침입 정책 시작하기

다음 주제에서는 침입 정책을 시작하는 방법을 설명합니다.

침입 정책 기본 사항

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 Talos 인텔리전스 그룹의 경험을 활용할 수 있는 여러 기본 침입 정책을 제공합니다. Talos는 이 정책에 대해 침입 및 전처리기 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.
- Cisco 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결합니다.
- 외부 경고, 민감한 데이터 전처리 및 전역 규칙 임계값과 같은 다양한 고급 설정을 구성합니다.
- 효율적으로 여러 침입 정책을 관리하기 위해 레이어를 구성 요소로 사용합니다.

인라인 배포에서 침입 정책은 트래픽을 차단하고 수정할 수 있습니다.

- 삭제 규칙은 일치하는 패킷을 삭제하고 침입 이벤트를 생성할 수 있습니다. 침입 또는 전처리기 삭제 규칙을 구성하려면 해당 상태를 Drop and Generate Events(이벤트 삭제 및 생성)로 설정합니다.
- 침입 규칙은 `replace` 키워드를 사용하여 악성 콘텐츠를 교체할 수 있습니다.

침입 규칙이 트래픽에 영향을 주려면 삭제 규칙 및 콘텐츠를 교체하는 규칙을 올바르게 구성해야 하며, 매니지드 디바이스를 인라인으로(즉, 인라인 인터페이스 집합으로) 올바르게 구축해야 합니다. 마지막으로, 침입 정책의 삭제 작업을 활성화하거나 **Drop when Inline(**인라인 시 삭제**)** 설정을 활성화해야 합니다.

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. 필수 전처리기를 비활성화하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 자동으로 전처리기를 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.

침입 정책을 위한 라이선스 요건

Threat Defense 라이선스

IPS

기본 라이선스

보호

침입 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 정책 관리

Intrusion Policy(침입 정책) 페이지(**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**)에서 다음 정보와 함께 현재의 맞춤형 침입 정책을 볼 수 있습니다.

- 정책이 최종 수정된 시간과 날짜(로컬 시간) 및 정책을 수정한 사용자
- **Drop When Inline(**인라인 시 삭제**)** 설정의 활성화 여부. 이는 인라인 배포에서 트래픽을 삭제하고 수정할 수 있도록 합니다. 인라인 구축은 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 디바이스에 구축되는 구성일 수 있습니다.
- 트래픽을 검사하기 위해 침입 정책을 사용하는 액세스 제어 정책 및 디바이스의 유형
- 정책에 저장되지 않은 변경 사항이 있는지 여부 및 현재 정책을 수정하고 있는 사람에 관한 정보
- 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**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 침입 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교를 참조하십시오.
- 생성 - **Create Policy(**정책 생성**)**를 클릭합니다. 참조:
  - Snort 2 정책의 경우 사용자 지정 Snort 2 침입 정책 생성, 5 페이지
  - Cisco Secure Firewall Management Center Snort 3 구성 가이드 최신 버전의 Snort 3 정책에 사용자 지정 *Snort 3* 침입 정책 생성 항목.
- 삭제 - 삭제하려는 정책 옆에 있는 **Delete(**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.
- Edit(편집) - 다음을 선택합니다.
  - **Snort 2** 버전; Snort 2 침입 정책 편집, 5 페이지 참조.
  - **Snort 3** 버전의 경우 Cisco Secure Firewall Management Center Snort 3 구성 가이드 최신 버전의 *Editing Snort 3* 침입 정책 항목을 참조하십시오.

  View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 내보내기 - 다른 Secure Firewall Management Center에서 가져올 침입 정책을 내보내려면 **YouTube EDU** ( )를 클릭합니다. Cisco Secure Firewall Management Center 관리 가이드의 구성 내보내기를 참조하십시오.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 구성 변경 사항 구축의 내용을 참조하십시오.
- 보고서 - **Report(**보고서**)** ( )을(를) 클릭합니다. 현재 정책 보고서 생성의 내용을 참조하십시오.

맞춤형 침입 정책 생성

새로운 침입 정책을 만드는 경우, 사용자는 반드시 고유한 이름을 제공하고, 기본 정책을 지정하며, 삭제 작업을 지정해야 합니다.

기본 정책은 침입 정책의 기본 설정을 정의합니다. 새로운 정책에서 구성을 변경하면 기본 정책 설정을 대체하지만 변경하지는 않습니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다.

사용자 지정 **Snort 2** 침입 정책 생성

프로시저

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

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다. 다른 정책에 저장되지 않은 변경 사항이 있는 경우, Intrusion Policy(침입 정책) 페이지로 돌아가라는 메시지가 나타나면 **Cancel(**취소**)**을 클릭합니다.

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

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.

단계 **5** 최초 **Base Policy(**기본 정책**)**를 선택합니다.

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

단계 **6** **Save(**저장**)**를 클릭합니다.

새로운 정책의 설정은 기본 정책의 설정과 같습니다.

