 특정 트래픽을 처리하기에 패킷이 부족한 경우 시스템은 다른 규칙에 대해 나머지 트래픽을 계속 평가합니다. 나머지 트래픽 중 하나라도 차단으로 설정된 규칙과 일치하면 세션이 차단됩니다. 그러나 시스템이 통과할 나머지 트래픽을 분석하는 경우 완전한 패킷 부족으로 해당 규칙에 대해 트래픽 상태가 보류 중으로 표시됩니다.

변수 집합

시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 변수 집합을 사용합니다. 집합 내 대부분의 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.

시스템은 단일 기본 변수 집합을 제공하는데, 이는 미리 정의된 기본 변수로 구성되어 있습니다. 대부분의 시스템이 제공하는 공유 개체 규칙과 표준 텍스트 규칙은 미리 정의된 이러한 기본 변수를 사용하여 네트워크와 포트 번호를 정의합니다. 예를 들어, 대부분의 규칙은 `$HOME_NET` 변수를 사용하여 보호된 네트워크를 지정하고 `$EXTERNAL_NET` 변수를 사용하여 보호되지 않은(또는 외부) 네트워크를 지정합니다. 또한, 전문 규칙은 종종 미리 정의된 다른 변수를 사용합니다. 예를 들어, 웹 서버에 대한 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

팁 시스템에서 제공한 침입 정책을 사용하는 경우에도 Cisco는 기본 변수 집합의 주요 기본 변수를 수정할 것을 강력하게 권장합니다. 올바르게 네트워크 환경을 반영하는 변수를 사용할 때, 처리는 최적화되고 시스템은 의심스러운 활동에 대해 관련 시스템을 모니터링할 수 있습니다. 고급 사용자는 하나 이상의 사용자 지정 침입 정책으로 페어링을 위한 사용자 지정 변수 집합을 만들고 사용할 수 있습니다.

중요 사용자 지정 변수 집합을 생성하는 경우 사용자 지정 변수 집합 이름의 첫 번째 문자로 숫자를 사용하지 마십시오(예: 3Snort). 이렇게 하면 Management Center의 Threat Defense 방화벽에 구성을 구축할 때 Snort 3 검증이 실패합니다.

침입 이벤트 생성

시스템은 가능한 침입을 식별하면 침입 또는 전처리기 이벤트(총칭하여 침입 이벤트라고도 함)를 생성합니다. 매니지드 디바이스는 Management Center에 자체 이벤트를 전송합니다. 여기서는 집계된 데이터를 보고 네트워크 자산에 대한 공격을 더 잘 이해할 수 있습니다. 인라인 구축에서 매니지드 디바이스는 유해한 것으로 알려진 패킷을 삭제 또는 교체할 수도 있습니다.

데이터베이스의 각 침입 이벤트는 이벤트 헤더를 포함하며, 이벤트 이름 및 분류에 관한 정보를 포함합니다. 여기에는 소스 및 대상 IP 주소, 포트, 이벤트를 생성한 프로세스, 이벤트의 날짜 및 시간, 그리고 공격의 출처 및 공격 대상에 대한 컨텍스트 관련 정보 등이 있습니다. 패킷 기반 이벤트의 경우, 시스템은 또한 해독된 패킷 헤더 및 패킷의 페이로드 또는 이벤트를 시작한 패킷의 복사본을 로깅합니다.

패킷 디코더, 전처리기 및 침입 규칙 엔진은 모두 시스템이 이벤트를 생성하도록 할 수 있습니다. 예를 들면 다음과 같습니다.

- (네트워크 분석 정책에서 구성된) 패킷 디코더가 어떤 옵션 또는 페이로드도 없는 IP 데이터그램의 크기인 20바이트보다 작은 IP 패킷을 수신한 경우, 디코더는 이를 이상 트래픽으로 해석합니다. 나중에 패킷을 검토하는 침입 정책에서 관련 디코더 규칙이 활성화될 경우 시스템은 검사기 이벤트를 생성합니다.
- IP 디프래그먼트화 검사기에 중복되는 일련의 IP 프래그먼트가 발생할 경우 검사기는 이를 잠재적인 공격으로 해석하며, 관련 검사기 규칙이 활성화된 경우 시스템은 검사기 이벤트를 생성합니다.
- 패킷에 의해 트리거될 때 침입 이벤트를 생성할 수 있도록 침입 규칙 엔진 내에서 대부분의 표준 텍스트 규칙 및 공유 개체 규칙이 작성됩니다.

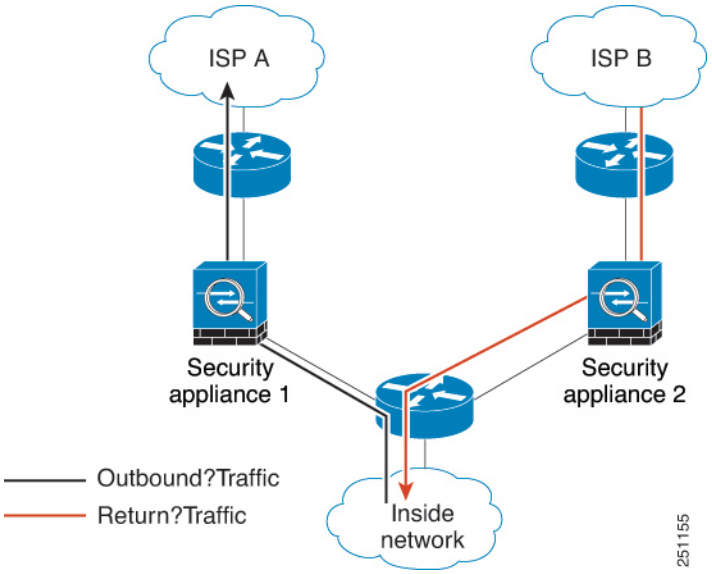
데이터베이스에 침입 이벤트가 누적됨에 따라 잠재적인 공격의 분석을 시작할 수 있습니다. 시스템은 침입 이벤트를 검토하고 네트워크 환경 및 보안 정책의 컨텍스트에서 중요성을 띠는지 여부를 평가하는 데 필요한 도구를 제공합니다.

Snort에서 비대칭 플로우 검사

비대칭 라우팅을 사용하는 인라인 구축에서 단방향 트래픽에 대한 Snort의 제한된 가시성으로 인해 패킷 표준화가 손상됩니다. Snort는 보이지 않는 플로우 방향에서 윈도우 크기 조정 또는 최대 세그먼트 크기(MSS)와 같은 TCP 핸드셰이크(Handshake) 매개변수를 고려할 수 없으므로 호스트가 많은 양의 패킷을 수신하게 될 수 있습니다.

다음 그림에서는 두 디바이스 모두 Snort 엔진을 실행 중입니다. 그러나 엔진에서는 전체 트래픽 플로우를 관찰하지 않습니다. 플로우의 TCP 3방향 핸드셰이크(Handshake) 가 완전히 캡처되지 않아 적용 가능한 표준화 유형이 제한됩니다. 그러나 다른 유효한 표준화는 Snort 엔진에 표시되는 플로우 측에서 수행됩니다.

그림 *1:* 비대칭 라우팅



비대칭 라우팅이 있는 환경에서 Snort는 추가 설정 없이도 동적 상황에 맞게 원활하게 조정됩니다. 플로우 패턴에 따라 작업을 동적으로 조정합니다. 비대칭 트래픽은 방화벽 효율성에 영향을 미칠 수 있으므로 최적의 선택이 아닐 수 있습니다. 그러나 Snort 는 필요한 경우 이러한 구축을 지원하도록 설계되었습니다.

시스템 제공 및 맞춤형 네트워크 분석 및 침입 정책

새로운 액세스 제어 정책을 생성하는 것이 시스템을 사용하여 트래픽 플로우를 관리하는 첫 과정 중 하나입니다. 기본적으로, 새로 만든 액세스 제어 정책은 트래픽을 검토하기 위해 시스템 제공 네트워크 분석 및 침입 정책을 호출합니다.

다음 다이어그램은 인라인 침입 방지 배포에서 새로 만든 액세스 제어 정책이 트래픽을 초반에 처리하는 방식을 보여줍니다. 전처리 및 침입 방지 단계는 강조 표시됩니다.

다음 방식을 참고하십시오.

- 기본 네트워크 분석 정책이 액세스 제어 정책에서 처리된 모든 트래픽의 전처리를 제어하는 방식. 초기에는 시스템이 제공한 *Balanced Security and Connectivity(*균형 잡힌 보안 및 연결성*)* 네트워크 분석 정책이 기본값입니다.
- 액세스 제어 정책의 기본 작업은 시스템이 제공한 *Balanced Security and Connectivity(*균형 잡힌 보안 및 연결성*)*에 의해 결정된 대로 모든 비 악성 트래픽을 허용합니다. 기본 작업에서 트래픽 통과를 허용하므로 침입 정책이 악성 트래픽을 검사하고 잠재적으로 차단하기 전에 검색 기능이 트래픽에서 호스트, 애플리케이션, 사용자 데이터를 검사할 수 있습니다.

- 정책은 기본 보안 인텔리전스 옵션(전역 차단 및 차단 금지 목록)을 사용하고, SSL 정책 내에서 암호화된 트래픽을 해독하지 않으며, 액세스 제어 규칙을 사용하여 네트워크 트래픽의 특수 처리 및 검사를 수행하지 않습니다.

침입 방지 배포를 조정하기 위해 취할 수 있는 간단한 조치는 시스템 제공 네트워크 분석 및 침입 정책의 서로 다른 집합을 기본값으로 사용하는 것입니다. Cisco는 시스템에서 이러한 정책의 여러 쌍을 제공합니다.

또는, 사용자 지정 정책을 생성하고 사용하여 침입 방지 배포를 맞춤화할 수 있습니다. 검사기 옵션, 침입 규칙 및 이 정책에 구성된 기타 고급 설정으로 네트워크의 보안 요구를 해결할 수 없는 경우가 있을 수 있습니다. 네트워크 분석 및 침입 정책을 설정하여 시스템이 침입 탐지를 위해 네트워크에서 트래픽을 처리하고 검사하는 방식을 매우 세부적으로 구성할 수 있습니다.

시스템 제공 네트워크 분석 및 침입 정책

Cisco는 시스템에서 네트워크 분석 정책과 침입 정책의 여러 쌍을 제공합니다. 시스템이 제공하는 네트워크 분석 및 침입 정책을 사용하여 Cisco Talos(Talos Intelligence Group)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 검사기 규칙 상태뿐 아니라 검사기의 초기 구성과 기타 고급 설정을 제공합니다.

모든 네트워크 프로파일, 트래픽 혼합 또는 방어 태세를 포괄하는 시스템 제공 정책은 없습니다. 각각은 잘 조정된 방어 정책의 시작점을 제공하는 일반적인 사례와 네트워크 설정을 다룹니다. 시스템에서 제공하는 정책을 그대로 사용해도 되지만 Cisco는 사용자의 네트워크에 맞게 조정하는 맞춤형 정책의 기반으로 사용할 것을 강력하게 권장합니다.

팁 시스템에서 제공한 네트워크 분석 및 침입 정책을 사용하고 있는 경우에도 자신의 네트워크 환경을 정확하게 반영할 수 있도록 시스템의 침입 변수를 구성해야 합니다. 최소한 기본값 집합의 주요 기본 변수는 수정하시기 바랍니다.

새로운 취약성이 알려지면 Talos에서 LSP(*Lightweight Security Package*)라고 하는 침입 규칙 업데이트를 릴리스합니다. 이 규칙 업데이트는 모든 시스템 제공 네트워크 분석 또는 침입 정책을 수정할 수 있고 새롭게 업데이트된 침입 규칙 및 검사기 규칙, 기존 규칙을 위한 수정된 상태, 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 업데이트가 구축에 영향을 미치는 경우, 웹 인터페이스에는 영향을 받는 침입 및 네트워크 분석 정책은 물론 해당 상위 액세스 제어 정책도 최신이 아닌 것으로 표시됩니다. 변경 사항이 적용되려면 업데이트된 정책을 다시 구축해야 합니다.

편의상 규칙 업데이트를 구성하여 영향을 받는 침입 정책을 단독으로 또는 영향을 받는 액세스 제어 정책과 조합하여 자동으로 다시 구축할 수 있습니다. 이를 통해 쉽고 자동적으로 사용자 배포를 최신 상태로 유지하여 최근 발견된 침입 및 익스플로잇으로부터 보호할 수 있습니다.

전처리 설정을 최신으로 유지하려면 반드시 액세스 제어 정책을 다시 구축해야 합니다. 그러면 현재 실행 중인 것과 다른 모든 관련 SSL, 네트워크 분석 및 파일 정책이 다시 적용되며, 고급 전처리 및 성능 옵션의 기본값도 업데이트할 수 있습니다.

Cisco는 시스템에서 다음 네트워크 분석 및 침입 정책을 제공합니다.

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

이 정책은 속도 및 탐지 모두에 구축됩니다. 이들은 함께 사용되며, 대다수 조직 및 배포 유형을 위해 좋은 시작점의 역할을 합니다. 시스템은 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 정책 및 설정을 대부분의 경우 기본값으로 사용합니다.

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

이 정책은 (모든 리소스에 접근할 수 있는) 연결성이 네트워크 인프라 보안에 우선하는 조직을 위해 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

이 정책은 네트워크 인프라 보안이 사용자 편의에 우선하는 조직을 위해 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) 정책보다 네트워크 인프라 보안이 더 강조되는 조직에 구축되며, 운영에 더 큰 영향을 미칠 수 있습니다. 예를 들어 이 침입 정책에서는 악성코드, 익스플로잇 킷, 오래된 일반적인 취약성, 통제되지 않은 알려진 익스플로잇 등 다수의 위협 범주에서 규칙을 활성화합니다.

No Rules Active(활성 규칙 불가**)** 침입 정책

No Rules Active(활성 규칙 불가) 침입 정책에서는 모든 침입 규칙 및 침입 규칙 임계값을 제외한 모든 고급 설정이 비활성화됩니다. 이 정책은 다른 시스템 제공 정책 중 하나에서 활성화된 규칙에 근거를 두는 것을 대신하여 사용자 고유의 침입 정책 생성을 원할 경우 시작점이 됩니다.

참고 선택한 시스템 제공 기본 정책에 따라 정책 설정은 달라집니다. 정책 설정을 보려면 정책 옆에 있는 **Edit(**편집**)** 아이콘을 클릭하고 **Base Policy(**기본 정책**)** 드롭다운 상자를 클릭합니다.

맞춤형 네트워크 분석 및 침입 정책의 이점

시스템 제공 네트워크 분석 및 침입 정책에 구성된 검사기 옵션, 침입 규칙 및 기타 고급 설정으로 조직의 보안 요구가 충분히 해결되지 않을 수도 있습니다.

사용자 지정 정책을 구축하는 것은 사용자 환경에서 시스템의 성능을 개선할 수 있으며, 사용자 네트워크에서 일어나는 악의적인 트래픽 및 정책 위반을 집중적으로 살펴볼 수 있도록 할 수 있습니다. 사용자 지정 정책을 생성하고 설정함에 따라 사용자는 시스템이 침입 탐지를 위해 네트워크에서 트래픽을 처리하고 검사하는 방식을 매우 세부적으로 구성할 수 있습니다.

모든 사용자 정책에는 기본 정책이 있으며, 이는 기본 레이어라고도 하는데, 정책의 모든 구성에 대한 기본 설정을 정의합니다. 레이어는 여러 네트워크 분석 또는 침입 정책을 효율적으로 관리하는 데 사용할 수 있는 구성 요소입니다.

대부분의 경우, 사용자 지정 정책은 시스템 제공 정책을 기반으로 하지만, 다른 사용자 지정 정책을 사용할 수 있습니다. 하지만, 사용자 지정 정책은 시스템 제공 정책을 정책 체인의 궁극적인 기반으로 둡니다. 사용자 지정 정책을 사용자 기반으로 사용하는 경우 규칙 업데이트는 시스템 제공 정책을 변경할 수 있으며, 규칙 업데이트를 가져오는 것이 사용자에게 영향을 미칠 수 있습니다. 규칙 업데이트가 구축에 영향을 미치는 경우, 웹 인터페이스는 영향받는 정책을 최신 상태가 아닌 것으로 표시합니다.

맞춤형 네트워크 분석 정책의 이점

기본적으로 하나의 네트워크 분석 정책이 액세스 제어 정책에서 다루는 모든 암호화되지 않은 트래픽을 전처리합니다. 이는 모든 패킷이 나중에 이들을 검토하는 침입 정책(따라서 침입 규칙 집합)에 관계없이 동일한 설정에 따라 디코딩 및 전처리된다는 것을 의미합니다.

초기에는 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본값입니다. 전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다.

사용 가능한 조정 옵션은 검사기에 따라 다르지만, 다음과 같은 몇 가지 방법으로 검사기와 디코더를 조정할 수 있습니다.

- 모니터링하는 트래픽에 적용하지 않는 검사기를 비활성화할 수 있습니다. 예를 들어, HTTP Inspect(HTTP 검사) 검사기는 HTTP 트래픽을 표준화합니다. 네트워크에 Microsoft IIS(Internet Information Services)를 사용하는 웹 서버가 없는 것이 확실하면 IIS 관련 트래픽을 검색하는 검사기 옵션을 비활성화하여 시스템 처리 오버헤드를 줄일 수 있습니다.

참고 사용자 지정 네트워크 분석 정책에서 검사기를 비활성화했지만 이후에 시스템이 활성화된 침입 또는 검사기 규칙에 대해 패킷을 평가하기 위해 해당 검사기를 사용해야 하는 경우, 네트워크 분석 정책 웹 인터페이스에서 검사기가 비활성화되어 있더라도 시스템은 검사기를 자동으로 활성화하여 사용합니다.

- 적절하다고 판단되는 경우, 포트를 지정하여 특정 검사기 활동에 집중합니다. 예를 들어 DNS 서버 응답이나 암호화된 SSL 세션을 모니터링하기 위한 추가 포트 또는 텔넷, HTTP 및 RPC 트래픽을 해독하는 포트를 식별할 수 있습니다.

복합적인 배포를 사용하는 고급 사용자의 경우, 다수의 네트워크 분석 정책을 생성할 수 있는데, 각각은 트래픽을 다르게 전처리하기 위해 조정된 것입니다. 그런 다음 이러한 정책을 사용하도록 시스템을 구성하여 서로 다른 보안 영역, 네트워크 또는 VLAN을 사용하는 트래픽의 전처리를 제어할 수 있습니다 (ASA FirePOWER 모듈은 VLAN에 의한 전처리를 제한할 수 없는 점에 유의하십시오.)

참고 사용자 지정 네트워크 분석 정책, 특히 다중 네트워크 분석 정책을 사용하여 전처리를 조작하는 것은 고급 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 반드시 주의하여 서로 보완하는 단일 패킷을 검토하는 네트워크 분석 및 침입 정책을 허용해야 합니다.

사용자 지정 침입 정책의 이점

처음에 침입 방지를 수행하도록 구성된 새로 만든 액세스 제어 정책에서 기본 작업은 모든 트래픽을 허용하지만, 먼저 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책으로 이를 검사합니다. 액세스 제어 규칙을 추가하거나 기본 작업을 변경하지 않는 한 모든 트래픽은 해당 침입 정책에 의해 검사됩니다.

침입 방지 배포를 사용자 정의하려면 여러 침입 정책을 만들 수 있는데, 각각은 트래픽을 검사하기 위해 서로 다르게 지정됩니다. 다음으로 어떤 정책이 어떤 트래픽을 검사하는지를 지정하는 규칙으로 액세스 제어 정책을 구성합니다. 액세스 제어 규칙은 간단하거나 복잡할 수 있으며, 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL 및 사용자를 포함하는 여러 기준을 사용하여 트래픽과 일치시키고 검사합니다.

침입 정책의 주요 기능은 다음과 같이 어떤 침입 및 검사기 규칙을 활성화할지 그리고 이러한 규칙을 어떻게 구성할지를 관리하는 것입니다.

- 각 침입 정책 내에서 사용자의 환경에 적용 가능한 모든 규칙이 활성화되어 있음을 확인해야 하며, 환경에 적용할 수 없는 규칙은 비활성화하여 성능을 향상시켜야 합니다. 악의적인 패킷을 삭제하거나 수정할 규칙을 지정할 수 있습니다.
- Cisco 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결할 수 있습니다.
- 필요에 따라 기존 규칙을 수정하고 새 표준 텍스트 규칙을 작성하여 새로운 익스플로잇을 포착하거나 보안 정책을 적용할 수 있습니다.

침입 정책에 만들 수 있는 다른 사용자 지정은 다음을 포함합니다.

- 중요한 데이터 전처리기는 신용 카드 번호 및 ASCII 문자로 표시된 Social Security numbers(사회보장 번호)와 같은 중요한 데이터를 탐지합니다. Back Orifice 공격, 몇몇 포트스캔 유형 및 과도한 트래픽으로 네트워크의 무력화를 시도하는 속도 기반 공격 등 특정 위협을 탐지하는 그 밖의 검사기는 네트워크 분석 정책에서 구성됩니다.
- 전역 임계값은 침입 규칙과 일치하는 트래픽이 얼마나 많이 지정된 기간 내 특정 주소 또는 주소 범위를 대상으로 하거나 특정 주소 또는 주소 범위로부터 발생하는지에 근거하여 시스템이 이벤트를 생성하도록 합니다. 이를 통해 많은 수의 이벤트로 인해 시스템이 마비되는 것을 방지할 수 있습니다.
- 침입 이벤트 알림을 차단하고 개별 규칙 또는 전체 침입 정책에 대한 임계값을 설정하여 많은 수의 이벤트로 인해 시스템이 마비되는 것을 방지할 수 있습니다.
- 웹 인터페이스 내 침입 이벤트다양한 보기 이외에도, syslog 기능에 로깅을 활성화하거나 SNMP 트랩 서버에 이벤트 데이터를 보낼 수 있습니다. 정책별로 침입 이벤트 알림 제한을 지정하고, 외부 로깅 기능에 침입 이벤트 알림을 설정하며, 침입 이벤트에 외부 응답을 구성할 수 있습니다.

이러한 정책 단위 경고 컨피그레이션 외에도 각 규칙이나 규칙 그룹에 대해 침입 이벤트의 이메일 경고를 전역적으로 활성화 또는 비활성화할 수 있습니다. 어떤 침입 정책이 패킷을 처리하는지와 상관없이 이메일 경고 설정이 사용됩니다.

사용자 지정 정책의 한계

전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 반드시 주의하여 구성이 서로 보완하는 단일 패킷을 처리하고 검토하는 네트워크 분석 및 침입 정책을 허용할 수 있도록 해야 합니다.

기본적으로, 시스템은 단일 액세스 제어 정책을 사용하여 매니지드 디바이스에서 처리된 모든 트래픽을 전처리하도록 하나의 네트워크 분석 정책을 사용합니다. 다음 다이어그램은 인라인 침입 방지 배포에서 새로 만든 액세스 제어 정책이 트래픽을 초반에 처리하는 방식을 보여줍니다. 전처리 및 침입 방지 단계는 강조 표시됩니다.

기본 네트워크 분석 정책이 액세스 제어 정책에서 처리된 모든 트래픽의 전처리를 제어하는 방식에 유의하십시오. 초기에는 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본값입니다.

전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다. 그러나 사용자 지정 네트워크 분석 정책에서 검사기를 비활성화했지만 시스템이 활성화된 침입 또는 검사기 규칙에 대해 전처리된 패킷을 평가해야 하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 검사기가 비활성화되어 있더라도 시스템은 검사기를 자동으로 활성화하여 사용합니다.

참고 검사기 비활성화를 통한 성능 이점을 얻으려면 침입 정책 중에 해당 검사기를 요구하는 규칙을 활성화한 정책이 없는지 반드시 확인해야 합니다.

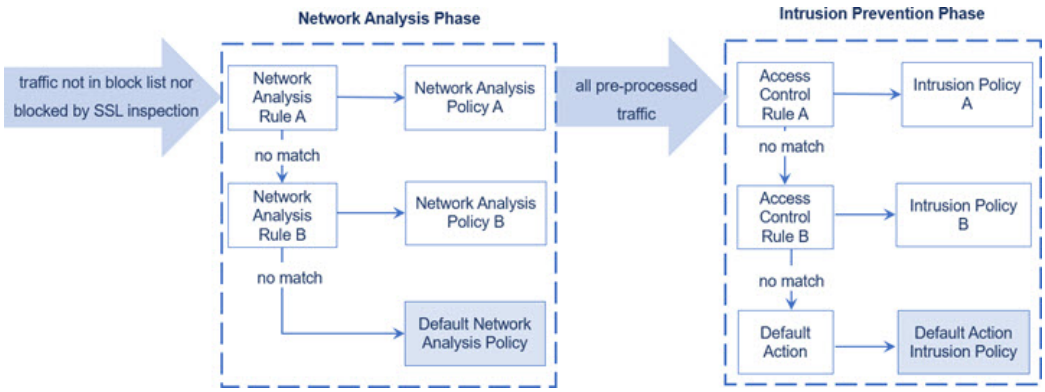
여러 사용자 지정 네트워크 분석 정책을 사용하는 경우 추가 문제가 발생합니다. 복잡한 구축을 수행하는 고급 사용자의 경우, 일치하는 트래픽을 전처리하는 맞춤형 네트워크 분석 정책을 할당하여 특정 보안 영역, 네트워크, VLAN에 맞게 전처리를 조정할 수 있습니다. (ASA FirePOWER는 VLAN에 의한 전처리를 제한할 수 없는 점에 유의하십시오.) 이를 수행하려면, 액세스 제어 정책에 사용자 지정 네트워크 분석 규칙을 추가합니다. 각 규칙에 규칙과 일치하는 트래픽의 전처리를 관리하는 연결된 네트워크 정책 분석이 있습니다.

팁 액세스 제어 정책의 고급 설정으로 네트워크 분석 규칙을 구성합니다. 다른 규칙 유형과는 달리, 네트워크 분석 규칙은 네트워크 분석 정책에 포함되지 않고 네트워크 분석 정책을 호출합니다.

시스템은 규칙 번호로 하향식 순서로 구성된 모든 네트워크 분석 규칙에 패킷을 일치시킵니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다. 이는 사용자에게 트래픽을 전처리하는 데 있어 많은 유연성을 제공하지만, 어느 네트워크 분석 정책이 패킷을 전처리했는지에 상관없이 모든 패킷은 고유의 프로세스에서 순차적으로 액세스 제어 규칙에

일치되므로 침입 정책에 의해 잠재적인 검사에도 일치된다는 점에 유의하십시오. 즉, 특정 네트워크 분석 정책을 통해 패킷을 전처리하면 해당 패킷이 특정 침입 정책으로 검토된다고 보장되지 않습니다. 반드시 신중하게 액세스 제어 정책을 구성하여 특정 패킷을 평가하는 올바른 네트워크 분석 및 침입 정책을 호출하도록 해야 합니다.

다음 다이어그램은 네트워크 분석 정책 (전처리) 선택 단계가 어떻게 해서 침입 방지 (규칙) 단계 전에 또는 별도로 발생하는지를 집중적으로 자세히 보여줍니다. 간소화를 위해 다이어그램은 탐색 및 파일/악성코드 검사 단계를 포함하지 않습니다. 이는 또한 기본 네트워크 분석 및 기본 작업 침입 정책을 강조 표시합니다.



이 시나리오에서 액세스 제어 정책은 두 개의 네트워크 분석 규칙 및 기본 네트워크 분석 정책으로 구성됩니다.

- Network Analysis Rule A(네트워크 분석 규칙 A)는 Network Analysis Policy A(네트워크 분석 규칙 A)로 일치하는 트래픽을 전처리합니다. 나중에 이 트래픽을 Intrusion Policy A(침입 정책 A)로 검사할 수 있습니다.
- Network Analysis Rule B(네트워크 분석 규칙 B)는 Network Analysis Policy B(네트워크 분석 규칙 B)로 일치하는 트래픽을 전처리합니다. 나중에 이 트래픽을 Intrusion Policy B(침입 정책 B)로 검사할 수 있습니다.
- 나머지 모든 트래픽은 기본 네트워크 분석 정책으로 전처리됩니다. 나중에, 이 트래픽을 액세스 제어 정책의 기본 작업과 관련된 침입 정책에 따라 검사할 수 있습니다.

시스템은 트래픽을 전처리한 후, 침입 탐지를 위해 트래픽을 검토할 수 있습니다. 다이어그램은 두 개의 액세스 제어 규칙 및 기본 작업으로 액세스 제어 정책을 보여 줍니다.

- Access Control Rule A(액세스 제어 규칙 A)가 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 Intrusion Policy A(침입 정책 A)로 검사됩니다.
- Access Control Rule B(액세스 제어 규칙 B)가 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 Intrusion Policy B(침입 정책 B)로 검사됩니다.
- 액세스 제어 정책의 기본 작업이 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 기본 작업의 침입 정책에 의해 검사됩니다.

각 패킷의 처리는 네트워크 분석 정책과 침입 정책 쌍에 의해 제어되지만, 시스템이 사용자를 대신하여 쌍을 조정하는 것은 아닙니다. Network Analysis Rule A(네트워크 분석 규칙 A) 및 Access Control

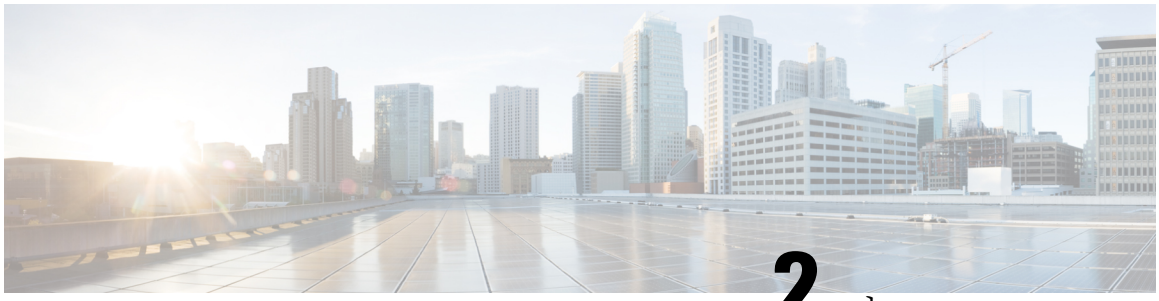
Rule A(액세스 제어 규칙 A)가 동일한 트래픽을 처리하지 않도록 액세스 제어 정책을 잘못 설정한 시나리오를 고려하십시오. 예를 들어, 특정 보안 영역에서 트래픽 처리를 제어하기 위해 페어링된 정책을 의도할 수 있지만 두 규칙의 조건에서 서로 다른 영역을 잘못 사용하는 것입니다. 그러면 트래픽이 잘못 전처리될 수 있습니다. 따라서, 네트워크 분석 규칙 및 사용자 지정 정책을 사용하여 전처리를 조작하는 것은 고급 작업입니다.

단일 연결의 경우, 시스템은 액세스 제어 규칙에 앞서 네트워크 분석 정책을 선택하지만, 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후에 발생한다는 점에 유의하십시오. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방식에 영향을 주지 않습니다.

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.



2 장

Snort 2에서 Snort 3로 마이그레이션

버전 7.0부터, Snort 3은 Management Center에 새로운 Threat Defense 구축에 대해 기본 검사 엔진입니다. 아직 Snort 2 검사 엔진을 사용 중이라면 지금 바로 Snort 3으로 전환하여 탐지 및 성능을 개선합니다.

Threat Defense을 버전 7.2~7.6으로 업그레이드하면 적격 Snort 2 디바이스도 Snort 3으로 업그레이드됩니다. 맞춤형 침입 또는 네트워크 분석 정책을 사용하기 때문에 부적합한 디바이스의 경우 여기에 설명된 대로 수동으로 Snort 3으로 업그레이드합니다.

개별 디바이스를 다시 예전으로 전환할 수는 있지만, 그렇게 해서는 안 됩니다.Snort 2는 향후 릴리스에서 더 이상 사용되지 않으며 결국 Threat Defense 업그레이드할 수 없게 됩니다.

Snort 3 검사 엔진

Snort 3는 버전 7.0 이상의 새로 등록된 Threat Defense 디바이스에 대한 기본 검사 엔진입니다. 그러나 하위 버전의 Threat Defense 디바이스의 경우 Snort 2가 기본 검사 엔진입니다. 매니지드 Threat Defense 디바이스를 버전 7.0 이상으로 업그레이드할 경우 검사 엔진은 Snort 2에 남아 있습니다. 버전 7.0 이상의 업그레이드된 Threat Defense 에서 Snort 3를 사용하려면 명시적으로 활성화해야 합니다. Snort 3가 디바이스의 검사 엔진으로 활성화되면 액세스 제어 정책을 통해 디바이스에 적용된 Snort 3 버전이 활성화되어 디바이스를 통과하는 모든 트래픽에 적용됩니다.

필요한 경우 Snort 버전을 전환할 수 있습니다. Snort 2와 Snort 3 침입 규칙은 매핑되며, 이 매핑은 시스템에서 제공됩니다. 그러나 Snort 2 및 Snort 3에서는 모든 침입 규칙의 일대일 매핑을 찾을 수 없습니다. Snort 2에서 규칙에 대한 규칙 작업을 변경한 경우 Snort 3로 전환하면 해당 변경 사항이 유지되지 않습니다. 변경 사항을 유지하려면 Snort 2를 Snort 3와 동기화해야 합니다. 동기화에 대한 자세한 내용은 Snort 2 규칙과 Snort 3 동기화 , 26 페이지 항목을 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.

Snort 2에서 Snort 3로 마이그레이션하는 방법

Snort 2에서 Snort 3로 마이그레이션하려면 Threat Defense 디바이스의 검사 엔진을 Snort 2에서 Snort 3로 전환해야 합니다.

다음 테이블에는 요구 사항에 따라 Snort 2에서 Snort 3로 디바이스를 마이그레이션하는 작업이 나열되어 있습니다.

단계	작업	절차 링크
1	Sntit 3 활성화	• 개별 디바이스에서 Snort 3 활성화, 23 페이지 • 여러 디바이스에서 Snort 3 활성화, 23 페이지
2	Snort 2 사용자 지정 규칙을 Snort 3로 변환	• 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 25 페이지 • 단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 25 페이지
3	Snort 2 규칙과 Snort 3 동기화	Snort 2 규칙과 Snort 3 동기화 , 26 페이지

Snort 2에서 Snort 3로 마이그레이션하기 위한 사전 요건

다음은 디바이스를 Snort 2에서 Snort 3로 마이그레이션하기 전에 고려해야 할 권장 사전 요건입니다.

- Snort에 대한 실제 지식이 있어야 합니다. Snort 3 아키텍처에 대한 자세한 내용은 Snort 3 도입을 참조하십시오.
- Management Center를 백업합니다. Management Center 백업을 참조하십시오.
- 침입 정책을 백업합니다. 구성 내보내기를 참조하십시오.
- 침입 정책을 복제합니다. 이를 위해서 침입 정책의 복사본을 생성하기 위한 기본 정책으로 기존 정책을 사용할 수 있습니다. **Intrusion Policies**(침입 정책) 페이지에서 **Create Policy**(정책 생성)를 클릭하고 **Base Policy**(기본 정책) 드롭다운 목록에서 기존 침입 정책을 선택합니다.

개별 디바이스에서 Snort 3 활성화

중요 구축 프로세스 중에는 현재 검사 엔진을 종료해야 하므로 일시적인 트래픽 손실이 발생할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 2 디바이스를 클릭하여 디바이스 홈 페이지로 이동합니다.

참고
디바이스가 Snort 2 또는 Snort 3로 나타나 디바이스의 현재 버전을 표시합니다.

단계 3 **Device(**디바이스**)** 탭을 클릭합니다.

단계 4 Inspection Engine(검사 엔진) 섹션에서 **Upgrade(**업그레이드**)**를 클릭합니다.

참고
Snort 3을 비활성화하려면 Inspection Engine(검사 엔진) 섹션에서 **Revert to Snort 2(Snort 2**로 되돌리기**)**를 클릭합니다.

단계 5 **Yes(**예**)**를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, 구성 변경 사항 구축, 28 페이지.

시스템은 구축 프로세스 중에 선택한 Snort 버전과 호환되도록 정책 설정을 변환합니다.

여러 디바이스에서 Snort 3 활성화

여러 디바이스에서 Snort 3를 활성화하려면 모든 필수 Threat Defense 디바이스가 버전 7.0 이상인지 확인하십시오.

중요 구축 프로세스 중에는 현재 검사 엔진을 종료해야 하므로 일시적인 트래픽 손실이 발생할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 2 Snort 3를 활성화하거나 비활성화할 모든 디바이스를 선택합니다.

참고
디바이스가 Snort 2 또는 Snort 3로 나타나 디바이스의 현재 버전을 표시합니다.

단계 3 **Select Bulk Action(**대량 작업 선택**)** 드롭다운 목록을 클릭하고 **Upgrade to Snort 3(Snort 3**로 업그레이드**)**를 선택합니다.

단계 4 **Yes(**예**)**를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, 구성 변경 사항 구축, 28 페이지.

시스템은 구축 프로세스 중에 선택한 Snort 버전과 호환되도록 정책 설정을 변환합니다.

Snort 2 사용자 지정 IPS 규칙을 Snort 3로 변환

서드파티 벤더의 규칙 집합을 사용하는 경우 해당 벤더에 연락하여 규칙이 Snort 3로 성공적으로 변환되는지 확인하거나 기본적으로 Snort 3용으로 작성된 대체 규칙 집합을 얻으십시오. 직접 작성한 사용자 지정 규칙이 있는 경우 변환 전에 Snort 3 규칙을 작성하는 방법을 숙지하여 변환 후 Snort 3 탐지를 최적화하도록 규칙을 업데이트할 수 있습니다. Snort 3의 규칙 작성에 대해 자세히 알아보려면 아래 링크를 참조하십시오.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Snort 3 규칙에 대해 자세히 알아보려는 경우 https://blog.snort.org/에서 다른 블로그를 참조할 수 있습니다.

시스템에서 제공하는 툴을 사용하여 Snort 2 규칙을 Snort 3 규칙으로 변환하려면 다음 절차를 참조하십시오.

- 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 25 페이지
- 단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 25 페이지

중요 Snort 2 NAP(네트워크 분석 정책) 설정은 Snort3에 자동으로 복사될 수 없습니다. NAP 설정은 Snort 3에서 수동으로 복제해야 합니다.

모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환

프로시저

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 3 왼쪽 창에 **All Rules(**모든 규칙**)**가 선택되어 있는지 확인합니다.

단계 4 **Tasks(**작업**)** 드롭다운 목록을 클릭하고 다음을 선택합니다.

- **Convert Snort 2 rules and import(Snort 2** 규칙 변환 및 가져오기**)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.
- **Convert Snort 2 rules and download(Snort 2** 규칙 변환 및 다운로드**)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 로컬 시스템에 다운로드합니다.

단계 5 **OK(**확인**)**를 클릭합니다.

참고

- 앞 단계에서 **Convert and import(**변환 및 가져오기**)**를 선택한 경우 변환된 모든 규칙은 **Local Rules(**로컬 규칙**)** 아래 새로 생성된 규칙 그룹 **All Snort 2 Converted Global(**모든 **Snort 2** 변환 전역**)**에 저장됩니다.
- 앞 단계에서 **Convert and download(**변환 및 다운로드**)**를 선택한 경우 규칙 파일을 로컬에 저장합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 규칙 그룹에 사용자 지정 규칙 추가, 60 페이지의 단계에 따라 업로드할 수 있습니다.

