액세스 제어 개요

액세스 제어 소개

액세스 제어는 빠른 경로가 아닌 네트워크 트래픽을 지정하고, 검사하고 로깅할 수 있는 정책 기반 기능입니다.

각 매니지드 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 네트워크 트래픽에 대한 정책의 대상 디바이스가 수집하는 정보를 사용하여 다음을 기반으로 트래픽을 필터링 및 제어할 수 있습니다.

- 소스와 목적지, 포트, 프로토콜 등 간단하고 쉽게 결정되는 전송 및 네트워크 레이어 특성
- 평판, 위험, 비즈니스 관련성, 사용된 애플리케이션 또는 방문한 URL 등의 특성을 비롯하여 트래픽에 대한 최신 상황 정보
- 영역, 사용자, 사용자 그룹 또는 ISE 속성
- 맞춤형 SGT(Security Group Tag)
- 암호화된 트래픽의 특성(추가 분석을 위해 이 트래픽을 해독할 수도 있음)
- 암호화되지 않은 또는 해독된 트래픽에 금지된 파일, 탐지된 악성코드 또는 침입 시도가 포함되었는지 여부
- 시간 및 요일(지원되는 디바이스)

각 유형의 트래픽 검사와 제어는 유연성과 성능을 최대화할 수 있는 방식으로 발생합니다. 예를 들어, 평판에 기반한 차단은 단순한 소스 및 대상 데이터를 사용하므로 프로세스 초기에 금지된 트래픽을 차단할 수 있습니다. 반면, 침입과 익스플로잇의 탐지 및 차단은 최후의 방어 수단입니다.

규칙 소개

다양한 정책 유형(액세스 제어, SSL, ID 등)의 규칙은 네트워크 트래픽에 대해 세분화된 제어를 시행합니다. 시스템은 사용자가 지정한 순서에 따라 첫 번째 일치 알고리즘을 사용해 규칙에 대한 트래픽을 평가합니다.

이러한 규칙은 다음과 같은 기본 특성 및 설정 메커니즘을 공유하는 일치하지 않는 정책 간의 다른 설정을 포함할 수 있습니다.

- 조건: 규칙 조건은 각 규칙을 처리하는 특정 트래픽을 지정합니다. 규칙마다 여러 조건을 구성할 수 있습니다. 트래픽은 규칙과 일치하는 모든 조건과 일치해야 합니다.
- 작업: 규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 규칙에 선택할 수 있는 작업 목록이 포함되지 않더라도 규칙과 관련된 작업이 있습니다. 예를 들어 사용자 지정 네트워크 분석 규칙은 "작업"으로 네트워크 분석 정책을 사용합니다. 다른 예로 모든 QoS 규칙이 동일하게 제한 트래픽을 평가하므로 QoS 규칙에는 명시적인 작업이 없습니다
- 위치: 규칙의 위치는 평가 순서를 결정합니다. 트래픽 평가에 정책을 사용할 경우 시스템은 트래픽이 사용자가 지정한 순서에 따른 규칙과 일치하는지 확인합니다. 일반적으로 시스템은 모든 규칙 조건이 트래픽과 일치하는 첫 번째 규칙에 따라 트래픽을 처리합니다. (추적 및 기록용인 모니터링 규칙은 예외입니다.) 적절한 규칙 순서는 네트워크 트래픽 처리에 필요한 리소스를 줄여 규칙 선점을 방지합니다.
- 범주: 일부 규칙 유형을 구조화하기 위해 각 상위 정책에서 사용자 지정 규칙 카테고리를 만들 수 있습니다.
- 로깅: 많은 규칙의 경우 로깅 설정은 규칙에 의해 처리되는 시스템 로그 연결 여부 및 그 방법을 제어합니다. 규칙이 최종 연결 속성을 결정하거나 특별히 연결을 기록하도록 되어있지 않으므로 일부 규칙(ID 및 네트워크 분석 규칙 등)은 로깅 설정을 포함하지 않습니다. 다른 예로 QoS 규칙은 로깅 설정을 포함하지 않습니다. 속도 제한이 있으므로 연결 기록을 할 수 없습니다.
- 설명: 일부 규칙 유형은 변경 사항을 저장할 때마다 설명을 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다.

팁 여러 정책 편집기의 오른쪽 클릭 메뉴는 편집, 삭제, 이동, 활성화 및 비활성화를 비롯해 많은 규칙 관리 옵션에 대한 바로 가기를 제공합니다.

자세한 내용은 관심 있는 규칙(예: 액세스 제어 규칙)을 설명하는 장을 참조하십시오.

관련 항목

애플리케이션 조건 및 필터 구성

애플리케이션 제어 모범 사례, 11 페이지

디바이스별 규칙 필터링

일부 정책 편집기를 사용하면 영향 받는 디바이스에 따른 규칙 보기를 필터링할 수 있습니다.

시스템은 규칙의 인터페이스 제약 조건을 사용하여 규칙이 디바이스에 영향을 미치는지 결정합니다. (보안 영역 또는 인터페이스 그룹 조건) 인터페이스로 규칙을 제한하는 경우, 해당 인터페이스가 위치한 디바이스는 해당 규칙에 영향을 받습니다. 인터페이스 제약 조건이 없는 규칙은 모든 인터페이스에 적용되므로 모든 디바이스에 적용됩니다.

QoS 규칙은 항상 인터페이스에 의해 제한됩니다.

참고 다음 절차는 액세스 제어 정책에 적용되지 않습니다. 액세스 제어 정책에서 특정 디바이스 또는 디바이스 집합에 적용되는 규칙을 보려면 필터 아이콘을 클릭하고 디바이스를 선택합니다.

프로시저

단계 **1** 정책 편집기에서 **Rules(**규칙**)**를 클릭하고 **Filter by Device(**디바이스로 필터링**)**를 클릭합니다.
대상 디바이스 및 디바이스 그룹의 목록이 표시됩니다.

단계 **2** 이런 디바이스 또는 그룹에 적용되는 규칙만을 표시하려면 하나 이상의 체크 박스에 체크합니다. 또는 재설정하여 모든 규칙을 표시하려는 경우 모두를 체크합니다.

팁 해당 값을 확인하려면 규칙 기준으로 마우스 포인터를 이동합니다. 기준이 디바이스 한정 오버라이드가 포함된 개체를 나타내는 경우 시스템은 해당 디바이스에 한정한 규칙 목록을 필터링할 때 오버라이드 값을 표시합니다. 기준이 도메인 한정 오버라이드가 포함된 개체를 나타내는 경우 시스템은 해당 도메인의 디바이스의 규칙 목록을 필터링할 때 오버라이드 값을 표시합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

규칙 및 기타 정책 경고

정책 및 규칙 편집기는 아이콘을 사용하여 트래픽 분석 및 흐름에 부정적인 영향을 미칠 수 있는 설정을 표시합니다. 문제에 따라 구축 시 시스템이 경고하거나 완전 구축을 차단할 수 있습니다.

팁 경고, 오류 또는 정보를 제공하는 텍스트를 읽을 아이콘에 마우스 포인터를 놓습니다.