관련 항목

레이어 내 침입 규칙
충돌 및 변경: 네트워크 분석 및 침입 정책

Snort 2 침입 정책 편집

프로시저

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

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

단계 **3** 구성하려는 침입 정책 옆의 **Snort 2** 버전을 클릭합니다.

단계 **4** 정책 수정:

- 기본 정책 변경 - **Base Policy(**기본 정책**)** 드롭다운 목록에서 기본 정책을 선택합니다(기반 정책 변경 참조).
- 고급 설정 구성 - 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다(침입 정책 고급 설정, 10 페이지 참조).
- Cisco 권장 침입 규칙 구성 - 탐색 패널에서 **Cisco Recommendations**를 클릭합니다. Cisco 권장 사항 생성 및 적용의 내용을 참조하십시오.
- 인라인 구축의 삭제 동작 - **Drop when Inline(**인라인 시 삭제**)**을 선택하거나 선택 취소합니다(인라인 배포에서 삭제 작업 설정하기, 9 페이지 참조).
- 권장 규칙 상태에 따라 규칙 필터링 - 권장 사항을 생성한 후 각 권장 사항 유형 옆에 있는 **View(**보기**)**를 클릭합니다. 모든 권장 사항을 보려면 **View Recommended Changes(**권장 변경 사항 보기**)**를 클릭합니다.
- 현재 규칙 상태에 따라 규칙 필터링 - 각 규칙 상태 유형(이벤트 생성, 이벤트 삭제 및 생성) 옆에 있는 **View(**보기**)**를 클릭합니다(침입 정책의 침입 규칙 필터 참조).
- 정책 레이어 관리 - 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다(레이어 관리 참조).
- 침입 규칙 관리 - **Manage Rules(**규칙 관리**)**를 클릭합니다(침입 정책의 침입 규칙 보기 참조).
- 기본 정책의 설정 보기 - **Manage Base Policy(**기본 정책 관리**)**를 클릭합니다(기본 레이어 참조).

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

관련 항목

Cisco 권장 사항 생성 및 적용
레이어에서 침입 규칙 구성
충돌 및 변경: 네트워크 분석 및 침입 정책

침입 정책 변경

새 침입 정책을 생성할 때, 기본 정책과 동일한 침입 규칙 및 고급 설정을 갖습니다.

시스템은 사용자당 하나의 침입 정책을 캐시합니다. 침입 정책을 수정하는 동안 메뉴를 선택하거나 다른 페이지로 이동하는 다른 경로를 선택하는 경우, 해당 페이지에서 나가더라도 변경 사항이 시스템 캐시에 남아 있습니다.

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 Firepower System에서 여러 침입 정책을 제공합니다. 시스템이 제공하는 침입 정책을 사용하여 Talos 인텔리전스 그룹의 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 Secure Firewall Management Center에 저장됩니다. 시스템은 또한 액세스 제어 규칙의 로깅 구성에 관계없이 침입이 발생한 연결의 종료를 Secure Firewall Management Center 데이터베이스에 자동으로 로깅합니다.

관련 항목

사전 정의된 기본 변수

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 만들거나 기존 규칙을 편집합니다. 액세스 제어 규칙 구성 요소 참조.

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 맞춤형 **Intrusion Policy(**침입 정책**)**를 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

- Deploy configuration changes(구성 변경 사항 구축)참조.

관련 항목

변수 세트

Snort® 재시작 시나리오

인라인 구축의 삭제 작업

인라인 구축에서 트래픽에 실제로 영향을 주지 않고 구성이 어떻게 작동하는지(즉, 관련 구성이 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 디바이스에 구축되는지) 평가하려면 삭제 동작을 비활성화합니다. 이 경우, 시스템은 침입 이벤트를 생성하지만 삭제 규칙을 트리거하는 패킷을 삭제하지는 않습니다. 결과에 만족하는 경우, 삭제 작업을 활성화할 수 있습니다.

수동 구축에서 또는 탭 모드의 인라인 구축에서, 시스템은 삭제 작업에 관계없이 트래픽에 영향을 줄 수 없습니다. 수동 구축에서 **Drop and Generate Events(**이벤트 삭제 및 생성**)** 으로 설정된 규칙은 **Generate Events(**이벤트 생성**)**으로 설정된 규칙과 동일하게 작동합니다. 시스템은 침입 이벤트를 생성하지만 패킷을 삭제할 수는 없습니다.

참고 파일 Block(차단) 작업으로 인해 패킷에 대해 Block(차단) 또는 Pending(보류 중) 파일 정책이 판정되고 나중에 동일한 패킷에서 IPS 이벤트가 생성된다고 가정합니다. 이 경우 IPS 이벤트는 IPS 정책이 탐지 모드(IDS)에 있는 경우에도 Would have dropped(삭제되었을 것임) 대신 Dropped(삭제됨)로 표시됩니다.

참고 FTP를 통한 악성코드의 전송을 차단하려면 악성코드 대응 를 올바르게 구성하는 것은 물론 액세스 제어 정책의 기본 침입 정책에서 **Drop when Inline(**인라인 시 삭제**)**을 활성화해야 합니다.