추가 지원 및 정보는 Snort 2 규칙을 Snort 3로 변환 비디오를 참조하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환

프로시저

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

단계 2 **Intrusion Policies(**침입 정책**)** 탭에서 **Show Snort 3 Sync status(Snort 3** 동기화 상태 표시**)**를 클릭합니다.

단계 3 침입 정책의 **Sync(**동기화**)** 아이콘( )을 클릭합니다.

참고
Snort 2 버전과 Snort 3 버전의 침입 정책이 동기화된 경우 **Sync(동기화)** 아이콘이 녹색( )으로 표시됩니다. 이는 변환할 사용자 지정 규칙이 없음을 나타냅니다.

단계 **4** 요약을 읽고 **Custom Rules(사용자 지정 규칙)** 탭을 클릭합니다.

단계 **5** 다음을 선택합니다.

- **Import converted rules to this policy(변환된 규칙을 이 정책으로 가져오기)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.
- **Download converted rules(변환된 규칙 다운로드)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 로컬 시스템에 다운로드합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 업로드 아이콘을 클릭하여 파일을 업로드할 수 있습니다.

단계 **6** **Re-Sync(재동기화)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

Snort 2 및 Snort 3 기본 정책 매핑 보기

프로시저

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

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

단계 **3** **IPS Mapping(IPS 매핑)**을 클릭합니다.

단계 **4** **IPS Policy Mapping(IPS 정책 매핑)** 대화 상자에서 **View Mappings(매핑 보기)**를 클릭하여 Snort 3에서 Snort 2로의 침입 정책 매핑을 확인합니다.

단계 **5** **OK(확인)**를 클릭합니다.

Snort 2 규칙과 Snort 3 동기화

Snort 2 버전 설정과 사용자 지정 규칙이 유지되고 Snort 3에 전달되도록 하기 위해 Management Center는 동기화 기능을 제공합니다. 동기화는 Snort 2 규칙 재정의 설정 및 사용자 지정 규칙에 도움이 됩니다. 이는 지난 몇 개월 또는 몇 년간 Snort 3 버전에서 복제하도록 변경되거나 추가되었을 수 있습니다. 이 유틸리티를 사용하면 Snort 2 버전 정책 구성을 Snort 3 버전과 동기화하여 비슷한 커버리지로 시작할 수 있습니다.

Management Center를 6.7 이하 버전에서 7.0 이상 버전으로 업그레이드하는 경우, 시스템에서 구성을 동기화합니다. Management Center가 7.0 이상 버전인 경우 상위 버전으로 업그레이드할 수 있으며, 업그레이드 중에는 콘텐츠가 동기화되지 않습니다.

디바이스를 Snort 3로 업그레이드하기 전에, Snort 2 버전을 변경하는 경우 이 유틸리티를 통해 Snort 2 버전에서 Snort 3 버전으로의 최신 동기화를 수행하여 유사한 커버리지로 시작할 수 있습니다.

참고 Snort 3로 전환한 후에는 정책의 Snort 3 버전을 독립적으로 관리하고 이 유틸리티를 일반 작업으로 사용하지 않는 것이 좋습니다.

중요

- Snort 2 규칙 재정의와 사용자 지정 규칙이 Snort 3에 복사되기만 하며 그 반대로는 복사되지 않습니다. Snort 2 및 Snort 3에서는 모든 침입 규칙의 일대일 매핑을 찾을 수 없습니다. 다음 절차를 수행할 때 두 버전에 있는 규칙에 대한 규칙 작업의 변경 사항이 동기화됩니다.
- 동기화 시 사용자 지정 규칙 또는 시스템 제공 규칙의 임계값 및 억제 설정이 Snort 2에서 Snort 3로 마이그레이션되지 않습니다.

프로시저

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

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

단계 **3** **Snort 3** 동기화 상태 표시를 클릭합니다.

단계 **4** 동기화되지 않은 침입 정책을 식별합니다.

단계 **5** **Sync(**동기화**)** 아이콘( )을 클릭합니다.

참고
Snort 2 버전과 Snort 3 버전의 침입 정책이 동기화된 경우 **Sync(**동기화**)** 아이콘이 녹색( )으로 표시됩니다.

단계 **6** 요약을 읽고 필요한 경우 요약 사본을 다운로드합니다.

단계 **7** **Re-Sync(**재동기화**)**를 클릭합니다.

참고

- 동기화된 설정은 Snort 3 침입 엔진이 디바이스에 적용되고 구축이 성공한 경우에만 적용됩니다.
- Snort 2 사용자 지정 규칙은 시스템 제공 툴을 사용하여 Snort 3로 변환할 수 있습니다. Snort 2 사용자 지정 규칙이 있는 경우 Custom Rules(사용자 지정 규칙) 탭을 클릭하고 화면의 지침에 따라

규칙을 변환합니다. 자세한 내용은 단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 25 페이지를 참고하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

구성 변경 사항 구축

컨피그레이션을 변경한 후 해당하는 디바이스에 구축합니다.

참고 이 주제에서는 구성 변경 사항 구축과 관련된 기본 단계를 다룹니다. 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에서 구성 변경 사항 구축 주제를 참조하여 단계를 진행하기 전에 변경 사항 구축의 사전 요건과 영향을 파악할 것을 강력하게 권장합니다.

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다.

프로시저

단계 **1** Secure Firewall Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭하고 **Deployment(**구축**)**를 선택합니다.

GUI 페이지에는 **Pending(**보류 중**)** 상태인 오래된 구성이 있는 디바이스가 나열됩니다.

- **Modified By(**수정 주체**)** 열에는 정책 또는 개체를 수정한 사용자가 나열됩니다. 디바이스 목록을 확장하여 각 정책 목록에 대한 정책을 수정한 사용자를 볼 수 있습니다.

  참고
  삭제된 정책 및 개체에 대해서는 사용자 이름이 제공되지 않습니다.

- **Inspect Interruption(**검사 중단**)** 열은 구축 중에 디바이스에서 트래픽 검사 중단이 발생할 수 있는지 여부를 나타냅니다.

  디바이스에 대한 이 열이 비어 있으면 구축 중에 해당 디바이스에서 트래픽 검사가 중단되지 않음을 나타냅니다.

- **Last Modified Time(**마지막 수정 시간**)** 열은 구성 변경을 마지막으로 수행한 시간을 지정합니다.

- **Preview(**미리보기**)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다.
- **Status(**상태**)** 열은 각 구축의 상태를 제공합니다.

단계 **2** 컨피그레이션 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스 별 구성 변경 사항을 보려면 확장 화살표( )을 클릭합니다.

  디바이스 옆의 확인란을 선택하면 디바이스에 대해 수행되고 디바이스 아래에 나열된 모든 변경 사항이 푸시되어 구축됩니다. 그러나 정책 선택( )를 사용하면 구축하지 않고 나머지 변경 사항을 보류하면서 구축할 개별 정책 또는 특정 구성을 선택할 수 있습니다.

  참고

  - **Inspect Interruption(**검사 중단**)** 열의 상태가 (**Yes(**예**)**)인 경우(구축하면 Threat Defense 디바이스에서 검사가 중단되며 트래픽도 중단될 수 있음) 확장된 목록에서 검사 중단( ) 중단을 야기하는 특정 구성을 표시합니다.
  - 인터페이스 그룹, 보안 영역 또는 개체가 변경되면 영향을 받는 디바이스는 Management Center에서 오래된 것으로 표시됩니다. 이러한 변경 사항을 적용하려면 이러한 인터페이스 그룹, 보안 영역 또는 개체가 포함된 정책도 이러한 변경 사항과 함께 구축해야 합니다. 영향을 받는 정책은 Management Center의 **Preview(**미리보기**)** 페이지에서 만료된 것으로 표시됩니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

다음 옵션을 이용할 수 있습니다.

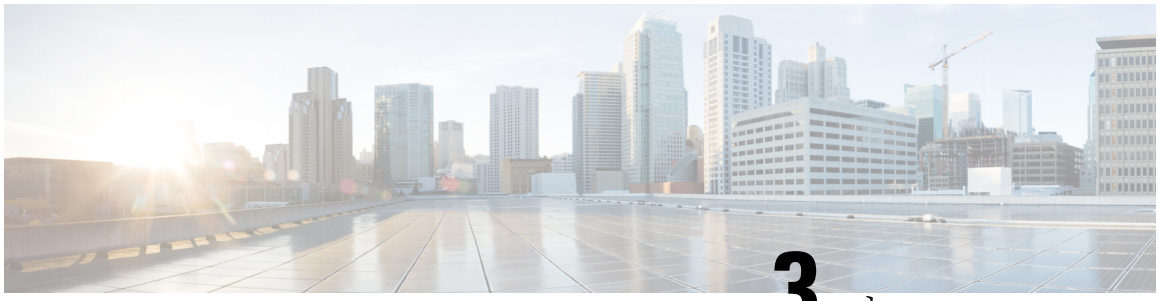
- Deploy(구축) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

다음에 수행할 작업

구축 중에 구축 장애가 발생하는 경우 해당 장애가 트래픽에 영향을 미칠 수 있습니다. 그러나 특정 조건에 따라 달라집니다. 구축에 특정 구성이 변경된 경우 구축 장애로 인해 트래픽이 중단될 수 있습니다. 자세한 내용은 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 구성 변경 사항 구축 주제를 참조하십시오.

I 부

Snort 3의 침입 탐지 및 방지



3 장

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

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

프로시저

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, 35 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.

프로시저

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:9621은 1:962 규칙만 표시하고, SID:9621,9622,9623은 서로 다른 SID의 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:SID로 필터링
  - CVE로 필터링
  - 코멘트로 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 재정의됨 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, 60 페이지를 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 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, 40 페이지의 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, 41 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 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

규칙 그룹 보고

규칙 그룹은 생성된 침입 이벤트에 반영되며, MITER 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*, 7.3*의 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.

프로시저

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 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 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.

프로시저

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

단계 **2** 침입 정책 관리:

- 생성 - **Create Policy(**정책 생성**)**를 클릭합니다(사용자 지정 Snort 3 침입 정책 생성 , 34 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 편집 ( )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, 35 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, 28 페이지 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. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크 상에 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.

프로시저

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.

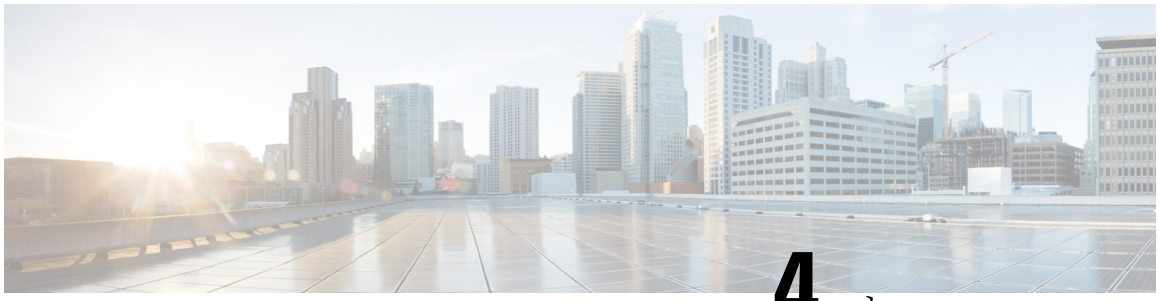
단계 **5** 침입 정책에 관련된 변수 집합을 변경하려면 **Variable Set(**변수 집합**)** 드롭다운 목록에서 값을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.



4 장

규칙을 사용하여 침입 정책 조정

이 장에서는 Snort 3의 사용자 지정 규칙, 침입 규칙 작업, 침입 정책의 침입 이벤트 알림 필터, Snort 2 사용자 지정 규칙을 Snort 3로 변환, 침입 정책에 사용자 지정 규칙이 있는 규칙 그룹 추가에 대한 정보를 제공합니다.

침입 규칙 조정 개요

공유 개체 규칙, 표준 텍스트 규칙, 검사기 규칙의 규칙 상태 및 기타 설정을 구성할 수 있습니다.

규칙 상태를 Alert(알림) 또는 Block(차단)으로 설정하여 규칙을 활성화할 수 있습니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 이벤트를 생성합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다. Block(차단)으로 설정된 규칙이 일치하는 트래픽에 대해 이벤트를 생성하거나 해당 트래픽을 삭제하도록 침입 정책을 설정할 수도 있습니다.

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

침입 규칙 또는 규칙 인수를 사용하려면 비활성화된 검사기가 필요한 경우 네트워크 분석 정책 웹 인터페이스에서 비활성화 상태로 남아 있다고 해도 시스템은 자동으로 검사기를 현재 구성으로 사용한다는 점에 유의하십시오.

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 검사기 중 하나와 연결된 검사기 규칙

다음 표에는 이러한 규칙 유형의 속성이 요약되어 있습니다.

표 *2:* 침입 규칙 유형

유형	**GID(generator ID)**	**SID(Snort ID)**	소스	복사 가능 여부	편집 가능 여부
공유 객체 규칙	3	1000000 미만	Cisco Talos(Talos Intelligence Group)	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 사용자 지정 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.

Talos는 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.

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.

Snort 3의 사용자 지정 규칙

로컬 규칙 파일을 가져와서 사용자 지정 침입 규칙을 생성할 수 있습니다. 규칙 파일은 확장자가 `.txt` 또는 `.rules`일 수 있습니다. 시스템은 규칙 생성에 사용된 방법에 상관없이 맞춤형 규칙을 로컬 규칙 카테고리에 저장합니다. 사용자 지정 규칙은 규칙 그룹에 속해야 합니다. 그런데 한 사용자 지정 규칙이 둘 이상의 그룹에 속할 수도 있습니다.

맞춤형 침입 규칙을 만들 때 시스템은 `GID: SID: Rev`형식의 고유한 규칙 번호를 규칙에 할당합니다. 이 번호의 요소는 다음과 같습니다.

- **GID** - Generator ID입니다. 사용자 지정 규칙의 경우 GID를 지정할 필요가 없습니다. 규칙을 업로드하는 동안 전역 도메인에 있는지 하위 도메인에 있는지에 따라 시스템이 GID를 자동으로 생성합니다. 모든 표준 텍스트 규칙의 경우, 전역 도메인에 있을 때 이 값은 2000입니다.
- **SID** - Snort ID입니다. 규칙이 시스템 규칙의 로컬 규칙인지 여부를 나타냅니다. 새 규칙을 생성할 때 고유한 SID를 규칙에 할당합니다.

  로컬 규칙의 SID 번호는 1000000에서 시작하며 각 새 로컬 규칙의 SID는 1씩 증가합니다.
- **Rev** - 수정 번호입니다. 새 규칙의 경우, 수정 번호는 1입니다. 사용자 지정 규칙을 변경할 때마다 수정 번호가 하나씩 증가합니다.

맞춤형 표준 텍스트 규칙에서 헤더 설정과 규칙 키워드 및 인수를 설정합니다. 규칙 헤더 설정을 사용하면 특정 프로토콜을 사용하며 특정 IP 주소 또는 포트를 오가는 트래픽만을 매칭하도록 규칙의 범위를 좁힐 수 있습니다.

참고

- Snort 3 사용자 지정 규칙은 수정할 수 없습니다. 사용자 지정 규칙의 규칙 텍스트 내 `classtype`에 유효한 분류 메시지가 있는지 확인하십시오. 분류를 사용하지 않거나 잘못된 분류를 사용하여 규칙을 가져온 경우 해당 규칙을 삭제하고 다시 생성합니다.
- Snort 3을 사용하여 사용자 지정 침입 규칙을 생성할 수 있습니다. 그러나 이러한 규칙 조정 및 문제 해결은 현재 제공되지 않습니다.

Snort 3에서 민감한 데이터 탐지

사회 보장 번호, 신용카드 번호, 이메일 같은 민감한 데이터가 인터넷에 고의적으로 또는 실수로 유출될 수 있습니다. 민감한 데이터 탐지는 민감한 데이터 유출 가능성을 탐지하고 이벤트를 생성하는

데 사용됩니다. 상당한 양의 PII(개인 식별 정보) 데이터가 전송되는 경우에만 이벤트가 생성됩니다. 민감한 데이터 탐지 기능은 이벤트 출력에서 PII를 마스킹할 수 있습니다.

sd_pattern 옵션

sd_pattern IPS 옵션을 사용하여 PII를 탐지하고 필터링합니다. 이 정보에는 신용카드 번호, 미국 사회 보장 번호, 전화번호 및 이메일 주소가 포함됩니다. 정규식(regex) 구문을 사용하여 고유한 PII를 정의할 수 있습니다.

sd_pattern 옵션에는 다음과 같은 설정이 있습니다.

- Pattern(패턴) - PDU에서 찾을 정규식을 지정하는 암시적 필수 설정입니다. 정규식(regex)은 PCRE 구문으로 작성해야 합니다.
- Threshold(임계값) - 이벤트를 생성하는 데 필요한 PDU 내 일치 항목의 수를 지정하는 명시적 설정으로, 선택 사항입니다.

  sd_pattern as IPS rule 옵션은 추가 검사기에 대한 요구 사항 없이 Snort에서 사용할 수 있습니다. 규칙 옵션의 구문은 다음과 같습니다.

  ```
  sd_pattern: "<pattern>"[, threshold <count>];
  ```

  예를 들면 다음과 같습니다.

  ```
  sd_pattern:"credit_card", threshold 2;
  ```

기본 제공 패턴

민감한 데이터에 대한 다섯 가지 기본 제공 패턴이 있습니다. "pattern" 설정에서 구축 당시 기본으로 내장된 패턴을 사용하려면 일치시켜야 하는 PII 유형의 이름을 지정해야 하며, 필요한 정규식(regex)으로 이를 대체합니다. PII 이름 및 정규식(regex) 매핑 또는 패턴은 다음과 같이 설명됩니다.

- credit_card—

  ```
  \d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}
  ```

- us_social—

  ```
  [0-8]\d{2}-\d{2}-\d{4}
  ```

- us_social_nodashes—

  ```
  [0-8]\d{8}
  ```

- Email—

  ```
  [a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9]
  (?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?
  ```

- us_phone—

  ```
  (?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})
  ```

PII 이름	패턴
credit_card	`\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}`
us_social	`[0-8]\d{2}-\d{2}-\d{4}`

PII 이름	패턴
us_social_nodashes	`[0-8]\d{8}`
Email	`[a-zA-Z0-9!#$%&'*+\/=?^_`{\|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?`
us_phone	`(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})`

이러한 패턴과 일치하는 데이터 마스킹은 신용카드, 미국 사회 보장 번호, 이메일, 미국 전화번호에 대해 시스템 제공 규칙 또는 구축 당시 기본으로 내장된 패턴을 사용할 때만 작동합니다. 마스킹은 사용자 지정 규칙 또는 사용자 정의 PII 패턴에 대해 작동하지 않습니다. 규칙은 민감한 데이터, gid:13을 위한 LSP(Lightweight Security Package)에서 사용할 수 있습니다. 기본적으로, 이러한 정책은 시스템 제공 정책에서는 활성화되지 않습니다.

LSP의 민감한 데이터 규칙은 구축 당시 기본으로 내장된 모든 패턴에 적용되며 다음 임계값을 갖습니다.

- credit_card: 2
- us_social: 2
- us_social_nodashes: 20
- email: 20
- us_phone: 20

sd_pattern 옵션을 사용하여 맞춤형 규칙을 생성하고 기존 규칙을 수정할 수 있습니다. 이렇게 하려면 Snort 3 침입 정책 인터페이스를 사용합니다.

다음은 사용자 지정 패턴 및 임계값과 함께 sd_pattern이 있는 규칙의 예입니다.

alert tcp (sid: 1000000001; sd_pattern:"[\w-\.]+@([\w-]+\.)+[\w-]{2,4}",threshold 4; msg: "email, threshold 4")

예

다음은 민감한 데이터 탐지를 사용하는 맞춤형 규칙의 예입니다.

구축 당시 기본으로 내장된 패턴이 있는 규칙:

```
alert tcp (
        msg:"SENSITIVE-DATA Email";
        flow:only_stream;
        pkt_data;
        sd_pattern:"email", threshold 5;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000001;
)
```

사용자 지정 패턴이 있는 규칙:

```
alert tcp (
        msg:"SENSITIVE-DATA US phone numbers";
        flow:only_stream;
        file_data;
```

```
        sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})", threshold
2;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000002;
)
```

다음은 구축 당시 기본으로 내장된 민감한 데이터 패턴이 포함된 전체 Snort IPS 규칙의 몇 가지 예입니다.

- alert tcp (sid:1; msg:"Credit Card"; sd_pattern:"credit_card", threshold 2;)
- alert tcp (sid:2; msg:"US Social Number"; sd_pattern:"us_social", threshold 2;)
- alert tcp (sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes", threshold 2;)
- alert tcp (sid:4; msg:"US Phone Number"; sd_pattern:"us_phone", threshold 2;)
- alert tcp (sid:5; msg:"Email"; sd_pattern:"email", threshold 2;)

데이터 마스킹 비활성화는 Secure Firewall Management Center 및 Secure Firewall Device Manager에서 지원되지 않습니다.

침입 정책의 Snort 3 침입 규칙 보기

침입 정책에서 규칙이 표시되는 방법을 조정할 수 있습니다. 또한 규칙 설정, 규칙 문서 및 기타 규칙 사양을 보려면 특정 규칙에 대한 세부 사항을 표시할 수 있습니다.

프로시저

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

단계 **2** 정책 옆의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.

단계 **3** 규칙을 보면서 다음을 수행할 수 있습니다.

- 규칙 필터링
- 규칙 그룹을 선택하여 해당 그룹과 관련된 규칙 확인
- 침입 규칙의 세부 사항 보기
- 규칙 코멘트 보기
- 규칙 문서 보기

이러한 작업 수행에 대한 자세한 내용은 Snort 3 침입 정책 편집, 35 페이지를 참조하십시오.

침입 규칙 작업

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

Cisco Talos(Talos Intelligence Group)는 각 기본 정책에서 각 침입 및 검사기 규칙의 기본 작업을 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 작업을 변경합니다. 규칙 업데이트가 기반 정책을 업데이트하도록 허용하면, 정책을 생성하기 위해 사용한 기본 정책(또는 기반으로 하는 기본 정책)에서 기본 작업이 변경될 때 정책에 있는 규칙의 기본 작업을 변경하는 것도 허용됩니다. 그러나 규칙 작업을 변경한 경우 규칙 업데이트가 변경 사항을 재정의하지 않습니다.

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

침입 규칙 작업 옵션

침입 정책에서 규칙의 작업을 다음 값으로 설정할 수 있습니다.

Alert(알림**)**

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.

Block(차단**)**

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.

Disable(비활성화**)**

시스템이 일치하는 트래픽을 평가하지 않도록 하려면 설정합니다.

참고 **Alert(**알림**)** 또는 **Block(**차단**)** 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 작업 설정

침입 규칙 작업은 정책별로 다릅니다.

프로시저

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

단계 2 수정하려는 정책 옆의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.

팁
이 페이지에는 다음 항목의 총 개수가 표시됩니다.

- 비활성화된 규칙
- Alert(알림)으로 설정된 활성화된 규칙
- Block(차단)으로 설정된 활성화된 규칙
- 재정의된 규칙

단계 3 규칙 작업을 설정할 규칙을 하나 이상 선택합니다.

단계 4 **Rule Action(**규칙 작업**)** 드롭다운 목록에서 규칙 작업 중 하나를 선택합니다. 다양한 규칙 작업에 대한 자세한 내용은 Snort 3 침입 정책 편집, 35 페이지를 참조하십시오.

단계 5 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 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 기록 및 표시하는 횟수를 제한하도록 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 검사기 규칙별 임계값을 설정할 수 있습니다.

침입 이벤트 임계값 구성

임계값을 설정하려면 먼저 임계값 설정 유형을 지정합니다.

표 *3:* 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 *4:* 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 *5:* 임계값 설정 인스턴스/시간 옵션

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

Snort 3의 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.

프로시저

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** 침입 규칙의 Alert Configuration(알림 구성) 열에서 **None(**없음**)** 링크를 클릭합니다.

단계 **4** **Edit(**편집**)**( )을 클릭합니다.

단계 **5** Alert Configuration(알림 구성) 창에서 **Threshold(**임계값**)** 탭을 클릭합니다.

단계 **6** **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 **7** **Track By(**추적 기준**)** 필드에서 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택하여 이벤트 인스턴스를 소스 IP 주소로 추적할지 대상 IP 주소로 추적할지 나타냅니다.

단계 8 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(**카운트**)** 필드에 입력합니다.

단계 9 이벤트 인스턴스를 추적할 기간(초 단위)을 지정하는 숫자를 **Seconds(**초**)** 필드에 입력합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

추가 지원 및 정보는 Snort 3 억제 및 임계값 비디오를 참조하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

침입 이벤트 임계값 보기 및 삭제

규칙에 대한 기존 임계값 설정을 보거나 삭제하려면 Rules Details(규칙 세부 정보) 보기를 사용하여 임계값에 대해 구성된 설정을 표시하고 해당 설정이 시스템에 적합한지 확인합니다. 적절하지 않은 경우 새 임계값을 추가하여 기존 값을 덮어쓸 수 있습니다.

프로시저

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 3 **Alert Configuration(**알림 구성**)** 열에 표시된 것과 같이 구성된 임계값이 있는 규칙을 선택합니다. **Alert Configuration(**알림 구성**)** 열은 규칙에 대한 링크로 **Threshold(**임계값**)**를 표시합니다.

단계 4 규칙의 임계값을 제거하려면 **Alert Configuration(**알림 구성**)** 열에서 **Threshold(**임계값**)** 링크를 클릭합니다.

단계 5 편집 ( )을 클릭합니다.

단계 6 **Threshold(**임계값**)** 탭을 클릭합니다.

단계 7 **Reset(**재설정**)**을 클릭합니다.

단계 8 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

침입 정책 삭제 구성

특정 IP 주소 또는 특정 범위의 IP 주소가 특정 규칙 또는 검사기를 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**)** > **Snort 3 All Rules(Snort 3** 모든 규칙**)**)에서 **Alert Configuration(**알림 구성**)** 열을 사용하여 억제 설정에 액세스할 수도 있습니다.

Snort 3의 침입 규칙에 대한 억제 설정

침입 규칙에서 규칙에 하나 이상의 억제를 설정할 수 있습니다.

시작하기 전에

소스 또는 대상 억제를 위해 추가할 네트워크 개체를 생성해야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** 침입 규칙의 Alert Configuration(알림 구성) 열에서 **None(**없음**)** 링크를 클릭합니다.

단계 **4** **Edit(**편집**)**()을 클릭합니다.

단계 **5** **Suppressions(**억제**)** 탭에서 다음 옵션 옆의 추가 아이콘(+)을 클릭합니다.

- 지정된 소스 IP 주소에서 시작되는 패킷에 의해 생성된 이벤트를 억제하려면 **Source Networks(**소스 네트워크**)**를 선택합니다.
- 지정된 대상 IP 주소로 이동하는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination Networks(**대상 네트워크**)**를 선택합니다.

단계 **6** **Network(**네트워크**)** 드롭다운 목록에서 사전 설정 네트워크 중 하나를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** (선택 사항) 필요한 경우 마지막 세 단계를 반복합니다.

단계 **9** Alert Configuration(알림 구성) 창에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

억제 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** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** 억제를 보거나 삭제할 규칙을 선택합니다.

단계 **4** **Alert Configuration(**알림 구성**)** 열에서 **Suppression(**억제**)**을 클릭합니다.

단계 **5** 편집 () 버튼을 클릭합니다.

단계 **6** **Suppressions(**억제**)** 탭을 클릭합니다.

단계 **7** 해당 억제 옆의 **Clear(**지우기**)**()를 클릭하여 억제를 제거합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 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.

프로시저

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

단계 **2** 수정하려는 정책 옆의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.

단계 **3** 모든 규칙이 나열된 페이지의 오른쪽에서 코멘트를 추가하려는 규칙을 선택합니다.

단계 **4** **Comments(**코멘트**)** 열 아래의 코멘트()를 클릭합니다.

단계 **5** **Comments(**코멘트**)** 필드에 규칙 코멘트를 입력합니다.

단계 **6** **Add Comment(**코멘트 추가**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

팁

시스템은 Comments(코멘트) 열의 규칙 옆에 코멘트(💬)를 표시합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

Snort 2 사용자 지정 규칙을 Snort 3로 변환

사용자 지정 규칙을 사용하는 경우 Snort 2에서 Snort 3로 변환하기 전에 Snort 3용 규칙 세트를 관리할 준비가 되었는지 확인합니다. 서드파티 벤더의 규칙 세트를 사용하는 경우 해당 벤더에 연락하여 규칙이 Snort 3로 성공적으로 변환되는지 확인하거나 기본적으로 Snort 3용으로 작성된 대체 규칙 세트를 얻으십시오. 직접 작성한 사용자 지정 규칙이 있는 경우 변환 전에 Snort 3 규칙을 작성하는 방법을 숙지하여 변환 후 Snort 3 탐지를 최적화하도록 규칙을 업데이트할 수 있습니다. Snort 3의 규칙 작성에 대해 자세히 알아보려면 아래 링크를 참조하십시오.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Snort 3 규칙에 대해 자세히 알아보려는 경우 https://blog.snort.org/에서 다른 블로그를 참조할 수 있습니다.

시스템 제공 툴을 사용하여 Snort 2 규칙을 Snort 3 규칙으로 변환하려면 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 58 페이지 항목을 참조하십시오.

👉

중요 Snort 2 NAP(Network Analysis Policy, 네트워크 분석 정책) 설정은 Snort3에 자동으로 복사될 수 없습니다. NAP 설정은 Snort 3에서 수동으로 복제해야 합니다.

모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환

프로시저

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** 왼쪽 창에 **All Rules(**모든 규칙**)**가 선택되어 있는지 확인합니다.

단계 **4** **Tasks(**작업**)** 드롭다운 목록을 클릭하고 다음을 선택합니다.

- **Convert Snort 2 rules and import(Snort 2** 규칙 변환 및 가져오기**)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.

- **Convert Snort 2 rules and download(Snort 2** 규칙 변환 및 다운로드**)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 로컬 시스템에 다운로드합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

참고

- 앞 단계에서 **Convert and import(**변환 및 가져오기**)**를 선택한 경우 변환된 모든 규칙은 **Local Rules(**로컬 규칙**)** 아래 새로 생성된 규칙 그룹 **All Snort 2 Converted Global(**모든 **Snort 2** 변환 전역**)**에 저장됩니다.
- 앞 단계에서 **Convert and download(**변환 및 다운로드**)**를 선택한 경우 규칙 파일을 로컬에 저장합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 규칙 그룹에 사용자 지정 규칙 추가, 60 페이지의 단계에 따라 업로드할 수 있습니다.

추가 지원 및 정보는 Snort 2 규칙을 Snort 3로 변환 비디오를 참조하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환

프로시저

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

단계 **2** **Intrusion Policies(**침입 정책**)** 탭에서 **Show Snort 3 Sync status(Snort 3** 동기화 상태 표시**)**를 클릭합니다.

단계 **3** 침입 정책의 **Sync(**동기화**)** 아이콘( )을 클릭합니다.

참고

Snort 2 버전과 Snort 3 버전의 침입 정책이 동기화된 경우 **Sync(**동기화**)** 아이콘이 녹색( )으로 표시됩니다. 이는 변환할 사용자 지정 규칙이 없음을 나타냅니다.

단계 **4** 요약을 읽고 **Custom Rules(**사용자 지정 규칙**)** 탭을 클릭합니다.

단계 **5** 다음을 선택합니다.

- **Import converted rules to this policy(**변환된 규칙을 이 정책으로 가져오기**)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.
- **Download converted rules(**변환된 규칙 다운로드**)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 로컬 시스템에 다운로드합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 업로드 아이콘을 클릭하여 파일을 업로드할 수 있습니다.

단계 6 **Re-Sync(**재동기화**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

규칙 그룹에 사용자 지정 규칙 추가

Management Center에서 사용자 지정 규칙을 업로드하면 로컬로 생성한 사용자 지정 규칙이 모든 Snort 3 규칙 목록에 추가됩니다.

프로시저

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 3 **Tasks(**작업**)** 드롭다운 목록을 클릭합니다.

단계 4 **Upload Snort 3 Rules(Snort 3** 규칙 업로드**)**를 클릭합니다.

단계 5 생성한 Snort 3 사용자 지정 규칙이 포함된 `.txt` 또는 `.rules` 파일을 끌어다 놓습니다.

단계 6 **OK(**확인**)**를 클릭합니다.

참고
선택한 파일에 오류가 있으면 더 이상 진행할 수 없습니다. 오류 파일을 다운로드하고 **Replace File(**파일 교체**)** 링크를 클릭하여 오류를 수정한 후에 파일의 버전 2를 업로드할 수 있습니다.

단계 7 규칙 그룹에 규칙을 연결하여 새 규칙을 그룹에 추가합니다.

Create New Custom Rule Group(새 사용자 지정 규칙 그룹 생성**)** 링크를 클릭하여 새 사용자 지정 규칙 그룹을 생성한 다음 새 그룹에 규칙을 추가할 수도 있습니다.

참고
기존 로컬 규칙 그룹이 없는 경우 **Create New Custom Rule Group to proceed(**계속하려면 새 사용자 지정 규칙 그룹 생성**)**를 클릭하여 계속 진행합니다. 새 규칙 그룹의 **Name(**이름**)**을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 8 다음 중 하나를 선택합니다.

- **Merge Rules(**규칙 병합**)** - 규칙 그룹의 기존 규칙과 추가하는 새 규칙을 병합합니다.
- **Replace all rules in the group with file contents(**그룹의 모든 규칙을 파일 콘텐츠로 교체**)** - 모든 기존 규칙을 추가하는 새 규칙으로 교체합니다.

참고
앞 단계에서 둘 이상의 규칙 그룹을 선택한 경우 **Merge Rules(**규칙 병합**)** 옵션만 사용할 수 있습니다.

단계 9 **Next(**다음**)**를 클릭합니다.

요약을 검토하여 추가되는 새 규칙 ID를 확인하고 필요한 경우 요약을 다운로드합니다.

단계 10 **Finish(**마침**)**를 클릭합니다.

중요 업로드된 모든 규칙의 규칙 작업은 비활성화된 상태입니다. 규칙을 활성화하려면 필요한 상태로 변경해야 합니다.

다음에 수행할 작업

- Management Center에서 사용자 지정 규칙을 업로드하면 생성한 사용자 지정 규칙이 모든 Snort 3 규칙 목록에 추가됩니다. 이러한 사용자 지정 규칙을 트래픽에 적용하려면 필요한 침입 정책에서 이러한 규칙을 추가하고 활성화합니다. 침입 정책에 사용자 지정 규칙이 포함된 규칙 그룹 추가에 대한 자세한 내용은 침입 정책에 사용자 지정 규칙이 포함된 규칙 그룹 추가, 61 페이지 항목을 참조하십시오. 사용자 지정 규칙 활성화에 대한 자세한 내용은 Snort 3의 사용자 지정 규칙 관리, 62 페이지 항목을 참조하십시오.
- 구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

침입 정책에 사용자 지정 규칙이 포함된 규칙 그룹 추가

시스템에서 업로드된 사용자 지정 규칙을 침입 정책에서 활성화해야만 트래픽에 이러한 규칙이 적용됩니다. Management Center에서 사용자 지정 규칙을 업로드한 후 새 사용자 지정 규칙이 포함된 규칙 그룹을 침입 정책에 추가합니다.

프로시저

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

단계 2 **Intrusion Policies(**침입 정책**)** 탭에서 침입 정책의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.

단계 3 Rule Groups(규칙 그룹) 검색 창 옆에 있는 **Add(**추가**)**(+)를 클릭합니다.

단계 4 **Add Rule Groups(**규칙 그룹 추가**)** 창에서 규칙 그룹 옆에 있는 > 아이콘을 클릭하여 로컬 규칙 그룹을 확장합니다.

단계 5 업로드된 사용자 지정 규칙 그룹 옆의 체크 박스를 선택합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

Snort 3의 사용자 지정 규칙 관리

시스템에서 업로드된 사용자 지정 규칙을 침입 정책에 추가하고 활성화해야만 트래픽에 이러한 규칙이 적용됩니다. 업로드된 사용자 지정 규칙을 모든 정책에서 활성화하거나 개별 정책에서 선택적으로 활성화할 수 있습니다.

하나 이상의 침입 정책에서 사용자 지정 규칙을 활성화하려면 다음 단계를 수행합니다.

프로시저

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 3 **Local Rules(**로컬 규칙**)**를 확장합니다.

단계 4 필요한 규칙 그룹을 선택합니다.

단계 5 규칙 옆의 체크 박스를 선택하여 규칙을 선택합니다.

단계 6 **Rule Actions(**규칙 작업**)** 드롭다운 목록에서 **Per Intrusion Policy(**침입 정책별**)**를 선택합니다.

단계 7 다음 중에서 선택합니다.

- **All Policies(**모든 정책**)** - 추가할 모든 규칙에 대해 동일한 규칙 작업을 수행합니다.
- **Per Intrusion Policy(**침입 정책별**)** - 각 침입 정책에 대해 서로 다른 규칙 작업을 수행합니다.

단계 8 다음과 같이 규칙 작업을 설정합니다.

- 앞 단계에서 All Policies(모든 정책)를 선택한 경우 **Select Override state(**재정의 상태 선택**)** 드롭다운 목록에서 필요한 규칙 작업을 선택합니다.
- 앞 단계에서 Per Intrusion Policy(침입 정책별)를 선택한 경우 해당 정책 이름에 대해 **Rule Action(**규칙 작업**)**을 선택합니다. 정책을 더 추가하려면 **Add Another(**다른 하나 추가**)**를 클릭합니다.

단계 9 선택적으로 **Comments(**코멘트**)** 텍스트 상자에 코멘트를 추가합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, 구성 변경 사항 구축, 28 페이지.

맞춤형 규칙 삭제

프로시저

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.
단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.
단계 3 왼쪽 창에서 **Local Rules(**로컬 규칙**)**를 확장합니다.
단계 4 삭제할 규칙의 체크 박스를 선택합니다.
단계 5 선택한 모든 규칙에 대한 규칙 작업이 **Disable(**비활성화**)**인지 확인합니다.

필요한 경우 아래 단계에 따라 선택한 여러 규칙에 대해 규칙 작업을 비활성화합니다.

a) **Rule Actions(**규칙 작업**)** 드롭다운 상자에서 **Per Intrusion Policy(**침입 정책별**)**를 선택합니다.
b) **All Policies(**모든 정책**)** 라디오 버튼을 선택합니다.
c) **Select Override state(**재정의 상태 선택**)** 드롭다운 목록에서 **Disable(**비활성화**)**을 선택합니다.
d) **Save(**저장**)**를 클릭합니다.
e) 삭제할 규칙의 체크 박스를 선택합니다.

