액세스 컨트롤 규칙

다음 주제에서는 액세스 제어 규칙을 구성하는 방법을 설명합니다.

액세스 제어 규칙 소개

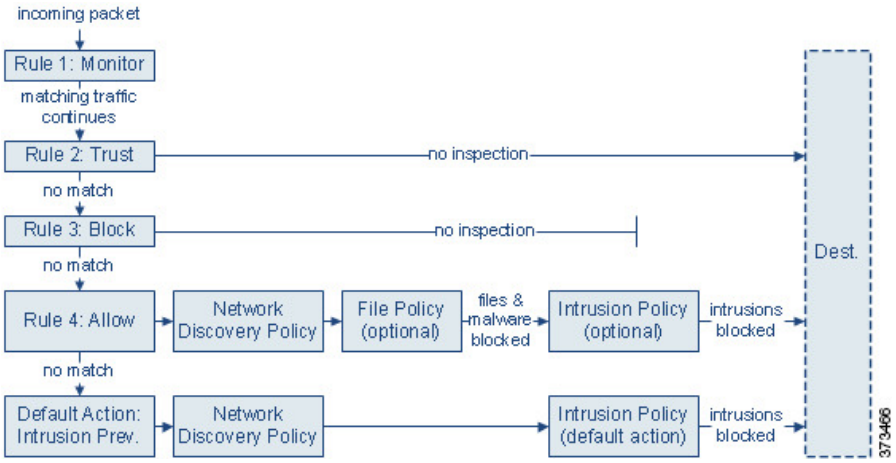
액세스 제어 정책 내에서 액세스 제어 규칙은 여러 매니지드 디바이스에서 네트워크 트래픽을 처리하는 세분화된 방법을 제공합니다.

참고 보안 인텔리전스 필터링, 해독, 사용자 식별, 일부 디코딩 및 전처리는 액세스 제어 규칙이 네트워크 트래픽을 평가하기 전에 수행됩니다.

시스템은 사용자가 지정하는 순서로 액세스 제어 규칙에 트래픽을 일치시킵니다. 대부분의 경우, 시스템은 모든 규칙의 조건이 트래픽과 일치하는 첫 번째 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다.

각 규칙에는 일치하는 트래픽의 모니터링, 신뢰, 차단 또는 허용 여부를 결정하는 작업이 있습니다. 트래픽을 허용하는 경우, 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다.

다음 시나리오에서는 트래픽이 인라인 침입 방지 배포에서 액세스 제어 규칙에 의해 평가될 수 있는 방법을 요약합니다.



이 시나리오에서, 트래픽은 다음과 같이 평가됩니다.

- 규칙 **1:** 모니터링은 가장 먼저 트래픽을 평가합니다. 모니터링 규칙은 네트워크 트래픽을 추적하고 로깅합니다. 시스템은 허용할지 아니면 거부할지 여부를 결정하기 위해 계속해서 트래픽을 추가 규칙에 일치시킵니다. (액세스 제어 규칙 모니터 작업, 7 페이지에서 중요 예외 및 주의 사항을 확인하십시오.)
- 규칙 **2:** 신뢰는 두 번째로 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 목적지로 전달되는 것이 허용되지만 ID 요건과 속도 제한은 계속 적용됩니다. 매칭하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- 규칙 **3:** 차단은 세 번째로 트래픽을 평가합니다. 매칭하는 트래픽은 추가 검사 없이 차단됩니다. 매칭하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- 규칙 **4:** 허용은 마지막 규칙입니다. 이 규칙에서, 일치하는 트래픽은 허용되지만 해당 트래픽 내 금지된 파일, 악성코드, 침입 및 익스플로잇은 탐지 및 차단됩니다. 나머지 금지되지 않은 비악성 트래픽은 목적지까지 허용되지만 ID 요건과 속도 제한은 계속 적용됩니다. 파일 검사나 침입 검사 중 하나만 수행하거나 둘 다 수행하지 않는 허용 규칙을 구성할 수 있습니다.
- 기본 작업은 어느 규칙과도 일치하지 않는 모든 트래픽을 처리합니다. 이 시나리오에서 기본 작업은 비악성 트래픽의 통과를 허용하기 전에 침입 방지를 수행하는 것입니다. 다른 배포에서는 추가 검사 없이 모든 트래픽을 신뢰하거나 차단하는 기본 작업이 있을 수 있습니다. (기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.)

액세스 제어 규칙 또는 기본 작업을 통해 허용되는 트래픽은 자동으로 네트워크 검색 정책에 의한 호스트, 애플리케이션, 사용자 데이터 검사 대상이 됩니다. 검색을 강화 또는 비활성화할 수는 있지만 명시적으로 활성화하지는 마십시오. 그러나 트래픽을 허용한다고 해서 자동으로 검색 데이터 수집이 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에 의해 명시적으로 모니터링되는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다. 또한 암호화된 세션에 대해서는 애플리케이션 검색이 제한됩니다.

암호 해독 구성에서 암호화 트래픽의 통과를 허용하는 경우 또는 암호 해독을 구성하지 않은 경우, 액세스 제어 규칙이 암호화된 트래픽을 처리합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 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.

액세스 제어 규칙 관리

액세스 제어 정책 편집기의 규칙 테이블에서는 현재 정책의 액세스 제어 규칙을 추가, 편집, 분류, 검색, 필터링, 이동, 활성화, 비활성화, 삭제하고 그 밖의 방식으로 관리할 수 있습니다.

액세스 제어 규칙을 올바르게 생성하고 지시하는 것은 복잡한 과제이지만 효율적인 배포 구축에 필수적입니다. 정책을 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이선스를 요구하거나, 잘못된 구성을 포함할 수 있습니다. 시스템이 트래픽을 예상대로 처리하도록 보장하기 위해, 액세스 제어 정책 인터페이스에는 규칙에 대한 강력한 경고 및 오류 피드백 시스템이 있습니다.

검색 표시줄을 사용하여 액세스 제어 정책 규칙 목록을 필터링합니다. **Show Only Matching Rules(**일치하는 규칙만 표시**)** 옵션을 선택 취소하여 모든 규칙을 볼 수 있습니다. 일치하는 규칙이 강조 표시됩니다.

정책 편집기에는 각 액세스 제어 규칙의 이름, 조건의 요약, 규칙 작업, 규칙의 검사 옵션 또는 상태를 알리는 아이콘이 표시됩니다. 이러한 아이콘은 다음을 나타냅니다.

- 시간 범위 옵션( )
- **Intrusion policy(**침입 정책**)** ( )
- **File policy(**파일 정책**)** ( )
- **Logging(**로깅**)** ( )
- **Warning(**경고**)** ( )
- **Error(**오류**)** ( )
- **Rule Conflict(**규칙 충돌**)** ( )

비활성화된 규칙은 흐리게 표시되며, 규칙 이름 뒤에 disabled(비활성화))가 표시됩니다.

규칙을 생성하거나 편집하려면 액세스 제어 규칙 편집기를 사용합니다.

- 다음을 수행할 수 있습니다.

- 규칙 이름을 구성하고 편집기 상단에서 해당 위치를 선택합니다.
- 편집기 위 또는 아래의 행을 선택하여 다른 규칙을 수정하도록 전환합니다.
- 왼쪽 목록을 사용하여 규칙 작업을 선택하고 침입 정책 및 변수 집합, 파일 정책, 시간 범위, 로깅 설정 옵션을 적용합니다.
- 규칙 이름 옆의 옵션을 사용하여 규칙 작업을 선택하고 침입 정책 및 변수 집합, 파일 정책 및 시간 범위를 적용하고 로깅 옵션을 설정합니다.

- **Sources(**소스**)** 및 **Destinations and Applications(**대상 및 애플리케이션**)** 열을 사용하여 일치 기준을 추가합니다. All(모두) 목록에서 옵션을 추가하거나 다른 탭으로 이동하여 원하는 옵션 유형(예: 보안 영역 또는 네트워크)을 더 쉽게 찾을 수 있습니다.
- 편집기의 맨 아래에서 규칙에 코멘트를 추가합니다.

관련 항목

액세스 제어 규칙 구성 요소, 4 페이지
액세스 제어 규칙 순서에 대한 모범 사례

액세스 제어 규칙 구성 요소

각 액세스 제어 규칙에는 고유한 이름 외에도, 다음과 같은 기본 구성 요소가 있습니다.

상태

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하지 않으며, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 정책 상속을 사용하는 경우, 규칙 1이 가장 바깥쪽 정책의 첫 번째 규칙입니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

규칙은 섹션과 카테고리에 속할 수도 있는데, 이는 체계상 그런 것뿐이며 규칙 위치에 영향을 주지 않습니다. 규칙 위치는 섹션과 카테고리에 걸쳐 이동합니다.

섹션 및 카테고리

액세스 제어 규칙을 쉽게 구성할 수 있도록, 모든 액세스 제어 정책에는 시스템에서 제공하는 Mandatory(필수) 및 Default(기본값)라는 두 가지 섹션이 있습니다. 액세스 제어 규칙을 더욱 체계화하기 위해 Mandatory(필수) 및 Default(기본값) 섹션 내에 맞춤 설정 규칙 카테고리를 생성할 수 있습니다.

정책 상속을 사용 중인 경우, 현재 정책의 규칙은 상위 정책의 Mandatory(필수) 및 Default(기본값) 섹션 사이에 중첩됩니다.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 조건은 단순하거나 복잡할 수 있으며 사용법은 라이선스에 따라 달라지는 경우가 많습니다.

트래픽은 규칙에 지정된 조건을 전부 충족해야 합니다. 예를 들어, Applications(애플리케이션) 조건에서 HTTPS는 지정하지 않고 HTTP를 지정하는 경우, URL 범주 및 평판 조건이 HTTPS 트래픽에 적용되지 않습니다.

적용 가능한 시간

규칙을 적용 가능한 기간의 날짜와 시간을 지정할 수 있습니다.

작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용(추가 검사 실행 또는 실행 안 함)할 수 있습니다. 시스템은 신뢰할 수 있거나 차단되거나 암호화된 트래픽에서 심층 검사를 수행하지 않습니다.

인스펙션

심층 검사 옵션은 사용자가 허용할 수도 있는 악성 트래픽을 시스템이 검사 및 차단하는 방법을 제어합니다. 규칙으로 트래픽을 허용하는 경우 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에, 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다.

로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다. 규칙과 매칭하는 트래픽을 기록할 수 있습니다. 일반적으로 연결의 시작이나 끝 또는 시작과 끝에서 세션을 로깅할 수 있습니다. 데이터베이스 및 시스템 로그(syslog) 또는 SNMP 트랩 서버에 대한 연결을 로깅할 수 있습니다.

Comments(의견)

액세스 제어 규칙의 변경 사항을 저장할 때마다 코멘트를 추가할 수 있습니다.

