침입 및 네트워크 분석 정책의 레이어

다음 주제에서는 침입 및 네트워크 분석 정책에서 레이어를 사용하는 방법을 설명합니다.

레이어 기본 사항

관리되는 디바이스가 많은 좀 더 큰 조직에는 여러 부서, 사업부 또는 경우에 따라 여러 회사의 고유한 요구를 지원하기 위한 다수의 침입 정책 및 네트워크 분석 정책이 있을 수 있습니다. 두 정책 유형의 구성은 여러 정책을 효율적으로 관리하기 위해 사용할 수 있는 레이어라는 구성 요소에 포함됩니다.

침입 및 네트워크 분석 정책의 레이어는 기본적으로 동일한 방식으로 작동합니다. 의식적으로 레이어를 사용하지 않고 각 정책 유형을 만들고 수정할 수 있습니다. 정책 구성을 수정할 수 있으며, 정책에 사용자 레이어를 추가하지 않은 경우 시스템은 초기 이름이 *My Changes(*내 변경 사항*)*인 구성 가능한 단일 레이어에 변경 사항을 자동으로 포함합니다. 또한, 최대 200개의 레이어를 추가할 수 있으며 이러한 레이어에서 설정의 조합을 구성할 수도 있습니다. 사용자 레이어를 복사, 병합, 이동 및 삭제할 수 있으며 가장 중요한 기능으로는 개별 사용자 레이어를 동일한 유형의 다른 정책과 공유할 수 있다는 점입니다.

네트워크 분석 및 침입 정책 레이어를 위한 라이선스 요건

Threat Defense 라이선스

IPS

기본 라이선스

보호

네트워크 분석 및 침입 정책 레이어에 대한 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 침입 관리자

레이어 스택

레이어 스택은 다음으로 구성됩니다.

사용자 레이어

사용자가 구성 가능한 레이어입니다. 사용자 구성 가능한 레이어를 복사, 병합, 이동 또는 삭제할 수 있으며, 사용자 구성 가능한 모든 레이어를 동일한 유형의 다른 정책과 공유할 수 있습니다. 이 레이어에는 처음에 My Changes라는 이름이 지정되는 자동 생성된 레이어가 포함됩니다.

기본 제공 레이어

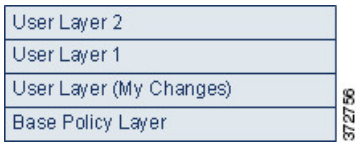
읽기 전용 기본 정책 레이어입니다. 이 레이어의 정책은 시스템 제공 정책 또는 사용자가 생성하는 맞춤형 정책일 수 있습니다.

기본적으로 네트워크 분석 또는 침입 정책에는 기본 정책 레이어 및 My Changes 레이어가 포함됩니다. 필요에 따라 사용자 레이어를 추가할 수 있습니다.

각 정책 레이어에는 네트워크 분석 정책의 모든 프리프로세서에 대한 또는 침입 정책의 모든 침입 규칙 및 고급 설정에 대한 완전한 구성이 포함되어 있습니다. 최하위 기반 정책 레이어에는 정책 생성 시 선택한 기반 정책의 모든 설정이 포함되어 있습니다. 상위 레이어의 설정이 하위 레이어의 동일한 설정에 비해 우선권을 갖습니다. 레이어에 명시적으로 설정되지 않은 기능은 명시적으로 설정된 다음 최상위 레이어에서 설정을 상속합니다. 시스템은 레이어를 병합합니다. 즉, 네트워크 트래픽을 처리할 때 모든 설정의 누적된 효과만 적용합니다.

팁 전적으로 기반 정책의 기본 설정에 기반하는 침입 또는 네트워크 분석 정책을 생성할 수 있습니다. 침입 정책의 경우에는 모니터링되는 네트워크의 특정 요구 사항에 맞게 침입 정책을 조정하려는 경우, Firepower 규칙 상태 권장 사항을 사용할 수도 있습니다.

다음 그림은 레이어 스택의 예를 보여줍니다. 여기에는 기본 정책 레이어 및 초기 My Changes 레이어 외에 두 개의 사용자 구성 가능한 레이어인 *User Layer 1* 및 *User Layer 2*가 포함되어 있습니다. 이 그림에서, 추가하는 사용자 구성 가능한 각 레이어는 처음에 스택의 최상위 레이어에 배치됩니다. 따라서 그림의 User Layer 2는 스택에서 가장 마지막에 추가된 것이며 최상위 레이어입니다.



규칙 업데이트가 정책을 수정하도록 허용하는지와 상관없이, 규칙 업데이트의 변경 사항은 레이어에서 사용자가 수행한 변경 사항을 재정의하지 않습니다. 이는 규칙 업데이트의 변경 사항이 기반 정책에서 이루어지며, 이것이 기반 정책 레이어의 기본 설정을 결정하기 때문입니다. 사용자 변경 사항은 항상 상위 레이어에서 이루어지므로, 규칙 업데이트가 기반 정책에 대해 수행하는 모든 변경 사항을 재정의합니다.