단계 6 **Rule Actions(**규칙 작업**)** 드롭다운 목록에서 **Delete(**삭제**)**를 선택합니다.
단계 7 Delete Rules(규칙 삭제) 팝업 창에서 **Delete(**삭제**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

규칙 그룹 삭제

시작하기 전에

삭제하려는 규칙 그룹을 해당 규칙 그룹이 포함된 모든 침입 정책에서 제외합니다. 침입 정책에서 규칙 그룹을 제외하는 단계는 Snort 3 침입 정책 편집, 35 페이지 항목을 참조하십시오.

프로시저

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.
단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.
단계 3 왼쪽 창에서 **Local Rules(**로컬 규칙**)**를 확장합니다.
단계 4 삭제할 규칙 그룹을 선택합니다.

단계 **5** 계속하기 전에 그룹의 모든 규칙에 대한 규칙 작업이 **Disable(**비활성화**)**로 설정되어 있는지 확인합니다.

규칙에 대한 규칙 작업이 **Disable(**비활성화**)** 이외로 설정된 경우 규칙 그룹을 삭제할 수 없습니다. 필요한 경우 아래 단계에 따라 모든 규칙에 대해 규칙 작업을 비활성화합니다.

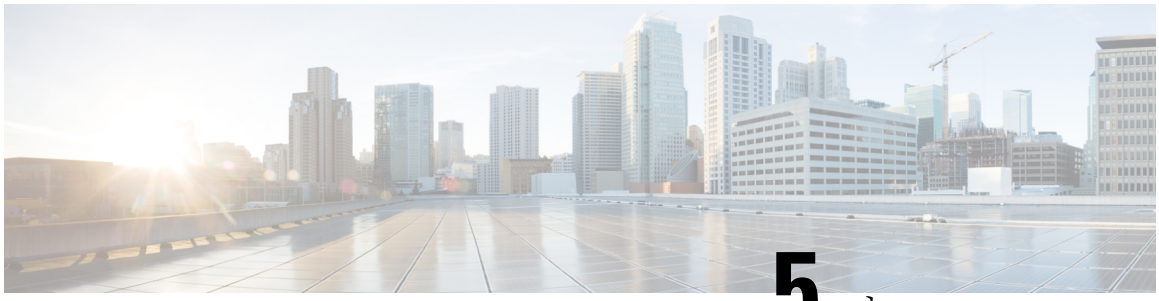
a) **Rule Actions(**규칙 작업**)** 드롭다운 목록 아래의 체크 박스를 선택하여 그룹의 모든 규칙을 선택합니다.
b) **Rule Actions(**규칙 작업**)** 드롭다운 상자에서 **Per Intrusion Policy(**침입 정책별**)**를 선택합니다.
c) **All Policies(**모든 정책**)** 라디오 버튼을 선택합니다.
d) **Select Override state(**재정의 상태 선택**)** 드롭다운 목록에서 **Disable(**비활성화**)**을 선택합니다.
e) **Save(**저장**)**를 클릭합니다.

단계 **6** 규칙 그룹 옆에 있는 **Delete(**삭제**)**( )를 클릭합니다.

단계 **7** Delete Rule Group(규칙 그룹 삭제) 팝업 창에서 **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.



5 장

네트워크 자산에 대한 침입 방지 맞춤화

이 장에서는 Secure Firewall 권장 규칙과 Secure Firewall 권장 규칙을 생성 및 적용하는 방법에 대한 인사이트를 제공합니다.

LSP 업데이트의 Snort 3 규칙 변경

정기 Snort 3 LSP(Lightweight Security Package) 업데이트 중에 기존 시스템 정의 침입 규칙이 새 침입 규칙으로 교체될 수 있습니다. 단일 규칙이 여러 규칙으로 교체되거나 여러 규칙이 단일 규칙으로 교체될 가능성이 있습니다. 이는 규칙을 결합하거나 확장하여 탐지가 개선될 수 있는 경우에 이루어집니다. 관리를 개선하기 위해 LSP 업데이트 과정에서 일부 기존 시스템 정의 규칙이 제거될 수 있습니다.

LSP 업데이트 중에 재정의된 시스템 정의 규칙의 변경 사항에 대한 알림을 받으려면 **Retain user overrides for deleted Snort 3 rules(**삭제된 **Snort 3** 규칙에 대한 사용자 재정의 유지**)** 체크 박스가 선택되어 있는지 확인합니다.

Retain user overrides for deleted Snort 3 rules(삭제된 **Snort 3** 규칙에 대한 사용자 재정의 유지**)** 체크 박스로 이동하려면 **Cog(**톱니바퀴**)(**⚙**)**를 클릭한 다음 **Configuration(**구성**)** > **Intrusion Policy Preferences(**침입 정책 기본 설정**)**를 선택합니다.

기본적으로 이 체크 박스는 선택되어 있습니다. 이 체크 박스를 선택하면 시스템은 LSP 업데이트의 일부로 추가된 새 교체 규칙에서 규칙 재정의를 유지합니다. 알림은 **Tasks(**작업**)** 탭의 **Cog(**톱니바퀴**)(**⚙**)** 옆에 있는 Notifications(알림) 아이콘 아래에 표시됩니다.

Secure Firewall 권장 규칙 개요

침입 규칙 권장 사항을 사용하여 네트워크에서 탐지된 호스트 자산 관련 취약성을 대상으로 지정할 수 있습니다. 운영 체제, 서버, 클라이언트 애플리케이션 프로토콜을 예로 들 수 있습니다. 침입 정책을모니터링되는 네트워크의 특정 요구를 조정할 수 있게 합니다.

시스템에서 각 IPS 정책 대 한 권장 사항 개별 집합을 만듭니다. 일반적으로 표준 텍스트 규칙 및 공유 개체 규칙에 대 한 규칙 상태 변경을 권장합니다. 그런데 검사기 및 디코더 규칙에 대한 변경 사항을 권장할 수도 있습니다.

규칙 상태 권장 사항을 생성할 때에 기본 설정을 사용 하 여 수도 있고 고급 설정을 구성할 수 있습니다. 고급 설정을 수행할 수 있습니다.

- 취약성에 대 한 네트워크에 있는 호스트 시스템 모니터링 재정의
- 규칙 오버 헤드에 따라 시스템이 권장 규칙에 영향을
- 규칙을 비활성화 하기 위한 권장 생성을 활성화할지 지정

또한 권장 사항을 즉시 사용하거나 권장 사항(및 영향을 받는 규칙)을 검토한 후 수락하도록 선택할 수 있습니다.

권장 규칙 상태를 사용하도록 선택하면 읽기 전용 Secure Firewall 권장 사항 레이어가 침입 정책에 추가되고 이후 권장 규칙 상태를 사용하지 않기로 선택하면 레이어가 제거됩니다.

침입 정책에서 가장 최근에 저장된 구성 설정에 따라 자동으로 권장 사항을 생성하도록 작업을 예약할 수 있습니다.

시스템은 다음과 같이 수동으로 설정한 규칙 상태를 변경하지 않습니다.

- 권장 사항을 생성하기 전에 지정된 규칙의 상태를 수동으로 설정하면 시스템이 향후 해당 규칙의 상태를 수정할 수 없게 됩니다.
- 권장 사항을 생성한 후 수동으로 지정된 규칙의 상태를 설정하면 해당 규칙의 권장 상태가 재정의됩니다.

팁 침입 정책 리포트는 권장 상태와 다른 규칙 상태를 가진 규칙 목록을 포함할 수 있습니다.

권장 필터링된 규칙 페이지를 표시하는 동안 또는 탐색 패널 또는 정책 정보 페이지에서 직접 규칙 페이지에 액세스한 후 규칙 상태를 수동으로 설정하고 규칙을 정렬하고 규칙 페이지에서 사용할 수 있는 다른 작업(예: 규칙 억제, 규칙 임계값 설정 등)을 수행할 수 있습니다.

참고 Cisco Talos(Talos Intelligence Group)는 시스템 제공 정책에서 각 규칙의 적절한 상태를 결정합니다. 시스템 제공 정책을 기본 정책으로 사용하여 시스템에서 Secure Firewall 권장 규칙 상태에 규칙을 설정하도록 허용하는 경우 네트워크 자산에 대해 권장하는 설정을 침입 정책 규칙에 일치시킵니다.

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.

Snort 3에서 새로운 Secure Firewall 권장 사항 생성

침입 정책에 대한 Secure Firewall 권장 사항을 생성한 다음 여기에 나열된 단계에 따라 Snort 3에서 새 권장 규칙 설정을 만듭니다. 규칙 오버헤드는 Snort 3에서 사용자가 선택한 임계값 정책을 기반으로 하는 보안 레벨로 해석됩니다. 권장 작업은 선택한 보안 레벨을 기반으로 하며, 기본 정책보다 높은 경우 권장 사항은 이벤트 생성에만 국한되지 않습니다.

Secure Firewall 권장 사항을 설정하기 전에 아래에 나열된 세 가지 사항 중 목표에 가장 일치하는 것이 무엇인지 자문해야 합니다.

- Increased Protection(보호 강화) - 호스트 데이터베이스에서 발견된 취약성을 기반으로 추가 규칙을 활성화하고 규칙을 자동으로 비활성화하지 않습니다. 이로 인해 규칙 집합이 커질 수 있습니다.
- Focused Protection(보호 우선) - 호스트 데이터베이스에서 발견된 취약성에 따라 추가 규칙을 활성화하며 기존 규칙을 비활성화합니다. 이렇게 하면 검색된 취약성에 따라 규칙 수를 늘리거나 줄일 수 있습니다.
- Higher Efficency(고효율) - 현재 활성화된 규칙 집합을 사용하고 호스트 데이터베이스에 없는 취약성에 대한 규칙은 모두 비활성화합니다. 이로 인해 활성화된 규칙 집합의 크기가 작아질 수 있습니다.

응답을 기반으로 하는 권장 작업은 다음과 같습니다.

- 권장 사항을 다음으로 가장 높은 보안 레벨로 설정하고 규칙 비활성화의 선택을 취소합니다.
- 권장 사항을 다음으로 가장 높은 보안 레벨로 설정하고 규칙 비활성화를 확인합니다.
- 권장 사항을 현재 보안 레벨로 설정하고 규칙 비활성화를 확인합니다.

시작하기 전에

Secure Firewall 권장 사항에는 다음 요구 사항이 있습니다.

- 권장 사항을 생성하려면 시스템에 호스트가 있는지 확인합니다.
- 권장 사항에 대해 구성된 보호받는 네트워크는 시스템에 있는 호스트에 매핑되어야 합니다.

프로시저

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

단계 2 침입 정책의 **Snort 3 Version(Snort 3** 버전**)** 버튼을 클릭합니다.

단계 3 **Recommendations (Not in Use)(**권장 사항**(**사용되지 않음**))** 레이어를 클릭하여 규칙 권장 사항을 구성합니다. **Start(**시작**)**를 클릭합니다.

Secure Firewall Rule Recommendations(Secure Firewall Firepower 규칙 권장 사항) 창에서 다음을 설정할 수 있습니다.

- **Security Level(**보안 레벨**)**: 보안 레벨을 선택하려면 클릭합니다. 필요에 따라, 입력 보안 레벨 및 보호된 네트워크에서 활성화되지 않은 규칙을 비활성화하려면 **Accept Recommendation to Disable Rules(**규칙을 비활성화하라는 권장 사항 수락**)** 체크 박스를 선택할 수 있습니다. 많은 알림 수로 인해 규칙 집합을 잘라내거나 검사 성능을 개선해야 하는 경우에만 이 옵션을 활성화하십시오. 보안 레벨은 다음과 같습니다.
  - 보안 레벨 1: Connectivity over Security(연결이 보안에 우선함)

    No Impact(영향 없음**)** - 새 규칙이 활성화되지 않으며 기존 규칙이 비활성화되지 않습니다. 보호를 강화하려면 더 높은 보안 레벨을 선택하십시오.

    Low Security(낮은 보안 수준**)**(체크 박스 선택됨) - 검색된 호스트의 잠재적 취약성과 일치하는 Connectivity Over Security(연결이 보안에 우선함) 규칙 집합의 규칙을 제외하고 모든 규칙이 비활성화됩니다. 대신 기본 정책을 조정하는 것이 좋습니다.
  - 보안 레벨 2: Balanced Security Over Connectivity(균형 잡힌 보안이 연결에 우선함)

    No Impact(영향 없음**)** - 새 규칙이 활성화되지 않으며 기존 규칙이 비활성화되지 않습니다. 보호를 강화하려면 더 높은 보안 레벨을 선택하십시오.

    Higher Efficiency(효율성 향상**)**(체크 박스 선택됨) - 검색된 호스트에서 잠재적인 취약점과 일치하는 기존 규칙을 유지하고 네트워크에서 찾을 수 없는 취약점에 대한 규칙을 비활성화합니다.
  - 보안 레벨 3: Security Over Connectivity(보안이 연결에 우선함)

    Increased Security(보안 강화**)** - Maximum Detection(최대 탐지) 규칙 집합을 기반으로 검색된 호스트에서 잠재적인 취약점과 일치하는 추가 규칙을 활성화합니다.

    Focused Security(보안 우선**)**(체크 박스 선택됨) - Security over Connectivity(보안이 연결에 우선함) 규칙 집합을 기반으로 검색된 호스트의 취약점과 일치하는 추가 규칙을 활성화하면서 검색된 호스트의 잠재적인 취약점과 일치하지 않는 기존 규칙은 비활성화합니다.
  - 보안 레벨 4: Maximum Detection(최대 탐지)

    Increased Security(보안 강화**)** - Security over Connectivity(보안이 연결에 우선함) 규칙 집합을 기반으로 검색된 호스트에서 잠재적인 취약점과 일치하는 추가 규칙을 활성화합니다.

Focused Security(보안 우선**)**(체크 박스 선택됨) - Maximum Detection(최대 탐지) 규칙 집합을 기반으로 검색된 호스트의 취약점과 일치하는 추가 규칙을 활성화하면서 검색된 호스트의 잠재적인 취약점과 일치하지 않는 기존 규칙은 비활성화합니다.

참고
Maximum Detection(최대 탐지)은 매우 많은 규칙을 활성화하며 성능에 영향을 미칠 수 있습니다. 생산 환경에 구축하기 전에 이 설정을 검토하고 테스트하는 것이 좋습니다.

- **Protected Networks(**보호되는 네트워크**)**: 권장 사항을 위해 검사할 모니터링 중인 네트워크 또는 개별 호스트를 지정합니다. 드롭다운 목록에서 하나 이상의 시스템 또는 사용자 정의한 네트워크 개체를 선택할 수 있습니다. 따로 선택하지 않은 경우 기본적으로 IPv4 또는 IPv6 네트워크가 선택됩니다.

  중요
  Secure Firewall 규칙 권장 사항은 네트워크 검색에 따라 다릅니다. Protected Networks(보호되는 네트워크)는 네트워크 검색 정책에 구성한 범위 내에서 검색된 모든 호스트에 적용됩니다. 자세한 내용은 *Cisco Secure Firewall Management Center* 디바이스 구성 가이드의 네트워크 검색 정책 장을 참조하십시오.

  Add +(추가 **+)** 버튼을 클릭하여 호스트 또는 네트워크 유형의 새 네트워크 개체를 생성하고 **Save(**저장**)**를 클릭합니다.

단계 **4** 권장 사항을 생성하고 적용합니다.

- **Generate(**생성**)**: 침입 정책에 대한 권장 사항을 생성합니다. 이 작업은 Recommended Rules (Not in use)(권장 규칙(사용되지 않음)) 아래에 규칙을 나열합니다.
- **Generate and Apply(**생성 및 적용**)**: 침입 정책에 대한 권장 사항을 생성하고 적용합니다. 이 작업은 Recommended Rules (In use)(권장 규칙(사용 중)) 아래에 규칙을 나열합니다.

권장 사항이 생성되었습니다. 모든 권장 규칙 및 해당 권장 작업이 포함된 새 권장 사항 탭이 나타납니다. 이 탭에서 새로운 권장 사항과 함께 규칙 작업 프리셋 필터도 사용할 수 있습니다.

단계 **5** 권장 사항을 확인한 다음 적절하게 적용하도록 선택할 수 있습니다.

- **Accept(**수락**)** - 침입 정책에 대해 이전에 생성된 권장 사항을 적용합니다.
- **Refresh(**새로 고침**)** - 침입 정책에 대한 규칙 권장 사항을 다시 생성하고 업데이트합니다.
- **Edit(**편집**)** - 권장 사항 입력 값을 제공한 다음 권장 사항을 생성할 수 있는 Recommendations(권장 사항) 대화 상자를 엽니다.
- **Remove All(**모두 제거**)** - 적용된 권장 규칙을 되돌리거나 정책에서 제거하며, Recommendations(권장 사항) 탭도 제거합니다.

All Rules(모든 규칙**)** 아래의 Recommended Rules(권장 규칙) 섹션에 권장 규칙이 나와 있습니다.

참고
침입 규칙에 대한 최종 작업은 규칙 작업 우선순위에 따라 적용되며 규칙 작업 우선순위는 다음과 같습니다.

Rule Override(규칙 재정의) > Generated Recommendations(생성된 권장 사항) > Group Override(그룹 재정의) > Base Policy Default Action(기본 정책 기본 작업)

활성화된 권장 사항의 경우 Management Center에서는 현재 상태(그룹 재정의, 기본 정책, 권장 사항 구성)를 고려하며 작업의 우선순위는 다음과 같습니다.

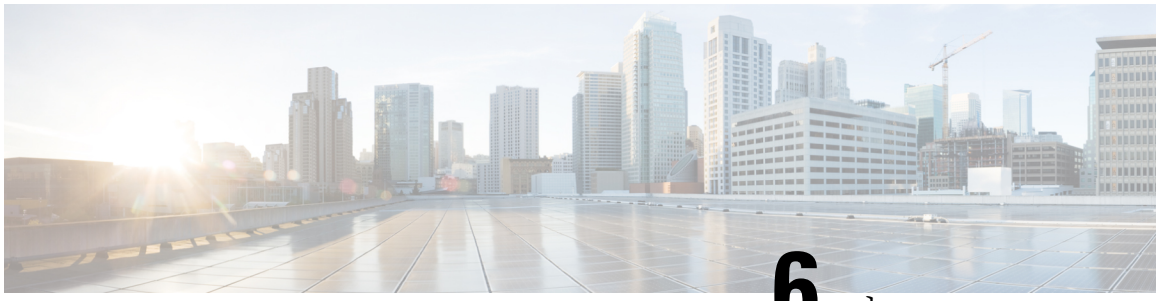
pass(통과) > block(차단) > reject(거부) > drop(삭제) > rewrite(재작성) > alert(알림)

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 28 페이지를 참고하십시오.

II 부

Snort 3의 고급 네트워크 분석



6 장

Snort 3 네트워크 분석 정책 시작하기

이 장에서는 네트워크 분석 정책의 기본 사항, 요건, 네트워크 분석 정책을 관리하는 방법에 대한 인사이트를 제공합니다. 또한 사용자 지정 네트워크 분석 정책 생성 및 네트워크 분석 정책 설정에 대한 정보도 제공합니다.

네트워크 분석 정책 개요

네트워크 분석 정책은 많은 트래픽 전처리 옵션을 관리하며, 액세스 제어 정책의 고급 설정에 의해 호출됩니다. 네트워크 분석 관련 전처리는 보안 인텔리전스 매칭 및 SSL 암호 해독 후, 그리고 액세스 제어 규칙이 패킷을 자세히 조사하기 전과 모든 침입 또는 파일 검사가 시작되기 전에 수행됩니다.

기본적으로, 시스템은 *Balanced Security and Connectivity*(균형 잡힌 보안 및 연결성) 네트워크 분석 정책을 사용하여 액세스 제어 정책에서 처리된 모든 트래픽을 전처리합니다. 그러나, 사용자는 이 전처리를 수행하는 기타 기본 네트워크 분석 정책을 선택할 수 있습니다. 사용자 편의를 위해, 시스템은 Cisco Talos Intelligence Group(Talos)이(가) 보안 및 연결의 특정 균형을 위해 조정한 변경할 수 없는 여러 네트워크 분석 정책 선택권을 제공합니다. 또한 맞춤형 전처리 설정이 있는 맞춤형 네트워크 분석 정책을 만들 수도 있습니다.

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. 네트워크 분석 및 칩임 정책은 함께 작동해 트래픽을 검색합니다.

또한 여러 맞춤형 네트워크 분석 정책을 작성한 다음, 다른 트래픽을 전처리하도록 할당하여 특정 보안 영역, 네트워크 및 VLAN에 맞게 트래픽 전처리 옵션을 조정할 수도 있습니다. (ASA FirePOWER은 VLAN에 의한 전처리를 제한할 수 없는 점에 유의하십시오.)

네트워크 분석 정책 관리

툴바에서 사용자 이름 하단에 시스템이 사용 가능한 도메인 트리를 표시합니다. 도메인을 전환하려면 액세스하려는 도메인을 선택합니다.

프로시저

단계 **1** 네트워크 분석 정책에 액세스하려면 다음 경로 중 하나를 선택합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**
- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**
- **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policy(**네트워크 분석 정책**)**

참고
맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 네트워크 분석 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다(*Cisco Secure Firewall Management Center* 구성 가이드에 있는 정책 비교 참조).

  참고
  Snort 2 정책만 비교할 수 있습니다.

- 생성 - 새 네트워크 분석 정책을 생성하려면 **Create Policy(**정책 생성**)**를 클릭합니다.

  네트워크 분석 정책의 두 가지 버전인 **Snort 2 Version(Snort 2** 버전**)**과 **Snort 3 Version(Snort 3** 버전**)**이 생성됩니다.

  - Snort 2 버전의 경우 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 *Snort 2*에 대한 사용자 지정 네트워크 분석 정책 생성을 참조하십시오.
  - Snort 3 버전의 경우 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 77 페이지의 내용을 참조하십시오.

- 삭제 - 네트워크 분석 정책을 삭제하려면 **Delete(**삭제**)** 아이콘을 클릭하고 정책 삭제 여부를 확인합니다. 액세스 제어 정책이 네트워크 분석 정책을 참조하는 경우 이를 삭제할 수 없습니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

- 편집 - 기존 네트워크 분석 정책을 편집하려면 **Edit(편집)** 아이콘을 클릭합니다.

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

- 보고서 - **Report(보고서)** 아이콘을 클릭합니다(*Cisco Secure Firewall Management Center* 구성 가이드에 있는 현재 정책 보고서 생성 참조).

네트워크 분석 정책에 사용되는 Snort 3 정의 및 용어

다음 표에는 네트워크 분석 정책에 사용되는 Snort 3 개념과 용어가 나와 있습니다.

표 *6:* 네트워크 분석 정책에 사용되는 *Snort 3* 정의 및 용어

용어	설명
검사기	검사기는 Snort 2 전처리기와 유사하게 패킷을 처리하는 플러그인입니다.
바인더 검사기	바인더 검사기는 특정 검사기가 액세스하여 고려해야 하는 경우 흐름을 정의합니다. 트래픽이 바인더 검사기에 정의된 조건과 일치하면 해당 검사기의 값/구성만 적용됩니다. 자세한 내용은 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 77 페이지의 바인더 검사기를 참조하십시오.
싱글톤 검사기	싱글톤 검사기에는 하나의 인스턴스가 포함됩니다. 싱글톤 검사기는 멀티톤 검사기와 같이 인스턴스 추가를 지원하지 않습니다. 싱글톤 검사기의 설정은 특정 트래픽 세그먼트가 아닌 해당 검사기와 일치하는 전체 트래픽에 적용됩니다. 자세한 내용은 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 77 페이지의 싱글톤 검사기를 참조하십시오.

용어	설명
멀티톤 검사기	멀티톤 검사기에는 필요에 따라 구성할 수 있는 여러 인스턴스가 포함되어 있습니다. 멀티톤 검사기는 네트워크, 포트, VLAN 등의 특정 조건을 기반으로 설정 구성을 지원합니다. 지원되는 설정 세트 하나를 인스턴스라고 합니다. 자세한 내용은 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 77 페이지의 멀티톤 검사기를 참조하십시오.
스키마	스키마 파일은 OpenAPI JSON 사양을 기반으로 하며 업로드되거나 다운로드되는 콘텐츠를 확인합니다. Swagger 편집기와 같은 서드파티 JSON 편집기를 사용하여 스키마 파일을 다운로드하고 열 수 있습니다. 스키마 파일은 사용할 수 있는 허용되는 값, 범위 및 허용되는 패턴을 사용하여 검사기에 대해 구성할 수 있는 매개 변수를 식별하는 데 도움이 됩니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 86 페이지를 참고하십시오.
샘플 파일	예제 구성이 포함된 기본 제공 템플릿으로, 검사기를 구성하는 데 도움이 됩니다. 샘플 파일에 포함된 예제 구성을 참조하여 필요에 따라 변경할 수 있습니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 86 페이지를 참고하십시오.
전체 구성	전체 검사기 구성을 단일 파일로 다운로드할 수 있습니다. 검사기 구성과 관련된 모든 정보를 이 파일에서 사용할 수 있습니다. 전체 구성은 기본 구성(Cisco Talos에서 LSP 업데이트의 일부로 배포)과 사용자 지정 NAP 검사기 구성을 병합한 구성입니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 86 페이지를 참고하십시오.

용어	설명
재정의된 구성	네트워크 분석 정책의 **Snort 3 Version(Snort 3 버전)** 페이지에서 다음과 같이 합니다. • **Actions(작업)** > **Upload(업로드)**에서 **Overridden Configuration(재정의된 구성)**을 클릭하여 재정의된 구성이 포함된 JSON 파일을 업로드할 수 있습니다. • **Actions(작업)** > **Download(다운로드)**에서 **Overridden Configuration(재정의된 구성)**을 클릭하여 재정의된 검사기 구성을 다운로드할 수 있습니다. 검사기 구성을 재정의하지 않은 경우 이 옵션은 비활성화됩니다. 검사기 구성을 재정의하면 이 옵션이 자동으로 활성화되어 다운로드할 수 있습니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 86 페이지를 참고하십시오.

관련 항목

Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 77 페이지
네트워크 분석 정책 사용자 정의, 86 페이지
네트워크 분석 정책 매핑, 83 페이지

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.

Snort 3에 대한 맞춤형 네트워크 분석 정책 생성

기본 네트워크 분석 정책은 일반적인 네트워크 요구 사항 및 최적의 성능에 맞게 조정됩니다. 일반적으로 기본 네트워크 분석 정책은 대부분의 네트워크 요구 사항을 충족하므로 정책을 사용자 정의하지 않아도됩니다. 그러나 특정 네트워크 요구 사항이 있거나 성능 문제가 발생할 경우 기본 네트워크 분석 정책을 사용자 지정할 수 있습니다. 네트워크 분석 정책을 사용자 지정하는 것은 고급 사용자 또는 Cisco 지원만 수행해야 하는 고급 구성입니다.

Snort 3의 네트워크 분석 정책 구성은 JSON 및 JSON 스키마를 사용하는 데이터 기반 모델입니다. OpenAPI 사양을 기반으로 하는 스키마를 통해 지원되는 검사기, 설정, 설정 유형 및 유효한 값을 확

인할 수 있습니다. Snort 3 검사기는 Snort 2 전처리기와 유사하게 패킷을 처리하는 플러그인입니다. 네트워크 분석 정책 구성은 JSON 형식으로 다운로드할 수 있습니다.

Snort 3의 검사기 및 설정 목록은 Snort 2 전처리기 및 설정 목록과 일대일로 매핑되지 않습니다. 또한 Snort 3에서 지원하는 검사기 및 설정의 일부만 Management Center에서 사용할 수 있습니다. Snort 3에 대한 자세한 내용은 https://snort.org/snort3 항목을 참조하십시오. Management Center에서 사용 가능한 검사기에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors 항목을 참조하십시오.

참고

- Management Center를 7.0 릴리스로 업그레이드하는 동안 네트워크 분석 정책의 Snort 2 버전에서 수행된 변경 사항은 업그레이드 후에 Snort 3으로 마이그레이션되지 않습니다.
- 침입 정책과 달리 Snort 2 네트워크 분석 정책 설정을 Snort 3에 동기화하는 옵션은 없습니다.

기본 검사기 업데이트

LSP(Lightweight Security Package) 업데이트에는 새 검사기 또는 기존 검사기 구성의 정수 범위 수정 사항이 포함될 수 있습니다. LSP를 설치하고 나면 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**의 **Inspectors(**검사기**)** 아래에서 새 검사기 및 업데이트된 범위를 사용할 수 있습니다.

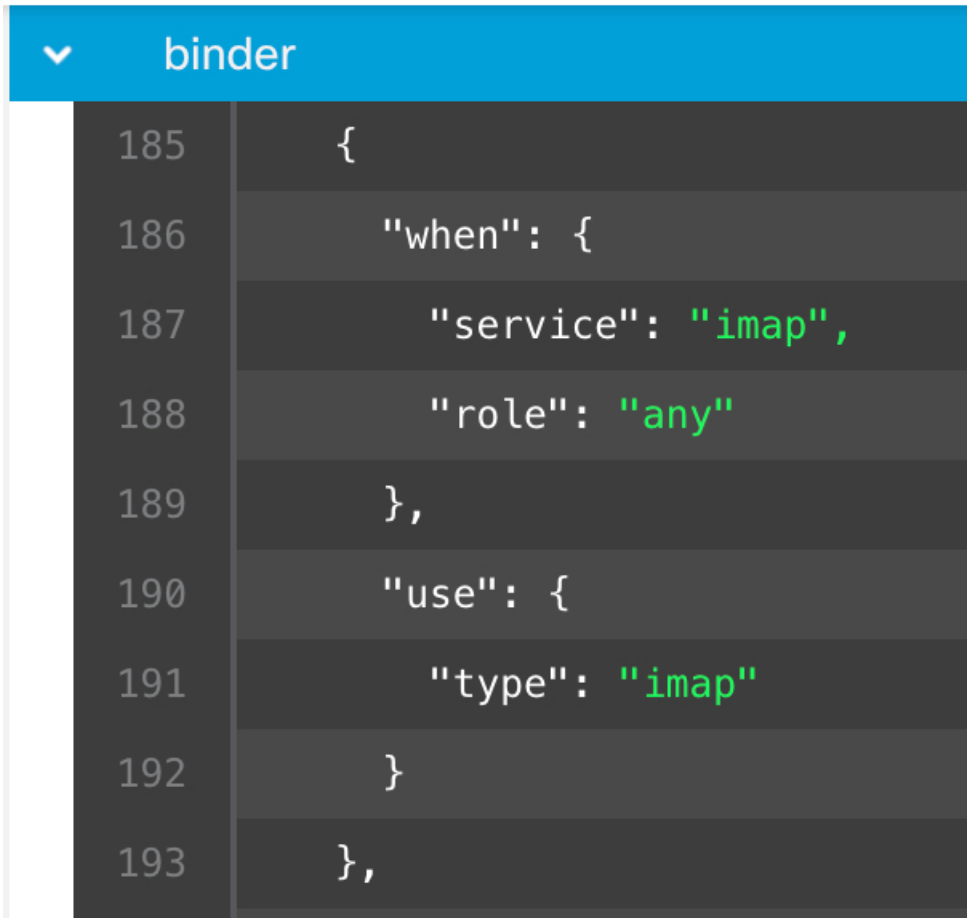
바인더 검사기

바인더 검사기는 특정 검사기가 액세스하여 고려해야 하는 경우 흐름을 정의합니다. 트래픽이 바인더 검사기에 정의된 조건과 일치하면 해당 검사기의 값/구성만 적용됩니다. 예를 들면 다음과 같습니다.

imap 검사기의 경우 바인더는 액세스할 때 다음 조건을 정의합니다. 조건:

- 서비스가 imap와 같습니다.
- 역할이 any와 같습니다.

이러한 조건이 충족되면 imap 유형을 사용합니다.



싱글톤 검사기

싱글톤 검사기에는 하나의 인스턴스가 포함됩니다. 싱글톤 검사기는 멀티톤 검사기와 같이 인스턴스 추가를 지원하지 않습니다. 싱글톤 검사기의 설정은 특정 트래픽 세그먼트가 아닌 전체 트래픽에 적용됩니다.

예를 들면 다음과 같습니다.

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

멀티톤 검사기

멀티톤 검사기에는 필요에 따라 구성할 수 있는 여러 인스턴스가 포함되어 있습니다. 멀티톤 검사기는 네트워크, 포트, VLAN 등의 특정 조건을 기반으로 설정 구성을 지원합니다. 지원되는 설정 세트 하나를 인스턴스라고 합니다. 기본 인스턴스가 있으며 특정 조건에 따라 인스턴스를 더 추가할 수도 있습니다. 트래픽이 해당 조건과 일치하면 해당 인스턴스의 설정이 적용됩니다. 그렇지 않은 경우 기본 인스턴스의 설정이 적용됩니다. 또한 기본 인스턴스의 이름은 검사기의 이름과 동일합니다.

멀티톤 검사기의 경우 재정의된 검사기 구성을 업로드할 때 JSON 파일의 각 인스턴스에 대해 일치하는 바인더 조건(검사기가 액세스 또는 사용되어야 하는 조건)도 포함/정의해야 합니다. 그렇지 않으면 업로드 오류가 발생합니다. 새 인스턴스를 생성할 수도 있지만 오류를 방지하기 위해 생성하는 모든 새 인스턴스에 대해 바인더 조건을 포함해야 합니다.

예를 들면 다음과 같습니다.

- 기본 인스턴스가 수정된 멀티톤 검사기

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- 기본 인스턴스와 기본 바인더가 수정된 멀티톤 검사기