관련 항목

- 액세스 제어 규칙 순서에 대한 모범 사례
- 액세스 제어 규칙 관리, 3 페이지
- 액세스 제어 규칙 생성 및 수정, 11 페이지
- 액세스 제어 규칙 작업, 6 페이지
- 액세스 제어 규칙 조건, 13 페이지
- 파일 및 침입 정책을 사용한 심층 검사
- 액세스 제어 규칙 코멘트

액세스 제어 규칙 순서

액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 액세스 제어 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 모든 규칙의 조건이 트래픽과 일치하는 첫 번째 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 모니터링 규칙을 제외하고, 시스템은 트래픽이 규칙과 일치하는 것으로 확인되고 나면 우선 순위가 낮은 추가 규칙을 기준으로 트래픽을 계속 평가하지 않습니다.

액세스 제어 규칙을 쉽게 구성할 수 있도록, 모든 액세스 제어 정책에는 시스템에서 제공하는 Mandatory(필수) 및 Default(기본값)라는 두 가지 섹션이 있습니다. 추가로 구성하려면 Mandatory(필

수) 또는 Default(기본값) 섹션 내에서 맞춤형 규칙 카테고리를 생성하면 됩니다. 카테고리를 생성한 후에는 삭제 및 이름 바꾸기가 가능하고 규칙을 카테고리 안으로, 밖으로, 내부에서, 주변으로 이동할 수는 있으나 카테고리를 이동할 수는 없습니다. 시스템은 섹션 및 카테고리 전반에 걸쳐 규칙 번호를 할당합니다.

정책 상속을 사용할 경우, 현재 정책의 규칙은 상위 정책의 Mandatory(필수) 및 Default(기본값) 규칙 섹션 사이에 중첩됩니다. 규칙 1은 현재 정책이 아닌 가장 바깥쪽 정책의 첫 번째 규칙이며, 시스템은 정책, 섹션, 카테고리 전반에 걸쳐 규칙 번호를 할당합니다.

액세스 제어 정책의 수정을 허용하는 사전 정의된 사용자 역할을 사용하면 규칙 카테고리 내에서 그리고 규칙 카테고리 간에 액세스 제어 규칙을 이동 및 수정할 수도 있습니다. 하지만, 사용자가 규칙을 이동하거나 변경하지 못하도록 제한하는 사용자 역할을 만들 수 있습니다. 액세스 제어 정책을 수정할 수 있는 모든 사용자는 맞춤형 카테고리에 규칙을 추가하고 해당 카테고리의 규칙을 제한 없이 수정할 수 있습니다.

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

팁 적절한 액세스 제어 규칙 순서는 네트워크 트래픽을 처리하는 데 필요한 리소스를 줄이고 규칙의 사전 대응을 방지합니다. 사용자가 생성한 규칙이 모든 조직과 배포에 고유하더라도 사용자의 필요를 처리하는 동안 성능을 최적화할 수 있는 규칙을 언제 지시할지에 대해 몇 가지 따라야 할 지침이 있습니다.

관련 항목

규칙 순서 지정 모범 사례

액세스 제어 규칙 작업

모든 액세스 제어 규칙에는 시스템이 일치하는 트래픽을 처리하고 로깅하는 방법을 결정하는 작업이 있습니다. 추가 검사와 함께 또는 추가 검사 없이, 모니터링, 신뢰, 차단 또는 허용할 수 있습니다.

액세스 제어 정책의 기본 작업은 모니터링을 제외한 작업을 이용하는 액세스 제어 규칙의 조건을 충족하지 않는 트래픽을 처리합니다.

액세스 제어 규칙 모니터 작업

Monitor(모니터링**)** 작업은 트래픽을 허용하거나 거부하도록 설계되지 않았습니다. 이 작업의 기본 목적은 일치하는 트래픽의 처리 방식에 상관없이 연결 로깅을 강제하는 것입니다.

연결이 모니터링 규칙과 일치한다면, 연결과 일치하는 다음 비 모니터링 규칙으로 트래픽 처리 및 추가 검사를 결정해야 합니다. 일치하는 다른 규칙이 없다면, 시스템은 기본 작업을 사용해야 합니다.

그러나 예외가 있습니다. 모니터링 규칙에 레이어 7 조건(예: 애플리케이션 조건)이 포함된다면, 시스템은 초기 패킷을 전달하고 연결을 설정하도록(또는 SSL 핸드셰이크를 완료하도록) 허용할 수 있습니다. 후속 규칙으로 연결을 차단해야 하는 경우도 마찬가지입니다. 이러한 초기 패킷은 후속 규칙을 기준으로 평가되지 않기 때문입니다. 이러한 패킷이 완전히 검사되지 않은 대상에 도달하지 않도록 하려면 액세스 제어 정책의 고급 설정에서 이러한 목적을 위한 침입 정책을 지정할 수 있습니다. 트래픽이 식별되기 전에 통과하는 패킷 검사을 참조하십시오. 레이어 7 식별을 완료하면, 시스템은 나머지 세션 트래픽에 적절한 작업을 적용합니다.

주의 모범 사례는 트래픽이 실수로 네트워크로 들어오지 않도록, 광범위하게 정의되는 모니터링 규칙의 레이어 7 조건을 규칙 우선순위 상위에 놓지 않는 것입니다. 또한 로컬에서 바인딩된 트래픽이 레이어 3 구축의 모니터링 규칙과 일치하면, 해당 트래픽은 검사를 우회할 수 있습니다. 트래픽의 검사를 보장하려면 트래픽을 라우팅하는 매니지드 디바이스의 고급 디바이스 설정에서 **Inspect Local Router Traffic(**로컬 라우터 트래픽 검사**)**을 활성화하십시오.

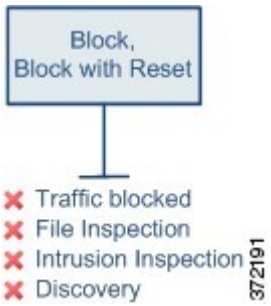
액세스 제어 규칙 신뢰 작업

Trust(신뢰**)** 작업은 심층 검사 또는 네트워크 검색 없이 트래픽이 통과하도록 허용합니다. 신뢰할 수 있는 트래픽에는 ID 요건 및 속도 제한이 계속 적용됩니다.

참고 FTP 및 SIP와 같은 일부 프로토콜은 시스템이 검사 프로세스를 통해 여는 보조 채널을 사용합니다. 경우에 따라 신뢰할 수 있는 트래픽이 모든 검사를 우회할 수 있으며 이러한 보조 채널을 제대로 열 수 없습니다. 이 문제가 발생하면 신뢰 규칙을 **Allow(**허용**)**로 변경합니다.

액세스 제어 규칙 차단 작업

Block(차단**)** 및 **Block with reset(**차단 후 초기화**)** 작업은 어떤 종류의 추가 검사도 없이 트래픽을 거부합니다.



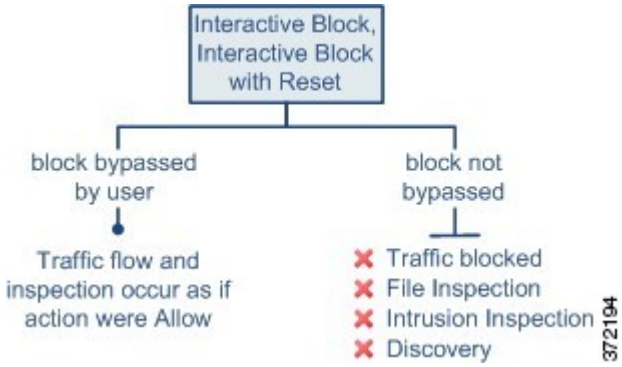
Block with reset(차단 후 재설정) 규칙은 *HTTP* 응답 페이지에 도달한 웹 요청을 제외하고 연결을 재설정합니다. 이것은 연결이 즉시 재설정되면 시스템이 웹 요청을 차단하는 경우에 표시되도록 사용자가 구성하는 응답 페이지가 표시될 수 없기 때문입니다. 자세한 내용은 HTTP 응답 페이지 및 인터랙티브 차단를 참고하십시오.

관련 항목

HTTP 응답 페이지 구성

액세스 제어 규칙 인터랙티브 차단 작업

Interactive Block(인터랙티브 차단**)** 및 **Interactive Block with reset(**재설정을 사용한 인터랙티브 차단**)** 작업은 웹 사용자에게 원하는 대상으로 계속 진행할 수 있는 선택권을 제공합니다.



사용자가 차단을 우회하는 경우, 규칙은 허용 규칙을 모방합니다. 따라서 인터랙티브 차단 규칙을 파일 및 침입 정책에 연결할 수 있으며, 일치하는 트래픽도 네트워크 검색 대상이 됩니다.

사용자가 차단을 우회하지 않거나 우회할 수 없는 경우, 규칙은 차단 규칙을 모방합니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.

인터랙티브 차단을 활성화하면 모든 차단된 연결을 재설정할 수 없습니다. 이것은 연결이 즉시 재설정되면 응답 페이지가 표시될 수 없기 때문입니다. **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 작업을 사용하여 웹 트래픽이 아닌 모든 트래픽을 차단 후 재설정하고, 웹 요청에 대해서는 계속 인터랙티브 차단을 활성화하십시오.

자세한 내용은 HTTP 응답 페이지 및 인터랙티브 차단를 참고하십시오.

관련 항목

해독 규칙 차단 작업

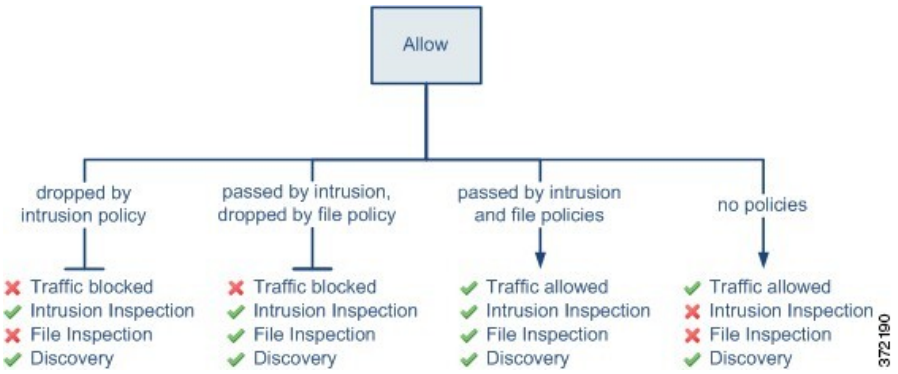
액세스 제어 규칙 허용 작업

Allow(허용**)** 작업은 일치하는 트래픽이 통과하도록 허용하지만 ID 요건과 속도 제한은계속 적용됩니다.

원하는 경우, 심층 검사를 사용하여 암호화되지 않은 트래픽과 해독된 트래픽이 목적지에 도달하기 전에 추가 검사하고 차단할 수 있습니다.