표 *1:* 정책 오류 아이콘

아이콘	설명	예
Error(오류**)** ()	규칙 또는 설정에 오류가 있는 경우, 영향을 받는 규칙을 비활성화해도 문제를 수정하기 전까지는 구축할 수 없습니다.	카테고리 및 평판 기반 URL 필터링을 수행하는 규칙은 URL 필터링 라이선스가 없는 디바이스를 대상으로 하기 전까지 유효합니다. 이 경우 규칙 옆에 오류 아이콘이 표시되며 규칙을 편집 또는 삭제하거나 정책의 대상을 다시 설정하거나 라이선스를 활성화하기 전까지 구축할 수 없습니다.
Warning(경고**)** ()	규칙 또는 다른 경고를 표시하는 정책을 구축할 수 있습니다. 그러나, 경고가 표시된 오류 구성은 적용되지 않습니다. 경고가 표시된 규칙을 비활성화하는 경우, 경고 아이콘이 사라집니다. 경고 아이콘은 근본적인 문제를 해결하지 않고 규칙을 활성화하는 경우 다시 나타납니다.	선점된 규칙 또는 설정 오류로 트래픽과 일치하지 않는 규칙은 효과가 없습니다. 이는 제외된 LDAP 사용자, 유효하지 않은 포트 등 애플리케이션과 일치하지 않는 빈 개체 그룹, 애플리케이션 필터를 사용한 조건을 포함합니다. 그러나 경고 아이콘이 라이선싱 오류 또는 모델 불일치를 표시하는 경우 해당 문제를 해결하기 전까지 구축할 수 없습니다.
Information(정보**)** ()	정보 아이콘은 트래픽의 흐름에 영향을 줄 수 있는 구성에 대한 유용한 정보를 제공합니다. 이 문제는 구축을 방해하지 않습니다.	시스템이 해당 연결에서 애플리케이션 또는 웹 트래픽을 식별할 때까지 일부 규칙에 어긋나는 처음 몇몇 연결 패킷을 일치시키는 작업을 건너뛸 수 있습니다. 이는 애플리케이션 및 HTTP 요청을 확인할 수 있도록 연결을 설정할 수 있게 합니다.
Rule Conflict(규칙 충돌**)** ()	규칙 충돌 분석을 활성화하면 충돌이 있는 규칙에 대한 규칙 테이블에 이 아이콘이 나타납니다.	충돌에는 중복 규칙, 중복 개체 및 숨겨진 규칙이 포함됩니다. 이전 규칙이 이미 기준과 일치했기 때문에 이중화 및 섀도우 규칙은 트래픽과 일치하지 않습니다. 중복 개체는 규칙을 불필요하게 복잡하게 만듭니다.

액세스 제어 정책 기본 작업

새로 생성된 액세스 제어 정책은 기본 작업을 사용하여 모든 트래픽을 처리하도록 대상 디바이스에 지시합니다.

간단한 액세스 제어 정책에서 기본 작업은 대상 디바이스가 모든 트래픽을 처리하는 방법을 지정합니다. 보다 복잡한 정책에서 기본 작업은 다음과 같은 트래픽을 처리합니다.

- IAB(Intelligent Application Bypass)가 신뢰하지 않는 트래픽
- 보안 인텔리전스 차단 목록 제외
- SSL 검사에서 차단되지 않은 트래픽(암호화된 트래픽만 해당)

- 정책 내 규칙 중 어느 것과도 일치하지 않는 것입니다(트래픽에 일치시키거나 트래픽을 로깅하지만 처리하거나 검사하지는 않는 모니터링 규칙은 제외).

액세스 제어 정책 기본 작업을 사용하여 추가 검사 없이 트래픽을 차단하거나 신뢰할 수 있고, 침입 및 검색 데이터 트래픽을 검사할 수 있습니다.

참고 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다. 기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화되어 있지만 활성화할 수는 있습니다.

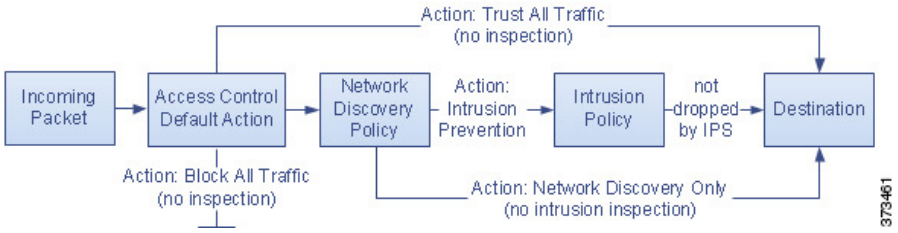
정책 상속을 사용하는 경우 가장 낮은 수준의 하위 항목에 대한 기본 작업에 따라 최종 트래픽 처리가 결정됩니다. 액세스 제어 정책은 기본 정책에서 기본 작업을 상속할 수 있지만 이 상속을 적용할 수는 없습니다.

다음 표는 각 기본 작업에 의해 처리된 트래픽에서 수행할 수 있는 검사 유형을 나열합니다.

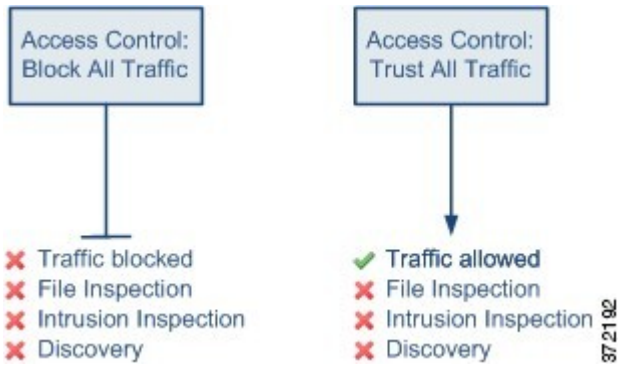
표 *2:* 액세스 제어 정책 기본 작업

기본 작업	트래픽에 미치는 영향	검사 유형 및 정책
액세스 제어: 모든 트래픽 차단	추가 검사 없이 차단	없음
액세스 제어: 모든 트래픽 신뢰	신뢰(추가 검사 없이 최종 대상에서 허용)	없음
침입 방지	허용. 사용자가 지정한 침입 정책에 의해 통과된 경우	지정된 침입 정책 및 관련 변수 집합을 사용한 침입 및 네트워크 검색 정책을 사용한 검색
네트워크 검색 한정	허용	네트워크 검색 정책을 사용한 검색만 해당
기본 정책에서 상속	기본 정책에 정의됨	기본 정책에 정의됨

다음 다이어그램은 테이블을 보여 줍니다.



다음 다이어그램은 **Block All Traffic(**모든 트래픽 차단**)** 및 **Trust All Traffic(**모든 트래픽 신뢰**)** 기본 작업을 설명합니다.



다음 다이어그램은 **Intrusion Prevention(**침입 방지**)** 및 **Network Discovery Only(**네트워크 검색 한정**)** 기본 작업을 설명합니다.

팁 **Network Discovery Only**의 목적은 검색 전용 구축 작업의 성능을 향상하는 것입니다. 침입 탐지 및 방지만 사용하려는 경우 다른 구성으로 검색을 비활성화할 수 있습니다.

파일 및 침입 정책을 사용한 심층 검사

심층 검사는 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로서 침입 및 파일 정책을 사용합니다.

- 침입 정책은 시스템의 침입 방지 기능을 제어합니다.

  자세한 내용은 침입 탐지 및 방지를 참조하십시오.

- 파일 정책은 시스템의 파일 제어 및 악성코드 대응 기능을 제어합니다.