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
```

```
            }
        ]
    }
}
```

- 사용자 지정 인스턴스와 사용자 지정 바인더가 추가된 멀티톤 검사기

```
{
    "http_inspect":{
        "enabled":true,
        "type":"multiton",
        "instances":[
            {
                "name":"http_inspect1",
                "data":{
                    "response_depth":5000
                }
            }
        ]
    },
    "binder":{
        "type":"binder",
        "enabled":true,
        "rules":[
            {
                "use":{
                    "type":"http_inspect",
                    "name":"http_inspect1"
                },
                "when":{
                    "role":"any",
                    "ports":"8080",
                    "proto":"tcp",
                    "service":"http"
                }
            }
        ]
    }
}
```

CIP(Common Industrial Protocol) Safety

CIP(Common Industrial Protocol) Safety는 디바이스의 안전한 작동을 지원하는 CIP의 확장 집합입니다. 또한 CIP 네트워크의 서로 다른 노드 간 페일 세이프 통신도 제공합니다.

CIP Safety 프로토콜은 다음 두 가지 주요 구성 요소로 구성됩니다.

- CIP Safety 세그먼트 - Forward Open(전송 열기) 메시지에서 후속 보안 세션을 위한 보안 매개변수를 교환하는 데 사용됩니다.
- CIP Safety 메시지 - 실제 보안 정보 교환에 사용됩니다.

CIP 검사기는 다음 항목을 탐지 및 식별합니다.

- 서비스형 CIP 및 클라이언트
- CIP Read, CIP Admin, CIP Infrastructure, CIP Write와 같은 페이로드

CIP 검사기는 CIP 세그먼트를 구문 분석하고 Forward Open(전송 열기) 요청에서 CIP 보안 세그먼트를 탐지할 수 있습니다.

CIP Safety 기능을 테스트하려면 CIP 검사기를 활성화해야 합니다. CIP 패킷의 보안 세그먼트 탐지 및 차단, 82 페이지의 내용을 참조하십시오.

CIP 패킷의 보안 세그먼트 탐지 및 차단

활용 사례: CIP Safety 세그먼트를 탐지 및 차단하는 동시에 다른 CIP 패킷은 허용하는 경우:

- **cip_safety**라는 사용자 지정 네트워크 분석 정책을 만듭니다.
- 액세스 제어 정책에서 액세스 제어 규칙을 생성하여 CIP Safety를 차단하고 다른 모든 패킷을 허용합니다.

CIP Safety 기능을 테스트하려면 Management Center에서 CIP 검사기를 활성화하고 액세스 제어 정책에 할당합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 생성한 네트워크 분석 정책 **cip_safety**의 **Snort 3** 버전을 클릭합니다.

단계 **3** **Inspectors(**검사기**)**에서 **cip**를 클릭하여 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 **4** 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Edit Inspector(**검사기 편집**)** 아이콘을 클릭하고 **cip**의 "enabled(활성화됨)" 필드를 false(기본값)에서 true로 변경합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** **cip** 검사기를 액세스 제어 정책에 할당하려면 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Edit(**편집**)**을 선택하고 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)** 옵션을 선택합니다.

단계 **8** **Network Analysis and Intrusion Policies(**네트워크 분석 및 침입 정책**)** 옆에 있는 편집 ( )을 클릭합니다.

단계 **9** **Network Analysis and Intrusion Policies(**네트워크 분석 및 침입 정책**)** 창에서 **Default Network Analysis Policy(**기본 네트워크 분석 정책**)** 드롭다운 목록에서 생성한 액세스 제어 정책 **cip_safety**를 선택합니다.

이제 CIP 검사기가 Management Center에서 활성화되며 CIP Safety를 차단하고 다른 모든 CIP 패킷을 허용하는 사용자 지정 액세스 제어 규칙을 생성할 수 있습니다.

단계 **10** CIP 안전 패킷 플로우를 포함하는 라이브 트래픽을 전송한 후에는 **Connection Events(**연결 이벤트**)**로 이동하여 페이로드가 이 절차에서 언급하는 탐지 및 차단 활용 사례에 대한 CIP Safety 패킷 로그를 포함하는 예상 페이로드인지 확인합니다. **CIP**는 애플리케이션 프로토콜 및 클라이언트로 탐지되

며(**Application Protocol(**애플리케이션 프로토콜), **Client(**클라이언트**)** 필드 참조), **CIP Safety**는 **Web Application(**웹 애플리케이션**)** 필드에 표시됩니다.

네트워크 분석 정책 매핑

네트워크 분석 정책의 경우 Cisco Talos는 Snort 3 버전에 해당하는 Snort 2 버전의 정책을 찾는 데 사용되는 매핑 정보를 제공합니다.

이 매핑을 통해 Snort 3 버전의 정책이 해당하는 Snort 2 버전을 사용할 수 있습니다.

네트워크 분석 정책 매핑 보기

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **NAP Mapping(NAP** 매핑**)**을 클릭합니다.

단계 **3** **View Mappings(**매핑 보기**)**의 화살표를 확장합니다.

Snort 2에 해당하는 정책에 자동으로 매핑되는 Snort 3 네트워크 분석 정책이 표시됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

네트워크 분석 정책 생성

기존의 모든 네트워크 분석 정책은 해당 Snort 2 및 Snort 3 버전과 함께 Management Center에서 사용할 수 있습니다. 새 네트워크 분석 정책을 생성하면 정책이 Snort 2 버전과 Snort 3 버전 모두로 생성됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Base Policy(**기본 정책**)**을 선택하고 **Save(**저장**)**를 클릭합니다.

새 네트워크 분석 정책을 생성하면 해당하는 **Snort 2** 버전 및 **Snort 3** 버전으로 생성됩니다.

네트워크 분석 정책 수정

네트워크 분석 정책을 수정하여 이름, 설명 또는 기본 정책을 변경할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **Edit(**수정**)**을 클릭하여 이름, 설명, 검사 모드 또는 기본 정책을 변경합니다.

주의
Detection(탐지**)** 모드 사용 중단: Management Center 7.4.0부터는 NAP(네트워크 분석 정책)의 경우 **Detection(**탐지**)** 검사 모드가 더 이상 사용되지 않으며 이후 릴리스에서 제거될 예정입니다.

Detection(탐지**)** 모드는 트래픽을 삭제(즉, 삭제될 트래픽을 표시)하도록 설정하기 전에 검사를 활성화하고 네트워크에서 작동하는 방식을 확인할 수 있도록 테스트 모드로 사용되었습니다.

모든 검사기 삭제가 규칙 상태에 의해 제어되고 각 검사기 삭제를 설정하여 이벤트를 생성할 수 있게 되면 이 동작이 개선됩니다. 이는 트래픽을 삭제하도록 규칙 상태를 구성하기 전에 테스트하기 위한 것입니다. 이제 Snort 3의 트래픽 삭제를 세부적으로 제어할 수 있으므로 **Detect(**탐지**)** 모드는 제품을 복잡하게 만들 뿐이고 필요하지 않으므로 탐지 모드가 더 이상 사용되지 않습니다.

Detection(탐지**)** 모드의 NAP를 **Prevention(**방지**)**으로 변경하는 경우 침입 이벤트의 트래픽을 처리하고 "will be dropped(삭제될)" 결과를 갖는 NAP는 이제 "삭제"되며 해당 트래픽이 이러한 이벤트의 트래픽을 삭제합니다. 이는 GID가 1 또는 3이 아닌 규칙에 적용됩니다. GID 1 및 3은 텍스트/컴파일된 규칙(일반적으로 Talos에서 제공하거나 사용자 지정/가져온 규칙)이며, 기타 모든 GID는 변칙에 대한 검사입니다. 이는 네트워크에서 트리거되는 좀 더 드문 규칙입니다. **Prevention(**방지**)** 모드로 변경하면 트래픽에 영향을 미치지 않습니다. 삭제된 트래픽에 적용 가능한 침입 규칙을 비활성화하고 단지 생성 또는 비활성화로 설정해야 합니다.

검사 모드로 **Prevention(**방지**)**을 선택하는 것이 좋지만 **Prevention(**방지**)**을 선택하는 경우 **Detection(**탐지**)** 모드로 되돌릴 수 없습니다.

참고
네트워크 분석 정책 이름, 설명, 기본 정책 및 검사 모드를 수정하면 Snort 2 및 Snort 3 버전에 모두 수정 사항이 적용됩니다. 특정 버전의 검사 모드를 변경하려는 경우 해당 버전의 네트워크 분석 정책 페이지에서 이 작업을 수행할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

네트워크 분석 정책 페이지에서 검사기 검색

네트워크 분석 정책의 Snort 3 버전 페이지에서 검색 창에 관련 텍스트를 입력하여 검사기를 검색해야 할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 2 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 3 **Search(**검색**)** 창에 검색할 검사기 이름 또는 관련 텍스트를 입력합니다.

검색한 텍스트와 일치하는 모든 검사기가 표시됩니다.

예를 들어, **pop**을 입력하면 팝 검사기와 바인더 검사기가 일치하는 결과로 화면에 표시됩니다.

관련 항목

사용자 지정 네트워크 분석 정책 구성의 예, 94 페이지
재정의 항목이 있는 검사기 목록 보기, 91 페이지
네트워크 분석 정책에 사용되는 Snort 3 정의 및 용어, 75 페이지
네트워크 분석 정책 사용자 정의, 86 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 89 페이지

검사기 구성 복사

요구 사항에 따라 네트워크 분석 정책의 Snort 3 버전에 대한 검사기 구성을 복사할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 2 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 3 **Inspectors(**검사기**)**에서 구성을 복사할 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 4 다음 중 하나 또는 모두의 검사기 구성을 클립보드에 복사하려면 **Copy to clipboard(**클립보드에 복사**)** 아이콘을 클릭합니다.

- 왼쪽 열의 **Default Configuration(**기본 컨피그레이션**)**
- 오른쪽 열의 **Overriden Configuration(**재정의된 컨피그레이션**)**

단계 5 필요한 사항을 수정하려면 복사한 검사기 구성을 JSON 편집기에 붙여 넣습니다.

관련 항목

네트워크 분석 정책 사용자 정의, 86 페이지

네트워크 분석 정책 사용자 정의

요구 사항에 따라 네트워크 분석 정책의 Snort 3 버전을 사용자 정의할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

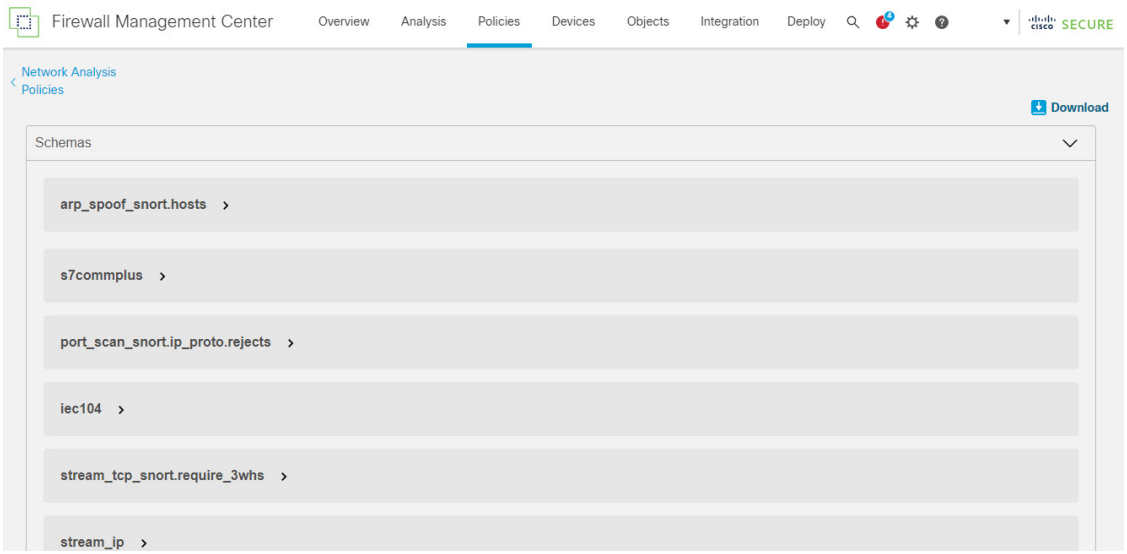
단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 **3** **Actions(**작업**)** 드롭 다운 메뉴를 클릭합니다.

다음 옵션이 표시됩니다.

- 스키마 보기
- 스키마 다운로드/샘플 파일/템플릿 다운로드
- 전체 설정 다운로드
- 재정의 설정 다운로드
- 재정의 설정 업로드

단계 **4** 브라우저에서 스키마 파일을 직접 열려면 **View Schema(**스키마 보기**)**를 클릭합니다.



단계 **5** 필요에 따라 스키마 파일, 샘플 파일/템플릿, 전체 구성 또는 재정의된 구성을 다운로드할 수 있습니다.

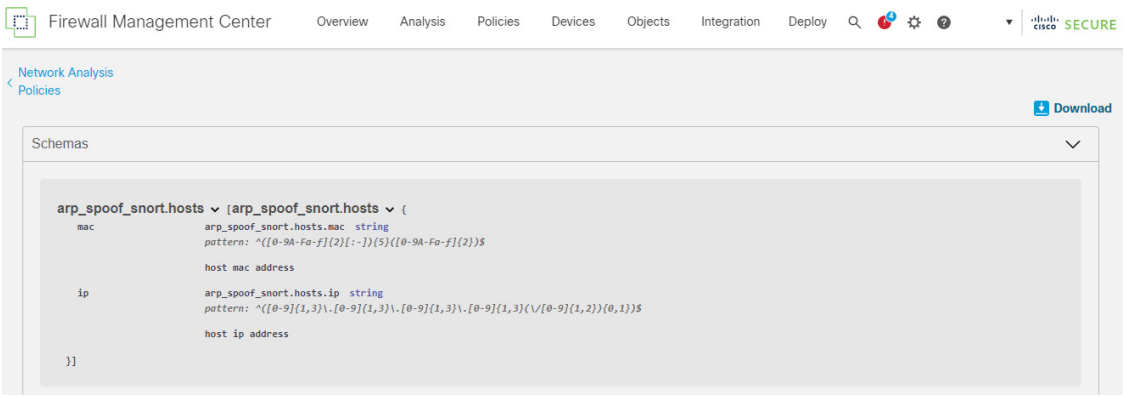
이러한 옵션은 허용되는 값, 범위 및 패턴, 기존 및 기본 검사기 구성, 재정의된 검사기 구성에 대한 통찰력을 제공합니다.

a) **Download Schema(**스키마 다운로드**)**를 클릭하여 스키마 파일을 다운로드합니다.

스키마 파일은 업로드하거나 다운로드하는 콘텐츠를 확인합니다. 서드파티 JSON 편집기를 사용하여 스키마 파일을 다운로드하고 열 수 있습니다. 스키마 파일은 사용할 수 있는 허용되는 값, 범위 및 허용되는 패턴을 사용하여 검사기에 대해 구성할 수 있는 매개 변수를 식별하는 데 도움이 됩니다.

예를 들어 *arp_spoof_snort* 검사기의 경우 호스트를 구성할 수 있습니다. 호스트에는 *mac* 및 *ip* 주소 값이 포함됩니다. 스키마 파일에는 이러한 값에 대해 다음과 같은 허용 패턴이 표시됩니다.

- **mac** – 패턴: `^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **ip** – 패턴:
  `^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}(/[0-9]{1,2}){0,1})$`



검사기 구성을 성공적으로 재정의하려면 스키마 파일의 허용되는 패턴에 따라 값, 범위, 패턴을 제공해야합니다. 그렇지 않으면 오류 메시지가 표시됩니다.

b) **Download Sample File / Template(**샘플 파일/템플릿 다운로드**)**을 클릭하여 예제 구성이 포함된 기존 템플릿을 사용하면 검사기를 구성하는 데 도움이 됩니다.

샘플 파일에 포함된 예제 구성을 참조하여 필요에 따라 변경할 수 있습니다.

c) 전체 검사기 구성을 단일 JSON 파일로 다운로드하려면 **Download Full Configuration(**전체 구성 다운로드**)**을 클릭합니다.

검사기를 개별적으로 확장하는 대신 전체 구성을 다운로드하여 필요한 정보를 찾을 수 있습니다. 검사기 구성과 관련된 모든 정보를 이 파일에서 사용할 수 있습니다.

d) **Download Overridden Configuration(**재정의된 구성 다운로드**)**을 클릭하여 재정의된 검사기 구성을 다운로드합니다.

단계 **6** 기존 구성을 재정의하려면 다음 단계를 수행합니다.

다음과 같은 방법으로 검사기 구성을 재정의하도록 선택할 수 있습니다.

- Management Center에서 직접 검사기에 대해 인라인 수정을 수행합니다. *Cisco Secure Firewall Management Center Snort 3* 구성 가이드의 네트워크 분석 정책 시작하기 장에 있는 검사기에 대한 인라인 수정으로 구성 재정의 항목을 참고하십시오.
- 계속해서 현재 절차를 따라 **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드합니다.

Management Center에서 직접 인라인 수정을 수행하도록 선택한 경우 현재 절차를 더 이상 따를 필요가 없습니다. 그렇지 않은 경우 이 절차를 완전히 따라야 합니다.

a) **Inspectors(**검사기**)**에서 기본 구성을 재정의할 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

검색 창에 관련 텍스트를 입력하여 검사기를 검색해야 할 수 있습니다.

b) 기본 검사기 구성을 클립보드에 복사하려면 **Copy to clipboard(**클립보드에 복사**)** 아이콘을 클릭합니다.

c) JSON 파일을 생성하고 기본 구성을 이 파일에 붙여 넣습니다.

d) 재정의할 검사기 구성을 유지하고 JSON 파일에서 다른 모든 구성 및 인스턴스를 제거합니다.

Sample File/Template(샘플 파일/템플릿**)**을 사용하여 기본 구성을 재정의하는 방법을 이해할 수도 있습니다. 이것은 Snort 3의 네트워크 분석 정책을 사용자 지정할 수 있는 방법을 설명하는 JSON 스니펫이 포함된 샘플 파일입니다.

e) 필요에 따라 검사기 구성을 변경합니다.

변경 사항을 검증하고 스키마 파일을 준수하는지 확인합니다. 멀티톤 검사기의 경우 모든 인스턴스의 바인딩 조건이 JSON 파일에 포함되어 있는지 확인합니다. 자세한 내용은 *Cisco Secure Firewall Management Center Snort 3* 구성 가이드의 **Snort 3**에 대한 맞춤형 네트워크 분석 정책 생성 항목에서 멀티톤 검사기를 참고하십시오.

f) 추가 기본 검사기 구성을 복사하는 경우 재정의된 구성이 포함된 기존 파일에 해당 검사기 구성을 추가합니다.

참고
복사된 검사기 구성은 JSON 표준을 준수해야 합니다.

g) 재정의된 구성 파일을 시스템에 저장합니다.

단계 **7** 을 클릭**Actions(**작업**)** 드롭다운 메뉴에서 Upload Overridden Configuration(재정의된 구성 업로드)를 선택하여 재정의된 구성이 포함된 JSON 파일을 업로드할 수 있습니다.

주의
필요한 변경 사항만 업로드합니다. 전체 구성을 업로드해서는 안 됩니다. 이렇게 하면 재정의가 고정되어 이후에 LSP 업데이트의 일부로 포함되는 기본 구성 변경 사항이 적용되지 않습니다.

파일을 끌어다 놓거나 클릭하여 시스템에 저장된 재정의된 검사기 구성이 포함된 JSON 파일을 찾아볼 수 있습니다.

- **Merge inspector overrides(**검사기 재정의 병합**)** - 공용 검사기가 없는 경우 업로드된 파일의 콘텐츠가 기존 구성과 병합됩니다. 공용 검사기가 있는 경우 업로드된 파일의 콘텐츠(공용 검사기 사용 대상)가 이전 콘텐츠보다 우선하며 해당 검사기의 이전 구성을 대체합니다.
- **Replace inspector overrides(**검사기 재정의 교체**)** - 이전의 모든 재정의를 제거하고 업로드된 파일의 새 콘텐츠로 대체합니다.

  주의
  이 옵션을 선택하면 이전의 모든 재정의가 삭제됩니다. 이 옵션을 사용하여 구성을 재정의하기 전에 정보에 입각한 결정을 내리십시오.

재정의된 검사기를 업로드하는 동안 오류가 발생할 경우 **Upload Overriden Configuration File(**재정의된 구성 파일 업로드**)** 팝업 창에 오류가 표시됩니다. 오류가 있는 파일을 다운로드한 다음 오류를 해결하고 파일을 다시 업로드할 수도 있습니다.

단계 **8** **Upload Overridden Configuration File(**재정의된 구성 파일 업로드**)** 팝업 창에서 **Import(**가져오기**)**를 클릭하여 재정의된 검사기 구성을 업로드합니다.

재정의된 검사기 구성을 업로드하면 검사기 옆에 재정의된 검사기임을 나타내는 주황색 아이콘이 표시됩니다.

또한 검사기 아래의 **Overridden Configuration(**재정의된 구성**)** 열에 재정의된 값이 표시됩니다.

Search(검색) 표시줄 옆에 있는 **Show Overrides Only(**재정의 항목만 표시**)** 확인란을 사용하여 재정의된 모든 검사기를 볼 수도 있습니다.

참고
항상 재정의된 구성을 다운로드한 다음 JSON 파일을 열고 이 파일의 검사기 구성에 새로운 변경/재정의를 추가하십시오. 이 작업은 기존의 재정의된 구성을 잃지 않도록 하는 데 필요합니다.

단계 **9** (선택 사항) 새 검사기 구성을 변경하기 전에 시스템에서 재정의된 구성 파일을 백업합니다.

팁
검사기 구성을 재정의할 때 수시로 백업을 수행하는 것이 좋습니다.

관련 항목

재정의된 구성을 기본 구성으로 되돌리기, 91 페이지
재정의 항목이 있는 검사기 목록 보기, 91 페이지
네트워크 분석 정책 페이지에서 검사기 검색, 84 페이지
검사기 구성 복사 , 85 페이지

검사기에 대한 인라인 수정으로 구성 재정의

네트워크 분석 정책의 Snort 3 버전의 경우, 검사기 구성을 인라인으로 수정하여 요구 사항에 따라 구성을 재정의할 수 있습니다.

또는 **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드할 수도 있습니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 86 페이지를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 **3** **Inspectors(**검사기**)**에서 기본 설정을 재정의할 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 **4** 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Edit Inspector(**검사기 수정**)**(연필) 아이콘을 클릭하여 검사기 구성을 변경합니다.

필요한 사항을 수정할 수 있는 Override Configuration(구성 재정의) 팝업 창이 나타납니다.

참고

- 재정의하려는 설정만 유지해야 합니다. 동일한 값을 사용하여 설정을 유지하면 해당 필드가 고정으로 설정됩니다. 따라서 이후에 Talos에서 해당 설정을 변경할 경우 현재 값이 유지됩니다.
- 사용자 지정 인스턴스를 추가하거나 삭제하는 경우 바인더 검사기에서도 해당 인스턴스에 대한 바인더 규칙을 추가하거나 삭제해야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

JSON 표준에 의거하여 오류가 있는 경우 오류 메시지가 표시됩니다.

단계 **6** **Save(**저장**)**를 클릭하여 변경사항을 저장합니다.

변경 사항이 OpenAPI 스키마 사양을 준수하는 경우 Management Center에서 구성을 저장할 수 있습니다. 그렇지 않은 경우 **Error saving overridden configuration(**재정의 구성 저장 오류**)** 팝업 창에 오류가 표시됩니다. 오류가 포함된 파일을 다운로드할 수도 있습니다.

관련 항목

네트워크 분석 정책 사용자 정의, 86 페이지
인라인 수정 시 저장하지 않은 변경 사항 되돌리기 , 90 페이지
재정의된 구성을 기본 구성으로 되돌리기, 91 페이지
사용자 지정 네트워크 분석 정책 구성의 예, 94 페이지

인라인 수정 시 저장하지 않은 변경 사항 되돌리기

검사기의 컨피그레이션을 재정의하기 위해 인라인 수정을 수행하거나 저장하지 않은 변경 사항을 되돌릴 수 있습니다. 이 작업은 저장하지 않은 모든 변경 사항을 가장 최근에 저장된 값으로 되돌리지만, 구성을 검사기의 기본 구성으로 되돌리는 것은 아닙니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 **3** **Inspectors(**검사기**)**에서 저장되지 않은 변경 사항을 되돌릴 필수 검사기를 확장합니다.

기본 컨피그레이션은 왼쪽 열에 표시되고 재정의된 컨피그레이션은 검사기의 오른쪽 열에 표시됩니다.

단계 **4** 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)** 아래에서 **Cross(**십자**)**(X) 아이콘을 클릭하여 검사기의 저장하지 않은 변경 사항을 되돌립니다.

또는 변경을 취소하려면 **Cancel(취소)**을 클릭합니다.

검사기 컨피그레이션에 대한 저장하지 않은 변경 사항이 없는 경우 이 옵션이 표시되지 않습니다.

관련 항목

재정의된 구성을 기본 구성으로 되돌리기, 91 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 89 페이지

재정의 항목이 있는 검사기 목록 보기

재정의된 모든 검사기 목록을 볼 수 있습니다.

프로시저

단계 **1** **Policies(정책)** > **Intrusion(침입)** > **Network Analysis Policies(네트워크 분석 정책)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3 버전)**으로 이동합니다.

단계 **3** Search(검색) 표시줄 옆에 있는 **Show Overrides Only(재정의 항목만 표시)** 체크 박스를 선택하여 재정의된 검사기 목록을 봅니다.

재정의된 모든 검사기는 이름 옆에 주황색 아이콘이 표시되어 쉽게 식별할 수 있습니다.

관련 항목

네트워크 분석 정책 페이지에서 검사기 검색, 84 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 89 페이지
네트워크 분석 정책 사용자 정의, 86 페이지

재정의된 구성을 기본 구성으로 되돌리기

검사기의 기본 구성을 재정의하기 위해 수행한 변경 사항을 되돌릴 수 있습니다. 다음 작업을 수행하면 재정의된 구성이 검사기의 기본 구성으로 되돌려집니다.

프로시저

단계 **1** **Policies(정책)** > **Intrusion(침입)** > **Network Analysis Policies(네트워크 분석 정책)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3 버전)**으로 이동합니다.

단계 **3** **Inspectors(검사기)**에서 재정의된 구성을 되돌릴 필수 검사기를 확장합니다.

재정의된 검사기는 이름 옆에 주황색 아이콘이 표시됩니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다. 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Revert to default configuration(**기본 구성으로 되돌리기(뒤로 화살표) 아이콘을 클릭하여 검사기의 재정의된 구성을 기본 구성으로 되돌립니다.

검사기의 기본 구성을 변경하지 않은 경우 이 옵션은 비활성화됩니다.

단계 **4** **Revert(**되돌리기**)**를 클릭하여 결정을 확인합니다.

단계 **5** **Save(**저장**)**를 클릭하여 변경사항을 저장합니다.

변경 사항을 저장하지 않으려면 **Cancel(**취소**)** 또는 **Cross(**십자**)**(X) 아이콘을 클릭합니다.

관련 항목

인라인 수정 시 저장하지 않은 변경 사항 되돌리기 , 90 페이지
네트워크 분석 정책 사용자 정의, 86 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 89 페이지
사용자 지정 네트워크 분석 정책 구성의 예, 94 페이지

Snort 3 정책 검증

다음은 Snort 3 정책을 검증하기 위해 사용자가 기록해 둘 수 있는 기본 정보 목록입니다.

- Management Center의 현재 버전은 여러 Threat Defense 버전을 관리할 수 있습니다.
- Management Center의 현재 버전은 Threat Defense 디바이스의 이전 버전에 적용할 수 없는 NAP 구성을 지원합니다.
- 현재 NAP 정책 및 검증은 현재 버전 지원에 따라 작동합니다.
- 변경 사항에 Threat Defense 의 이전 버전에 유효하지 않은 콘텐츠가 포함될 수 있습니다.
- 정책 구성 변경 사항은 현재 버전에 대해 유효한 구성이고 현재 Snort 3 바이너리 및 NAP 스키마를 사용하여 수행되는 경우 수락됩니다.
- 이전 버전 Threat Defense 의 경우 구축 중에 해당 특정 버전에 대한 NAP 스키마 및 Snort 3 바이너리를 사용하여 검증이 수행됩니다. 지정된 버전에 적용할 수 없는 구성이 있는 경우, 지정된 버전에서 지원되지 않는 구성은 구축되지 않으며 나머지 구성만 구축된다는 정보 또는 경고가 사용자에게 제공됩니다.

이 절차에서 NAP 정책을 액세스 제어 정책에 연결하고 이를 디바이스에 구축할 경우, 가령 Snort 3 정책을 검증하는 데 속도 필터 구성과 같은 모든 검사기가 적용됩니다.

프로시저

단계 **1** **NAP** 정책 구성 재정의 단계**:** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**의 **Inspectors(**검사기**)**에서 기본 설정을 재정의할 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 2 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Edit Inspector(**검사기 편집**)**(연필) 아이콘을 클릭하여 rate_filter와 같은 검사기를 변경합니다.

rate_filter 검사기에 필요한 편집을 수행할 수 있는 Override Configuration(구성 재정의) 팝업 창이 나타납니다.

단계 3 **OK(**확인**)**를 클릭합니다.

단계 4 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

또는 **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드할 수도 있습니다.

단계 5 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**에서 **Actions(**작업**)** 드롭다운 메뉴를 클릭합니다.

단계 6 **Upload(**업로드**)**에서 **Overrideden Configuration(**재정의된 구성**)**을 클릭하여 재정의된 구성이 포함된 JSON 파일을 업로드할 수 있습니다.

주의
필요한 변경 사항만 업로드합니다. 전체 구성을 업로드해서는 안 됩니다. 이렇게 하면 재정의가 고정되어 이후에 LSP 업데이트의 일부로 포함되는 기본 구성 변경 사항이 적용되지 않습니다.

파일을 끌어다 놓거나 클릭하여 시스템에 저장된 재정의된 검사기 구성이 포함된 JSON 파일을 찾아볼 수 있습니다.

- **Merge inspector overrides(**검사기 재정의 병합**) -** 공용 검사기가 없는 경우 업로드된 파일의 콘텐츠가 기존 구성과 병합됩니다. 공용 검사기가 있는 경우 업로드된 파일의 콘텐츠(공용 검사기 사용 대상)가 이전 콘텐츠보다 우선하며 해당 검사기의 이전 구성을 대체합니다.
- **Replace inspector overrides(**검사기 재정의 교체**) -** 이전의 모든 재정의를 제거하고 업로드된 파일의 새 콘텐츠로 대체합니다.

  주의
  이 옵션을 선택하면 이전의 모든 재정의가 삭제되므로 이 옵션으로 구성을 재정의하기 전에 정보에 입각하여 올바른 결정을 내려야 합니다.

재정의된 검사기를 업로드하는 동안 오류가 발생할 경우 **Upload Overriden Configuration File(**재정의된 구성 파일 업로드**)** 팝업 창에 오류가 표시됩니다. 오류가 있는 파일을 다운로드한 다음 오류를 해결하고 파일을 다시 업로드할 수도 있습니다.

단계 7 액세스 제어 정책에 **NAP** 정책을 연결하는 단계**:** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 **Edit(**편집**)**을 클릭합니다.

단계 8 **Default Network Analysis Policy(**기본 네트워크 분석 정책**)** 드롭다운 목록에서 기본 네트워크 분석 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, **Edit(**편집**)**을 클릭하여 새 창에서 정책을 편집할 수 있습니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 9 **OK(**확인**)**를 클릭합니다.

단계 10 **Save**를 클릭하여 정책을 저장합니다.

단계 11 아니면 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 **Edit(**편집**)**을 클릭합니다.

단계 **12** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **13** 추가할 조건을 클릭하여 규칙 조건을 구성합니다.

단계 **14** **Network Analysis(**네트워크 분석**)**을 클릭하고 이 규칙과 일치하는 트래픽을 전처리하는 데 사용할 **Network Analysis Policy(**네트워크 분석 정책**)**를 선택합니다.

단계 **15** **Add(**추가**)**를 클릭합니다.

단계 **16** **Deployment(**구축**):** Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment(**구축**)**를 선택합니다.

단계 **17** 컨피그레이션 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스별 구성 변경 사항을 보려면 **Expand Arrow(**확장 화살표**)**를 클릭합니다.

  디바이스 체크 박스를 선택하면 디바이스 아래에 나열된 디바이스에 대한 모든 변경 사항이 푸시되어 구축됩니다. 그러나 **Policy Selection(**정책 선택**)**을 사용하면 나머지 변경 사항을 구축하지 않고 보류하면서 구축할 개별 정책 또는 구성을 선택할 수 있습니다.

  필요에 따라, 수정되지 않은 관련 정책을 선택적으로 보거나 숨기는 데 **Show or Hide Policy(**정책 표시 또는 숨기기**)**를 사용할 수 있습니다.

단계 **18** **Deploy(**구축**)**를 클릭합니다.

단계 **19** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

참고
Snort 3 네트워크 분석 정책에 이 Threat Defense 버전에 대해 유효하지 않은 검사기 또는 속성이 포함되어 있으며 구축 시 잘못된 설정이 생략된다는 경고가 표시됩니다. 잘못된 검사기는 7.1 버전 이하의 디바이스에 대해서만 ["rate_filter"]입니다.

사용자 지정 네트워크 분석 정책 구성의 예

이것은 Snort 3의 네트워크 분석 정책을 사용자 지정할 수 있는 방법을 설명하는 JSON 스니펫이 포함된 샘플 파일입니다. 다음과 같은 방법으로 검사기 구성을 재정의하도록 선택할 수 있습니다.

- Management Center에서 직접 검사기에 대해 인라인 수정을 수행합니다. 검사기에 대한 인라인 수정으로 구성 재정의, 89 페이지의 내용을 참조하십시오.
- **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드합니다. 네트워크 분석 정책 사용자 정의, 86 페이지의 내용을 참조하십시오.

이러한 옵션을 선택하기 전에 네트워크 분석 정책 재정의를 성공적으로 정의하는 데 도움이 되는 다음과 같은 세부 정보와 예를 모두 검토하십시오. 위험과 오류를 방지하기 위해 여기에 설명된 다양한 시나리오의 예를 읽고 이해해야 합니다.

Actions(작업**)** 드롭다운 메뉴에서 검사기 구성을 재정의하도록 선택하는 경우 네트워크 분석 정책 재정의를 위한 JSON 파일을 생성하고 업로드해야 합니다.

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.

다음은 다양한 시나리오의 예입니다.

기본 정책의 기본 상태가 비활성화된 경우 싱글톤 검사기 활성화

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

기본 정책의 기본 상태가 활성화된 경우 싱글톤 검사기 비활성화

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

기본 정책의 기본 상태가 비활성화된 경우 멀티톤 검사기 활성화

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

기본 정책의 기본 상태가 활성화된 경우 멀티톤 검사기 비활성화

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

싱글톤 검사기에 대한 특정 설정의 기본값 재정의

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
```

```
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

멀티톤 검사기에서 기본 인스턴스(인스턴스 이름이 검사기 유형과 일치)의 특정 설정 재정의

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

필요한 변경 사항이 있는 기본 인스턴스에 대한 바인더 규칙 추가

참고 기본 바인더 규칙은 수정할 수 없으며 항상 끝에 추가됩니다.

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

새 사용자 지정 인스턴스 추가

참고 해당하는 바인더 규칙 항목을 바인더 검사기에서 정의해야 합니다.

```
{
  "telnet": {
```

```
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

싱글톤 인스턴스 및 멀티톤 기본 인스턴스 재정의, 단일 **JSON** 재정의에서 새 멀티톤 인스턴스 생성

단일 JSON 재정의에서 다음 사항을 보여주는 예:

- 싱글톤 인스턴스 재정의(**normalizer** 검사기)
- 멀티톤 기본 인스턴스 재정의 (**http_inspect** 검사기)
- 새 멀티톤 인스턴스 생성(**telnet** 검사기)

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
```

```
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

참고 바인더 규칙에서 기본 인스턴스의 **name** 속성은 지정할 필요가 없습니다.

arp_spoof 구성

arp_spoof를 구성하는 예:

arp_spoof 검사기에는 속성에 대한 기본 구성이 없습니다. 다음은 재정의를 제공할 수 있는 경우를 보여줍니다.

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
```

```
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}
```

rate_filter 구성

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

다중 계층 네트워크 분석 정책이 사용되는 경우 바인더 규칙 구성

이 예에서는 하위 정책에 새 사용자 지정 인스턴스를 추가하는 방법과 바인더 규칙을 작성하는 방법을 보여줍니다. 바인더 규칙은 목록으로 정의되므로 규칙이 자동으로 병합되지 않아 상위 정책에 정의된 규칙을 선택하고 이를 기반으로 새 규칙을 작성하는 것이 중요합니다. 하위 정책에서 사용 가능한 바인더 규칙은 전체적으로 적용됩니다.

Threat Defense 에서는 기본 Cisco Talos 정책 규칙이 이러한 사용자 정의 재정의에 추가됩니다.

상위 정책:

telnet_parent_instance라는 이름의 사용자 지정 인스턴스와 해당 바인더 규칙을 정의했습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
```

```
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

하위 정책:

이 네트워크 분석 정책에는 위에서 언급한 정책이 기본 정책으로 포함되어 있습니다. **telnet_child_instance**라는 이름의 사용자 지정 인스턴스를 정의하고 이 인스턴스에 대한 바인더 규칙도 정의했습니다. 상위 정책의 바인더 규칙을 여기에 복사한 다음 규칙의 특성에 따라 하위 정책 바인더 규칙을 그 앞이나 뒤에 추가할 수 있습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
```

```
  }
}
```

일반적인 목록 검사기 속성 구성

목록 유형의 속성에 대한 재정의를 변경하는 동안에는 부분 재정의가 아니라 전체 콘텐츠를 전달하는 것이 중요합니다. 이는 기본 정책 속성이 다음과 같이 정의된 경우를 의미합니다.

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

value1을 **value1-new**로 수정하려는 경우 재정의 페이로드는 다음과 같아야 합니다.

올바른 방법:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

잘못된 방법:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

smtp 검사기에서 **alt_max_command_line_len** 속성의 잘린 값을 가져와서 이 구성을 이해할 수 있습니다. **smtp** 검사기의 기본 정책 구성이 다음과 같다고 가정해 보겠습니다.

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
```

```
            "decompress_zip": false,
            "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "ignore_data": false,
            "max_command_line_len": 512,
            "max_header_line_len": 1000,
            "log_rcptto": false,
            "decompress_swf": false,
            "max_response_line_len": 512,
            "b64_decode_depth": -1,
            "max_auth_command_line_len": 1000,
            "log_email_hdrs": false,
            "xlink2state": "alert",
            "binary_data_cmds": "BDAT XEXCH50",
            "auth_cmds": "AUTH XAUTH X-EXPS",
            "log_filename": false,
            "uu_decode_depth": -1,
            "ignore_tls_data": false,
            "data_cmds": "DATA",
            "bitenc_decode_depth": -1,
            "alt_max_command_line_len": [
              {
                "length": 255,
                "command": "ATRN"
              },
              {
                "command": "AUTH",
                "length": 246
              },
              {
                "length": 255,
                "command": "BDAT"
              },
              {
                "length": 246,
                "command": "DATA"
              }
            ],
            "log_mailfrom": false,
            "decompress_pdf": false,
            "normalize": "none",
            "email_hdrs_log_depth": 1464,
            "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "qp_decode_depth": -1
          }
        }
      ],
      "enabled": true
    }
}
```

이제 다음과 같이 **alt_max_command_line_len** 목록에 두 개의 개체를 더 추가합니다.

```
{
    "length": 246,
    "command": "XEXCH50"
```

```
},
{
    "length": 246,
    "command": "X-EXPS"
}
```

그러면 사용자 지정 네트워크 분석 정책 재정의 JSON이 다음과 같이 표시됩니다.

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

다중 계층 네트워크 분석 정책이 멀티톤 검사기에서 사용되는 경우 바인더 규칙 구성

이 예에서는 하위 정책의 속성을 재정의하는 방법과 병합된 구성이 인스턴스의 하위 정책에 사용되는 방식을 보여줍니다. 하위 정책에 정의된 모든 재정의는 상위 정책과 병합됩니다. 예를 들어 속성 1과 속성 2가 상위 정책에서 재정의되고 속성 2와 속성 3이 하위 정책에서 재정의되는 경우 병합된 구성이 하위 정책에 적용됩니다. 즉, 속성 1(상위 정책에 정의됨), 속성 2(하위 정책에 정의됨) 및 속성 3(하위 정책에 정의됨)이 디바이스에 구성됩니다.

상위 정책:

여기서는 **telnet_parent_instance**라는 이름의 사용자 지정 인스턴스를 정의하고 사용자 지정 인스턴스에서 **normalize**와 **encrypted_traffic**이라는 2개의 속성을 재정의했습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

하위 정책:

이 네트워크 분석 정책에는 위에서 언급한 정책이 기본 정책으로 포함되어 있습니다. 상위 정책에서 **encrypted_traffic** 속성을 재정의했으며 새 속성 **ayt_attack_thresh**도 재정의했습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

위의 정책 JSON을 사용하면 네트워크 분석 정책을 구축할 때 다음과 같이 병합된 JSON이 디바이스에 구성됩니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
```

```
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

이 예에서는 사용자 지정 네트워크 분석 정책의 세부 사항을 보여줍니다. 기본 인스턴스에서도 동일한 동작이 나타납니다. 또한 싱글톤 검사기에서도 유사한 병합이 수행됩니다.

네트워크 분석 정책에 대한 모든 검사기 재정의 제거:

특정 네트워크 분석 정책에 대한 모든 재정의를 제거할 때마다 빈 JSON을 업로드할 수 있습니다. 재정의를 업로드하는 동안 **Replace inspector overrides(**검사기 재정의 교체**)** 옵션을 선택합니다.