- 침입 정책을 사용하여 침입 탐지 및 방지 구성에 따라 네트워크 트래픽을 분석하고 해당 구성에 따라 문제가 되는 패킷을 삭제할 수 있습니다.
- 파일 정책을 사용하여 파일 제어를 수행할 수 있습니다. 파일 제어를 수행하면, 사용자가 특정 애플리케이션 프로토콜에서 특정 유형의 파일을 업로드(전송) 또는 다운로드(수신)하는 행동을 탐지하고 차단할 수 있습니다.
- 또한 파일 정책을 사용하여 네트워크 기반 AMP(Advanced Malware Protection)를 수행할 수 있습니다. 악성코드 대응 는 파일에서 악성 코드를 검사하고 구성에 따라 탐지된 악성코드를 차단할 수 있습니다.

다음 다이어그램은 허용 규칙 또는 사용자가 우회한 인터랙티브 차단 규칙의 조건을 충족하는 트래픽에서 수행되는 검사 유형을 보여줍니다. 파일 검사는 침입 검사 전에 발생합니다. 차단된 파일에 대해서는 침입 관련 익스플로잇을 검사하지 않습니다.



간소화를 위해, 다이어그램은 액세스 제어 규칙과 침입 정책 및 파일 정책 둘 다 연관되어 있는 또는 둘 다 연관되어 있지 않은 상황을 위한 트래픽 흐름을 표시합니다. 그러나 하나가 없더라도 다른 하나를 구성할 수 있습니다. 파일 정책이 없으면 트래픽 흐름은 침입 정책에 의해 결정되고, 침입 정책이 없으면 트래픽 흐름은 파일 정책에 의해 결정됩니다.

침입 또는 파일 정책에 의해 트래픽이 검사되든 삭제되든 상관없이 시스템은 네트워크 검색을 사용하여 트래픽을 검사할 수 있습니다. 그러나 트래픽을 허용한다고 해서 자동으로 검색 검사가 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에 의해 명시적으로 모니터링되는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다. 또한 암호화된 세션에 대해서는 애플리케이션 검색이 제한됩니다.

액세스 제어 규칙 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

액세스 제어 규칙에 대한 지침 및 제한 사항

- 능동적으로 사용 중인 액세스 제어 규칙을 수정한다면, 구축 시 설정 된 연결에는 변경 사항이 적용되지 않습니다. 업데이트된 규칙은 이후 연결의 일치 여부를 확인하는 데 사용됩니다. 그러나 시스템이 (예를 들어 침입 정책을 사용해) 연결을 능동적으로 검사한다면, 변경된 매칭 또는 작업 기준을 기존 연결에 적용합니다.

  threat defense의 경우에는 설정된 연결을 threat defense **clear conn** CLI 명령을 사용해 중단하면, 변경 사항을 모든 현재 연결에 적용할 수 있습니다. 연결 소스가 연결을 다시 설정하며 따라서 새로운 규칙에 대해 적절히 매칭됨이 예상되기 때문에, 이러한 연결을 중단해도 괜찮을 때만 이 작업을 수행하십시오.

- 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. 방화벽 인터페이스에 적용된 액세스 규칙에는 사용할 수 없습니다.
- 액세스 제어 규칙당 일치 기준당 최대 개체 수는 200입니다. 예를 들어 단일 액세스 제어 규칙에 최대 200개의 네트워크 개체를 포함할 수 있습니다.

액세스 제어 규칙 관리

다음 주제에서는 액세스 제어 규칙을 관리하는 방법에 대해 설명합니다.

액세스 제어 규칙 범주 추가

액세스 제어 정책의 Mandatory(필수) 및 Default(기본) 규칙 섹션을 맞춤 설정 카테고리로 나눌 수 있습니다. 카테고리를 생성한 후에는 삭제 및 이름 바꾸기가 가능하고 규칙을 카테고리 안으로, 밖으로, 내부에서, 주변으로 이동할 수는 있으나 카테고리를 이동할 수는 없습니다. 시스템은 섹션 및 카테고리 전반에 걸쳐 규칙 번호를 할당합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Add Category(**카테고리 추가**)**를 클릭합니다.

팁 정책에 이미 규칙이 포함된 경우, 새로운 규칙을 추가하기 전에 기존 규칙에 대한 행의 빈 영역을 클릭하여 새로운 카테고리의 위치를 지정합니다. 기존 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Insert new category(**새 카테고리 삽입**)**를 선택할 수도 있습니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** **Insert(**삽입**)** 드롭다운 목록에서 카테고리를 추가할 곳을 선택합니다.

- 섹션의 모든 기존 카테고리 아래에 카테고리를 삽입하려면 **into Mandatory(**필수로**)** 또는 **into Default(**기본으로**)**를 선택합니다.
- 기존 카테고리 위에 카테고리를 삽입하려면 **above category(**카테고리 위**)**를 선택한 다음 카테고리를 선택합니다.
- 액세스 제어 규칙 위 또는 아래에 카테고리를 삽입하려면 **above rule(**규칙 위**)** 또는 **below rule(**규칙 아래**)**를 선택한 다음 기존 규칙 번호를 입력합니다.

단계 **4** **Apply(**적용**)**을 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

액세스 제어 규칙 생성 및 수정

액세스 제어 규칙을 사용하여 특정 트래픽 클래스에 작업을 적용합니다. 규칙을 사용하면 적절한 트래픽을 선택적으로 허용하고 원치 않는 트래픽을 삭제할 수 있습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하려면 **Add Rule(**규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 **Edit(**수정**)** ( )을 클릭합니다.

- 여러 규칙을 편집하려면 확인란을 사용하여 여러 규칙을 선택한 다음 **Edit(**편집**)** 또는 검색 상자 옆에 있는 **Select Action(**작업 선택**)** 목록에서 다른 작업을 선택합니다.
- 규칙 조건에서 개체의 구성을 변경하는 인라인 편집을 수행하려면 값을 마우스 오른쪽 버튼으로 클릭하고 **Edit(**편집**)**를 선택합니다. 마우스 오른쪽 버튼 클릭 메뉴를 사용하여 항목을 제거하거나 필터에 추가하거나 텍스트 또는 값을 복사할 수도 있습니다.

규칙 옆에 **View(**보기**)** ( )가 대신 표시되는 경우에는 해당 규칙이 상위 정책에 속하거나 규칙을 수정할 권한이 없는 것입니다.

단계 **2** 새 규칙인 경우 **Name(**이름**)**을 입력합니다.

단계 **3** 규칙 구성 요소를 구성합니다.

여러 규칙을 대량 편집하는 경우에는 옵션의 하위 집합만 사용할 수 있습니다.

- Position(위치) — 규칙 위치를 지정합니다(액세스 제어 규칙 순서, 5 페이지 참조).
- Action(작업) — 규칙 **Action(**작업**)**을 선택합니다(액세스 제어 규칙 작업, 6 페이지 참조).
- Deep Inspection(심층 검사) - (선택 사항) Allow(허용) 및 Interactive Block(인터랙티브 차단) 규칙의 경우 **Intrusion Policy(**침입 정책**)**, **Variable Set(**변수 집합**)** 및 **File Policy(**파일 정책**)**에 대한 옵션을 선택합니다. 침입 및 파일 정책을 개별적으로 적용할 수 있습니다. 둘 다 구성할 필요는 없습니다.
- Time Range(시간 범위) - (선택 사항) threat defense 디바이스의 경우 규칙을 적용할 수 있는 요일과 시간을 선택합니다. 옵션을 선택하지 않으면 규칙이 항상 활성화됩니다. 자세한 내용은 시간 범위 개체 생성를 참조하십시오.
- Logging(로깅) - **Logging(**로깅**)**을 클릭하여 연결 로깅 및 SNMP 트랩에 대한 옵션을 지정합니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 연결 로깅 모범 사례를 참조하십시오.
- 조건 - 추가할 개체 또는 소스 또는 대상을 선택한 다음 **Add to Sources(**소스에 추가**)** 또는 **Add to Destinations and Applications(**대상 및 애플리케이션에 추가**)**를 클릭하여 일치하는 연결 조건을 추가합니다. 탭을 클릭하여 사용 가능한 개체 목록을 Networks(네트워크), Security Zones(보안 영역), Applications(애플리케이션) 등으로 제한할 수 있습니다. 그러나 소스 및 대상 열에는 현재 탭에 관계없이 항상 선택한 모든 개체가 표시됩니다. 자세한 내용은 액세스 제어 규칙 조건, 13 페이지을 참조하십시오.
- Comments(코멘트) - 대화 상자의 맨 아래에 있는 코멘트 목록을 열고 코멘트를 입력한 다음 **Post(**게시**)**를 클릭하여 코멘트를 추가합니다.

단계 **4** **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

시간 기반 규칙을 구축할 경우, 정책이 할당된 디바이스의 표준 시간대를 지정합니다. 시간대의 내용을 참조하십시오.

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

관련 항목

액세스 제어 규칙 순서에 대한 모범 사례

액세스 제어 규칙 조건

규칙 조건은 각 규칙의 대상으로 지정하려는 연결의 특성을 정의합니다. 규칙에 의해 처리되어야 하는 모든 트래픽에만 적용되도록 규칙을 정밀하게 조정하려면 조건을 사용합니다. 다음 주제에서는 사용할 수 있는 일치 조건에 대해 설명합니다.

보안/터널 영역 규칙 조건

보안 영역 및 터널 영역을 사용하여 규칙에 대한 트래픽을 선택할 수 있습니다.

보안 영역은 네트워크를 세그멘테이션화하여 여러 디바이스에 걸쳐 인터페이스를 그룹화하는 방법을 통해 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다. 터널 영역을 사용하면 터널 내에서 캡슐화된 연결에 액세스 제어 규칙을 적용하는 대신 터널로 처리해야 하는 GRE와 같은 터널링된 트래픽을 식별할 수 있습니다.

보안 영역을 사용하여 소스 및 대상 인터페이스로 트래픽을 제어할 수 있습니다. 소스 및 대상 영역 모두 영역 조건에 추가할 경우 소스 영역 중 하나의 인터페이스에서 트래픽 매치를 시작하고 규칙과 일치하도록 대상 영역 중 하나의 인터페이스에서 종료해야 합니다. 보안 영역의 모든 인터페이스가 동일한 유형이어야 하는 것과 마찬가지로(모든 인라인, 수동, 스위칭 또는 라우팅), 영역 조건에 사용된 모든 영역도 동일한 유형이어야 합니다. 패시브 방식으로 구축된 디바이스는 트래픽을 전송하지 않으므로 패시브 인터페이스를 대상 영역으로 하면서 영역을 사용할 수 없습니다.