  자세한 내용은 네트워크 악성코드 보호 및 파일 정책를 참조하십시오.

액세스 제어는 심층 검사 전에 이루어집니다. 액세스 제어 규칙 및 액세스 제어 기본 작업은 정책 및 파일 정책으로 어떤 트래픽을 검사할지 결정합니다.

침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽이 통과하기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 우선 트래픽을 검사하도록 할 수 있습니다.

액세스 제어 정책에서는 하나의 침입 정책을 각 허용 및 인터랙티브 차단 규칙 및 기본 작업과 연결할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다.

침입 및 파일 정책을 액세스 제어 규칙과 결합하려면 다음을 확인합니다.

- 침입 방지를 수행하는 액세스 제어 규칙 설정
- 악성코드 보호를 수행하는 액세스 제어 규칙 구성

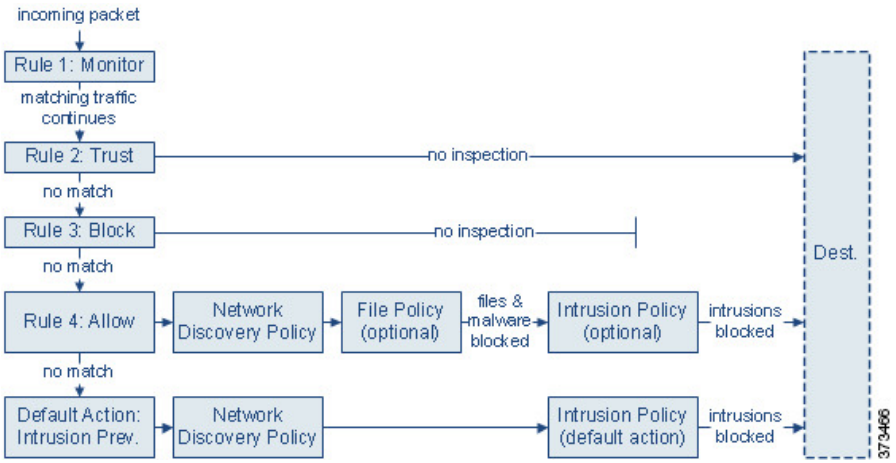
참고 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

관련 항목

정책이 트래픽에서 침입을 검토하는 방법
파일 정책

침입 정책 및 파일 정책을 사용한 액세스 제어 트래픽 처리

다음 다이어그램에는 네 가지 다른 유형의 액세스 제어 규칙 및 기본 작업이 포함된 액세스 제어 정책으로 제어되는 인라인 침입 방지 및 악성코드 대응 구축 시 트래픽의 흐름이 나와 있습니다.



위 시나리오에서 정책의 처음 세 액세스 제어 규칙(모니터, 신뢰, 차단)은 일치하는 트래픽을 검사할 수 없습니다. 모니터 규칙은 네트워크 트래픽을 추적하고 로깅하지만 검사하지는 않으므로 시스템은 트래픽을 추가 규칙과 계속 대조하여 트래픽을 허용할지 거부할지 결정합니다. (액세스 제어 규칙 모니터 작업에서 중요 예외 및 주의 사항을 확인하십시오.) 신뢰 및 차단 규칙은 어떠한 종류의 추가 검사 없이도 일치하는 트래픽을 처리하지만 일치하지 않는 트래픽은 다음 액세스 제어 규칙으로 계속 진행합니다.

정책의 네 번째이자 마지막 규칙인 허용 규칙은 다양한 다른 정책을 호출하여 다음과 같은 순서로 일치하는 트래픽을 검사하고 처리합니다.

- 검색**:** 네트워크 검색 정책 - 우선 네트워크 검색 정책은 검색 데이터에 대해 트래픽을 검사합니다. 검색은 수동 분석이며 트래픽 흐름에 영향을 미치지 않습니다. 검색을 명시적으로 활성화하지 않더라도 검색을 강화하거나 비활성화할 수 있습니다. 그러나 트래픽을 허용한다고 해서 자동으로 검색 데이터 수집이 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에서 명시적으로 모니터링하는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다.
- 악성코드 대응 및 파일 제어**:** 파일 정책 - 검색에 의해 트래픽이 검사된 후 시스템은 트래픽에서 금지된 파일과 악성코드를 검사할 수 있습니다. 악성코드 대응 는 PDF, Microsoft Office 문서 등을 포함한 여러 파일 형식에서 악성코드를 탐지하고 선택적으로 차단할 수 있습니다. 조직에서 악성코드 파일의 전송뿐만 아니라 특정 유형의 모든 파일(해당 파일의 악성코드 포함 여부에 상관없이)을 차단하려는 경우, 파일 제어를 사용하면 특정 파일 유형의 전송에 대해 네트워크 트래픽을 모니터링한 다음 해당 파일을 차단하거나 허용할 수 있습니다.
- 침입 방지**:** 침입 정책 - 파일 검사 후 시스템에서는 침입 및 익스플로잇에 대해 트래픽을 검사할 수 있습니다. 침입 정책은 패턴을 기반으로 디코딩된 패킷에서 공격을 검사하며 악의적인 트래픽을 차단하거나 변경할 수 있습니다. 침입 정책은 변수 집합과 페어링되는데, 이를 통해 네트워크 환경을 올바르게 반영하는 지정된 값을 사용할 수 있습니다.
- 대상 - 위에 설명된 모든 확인을 통과하는 트래픽은 대상에 도달합니다.

인터랙티브 차단 규칙(다이어그램에 표시되지 않음)에는 허용 규칙과 동일한 검사 옵션이 있습니다. 이를 사용하면 사용자가 경고 페이지를 클릭하여 차단된 웹 페이지를 우회할 경우 악의적인 콘텐츠에 대해 트래픽을 검사할 수 있습니다.

모니터링을 제외한 작업을 이용하는 정책의 액세스 제어 규칙과 일치하지 않는 트래픽은 기본 작업에 의해 처리됩니다. 이 시나리오에서 기본 작업은 사용자가 지정한 침입 정책에서 통과시키는 트래픽이 최종 대상에 도달하도록 허용하는 침입 방지 작업입니다. 다른 구축에는 추가 검사 없이 모든 트래픽을 신뢰하거나 차단하는 기본 작업이 있을 수 있습니다. 시스템은 기본 작업에서 허용하는 트래픽에 대해 검색 데이터 및 침입 여부를 검사할 수 있으나, 금지된 파일 또는 악성코드 여부는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 없습니다.

참고 액세스 제어 정책으로 연결을 분석할 경우, 시스템에서는 어떤 액세스 제어 규칙(있는 경우)으로 트래픽을 처리할 것인지 결정하기 전에 해당 연결의 처음 몇 가지 패킷을 처리하여, 통과되도록 허용해야 합니다. 그러나 이러한 패킷이 검사되지 않은 상태로 대상에 도달하지 않도록 침입 정책(액세스 제어 정책의 고급 설정)을 지정하여 해당 패킷을 검사하고 침입 이벤트를 생성할 수 있습니다.

파일 및 침입 검사 순서

액세스 제어 정책에서 여러 허용 및 인터랙티브 차단 규칙을 다양한 침입 및 파일 정책에 연결하여 검사 프로파일과 다양한 트래픽 유형을 대조할 수 있습니다.