```
{
}
```

관련 항목

네트워크 분석 정책에 사용되는 Snort 3 정의 및 용어, 75 페이지
네트워크 분석 정책 매핑, 83 페이지
Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 77 페이지
네트워크 분석 정책 페이지에서 검사기 검색, 84 페이지
검사기 구성 복사 , 85 페이지
네트워크 분석 정책 사용자 정의, 86 페이지
재정의 항목이 있는 검사기 목록 보기, 91 페이지

네트워크 분석 정책 설정 및 캐시된 변경 사항

새로운 네트워크 분석 정책을 생성하는 경우 해당 기본 정책의 설정과 동일합니다.

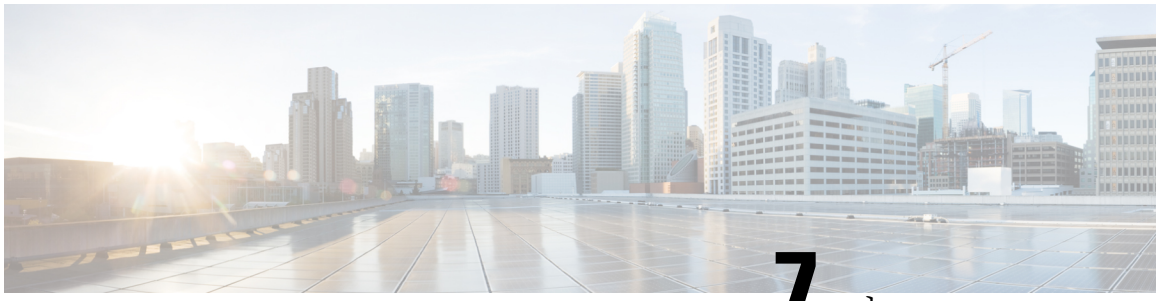
네트워크 분석 정책을 조정할 경우, 특히 검사기를 비활성화할 경우, 일부 검사기 및 침입 규칙은 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 검사기를 비활성화한 경우, 검사기가 네트워크 분석 정책 웹 사용자 인터페이스에서 비활성화된 상태로 남아 있다고 해도 시스템은 자동으로 검사기를 현재의 설정으로 사용합니다.

참고 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.

시스템은 사용자당 1개의 네트워크 분석 정책을 캐시합니다. 네트워크 분석 정책을 수정하는 동안 모든 메뉴 또는 다른 페이지로 이동하는 다른 경로를 선택하는 경우, 해당 페이지를 벗어난다고 해도 변경 사항은 시스템 캐시에 유지됩니다.

III 부

Snort 3의 암호화된 가시성 엔진



7 장

암호화된 가시성 엔진

EVE(암호화된 가시성 엔진)는 TLS 암호화를 사용하는 클라이언트 애플리케이션 및 프로세스를 식별하는 데 사용됩니다. 이를 통해 가시성이 향상되며 관리자가 작업을 수행하고 환경 내에서 정책을 시행할 수 있습니다. EVE 기술은 악성코드를 식별하고 중지하는 데도 사용할 수 있습니다.

암호화된 가시성 엔진 개요

암호화된 가시성 엔진(EVE)은 암호를 해독하지 않고도 암호화된 세션에 대한 더 많은 가시성을 제공하는 데 사용됩니다. 암호화된 세션에 대한 이러한 인사이트는 Cisco의 VDB(취약성 데이터베이스)에 패키지된 Cisco의 오픈 소스 라이브러리에서 가져옵니다. 라이브러리는 암호화된 수신 세션을 핑거프린트하고 분석하여 알려진 핑거프린트 집합과 일치시킵니다. 이 알려진 핑거프린트 데이터베이스는 Cisco VDB에서도 사용할 수 있습니다.

참고 암호화된 가시성 엔진 기능은 Snort 3을 실행하는 Management Center 매니지드 디바이스에서만 지원됩니다. 이 기능은 Snort 2 디바이스, device manager 매니지드 디바이스 또는 CDO에서 지원되지 않습니다.

EVE의 몇 가지 중요한 기능은 다음과 같습니다.

- EVE에서 파생된 정보를 사용하여 트래픽에 대한 액세스 제어 정책 작업을 수행할 수 있습니다.
- Cisco Secure Firewall에 포함된 VDB에는 높은 신뢰도 값으로 EVE에서 탐지한 일부 프로세스에 애플리케이션을 할당할 수 있는 기능이 있습니다. 또는 맞춤형 애플리케이션 탐지기를 생성하여 다음을 수행할 수 있습니다.

- EVE 탐지 프로세스를 새로운 사용자 정의 애플리케이션에 매핑합니다.
- EVE 탐지 프로세스에 애플리케이션을 할당하는 데 사용되는 프로세스 신뢰도의 기본 제공 값을 재정의합니다.

  Cisco Secure Firewall Management Center 구성 가이드의 애플리케이션 탐지 장에 나와 있는 사용자 지정 애플리케이션 탐지기 구성 및 **EVE** 프로세스 할당 지정 섹션을 참조하십시오.

- EVE는 암호화된 트래픽에서 클라이언트 Hello 패킷을 생성한 클라이언트의 운영 체제 유형 및 버전을 탐지할 수 있습니다.
- EVE는 QUIC(빠른 UDP 인터넷 연결) 트래픽의 핑거프린트 및 분석도 지원합니다. Client Hello 패킷의 서버 이름이 **Connection Events(**연결 이벤트**)** 페이지의 URL 필드에 표시됩니다.

주의 Management Center에서 EVE를 사용하려면 디바이스에 유효한 IPS 라이선스가 있어야 합니다. IPS 라이선스가 없으면 정책에 경고가 표시되고 구축이 허용되지 않습니다.

참고

- EVE는 SSL 세션의 운영 체제 유형 및 버전을 탐지할 수 있습니다. 애플리케이션, 패키지 관리 소프트웨어 등을 실행하는 등 운영 체제를 정상적으로 사용하면 OS 탐지가 트리거될 수 있습니다. 클라이언트 OS 탐지를 보려면 EVE 토글 버튼을 활성화하는 것 외에도 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**에서 **Hosts(**호스트**)**를 활성화해야 합니다. 호스트 IP 주소에서 가능한 운영 체제 목록을 보려면 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**을 클릭한 다음 필요한 호스트를 선택합니다.
- EVE는 캡슐화된 트래픽에 대한 가시성 또는 인사이트를 제공하지 않습니다.

관련 링크

EVE 구성, 112 페이지
EVE 예외 규칙 구성, 115 페이지

EVE의 작동 방식

EVE(암호화된 가시성 엔진)는 TLS 핸드셰이크의 Client Hello 부분을 검사하여 클라이언트 프로세스를 식별합니다. Client Hello는 서버로 전송되는 초기 데이터 패킷입니다. 이것으로 호스트의 클라이언트 프로세스를 확인할 수 있습니다. 이 핑거프린트는 대상 IP 주소 와 같은 다른 데이터와 결합되어 EVE의 애플리케이션 식별을 위한 기반을 제공합니다. TLS 세션 설정에서 특정 애플리케이션 핑거프린트를 식별함으로써, 시스템은 클라이언트 프로세스를 식별하고 적절한 작업(허용/차단)을 취할 수 있습니다.

EVE는 5,000개가 넘는 클라이언트 프로세스를 식별할 수 있습니다. 시스템은 액세스 제어 규칙의 기준으로 사용할 수 있도록 이러한 프로세스 중 일부를 클라이언트 애플리케이션에 매핑합니다. 이를

통해 시스템에서는 TLS 해독을 활성화하지 않고도 이러한 애플리케이션을 식별하고 제어할 수 있습니다. EVE 기술은 알려진 악의적인 프로세스의 핑거프린트를 사용하여 아웃바운드 해독 없이 암호화된 악의적인 트래픽을 식별하고 차단하는 데에도 사용될 수 있습니다.

Cisco는 머신러닝(ML) 기술을 통해 10억 개 이상의 TLS 핑거프린트와 10,000개 이상의 악성코드 샘플을 매일 처리하여 EVE 핑거프린트를 생성하고 업데이트 합니다. 이러한 업데이트는 Cisco VDB(Vulnerability Database) 패키지를 사용하는 고객에게 제공됩니다.

EVE는 핑거프린트를 인식하지 못하는 경우 클라이언트 애플리케이션을 식별하고 IP 주소, 포트 및 서버 이름과 같은 대상 세부 정보를 사용하여 첫 번째 플로우의 위협 점수를 추정합니다. 이 시점에서 핑거프린트의 상태는 임의 지정되며 디버그 로그에서 상태를 볼 수 있습니다. 핑거프린트가 동일한 후속 플로우의 경우 EVE는 재분석을 건너뛰고 핑거프린트 상태를 레이블 없음으로 표시합니다. EVE의 낮음 또는 매우 낮음 점수 임계값에 따라 트래픽을 차단하려는 경우 초기 플로우가 차단됩니다. 그러나 애플리케이션의 지문이 캐시되면 이후 플로우는 허용됩니다.

보안 침해 지표 이벤트

암호화된 가시성 엔진 탐지에 대한 호스트의 보안 침해 지표(IoC) 이벤트를 사용하면 EVE에서 보고한 대로 악성코드 신뢰도 수준이 매우 높은 연결 이벤트를 확인할 수 있습니다. IoC 이벤트는 악성 클라이언트를 사용하는 호스트에서 생성된 암호화된 세션에 대해 트리거됩니다. 악성 호스트의 IP 주소, MAC 주소, OS 정보 및 의심스러운 활동의 타임스탬프와 같은 정보를 볼 수 있습니다.

연결 이벤트에서 암호화된 가시성 위협 신뢰도 점수가 'Very High(매우 높음)'인 세션은 IoC 이벤트를 분류합니다. **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**에서 **Hosts(**호스트**)**를 활성화해야 합니다. Management Center의 다음에서 IoC 이벤트 존재 여부를 확인할 수 있습니다.

- **Analysis(**분석**)** > **Indications of Compromise(**보안 침해 지표**)**
- **Analysis(**분석**)** > **Network Map(**네트워크 맵**)** > **Indications of Compromise(**보안 침해 지표**)** > 선택해야 하는 호스트를 선택합니다.

  다음에서 IoC를 생성한 세션의 프로세스 정보를 볼 수 있습니다.

  Analysis(분석**)** > **Connection Events(**연결 이벤트**)** > **Table View of Connection Events(**연결 이벤트의 테이블 보기**)** > **IoC** 열. Encrypted Visbility(암호화된 가시성) 필드 및 IoC 필드를 수동으로 선택해야 합니다.

EVE의 QUIC 핑거프린팅

Snort는 EVE를 기반으로 Quick UDP 인터넷 연결(QUIC 세션)에서 클라이언트 애플리케이션을 식별할 수 있습니다. QUIC 핑거프린트는 다음을 수행할 수 있습니다.

- 암호 해독을 활성화하지 않고 QUIC를 통해 애플리케이션을 탐지합니다.
- 암호 해독을 활성화하지 않고 악성코드를 식별합니다.
- 서비스 애플리케이션을 탐지합니다. QUIC 프로토콜을 통해 탐지된 서비스를 기반으로 액세스 제어 규칙을 할당할 수 있습니다.

EVE 구성

프로시저

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

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

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

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

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

단계 6 **Use EVE for Application Detection(**애플리케이션 탐지에 **EVE** 사용**)**—이 토글 버튼은 기본적으로 활성화되어 있으며, 이는 EVE가 프로세스에 클라이언트 애플리케이션을 할당할 수 있음을 의미합니다.

연결 이벤트 또는 통합 이벤트의 **Encrypted Visibility Fingerprint(**암호화된 가시성 핑거프린트**)** 열 헤더에 EVE의 핑거프린트 정보가 추가됩니다. 수집된 EVE 데이터를 추가로 분석하려면 핑거프린트 정보를 마우스 오른쪽 버튼으로 클릭하여 드롭다운 메뉴를 엽니다. 메뉴에서 **View Encrypted Visibility Engine Process Analysis(**암호화된 가시성 엔진 프로세스 분석 보기**)**를 클릭하여 appid.cisco.com으로 이동해 핑거프린트, VDB 버전 등의 세부 정보를 확인합니다. 핑거프린트 문자열이 동일한 여러 행과 이러한 행과 관련된 잠재적 프로세스 이름 및 발생률이 표시됩니다. 발생률은 데이터 수집 시스템의 특정 핑거프린트와 관련된 프로세스의 빈도를 나타냅니다. 프로세스 이름을 선택하고 **Submit Request(**요청 제출**)**를 클릭하여 EVE의 프로세스 탐지의 불일치에 대한 피드백을 제공할 수 있습니다. 예를 들어 탐지된 프로세스 이름이 전송되는 트래픽과 일치하지 않거나 특정 핑거프린트에 대해 프로세스 이름이 전혀 탐지되지 않는 경우 요청을 제출할 수 있습니다.

Use EVE for Application Detection(애플리케이션 탐지에 **EVE** 사용) 토글 버튼을 비활성화합니다.

- AppID로 식별된 클라이언트가 프로세스에 할당되고 EVE 프로세스 및 점수를 볼 수 있지만 EVE 탐지 프로세스가 애플리케이션에 매핑되지 않으며 작업이 수행되지 않습니다. **Connection Events(**연결 이벤트**)** 또는 **Unified Events(**통합 이벤트**)**에서 이벤트의 상세정보를 볼 수 있습니다. 연결 이벤트(애플리케이션 할당 포함 및 제외)의 차이를 확인하려면 **Client Application(**클라이언트 애플리케이션**)** 열 헤더를 참조하십시오.
- 연결 이벤트 또는 통합 이벤트의 **Encrypted Visibility Fingerprint(**암호화된 가시성 핑거프린트**)** 필드가 비어 있습니다.

단계 7 **Block Traffic Based on EVE Score(EVE** 점수 기준으로 트래픽 차단**)** 토글 버튼을 활성화하여 EVE의 위협 신뢰도 점수를 기준으로 트래픽을 차단합니다. 잠재적인 위협인 모든 수신 트래픽은 기본적으로 차단됩니다.

기본 차단 임계값은 99%이며, 이는 다음을 의미합니다.

- EVE가 트래픽을 99% 이상의 신뢰도로 악성코드로 탐지하면 트래픽이 차단됩니다.

- EVE가 트래픽을 99% 미만의 신뢰도로 악성코드로 탐지하는 경우, EVE는 작업을 수행하지 않습니다.

참고
EVE가 트래픽을 차단한 경우 **Connection Events(**연결 이벤트**)** 페이지에서 **Reason(**이유**)** 열 헤더에 **Encrypted Visiblity Block(**암호화된 가시성 차단**)**이 표시됩니다.

단계 **8** 슬라이더를 사용하여 **Very Low(**매우 낮음**)**에서 **Very High(**매우 높음**)**까지 EVE의 위협 신뢰도에 따라 차단 임계값을 조정할 수 있습니다.

단계 **9** 더 세부적인 제어를 위해 **Advanced Mode(**고급 모드**)** 토글 버튼을 활성화합니다. 이제 트래픽 차단에 대한 특정 EVE 위협 신뢰도 점수를 할당할 수 있습니다. 기본 차단 임계값은 99%입니다.

주의
최적의 성능을 보장하기 위해 임계값을 50% 미만으로 설정하는 것이 좋습니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다.

EVE 이벤트 보기

Encrypted Visibility Engine(암호화된 가시성 엔진**)**이 활성화되고 액세스 제어 정책이 구축되면 시스템을 통해 라이브 트래픽 전송을 시작할 수 있습니다. **Connection Events(**연결 이벤트**)** 페이지에서 로깅된 연결 이벤트를 볼 수 있습니다. 연결 이벤트에 액세스하려면 Management Center에서:

프로시저

단계 **1** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 클릭합니다.

단계 **2** **Table View of Connection Events(**연결 이벤트 테이블 보기**)** 탭을 클릭합니다.

Analysis(분석 **)** 메뉴 아래에 있는 **Unified Events(**통합 이벤트**)** 뷰어에서 연결 이벤트 필드를 볼 수도 있습니다.

암호화 가시성 엔진은 연결을 시작한 클라이언트 프로세스, 클라이언트의 OS 및 프로세스에 악성코드가 포함되어 있는지 여부를 식별할 수 있습니다.

Connection Events(연결 이벤트**)** 페이지에서 Encrypted Visibility Engine(암호화된 가시성 엔진)에 대해 추가된 다음 열을 명시적으로 활성화해야 합니다.

- 암호화된 가시성 프로세스 이름

- 암호화된 가시성 프로세스 신뢰도 점수
- 암호화된 가시성 위협 신뢰도
- 암호화된 가시성 위협 신뢰도 점수
- 탐지 유형

이러한 필드에 대한 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 연결 및 보안 관련 연결 이벤트 장에서 연결 및 보안 인텔리전스 이벤트 필드 섹션을 참조하십시오.

참고 **Connection Events(**연결 이벤트**)** 페이지에서 프로세스에 애플리케이션이 할당된 경우 **Detection Type(**탐지 유형**)** 열에 EVE에서 클라이언트 애플리케이션을 식별했음을 나타내는 암호화된 가시성 엔진이 표시됩니다. 프로세스 이름에 애플리케이션을 할당하지 않은 경우 **Detection Type(**탐지 유형**)** 열에 클라이언트 애플리케이션을 식별한 엔진이 AppID임을 나타내는 **AppID**가 표시됩니다.

EVE 대시보드 보기

다음 대시보드에서 EVE 분석 정보를 볼 수 있습니다.

시작하기 전에

EVE(암호화된 가시성 엔진) 위젯을 보려면 다음을 수행합니다.

- 액세스 제어 정책에서 **Advanced Settings(**고급 설정**)** 에서 **Encrypted Visisibility Engine(EVE)(**암호화된 가시성 엔진**)**을 활성화해야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Dashboards(**대시보드**)**로 이동하고 **Dashboard(**대시보드**)**를 클릭합니다.

단계 **2** **Summary Dashboard(**요약 대시보드**)** 창에서 스위치 대시보드 링크를 클릭하고 드롭다운 상자에서 **Application Statistics(**애플리케이션 통계**)**를 선택합니다.

단계 **3** 다음 두 개의 대시보드를 보려면 **Encrypted Visibility Engine(**암호화 가시성 엔진**)** 탭을 선택합니다.

- **Top Encrypted Visibility Engine Discovered Processes(**상위 **TLS** 핑거프린트 발견 프로세스**)** - 네트워크에서 사용 중인 상위 클라이언트 프로세스 이름 및 연결 수를 표시합니다. 테이블에서 프로세스 이름을 클릭하면 프로세스 이름별로 필터링된 **Connection Events(**연결 이벤트**)** 페이지의 필터링된 보기를 볼 수 있습니다.
- **Connections by Encrypted Visibility Engine(**암호화된 가시성 엔진에 의한 연결**)** — 신뢰 수준(Very High(매우 높음), Very Low(매우 낮음) 등)별로 연결을 표시합니다. 테이블에서 위협 신뢰

도 레벨을 클릭하여 신뢰도 레벨별로 필터링된 **Connection Events(**연결 이벤트**)** 페이지의 필터링된 보기를 볼 수 있습니다.

EVE 예외 규칙 구성

EVE의 차단 조치를 우회하여 신뢰할 수 있는 연결 및 서비스의 연속성을 보장하기 위해 EVE(암호화된 가시성 엔진) 예외 규칙을 생성할 수 있습니다. 예외 규칙에 프로세스 이름 및 대상 IP 주소와 같은 속성을 추가할 수 있습니다. 예를 들어 신뢰할 수 있는 네트워크에 대해 EVE의 차단 판정을 우회하고자 할 수 있습니다. 우회된 네트워크의 모든 연결은 위협 신뢰 수준을 기반으로 EVE의 차단 판정에서 제외됩니다.

프로시저

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

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

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

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

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

단계 **6** **Block Traffic Based on EVE Score(EVE** 점수 기준으로 트래픽 차단**)** 토글 버튼을 활성화하여 EVE의 위협 신뢰도 수준을 기준으로 트래픽을 차단합니다.

단계 **7** **Add Exception Rule(**예외 규칙 추가**)**을 클릭하고 다음 속성 중 하나 이상을 추가합니다.

a) **Process Name(**프로세스 이름**)** 탭에서 EVE 식별 프로세스 이름을 입력하고 창 오른쪽의 **Add to Process(**프로세스에 추가**)**를 클릭합니다.

동일한 예외 규칙에 여러 프로세스 이름을 추가할 수 있습니다. 프로세스 이름을 기반으로 하는 EVE 예외 목록은 대/소문자 및 공백을 구분하는 EVE 식별 프로세스 이름에서만 작동합니다.

b) **Network Objects(**네트워크 개체**)** 탭에서 다음 중 하나를 수행합니다.

- 목록에서 IP 주소를 하나 이상 선택하고 **Selected Networks(**선택한 네트워크**)** 목록에 추가합니다.
- **Selected Networks(**선택한 네트워크**)** 아래에 IP 주소를 수동으로 입력하고 **+** 아이콘을 클릭하여 선택한 네트워크 목록에 추가합니다.

c) (선택 사항) 모든 탭에서 사용 가능한 **Comment(**의견**)** 필드에 필수 속성을 EVE 예외 규칙에 추가하는 이유를 입력할 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭하여 EVE 예외 규칙을 저장합니다.

단계 **9** 디바이스에 액세스 제어 정책을 저장하고 구축합니다.

참고 연결은 예외 규칙과 일치하는 경우, EVE의 차단 판정을 우회합니다. 통합 이벤트 뷰어에서 EVE의 작업을 볼 수 있습니다. **Reason(**이유**)** 열 헤더에는 이러한 EVE가 우회한 트래픽이 식별 되기 때문에 **EVE Exempted(EVE** 제외됨**)**가 표시됩니다.

통합 이벤트에서 예외 규칙 추가

Unified Events(통합 이벤트**)** 창을 사용하여 EVE에 의해 차단된 연결에 대한 예외 규칙을 추가할 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 클릭합니다.

단계 **2** **Encrypted Visibility Block(**암호화된 가시성 차단**)**을 이유로 한 **Reason(**이유**)** 열에서 셀 내부의 줄임표 아이콘(3개의 세로 점)을 클릭합니다.

단계 **3** 드롭다운 목록에서 **Add EVE Exception Rule(EVE** 예외 규칙 추가**)**을 선택합니다.

단계 **4** 표시되는 **Encrypted Visibility Engine(**암호화된 가시성 엔진**)** 창에서 규칙은 예외 목록의 맨 아래에 자동으로 추가됩니다. 구성을 저장 및 구축하기 전에 추가된 규칙을 검토하고 변경할 수 있습니다.

이벤트 강화

MITRE ATT 및 CK에 대한 컨텍스트 보강은 Talos 분류 및 EVE(암호화된 가시성 엔진)에서 제공됩니다. Talos 와 EVE 보강은 모두 Talos 분류를 사용하여 전달됩니다. EVE 보강은 EVE가 활성화된 경우에 작동합니다. EVE 활성화에 대한 자세한 내용은 EVE 구성, 112 페이지의 내용을 참조하십시오.

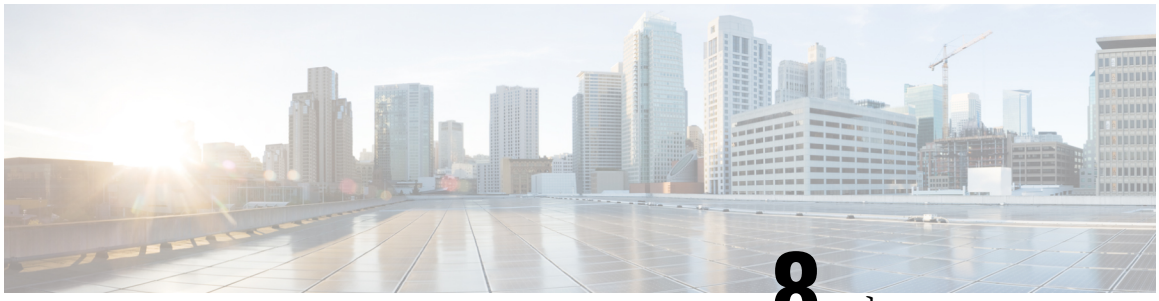
Connection Events(연결 이벤트**)** 페이지에서 보강 이벤트 콘텐츠의 일부로 추가된 다음 열 헤더를 볼 수 있습니다. 이러한 열을 명시적으로 활성화해야 합니다.

- **MITRE ATT&CK**
- 기타 강화

이러한 필드에 대한 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드 7.6의 연결 및 보안 관련 연결 이벤트 장에서 연결 및 보안 인텔리전스 이벤트 필드 섹션을 참조하십시오.

IV 부

Snort 3의 엘리펀트 플로우 탐지



8 장

엘리펀트 플로우 탐지

엘리펀트 플로우는 네트워크 링크를 통해 측정된 TCP(또는 기타 프로토콜) 플로우에 의해 설정된 매우 큰(총 바이트) 연속 플로우입니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큰 상태입니다. 이로 인해 Snort 코어에서 성능 저하가 발생할 수 있습니다. 엘리펀트 플로우는 많지 않지만 일정 기간 동안 총 대역폭의 과도한 공유를 차지할 수 있습니다. 이로 인해 높은 CPU 사용률, 패킷 삭제 등의 문제가 발생할 수 있습니다.

Management Center 7.2.0부터(Snort 3 디바이스만 해당) 엘리펀트 플로우 기능을 사용하여 엘리펀트 플로우를 탐지하고 교정할 수 있습니다. 이는 시스템 스트레스를 줄이고 언급된 문제를 해결하는 데 도움이 됩니다.

엘리펀트 플로우 탐지 및 교정 정보

엘리펀트 플로우 탐지 기능을 사용하여 엘리펀트 플로우를 탐지하고 교정할 수 있습니다. 적용할 수 있는 교정 작업은 다음과 같습니다.

- **Bypass elephant flow(**엘리펀트 플로우 우회**)** - Snort 검사를 우회하도록 엘리펀트 플로우를 구성할 수 있습니다. 구성된 경우 Snort는 해당 플로우에서 패킷을 수신하지 않습니다.
- **Throttle elephant flow(**엘리펀트 플로우 제한**)** – 플로우에 속도 제한을 적용하고 플로우를 계속 검사합니다. 플로우 속도는 동적으로 계산되며, 플로우 속도의 10%가 감소합니다. Snort는 판정(플로우 속도가 10% 감소한 QoS 플로우)을 방화벽 엔진으로 전송합니다. 식별되지 않은 애플리케이션을 포함하여 모든 애플리케이션을 우회하도록 선택하는 경우, 어떤 플로우에 대해서도 스로틀 작업(속도 제한)을 구성할 수 없습니다.

참고 엘리펀트 플로우 탐지가 작동하려면 Snort 3이 탐지 엔진이어야 합니다.

Intelligent Application Bypass에서 엘리펀트 플로우 업그레이드

IAB(Intelligent Application Bypass)는 7.2.0 이상 버전의 Snort 3 디바이스에 더 이상 사용되지 않습니다.

7.2.0 이상을 실행하는 디바이스의 경우, AC 정책의 **Elephant Flow Settings(**엘리펀트 플로우 설정**)**(Advanced settings(고급 설정) 탭)에서 엘리펀트 플로우 설정을 구성해야 합니다.

7.2.0 이상으로 업그레이드한 후 Snort 3 디바이스를 사용하는 경우 엘리펀트 플로우 설정은 **Intelligent Application Bypass Settings(IAB(Intelligent Application Bypass)** 설정**)** 섹션이 아닌 **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 섹션에서 선택 및 구축됩니다. 따라서 엘리펀트 플로우 구성 설정으로 마이그레이션되지 않은 디바이스는 다음 구축 시 엘리펀트 플로우 구성을 잃게 됩니다.

다음 표에는 Snort 3 또는 Snort 2 엔진을 실행하는 7.2.0 이상 버전 및 7.1.0 이하 버전에 적용할 수 있는 IAB 또는 엘리펀트 플로우 구성이 나와 있습니다.

Management Center	**Threat Defense**	엘리펀트 플로우 또는 **IAB** 구성
Management Center 7.0 또는 7.1	Snort 2 디바이스	IAB의 구성을 적용할 수 있습니다.
	Snort 3 디바이스	IAB의 구성을 적용할 수 있습니다.
Management Center 7.2.0	Snort 2 디바이스	IAB의 구성을 적용할 수 있습니다.
	Snort 3 디바이스(7.1.0 이하)	IAB의 구성을 적용할 수 있습니다.
	Snort 3 디바이스(7.2.0 이상)	엘리펀트 플로우의 구성을 적용할 수 있습니다.

엘리펀트 플로우 구성

엘리펀트 플로우에서 작업을 수행하도록 엘리펀트 플로우를 구성할 수 있습니다. 이는 시스템 위협, 높은 CPU 사용률, 패킷 삭제 등의 문제를 해결하는 데 도움이 됩니다.

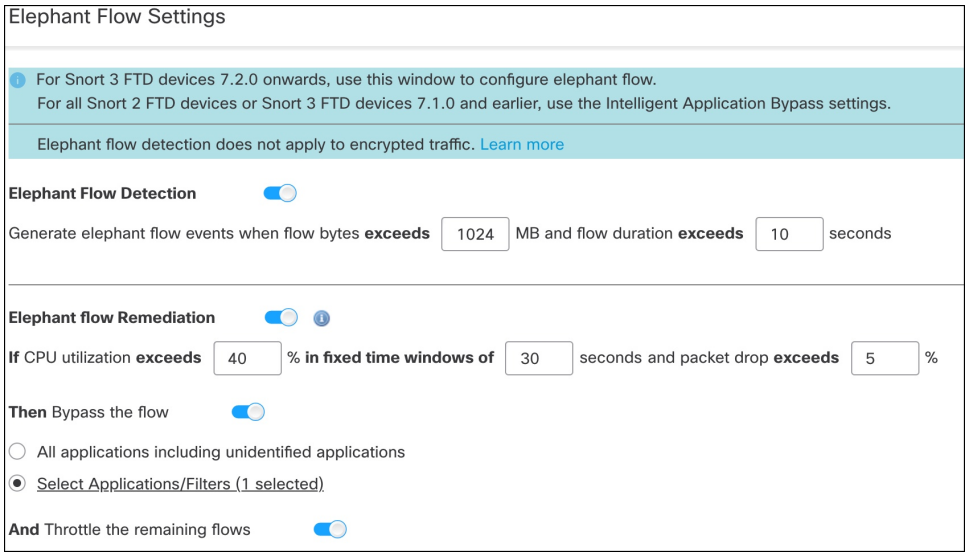
주의 Snort를 통해 처리하지 않는 사전 필터링되거나, 신뢰할 수 있거나, 빠르게 전달된 플로우에는 엘리펀트 플로우 탐지를 적용할 수 없습니다. Snort에서 엘리펀트 플로우를 탐지하므로 암호화된 트래픽에는 엘리펀트 플로우 탐지를 적용할 수 없습니다.

프로시저

단계 1 액세스 제어 정책 편집기에서 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 클릭합니다. 그런 다음 **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 옆에 있는 편집(✎)을 클릭합니다.

보기 아이콘(보기(👁))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

그림 ***2:*** 엘리펀트 플로우 탐지 구성



단계 2 **Elephant Flow Detection(**엘리펀트 플로우 탐지**)** 토글 버튼은 기본적으로 활성화되어 있습니다. 플로우 바이트 및 플로우 지속시간의 값을 구성할 수 있습니다. 설정된 값을 초과하면 엘리펀트 플로우 이벤트가 생성됩니다.

단계 3 엘리펀트 플로우를 교정하려면 **Elephant Flow Remediation(**엘리펀트 플로우 교정**)** 토글 버튼을 활성화합니다.

단계 4 엘리펀트 플로우의 교정 기준을 설정하려면 CPU 사용률(%), 고정 기간의 지속 시간 및 패킷 삭제율(%) 값을 구성합니다.

CPU 사용률은 엘리펀트 플로우 별로 계산되며 플로우 레이턴시에서 파생됩니다. CPU 사용률이 설정된 임계값을 초과하고 고정 기간 및 패킷 삭제 등의 다른 구성도 일치하는 경우, 엘리펀트 플로우 교정 작업이 적용됩니다. 마찬가지로, 패킷 삭제 계산은 CPU당 삭제되는 패킷을 기반으로 합니다. 패킷 삭제 퍼센트가 특정 CPU에 설정된 값을 초과하면 교정 작업이 적용됩니다. 예를 들어 구성이 기본값(CPU 사용률 40%, 고정 기간 30초, 패킷 삭제 5%)으로 설정되어 있다고 가정합니다. 특정 CPU에서, 패킷 삭제의 5% 이상이 탐지되고 30초의 고정 시간 프레임 안에 플로우 당 CPU 사용률이 40%를 초과할 경우 플로우가 우회되거나 제한됩니다.

단계 5 엘리펀트 플로우 교정이 구성된 기준을 충족하는 경우 다음 작업을 수행할 수 있습니다.

1. **Bypass the flow(**플로우 우회**)** - 선택한 애플리케이션 또는 필터에 대해 Snort 검사를 우회하려면 이 버튼을 활성화합니다. 다음 중에서 선택합니다.

   - **All applications including unidentified applications(**알 수 없는 애플리케이션을 포함한 모든 애플리케이션**)** - 모든 애플리케이션 트래픽을 우회하려면 이 옵션을 선택합니다. 이 옵션을 구성하는 경우 어떤 플로우의 스로틀 작업(속도 제한)도 구성할 수 없습니다.
   - **Select Applications/Filters**(애플리케이션/필터 선택) - 트래픽을 우회하려는 애플리케이션 또는 필터를 선택하려면 이 옵션을 선택합니다. Cisco Secure Firewall Management Center 디바이스 컨피그레이션 가이드 의 액세스 제어 규칙 장에서 애플리케이션 조건 및 필터 구성항목을 참조하십시오.

2. **Throttle flow(**플로우 제한**)** – 플로우에 속도 제한을 적용하고 플로우를 계속 검사하려면 이 버튼을 활성화합니다. 애플리케이션 또는 필터를 선택하여 Snort 검사를 우회하고 나머지 플로우를 제한할 수 있습니다.

참고
제한된 엘리펀트 플로우에서 시스템이 위협을 받지 않는 경우(즉, Snort 패킷 삭제율이 구성된 임계값보다 작은 경우) 스로틀이 자동으로 제거됩니다. 따라서 속도 제한도 제거됩니다.

다음과 같은 Threat Defense 명령을 사용하여 제한된 엘리펀트 플로우에서 스로틀을 수동으로 제거할 수도 있습니다.

- **clear efd-throttle <5-tuple/all> bypass** — 이 명령은 제한된 엘리펀트 플로우에서 스로틀을 제거하고 Snort 검사를 우회합니다.
- **clear efd-throttle <5-tuple/all>** — 이 명령은 제한된 엘리펀트 플로우에서 스로틀을 제거하고 Snort 검사를 계속합니다. 이 명령을 사용하면 엘리펀트 플로우 교정을 건너뛰게 됩니다.

  이러한 명령에 대한 자세한 내용은 Cisco Secure Firepower Threat Defense 명령 참조에 나와 있습니다.

단계 **6** **Remediation Exemption Rule(**교정 제외 규칙**)** 섹션에서 **Add Rule(**규칙 추가**)**를 클릭하여 교정에서 제외할 플로우에 대한 L4 ACL(액세스 제어 목록) 규칙을 설정합니다.

단계 **7** **Add Rule(**규칙 추가**)** 창에서 **Networks(**네트워크**)** 탭을 사용하여 네트워크 세 부 정보(소스 네트워크와 대상 네트워크)를 추가합니다. **Ports(**포트**)** 탭에서 소스 포트와 목적지 포트를 추가합니다.

엘리펀트 플로우가 탐지되고 정의된 규칙과 일치하는 경우, **Connection Events(**연결 이벤트**)**의 **Reason(**이유**)** 열 헤더에서 **Elephant Flow Exempted(**엘리펀트 플로우 제외**)**라는 이유가 있는 이벤트가 생성됩니다.

단계 **8** **Remediation Exemption Rule(**교정 제외 규칙**)** 섹션에서 교정 작업에서 제외되는 플로우를 볼 수 있습니다.

단계 **9** **OK(**확인**)**를 클릭하여 엘리펀트 플로우 설정을 저장합니다.

단계 **10** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축를 참조하십시오.

엘리펀트 플로우 설정을 구성한 후에는 연결 이벤트를 모니터링하여 플로우가 탐지, 우회 또는 제한되는지 확인합니다. 연결 이벤트의 **Reason** (이유) 필드에서 해당 내용을 확인할 수 있습니다. 엘리펀트 플로우 연결의 세 가지 이유는 다음과 같습니다.

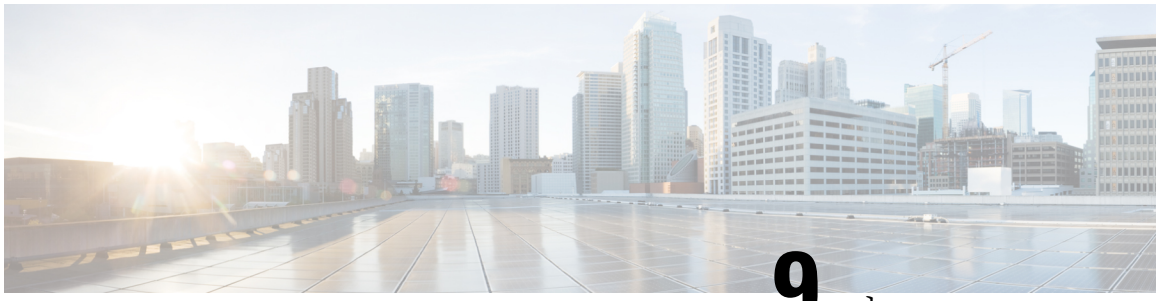
- 엘리펀트 플로우
- 엘리펀트 플로우 제한
- 엘리펀트 플로우 신뢰

주의 엘리펀트 플로우 탐지만 활성화하면 엘리펀트 플로우에 대한 연결 이벤트가 생성되지 않습니다. 다른 이유로 연결 이벤트가 이미 로깅되고 플로우가 엘리펀트 플로우인 경우, **Reason** (이유) 필드에 이 정보가 포함됩니다. 그러나 모든 엘리펀트 플로우를 로깅하려면 해당 액세스 제어 규칙에서 연결 로깅을 활성화해야 합니다.

자세한 내용은 Cisco Secure Firewall 엘리펀트 플로우 탐지 를 참조하십시오.

V 부

Snort 3 활용 사례



9 장

Secure Firewall Management Center에서 Snort 2를 Snort 3로 마이그레이션

Snort 2에서 Snort 3로 마이그레이션

Snort는 버전 2에서 버전 3으로 업그레이드되며 상당한 변경 사항이 적용된 침입 탐지 및 방지 시스템입니다. Snort 3의 향상된 기능을 활용하려면 Snort 2에서 기존 규칙 집합을 마이그레이션하는 것이 중요합니다. 이 마이그레이션 프로세스에는 Snort 2 규칙을 Snort 3 규칙 구문으로 변환 및 조정하며 향상된 탐지 및 성능을 위해 최적화하는 작업이 포함됩니다.

경우에 따라 조직은 Secure Firewall Management Center에서 관리하는 Threat Defense 디바이스를 사용할 수 있습니다. 조직은 Snort 2에서 Snort 3로 마이그레이션하는 동안 하이브리드 구축 접근 방식을 선택할 수 있습니다. 이 접근 방식을 사용하면 점진적 전환이 가능하며 잠재적인 중단(있는 경우)을 최소화할 수 있습니다.

Snort 3로의 마이그레이션 이점

- 향상된 프로토콜 지원 - Snort 3는 향상된 프로토콜 지원을 제공하므로, 암호화된 트래픽을 포함하여 광범위한 최신 프로토콜에 걸쳐 위협을 모니터링하고 탐지할 수 있습니다.
- 간소화된 규칙 관리 - Snort 3는 사용자 친화적 규칙 언어 및 규칙 관리 시스템을 제공하므로, 규칙을 보다 쉽게 생성, 수정 및 관리할 수 있습니다.

- 향상된 성능 - Snort 3는 더 많은 트래픽을 더욱 효율적으로 처리하도록 최적화되어 성능 병목 현상의 위험을 줄이고 적시에 위협 탐지를 보장합니다.

샘플 비즈니스 시나리오

Alice는 네트워크 인프라를 모니터링하고 보호하기 위해 Snort 검사 엔진에 크게 의존하는 대규모 조직에서 보안 분석가로 일하고 있습니다. 이 조직에서는 수년 동안 Snort 버전 2를 사용해 왔지만, 몇 가지 제한 사항과 문제가 발생했습니다.

네트워크 관리자인 Bon은 이러한 문제를 해결하고 조직의 네트워크 보안 기능을 강화하기 위해 Snort 2에서 Snort 3로 마이그레이션하려고 합니다.

또한 이러한 마이그레이션을 수행하면 네트워크 보안 모니터링이 개선되고, 성능이 향상되며, 규칙 관리가 간소화됩니다.

Snort 2에서 Snort 3로 마이그레이션하기 위한 모범 사례

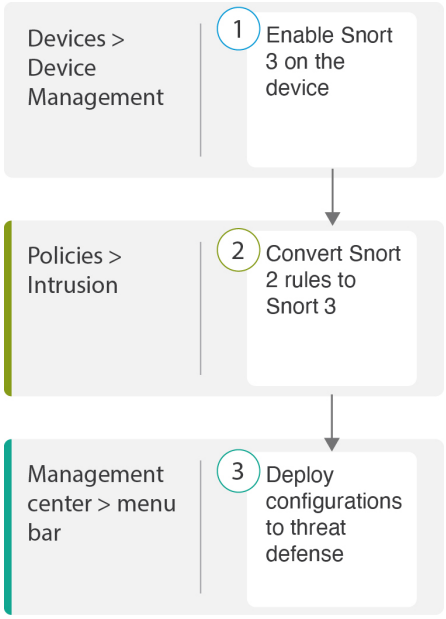
- 마이그레이션을 수행하기 전에 침입 정책을 백업합니다. *Cisco Secure Firewall Management Center 관리 가이드*의 구성 내보내기 작업을 참조하십시오.
- 디바이스를 Snort 3로 업그레이드하기 전에 Snort 2에서 변경한 경우 Snort 2에서 Snort 3로 최신 동기화를 포함하도록 동기화 유틸리티를 사용하여 유사한 커버리지로 시작할 수 있습니다. Snort 2 규칙과 Snort 3 동기화 , 26 페이지의 내용을 참조하십시오.
- Snort 2 맞춤형 규칙은 Snort 3로 자동 변환되지 않으므로 수동으로 마이그레이션해야 합니다. Snort 2 사용자 지정 IPS 규칙을 Snort 3로 변환, 24 페이지의 내용을 참조하십시오.
- 동기화는 임계값 또는 억제가 포함된 Snort 2 규칙을 마이그레이션하지 않습니다. 이러한 규칙은 Snort 3에서 다시 생성해야 합니다.

사전 요구 사항

- Snort에 대한 실제 지식이 있어야 합니다. Snort 3 아키텍처에 대한 자세한 내용은 Snort 3 도입을 참조하십시오.
- Management Center를 백업합니다. Management Center 백업을 참조하십시오.
- 침입 정책을 백업합니다. 구성 내보내기를 참조하십시오.

엔드 투 엔드 마이그레이션 워크플로우

다음 순서도에는 Secure Firewall Management Center에서 Snort 2를 Snort 3로 마이그레이션하기 위한 워크플로우가 나와 있습니다.



단계	설명
1	디바이스에서 Snort 3를 활성화합니다. Threat Defense에서 Snort 3 활성화, 129 페이지의 내용을 참조하십시오.
2	Snort 2 규칙을 Snort 3로 변환합니다. 단일 침입 정책의 Snort 2 규칙을 Snort 3로 변환, 130 페이지의 내용을 참조하십시오.
3	구성을 구축합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

Threat Defense에서 Snort 3 활성화

주의 구축 프로세스 중에는 현재 검사 엔진을 종료해야 하므로 일시적인 트래픽 손실이 발생할 수 있습니다.

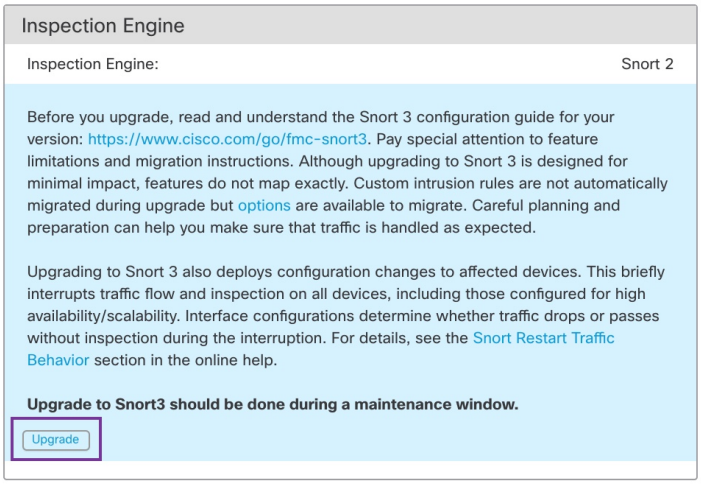
프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 해당 디바이스를 클릭하여 디바이스 홈페이지로 이동합니다.

단계 **3** **Device(**디바이스**)** 탭을 클릭합니다.

단계 **4** **Inspection Engine(**검사 엔진**)** 섹션에서 **Upgrade(**업그레이드**)**를 클릭합니다.



단계 **5** **Yes(**예**)**를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

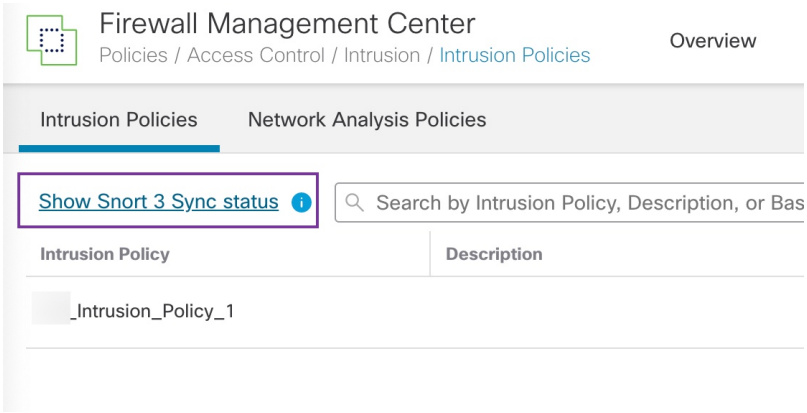
시스템은 구축 프로세스 중에 선택한 Snort 버전과 호환되도록 정책 설정을 변환합니다.

단일 침입 정책의 Snort 2 규칙을 Snort 3로 변환

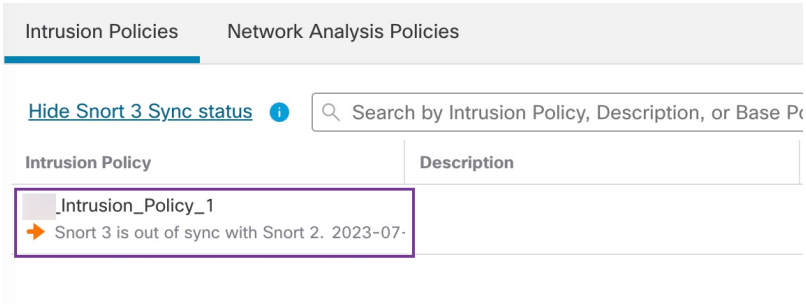
프로시저

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

단계 **2** **Intrusion Policies(**침입 정책**)** 탭에서 **Show Snort 3 Sync status(Snort 3** 동기화 상태 표시**)**를 클릭합니다.

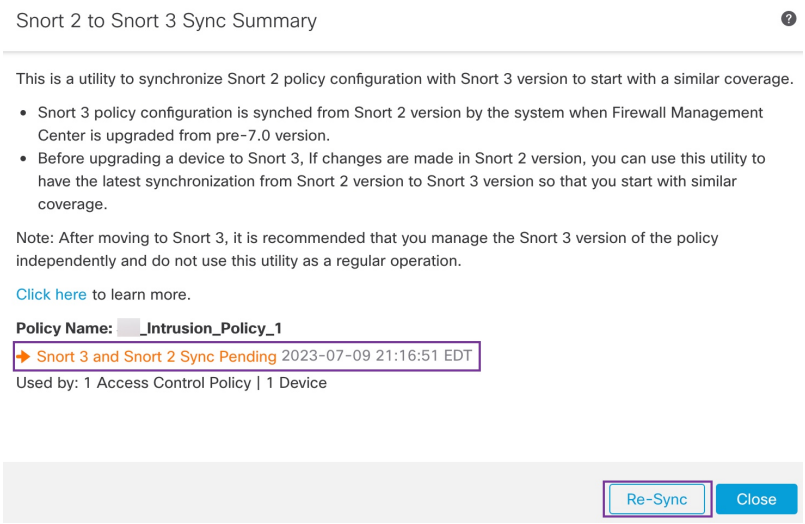


정책에 주황색 화살표가 표시되면 Snort 2 및 Snort 3 버전의 침입 정책이 동기화되지 않았음을 나타냅니다.



단계 **3** 주황색 화살표를 클릭합니다.

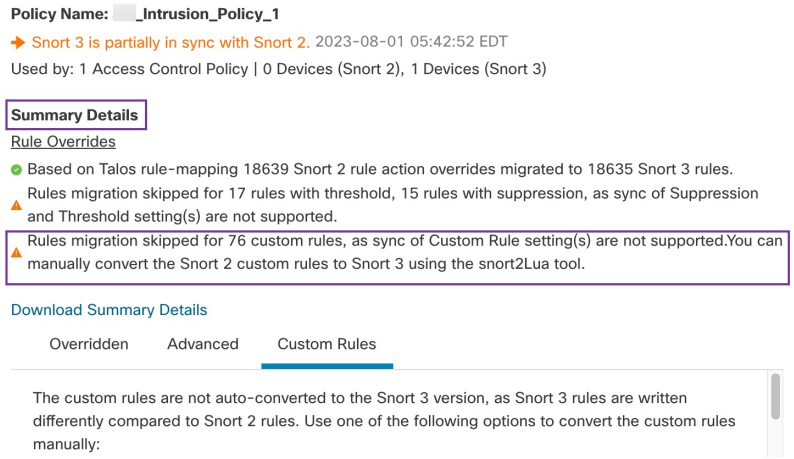
Snort 2 to Snort 3 Sync Summary(Snort 2에서 **Snort 3**로의 동기화 요약**)** 페이지에 Snort 2에서 Snort 3로의 동기화가 보류 중이라는 메시지가 표시됩니다.



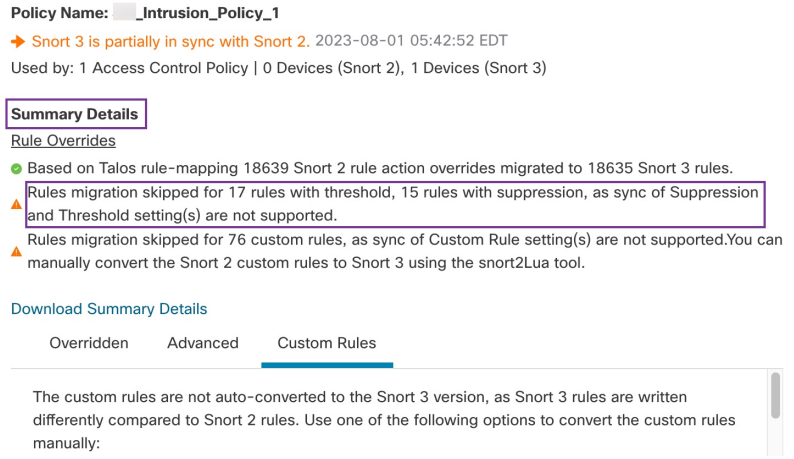
단계 **4** **Re-Sync(**재동기화**)**를 클릭하여 동기화를 시작합니다.

참고
Re-Sync(재동기화**)**를 클릭하면 snort2Lua 툴이 규칙을 Snort 2에서 Snort 3로 변환합니다.

Summary Details(요약 세부 정보**)** 섹션에는 마이그레이션되었거나 건너뛴 규칙이 나열됩니다. 이 활용 사례에는 동기화 프로세스 중에 건너뛴 사용자 지정 Snort 2 규칙 76개, 임계값이 있는 규칙 17개, 억제가 포함된 규칙 15개가 있습니다. 사용자 지정 규칙을 마이그레이션하려면 다음 단계로 이동합니다.

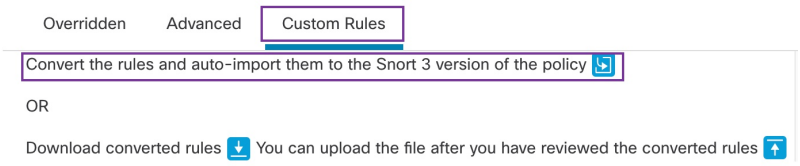


임계값 및 억제가 포함된 규칙을 마이그레이션하려면 단계 6으로 이동합니다.



단계 **5** 76개의 사용자 지정 규칙을 마이그레이션하려면 다음 단계 중 하나를 수행합니다.

- **Custom Rules(**사용자 지정 규칙**)** 탭에서 **Import(**가져오기**)** 아이콘을 클릭하여 로컬 규칙을 Snort 3 버전 정책으로 변환하고 자동으로 가져옵니다.

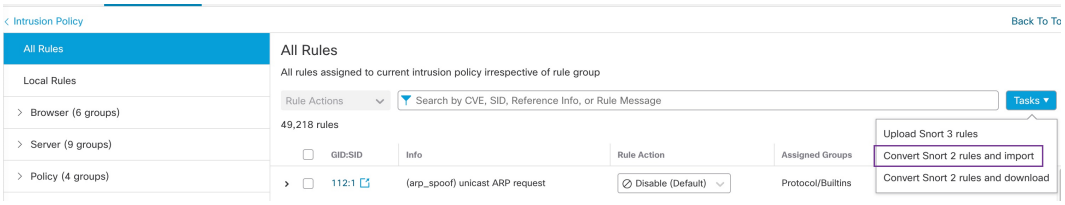


  규칙을 성공적으로 가져오고 나면 확인 메시지가 표시됩니다.

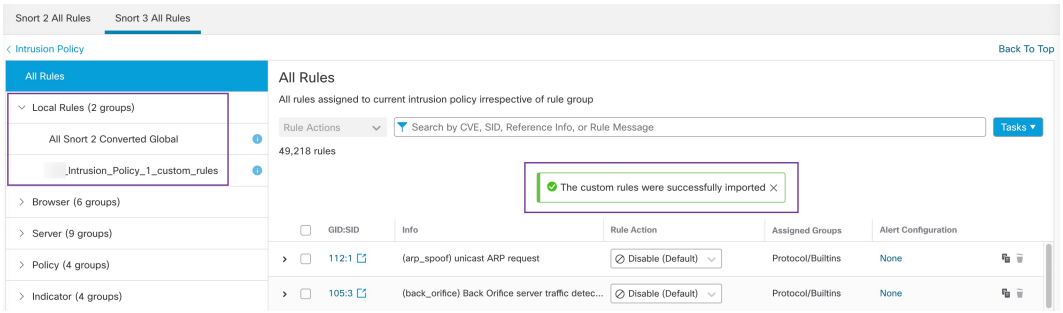
- **Objects(**개체**) > Intrusion Rules(**침입 규칙**)**를 선택하고 **Snort 3 All Rules(**모든 **Snort 3** 규칙**)**를 클릭합니다.

  1. 왼쪽 패널에서 **Local Rules(**로컬 규칙**)**를 클릭하여 규칙이 마이그레이션되었는지 확인합니다. Snort 2의 사용자 지정 규칙은 마이그레이션되지 않았습니다.

2. **Tasks(**작업**)** 드롭다운 목록에서 **Convert Snort 2 rules and import(Snort 2** 규칙 변환 및 가져오기**)**를 선택합니다.

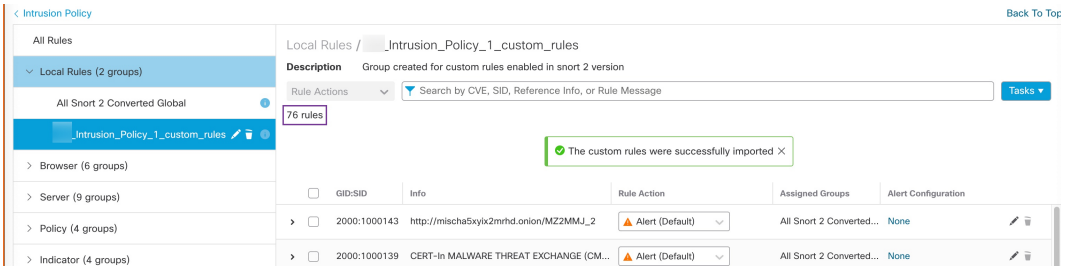


3. **OK(**확인**)**를 클릭합니다.



새로 생성된 규칙 그룹**(All Snort 2 Converted Global(**모든 **Snort 2** 변환 전역**))**이 왼쪽 패널의 **Local Rules(**로컬 규칙**)**에 생성됩니다.

다음 그림에 나와 있는 것처럼 76개의 사용자 지정 규칙이 모두 마이그레이션되었습니다.



아니면 이전 단계에서 **Convert Snort 2 rules and download(Snort 2** 규칙 변환 및 다운로드**)**를 선택하여 규칙 파일을 로컬에 저장할 수 있습니다. 다운로드한 파일에서 변환된 규칙을 검토한 후 나중에 **Upload Snort 3 Rules(Snort 3** 규칙 업로드**)** 옵션을 사용하여 업로드할 수 있습니다.

단계 **6** .txt 형식의 규칙을 다운로드하려면 **Download Summary Details(**요약 세부 정보 다운로드**)** 링크를 클릭합니다.

다음은 표시되는 요약의 샘플입니다.

