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 엔진의 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 기능

을 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 보기를 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 동기화를 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 규칙를 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 편집의 내용을 참조하십시오.

  침입 이벤트에서의 규칙 그룹 보고에 대해서는 규칙 그룹 보고의 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 엔진의 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.

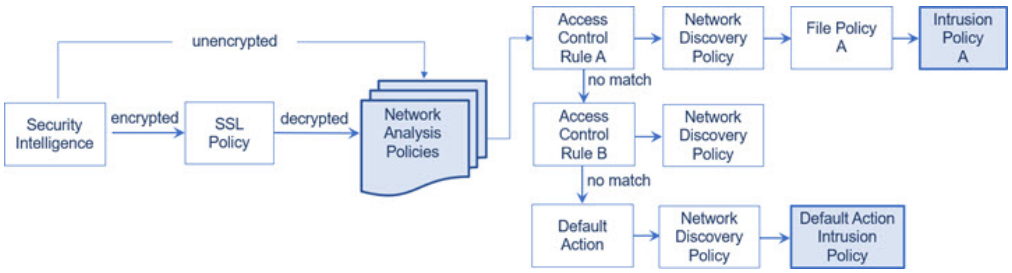
표 ***1: Snort 3***의 기능 제한 사항

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.

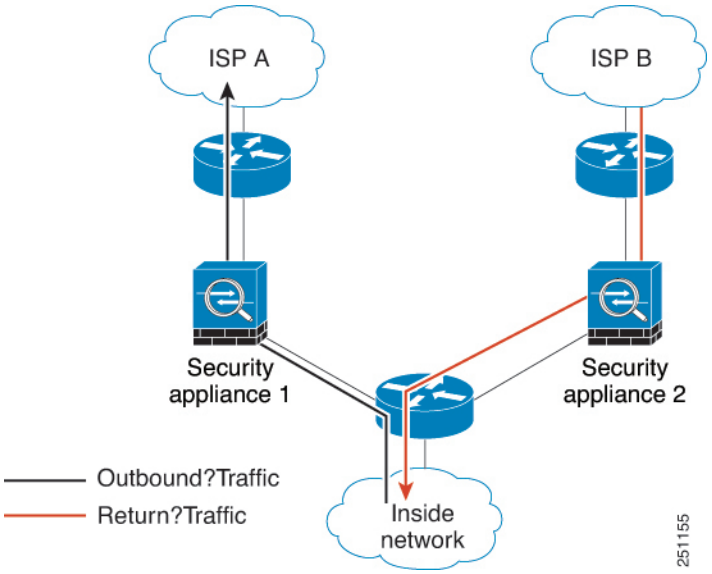
데이터베이스에 침입 이벤트가 누적됨에 따라 잠재적인 공격의 분석을 시작할 수 있습니다. 시스템은 침입 이벤트를 검토하고 네트워크 환경 및 보안 정책의 컨텍스트에서 중요성을 띠는지 여부를 평가하는 데 필요한 도구를 제공합니다.

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.

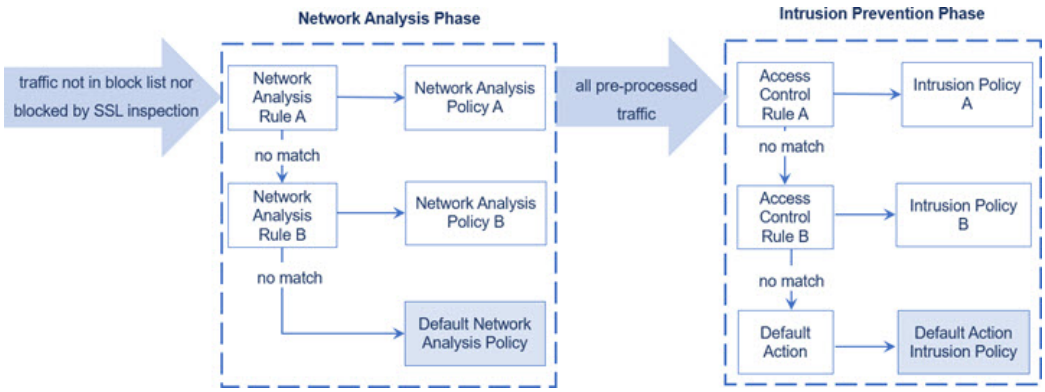
여러 사용자 지정 네트워크 분석 정책을 사용하는 경우 추가 문제가 발생합니다. 복잡한 구축을 수행하는 고급 사용자의 경우, 일치하는 트래픽을 전처리하는 맞춤형 네트워크 분석 정책을 할당하여 특정 보안 영역, 네트워크, VLAN에 맞게 전처리를 조정할 수 있습니다. (ASA FirePOWER는 VLAN에 의한 전처리를 제한할 수 없는 점에 유의하십시오.) 이를 수행하려면, 액세스 제어 정책에 사용자 지정 네트워크 분석 규칙을 추가합니다. 각 규칙에 규칙과 일치하는 트래픽의 전처리를 관리하는 연결된 네트워크 정책 분석이 있습니다.

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.