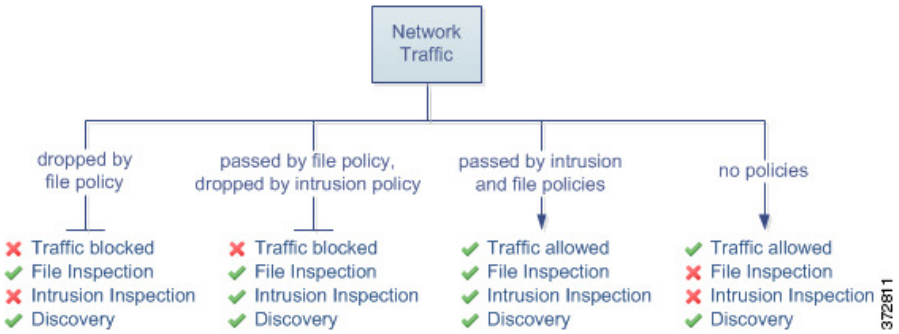
참고 트래픽이 침입 방지 또는 네트워크 검색 한정 기본 작업에 의해 허용된 경우 검색 데이터 및 침입은 검사할 수 있지만, 금지된 파일 또는 악성코드는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 없습니다.

동일한 규칙에서 파일 및 침입 검사를 모두 수행할 필요는 없습니다. Allow or Interactive Block(허용 또는 인터랙티브 차단) 규칙과 일치하는 연결의 경우:

- 파일 정책이 없는 경우, 트래픽 흐름은 침입 정책에 의해 결정됨
- 침입 정책이 없는 경우, 트래픽 흐름은 파일 정책에 의해 결정됨
- 두 가지 정책이 모두 없는 경우, 허용되는 트래픽은 네트워크 검색 한정에 의해 검사됨

팁 시스템은 신뢰할 수 있는 트래픽에는 검사를 수행하지 않습니다. 침입 또는 파일 정책 없이 허용 규칙을 구성하면 트래픽을 신뢰 규칙처럼 통과시키지만 허용 규칙을 통해 일치하는 트래픽에서 검색을 수행할 수 있습니다.

아래 다이어그램은 허용 규칙 또는 사용자가 우회한 인터랙티브 차단 규칙의 조건을 충족하는 트래픽에서 수행할 수 있는 검사 유형을 보여줍니다. 간단한 설명을 위해 다이어그램에는 침입 정책과 파일 정책 모두 단일 액세스 제어 규칙에 연결되거나 모두 연결되지 않은 상황의 트래픽 흐름을 보여줍니다.



액세스 제어 규칙으로 처리되는 단일한 연결의 경우, 침입 검사 전에 파일 검사가 이루어집니다. 즉, 시스템에서는 파일 정책 또는 침입에 의해 차단된 파일은 검사하지 않습니다. 파일 검사 내에서 유형을 기준으로 한 간단한 차단은 악성코드 검사 및 차단보다 우선합니다.

예를 들어, 액세스 제어 규칙에 정의된 대로 특정 네트워크 트래픽을 일반적으로 허용하고자 하는 시나리오를 가정해보겠습니다. 그러나 일종의 예방 조치로서 실행 파일의 다운로드를 차단하고, 다운로드된 PDF의 악성코드 여부를 검사하고 검색된 모든 인스턴스를 차단하며, 트래픽에 침입 검사를 수행하고자 합니다.

일시적으로 허용하고자 하는 트래픽의 특성과 일치하는 규칙으로 액세스 제어 정책을 생성하고 이를 침입 정책과 파일 정책에 모두 연결합니다. 파일 정책은 모든 실행 파일의 다운로드를 차단하며, 검사를 수행하고 악성코드가 포함된 PDF를 차단합니다.

- 우선 시스템에서는 파일 정책에 지정된 것과 일치하는 간단한 유형을 기준으로 모든 실행 파일의 다운로드를 차단합니다. 이러한 파일은 즉시 차단되기 때문에 악성코드 또는 침입 검사 대상에서 제외됩니다.
- 그다음, 시스템에서는 네트워크의 호스트에 다운로드된 PDF에 악성코드 클라우드 조회를 수행합니다. 악성코드 속성이 포함된 모든 PDF 파일은 차단되며 침입 검사 대상에서 제외됩니다.
- 마지막으로, 시스템에서는 액세스 제어 규칙과 연결된 침입 정책을 사용하여 모든 나머지 트래픽을 검사하며 여기에는 파일 정책으로 차단되지 않은 파일이 포함됩니다.

참고 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 수 있습니다.

액세스 제어 정책 상속

다중 도메인 구축에서 특히 유용하며 액세스 제어 정책을 중복할 수 있습니다. 각 정책은 상위(또는 기본) 정책의 규칙 및 설정을 상속합니다. 이 상속을 적용하거나 하위 정책을 허용하여 해당 상위 항목을 재정의할 수 있습니다.

액세스 컨트롤은 계층적 정책 기반 실행을 사용합니다. 도메인 계층을 생성하는 것처럼 액세스 제어 정책의 해당 계층을 생성할 수 있습니다. 하위 항목 또는 차일드, 액세스 제어 정책은 직속 부모 또는 기본 정책으로부터 규칙과 설정을 상속합니다. 기본 정책은 다른 부모 정책으로부터 규칙과 설정을 상속 받았을 수 있습니다.

액세스 제어 정책의 규칙은 상위 정책의 Mandatory(필수) 및 Default(기본값) 규칙 섹션 사이에 중첩됩니다. 이 구현은 상위 정책의 필수 규칙을 적용하지만 현재 정책이 상위 정책의 기본 규칙을 선점하는 규칙을 작성하도록 허용합니다.

다음 설정을 잠금 처리하여 모든 하위 정책에서 적용할 수 있습니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

- 보안 인텔리전스 - IP 주소, URL 및 도메인 이름에 대한 최신 평판 인텔리전스를 기반으로 연결을 허용하거나 차단합니다.
- HTTP 응답 페이지 - 사용자의 웹 사이트 요청을 차단할 때 사용자 정의 또는 시스템 제공 응답 페이지를 표시합니다.
- 고급 설정 - 관련 하위 정책, 네트워크 분석 설정, 성능 설정 및 기타 일반 옵션을 지정합니다.

정책 상속을 사용하는 경우, 가장 낮은 수준의 하위 항목에 대한 기본 작업에 따라 최종 트래픽 처리가 결정됩니다. 액세스 제어 정책은 상위 정책에서 기본 작업을 상속할 수 있지만 이 상속을 적용할 수는 없습니다.

정책 상속 및 멀티 테넌시

액세스 컨트롤의 계층적 정책 기반 실행은 멀티 테넌시를 보완합니다.

일반적인 다중 도메인 구축에서 액세스 제어 정책 계층은 도메인 구조에 해당하며, 매니지드 디바이스에 최하위 수준 액세스 제어 정책을 적용합니다. 이 구현은 상위 도메인 수준에서 선택적 액세스 제어 적용을 허용하고 하위 도메인 관리자는 구축별 설정을 조정할 수 있습니다. (하위 도메인의 관리자를 제한하려면 정책 상속 및 적용을 단독으로 수행하지 말고 역할을 사용해야 합니다.)

예를 들어 조직의 전역 도메인 관리자는 전역 수준에서 액세스 제어 정책을 만들 수 있습니다. 그런 다음 기능별로 하위 도메인으로 구분된 모든 디바이스가 해당 전역 수준 정책을 기본 정책으로 사용하도록 요구할 수 있습니다.