기본 레이어

침입 또는 네트워크 분석 정책의 기반 레이어(기반 정책이라고도 함)는 정책의 모든 구성에 대한 기본 설정을 정의하며 정책에서 최하위 레이어입니다. 새 정책을 생성할 때 새 레이어를 추가하지 않은 채 설정을 변경하면 변경 사항은 My Changes(내 변경 사항) 레이어에 저장되며 기반 정책의 설정을 재정의합니다(그러나 변경하지는 않음).

시스템 제공 기반 정책

Firepower System은 여러 쌍의 네트워크 분석 정책과 침입 정책을 제공합니다. 시스템이 제공하는 네트워크 분석 및 침입 정책을 사용하여 Talos 인텔리전스 그룹의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 전처리기 규칙 상태뿐 아니라 전처리기의 초기 구성과 기타 고급 설정을 제공합니다. 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다.

시스템이 제공하는 정책을 기반으로 사용할 경우, 규칙 업데이트를 가져오면 기반 정책의 설정을 수정할 수 있습니다. 하지만 시스템이 시스템 제공 기반 정책을 자동으로 변경하지 않도록 맞춤형 정책을 구성할 수 있습니다. 이를 통해 규칙 업데이트와는 별개의 일정에 따라 시스템 제공 기본 정책을 수동으로 업데이트할 수 있습니다. 어떤 경우든, 규칙 업데이트가 기반 정책에 대해 수행하는 변경 사항은 My Changes(내 변경 사항) 또는 다른 레이어의 설정을 변경하거나 재정의하지 않습니다.

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.

맞춤형 기본 정책

맞춤형 정책을 기반으로 사용할 수 있습니다. 사용자 지정 정책의 설정을 조정하여 가장 중요하다고 생각되는 방식으로 트래픽을 검사할 수 있으며, 이에 따라 관리되는 디바이스의 성능과 디바이스가 생성하는 이벤트에 효과적으로 대응하는 능력 모두를 향상시킬 수 있습니다.

다른 정책의 기반으로 사용하는 맞춤형 정책을 변경하면 해당 변경 사항은 기반을 사용하는 정책의 기본 설정으로 자동으로 사용됩니다.

또한 모든 정책에는 정책 체인의 궁극적인 기반으로 시스템 제공 정책이 있기 때문에 맞춤형 기본 정책을 사용하는 경우에도 규칙 업데이트가 정책에 영향을 미칠 수 있습니다. 체인 내 첫 번째 사용자 지정 정책(시스템이 제공하는 정책을 기본으로 사용하는 것)은 규칙 업데이트가 해당 기본 정책을 수정하는 것을 허용하며, 사용자 정책에도 영향을 줄 수 있습니다.

기본 정책을 변경하는 방법에 상관없이(규칙 업데이트로 변경하거나 기본 정책으로 사용하는 맞춤형 정책을 수정하면서 변경하거나) 이러한 변경은 My Changes 또는 다른 레이어의 설정을 변경하거나 재정의하지 않습니다.

규칙 업데이트가 기본 정책에 미치는 영향

규칙 업데이트를 가져올 때 시스템은 시스템에서 제공한 침입, 액세스 제어, 네트워크 분석 정책을 수정합니다. 규칙 업데이트에는 다음이 포함될 수 있습니다.

- 수정된 네트워크 분석 전처리기 설정
- 침입 및 액세스 제어 정책의 수정된 고급 설정
- 신규 및 업데이트된 침입 규칙
- 기존 규칙의 수정된 상태
- 새 규칙 카테고리와 기본 변수

규칙 업데이트는 시스템 제공 정책에서 기존 규칙을 삭제할 수도 있습니다.

기본 변수 및 규칙 카테고리를 변경하면 시스템 수준에서 처리됩니다.

시스템 제공 정책을 침입 또는 네트워크 분석 기본 정책으로 사용하는 경우, 규칙 업데이트가 기본 정책(이 경우, 시스템 제공 정책의 복사본)을 수정하도록 허용할 수 있습니다. 규칙 업데이트가 기본 정책을 업데이트하는 것을 허용할 경우, 새로운 규칙 업데이트는 기본 정책으로 사용하는 시스템 제공 정책에 대한 변경 사항과 동일하게 기본 정책을 변경합니다. 해당 설정을 수정하지 않은 경우 기반 정책의 설정이 현재 정책의 설정을 결정합니다. 그러나 규칙 업데이트는 현재 정책에서 수행하는 변경 사항을 재정의하지 않습니다.

규칙 업데이트가 기본 정책을 수정하도록 허용하지 않는 경우, 하나 이상의 규칙 업데이트를 가져온 후 기본 정책을 수동으로 업데이트할 수 있습니다.

침입 정책의 규칙 상태와 상관없이 또는 규칙 업데이트가 기본 침입 정책을 업데이트하도록 허용하는지 여부와 상관없이, 규칙 업데이트는 Talos가 삭제하는 침입 규칙을 항상 삭제합니다.

변경 사항을 네트워크 트래픽에 다시 구축할 때까지 현재 구축된 침입 정책의 규칙은 다음과 같이 작동합니다.

- 비활성화된 침입 규칙은 비활성화 상태를 유지합니다.
- **Generate Events(**이벤트 생성**)**로 설정된 규칙은 트리거될 때 계속해서 이벤트를 생성합니다.
- **Drop and Generate Events(**이벤트 삭제 및 생성**)**로 설정된 규칙은 트리거될 때 계속해서 이벤트를 생성하고 위반 패킷을 삭제합니다.