```
"id": "00505691-15DC-0ed3-0000-004294988561",
"name": "_Intrusion_Policy_1",
"type": "IntrusionPolicy",
"syncStatus": {
  "source": {
    "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
    "type": "IntrusionPolicy"
  },
```

```
    "status": "WARN",
    "description": "Migration is partially successful. Some of the rules are not copied to
 Snort3.",
    "timestamp": 1690883954814,
    "lastUser": {
      "name": "admin"
    },
    "details": [
      {
        "type": "Summary",
        "status": "INFO",
        "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides
migrated to 18635 Snort 3 rules."
      },
      {
        "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,

1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,

1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,

1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,

1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,

1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,

1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,

1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

         1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
        "type": "PolicyInfo",
        "description": "Corresponding Snort 2 policy overridden custom (local) rules."
      },
      {
        "type": "AssignedDevices",
        "status": "INFO",
        "description": "Snort3:0 , Snort2:0"
      },
      {
        "id": "122:6",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
      },
      {
        "id": "122:15",
        "type": "Threshold",
        "status": "ERROR",
```

```
    "description": "PSNG_IP_PORTSWEEP_FILTERED"
  },
 {
    "id": "122:1",
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_TCP_PORTSCAN"
 },
```

단계 **7** **Close(**닫기**)**를 클릭하여 **Sync Summary(**동기화 요약**)** 대화 상자를 닫습니다.

단계 **8** : ERROR 상태의 규칙을 확인하려면 **Policies(**정책**) > Intrusion(**침입**)**을 선택하고 **Snort 2** 버전 침입 정책을 클릭합니다.

단계 **9** **Policy Information(**정책 정보**)**에서 **Rules(**규칙**)**를 클릭하고 규칙을 기준으로 필터링합니다. 예를 들어, 규칙을 찾으려면 **Filter(**필터**)** 필드에 **PSNG_TCP_PORTSCAN**을 입력합니다.

단계 **10** **Show Details(**세부 정보 표시**)**를 클릭하여 규칙의 상세 버전을 확인합니다.

단계 **11** Snort 3 규칙 지침을 사용하여 Snort 3에서 다시 규칙을 생성하고 파일을 .txt 또는 .rules 파일로 저장합니다. 자세한 내용은 www.snort3.org를 참조하십시오.

단계 **12** 방금 로컬로 만든 사용자 지정 규칙을 모든 Snort 3 규칙 목록에 업로드합니다. 규칙 그룹에 사용자 지정 규칙 추가를 참조하십시오.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

구성 변경 사항 구축

컨피그레이션을 변경한 후 해당하는 디바이스에 구축합니다.

참고 이 주제에서는 구성 변경 사항 구축과 관련된 기본 단계를 다룹니다. 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에서 구성 변경 사항 구축 주제를 참조하여 단계를 진행하기 전에 변경 사항 구축의 사전 요건과 영향을 파악할 것을 강력하게 권장합니다.

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다.

프로시저

단계 **1** Secure Firewall Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭하고 **Deployment(**구축**)**를 선택합니다.

GUI 페이지에는 **Pending(**보류 중**)** 상태인 오래된 구성이 있는 디바이스가 나열됩니다.

- **Modified By(**수정 주체**)** 열에는 정책 또는 개체를 수정한 사용자가 나열됩니다. 디바이스 목록을 확장하여 각 정책 목록에 대한 정책을 수정한 사용자를 볼 수 있습니다.

  참고
  삭제된 정책 및 개체에 대해서는 사용자 이름이 제공되지 않습니다.

- **Inspect Interruption(**검사 중단**)** 열은 구축 중에 디바이스에서 트래픽 검사 중단이 발생할 수 있는지 여부를 나타냅니다.

  디바이스에 대한 이 열이 비어 있으면 구축 중에 해당 디바이스에서 트래픽 검사가 중단되지 않음을 나타냅니다.

- **Last Modified Time(**마지막 수정 시간**)** 열은 구성 변경을 마지막으로 수행한 시간을 지정합니다.
- **Preview(**미리보기**)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다.
- **Status(**상태**)** 열은 각 구축의 상태를 제공합니다.

단계 **2** 컨피그레이션 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스 별 구성 변경 사항을 보려면 확장 화살표( )을 클릭합니다.

  디바이스 옆의 확인란을 선택하면 디바이스에 대해 수행되고 디바이스 아래에 나열된 모든 변경 사항이 푸시되어 구축됩니다. 그러나 정책 선택( )를 사용하면 구축하지 않고 나머지 변경 사항을 보류하면서 구축할 개별 정책 또는 특정 구성을 선택할 수 있습니다.

  참고
  - **Inspect Interruption(**검사 중단**)** 열의 상태가 (**Yes(**예**)**)인 경우(구축하면 Threat Defense 디바이스에서 검사가 중단되며 트래픽도 중단될 수 있음) 확장된 목록에서 검사 중단( ) 중단을 야기하는 특정 구성을 표시합니다.
  - 인터페이스 그룹, 보안 영역 또는 개체가 변경되면 영향을 받는 디바이스는 Management Center에서 오래된 것으로 표시됩니다. 이러한 변경 사항을 적용하려면 이러한 인터페이스 그룹, 보안 영역 또는 개체가 포함된 정책도 이러한 변경 사항과 함께 구축해야 합니다. 영향을 받는 정책은 Management Center의 **Preview(**미리보기**)** 페이지에서 만료된 것으로 표시됩니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

단계 4 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- Deploy(구축) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

다음에 수행할 작업

구축 중에 구축 장애가 발생하는 경우 해당 장애가 트래픽에 영향을 미칠 수 있습니다. 그러나 특정 조건에 따라 달라집니다. 구축에 특정 구성이 변경된 경우 구축 장애로 인해 트래픽이 중단될 수 있습니다. 자세한 내용은 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 구성 변경 사항 구축 주제를 참조하십시오.

10 장

Secure Firewall Management Center에서 Snort 3 권장 사항 생성

Snort 3 규칙 권장 사항

규칙 권장 사항은 호스트 환경과 관련된 규칙을 사용하여 침입 정책을 자동으로 조정합니다. 네트워크에 없는 취약성에 대한 규칙을 비활성화하여 추가 규칙을 활성화하거나 현재 규칙 집합을 조정할 수 있습니다. 자세한 내용은 Secure Firewall 권장 규칙 개요, 66 페이지를 참고하십시오.

어떻게 프로그램을 사용할 수 있습니까?

Management Center는 IP 주소, 호스트 이름, 운영 체제, 서비스, 사용자, 클라이언트 애플리케이션과 같은 세부 정보를 사용하여 네트워크의 호스트 데이터베이스를 수동 검색을 통해 구축합니다. 시스템은 이 정보를 기반으로 검색된 각 호스트에 취약성을 매핑합니다. 권장 사항 기능은 이 호스트 데이터베이스를 사용하여 환경에 적용할 규칙을 결정합니다.

Snort 3에는 네 가지 보안 레벨이 있으며, 각 보안 레벨은 특정 Talos 정책에 해당합니다. 다음과 같습니다.

- 레벨 1 - Connectivity over Security(연결이 보안에 우선함)
- 레벨 2 - Balanced Security and Connectivity(균형 잡힌 보안 및 연결성)
- 레벨 3 - Security over Connectivity(보안이 연결에 우선함)
- 레벨 4 - Maximum Detection(최대 탐지)

Accept Recommendations to Disable Rules(규칙 비활성화를 위한 권장 사항 수락**)** 체크 박스를 선택하여 네트워크의 호스트에 없는 취약성에 대한 규칙을 비활성화합니다. 많은 알림 수로 인해 규칙 집합을 잘라내야 하거나 검사 성능을 개선하려는 경우에만 이 옵션을 선택하십시오.

이점

- 권장 사항을 구성하면 호스트 환경과 관련된 규칙을 사용하여 특정 위협 유형을 더욱 효과적으로 탐지하도록 침입 정책을 맞춤화할 수 있습니다.
- 권장 사항은 오탐 및 미탐을 줄여 인시던트 대응 프로세스의 효율성과 효과를 높입니다.

샘플 비즈니스 시나리오

대규모 기업 네트워크에서는 Snort 3를 기본 침입 탐지 및 방지 시스템으로 사용합니다. 빠르게 진화하는 위협 환경에서는 강력한 네트워크 보안 조치를 채택해야 합니다. 이 보안 팀은 사고 대응 기능을 개선하고자 합니다. 이를 수행하는 방법 중 하나는 호스트 네트워크에서 탐지된 취약성을 기반으로 권장 사항 또는 규칙 집합을 생성하는 것입니다. 이를 통해 침입 정책을 최적화하여 네트워크를 보다 효과적으로 보호할 수 있습니다.

모범 사례

- 정확한 품질의 호스트 데이터가 있어야 합니다.

  네트워크 검색의 수동 특성으로 인해 Threat Defense 디바이스는 보호되는 호스트와 최대한 가깝게 배치해야 합니다. 그러면 Threat Defense 디바이스가 이러한 호스트를 오가는 네트워크 트래픽을 감시할 수 있으며, 따라서 네트워크에 있는 애플리케이션, 서비스, 취약점에 대한 정확한 데이터를 얻을 수 있습니다.
- 디바이스는 이스트-웨스트 및 노스-사우스 트래픽 플로우에 대한 가시성이 있어야 정확한 호스트 프로파일을 구축할 수 있습니다.
- 권장 사항을 자동으로 업데이트하도록 예약된 작업을 생성할 수 있습니다.

사전 요구 사항

- 권장 사항을 생성하려면 시스템에 호스트가 있는지 확인합니다.
- 권장 사항에 대해 구성된 보호받는 네트워크는 시스템에 있는 호스트에 매핑되어야 합니다.

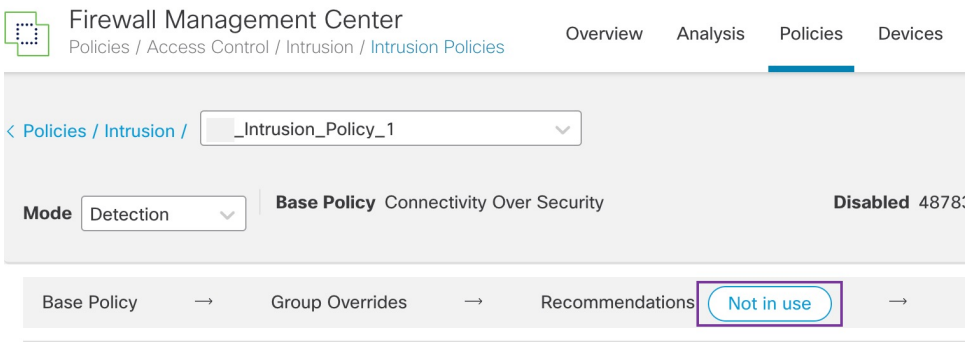
Snort 3 권장 사항 생성

프로시저

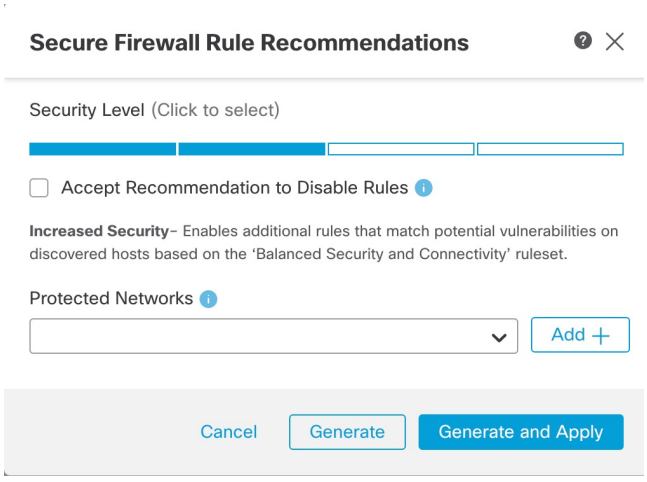
단계 1 **Policies(정책) > Intrusion(침입)**을 선택합니다.

단계 2 해당하는 침입 정책의 **Snort 3 Version(Snort 3 버전)** 버튼을 클릭합니다.

단계 3 **Recommendations (Not in Use)(권장 사항(사용되지 않음))** 레이어를 클릭하여 규칙 권장 사항을 구성합니다.



Cisco Recommended Rules(Cisco 권장 규칙) 창에서 보안 레벨을 설정할 수 있습니다.



단계 4 클릭하여 보안 레벨을 선택합니다.

단계 5 (선택 사항) 네트워크의 호스트에 없는 취약성에 대해 작성된 규칙을 비활성화하려면 **Accept Recommendation to Disable Rules(규칙 비활성화를 위한 권장 사항 수락)** 체크 박스를 선택합니다.

많은 알림 수로 인해 규칙 집합을 잘라내야 하거나 검사 성능을 개선하려는 경우에만 이 옵션을 사용하십시오.

단계 **6** **Protected Networks(**보호되는 네트워크**)** 드롭다운 목록에서 권장 사항에서 검사해야 하는 네트워크 개체를 선택합니다. 따로 선택하지 않은 경우 기본적으로 IPv4 또는 IPv6 네트워크가 선택됩니다.

Add +(추가 **+)**를 클릭하여 **Host(**호스트**)** 또는 **Network(**네트워크**)** 유형의 새 네트워크 개체를 생성하고 **Save(**저장**)**를 클릭합니다.

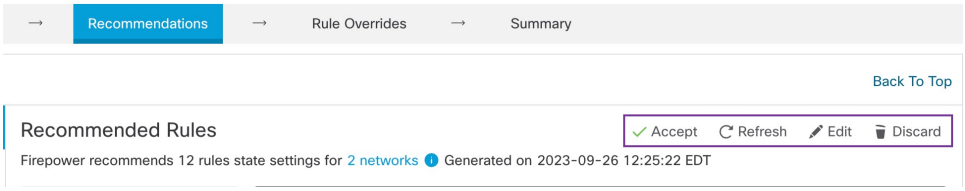
단계 **7** 권장 사항을 생성하고 적용합니다.

- **Generate(**생성**)** - 침입 정책에 대한 권장 사항을 생성합니다. 이 작업은 **Recommended Rules (Not in use)(**권장 규칙**(**사용되지 않음**))** 아래에 규칙을 나열합니다.
- **Generate and Apply(**생성 및 적용**)** - 침입 정책에 대한 권장 사항을 생성하고 적용합니다. 이 작업은 **Recommended Rules (Not in use)(**권장 규칙**(**사용되지 않음**))** 아래에 규칙을 나열합니다.

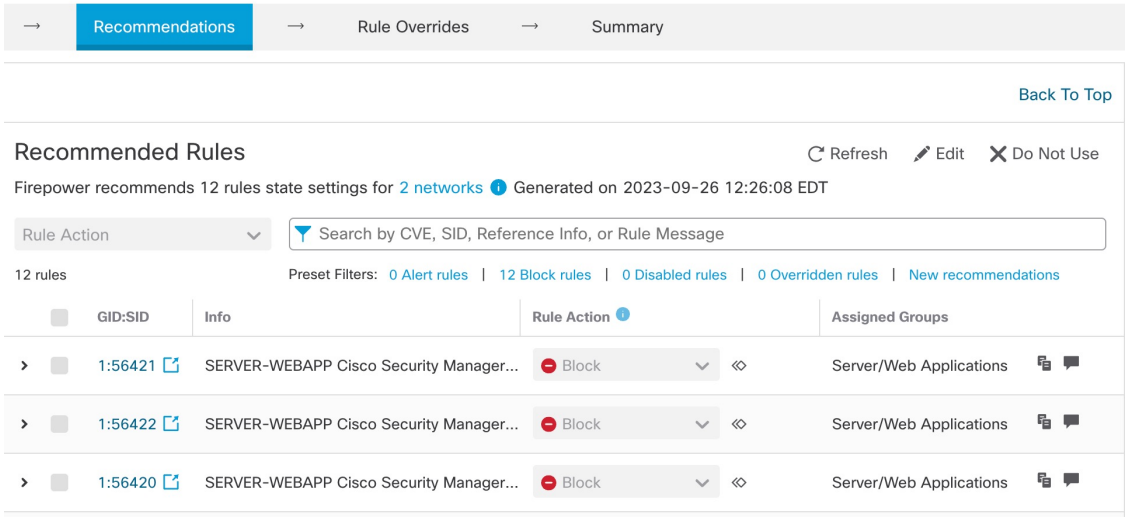
권장 사항이 생성되었습니다. 모든 권장 규칙 및 해당 권장 작업이 포함된 새 권장 사항 탭이 나타납니다. 이 탭에서 새로운 권장 사항 외에도 규칙 작업 프리셋 필터를 사용할 수 있습니다.

단계 **8** 권장 사항을 확인한 다음 적절하게 적용합니다.

- **Accept(**수락**)** - 침입 정책에 대해 이전에 생성된 권장 사항을 적용합니다.
- **Refresh(**새로 고침**)** - 침입 정책에 대한 규칙 권장 사항을 다시 생성하고 업데이트합니다.
- **Edit(**편집**)** - 권장 사항 입력 값을 제공한 다음 권장 사항을 생성할 수 있는 **Recommendations(**권장 사항**)** 대화 상자를 엽니다.
- **Discard(**폐기**)** - 적용된 권장 규칙을 되돌리거나 정책에서 제거합니다. **Recommendations(**권장 사항**)** 탭도 제거합니다.

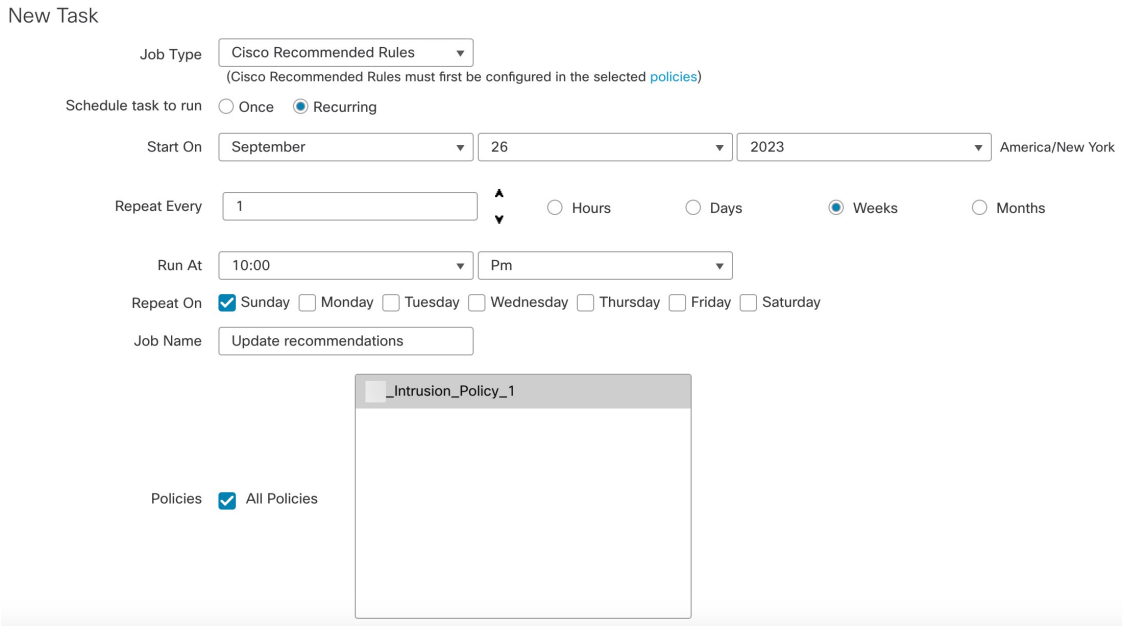


All Rules(모든 규칙**)** 아래의 Recommended Rules(권장 규칙) 섹션에 권장 규칙이 나와 있습니다.



단계 **9** 권장 사항을 효과적으로 사용하려면 주기적으로 업데이트해야 합니다. 다음 단계를 수행합니다.

1. **System(**시스템**) >Tools(**툴**) > Scheduling(**예약**)**을 선택합니다.
2. **Add Task(**작업 추가**)**를 클릭합니다.