터널 영역을 사용하는 경우 터널링된 트래픽을 영역과 연결할 수 있도록 사전 필터 정책에 일치하는 규칙이 있는지 확인합니다. 그런 다음 규칙에서 소스 영역으로 터널 영역을 선택할 수 있습니다. 터널 영역은 대상이 될 수 없습니다. 터널의 영역을 터널 영역으로 다시 지정하는 사전 필터 규칙이 없는 경우 터널에 대한 액세스 제어 규칙은 어떤 연결에도 적용되지 않습니다. 특정 인터페이스를 통해 디바이스에서 나가는 대상 터널에 대상 보안 영역을 지정할 수 있습니다.

보안 영역 고려 사항

보안 영역 기준을 결정할 때는 다음 사항을 고려하십시오.

- 특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.
- 액세스 제어 규칙은 디바이스 구성에서 ACE(ACL 항목)를 생성하여 가능한 경우 조기 처리 및 삭제를 제공합니다. 규칙에서 보안 영역을 지정하면 영역의 각 인터페이스에 대해 ACE가 생성되므로 ACL의 크기가 크게 증가할 수 있습니다. 액세스 제어 규칙에서 생성된 ACL이 너무 크면 시스템 성능에 영향을 줄 수 있습니다.

- 다중 도메인 구축에서, 상위 도메인에 생성된 영역은 다른 도메인의 디바이스에 있는 인터페이스를 포함할 수 있습니다. 하위 도메인의 영역 조건을 구성할 경우, 컨피그레이션은 사용자가 볼 수 있는 인터페이스에만 적용됩니다.

네트워크 규칙 조건

네트워크 규칙 조건은 트래픽의 네트워크 주소 또는 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- IP 주소 또는 지리적 위치의 트래픽을 일치시키려면 소스 목록에 기준을 추가합니다.
- 트래픽을 IP 주소 또는 지리적 위치와 일치시키려면 대상 목록에 기준을 추가합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.

  가능하면 여러 네트워크 개체를 단일 개체 그룹으로 결합합니다. 둘 이상의 개체(소스 또는 대상에 대해 개별적으로)를 선택하면 시스템에서 (구축 중에) 개체 그룹을 자동으로 생성합니다. 기존 그룹을 선택하면 개체 그룹 중복을 방지할 수 있으며 중복 개체가 많을 경우 CPU 사용량에 대한 잠재적 영향을 줄일 수 있습니다.

  FQDN(Fully Qualified Domain Name)을 사용하여 주소를 정의하는 개체를 사용할 수 있습니다. 주소는 DNS 조회를 통해 확인됩니다. 그러나 FQDN 개체는 Snort3 액세스 제어 정책 및 액세스 제어 정책의 원본 클라이언트 네트워크, SGT/ISE 속성, 네트워크 분석 및 침입 정책, 보안 인텔리전스, 위협 탐지, 엘리펀트 플로우 설정 섹션에서도 지원되지 않습니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다.

네트워크 조건의 원본 클라이언트(프록시된 트래픽 필터링)

일부 규칙에서는 원본 클라이언트에 따라 프록시된 트래픽을 처리할 수 있습니다. 소스 네트워크 조건을 사용하여 프록시 서버를 지정한 다음 원본 클라이언트 제약 조건을 추가하여 원본 클라이언트 IP 주소를 지정합니다. 시스템에서는 패킷의 XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의 HTTP 헤더 필드를 사용하여 원본 클라이언트 IP를 확인합니다.

프록시의 IP 주소가 규칙의 소스 네트워크 제약 조건과 매치하고 원본 클라이언트 IP 주소가 규칙의 원본 클라이언트 제약 조건과 매치하면 트래픽이 규칙과 매치하는 것입니다. 예를 들어 특정 원본 클라이언트 주소에서 보낸 트래픽을 허용하되 특정 프록시를 사용하는 경우로 제한하려면 3가지 액세스 제어 규칙을 생성합니다.

액세스 제어 규칙 1: 특정 IP 주소(209.165.201.1)의 프록시 설정된 트래픽 차단

소스 네트워크: 209.165.201.1
원본 클라이언트 네트워크: 없음/모두
작업: 차단

액세스 제어 규칙 2: 해당 트래픽의 프록시 서버가 사용자가 선택한 프록시 서버인 경우에만 동일한 IP 주소의 프록시 설정된 서버 허용(209.165.200.225 또는 209.165.200.238)

소스 네트워크: 209.165.200.225, 209.165.200.238
원본 클라이언트 네트워크: 209.165.201.1
작업: 허용

액세스 제어 규칙 3: 다른 프록시 서버를 사용할 경우 동일한 IP 주소의 프록시 설정된 트래픽 차단

소스 네트워크: 모두
원본 클라이언트 네트워크: 209.165.201.1
작업: 허용

VLAN 태그 규칙 조건

참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. VLAN 태그가 있는 액세스 규칙은 방화벽 인터페이스의 트래픽과 일치하지 않습니다.

VLAN 규칙 조건은 Q-in-Q(스택 VLAN) 트래픽을 포함한 VLAN 태그가 있는 트래픽을 제어합니다. 시스템은 가장 안쪽의 VLAN 태그를 사용하여 VLAN 트래픽을 필터링하며, 규칙에서 가장 바깥쪽의 VLAN 태그를 사용하는 사전 필터 정책은 예외입니다.

다음 Q-in-Q 지원에 유의하십시오.

- Firepower 4100/9300의 Threat Defense - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- 다른 모든 모델의 Threat Defense:
  - 인라인 집합 및 패시브 인터페이스 - Q-in-Q를 지원합니다(최대 2개의 VLAN 태그 지원).
  - 방화벽 인터페이스 - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).

사전 정의된 개체를 사용하여 VLAN 조건을 작성하거나, 1에서 4094 사이의 VLAN 태그를 수동으로 입력할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

클러스터에서 VLAN 일치에 문제가 발생하면 액세스 제어 정책 고급 옵션인 Transport/Network Preprocessor Settings(전송/네트워크 전처리기 구성)를 편집하고 **Ignore VLAN header when tracking connections(**연결 추적 시 **VLAN** 헤더 무시**)** 옵션을 선택합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

사용자 규칙 조건

사용자 규칙 조건은 연결을 시작한 사용자 또는 사용자가 속한 그룹을 기준으로 트래픽을 매칭합니다. 예를 들어, Finance 그룹의 모든 사용자가 네트워크 리소스에 액세스하는 것을 금지하도록 Block(차단) 규칙을 구성할 수 있습니다.

액세스 제어 규칙의 경우에만 먼저 액세스 제어에 다른 정책 연결에 설명된 대로 ID 정책을 액세스 제어 정책과 연결해야 합니다.

구성된 영역에 대한 사용자 및 그룹을 구성하는 것 외에도 다음 특수 ID 사용자에 대한 정책을 설정할 수 있습니다.

- Failed Authentication(실패한 인증): 캡티브 포털(captive portal) 인증에 실패한 사용자입니다.
- Guest(게스트): 캡티브 포털에서 게스트 사용자로 구성된 사용자입니다.
- No Authentication Required(인증 필요 없음): ID가 **No Authentication Required(**인증 필요 없음**)** 규칙 작업과 일치하는 사용자입니다.
- Unknown(알 수 없음): 식별할 수 없는 사용자입니다. 예를 들어 구성된 영역에 의해 다운로드되지 않은 사용자입니다.

애플리케이션 규칙 조건

시스템에서 IP 트래픽을 분석할 때, 사용자의 네트워크에서 자주 사용되는 애플리케이션을 식별하여 분류할 수 있습니다. 이 검색 기반 애플리케이션 인식은 애플리케이션 컨트롤을 위한 기본 요소로, 애플리케이션 트래픽을 제어하는 기능입니다.

시스템에서 제공되는 애플리케이션 필터는 유형, 위험, 사업 타당성, 카테고리, 태그라는 기본 특성에 따라 애플리케이션을 구성하여 애플리케이션 컨트롤을 수행할 수 있도록 지원합니다. 시스템에서 제공되는 필터를 조합하거나 애플리케이션을 맞춤형으로 조합하여 재사용 가능한 사용자 정의 필터를 생성할 수 있습니다.

정책의 애플리케이션 규칙 조건마다 적어도 하나의 탐지기가 활성화되어야 합니다. 애플리케이션에 탐지기가 활성화되지 않은 경우, 시스템은 시스템에서 제공된 모든 탐지기를 해당 애플리케이션에 자동으로 활성화합니다. 시스템에서 제공된 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 활성화합니다. 애플리케이션 탐지기에 대한 자세한 내용은 애플리케이션 탐지기 기초을 참조하십시오.

두 애플리케이션 필터를 모두 사용하거나 개별적으로 지정된 애플리케이션을 사용하여 완전한 커버리지를 보장할 수 있습니다. 그러나 액세스 제어 규칙 순서를 지정하기 전에 다음을 참고하십시오.

애플리케이션 필터의 이점

애플리케이션 필터는 애플리케이션 컨트롤을 신속하게 구성하는 데 도움이 됩니다. 예를 들어 시스템에서 제공되는 필터를 손쉽게 사용하여 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하고 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 시스템에서는 해당 세션을 차단합니다.

애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템이 애플리케이션 트래픽을 정상적으로 제어할 수 있습니다. Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 애플리케이션 탐지기를 자주 업데이트하고 추가하므로, 시스템에서는 최신 탐지기를 사용하여 애플리케이션 트래픽을 모니터링할 수 있습니다. 자체 탐지기를 생성하고 이러한 탐지기로 탐지한 애플리케이션에 특성을 할당할 수도 있으며, 이는 기존 필터에 자동으로 추가됩니다.

애플리케이션 특성

시스템은 다음 표에서 설명하는 조건을 사용해 탐지하는 각 애플리케이션을 구별합니다. 애플리케이션 필터로 이러한 특성을 사용합니다.

표 ***1:*** 애플리케이션 특성

특성	설명	예
유형	애플리케이션 프로토콜은 호스트 간 통신을 나타냅니다. 클라이언트는 호스트에서 실행 중인 소프트웨어를 나타냅니다. 웹 애플리케이션은 HTTP 트래픽에 대한 콘텐츠 또한 요청 URL을 나타냅니다.	HTTP 및 SSH는 애플리케이션 프로토콜입니다. 웹 브라우저 및 이메일 클라이언트는 클라이언트입니다. MPEG 비디오 및 Facebook은 웹 애플리케이션입니다.
위험	애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성입니다.	피어 투 피어 애플리케이션은 고위험 경향이 있습니다.
사업 타당성	애플리케이션이 오락이 아닌 조직의 비즈니스 운영 컨텍스트 내에서 사용될 가능성입니다.	게임 애플리케이션은 비즈니스 연관성이 매우 낮은 경향이 있습니다.
카테고리	가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.	Facebook은 소셜 네트워킹 카테고리에 포함됩니다.
태그	애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.	비디오 스트리밍 웹 애플리케이션은 종종 높은 대역폭 및 광고 표시 태그가 지정됩니다.