규칙 업데이트는 다음 조건이 모두 충족되지 않으면 사용자 지정 기본 정책을 수정하지 않습니다.

- 규칙 업데이트를 통해 상위 정책의 시스템이 제공하는 기본 정책, 즉 사용자 지정 기본 정책을 생성한 정책을 수정할 수 있습니다.
- 상위 기본 정책 내 해당 설정을 대체하는 상위 정책을 변경하지 않았습니다.

두 조건이 충족된 경우, 상위 정책을 저장하면 규칙 업데이트 내 변경 사항이 하위 정책, 즉, 사용자 지정 기본 정책을 사용하는 정책에 전달됩니다.

예를 들어 규칙 업데이트가 이전에 비활성화된 침입 규칙을 활성화하여 상위 침입 정책의 규칙 상태를 수정하지 않은 경우, 상위 정책을 저장하면 수정된 규칙 상태가 기반 정책에 전달됩니다.

마찬가지로, 규칙 업데이트가 기본 프리프로세서 설정을 수정하고 상위 네트워크 분석 정책에서 설정을 수정하지 않은 경우, 상위 정책을 저장하면 수정된 설정이 기반 정책에 전달됩니다.

기반 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**)** > **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** 필요한 침입 정책 행에서 **Edit(**수정**)** ( )을(를) 클릭합니다.

단계 **4** **Base Policy(**기본 정책**)** 드롭다운 목록에서 기본 정책을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책

Cisco 추천 레이어

침입 정책에서 규칙 상태 권장 사항을 생성할 때 권장 사항을 기반으로 규칙 상태를 자동으로 수정할지 여부를 선택할 수 있습니다.

다음 그림에서 보듯 권장 규칙 상태를 사용하면 읽기 전용 기본 제공 Cisco 레이어가 기반 레이어 바로 위에 삽입됩니다.

이 레이어는 침입 정책에 고유합니다.

나중에 권장 규칙 상태를 사용하지 않기로 선택하면 시스템은 Cisco 레이어를 제거합니다. 이 레이어는 수동으로 삭제할 수 없지만 권장 규칙 상태의 사용 여부를 선택하여 추가하고 삭제할 수 있습니다.

Cisco Recommendations 레이어를 추가하면 탐색 패널의 Policy Layers(정책 레이어) 아래에 Cisco Recommendations 링크가 추가됩니다. 이 링크를 클릭하면 Cisco Recommendations 레이어 페이지의 읽기 전용 보기가 나타납니다. 여기에서 Rules(규칙) 페이지의 권장 사항으로 필터링된 보기에 읽기 전용 모드로 액세스할 수 있습니다.

권장 규칙 상태를 사용하면 탐색 패널의 Cisco Recommendations 링크 아래에 Rules(규칙) 하위 링크도 추가됩니다. Rules(규칙) 하위 링크를 클릭하면 Cisco Recommendations 레이어에서 Rules(규칙) 페이지의 읽기 전용 표시에 액세스할 수 있습니다. 이 보기에서 다음에 유의하십시오.

- 상태 열에 규칙 상태 아이콘이 없으면 해당 상태는 기본 정책에서 상속된 것입니다.
- 이 보기 또는 다른 Rules(규칙) 페이지 보기의 Cisco Recommendations 열에 규칙 상태 아이콘이 없으면 이 규칙에 대한 권장 사항이 없는 것입니다.

관련 항목

네트워크 자산에 대한 침입 방지 맞춤화

레이어 관리

Policy Layers(정책 레이어) 페이지는 네트워크 분석 또는 침입 정책에 대한 완전한 레이어 스택을 요약하는 단일 페이지를 제공합니다. 이 페이지에서 공유 및 비공유 레이어를 추가하고, 레이어를 복사, 병합, 이동 및 삭제하고, 각 레이어의 요약 페이지에 액세스하고, 각 레이어 내에서 활성화, 비활성화 및 재정의된 구성에 대한 구성 페이지에 액세스할 수 있습니다.

각 레이어에 대해 다음 정보를 볼 수 있습니다.

- 레이어가 기본 제공 레이어인지, 공유된 사용자 레이어인지, 공유되지 않은 사용자 레이어인지 여부
- 가장 높은(효과적인) 프리프로세서 또는 고급 설정 구성이 포함되어 있는 레이어(기능 이름별)
- 침입 정책에서, 상태가 레이어에 설정되어 있고 각 규칙 상태에 대해 규칙 수가 설정된 침입 규칙의 수

Policy Layers(정책 레이어) 페이지는 또한 활성화된 모든 전처리기(네트워크 분석) 또는 고급 설정(침입), 침입 정책, 침입 규칙의 최종 효과에 대한 요약을 제공합니다.

각 레이어의 요약에 있는 기능 이름은 어떤 구성이 레이어에서 활성화, 비활성화, 재정의 또는 상속되었는지를 다음과 같이 나타냅니다.