하위 도메인 관리자가 Secure Firewall Management Center에 액세스하여 액세스 제어를 구성하면 전역 수준의 정책을 있는 그대로 배포할 수 있습니다. 또는 전역 수준 정책의 범위 내에서 하위 수준의 액세스 제어 정책을 만들고 구축할 수 있습니다.

참고 액세스 제어 상속 및 적용의 가장 유용한 구현이 멀티 테넌시를 보완하지만 단일 도메인 내에서 액세스 제어 정책의 계층 구조를 생성할 수 있습니다. 또한 모든 수준에서 액세스 제어 정책을 지정하고 구축할 수도 있습니다.

애플리케이션 제어 모범 사례

다음 주제에서는 액세스 제어 규칙을 사용하여 애플리케이션을 제어하기 위한 권장 모범 사례에 대해 설명합니다.

애플리케이션 제어 권장 사항

애플리케이션 제어와 관련해서 다음의 지침과 제한 사항에 유의해야 합니다.

적응형 프로파일링을 사용하는지 확인

적응형 프로파일을 사용하지 않고 기본 상태로 유지된 경우 액세스 제어 규칙은 애플리케이션 제어를 수행할 수 없습니다.

애플리케이션 탐지기 자동 활성화

탐지하려는 애플리케이션에 대해 탐지기를 사용하고 있지 않으면 시스템은 해당 애플리케이션에 대해 모든 시스템 제공 탐지기를 자동으로 사용합니다. 시스템 제공 탐지기가 없으면 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 대해 사용합니다.

애플리케이션이 식별되기 전에 통과해야 하는 패킷을 검사하도록 정책 설정

시스템은 다음의 두 가지 조건을 만족하지 않는 경우 인텔리전트 애플리케이션 우회(IAB) 및 속도 제한을 포함한 애플리케이션 제어를 수행할 수 없습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 시스템이 세션에서 애플리케이션 식별

이 식별은 3~5개 패킷 내에서 이루어지거나 트래픽이 암호화된 경우 SSL 핸드세이크의 서버 인증 교환 이후에 이루어져야 합니다.

중요! 시스템에서 이러한 초기 패킷을 검사하도록 하려면 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정의 내용을 참조하십시오.

초기 트래픽이 기타 모든 기준과는 일치하는데 애플리케이션 식별이 불완전한 경우 시스템은 패킷 통과 및 연결 설정 또는 SSL 핸드셰이크 완료를 허용합니다. 시스템은 식별을 완료하면 나머지 세션 트래픽에 적절한 작업을 적용합니다.

참고 시스템에서 서버를 인식하려면 서버가 애플리케이션의 프로토콜 요구 사항을 준수해야 합니다. 예를 들어 ACK가 예상될 때 ACK 대신 keep-alive 패킷을 전송하는 서버가 있는 경우 해당 애플리케이션이 식별되지 않을 수 있으며 연결이 애플리케이션 기반 규칙과 일치하지 않습니다. 대신, 일치하는 다른 규칙 또는 기본 작업에 의해 처리됩니다. 이는 허용하려는 연결이 대신 거부될 수 있음을 의미할 수 있습니다. 이 문제가 발생하고 프로토콜 표준을 따르도록 서버를 수정할 수 없는 경우, 예를 들어 IP 주소 및 포트 번호를 일치시켜 해당 서버에 대한 트래픽을 다루는 비 애플리케이션 기반 규칙을 작성해야 합니다.

URL 및 애플리케이션 필터링용 별도의 규칙 생성

애플리케이션과 URL 기준을 결합하면 특히 암호화된 트래픽에 대해 예기치 않은 결과가 발생할 수 있으므로 가능하면 URL 및 애플리케이션 필터링에 대한 별도의 규칙을 만듭니다.

애플리케이션+URL 규칙이 더 일반적인 애플리케이션 전용 또는 URL 전용 규칙에 대한 예외 역할을 하지 않는 한, 애플리케이션 및 URL 기준을 모두 포함하는 규칙은 애플리케이션 전용 또는 URL 전용 규칙 뒤에 와야 합니다.

애플리케이션 및 기타 규칙 이전의 **URL** 규칙

가장 효과적인 URL 일치를 위해 특히 URL 규칙이 차단 규칙이고 다른 규칙이 다음 조건을 모두 만족하는 경우 다른 규칙 전에 URL 조건을 포함하는 규칙을 배치합니다.

- 애플리케이션 조건을 포함합니다.
- 검사할 트래픽은 암호화되어야 합니다.

암호화된 트래픽과 암호 해독된 트래픽에 대한 애플리케이션 제어

시스템은 암호화된 트래픽과 암호 해독된 트래픽을 식별하고 필터링할 수 있습니다.

- 암호화된 트래픽 - 시스템은 SMTPS, POPS, FTPS, TelnetS, IMAPS를 비롯하여 StartTLS로 암호화된 애플리케이션 트래픽을 탐지할 수 있습니다. 또한, TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서의 주체로 구별되는 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다. 이러한 애플리케이션은 `SSL` 프로토콜 태그가 지정됩니다. SSL 규칙에서는 이런 애플리케이션만 선택할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다.

- 암호 해독된 트래픽 - 시스템은 암호화되거나 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에 `decrypted traffic` 태그를 할당합니다.

TLS 서버 ID 검색 및 애플리케이션 제어

RFC 8446에서 정의한 TLS(Transport Layer Security) 프로토콜 1.3의 최신 버전은 보안 통신을 제공하기 위해 많은 웹 서버에서 선호하는 프로토콜입니다. TLS 1.3 프로토콜은 추가 보안을 위해 서버의 인증서를 암호화하며, 액세스 제어 규칙의 애플리케이션 및 URL 필터링 기준과 일치하는 데 인증서가 필요하므로 Firepower System은 전체 패킷의 암호를 해독하지 않고 서버 인증서를 추출하는 방법을 제공합니다.

애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 해독 정책에는 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.

자세한 내용은 액세스 제어 정책 고급 설정를 참고하십시오.

활성 권한 부여에서 애플리케이션 제외

ID 정책에서는 특정 애플리케이션을 액티브 인증에서 제외하여 트래픽이 액세스 제어로 계속 이동하도록 허용할 수 있습니다. 이러한 애플리케이션에는 `User-Agent Exclusion` 태그가 지정됩니다. ID 규칙에서는 이러한 애플리케이션만 선택할 수 있습니다.

페이로드 없이 애플리케이션 트래픽 패킷 처리

액세스 제어를 수행할 때 시스템은 애플리케이션이 식별된 연결에서 페이로드가 없는 패킷에 기본 정책 작업을 적용합니다.

참조된 애플리케이션 트래픽 처리

광고물 트래픽과 같이 웹 서버에서 참조된 트래픽을 처리하려면 참조하는 애플리케이션이 아닌 참조되는 애플리케이션의 일치 여부를 확인합니다.

다중 프로토콜을 사용하는 애플리케이션(Skype, Zoho)의 애플리케이션 트래픽 제어

일부 애플리케이션은 다중 프로토콜을 사용합니다. 해당 트래픽을 제어하려면 액세스 제어 정책이 모든 관련 옵션을 포함하는지 확인합니다. 예를 들면 다음과 같습니다.