관련 항목

애플리케이션 제어 구성 모범 사례

애플리케이션 조건 및 필터 구성

애플리케이션 조건 또는 필터를 구성하려면 사용 가능한 애플리케이션 목록에서 제어를 원하는 트래픽의 애플리케이션을 선택합니다. 선택적으로(권장 사항), 필터를 사용해 사용 가능한 애플리케이션을 제약합니다. 동일한 조건에서 필터 및 개별적으로 지정된 애플리케이션을 사용할 수 있습니다.

시작하기 전에

- 적응형 프로파일은 애플리케이션 제어를 수행하기 위해 적응형 프로파일 구성의 설명대로 액세스 제어 규칙에 대해 반드시 활성화(기본 상태)가 되어 있어야 합니다.
- 콘텐츠 제한을 구현하는 경우 이 절차 대신 액세스 제어 규칙을 사용하여 콘텐츠 제한 시행의 절차를 따르십시오.
- 클래식 디바이스 모델의 경우 이러한 조건을 설정하려면 제어 라이선스가 있어야 합니다.

프로시저

단계 1 규칙 또는 구성 편집기를 호출합니다.

- 액세스 제어, 암호 해독, QoS 규칙 조건 - 규칙 편집기에서 **Applications(**애플리케이션**)**을 클릭합니다.
- ID 규칙 조건 - 규칙 편집기에서 **Realms & Settings(**영역 및 설정**)**을 클릭하고 액티브 인증을 활성화하려면 ID 규칙 생성를 참조합니다.
- 애플리케이션 필터 - 개체 관리자의 애플리케이션 필터 페이지에서 애플리케이션 필터를 추가하거나 편집합니다. 필터의 고유 이름을 제공합니다.
- 인텔리전트 애플리케이션 우회(IAB) - 액세스 제어 정책 편집기에서 **Advanced(**고급**)**을 클릭하고 IAB 세팅을 편집한 뒤 **Bypassable Applications and Filters(**우회 가능한 애플리케이션 및 필터**)**를 클릭합니다.

단계 2 **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 추가하려는 애플리케이션을 찾아 선택합니다.

Available Applications(사용 가능한 애플리케이션**)**에 표시된 애플리케이션을 제한하기 위해 하나 이상의 **Application Filters(**애플리케이션 필터**)**를 선택하거나 개별 애플리케이션을 검색합니다.

팁 요약 정보 및 내부 검색 링크를 표시하기 위해 애플리케이션 옆의 **Information(**정보**)** ( ) 을 클릭합니다. **Unlock(**잠금 해제**)**은 시스템이 암호화된 트래픽에서만 확인할 수 있는 애플리케이션을 표시합니다.

하나 또는 여러 필터를 선택할 때 사용 가능한 애플리케이션 목록은 조건에 맞는 애플리케이션만 표시합니다. 시스템에서 제공된 여러 필터를 선택할 수 있지만 사용자 지정 필터는 선택할 수 없습니다.

- 동일한 속성(위험, 비즈니스 연관성 등)에 대한 여러 필터 - 애플리케이션 트래픽은 하나의 필터에만 일치해야 합니다. 중간 또는 고위험 필터를 선택하는 경우 사용 가능한 애플리케이션 목록은 모든 중간 및 고위험 애플리케이션을 표시합니다.

- 다른 애플리케이션 속성에 대한 필터 - 애플리케이션 트래픽은 두 필터 유형에 모두 일치해야합니다. 예를 들어 고위험 및 비즈니스 연관성이 낮은 필터를 선택하는 경우 사용 가능한 애플리케이션 목록은 두 조건을 모두 만족하는 애플리케이션만을 표시합니다.

단계 **3** **Add Application(**애플리케이션 추가**)** 또는 **Add to Rule(**규칙에 추가**)**을 클릭하거나 끌어서 놓습니다.

팁 더 많은 필터 및 애플리케이션을 추가하기 전에 현재 선택 사항을 지우려면 **Clear Filters(**필터 지우기**)**를 클릭합니다.

단계 **4** 규칙 또는 설정을 저장하거나 편집합니다.

다음에 수행할 작업

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

포트, 프로토콜 및 **ICMP** 코드 규칙 조건

포트 조건은 소스 및 대상 포트를 기준으로 트래픽과 일치합니다. 규칙 유형에 따라, "포트"는 다음 중 하나를 나타낼 수 있습니다.

- TCP 및 UDP — 포트를 기준으로 TCP 및 UDP 트래픽을 제어할 수 있습니다. 시스템은 괄호 내 프로토콜 번호와 선택적으로 결합된 포트 또는 포트 범위를 사용하여 이 구성을 나타냅니다. 예: TCP(6)/22
- ICMP — 인터넷 레이어 프로토콜과 선택적 유형 및 코드에 따라 ICMP 및 ICMPv6(IPv6-ICMP) 트래픽을 제어할 수 있습니다. 예: ICMP(1):3:3
- Protocol(프로토콜) - 포트를 사용하지 않는 다른 프로토콜을 사용하여 트래픽을 제어할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

포트 기반 규칙 모범 사례

포트를 지정하는 것은 애플리케이션을 대상으로 하는 기존의 방법입니다. 그러나 고유한 포트를 사용하여 액세스 제어 블록을 우회하도록 애플리케이션을 설정할 수 있습니다. 따라서 트래픽을 대상으로 지정하려면 가능한 경우 항상 포트 기준 대신 애플리케이션 필터링 기준을 사용하십시오. 사전 필터 규칙에서는 애플리케이션 필터링을 사용할 수 없습니다.

FTP와 같이 제어와 데이터 흐름을 위해 별도의 채널을 동적으로 여는 애플리케이션에도 애플리케이션 필터링이 권장됩니다. 포트 기반 액세스 제어 규칙을 사용하면 이러한 종류의 애플리케이션이 올바르게 작동하지 못하게 되어 적절한 연결이 차단될 수 있습니다.

소스 및 대상 포트 제약 조건 사용

소스 및 대상 포트 제약 조건을 모두 추가할 경우 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어, 소스 포트로 DNS over TCP를 추가한 경우, 대상 포트에 Yahoo 메신저 음성 채팅(TCP)을 추가할 수 있지만 Yahoo 메신저 음성 채팅(UDP)은 해당되지 않습니다.

소스 포트만 또는 대상 포트만 추가할 경우 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어, DNS over TCP 및 DNS over UDP 모두를 단일 액세스 제어 규칙의 대상 포트 조건으로 추가할 수 있습니다.

비 **TCP** 트래픽을 포트 조건과 일치

비 포트 기반 프로토콜을 매칭할 수 있습니다. 기본적으로 포트 조건을 지정하지 않으면 IP 트래픽이 일치하게 됩니다. 비 TCP 트래픽과 일치하도록 포트 조건을 구성할 수 있지만, 몇 가지 제한 사항이 있습니다.

- 액세스 제어 규칙 - 기본 디바이스의 경우 GRE(47) 프로토콜을 대상 포트 조건으로 사용하는 방법으로 GRE 캡슐화 트래픽을 액세스 제어 규칙과 매치할 수 있습니다. GRE 제한 규칙에는 네트워크 기반 조건(영역, IP 주소, 포트, VLAN 태그)만 추가할 수 있습니다. 또한, 시스템은 외부 헤더를 사용하여 액세스 제어 정책의 모든 트래픽을 GRE 제한 규칙과 일치시킵니다. threat defense 디바이스의 경우, 사전 필터 정책의 터널 규칙을 사용하여 GRE 캡슐화된 트래픽을 제어합니다.
- Decryption(암호 해독) 규칙 — 이러한 규칙은 TCP 포트 조건만 지원합니다.
- IMCP 에코 - 대상 ICMP 포트의 유형이 0으로 설정되었거나 대상 ICMPv6 포트의 유형이 129로 설정된 경우 요청하지 않은 에코 응답만 매치합니다. ICMP 에코 요청에 대한 응답으로 전송된 ICMP 에코 응답은 무시됩니다. 모든 ICMP 에코에 일치하는 규칙의 경우, ICMP 유형 8 또는 ICMPv6 유형 128을 사용합니다.

URL 규칙 조건

네트워크의 사용자가 액세스할 수 있는 웹 사이트를 제어하기 위해 URL 조건을 사용합니다.

자세한 내용은 URL 필터링를 참조하십시오.

동적 속성 규칙 조건

동적 속성에는 다음이 포함됩니다.

- 동적 개체 (예: Cisco Secure Dynamic Attributes Connector)

  동적 속성 커넥터을 사용하면 클라우드 제공자에서 데이터(예: 네트워크 및 IP 주소)를 수집하여 Firepower Management Center로 전송하여 액세스 제어 규칙에 사용할 수 있습니다. .

  동적 속성 커넥터에 대한 자세한 내용은 Cisco Secure Dynamic Attributes Connector 구성 가이드의 내용을 참조하십시오.

- SGT 개체
- 위치 IP 개체
- 디바이스 유형 개체

- 엔드포인트 프로파일 개체

동적 속성은 액세스 제어 규칙에서 소스 기준 및 대상 기준으로 사용할 수 있습니다. 다음 지침을 사용하십시오.

- 서로 다른 유형의 개체는 함께 AND 됨
- 유사한 유형의 개체는 함께 OR 됨

예를 들어 소스 대상 기준 SGT 1, SGT 2 및 디바이스 유형 1을 선택하는 경우 디바이스 유형 1이 SGT 1 또는 SGT 2에서 탐지되면 규칙이 일치합니다.

*API*가 생성한 동적 개체 정보

동적 개체는 REST API 호출을 사용하거나 Cisco Secure Dynamic Attributes Connector를 사용하여 검색되는 하나 이상의 IP 주소를 지정하는 개체입니다. 클라우드 소스에서 IP 주소를 업데이트할 수 있습니다. 이러한 동적 개체는 나중에 액세스 제어 정책을 구축할 필요 없이 액세스 제어 규칙에 사용할 수 있습니다.

동적 속성 커넥터에 대한 자세한 내용은 *Cisco Secure Dynamic Attributes* 구성 가이드(가이드 링크)를 참조하십시오.

동적 개체와 네트워크 개체의 차이점은 다음과 같습니다.

- 동적 속성 커넥터를 사용하여 생성된 동적 개체는 생성되는 즉시 management center에 푸시되며 정기적인 간격으로 업데이트됩니다.
- API가 생성한 동적 개체:
  - 네트워크 개체와 매우 유사하게 액세스 제어 규칙에서 사용할 수 있는 CIDR(Classless Inter-Domain Routing)이 있거나 없는 IP 주소입니다.
  - 정규화된 도메인 이름 또는 주소 범위를 지원하지 않습니다.
  - API를 사용하여 업데이트해야 합니다.

관련 항목

API가 생성한 동적 개체 추가 또는 편집

동적 속성 조건 구성

액세스 제어 규칙에 대해 동적 속성을 구성하는 경우 동일한 유형의 개체가 함께 OR 되고 다른 유형의 개체가 함께 AND 됩니다. 이 항목의 끝에 예가 나와 있습니다.