기능 상태	기능 이름
레이어에서 활성화됨	일반 텍스트로 작성됨
레이어에서 비활성화됨	삭제됨
상위 레이어에서 구성에 의해 대체됨	기울임 꼴 텍스트로 작성됨
하위 레이어에서 상속됨	없음

네트워크 분석 또는 침입 정책에 최대 200개의 레이어를 추가할 수 있습니다. 레이어를 추가하면 정책에서 최상위 레이어로 나타납니다. 초기 상태는 모든 기능에 대한 Inherit(상속) 상태이며, 침입 정책에 이벤트 필터링, 동적 상태 또는 알림 규칙 작업이 설정되어 있지 않습니다.

레이어를 정책에 추가할 때 사용자 구성 가능한 레이어에 고유한 이름을 지정합니다. 나중에 이름을 변경할 수 있으며, 원하는 경우, 레이어를 수정할 때 표시되는 설명을 추가하거나 수정할 수 있습니다.

레이어를 복사하거나 User Layers(사용자 레이어) 페이지 영역 내에서 레이어를 위 또는 아래로 이동하거나 초기 My Changes 레이어를 포함한 사용자 레이어를 삭제할 수 있습니다. 다음과 같은 고려 사항을 참고하십시오,

- 레이어를 복사하면 복사본이 최상위 레이어로 나타납니다.
- 공유 레이어를 복사하면 처음에는 공유되지 않고 나중에 원하는 경우 공유할 수 있는 레이어가 생성됩니다.
- 공유 레이어는 삭제할 수 없습니다. 공유가 활성화되었지만 다른 정책과 공유되지 않은 레이어는 공유 레이어가 아닙니다.

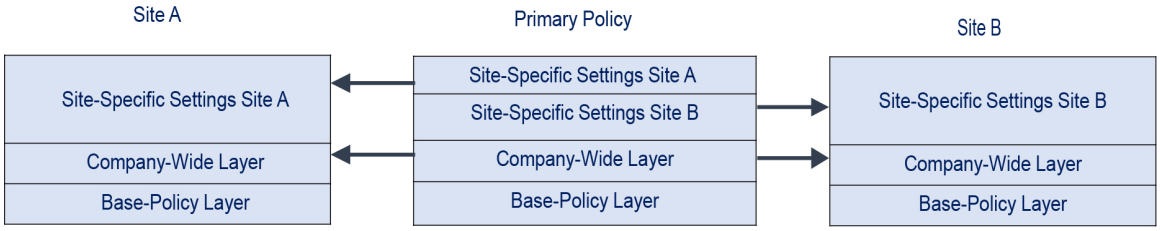
사용자 구성 가능 레이어를 바로 아래의 다른 사용자 구성 가능 레이어와 병합할 수 있습니다. 병합된 레이어는 각 레이어의 고유한 설정을 모두 보유하며, 두 레이어 모두 동일한 프리프로세서에 대한 설정, 침입 규칙 또는 고급 설정을 포함한 경우 상위 레이어의 설정을 수용합니다. 병합된 레이어는 하위 레이어의 이름을 유지합니다. 다른 정책에 추가할 수 있는 공유 가능 레이어를 생성하는 정책에서 공유 가능 레이어 바로 위의 비공유 레이어는 공유 가능 레이어와 병합할 수 있지만 공유 가능 레이어를 아래 있는 비공유 레이어와 병합할 수 없습니다. 또 다른 정책에서 생성한 공유 레이어를 추가하는 정책에서는 공유 레이어를 바로 아래에 있는 비공유 레이어와 병합할 수 있으며 이 경우 그

결과 레이어는 더 이상 공유되지 않습니다. 비공유 레이어는 그 아래에 있는 공유 레이어와 병합할 수 없습니다.

공유 레이어

공유 레이어는 공유를 허용하는 다른 정책에서 레이어를 생성한 후 정책에 추가 하는 레이어입니다. 공유 가능 레이어는 공유를 허용하는 레이어입니다.

다음 그림은 전사적 레이어와 사이트 A 및 B를 위한 사이트별 레이어를 생성하고 이를 공유하도록 허용하는 기본 정책의 예를 보여줍니다. 그런 다음 이를 사이트 A 및 B에 대한 정책에 공유 레이어로 추가합니다.



기본 정책의 전사적 레이어에는 사이트 A와 B에 적용할 수 있는 설정이 포함됩니다. 사이트별 레이어에는 각 사이트에 한정된 설정이 포함됩니다. 예를 들어 네트워크 분석 정책의 경우 Site A(사이트 A)에는 모니터링되는 네트워크에 웹 서버가 없을 수 있으며 HTTP Inspect 프리프로세서의 보호 또는 처리 오버헤드가 필요하지 않을 수 있지만, 두 사이트에 모두 TCP 스트림 전처리가 필요할 수 있습니다. 두 사이트 모두와 공유하는 전사적 레이어에서 TCP 스트림 프로세싱을 활성화할 수 있고, Site A(사이트 A)와 공유하는 사이트별 레이어에서 HTTP Inspect 프리프로세서를 비활성화할 수도 있으며, Site B(사이트 B)와 공유하는 사이트별 레이어에서 HTTP Inspect 프리프로세서를 활성화할 수도 있습니다. 또한 구성 조정에 필요한 경우 사이트별 정책의 상위 레이어에서 구성을 수정하여 각 사이트에 대한 정책을 추가적으로 조정할 수도 있습니다.