- Skype - Skype 트래픽을 제어하려면 개별 애플리케이션을 선택하는 대신 **Application Filters(**애플리케이션 필터**)** 항목에서 **Skype** 태그를 선택합니다. 이렇게 하면 시스템이 동일한 방법으로 모든 Skype 트래픽을 탐지하고 제어할 수 있도록 할 수 있습니다.
- Zoho - Zoho 메일을 제어하려면 사용 가능한 애플리케이션 목록에서 **Zoho** 및 **Zoho mail**을 모두 선택합니다.

콘텐츠 제한 기능용으로 지원되는 검색 엔진

시스템은 특정 검색 엔진에 대해서만 안전 검색 필터링을 지원합니다. 이러한 검색 엔진의 애플리케이션 트래픽에는 `safesearch supported` 태그가 할당됩니다.

우회 애플리케이션 트래픽 제어

애플리케이션 관련 참고 사항 및 제한 사항, 16 페이지의 내용을 참조하십시오.

애플리케이션 제어 구성 모범 사례

다음과 같이 네트워크에 대한 애플리케이션의 액세스를 제어하는 것이 좋습니다.

- 보안 수준이 낮은 네트워크에서 보안 수준이 높은 네트워크로 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Port(**포트**)** (Selected Destination Port)(선택한 대상 포트) 조건을 사용합니다.

  예를 들어, 인터넷(보안 수준 낮음)에서 내부 네트워크(보안 수준 높음)으로 ICMP 트래픽을 허용합니다.

- 사용자 그룹의 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Application(**애플리케이션**)** 조건을 사용합니다.

  예를 들어, 계약업체 그룹 구성원의 Facebook 액세스를 차단합니다.

⚠

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.

다음 표에서 액세스 제어 규칙을 설정하는 방법에 대한 예시가 제공됩니다.

제어의 유형	조치	영역, 네트워크, **VLAN** 태그	사용자	애플리케이션	포트	**URL**	**SGT/ISE** 속성	검사, 로깅, 코멘트
애플리케이션에서 포트(예: SSH)를 사용하는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow(**허용**)**)	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	모두	설정하지 마십시오.	사용 가능한 포트: **SSH** **Selected Destination Ports(**선택한 대상 포트**)**에 추가	모두	ISE/ISE-PIC에만 사용합니다.	모두
애플리케이션에서 포트(예: ICMP)를 사용하지 않는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow(**허용**)**)	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	모두	설정하지 마십시오.	선택한 대상 포트 프로토콜: **ICMP** **Type(**유형**)**: **Any (**모든**)**	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	모두
사용자 그룹의 애플리케이션 액세스	선택(이 예에서는 **Block(**차단**)**)	선택	사용자 그룹(이 예에서는 계약업체 그룹)을 선택합니다.	애플리케이션의 이름(이 예에서는 **Facebook**)을 선택합니다.	설정하지 마십시오.	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	선택

애플리케이션 특성

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

표 *3:* 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.

애플리케이션 관련 참고 사항 및 제한 사항

- Office 365 관리자 포털:

  제한 사항: 액세스 정책이 시작 및 종료 시 로깅을 활성화한 경우 첫 번째 패킷은 Office 365로 감지되고 연결 종료는 Office 365 관리자 포털로 감지됩니다. 이는 블로킹에 영향을 주지 않습니다.

- Skype:

  애플리케이션 제어 권장 사항, 11 페이지의 내용을 참조하십시오.

- GoToMeeting

  GoToMeeting을 완벽하게 탐지하려면 규칙에 다음 애플리케이션이 모두 있어야 합니다.

  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting 플랫폼
  - LogMeIn
  - STUN

- Zoho:

  애플리케이션 제어 권장 사항, 11 페이지의 내용을 참조하십시오.

- Bittorrent, Tor, Psyphon, Ultrasurf 등의 우회 애플리케이션:

  우회 애플리케이션의 경우 기본적으로 가장 신뢰도가 높은 시나리오만 인식됩니다. 이 트래픽의 활동(차단 또는 QoS 구현 등)이 필요한 경우 효율성을 높이기 위해 더 적극적인 탐지 설정이 필요합니다. 이런 변경으로 오탐이 발생할 수 있으므로 이 작업을 수행하기 위해서는 설정을 검토하기 위한 TAC에 연결합니다.

- WeChat:

  WeChat을 허용하는 경우 선택적으로 WeChat Media를 차단할 수 없습니다.

- RDP(원격 데스크톱 프로토콜):

  RDP 애플리케이션을 허용해도 파일 전송이 허용되지 않는 경우, RDP에 대한 규칙에 TCP 및 UDP 포트 3389가 모두 포함되어 있는지 확인합니다. RDP 파일 전송은 UDP를 사용합니다.

액세스 제어 규칙 순서에 대한 모범 사례

효과적인 구축을 위해서는 규칙을 올바르게 구성하고 그 순서를 지정해야 합니다. 다음 주제는 규칙 성능 지침을 요약합니다.

참고 컨피그레이션 변경 사항을 구축할 때 시스템은 모든 규칙을 함께 평가하며, 타겟 디바이스가 네트워크 트래픽을 평가하는 데 사용하는 확장된 기준 집합을 생성합니다. 이러한 기준이 타겟 디바이스의 리소스(물리적 메모리, 프로세서 등)를 초과할 경우, 해당 디바이스에 구축할 수 없습니다.

액세스 제어의 모범 사례

다음 요구 사항 및 일반적인 모범 사례를 검토합니다.

- 사전 필터 정책을 사용하여 원치 않는 트래픽에 대해 초기에 차단 기능을 제공하고, 액세스 제어 검사를 활용하지 않는 트래픽의 경로를 단축합니다. 자세한 내용은 단축경로(Fastpath) 모범 사례를 참고하십시오.
- 구축에 라이선스를 부여하지 않고 시스템을 구성할 수는 있지만, 대부분의 기능을 사용하려면 구축 전에 적절한 라이선스를 활성화해야 합니다.
- 액세스 제어 정책을 구축할 때 해당 규칙은 기존 연결에 적용되지 않습니다. 기존 연결의 트래픽은 구축된 새 정책에 의해 바인딩되지 않습니다. 또한 정책 적중 횟수는 정책과 일치하는 연결의 첫 번째 패킷에 대해서만 증가합니다. 따라서 정책과 일치할 수 있는 기존 연결의 트래픽은 적중 횟수에서 생략됩니다. 정책 규칙을 효과적으로 적용하려면 기존 연결 세션을 지운 다음 정책을 구축합니다.

- 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.
- 시스템이 트래픽에 영향을 미치려면 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 관련 구성을 매니지드 디바이스에 구축해야 합니다.

  경우에 따라 시스템에서는 탭 모드의 인라인 디바이스를 비롯하여 수동으로 구축된 디바이스에 인라인 구성을 구축하지 못하도록 할 수 있습니다.

  다른 경우에는 정책이 성공적으로 구축될 수 있지만 수동 구축된 디바이스를 사용하여 트래픽을 차단하거나 변경하려고 하면 예상치 못한 결과가 발생할 수 있습니다. 예를 들어, 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에 시스템은 각 차단된 연결에 대한 여러 초기 연결 이벤트를 보고할 수 있습니다.
- URL 필터링, 애플리케이션 탐지, 속도 제한 및 지능형 애플리케이션 우회를 비롯한 특정 기능은 시스템에서 트래픽을 식별하기 위해 일부 패킷이 통과하도록 허용해야 합니다.