참고 이 절차는 레거시 UI를 기반으로 합니다. New UI Layout(새 UI 레이아웃)에서 **Sources(**소스**)** 또는 **Destinations and Applications(**대상 및 애플리케이션**)** 필드의 **Add(**추가**)** (+)를 클릭하여 동적 속성을 추가할 수 있습니다.

시작하기 전에

동적 개체를 생성하고 이러한 개체가 액세스 제어 정책에서 어떻게 사용되는지 파악합니다.

동적 개체에 대한 자세한 내용은 API가 생성한 동적 개체 정보의 내용을 참조하십시오.

액세스 제어 정책에서 동적 개체를 사용하는 방법에 대한 자세한 내용은 동적 속성 규칙 조건, 20 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 규칙 편집기에서 **ISE Attributes(ISE** 속성**)**를 클릭합니다.

단계 **2** Available Attributes(사용 가능한 속성) 섹션에서 다음 중 하나를 수행합니다.

- 필드에 모든 속성 이름의 일부를 입력합니다.
- 해당 유형의 개체만 보려면 **Security Group Tag(**보안 그룹 태그**)** 또는 **Dynamic Objects(**동적 개체**)**를 클릭합니다.

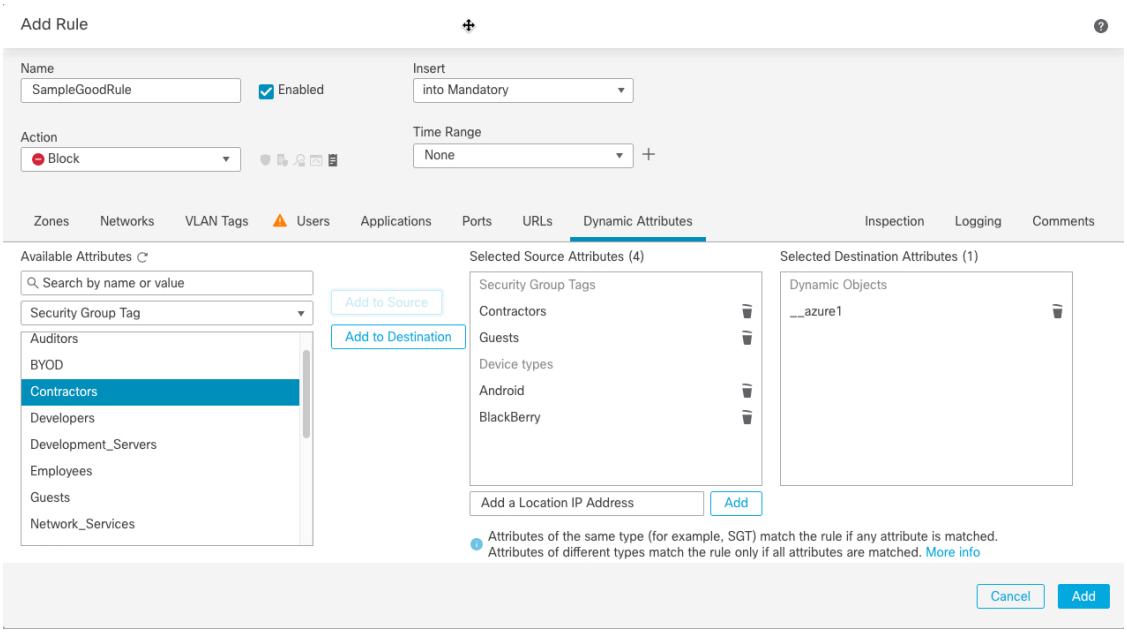
단계 **3** 선택한 개체를 소스 일치 기준에 적용하려면 **Add to Source(**소스에 추가**)**를 클릭합니다.

단계 **4** 선택한 개체를 대상 일치 기준에 적용하려면 **Add to Destination(**대상에 추가**)**을 클릭합니다.

단계 **5** 규칙 구성을 완료했으면 **Save(**저장**)**를 클릭합니다.

예**:** 차단 규칙에서 여러 소스 조건 사용

다음 예에서는 보안 그룹 태그 계약자 또는 게스트의 트래픽을 차단하고 디바이스 유형 Android 또는 Blackberry에서 동적 개체 **__azure1**에 액세스하지 못하도록 차단합니다.



다음에 수행할 작업

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

시간 및 날짜 규칙 조건

연속 시간 범위 또는 반복 기간을 지정할 수 있습니다.

예를 들어 규칙은 주중 근무 시간 중 또는 매주 또는 공휴일 셧다운 기간에만 적용할 수 있습니다.

시간 기반 규칙은 트래픽을 처리하는 디바이스의 로컬 시간을 기준으로 적용됩니다.

시간 기반 규칙은 FTD 디바이스에서만 지원됩니다. 시간 기반 규칙이 있는 정책을 다른 유형의 디바이스에 할당하는 경우 해당 디바이스에서 규칙과 연결된 시간 제한이 무시됩니다. 이 경우 경고가 표시됩니다.

액세스 제어 규칙 활성화 및 비활성화

액세스 제어 규칙을 만드는 경우, 이는 기본적으로 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다. 액세스 제어 정책에서 규칙 목록을 볼 때, 비활성화된 규칙은 계속 수정할 수 있지만 회색으로 표시됩니다.

규칙 편집기를 사용하여 액세스 제어 규칙을 활성화하거나 비활성화할 수도 있습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 규칙을 마우스 오른쪽 버튼으로 클릭하고 규칙 상태를 선택합니다.

규칙 옆에 **View(**보기**)** (👁)가 대신 표시되는 경우에는 해당 규칙이 상위 정책에 속하거나 규칙을 수정할 권한이 없는 것입니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

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

관련 항목

액세스 제어 규칙 구성 요소, 4 페이지

하나의 액세스 제어 정책에서 다른 정책으로 액세스 제어 규칙 복사

액세스 제어 규칙을 한 액세스 제어 정책에서 다른 액세스 제어 정책으로 복사할 수 있습니다. 액세스 제어 정책의 **Default(**기본**)** 섹션 또는 **Mandatory(**필수**)** 섹션에 규칙을 복사할 수 있습니다.

주석을 제외한 복사된 규칙의 모든 설정은 붙여 넣은 버전으로 유지됩니다.

프로시저

단계 **1** 다음 중 하나를 수행합니다.

- 단일 규칙을 복사하려면 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Copy to Different Policy(**다른 정책에 복사**)**를 선택합니다.
- 여러 규칙을 복사하려면 해당 확인란을 선택한 다음 **Select Bulk Action(**대량 작업 선택**)** 메뉴에서 **Copy to Different Policy(**다른 정책에 복사**)**를 선택합니다.

단계 **2** **Access Policy(**액세스 정책**)** 드롭 다운 목록에서 대상 액세스 제어 정책을 선택합니다.

단계 **3** **Place Rules(**규칙 배치**)** 드롭 다운 목록에서 복사한 규칙을 배치할 위치를 선택합니다. Mandatory(필수) 또는 Default(기본값) 섹션의 맨 아래에 배치할 수 있습니다.

단계 **4** **Copy(**복사**)**를 클릭합니다.

다음에 수행할 작업

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

사전 필터 정책으로 액세스 제어 규칙 이동

액세스 제어 규칙을 액세스 제어 정책에서 연결된 기본값이 아닌 사전 필터 정책으로 이동할 수 있습니다.

먼저 사용자 정의 사전 필터 정책을 액세스 제어 정책에 적용해야 합니다. 기본 사전 필터 정책에는 규칙을 사용할 수 없으므로 액세스 제어 규칙을 기본 사전 필터 정책으로 이동할 수 없습니다.

시작하기 전에

계속하기 전에 다음 사항에 유의하십시오.

- 액세스 제어 규칙을 사전 필터 정책으로 이동할 때는 액세스 제어 규칙의 레이어 7(L7) 매개 변수를 이동할 수 없습니다. L7 매개 변수는 작업 중에 삭제됩니다.
- 규칙을 이동하면 액세스 제어 규칙 구성의 코멘트가 손실됩니다. 그러나 소스 액세스 제어 정책을 언급하는 새로운 주석이 이동된 규칙에 추가됩니다.
- **Action(**작업**)** 매개 변수로 **Monitor(**모니터링**)**가 설정된 상태에서는 액세스 제어 규칙을 이동할 수 없습니다.
- 액세스 제어 규칙의 **Action(**작업**)** 매개 변수는 이동할 때 사전 필터 규칙의 적절한 작업으로 변경됩니다. 액세스 제어 규칙의 각 작업이 무엇에 매핑되는지 확인하려면 다음 표를 참조하십시오.

액세스 제어 규칙 작업	사전 필터 규칙의 작업
허용	분석

액세스 제어 규칙 작업	사전 필터 규칙의 작업
차단	차단
Block with Reset(차단 후 재설정)	차단
인터랙티브 차단(Block)	차단
재설정 인터랙티브 차단(Block)	차단
신임	단축 경로

- 마찬가지로 액세스 제어 규칙에 구성된 작업을 기반으로 다음 표에 나와 있는 것처럼 규칙을 이동한 후 로깅 구성이 적절한 설정으로 설정됩니다.

액세스 제어 규칙 작업	사전 필터 규칙에서 활성화된 로깅 구성
허용	확인란이 선택되지 않았습니다.
차단	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩
Block with Reset(차단 후 재설정)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩
인터랙티브 차단(Block)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩

액세스 제어 규칙 작업	사전 필터 규칙에서 활성화된 로깅 구성
재설정 인터랙티브 차단(Block)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩
신임	• Log at Beginning of Connection(연결 시작 시 로깅) • Log at End of Connection(연결 종료 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩

- 소스 정책에서 규칙을 이동하는 동안 다른 사용자가 해당 규칙을 수정하면 메시지가 표시됩니다. 페이지를 새로 고친 후 프로세스를 계속 진행할 수 있습니다.

프로시저

단계 **1** 다음 중 하나를 수행합니다.

- 단일 규칙을 이동하려면 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Move to Prefilter Policy(**사전 필터 정책으로 이동**)**를 선택합니다.
- 여러 규칙을 이동하려면 해당 확인란을 선택한 다음 **Select Bulk Action(**대량 작업 선택**)** 메뉴에서 **Move to Prefilter Policy(**사전 필터 정책으로 이동**)**를 선택합니다.

단계 **2** **Place Rules(**규칙 배치**)** 드롭 다운 목록에서 이동한 규칙을 배치할 위치를 선택합니다.

- 마지막 규칙 집합으로 배치하려면 맨 아래에를 선택합니다.
- 첫 번째 규칙 집합으로 배치하려면 상단에를 선택합니다.

단계 **3** **Move(**이동**)**를 클릭합니다.