기본 정책 예에서 합병된 최종 설정이 트래픽 모니터링에 유용할 것이라고 말할 수는 없지만, 사이트별 정책의 구성 및 업데이트에서 절약되는 시간을 고려하면 정책 레이어를 유용하게 응용하는 예라고 할 수 있습니다.

다른 많은 레이어 구성도 가능합니다. 예를 들어 회사, 부서, 네트워크, 심지어 사용자 단위로도 정책 레이어를 정의할 수 있습니다. 침입 정책의 경우 한 레이어에는 고급 설정을 포함하고 다른 레이어에는 규칙 설정을 포함할 수도 있습니다.

사용자 구성 가능한 레이어를 동일한 유형의 다른 정책(침입 또는 네트워크 분석)과 공유할 수 있습니다. 공유 가능 레이어 내에서 구성을 수정한 다음 변경 사항을 커밋하면 시스템은 레이어를 공유하는 모든 정책을 업데이트하고 영향을 받는 모든 정책의 목록을 제공합니다. 레이어를 생성한 정책에 있는 기능 구성만 변경할 수 있습니다.

다른 정책에서 추가한 레이어에 대해서는 공유를 비활성화할 수 없습니다. 먼저 다른 정책에서 레이어를 삭제하거나 다른 정책을 삭제해야 합니다.

공유하고자 하는 레이어가 생성된 사용자 지정 정책이 기본 정책인 경우 정책에 공유 레이어를 추가할 수 없습니다. 이렇게 하면 정책에 순환 종속성이 부여됩니다.

다중 도메인 구축에서는 상위 정책의 공유 레이어를 하위 도메인의 정책에 추가할 수 있습니다.

레이어 관리

프로시저

단계 **1** Snort 2 정책을 편집하는 동안 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다.

단계 **2** Policy Layers(정책 레이어) 페이지에서 다음 관리 작업을 수행할 수 있습니다.

- 다른 정책에서 공유 레이어 추가 - User Layers(사용자 레이어) 옆에 있는 **Add Shared Layer(**공유 레이어 추가**) Add(**추가**)** (+)을 클릭하고 **Add Shared Layer(**공유 레이어 추가**)** 드롭다운 목록에서 레이어를 선택한 다음 **OK(**확인**)**를 클릭합니다.
- 비공유 레이어 추가 - User Layers(사용자 레이어) 옆에 있는 Add Layer(레이어 추가) 아이콘(**Add(**추가**)** (+))을 클릭하고 **Name(**이름**)**을 입력한 다음 **OK(**확인**)**를 클릭합니다.
- 레이어 설명 추가 또는 변경 - 레이어 옆에 있는 **Edit(**수정**)** (✎)을 클릭한 다음 **Description(**설명**)**을 추가하거나 변경합니다.
- 레이어를 다른 정책과 공유하도록 허용 - 레이어 옆에 있는 **Edit(**수정**)** (✎)을 클릭한 다음 **Sharing(**공유**)** 확인란의 선택을 취소합니다.
- 레이어 이름 변경 - 레이어 옆에 있는 **Edit(**수정**)** (✎)을 클릭한 다음 **Name(**이름**)**을 변경합니다.
- 레이어 복사 - 레이어의 **Copy(**복사**)** (⧉)를 클릭합니다.
- 레이어 삭제 - 레이어의 **Delete(**삭제**)** (🗑)를 클릭한 다음 **OK(**확인**)**를 클릭합니다.
- 두 레이어 병합 - 두 레이어 중 위 레이어의 **Merge(**병합**)** (⧉)를 클릭한 다음**OK(**확인**)**를 클릭합니다.
- 레이어 이동 - 레이어 요약에서 빈 영역을 클릭하고 위치 화살표가 레이어를 이동하려는 레이어 위나 아래에 있는 선을 가리킬 때까지 끕니다.

단계 **3** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 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

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책

레이어 탐색

프로시저

단계 **1** Snort 2 정책을 편집하는 동안 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다. Snort 2 정책에 액세스하려면 **Policies(**정책**)** > **Intrusion(**침입**)** > **Intrusion Policies(**침입 정책**)** 탭을 선택한 다음 편집하려는 정책에 대해 **Snort 2**를 클릭합니다.

단계 **2** 다음 작업을 수행하여 레이어 간에 이동할 수 있습니다.

- 전처리기 또는 고급 설정 페이지에 액세스 - 레이어 수준 전처리기 또는 고급 설정 구성 페이지에 액세스하려면 해당 레이어 행에서 기능 이름을 클릭합니다. 구성 페이지는 기본 정책 및 공유 레이어에 있는 읽기 전용 페이지입니다.
- 규칙 페이지 액세스 - 규칙 상태 유형으로 필터링된 레이어 수준 규칙 설정 페이지에 액세스하려면 레이어 요약에서 **Drop and Generate Events(**이벤트 삭제 및 생성**)**, **Generate Events(**이벤트 생성**)** 또는 **Disabled(**비활성화**)**를 클릭합니다. 선택한 규칙 상태로 설정된 규칙이 레이어에 포함되지 않는 경우 규칙이 표시되지 않습니다.
- Policy Information(정책 정보) 페이지 표시 - Policy Information(정책 정보) 페이지를 표시 하려면 탐색 패널에서 **Policy Summary(**정책 요약**)**를 클릭합니다.
- 레이어 요약 페이지 표시 - 레이어 요약 페이지를 표시하려면 레이어 행에서 레이어 이름을 클릭하거나 사용자 레이어 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. 공유 레이어에 대한 읽기 전용 요약 페이지에 액세스하려면 **View(**보기**)** ( )를 클릭할 수도 있습니다.