침입 이벤트를 볼 때, 워크플로는 인라인 결과를 포함할 수 있는데, 이는 트래픽이 실제로 삭제되었는지 여부 또는 단지 트래픽이 삭제되었을 가능성이 있는지 여부를 나타냅니다.

인라인 배포에서 삭제 작업 설정하기

프로시저

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

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

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

단계 **3** 정책의 삭제 작업을 설정합니다.

- 침입 규칙이 트래픽에 영향을 미치고 이벤트를 생성할 수 있게 하려면 **Drop When Inline(**인라인 시 삭제**)** 확인란을 선택합니다.
- 이벤트는 계속 생성하면서 침입 규칙이 트래픽에 영향을 미치지 못하도록 하려면 **Drop when Inline(**인라인 시 삭제**)** 확인란 선택을 취소합니다.

단계 **4** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

이중 시스템 구축의 삭제 작업

네트워크에 직접 연결된 두 시스템이 있는 경우, 첫 번째 시스템이 이벤트를 삭제하고 두 번째 시스템에서 삭제 또는 "would have dropped(삭제했을)" 이벤트를 기록하는 것은 정상입니다. 첫 번째 시스템은 파일의 마지막 패킷을 스캔할 때까지 패킷을 삭제하기로 결정하고, 두 번째 시스템 역시 트래픽을 검사하고 트래픽을 "to be dropped(삭제될)" 트래픽으로 식별합니다.

예를 들어 첫 번째 패킷이 규칙을 트리거하는 5패킷 HTTP GET 요청은 첫 번째 시스템에 의해 차단되고 마지막 패킷만 삭제됩니다. 두 번째 시스템은 4패킷만 수신하고 연결은 삭제되지만 두 번째 시스템은 세션을 잘라내는 동안 최종적으로 부분적 GET 요청을 플러싱할 때 인라인 결과와 동일한 "would have dropped(삭제했을)"가 있는 규칙을 트리거합니다.

침입 정책 고급 설정

침입 정책의 고급 설정을 구성하려면 특정한 전문성이 필요합니다. 침입 정책에 대한 기본 정책은 기본적으로 활성화되는 고급 설정 및 각각에 대한 기본 구성을 결정합니다.

침입 정책의 탐색 패널에 있는 **Advanced Settings(**고급 설정**)**를 선택하는 경우, 정책은 유형별 고급 설정을 나열합니다. Advanced Settings(고급 설정) 페이지에서 침입 정책의 고급 설정을 활성화하거나 비활성화할 수 있으며, 고급 설정 구성 페이지에 액세스할 수도 있습니다. 고급 설정은 구성할 수 있도록 활성화되어 있어야 합니다.

고급 설정을 비활성화하면 하위 링크 및 **Edit(**수정**)** 링크는 더 이상 표시되지 않지만, 구성은 유지됩니다. 일부 침입 정책 구성(침입 규칙에 대한 중요한 데이터 규칙, SNMP 경고)은 활성화되고 고급 설정을 정확하게 구성해야 합니다.

고급 설정에서 구성을 수정하는 데는 수정하고 있는 구성과 네트워크에 미칠 잠재적 영향에 대한 이해가 필요합니다.

특정 위협 탐지

중요한 데이터 전처리기는 신용 카드 번호 및 ASCII 문자로 표시된 Social Security numbers(사회 보장 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 전처리기는 네트워크 분석 정책에서 구성됩니다.

침입 규칙 임계값

전역 규칙 임계값은 임계값을 사용하여 시스템이 로깅하고 침입 이벤트를 표시하는 횟수를 제한할 수 있도록 하여 많은 이벤트로 인해 시스템이 마비되는 것을 방지합니다.

외부 응답

웹 인터페이스 내의 다양한 침입 이벤트 보기 외에도 시스템 로그(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.

관련 항목

민감한 데이터 탐지 기본 사항
전역 규칙 임계값 기본 사항

침입 탐지 및 방지에 대한 성능 최적화

Firepower System이 침입 탐지 및 방지를 수행하도록 하되 검색 데이터를 활용할 필요가 없는 경우, 아래 설명처럼 새 검색을 비활성화하여 성능을 최적화할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 다음 사용자 역할 중 하나를 보유해야 합니다.

- 액세스 제어를 위한 관리자, 액세스 관리자 또는 네트워크 관리자
- 네트워크 검색을 위한 관리자 또는 검색 관리자

프로시저

단계 **1** 대상 디바이스에 구축된 액세스 제어 정책과 연결된 규칙을 수정하거나 삭제합니다. 해당 디바이스에 연결된 액세스 규칙에는 사용자, 애플리케이션 또는 URL 조건이 있을 수 없습니다(액세스 제어 규칙 생성 및 수정 참조).

단계 **2** 대상 디바이스의 네트워크 검색 정책에서 모든 규칙을 삭제합니다(네트워크 검색 규칙 구성 참조).

단계 **3** 변경된 구성을 대상 디바이스에 구축합니다(구성 변경 사항 구축 참조).