  이러한 패킷이 검사되지 않은 대상에 도달하지 못하도록하려면 트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례 및 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정의 내용을 참조하십시오.
- 액세스 제어 정책의 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.
- 일부 기능은 특정 디바이스 모델에서만 사용할 수 있습니다. 경고 아이콘 및 확정 대화 상자는 지원되지 않는 기능을 지정합니다.
- Syslog를 사용하거나 이벤트를 외부에 저장하려는 경우 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.
- 기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화되어 있지만 활성화할 수는 있습니다.
- 액세스 제어 규칙 생성, 순서 지정 및 구현에 대한 모범 사례는 액세스 제어 규칙 순서에 대한 모범 사례, 17 페이지 및 하위 주제에 자세히 설명되어 있습니다.

규칙 순서 지정 모범 사례

일반 지침:

- 일반적으로 정책 상단에서 모든 트래픽에 적용되는 최우선 규칙을 지정합니다.
- 구체적인 규칙은 일반적인 규칙보다 먼저 배치해야 합니다(특히, 구체적인 규칙이 일반적인 규칙에 대한 예외인 경우).

  그렇지 않으면 트래픽이 일반 규칙과 먼저 일치하며 적용 가능한 특정 규칙에 도달하지 않습니다.

- IP 주소, 보안 영역, 포트 번호 등 레이어-3/4 기준만을 기반으로 하여 트래픽을 삭제하는 규칙은 가능한 한 먼저 배치해야 합니다. 이러한 기준을 기반으로 하는 규칙은 일치하는 연결을 식별하기 위한 검사가 필요하지 않습니다.
- 구체적인 삭제 규칙은 가능한 경우 항상 정책 상위에 둡니다. 이렇게 하면 부적절한 트래픽에 대해 가능한 한 빠른 결정을 내릴 수 있습니다.
- URL 필터링, 애플리케이션 기반과 위치 기반 규칙 및 검사가 필요한 기타 규칙은 레이어 3/4 기준(예: IP 주소, 보안 영역, 포트 번호)만을 바탕으로 트래픽을 삭제하는 규칙 뒤에 와야 하며, 파일 및 침입 정책을 지정하는 규칙 앞에 와야 합니다.
- URL 필터링 규칙을 애플리케이션 규칙 위에 두고, 마이크로 애플리케이션 규칙 및 CIP(Common Industrial Protocol) 하위 분류 애플리케이션 필터링 규칙을 사용하여 애플리케이션 규칙을 따릅니다.
- 파일 정책 및 침입 정책을 지정하는 규칙은 규칙 순서의 맨 아래에 와야 합니다. 이러한 규칙에는 리소스를 많이 사용하는 심층 검사가 필요하며, 심층 검사가 필요한 잠재적인 위협 수를 최소화하려면 성능상의 이유로 먼저 덜 집중적인 방법을 사용하여 최대한 많은 위협을 제거해야 합니다.
- 항상 조직의 요구 사항에 맞게 규칙의 순서를 지정해야 합니다.

위의 지침에 대한 예외 및 추가 사항은 아래 섹션에 나와 있습니다.

규칙 선점

평가 순서에서 앞서는 규칙이 트래픽에 우선 일치하기 때문에 규칙이 트래픽과 일치하지 않는 경우 규칙 선점이 발생합니다. 규칙의 조건은 다른 규칙의 선점 여부를 제어합니다. 다음 예에서는 첫 번째 규칙이 관리 트래픽을 허용하기 때문에 두 번째 규칙이 차단할 수 없습니다.

액세스 제어 규칙 1: 관리자 사용자 허용
액세스 제어 규칙 2: 관리자 사용자 차단

모든 유형의 규칙 조건은 후속 규칙에 사전 대응할 수 있습니다. 첫 번째 SSL 규칙의 VLAN 범위는 VLAN을 두 번째 규칙으로 포함하므로 첫 번째 규칙이 두 번째 규칙보다 사전에 대응합니다.

SSL 규칙 1: VLAN 22-33을 암호화하지 않음
SSL 규칙 2: VLAN 27 차단

다음 예에서는 VLAN이 설정되지 않아 규칙 1이 모든 VLAN과 일치하므로 규칙 1이 VLAN 2에 일치시키려는 규칙 2를 선점합니다.

액세스 제어 규칙 1: 소스 네트워크 10.4.0.0/16 허용
액세스 제어 규칙 2: 소스 네트워크 10.4.0.0/16, VLAN 2 허용

규칙은 모든 설정 조건이 동일한 후속 규칙을 선점합니다.

QoS 규칙 1: VLAN 1 URL www.netflix.com 속도 제한
QoS 규칙 2: VLAN 1 URL www.netflix.com 속도 제한

조건이 다른 경우 후속 규칙의 선점이 발생하지 않습니다.

QoS 규칙 1: VLAN 1 URL www.netflix.com 속도 제한
QoS 규칙 2: VLAN 2 URL www.netflix.com 속도 제한

예: 사전 대응을 방지하기 위해 **SSL** 규칙 순서 지정

예를 들어 신뢰받는 CA(Good CA)에서 악성 엔티티(Bad CA)에 CA 인증서를 잘못 발급했지만 아직 그 인증서를 폐기하지 않았습니다. 신뢰할 수 없는 CA에서 발행한 인증서로 암호화된 트래픽을 차단하지만 신뢰할 수 있는 CA의 신뢰 체인의 트래픽은 허용하는 SSL 정책을 사용하려 합니다. CA 인증서 및 모든 중간 CA 인증서를 업로드한 후 다음 순서에 따라 규칙이 포함된 SSL 정책을 구성합니다.

SSL 규칙 1: 발급자 차단 CN=www.badca.com
SSL 규칙 2: 발급자 암호 해독 안 함 CN=www.goodca.com

규칙을 반대로 설정할 경우 불량 CA가 신뢰하는 트래픽을 포함해 우수한 CA가 신뢰하는 모든 트래픽을 우선 일치시킵니다. 어떤 트래픽도 이후의 불량 CA 규칙에 일치시키지 않으므로 악성 트래픽이 차단되지 않고 허용될 수 있습니다.

규칙 작업 및 규칙 순서

규칙의 작업은 시스템에서 일치하는 트래픽을 처리하는 방법을 결정합니다. 추가로 트래픽 처리를 수행하거나 확인하여 리소스를 많이 소모하는 규칙 앞에 그렇지 않은 규칙을 배치하면 성능이 향상됩니다. 시스템은 검사 대상이었던 트래픽으로 전환할 수 있습니다.

다음 예는 여러 정책에서 중요 규칙이 없고 사전 대응이 문제가 되지 않는 규칙 집합 중 규칙 순서를 정하는 방법을 나타냅니다.

규칙이 애플리케이션 조건을 포함하는 경우에도 애플리케이션 제어 구성 모범 사례, 14 페이지의 내용을 참조하십시오.

최적의 순서: 암호 해독 규칙

암호 해독뿐 아니라 암호 해독된 트래픽의 추가 분석에도 리소스를 필요로 합니다. 트래픽의 암호를 해독하는 규칙을 나중에 배치하십시오.

참고 특정 매니지드 디바이스는 하드웨어 내에서 TLS/SSL 트래픽의 암호화 및 암호 해독을 지원하여 성능을 대폭 향상합니다. 자세한 내용은 TLS 암호화 가속를 참조하십시오.