단계 **3** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 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

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책

레이어 내 침입 규칙

레이어에 대한 Rules(규칙) 페이지에서 개별 레이어 설정을 볼 수도 있고, Rules(규칙) 페이지의 정책 보기에서 모든 설정의 최종 효과를 볼 수도 있습니다. Rules(규칙) 페이지의 정책 보기에서 규칙 설정을 수정할 경우 정책에서 사용자 구성 가능한 최상위 레이어를 수정하게 됩니다. Rules(규칙) 페이지의 레이어 드롭다운 목록을 사용하여 다른 레이어로 전환할 수 있습니다.

다음 표에서는 여러 레이어에서 동일한 설정 유형을 구성하는 효과에 대해 설명합니다.

표 *1:* 레이어 규칙 설정

설정 수	설정 유형	목적
하나	규칙 상태	하위 레이어의 규칙에 대해 설정된 규칙 상태를 재정의하고, 하위 레이어에서 구성된 해당 규칙에 대한 모든 임계값, 억제, 등급 기반 규칙 상태 및 알림을 무시합니다. 규칙이 기반 정책 또는 하위 레이어에서 상태를 상속하도록 하려면 규칙 상태를 Inherit(상속)로 설정합니다. 침입 정책 Rules(규칙) 페이지에서 작업하는 경우, 침입 정책 Rules(규칙) 페이지는 모든 규칙 설정의 기본 효과의 중첩 보기이기 때문에 규칙 상태를 Inherit(상속)로 설정할 수 없습니다.
하나	임계값 SNMP 알림	하단 레이어의 규칙에 대해 동일한 유형의 설정을 무시합니다. 임계값을 설정하여 레이어에서 규칙에 대한 기존 임계값을 모두 덮어쓴다는 점을 참고하십시오.
하나 이상	억제등급 기반 규칙 상태	규칙 상태가 설정되어 있는 첫 번째 레이어까지 각각의 선택한 규칙에 대한 동일한 유형의 설정을 중첩적으로 결합합니다. 규칙 상태가 설정되어 있는 레이어 아래의 설정은 무시됩니다.
하나 이상	코멘트	규칙에 코멘트를 추가합니다. 코멘트는 정책이나 레이어별이 아니라 규칙별로 추가됩니다. 모든 레이어의 규칙에 하나 이상의 코멘트를 추가할 수 있습니다.

예를 들어, 규칙 상태를 한 레이어에서는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정하고 상위 레이어에서는 Disabled(비활성화)로 설정할 경우, 침입 정책 Rules(규칙) 페이지는 규칙이 비활성화되었음을 나타냅니다.

다른 예로, 한 레이어에서는 규칙에 대한 소스 기반 삭제를 192.168.1.1로 설정하고, 다른 레이어에서는 규칙에 대한 대상 기반 삭제를 192.168.1.2로 설정하는 경우, Rules(규칙) 페이지는 소스 주소 192.168.1.1 및 대상 주소 192.168.1.2에 대한 이벤트를 삭제하는 것이 중첩 효과임을 보여줍니다. 억제 및 등급 기반 규칙 상태 설정은 선택한 각 규칙에 대해 동일한 유형의 설정을 규칙에 대해 규칙 상태가 설정된 첫 번째 레이어까지 아래로 누적 결합합니다. 규칙 상태가 설정되어 있는 레이어 아래의 설정은 무시됩니다.

특정 레이어의 각 Rules(규칙) 페이지에서 색상 구분은 다음과 같이 유효 상태가 상위 레이어, 하위 레이어 또는 현재 레이어 중 어디에 있는지 나타냅니다.

- 빨간색 - 유효 상태가 상위 레이어에 있습니다
- 노란색 - 유효 상태가 하위 레이어에 있습니다
- 음영 처리되지 않음 - 유효 상태가 현재 레이어에 있습니다

침입 정책 Rules(규칙) 페이지는 모든 규칙 설정의 기본 효과에 대한 중첩 보기이므로, 규칙 상태는 이 페이지에서 색으로 지정되지 않습니다.

레이어에서 침입 규칙 구성

침입 정책에서 사용자 구성 가능한 레이어의 규칙에 대해 규칙 상태, 이벤트 필터링, 동적 상태, 알림, 규칙 코멘트를 설정할 수 있습니다. 변경하려는 레이어에 액세스한 후 침입 정책 Rules(규칙) 페이지에서 하듯 레이어에 대한 Rules(규칙) 페이지에서 설정을 추가합니다.

프로시저

단계 **1** Snort 2 침입 정책을 편집하는 동안 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 확장합니다.

단계 **2** 수정할 정책 레이어를 확장합니다.

단계 **3** 수정할 정책 레이어 바로 아래에 있는 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 규칙을 사용하여 침입 정책 조정에서 설명하는 설정을 수정합니다.