3. **Job Type(**작업 유형**)** 드롭다운 목록에서 **Cisco Recommended Rules(Cisco** 권장 규칙**)**를 선택합니다.
4. 필요에 따라 필수 필드를 업데이트합니다.



5. **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

구성 변경 사항 구축

컨피그레이션을 변경한 후 해당하는 디바이스에 구축합니다.

참고 이 주제에서는 구성 변경 사항 구축과 관련된 기본 단계를 다룹니다. 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에서 구성 변경 사항 구축 주제를 참조하여 단계를 진행하기 전에 변경 사항 구축의 사전 요건과 영향을 파악할 것을 강력하게 권장합니다.

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다.

프로시저

단계 **1** Secure Firewall Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭하고 **Deployment(**구축**)**를 선택합니다.

GUI 페이지에는 **Pending(**보류 중**)** 상태인 오래된 구성이 있는 디바이스가 나열됩니다.

- **Modified By(**수정 주체**)** 열에는 정책 또는 개체를 수정한 사용자가 나열됩니다. 디바이스 목록을 확장하여 각 정책 목록에 대한 정책을 수정한 사용자를 볼 수 있습니다.

  참고
  삭제된 정책 및 개체에 대해서는 사용자 이름이 제공되지 않습니다.

- **Inspect Interruption(**검사 중단**)** 열은 구축 중에 디바이스에서 트래픽 검사 중단이 발생할 수 있는지 여부를 나타냅니다.

  디바이스에 대한 이 열이 비어 있으면 구축 중에 해당 디바이스에서 트래픽 검사가 중단되지 않음을 나타냅니다.

- **Last Modified Time(**마지막 수정 시간**)** 열은 구성 변경을 마지막으로 수행한 시간을 지정합니다.
- **Preview(**미리보기**)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다.
- **Status(**상태**)** 열은 각 구축의 상태를 제공합니다.

단계 **2** 컨피그레이션 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스 별 구성 변경 사항을 보려면 확장 화살표( )을 클릭합니다.

  디바이스 옆의 확인란을 선택하면 디바이스에 대해 수행되고 디바이스 아래에 나열된 모든 변경 사항이 푸시되어 구축됩니다. 그러나 정책 선택( )를 사용하면 구축하지 않고 나머지 변경 사항을 보류하면서 구축할 개별 정책 또는 특정 구성을 선택할 수 있습니다.

  참고

  - **Inspect Interruption(**검사 중단**)** 열의 상태가 (**Yes(**예**)**)인 경우(구축하면 Threat Defense 디바이스에서 검사가 중단되며 트래픽도 중단될 수 있음) 확장된 목록에서 검사 중단( ) 중단을 야기하는 특정 구성을 표시합니다.
  - 인터페이스 그룹, 보안 영역 또는 개체가 변경되면 영향을 받는 디바이스는 Management Center에서 오래된 것으로 표시됩니다. 이러한 변경 사항을 적용하려면 이러한 인터페이스 그룹, 보안 영역 또는 개체가 포함된 정책도 이러한 변경 사항과 함께 구축해야 합니다. 영향을 받는 정책은 Management Center의 **Preview(**미리보기**)** 페이지에서 만료된 것으로 표시됩니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- Deploy(구축) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

다음에 수행할 작업

구축 중에 구축 장애가 발생하는 경우 해당 장애가 트래픽에 영향을 미칠 수 있습니다. 그러나 특정 조건에 따라 달라집니다. 구축에 특정 구성이 변경된 경우 구축 장애로 인해 트래픽이 중단될 수 있습니다. 자세한 내용은 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 구성 변경 사항 구축 주제를 참조하십시오.

11 장

EVE 위협 신뢰도 점수를 기반으로 트래픽 차단

암호화된 가시성 엔진 정보

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

이점

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

샘플 비즈니스 시나리오

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

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

사전 요구 사항

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

고수준 워크플로우

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

EVE에서 차단 임계값 구성

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

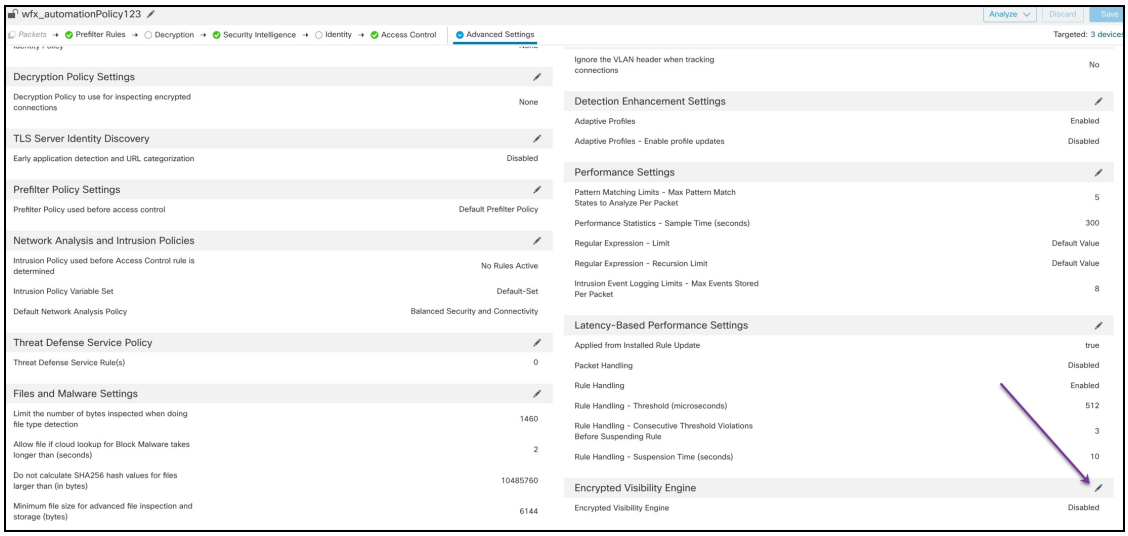
프로시저

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

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

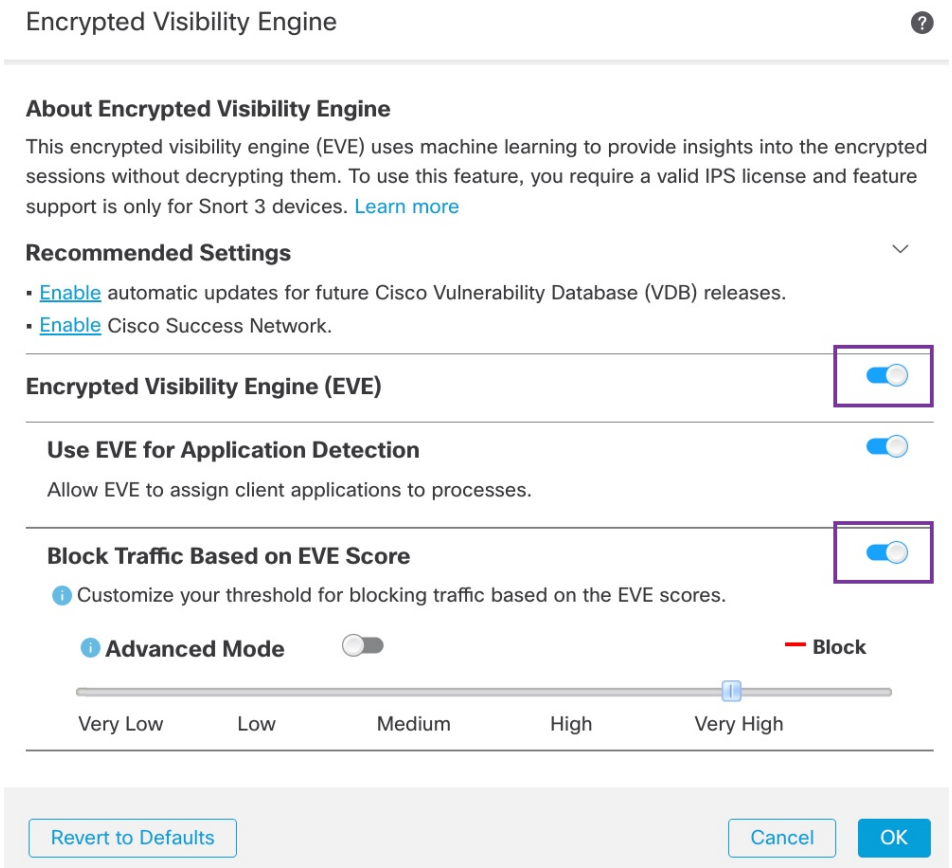
단계 **3** 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

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



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

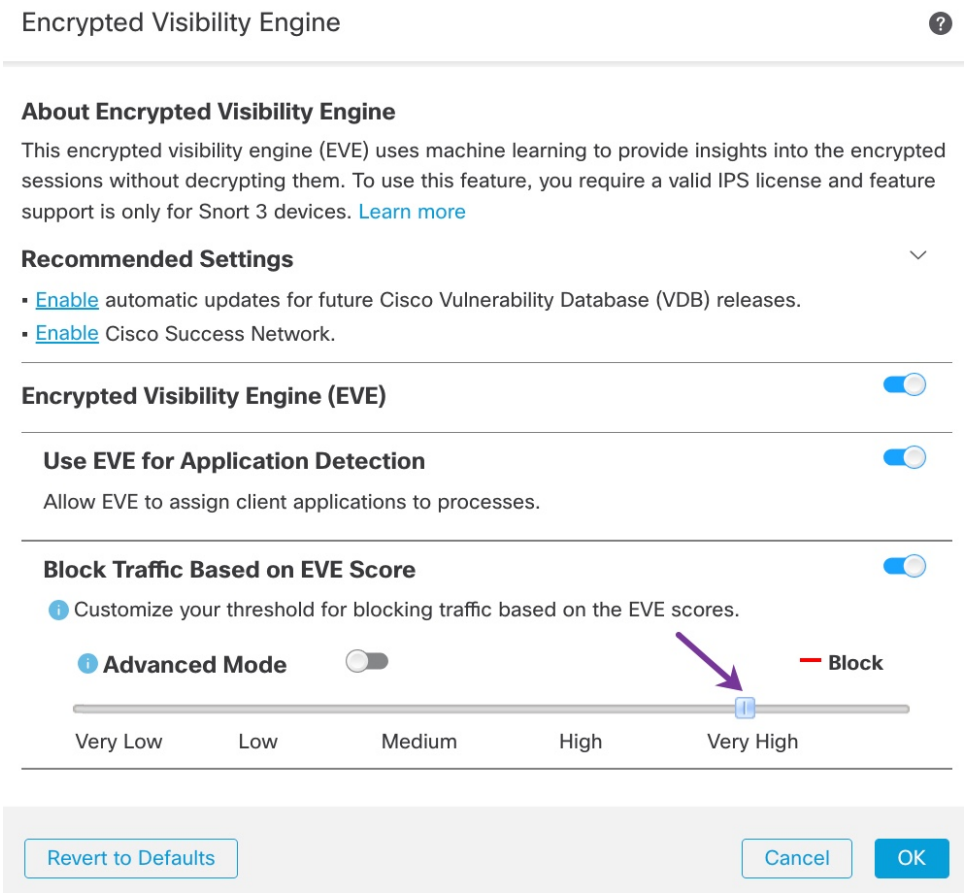
단계 **6** **Block Traffic Based on EVE Score(EVE** 점수 기반 트래픽 차단**)** 토글 버튼을 활성화합니다. 잠재적인 위협인 모든 수신 트래픽은 기본적으로 차단됩니다.



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

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

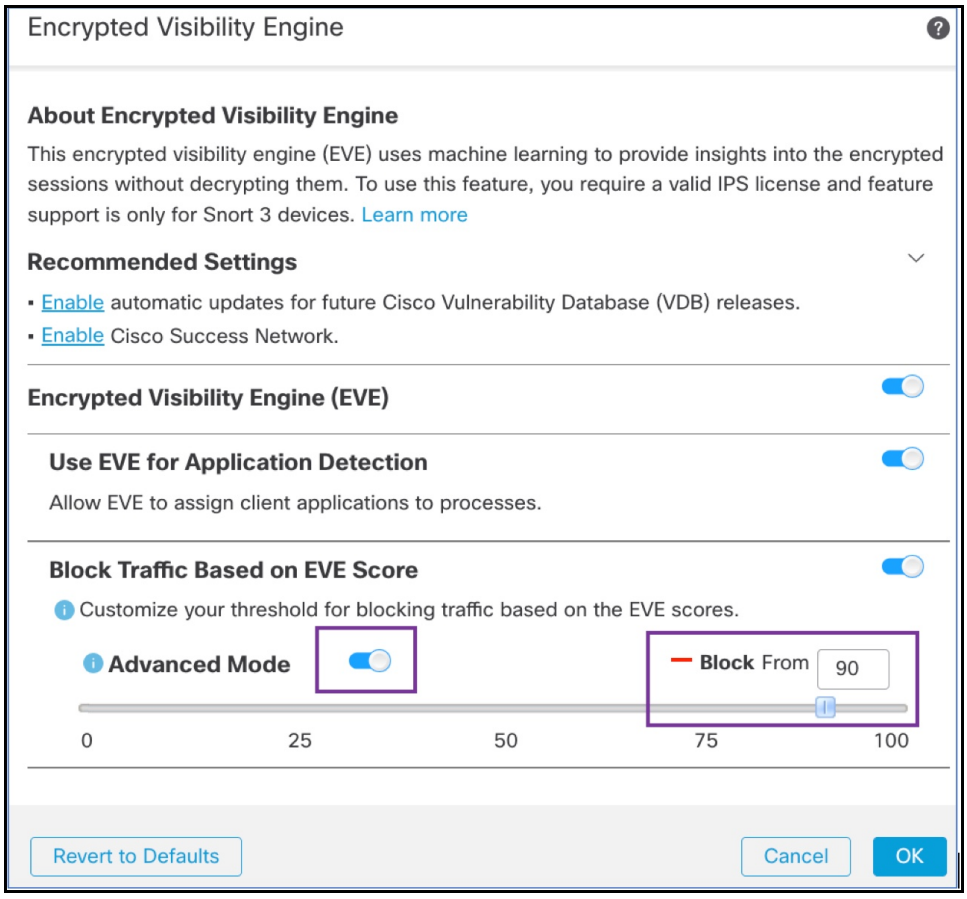
단계 **7** 슬라이더를 사용하여 EVE 위협 신뢰도를 기반으로 차단 임계값을 조정합니다. 범위는 **Very Low(**매우 낮음**)**에서 **Very High(**매우 높음**)**까지입니다. 이 예에서는 슬라이더가 **Very High(**매우 높음**)**로 설정되어 있습니다.



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

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

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



단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

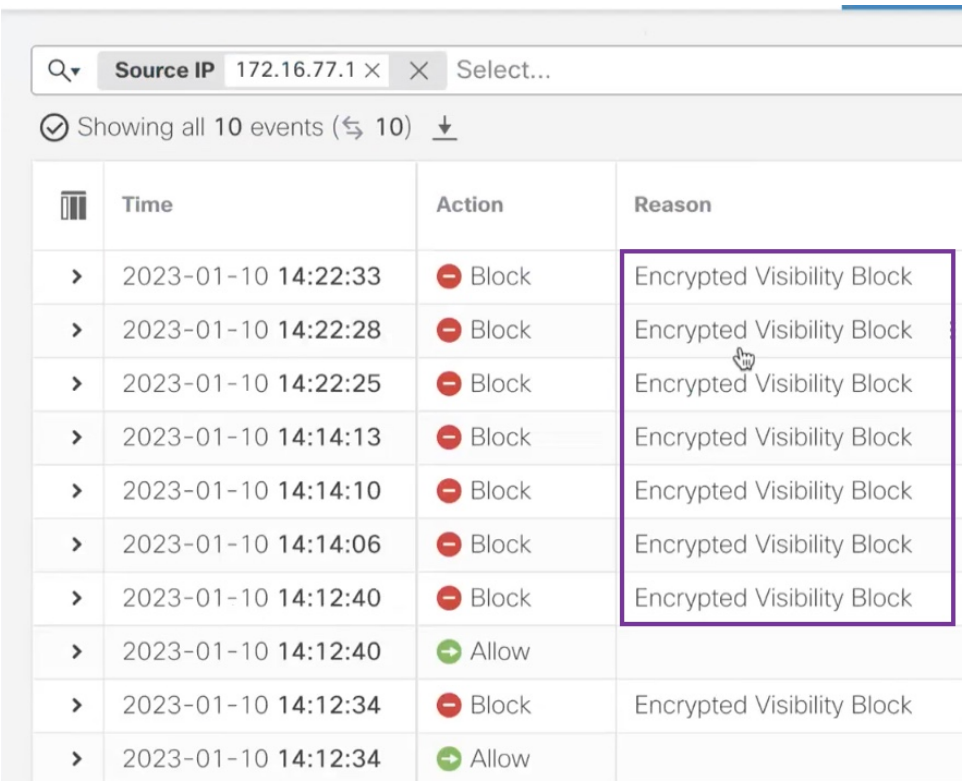
구성 변경 사항을 구축합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

EVE 이벤트 보기

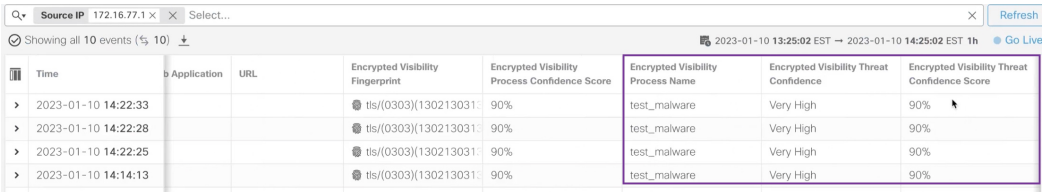
프로시저

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

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



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



추가 참조 자료

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

암호화된 가시성 엔진

12 장

엘리펀트 플로우 탐지 결과 구성

엘리펀트 플로우 정보

엘리펀트 플로우는 매우 크며(총 바이트), 네트워크 링크를 통해 측정되는 TCP(또는 기타 프로토콜) 플로우에 의해 설정된 네트워크 연결이 상대적으로 오래 실행됩니다. 기본적으로 엘리펀트 플로우는 10초당 1GB보다 큰 플로우 또는 연결입니다. 이로 인해 Snort 코어에서 성능 저하 또는 문제가 발생할 수 있습니다. 엘리펀트 플로우는 잠재적으로 CPU 리소스를 과도하게 사용할 수 있으며 탐지 리소스를 놓고 경쟁하는 다른 플로우에 영향을 미칠 수 있고, 레이턴시 증가나 패킷 삭제 등의 문제를 일으킬 수 있어 중요합니다.

엘리펀트 플로우 탐지 및 교정의 이점

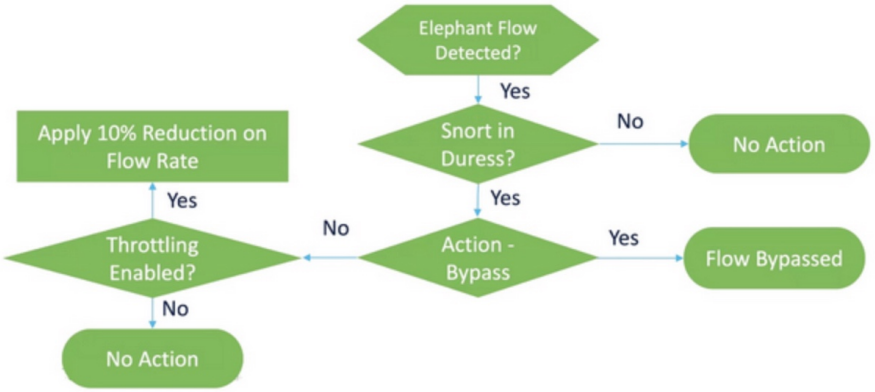
- 엘리펀트 플로우 구성을 사용하면 엘리펀트 플로우를 우회하거나 제한하는 옵션이 지원되며 사용자 지정이 가능합니다.
- 선택한 애플리케이션을 기반으로 플로우를 우회하거나 제한하도록 선택하여 의심스러운 트래픽에 대해 Snort 검사를 제공하면서 신뢰할 수 있는 트래픽을 더 많이 우회할 수 있습니다.
- 엘리펀트 플로우 교정은 특정 요건에 따라 우선순위를 지정하고 내부 애플리케이션에 더 많은 대역폭을 확보하는 데 도움이 됩니다.

엘리펀트 플로우 워크플로우

구성된 매개변수를 기준으로 엘리펀트 플로우가 탐지되면 플로우를 우회하거나 제한하도록 선택할 수 있습니다. 플로우를 우회하는 경우 해당 트래픽은 Snort 검사 없이 통과할 수 있습니다. 제한은 플로우 처리량이 감소되었음을 나타냅니다. 플로우 속도 감소는 CPU 사용률이 구성된 임계값 아래로 감소할 때까지 10% 증분으로 이루어집니다. 엘리펀트 플로우를 식별하고 추가 CPU 및 시간 창 매개변수를 충족한 후에 우회 또는 제한이 발생합니다. 엘리펀트 플로우를 식별하기 전에 침입 정책은 허용 규칙에서 구성했다고 가정하고 플로우를 처리합니다. 이는 대부분의 공격이 연결에서 매우 초기에 감지되기 때문에 엘리펀트 플로우가 완전히 검사되지 않은 상태로 시스템을 통과할 수 없다는 것을 의미합니다.

플로우가 처리되는 방식을 알아보려면 다음 다이어그램을 참조하십시오.

그림 *3:* 엘리펀트 플로우 워크플로우



시스템이 Snort 위협 조건(성능 문제)을 탐지하지 않는 한, 어떤 작업도 수행되지 않습니다. 플로우가 크다고 해서 플로우를 제한하거나 우회하지 않습니다. 또한 제한과 우회 작업은 함께 사용할 수 없습니다. 즉, 플로우를 우회하거나 제한할 수 있지만 둘 다 수행할 수는 없습니다.

위협을 유발하는 엘리펀트 플로우를 모두 우회하지 않으려면 특정 애플리케이션에 대해서만 우회 옵션을 제한할 수 있습니다. 성능을 제한하지 않고 신뢰하는 애플리케이션에 대한 연결의 우선순위를 정할 수 있습니다. 우회해야 하는 애플리케이션을 구성할 수 있지만, 위협을 유발하는 나머지 플로우는 제한됩니다. 이렇게 하면 대역폭은 감소하지만, 다른 신뢰할 수 없는 애플리케이션 플로우는 전체 Snort 검사를 계속 수신하게 됩니다.

샘플 비즈니스 시나리오

데이터 센터에서는 클러스터 간 데이터 복제, 가상 머신 통합, 데이터베이스 백업과 같은 여러 활동이 이루어지고 있습니다. 조직의 사용자는 OTT에서 비디오를 시청하거나 다운로드할 수 있습니다. 이러한 활동의 대역폭 사용률은 엘리펀트 플로우를 야기하고 네트워크 속도를 저하하며 중요한 작업의 성능에 영향을 줄 수 있습니다. 네트워크 관리자는 특정 요구 사항에 따라 대역폭 문제를 유발하고 해결하는 대규모 플로우에 대한 정보를 알고 싶어 합니다.

예를 들어, WebEx 트래픽(조직에서 실시간 영상 회의에 사용)에 대한 Snort 검사를 우회하도록 엘리펀트 플로우 매개변수를 구성하고 비디오, 영화 등을 포함한 나머지 애플리케이션 또는 연결을 제한하는 방법을 살펴보겠습니다.

사전 요구 사항

- Management Center 7.2.0 이상을 실행 중이며 매니지드 Threat Defense도 7.2.0 이상인지 확인합니다.
- 엘리펀트 플로우 탐지를 활성화한다고 해서 추가 연결 이벤트가 생성되지는 않습니다. 엘리펀트 플로우 탐지 기능은 이미 Management Center에 로깅되어 있는 일치하는 연결에 엘리펀트 플로우 표기법을 추가합니다. 이러한 이벤트를 로깅하려면 액세스 제어 정책에서 연결 로깅을 활성화해야 합니다. 특정 규칙에 대해 이 작업을 수행하거나 엘리펀트 플로우를 포함한 모든 연결을 로깅하는 Monitor(모니터) 규칙을 추가할 수 있습니다.

엘리펀트 플로우 매개변수 구성

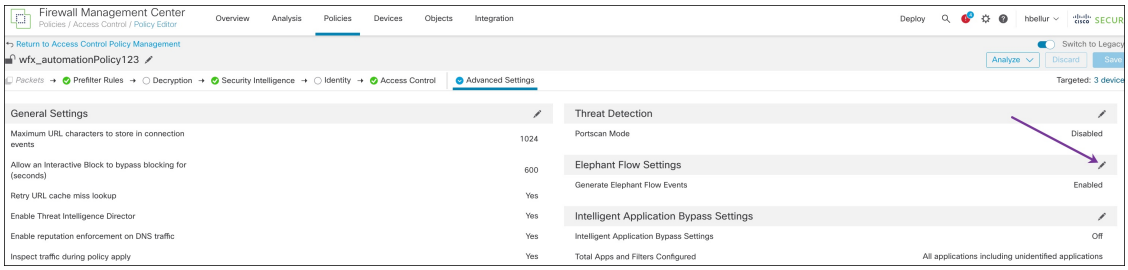
프로시저

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

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

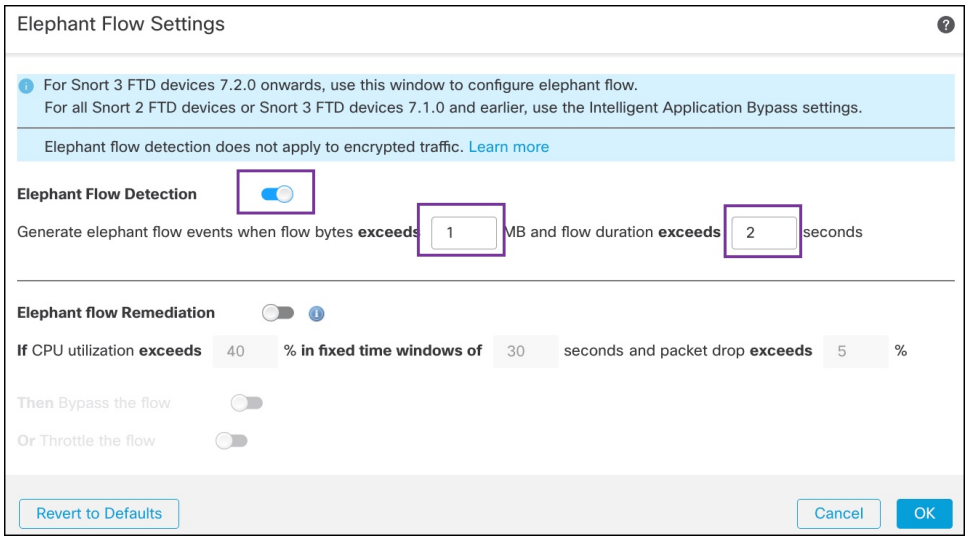
단계 **3** 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **4** **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 옆에 있는 **Edit(**편집**)**(✎)을 클릭합니다.



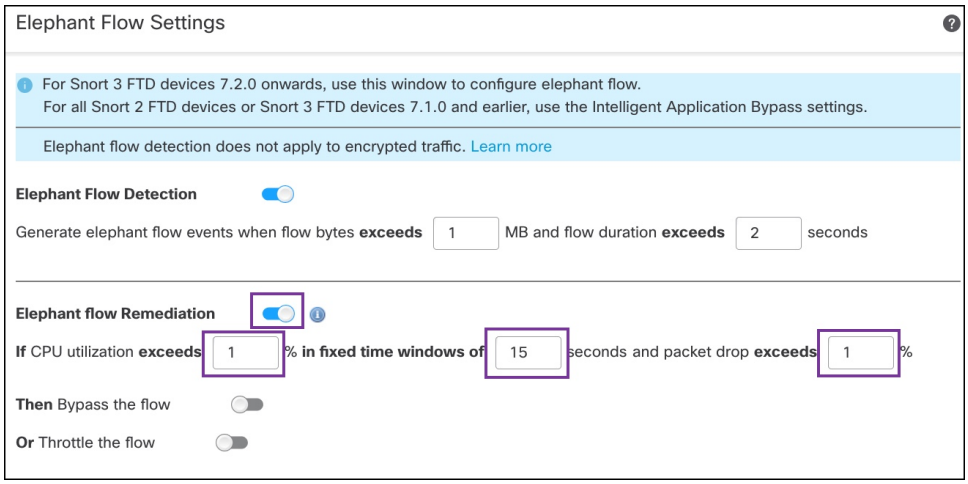
단계 **5** **Elephant Flow Detection(**엘리펀트 플로우 탐지**)** 토글 버튼은 기본적으로 활성화되어 있습니다. 기본 설정은 탐지만 활성화하며, 기본 작업은 구성되지 않습니다. 탐지 설정을 사용하면 플로우 바이트 및 기간을 조정하여 시스템에서 엘리펀트 플로우를 식별할 수 있습니다.

다음 그림에 나와 있는 것처럼 테스트 설정으로 플로우 바이트 및 기간 매개변수를 구성합니다.

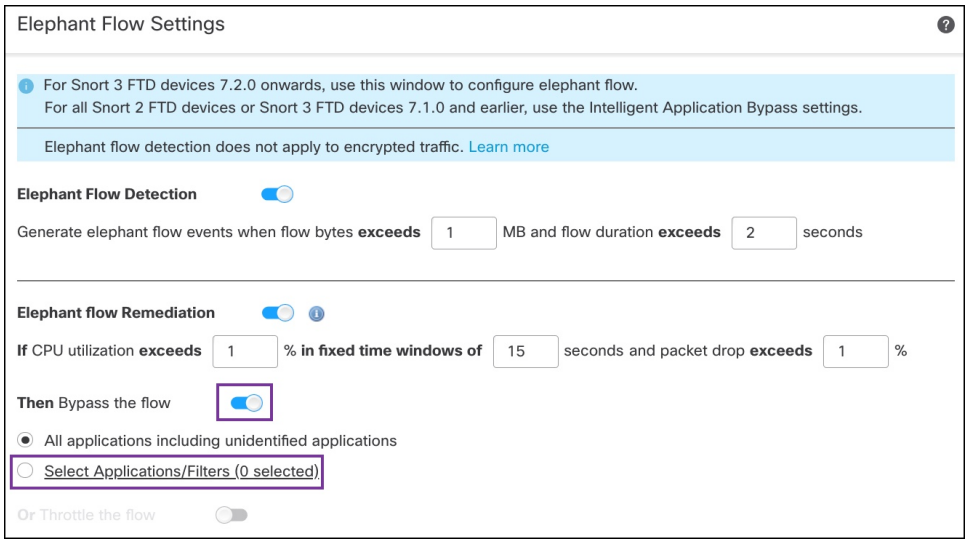


단계 **6** **Elephant Flow Remediation(**엘리펀트 플로우 교정**)** 토글 버튼을 활성화합니다. 엘리펀트 플로우가 탐지되면 플로우를 우회하거나 제한하도록 선택할 수 있습니다. 플로우를 우회하면 트래픽이 Snort 검사 없이 통과할 수 있습니다. 제한은 플로우 처리량이 감소되었음을 나타냅니다. CPU 사용률이 구성된 임계값 미만으로 감소할 때까지 10% 단위로 속도 감소가 이루어집니다.

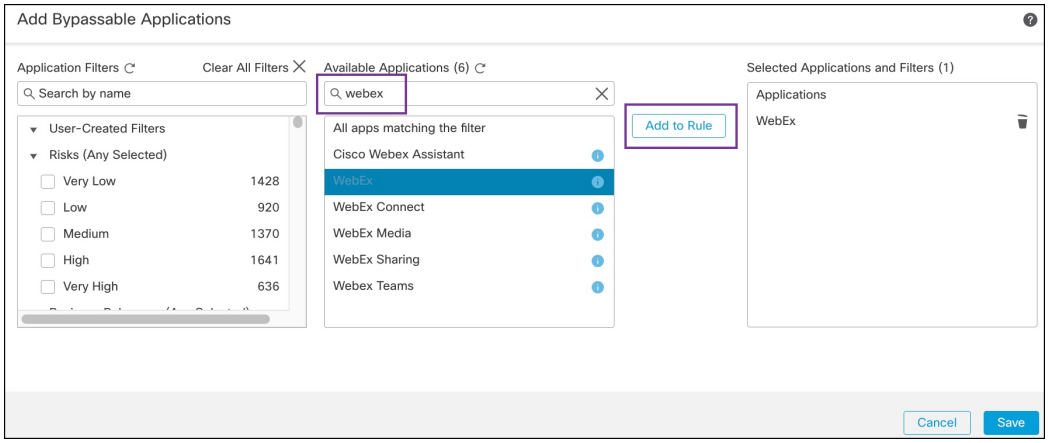
다음 그림에 표시된 것과 같이 엘리펀트 플로우 교정 매개변수를 테스트 설정으로 구성합니다.



단계 **7** **Bypass the flow(**플로우 우회**)** 토글 버튼을 활성화하고 **Select Applications/Filters(**애플리케이션/필터 선택**)** 라디오 버튼을 클릭합니다.



단계 **8** **Application Filters(**애플리케이션 필터**)**에서 **WebEx** 애플리케이션을 검색하여 선택하고, 규칙에 추가한 다음 **Save(**저장**)**를 클릭합니다. 즉, 구성된 매개변수에 따라 이러한 WebEx 연결이 엘리펀트 플로우로 탐지되면 WebEx 연결이 신뢰되고 우선순위가 지정되며 Snort 검사를 건너뜁니다.



단계 **9** 위협을 유발하는 나머지 플로우를 제한하려면 **Throttle(**제한**)** 토글 버튼을 활성화합니다. 이렇게 하면 Snort 위협 조건이 충족될 때까지 다른 모든 플로우의 속도가 10%씩 느려집니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

엘리펀트 플로우에 대한 이벤트 보기

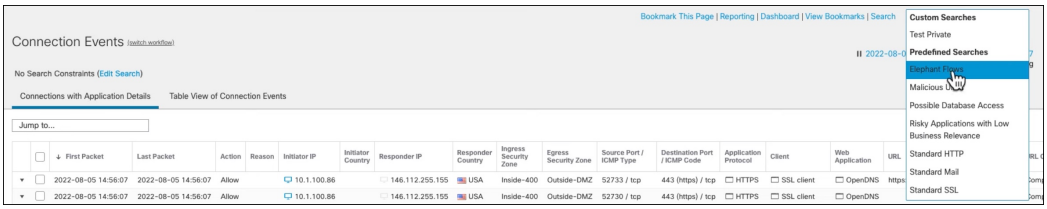
엘리펀트 플로우 설정을 구성한 후 연결 이벤트를 모니터링하여 플로우가 탐지, 우회 또는 제한되었는지 확인합니다. 연결 이벤트의 **Reason(**사유**)** 필드에서 이 정보를 확인할 수 있습니다. 엘리펀트 플로우 연결의 세 가지 유형은 다음과 같습니다.

- 엘리펀트 플로우
- 엘리펀트 플로우 제한
- 엘리펀트 플로우 신뢰