다음에 수행할 작업

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

액세스 제어 규칙 포지셔닝

액세스 제어 정책 내에서 기존 규칙을 이동하거나 원하는 위치에 새 규칙을 삽입할 수 있습니다. 카테고리에 규칙을 추가하거나 카테고리로 규칙을 이동하면 시스템은 해당 규칙을 카테고리 마지막에 배치합니다.

시작하기 전에

액세스 제어 규칙 순서에 대한 모범 사례에서 규칙 순서 지침을 검토합니다.

프로시저

단계 **1** 다음 중 하나를 수행합니다.

- 새 규칙 - 기존 규칙 사이의 선 위에 마우스를 놓고 **Add Rule(**규칙 추가**)**을 클릭하여 새 규칙을 삽입합니다. 위치는 Add Rule(규칙 추가) 대화 상자의 **Insert(**삽입**)** 상자에서 선택됩니다. 다른 규칙을 선택하여 위치를 조정할 수 있습니다. 마우스 오른쪽 버튼 클릭 메뉴에서 **Add Rule above(**위의 규칙 추가**)** 또는 **Add Rule Below(**아래 규칙 추가**)**를 선택할 수도 있습니다.
- 기존 규칙(규칙 테이블 보기) - 단일 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Reposition Rule(**규칙 위치 조정**)**을 선택합니다. 여러 규칙을 그룹으로 이동하려면 해당 확인란을 선택한 다음 **Select Bulk Action(**대량 작업 선택**)** 메뉴에서 **Reposition Rules(**규칙 위치 조정**)**를 선택합니다.
- 기존 규칙 편집 시 - 규칙 이름 옆에 있는 **Reposition Rule(**규칙 위치 조정**)** 아이콘을 클릭합니다.

단계 **2** 규칙을 이동하거나 삽입할 곳을 선택합니다.

- **into Mandatory(**필수로**)** 또는 **into Default(**기본으로**)**를 선택합니다.
- **into Category(**범주로**)**를 선택한 다음 범주를 선택합니다.
- **above rule(**규칙 위**)** 또는 **below rule(**규칙 아래**)**를 선택한 다음 규칙을 선택합니다.

단계 **3** **Move(**이동**)** 또는 **Confirm(**확인**)**을 클릭하고 규칙을 편집하는 경우 저장합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

액세스 제어 규칙에 설명 추가

액세스 제어 규칙을 만들거나 수정할 때 코멘트를 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다. 각 코멘트 및 코멘트가 추가된 각 날짜를 추가한 사용자와 마찬가지로 규칙을 위한 모든 코멘트의 목록을 표시할 수 있습니다.

규칙을 저장할 때, 마지막 저장 이후 만들어진 모든 코멘트는 읽기 전용이 됩니다.

액세스 제어 규칙 코멘트를 검색하려면 Rule listing(규칙 목록) 페이지의 "Search Rules(규칙 검색)" 표시줄을 사용합니다.

프로시저

단계 **1** 액세스 제어 규칙 편집기에서 **Comments(**코멘트**)**를 클릭합니다.

단계 **2** 코멘트를 입력하고 **Add Comment(**코멘트 추가**)**를 클릭합니다. 규칙을 저장할 때까지 이 코멘트를 수정하거나 삭제할 수 있습니다.

단계 **3** 규칙을 저장합니다.

액세스 제어 규칙의 예시

다음 항목에서는 액세스 제어 규칙의 예를 제공합니다.

보안 영역을 사용한 액세스 제어 방법

호스트에 인터넷에 대한 무제한 액세스를 허용하더라도 수신 트래픽에서 침입 및 악성코드를 검사하여 호스트를 보호하는 경우의 구축을 고려하십시오.

우선, 내부 및 외부의 보안 영역 2개를 생성합니다. 그런 다음, 하나 이상의 디바이스에 있는 인터페이스 쌍을 이러한 영역에 할당합니다. 각 쌍의 인터페이스 하나는 내부 영역에, 다른 인터페이스 하나는 외부 영역에 할당합니다. 내부에서 네트워크에 연결된 호스트는 보호된 자산을 나타냅니다.

참고 모든 내부 (또는 외부) 인터페이스를 단일 영역으로 그룹화할 필요는 없습니다. 구축 및 보안 정책에 알맞은 그룹화를 선택합니다.

그런 다음 대상 영역 조건을 Internal로 설정한 액세스 제어 규칙을 구성합니다. 이 단순한 규칙은 내부 영역 내의 모든 인터페이스에서 디바이스를 나가는 트래픽과 일치됩니다. 일치하는 트래픽에서 침입 및 악성코드를 검사하려면 **Allow(**허용**)** 규칙 작업을 선택한 다음 해당 규칙을 침입 및 파일 정책과 연결합니다.

애플리케이션 사용량을 제어하는 방법

웹은 기업에 애플리케이션을 제공하는 데 흔히 사용되는 플랫폼으로 자리잡았습니다. 브라우저 기반 애플리케이션 플랫폼이 사용될 수도 있고, 기업 네트워크 안팎으로 애플리케이션을 전송하는 방법으로 웹 프로토콜을 사용하는 리치 미디어 애플리케이션이 사용될 수도 있습니다.

Threat Defense 연결을 검사하여 사용 중인 애플리케이션을 확인합니다. 따라서 특정 TCP/UDP 포트만 대상으로 하는 것이 아니라 애플리케이션을 대상으로 하는 액세스 제어 규칙을 작성할 수 있습니

다. 그러므로 같은 포트를 사용하는 웹 기반 애플리케이션도 선택적으로 허용하거나 차단할 수 있습니다.

허용하거나 차단할 특정 애플리케이션을 선택할 수도 있지만, 유형/범주/태그/위험/사업 타당성을 기준으로 규칙을 작성할 수도 있습니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

이 활용 사례에서는 익명성 도구/프록시 범주에 속하는 모든 애플리케이션을 차단합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택하고 액세스 제어 정책을 편집합니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭하고 애플리케이션 제어를 위한 규칙을 구성합니다.

a) Block_Anonymizers와 같이 의미 있는 이름을 규칙에 지정합니다.

b) **Action(**작업**)**에 대해 **Block(**차단**)**을 선택합니다.

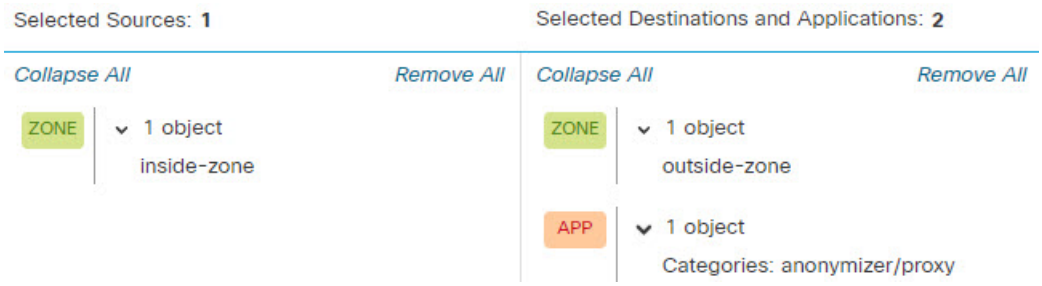
c) 영역을 구성했으며 이 규칙을 내부에서 외부로 이동하는 트래픽에 적용하려면 **Zones(**영역**)** 탭을 선택하고 내부 영역을 소스 영역으로 선택하고 외부 영역을 대상 영역으로 선택합니다.

d) **Applications(**애플리케이션**)** 탭을 클릭하고 일치시킬 애플리케이션을 선택한 다음 **Add Application(**애플리케이션 추가**)**을 클릭합니다.

범주 및 위험 수준과 같은 기준을 선택하면 기준과 일치하는 애플리케이션을 정확하게 표시하도록 기준 오른쪽의 목록이 업데이트됩니다. 작성하는 규칙은 이러한 애플리케이션에 적용됩니다.

이 목록을 자세히 확인하십시오**.** 예를 들어 위험도가 매우 높은 애플리케이션은 모두 차단하는 경우가 많습니다. 하지만 이 문서를 작성하는 시점에서 TFTP는 위험도가 매우 높은 위험으로 분류됩니다. 대부분의 조직은 이 애플리케이션을 차단하기를 원치 않을 것입니다. 시간을 할애하여 다양한 필터 기준을 적용해 보고 선택한 필터와 일치하는 애플리케이션을 확인하십시오. 이러한 목록은 VDB가 업데이트될 때마다 변경될 수 있습니다.

이 예에서는 범주 목록에서 익명성 도구/프록시를 선택하고 대상 및 애플리케이션에 추가합니다. 이제 일치 기준이 다음 그림과 같이 표시됩니다.



e) 규칙 작업 옆에 있는 **Logging(**로깅**)**을 클릭하고 연결 시작 시 로깅을 활성화합니다. 사용하는 경우 시스템 로그 서버를 선택할 수 있습니다.

이 규칙에 의해 차단되는 연결에 대한 정보를 확인하려면 로깅을 활성화해야 합니다.

단계 **3** 프로토콜 및 포트 기준만 사용하지만 애플리케이션 규칙에 의해 차단되어야 하는 트래픽은 허용하지 않는 규칙 뒤에 오도록 규칙을 이동합니다.

일치하는 애플리케이션에는 Snort 검사가 필요합니다. 프로토콜 및 포트만 사용하는 규칙에는 Snort 검사가 필요하지 않으므로 액세스 제어 정책의 맨 위에 이러한 간단한 규칙을 가능한 한 많이 그룹화하여 시스템 성능을 개선할 수 있습니다.

단계 **4** 변경 사항을 구축하고

애플리케이션 규칙 적중 횟수 및 분석 대시보드를 사용하여 이 규칙의 성능 및 사용자가 이러한 애플리케이션을 시도하는 빈도를 확인할 수 있습니다.

위협을 차단하는 방법

액세스 제어 규칙에 침입 정책을 추가하여 차세대 IPS(침입 방지 시스템) 필터링을 구현할 수 있습니다. 침입 정책은 네트워크 트래픽을 분석하여 트래픽 콘텐츠와 알려진 위협을 비교합니다. 연결이 모니터링 대상 위협과 일치하는 경우 시스템은 연결을 삭제하여 공격을 방지합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입을 검사하기 전에 수행됩니다. 침입 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책을 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 **allow(**허용**)**하는 규칙에 대해서만 침입 정책을 구성할 수 있습니다. 트래픽을 **trust(**신뢰**)** 또는 **block(**차단**)**하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한 단순 차단을 사용하지 않으려는 경우 침입 정책을 기본 작업으로 구성할 수 있습니다.

허용하는 트래픽의 침입 가능성을 검사하는 것 외에, 보안 인텔리전스 정책을 사용하여 알려진 잘못된 IP 주소에서 나가거나 들어오는 모든 트래픽이나 알려진 잘못된 URL로 나가는 모든 트래픽을 사전에 차단할 수 있습니다.