팁 수정 가능한 레이어에서 개별 설정을 삭제하려면 레이어의 Rules(규칙) 페이지에서 규칙 메시지를 두 번 클릭하여 규칙 세부 정보를 표시합니다. 삭제할 설정 옆에 있는 **Delete**를 클릭한 다음 **OK**를 두 번 클릭합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 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

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책

다중 레이어에서 규칙 설정 제거

침입 정책의 여러 레이어에서 특정 유형의 이벤트 필터, 동적 상태 또는 알림을 동시에 제거할 수 있습니다. 시스템은 선택한 설정을 제거하고 정책에서 수정 가능한 최고 레이어에 규칙에 대한 나머지 설정을 복사합니다.

시스템은 모든 설정을 제거하거나 규칙 상태가 설정되어 있는 레이어를 발견할 때까지 설정된 각 레이어를 통해 설정 유형을 아래로 제거합니다. 후자의 경우, 시스템은 해당 레이어에서 설정을 제거하고 설정 유형 제거를 중지합니다.

시스템이 기본 정책 또는 공유 레이어에서 설정 유형을 발견할 때, 그리고 정책 내 최고 레이어가 수정 가능한 경우, 시스템은 규칙에 대한 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어에 복사합니다. 또는 정책 내 최고 레이어가 공유 레이어인 경우, 시스템은 공유 레이어 위에 수정 가능한 새 레이어를 만들고 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어에 복사합니다.

참고 공유 레이어 또는 기본 정책에서 파생된 규칙 설정을 제거하면 하단 레이어 또는 기본 정책에서 이 규칙에 대한 모든 변경이 무시됩니다. 하단 레이어 또는 기본 정책에서 변경 사항 무시를 중지하려면, 최상위 레이어의 요약 페이지에서 규칙 상태를 **Inherit(**상속**)**로 설정합니다.

프로시저

단계 **1** Snort 2 침입 정책을 편집하는 동안 탐색 패널에서 **Policy Information(**정책 정보**)** 바로 아래에 있는 **Rules(**규칙**)**를 클릭합니다. Snort 2 정책에 액세스하려면 **Policies(**정책**)** > **Intrusion(**침입**)** > **Intrusion Policies(**침입 정책**)** 탭을 선택한 다음 편집하려는 정책에 대해 **Snort 2**를 클릭합니다.

팁 또한 레이어의 Rules(규칙) 페이지에 있는 레이어 드롭다운 목록에서 **Policy(**정책**)**를 선택하거나 Policy Information(정책 정보) 페이지에서 **Manage Rules(**규칙 관리**)**를 선택할 수 있습니다.

단계 **2** 여러 설정을 제거할 하나 이상의 규칙을 선택합니다.

- 특정 규칙 선택 - 특정 규칙을 선택하려면 각 규칙 옆에 있는 확인란을 선택합니다.
- 모든 규칙 선택 - 현재 목록에서 모든 규칙을 선택하려면 열 맨위의 확인란을 선택합니다.

단계 **3** 다음 옵션 중 하나를 선택합니다.

- **Event Filtering(**이벤트 필터링**)** > **Remove Thresholds(**임계값 제거**)**
- **Event Filtering(**이벤트 필터링**)** > **Remove Suppressions(**억제 제거**)**
- **Dynamic State(**동적 상태**)** > **Remove Rate-Based Rule States(**등급 기반 상태 제거**)**
- **Alerting(**알림**)** > **Remove SNMP Alerts(SNMP** 알림 제거**)**

참고 공유 레이어 또는 기본 정책에서 파생된 규칙 설정을 제거하면 하단 레이어 또는 기본 정책에서 이 규칙에 대한 모든 변경이 무시됩니다. 하단 레이어 또는 기본 정책에서 변경 사항 무시를 중지하려면, 최상위 레이어의 요약 페이지에서 규칙 상태를 **Inherit(**상속**)**로 설정합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 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

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책

사용자 지정 기본 정책에서 규칙 변경 허용하기

레이어를 추가하지 않은 사용자 지정 네트워크 분석 또는 침입 정책이 다른 사용자 지정 정책을 기본 정책으로 사용할 때, 다음과 같은 경우 해당 규칙 상태를 상속할 규칙을 설정해야 합니다.

- 기본 정책에서 규칙에 설정된 이벤트 필터, 동적 상태 또는 SNMP 알림을 삭제하는 경우 및
- 해당 규칙이 기본 정책으로 사용하는 다른 사용자 지정 정책에서 사용자가 차후에 변경하는 사항을 허용하기를 원하는 경우

프로시저

단계 **1** Snort 2 침입 정책을 편집하는 동안 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 확장합니다.

단계 **2** **My Changes(**내 변경 사항**)**를 확장합니다.

단계 **3** **My Changes(**내 변경 사항**)** 바로 아래에 있는 **Rules(**규칙**)** 링크를 클릭합니다.

단계 **4** 설정을 수용하려는 하나 이상의 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙 선택 - 특정 규칙을 선택하려면 각 규칙 옆에 있는 확인란을 선택합니다.
- 모든 규칙 선택 - 현재 목록에서 모든 규칙을 선택하려면 열 맨위의 확인란을 선택합니다.