1. 모니터링 - 일치하는 연결을 기록하지만 트래픽에 다른 작업을 수행하지 않는 규칙
2. 차단, 재설정과 함께 차단 - 추가 검사 없이 트래픽을 차단하는 규칙입니다.
3. 암호 해독 안 함 - 암호화된 트래픽의 암호를 해독하지 않고 암호화된 세션을 액세스 제어 규칙에 전달하는 규칙 이런 세션의 페이로드는 심층 검사 대상이 아닙니다.
4. 암호 해독 - 알려진 키 - 확인된 개인 키로 수신 트래픽을 암호 해독하는 규칙
5. 암호 해독 - 다시 서명 - 서버 인증서에 다시 서명을 하여 발신 트래픽을 암호 해독하는 규칙

최적의 순서: 액세스 제어 규칙

특히 여러 사용자 정의 침입 정책과 변수 집합을 사용하는 경우 침입, 파일, 악성코드 검사 시 리소스를 사용합니다. 심층 검사를 마지막으로 호출하는 액세스 제어 규칙을 배치합니다.

1. 모니터링 - 일치하는 연결을 기록하지만 트래픽에 다른 작업을 수행하지 않는 규칙 (액세스 제어 규칙 모니터 작업에서 중요 예외 및 주의 사항을 확인하십시오.)
2. 신뢰, 차단, 재설정과 함께 차단 - 추가 검사 없이 트래픽을 처리하는 규칙 신뢰할 수 있는 트래픽에는 ID 정책에 적용된 인증 요건 및 속도 제한이 적용됩니다.
3. 허용, 상호 작용 차단(심층 검사 없음) - 트래픽을 추가로 검사하지 않지만 검색을 허용하는 규칙 허용된 트래픽에는 ID 정책에 적용된 인증 요건 및 속도 제한이 적용됩니다.
4. 허용, 상호 작용 차단(심층 검사) - 금지된 파일, 악성코드, 익스플로잇에 대해 심층 검사를 수행하는 파일 또는 침입 정책과 관련된 규칙

애플리케이션 규칙 순서

애플리케이션 조건이 포함된 규칙은 목록에서 낮은 순서로 이동할 경우 트래픽과 일치할 가능성이 높습니다.

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.

자세한 정보와 예시는 애플리케이션 제어 구성 모범 사례, 14 페이지 및 애플리케이션 제어 권장 사항, 11 페이지의 내용을 참조하십시오.

URL 규칙 순서

가장 효과적인 URL 일치를 위해 특히 URL 규칙이 차단 규칙이고 다른 규칙이 다음 조건을 모두 만족하는 경우 다른 규칙 전에 URL 조건을 포함하는 규칙을 배치합니다.

- 애플리케이션 조건을 포함합니다.
- 검사할 트래픽은 암호화되어야 합니다.

규칙에 대해 예외를 설정하는 경우 다른 규칙 위에 예외를 배치합니다.

규칙 간소화 및 집중모범 사례

간소화: 과잉 구성하지 않습니다.

개별 규칙 기준을 최소화합니다. 규칙 조건에 최소한의 개별 요소를 사용합니다. 예를 들어 네트워크 조건에서 개별 IP 주소 대신 IP 주소 블록을 사용합니다.

하나의 조건이 처리하려는 트래픽과 일치시키는 데 충분하다면 두 조건을 사용하지 마십시오. 이중 조건을 사용하면 구축된 구성이 크게 확장될 수 있으며, 이로 인해 디바이스 성능에 문제가 발생할 수 있으며, 클러스터 및 고가용성 유닛에 다시 조인할 때 예기치 않은 디바이스 동작이 발생할 수 있습니다. 대표적인 예는 다음과 같습니다.

- 여러 인터페이스를 나타내는 보안 영역은 신중하게 사용하십시오. 소스 및 대상 네트워크를 조건으로 지정하고 이러한 네트워크가 대상 트래픽과 일치하는 데 충분할 경우 보안 영역을 지정할 필요가 없습니다.
- 예를 들어 내부 인터페이스 집합을 인터넷의 모든 대상과 일치시키려면 내부 인터페이스를 포함하는 소스 보안 영역을 사용하면 됩니다. 네트워크 또는 대상 인터페이스 기준이 필요하지 않습니다.

요소를 개체에 결합하는 것은 성능을 개선하지 않습니다. 예를 들어, 50개의 개별적인 IP 주소를 포함하는 네트워크 개체를 사용하면 사용자가 얻을 수 있는 이점은 성능에 관한 것이 아닌 구성적인 것에 한정되며, 조건에 해당 IP 주소를 개별적으로 포함하는 것입니다.

애플리케이션 탐지와 관련한 권장 사항은 애플리케이션 제어 구성 모범 사례, 14 페이지을 참조하십시오.

집중: 특히 인터페이스에서 리소스를 많이 사용하는 규칙을 구체적으로 제한

규칙 조건을 최대한 사용하여 리소스를 많이 사용하는 규칙을 트래픽을 구체적으로 정의합니다. 폭넓은 조건을 가진 규칙이 여러 유형의 트래픽에 일치하며 추후 더 많은 특정 규칙에 사전 정의될 수 있기 때문에 집중 규칙이 중요합니다. 리소스를 많이 사용하는 규칙은 다음과 같습니다.

- 트래픽의 암호를 해독하는 TLS/SSL 규칙 - 암호 해독뿐 아니라 암호 해독된 트래픽의 추가 분석에도 리소스가 필요합니다. 집중하여 가능한 곳에서 암호화된 트래픽을 해독하지 않도록 선택 또는 차단합니다.

  특정 Threat Defense 모델은 하드웨어에서 TLS/SSL 암호화 및 해독을 수행하여 성능을 크게 향상시킵니다. 자세한 내용은 TLS 암호화 가속를 참조하십시오.

- 심화 검사를 호출하는 액세스 제어 규칙 - 특히 여러 사용자 정의 침입 정책 및 변수 세트를 사용하는 경우 침입, 파일, 악성코드 검사에 리소스를 사용합니다. 필요한 경우에만 심화 검사를 호출합니다.

최대 성능 향상을 위해 인터페이스로 규칙을 제한합니다. 규칙이 모든 디바이스의 인터페이스를 제외할 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

최대 액세스 제어 규칙 및 침입 정책 개수

대상 디바이스에서 지원하는 최대 액세스 제어 규칙 또는 침입 정책 수는 정책 복잡성, 물리적 메모리 및 디바이스의 프로세서 수 등 여러 요인에 따라 달라집니다.

장치에서 지원되는 최대 한도를 초과하면 액세스 제어 정책을 구축할 수 없으며 재평가가 필요합니다.

침입 정책에 대한 지침:

- 액세스 제어 정책에서는 하나의 침입 정책을 각 허용 및 인터랙티브 차단 규칙 및 기본 작업과 연결할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다.
- 침입 정책 또는 변수 집합을 통합하여 단일한 침입 정책 변수 집합 쌍을 여러 개의 액세스 제어 규칙과 연결할 수 있습니다. 일부 디바이스에서 모든 침입 정책에 단일 변수 집합만 사용할 수 있거나 전체 디바이스에 단일 침입 정책-변수 집합 쌍을 사용할 수 있습니다.