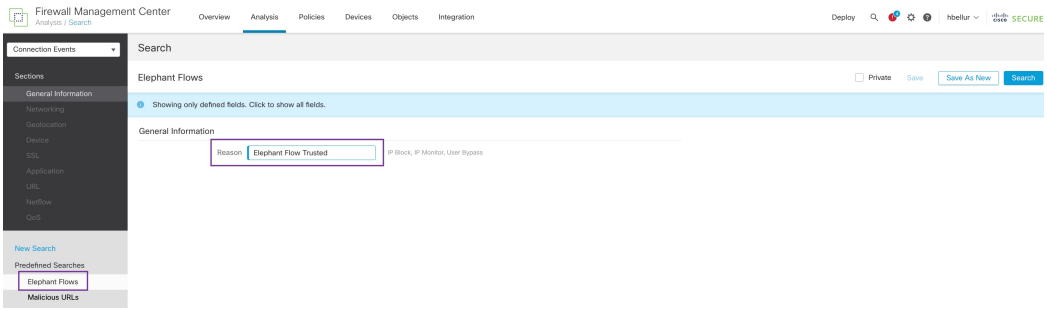
프로시저

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

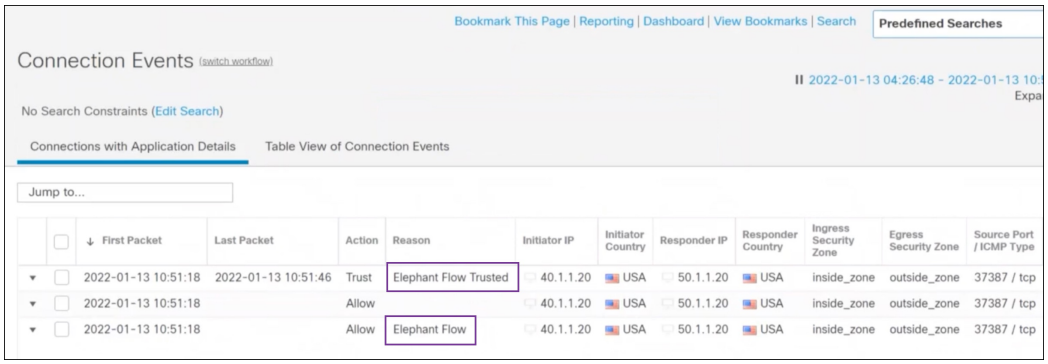
단계 **2** **Connection Events(**연결 이벤트**)** 페이지의 **Predefined Search(**사전 정의된 검색**)** 드롭다운 목록에서 **Elephant Flows(**엘리펀트 플로우**)**를 선택하여 엘리펀트 플로우 이벤트를 표시합니다.



팁
Elephant Flow Trusted(엘리펀트 플로우 신뢰**)** 또는 **Elephant Flow Throttled(**엘리펀트 플로우 제한**)** 이벤트 유형을 보려면 페이지 왼쪽 상단 모서리에 있는 **Edit Search(**검색 편집**)** 링크를 클릭하고 **Reason(**사유**)** 필드에서 왼쪽 패널의 **Elephant Flow(**엘리펀트 플로우**)**를 선택합니다. 검색하려는 대상에 따라 **Elephant Flow Trusted(**엘리펀트 플로우 신뢰**)** 또는 **Elephant Flow Throttled(**엘리펀트 플로우 제한**)**를 입력합니다.



단계 **3** 플로우 중에 탐지되어 **Reason(**사유**)** 필드에 **Elephant Flow(**엘리펀트 플로우**)**로 표시된 엘리펀트 플로우를 확인합니다. 플로우 종료 시에는 우회되고 **Reason(**사유**)** 필드에 **Elephant Flow Trusted(**엘리펀트 플로우 신뢰**)**가 표시됩니다.



엘리펀트 플로우 교정 제외 구성

교정에서 제외할 플로우에 대한 L4 ACL(액세스 제어 목록) 규칙을 구성할 수 있습니다. 플로우가 엘리펀트 플로우로 탐지되고 해당 플로우가 정의된 규칙과 일치하는 경우 해당 플로우는 교정 작업에서 제외됩니다.

시작하기 전에

Management Center 7.4.0 이상을 실행해야 하며, 매니지드 Threat Defense도 7.4.0 이상이어야 합니다.

프로시저

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

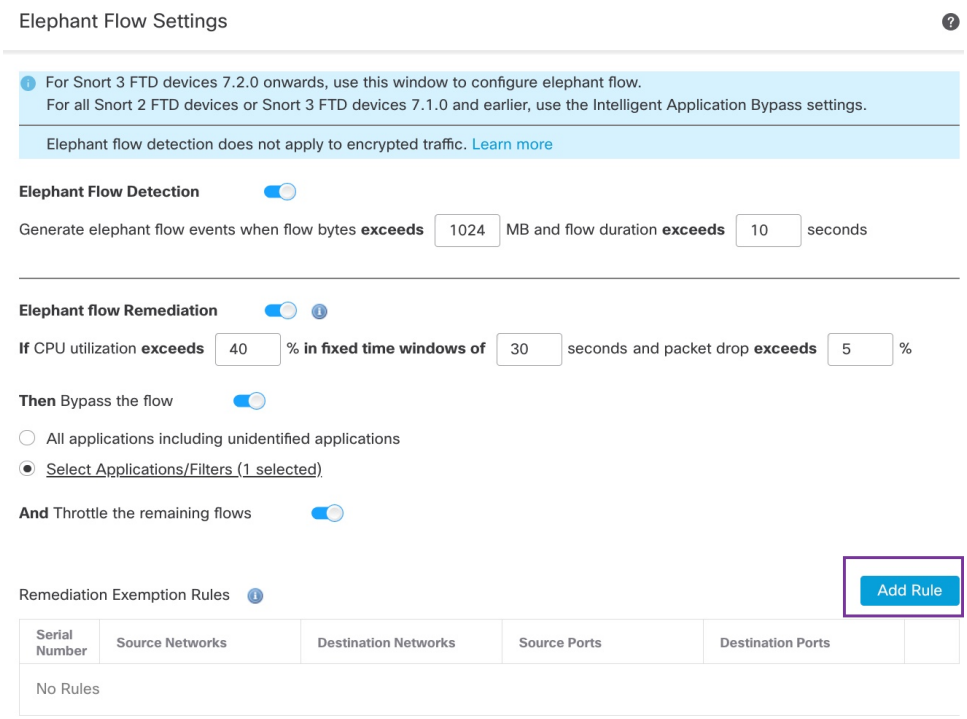
단계 2 편집하려는 액세스 제어 정책 옆에 있는 **Edit(**편집**)**( )을 클릭합니다.

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

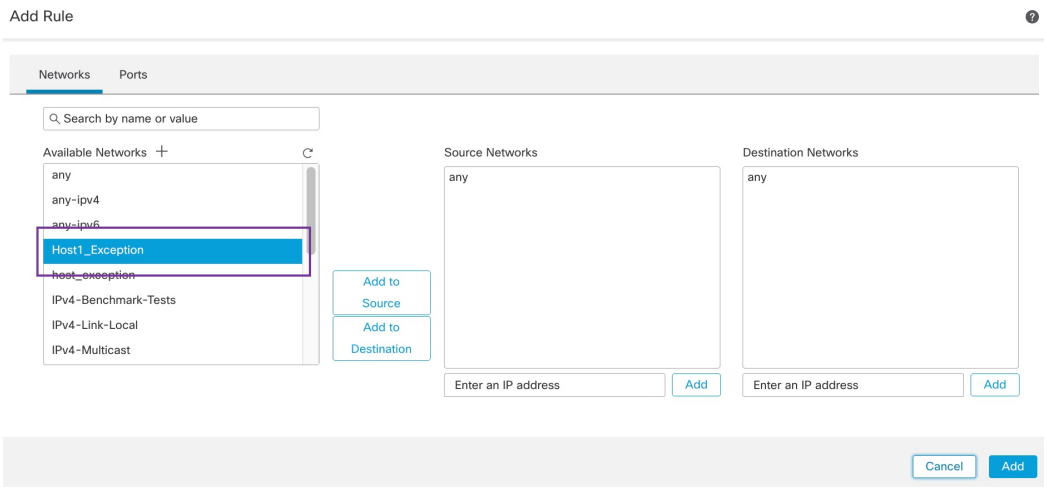
단계 4 **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 옆에 있는 **Edit(**편집**)**( )을 클릭합니다.

단계 5 엘리펀트 플로우 탐지 및 교정 매개변수를 구성했는지 확인합니다. 엘리펀트 플로우 매개변수 구성, 155 페이지의 내용을 참조하십시오.

단계 6 **Remediation Exemption Rules(**교정 제외 규칙**)** 옆에 있는 **Add Rule(**규칙 추가**)** 버튼을 클릭합니다.



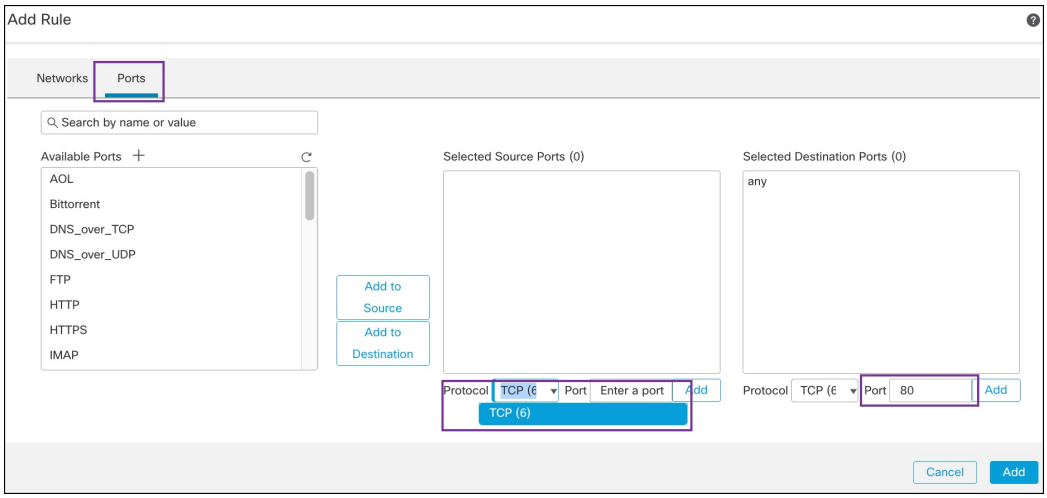
단계 **7** **Available Networks(**사용 가능한 네트워크**)** 목록에서 엘리펀트 플로우 교정에서 제외하도록 구성된 호스트를 선택합니다. 이 예에서는 "Host1_Exception"이라는 호스트를 생성했습니다.



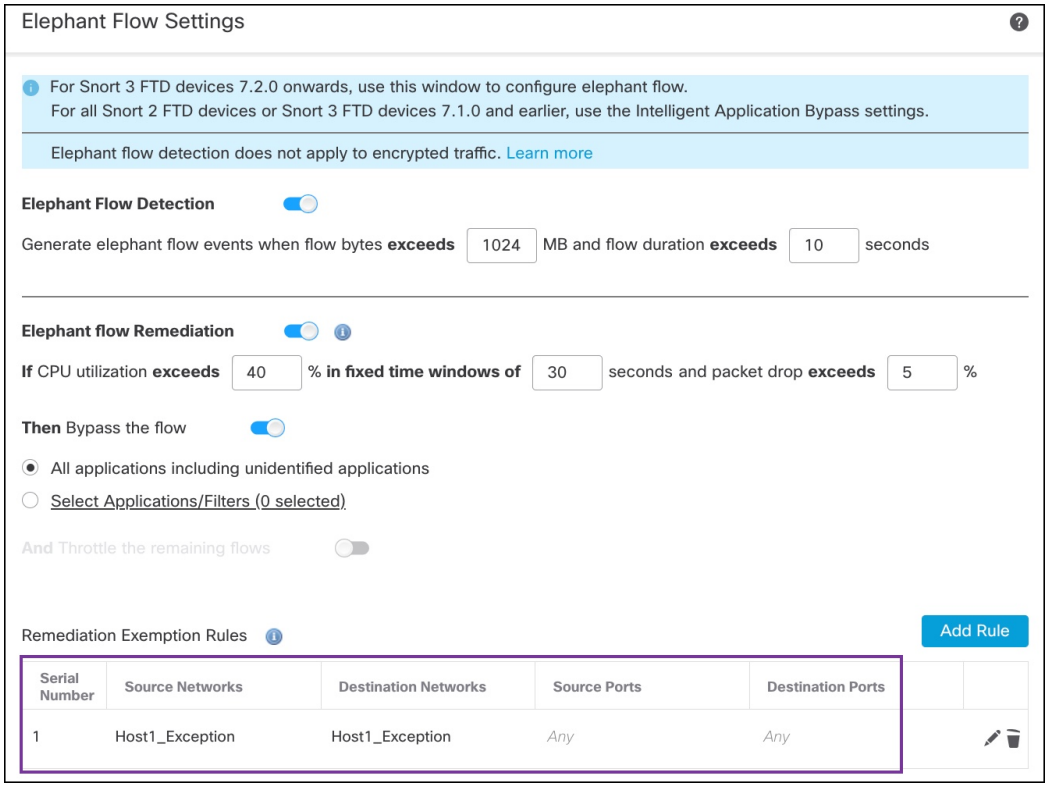
단계 **8** 필요에 따라 **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**을 클릭하여 이 호스트를 소스 또는 대상에 추가합니다.

단계 **9** **Ports(**포트**)** 탭을 클릭합니다.

단계 **10** 소스 포트에 대해 **Protocol as TCP(TCP**형 프로토콜**)**를 선택하고 목적지 포트로 **80**을 입력한 다음 **Add(**추가**)**를 클릭합니다.



단계 **11** **OK(**확인**)**를 클릭합니다.



단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

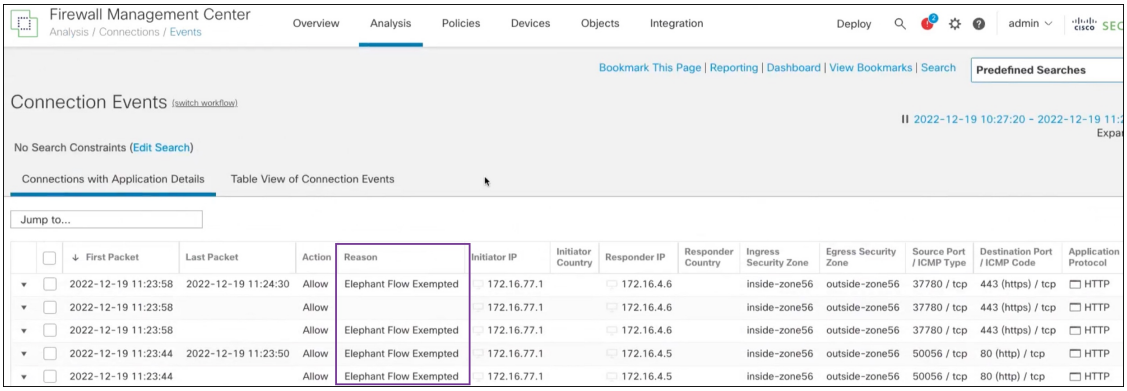
구성 변경 사항을 구축합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

엘리펀트 플로우 교정 제외에 대한 이벤트 보기

프로시저

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

단계 **2** 교정에서 제외된 엘리펀트 플로우를 확인합니다. **Reason(**사유**)** 필드에 **Elephant Flow Exempted(**엘리펀트 플로우 제외됨**)**가 표시됩니다.



추가 참조 자료

자세한 개념 정보는 이 가이드에 나와 있는 Snort 3의 엘리펀트 플로우 탐지 장이나 다음 링크의 콘텐츠를 참조하십시오.

- 엘리펀트 플로우 탐지

13 장

Snort 3 침입 정책에서 MITRE 프레임워크를 사용하여 위협 완화

MITRE ATT&CK 프레임워크 정보

MITRE ATT&CK 프레임워크는 공격자가 시스템을 손상시키기 위해 사용하는 위협(전술, 기술, 절차)를 간략하게 설명하는 포괄적인 기술 자료입니다. 이러한 TTP를 다양한 운영체제 및 플랫폼을 위한 매트릭스로 구성하고, 각 공격 단계(전술)를 특정 방법(기술)에 매핑합니다. 각 기술에는 실행, 절차, 방어, 탐지, 실제 사례에 대한 정보가 포함됩니다.

참고 MITRE ATT&CK에 대한 자세한 내용은 https://attack.mitre.org를 참조하십시오.

관리 센터는 MITRE ATT&CK 프레임워크를 사용하여 다음 기능을 통합하여 위협 탐지 및 대응을 개선합니다.

- 침입 이벤트에는 TTP가 포함되며, 이를 통해 관리자는 취약성 유형, 대상 시스템 또는 위협 범주에 따라 규칙을 그룹화하여 트래픽을 더 세부적으로 관리할 수 있습니다.
- 일부 멀웨어 이벤트는 TTP를 사용하여 위협을 탐지하고 대응하는 기능을 강화합니다.
- 통합 이벤트 및 기본 이벤트 뷰어에는 Talos 분류의 전술, 기술, 공격 라이프사이클 그래프 및 상황별 보강 정보가 표시됩니다. 이러한 보강 기능에는 MITRE 태그 및 관련 전략, 기술 및 하위 기술의 계층적 보기가 포함됩니다. MITRE 식별자를 사용하여 이벤트를 필터링할 수도 있습니다.

MITRE 프레임워크의 이점

- MITRE TTP(전략, 기술 및 절차)가 침입 이벤트에 추가되어 있으며, 관리자는 MITRE ATT&CK 프레임워크를 기반으로 트래픽에 대해 조치를 취할 수 있습니다. 이렇게 하면 관리자는 보다 세밀하게 트래픽을 보고 처리할 수 있으며 취약성 유형, 대상 시스템 또는 위협 범주별로 규칙을 그룹화할 수 있습니다.
- MITRE ATT&CK 프레임워크에 따라 침입 규칙을 구성할 수 있습니다. 이를 통해 특정 공격자의 전술과 기술에 따라 정책을 맞춤화할 수 있습니다.

MITRE 네트워크를 위한 샘플 비즈니스 시나리오

대규모 기업 네트워크에서는 Snort 3를 기본 침입 탐지 및 방지 시스템으로 사용합니다. 빠르게 진화하는 위협 환경에서 강력한 네트워크 보안 조치의 채택은 꼭 필요하며 중요합니다. 네트워크 관리자는 구성된 정책이 관심 트래픽을 찾는지, 알려진 공격 그룹을 추적하고 있는지를 알아야 합니다. 예를 들어, 공격자가 예기치 않은 행동을 유발하기 위해 시스템이나 애플리케이션의 취약점을 악용하려고 시도하는지 알고 싶을 수 있습니다. 시스템의 취약점은 버그, 결함 또는 설계 취약점일 수 있습니다. 애플리케이션은 웹사이트, 데이터베이스, SMB(Server Message Block) 또는 SSH(Secure Shell)와 같은 표준 서비스, 네트워크 디바이스 관리 및 관리 프로토콜 또는 애플리케이션(예: 웹 서버 및 관련 서비스)일 수 있습니다.

MITRE 프레임워크가 제공하는 인사이트는 관리자에게 특정 자산에 대한 보호를 지정하고 특정 위협 그룹으로부터 네트워크 를 보호할 수 있는 더욱 정확한 기회를 제공합니다.

MITRE 프레임워크 사전 요건

- Secure Firewall Management Center 및 Secure Firewall Threat Defence 버전 7.3.0 이상을 Snort 3과 함께 실행하고 있어야 합니다.
- 하나 이상의 침입 정책이 있어야 합니다. 사용자 지정 Snort 3 침입 정책 생성 , 34 페이지의 내용을 참조하십시오.

Snort 3 침입 정책 보기 및 편집

프로시저

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

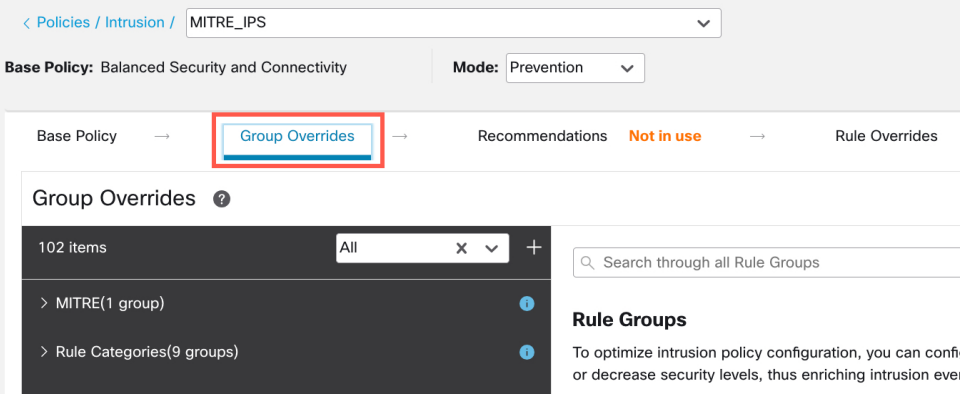
단계 2 **Intrusion Policies(침입 정책)** 탭이 선택되었는지 확인합니다.

단계 3 보거나 편집하려는 침입 정책 옆의 **Snort 3 Version(Snort 3 버전)**을 클릭합니다.

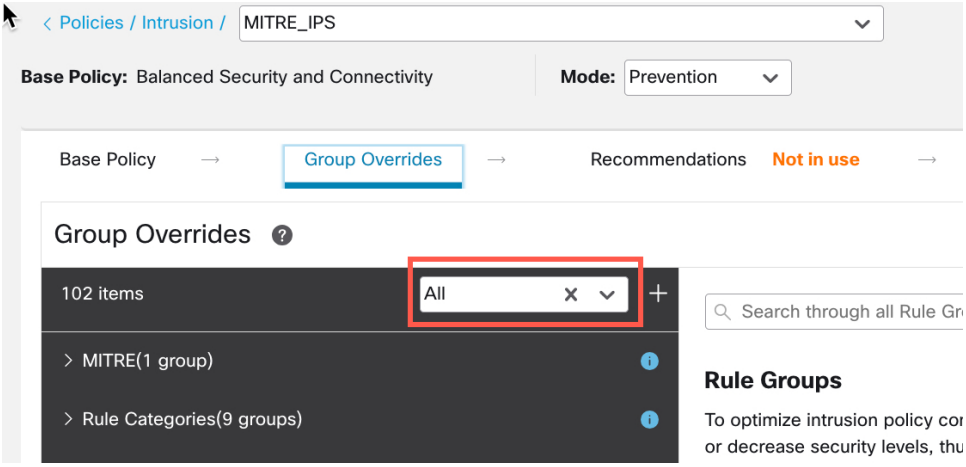
단계 4 표시되는 Snort 헬퍼 가이드를 닫습니다.

단계 5 **Group Overrides(**그룹 재정의**)** 레이어를 클릭합니다.

이 레이어는 규칙 그룹의 모든 범주를 계층적 구조로 나열합니다. 각 규칙 그룹 아래에서 마지막 리프 규칙 그룹으로 드릴다운할 수 있습니다.

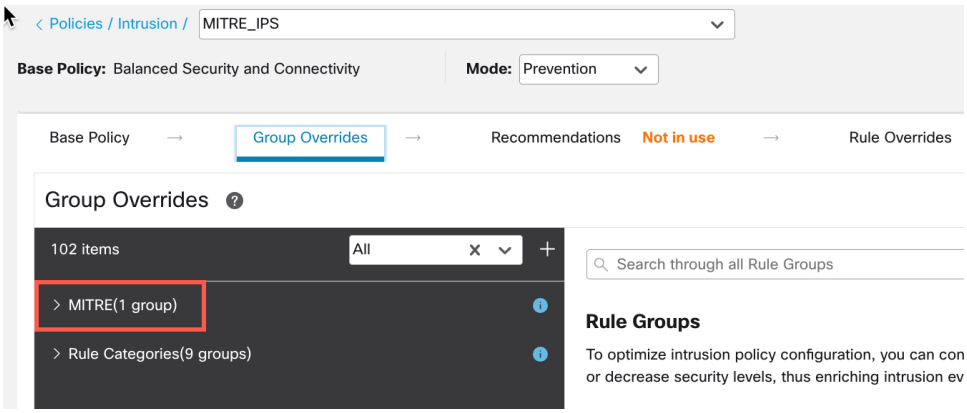


단계 6 **Group Overrides(**그룹 재정의**)** 아래의 드롭다운 목록에서 **All(**모두**)**이 선택되어 해당하는 침입 정책에 대한 모든 규칙 그룹이 왼쪽 창에 표시됩니다.

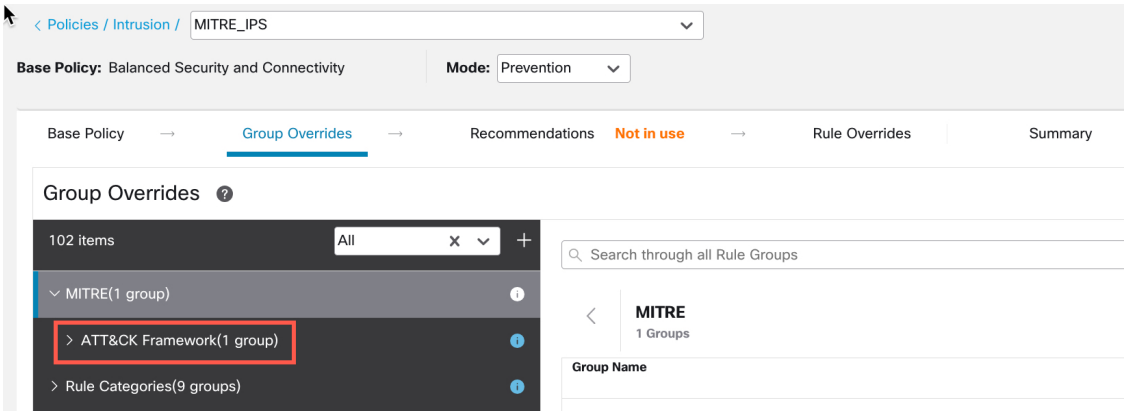


단계 7 왼쪽 창에서 **MITRE**를 클릭합니다.

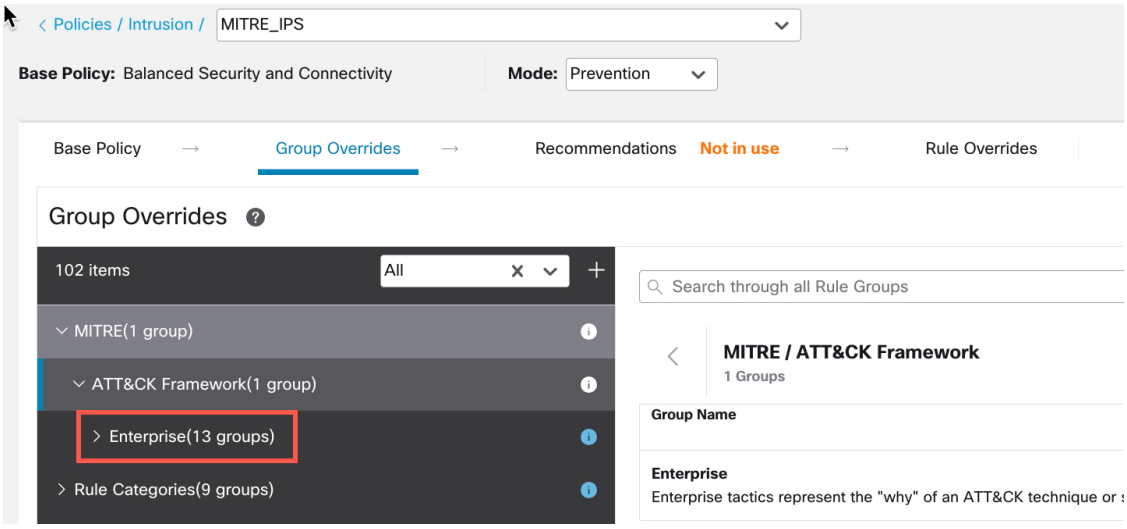
참고
특정 요건에 따라 **Rule Categories(**규칙 범주**)** 규칙 그룹 또는 그 아래에 있는 다른 규칙 그룹 및 하위 규칙 그룹을 선택할 수 있습니다. 모든 규칙 그룹은 MITRE 프레임워크를 사용합니다.



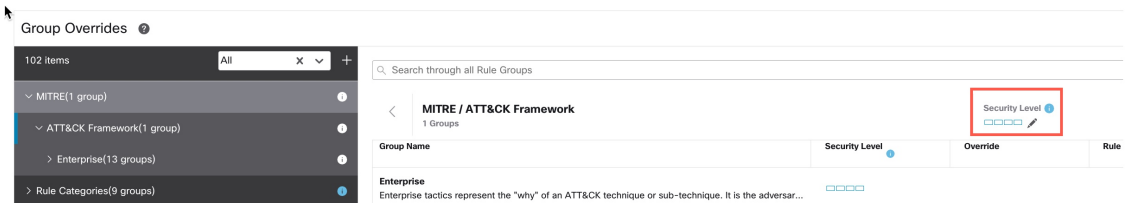
단계 **8** **MITRE**에서 **ATT&CK Framework(ATT&CK** 프레임워크**)**를 클릭하여 드릴다운합니다.



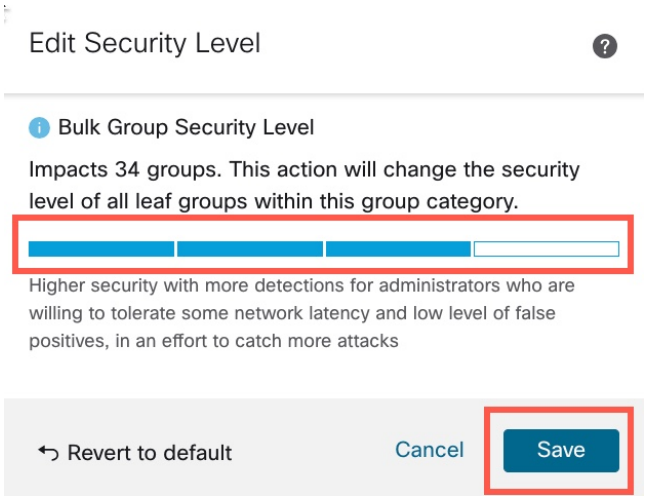
단계 **9** **ATT&CK Framework(ATT&CK** 프레임워크**)**에서 **Enterprise(**엔터프라이즈**)**를 클릭하여 프레임워크를 확장합니다.



단계 **10** **Enterprise(**엔터프라이즈**)** 규칙 그룹 범주에 속하는 모든 관련 규칙 그룹의 보안 수준을 대량으로 변경하려면 규칙 그룹의 **Security Level(**보안 수준**)** 옆에 있는 **Edit(**편집**)(**✎**)** 아이콘을 클릭합니다.

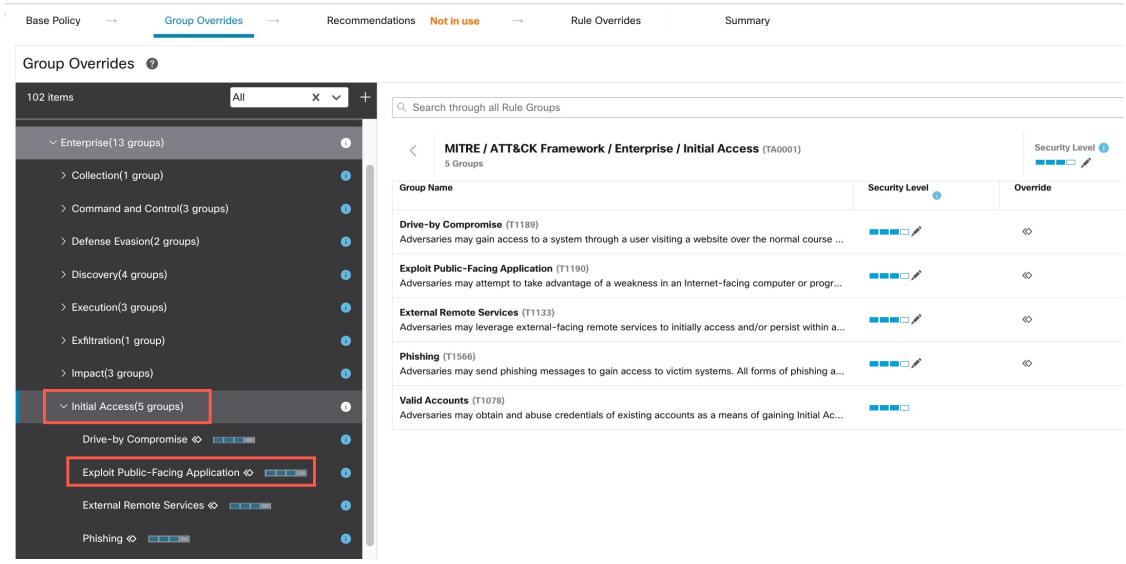


단계 **11** **Edit Security Level(**보안 수준 편집**)** 창에서 **Security Level(**보안 수준**)**(이 예에서는 **3**)을 선택하고 **Save(**저장**)**를 클릭합니다.

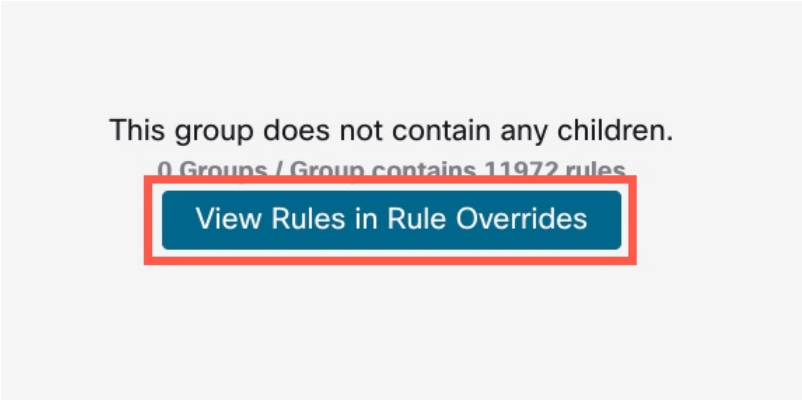


단계 **12** **Enterprise(**엔터프라이즈**)**에서 **Initial Access(**초기 액세스**)**를 클릭하여 확장합니다.

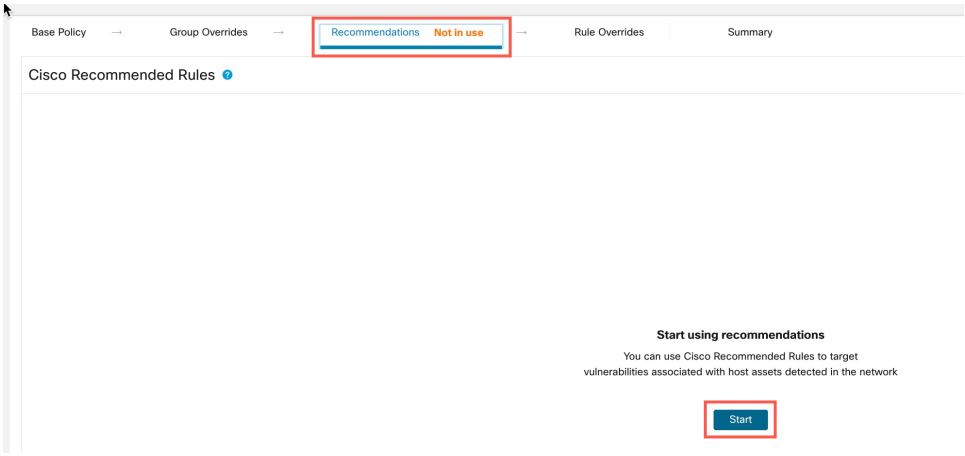
단계 **13** **Initial Access(**초기 액세스**)**에서 마지막 리프 그룹인 **Exploit Public-Facing Application(**공개 애플리케이션 익스플로잇**)**을 클릭합니다.



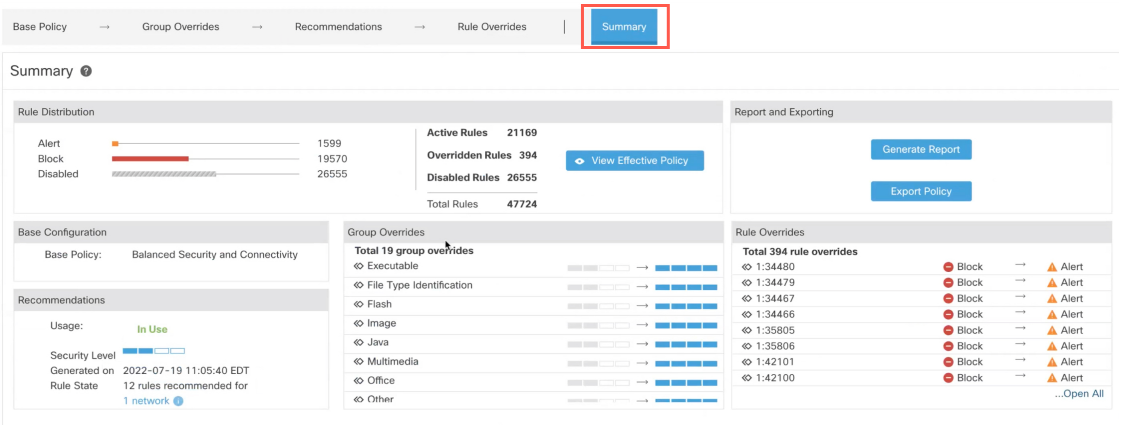
단계 **14** **View Rules in Rule Overrides(**규칙 오버라이드의 규칙 보기**)**를 클릭하여 다른 규칙에 대한 다른 규칙, 규칙 세부 정보, 규칙 작업 등을 봅니다. **Rule Overrides(**규칙 재정**)**의 레이어에서 하나 또는 여러 규칙에 대한 규칙 작업을 변경할 수 있습니다.



단계 **15** **Recommendations(**권장 사항**)** 레이어를 클릭한 다음 **Start(**시작**)**를 클릭하여 Cisco 권장 규칙 사용을 시작합니다. 침입 규칙 권장 사항을 사용하여 네트워크에서 탐지된 호스트 자산 관련 취약성을 대상으로 지정할 수 있습니다. 자세한 내용은 Snort 3에서 새로운 Secure Firewall 권장 사항 생성, 67 페이지를 참고하십시오.



단계 **16** **Summary(**요약**)** 레이어를 클릭하면 정책에 대한 현재 변경 사항을 전체적으로 볼 수 있습니다. 규칙 재정의, 보안 수준 변경 및 Cisco 권장 규칙 생성을 기반으로 정책의 규칙 배포, 그룹 재정의, 규칙 재정의, 규칙 권장 사항 등을 확인하여 변경 사항을 확인할 수 있습니다.



다음에 수행할 작업

침입 정책을 구축하여 Snort 규칙에 의해 트리거되는 이벤트를 탐지하고 기록합니다. 구성 변경 사항 구축, 28 페이지의 내용을 참조하십시오.

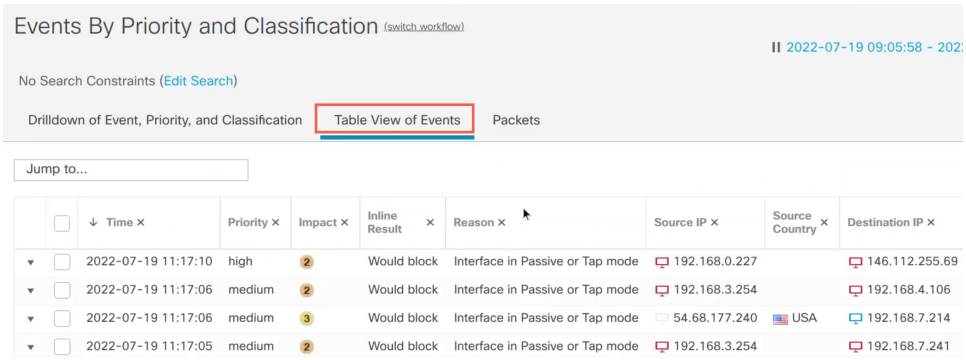
침입 이벤트 보기

Classic Event Viewer(클래식 이벤트 뷰어) 및 **Unified Event Viewer**(통합 이벤트 뷰어) 페이지의 침입 이벤트에서 MITRE ATT&CK 기술 및 규칙 그룹을 볼 수 있습니다. Talos는 Snort 규칙(GID:SID)에서 MITRE ATT&CK 기술 및 규칙 그룹으로의 매핑을 제공합니다. 이러한 매핑은 LSP(Lightweight Security Package)의 일부로 설치됩니다.

프로시저

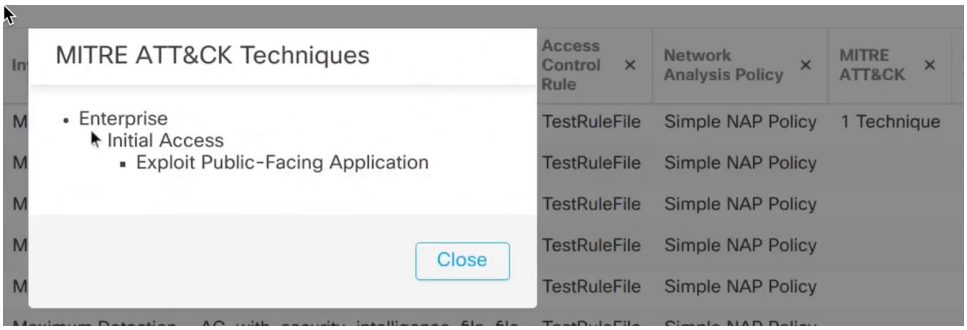
단계 **1** **Analysis**(분석)를 클릭하고 **Intrusion**(침입) 아래에서 **Events**(이벤트)를 선택합니다.

단계 **2** **Table View of Events**(이벤트 테이블 보기) 탭을 클릭합니다.



단계 **3** **MITRE ATT&CK**아래에서 침입 이벤트 기술을 확인할 수 있습니다. MITRE ATT&CK 기술을 보려면 **1 Technique(1** 기술**)**을 클릭합니다.

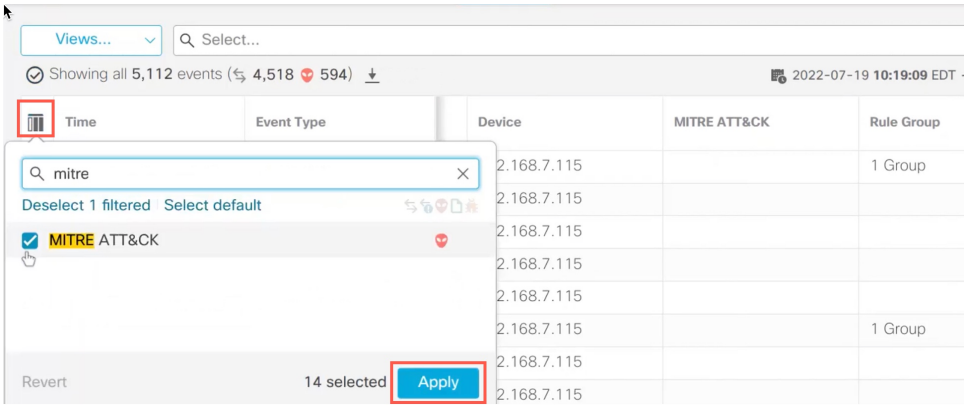
이 예시에서는 공개 애플리케이션 익스플로잇 이 기술입니다.



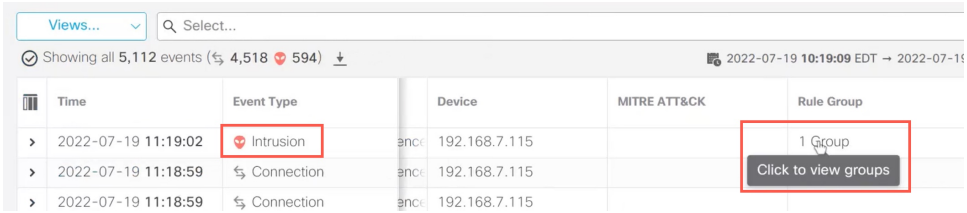
단계 **4** **Close(**닫기**)**를 클릭합니다.

단계 **5** **Analysis(**분석**)**를 클릭하고 **Unified Events(**통합 이벤트**)**를 선택합니다.

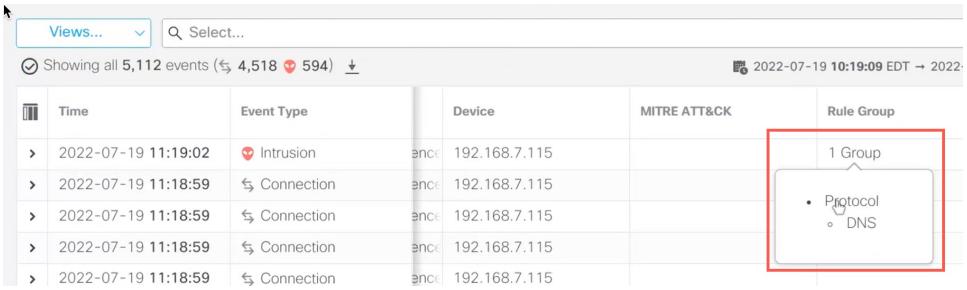
단계 **6** 활성화되지 않은 경우 열 선택기 아이콘을 클릭하여 **MITRE ATT&CK** 및 **Rule Group(**규칙 그룹**)** 열을 활성화합니다.



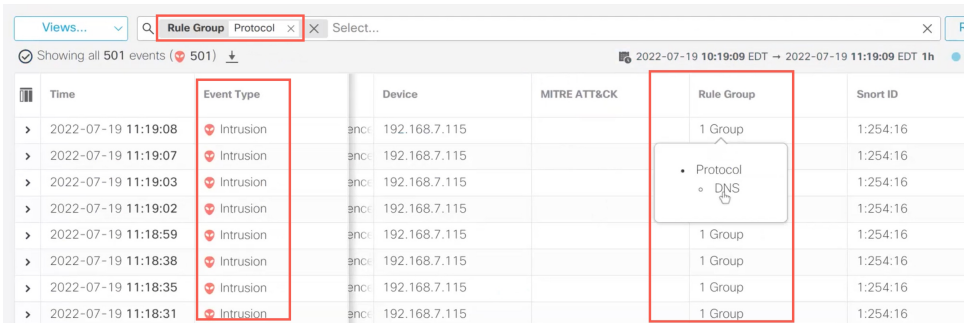
단계 **7** 이 예에서 침입 이벤트는 하나의 규칙 그룹에 매핑된 이벤트에 의해 트리거됩니다. **Rule Group(**규칙 그룹**)** 열에서 **1 Group(1** 그룹**)**을 클릭합니다.



단계 **8** 상위 규칙 그룹 및 그 아래의 DNS(Domain Name System) 규칙 그룹인 **Protocol(**프로토콜**)**을 볼 수 있습니다. **Protocol(**프로토콜**)** > **DNS**를 선택하여 규칙 그룹이 하나 이상 있는 모든 침입 이벤트를 검색합니다.



검색 결과가 표시됩니다.



추가 참조 자료

- Snort 3의 침입 정책
- Snort 3 침입 정책 편집, 35 페이지
- 악성코드 이벤트의 MITRE 정보