단계 **5** **Rule State(**규칙 상태**)** 드롭다운 목록에서 **Inherit(**상속**)**를 선택합니다.

단계 **6** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 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

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책

레이어의 사전 처리기 및 고급 설정

침입 정책의 네트워크 분석 및 고급 설정에서 전처리기를 구성하기 위해 유사한 메커니즘을 사용합니다. 네트워크 분석 Settings(설정) 페이지에서 전처리기 및 침입 정책 Advanced Settings(고급 설정) 페이지에서 침입 정책 고급 설정을 활성화 및 비활성화할 수 있습니다. 이 페이지는 또한 모든 관련 기능에 대한 효과적인 상태의 개요를 제공합니다. 예를 들어, 네트워크 분석 SSL 전처리기가 한 레이어에서 비활성화되고 상위 레이어에서 활성화된 경우 Settings(설정) 페이지에서는 활성화된 것으로 보여줍니다. 이 페이지에서 변경된 사항은 정책의 상단 레이어에 나타납니다. Back Orifice 전처리기에는 사용자 구성 가능한 옵션이 없습니다.

또한 전처리기나 고급 설정을 활성화하거나 비활성화할 수 있으며, 사용자 구성 가능한 레이어에 대한 요약 페이지에서 해당 구성 페이지에 액세스할 수 있습니다. 이 페이지에서 레이어 이름 및 설명을 변경하고 동일한 유형의 다른 정책과 레이어를 공유할지 여부를 구성할 수 있습니다. 탐색 패널에서 **Policy Layers(**정책 레이어**)** 아래 레이어 이름을 선택하여 다른 레이어에 대한 요약 페이지로 전환할 수 있습니다.

전처리기 또는 고급 설정을 활성화하면 탐색 패널에서 레이어 이름 아래에 해당 기능에 대한 구성 페이지에 하위 링크가 나타나고, 레이어에 대한 요약 페이지의 기능 옆에 **Edit(**수정**)** ( )이 나타납니다. 이는 레이어의 기능을 비활성화하거나 Inherit(상속)로 설정하면 사라집니다.

전처리기 또는 고급 설정의 상태(활성화 또는 비활성화)를 설정하면 하단 레이어에서 해당 기능의 상태 및 구성 설정을 무시합니다. 기본 정책 또는 하단 레이어에서 전처리기 또는 고급 설정이 상태와 구성을 상속하는 것을 원하는 경우, 규칙 상태를 **Inherit(**상속**)**로 설정합니다. Settings(설정) 또는 Advanced Settings(고급 설정) 페이지에서 작업하는 경우 Inherit(상속)을 선택할 수 없다는 점에 유의하십시오. 현재 활성화된 기능을 상속하는 경우, 탐색 패널의 하위 링크와 구성 페이지의 수정 아이콘이 더 이상 표시되지 않습니다.

시스템은 기능이 활성화된 가장 높은 레이어에서 구성을 사용합니다. 명시적으로 구성을 수정하지 않은 경우, 시스템은 기본 구성을 사용합니다. 예를 들어, 한 레이어에서 네트워크 분석 DCE/RPC 전처리기를 활성화하고 수정하는 경우, 그리고 상위 레이어에서는 그것을 활성화하지만 변경하지 않는 경우, 시스템은 상위 레이어의 기본 구성을 사용합니다.

각 레이어 요약 페이지에서 색상 구분은 다음과 같이 유효 구성이 상위 레이어, 하단 레이어 또는 현재 레이어 중 어디에 있는지 나타냅니다.

- 빨간색 - 유효한 구성이 상위 레이어에 있음
- 노란색 - 유효한 구성이 하위 레이어에 있음
- 음영 처리되지 않음 - 유효 상태가 현재 레이어에 있음

Settings(설정) 및 Advanced Settings(고급 설정) 페이지는 관련된 모든 설정의 복합적인 보기이므로, 이 페이지는 효과적인 구성의 위치를 나타내는 색상 구분을 사용하지 않습니다.

레이어 내 전처리기 및 고급 설정 구성

프로시저

단계 **1** Snort 2 정책을 편집할 때, 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 확장한 후 수정할 레이어 이름을 클릭합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 레이어 **Name(**이름**)**을 변경합니다.
- **Description(**설명**)**을 추가하거나 변경합니다.
- 다른 정책과 레이어를 공유할 수 있는지 지정하려면 **Sharing(**공유**)** 확인란을 선택하거나 선택 취소합니다.
- 활성화된 전처리기/고급 설정의 구성 페이지에 액세스하려면 **Edit(**수정**)** ( ) 또는 기능 하위 링크를 클릭합니다.

- 현재 레이어에서 전처리기/고급 설정을 비활성화하려면 기능 옆에 있는 **Disabled(**비활성화**)**를 클릭합니다.
- 현재 레이어에서 전처리기/고급 설정을 활성화하려면 기능 옆에 있는 **Enabled(**활성화**)**를 클릭합니다.
- 현재 레이어 아래 최상위 레이어의 설정에서 전처리기/고급 설정 상태 및 구성을 상속하려면 **Inherit(**상속**)**를 클릭합니다.

단계 **3** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 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

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책