이 예에서는 내부 192.168.1.0/24 네트워크의 외부 액세스를 허용하는 침입 정책을 추가하고, 원치 않는 연결을 선택적으로 제거하는 차단 규칙이 이미 있는 것으로 가정하고, 사전 차단을 수행하는 보안 인텔리전스 정책도 추가합니다.

시작하기 전에

이 규칙을 사용하는 모든 매니지드 디바이스에 IPS 라이선스를 적용해야 합니다.

이 예에서는 내부 및 외부 인터페이스에 대한 보안 영역과 내부 네트워크에 대한 네트워크 개체를 이미 생성했다고 가정합니다.

프로시저

단계 **1** 침입 정책을 적용하는 액세스 제어 규칙을 생성합니다.

a) 액세스 제어 정책 편집기에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 규칙에 의미 있는 이름(예: Inside_Outside)을 지정하고 규칙 작업이 **Allow(**허용**)**인지 확인합니다.

c) **Intrusion Policy(**침입 정책**)**의 경우 Balanced Security and Connectivity(보안과 연결의 균형 유지)를 선택합니다. 기본 변수 집합을 수락하거나 사용자 지정하려는 경우 직접 선택할 수 있습니다.

Balanced Security and Connectivity(보안과 연결의 균형 유지**)** 정책은 대부분의 네트워크에 적합합니다. 이 정책은 과도하게 적극적이지 않은 적절한 침입 방어 기능을 제공합니다. 침입 방지 기능이 너무 적극적이면 삭제되면 안 되는 트래픽이 삭제될 수 있습니다. 트래픽이 너무 많이 삭제되는지 확인하려는 경우 **Connectivity over Security(**연결이 보안에 우선함**)** 정책을 선택하여 침입 검사의 레벨을 높일 수 있습니다.

적극적인 보안을 적용해야 하는 경우에는 **Security over Connectivity(**보안이 연결에 우선함**)** 정책을 사용해 보십시오. **Maximum Detection(**최대 탐지**)** 정책은 네트워크 인프라 보안을 더욱 강화하며, 사용하는 경우 운영에 더 큰 영향을 미칠 수 있습니다.

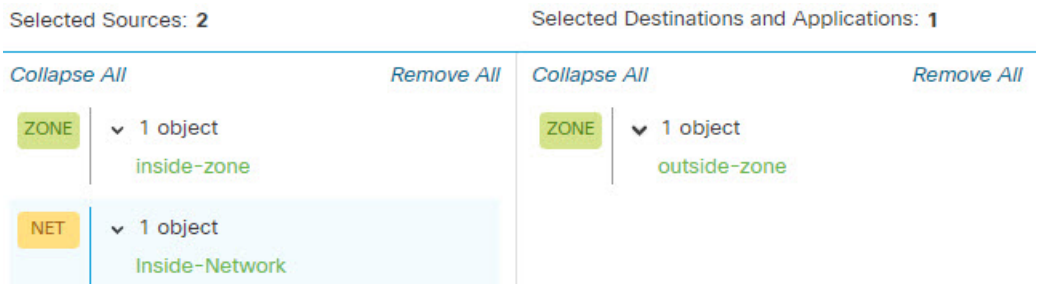
고유한 사용자 지정 정책을 생성하는 경우 해당 정책을 대신 선택할 수 있습니다.

변수 집합에 대한 설명은 이 예의 범위를 벗어납니다. 변수 집합 및 사용자 지정 정책에 대한 자세한 내용은 침입 정책 장을 참조하십시오.

d) **Zones(**영역**)** 탭을 선택하고 소스 기준에 내부 보안 영역을 추가하고 대상 기준에 외부 영역을 추가합니다.

e) **Networks(**네트워크**)** 탭을 선택하고 내부 네트워크를 정의하는 네트워크 개체를 소스 기준에 추가합니다.

일치 기준은 다음과 유사해야 합니다.



f) **Logging(**로깅**)**을 클릭하고 필요에 따라 연결 시작 또는 종료 시 또는 둘 다에서 로깅을 활성화합니다.

g) **Apply(**적용**)**를 클릭하여 규칙을 저장한 다음 **Save(**저장**)**를 클릭하여 업데이트된 정책을 저장합니다.

h) 규칙을 액세스 제어 정책의 적절한 위치로 이동합니다.

단계 **2** 알려진 잘못된 호스트 및 사이트와의 연결을 사전에 삭제하도록 보안 인텔리전스 정책을 구성합니다.

보안 인텔리전스를 사용하여 위협으로 알려진 호스트 또는 사이트와의 연결을 차단하면 시스템이 DPI(Deep Packet Inspection)를 수행하여 각 연결의 위협을 식별하는 데 필요한 시간을 절약할 수 있습니다. 보안 인텔리전스를 사용하면 원치 않는 트래픽을 일찍 차단할 수 있으므로 시스템이 실제로 중요한 트래픽을 처리하는 데 더 많은 시간을 할애할 수 있습니다.

a) 액세스 제어 정책을 편집하는 동안 패킷 경로에서 **Security Intelligence** 링크를 클릭합니다.

이 링크에는 두 개의 정책, 즉 상단의 DNS 정책과 하단의 보안 인텔리전스(네트워크 및 URL)가 포함되어 있습니다. 이 예에서는 네트워크 및 URL 목록을 구성합니다. 기본적으로 이러한 목록에는 이미 전역 차단 및 차단 안 함 목록이 포함되어 있지만, 항목을 추가할 때까지 이러한 목록은 기본적으로 비어 있습니다.

b) **Networks(**네트워크**)**를 선택하고 **Any(**모든**)** 보안 영역을 선택한 상태에서 전역 목록과 첫 번째 보안 인텔리전스 범주(아마도 공격자)가 나올 때까지 목록에서 아래로 스크롤합니다. Attackers(공격자)를 클릭한 다음 범주 끝까지 스크롤한 다음(Tor_exit_node) Shift+클릭하여 모든 범주를 선택합니다. **Add To Block List(**차단 목록에 추가**)**를 클릭합니다.

c) **URL** 탭 및 **Any(**모든**)** 보안 영역을 선택하고 Shift+클릭을 사용하여 동일한 범주의 URL 버전을 선택합니다. **Add To Block List(**차단 목록에 추가**)**를 클릭합니다.

d) **Save**를 클릭하여 정책을 저장합니다.

e) 필요에 따라 차단 또는 차단 안 함 목록에 네트워크 및 URL 개체를 추가할 수 있습니다.

Do Not Block(차단 안 함**)** 목록은 실제 "허용" 목록이 아닙니다. 예외 목록입니다. 예외 목록의 주소나 URL이 차단 목록에도 나타나는 경우 해당 주소나 URL에 대한 연결을 액세스 제어 정책으로 전달할 수 있습니다. 이 방법을 통해 특정 피드를 차단할 수 있습니다. 그러나 원하는 주소나 사이트가 차단되고 있음이 나중에 확인되는 경우에는 피드를 완전히 제거할 필요 없이 예외 목록을 사용하여 해당 차단을 재정의할 수 있습니다. 이러한 연결은 나중에 액세스 제어 및 침입 정책(구성된 경우)을 통해 평가됩니다. 따라서 침입 검사 중에 위협을 포함하는 연결을 식별하여 차단할 수 있습니다.

이벤트 및 대시보드를 사용하여 정책에서 실제로 삭제하는 트래픽과 **Do Not Block(**차단 안 함**)** 목록에 주소 또는 URL을 추가해야 하는지 여부를 결정합니다.

단계 **3** 변경 사항을 배포합니다.

액세스 컨트롤 규칙 기록

기능	버전	세부 사항
액세스 제어 규칙당 일치 기준당 최대 개체 수는 200입니다.	7.3	이전에는 단일 액세스 제어 규칙에서 일치 기준당 최대 50개의 개체를 포함할 수 있었습니다. 예를 들어 단일 액세스 제어 규칙에 최대 50개의 네트워크 개체를 포함할 수 있습니다. 이제 단일 규칙에서 일치 기준당 200개의 개체로 제한됩니다. 증가된 개체 제한을 허용하도록 액세스 제어 정책을 업데이트했습니다.
액세스 제어 규칙 코멘트 검색	6.7	이제 **Search Rules(**검색 규칙**)** 표시줄에 코멘트를 검색할 수 있는 옵션이 제공됩니다. 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지, **Search Rules(**검색 규칙**)** 텍스트 입력 필드 지원되는 플랫폼: management center
액세스 제어 및 사전 필터 정책 간에 규칙 복사 또는 이동	6.7	액세스 제어 규칙을 한 액세스 제어 정책에서 다른 액세스 제어 정책으로 복사할 수 있습니다. 액세스 제어 규칙을 액세스 제어 정책에서 연결된 사전 필터 정책으로 이동할 수도 있습니다. 신규/수정된 페이지: Access control policy(액세스 제어 정책) 페이지 - 선택한 규칙에 대해 마우스 오른쪽 버튼을 클릭하면 복사 및 이동에 대한 추가 옵션이 제공됩니다. 지원되는 플랫폼: management center
액세스 제어 규칙에서 특정 설정 대량 편집	6.6	정책의 규칙 목록에서 Shift 키나 Control 키를 누른 상태에서 클릭하여 여러 규칙을 선택한 다음 마우스 오른쪽 버튼을 클릭하여 옵션을 선택합니다. 대량 작업으로는 규칙 활성화 또는 비활성화, 규칙 작업 선택, 대부분의 검사 및 로깅 설정 편집을 예로 들 수 있습니다. 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지 지원되는 플랫폼: management center
설정된 규칙에 대한 향상된 검색	6.6	설정된 규칙에 대한 검색을 개선했습니다. 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지 지원되는 플랫폼: management center

기능	버전	세부 사항
규칙 애플리케이션의 시간 범위	6.6	적용할 규칙에 대해 절대적이거나 반복되는 시간 또는 시간 범위를 지정할 수 있습니다. 규칙은 트래픽을 처리하는 디바이스의 표준 시간대에 따라 적용됩니다. 신규/수정된 페이지: • Access Control Add Rule(액세스 제어 규칙 추가) 페이지의 새로운 옵션 • 매니지드 디바이스의 표준 시간대를 지정하기 위한 **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**) > Threat Defense(**위협 방어**)** 페이지의 관련 새 옵션. 지원되는 플랫폼: threat defense 디바이스 전용
Access control rules(액세스 제어 규칙) 페이지에서 개체 세부 사항 보기	pre-6.6	규칙 목록 또는 규칙 설정 대화 상자에서 개체에 대한 정보를 보려면 개체를 마우스 오른쪽 버튼으로 클릭합니다. 신규/수정된 페이지: **Policies(**정책**) > Access Control(**액세스 제어**) > Access Control(**액세스 제어**)** 및 **Add Rule(**규칙 추가**)** 페이지 지원되는 플랫폼: management center

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