액세스 제어의 이해

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
- 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.

Access Control Policy Default Action(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.

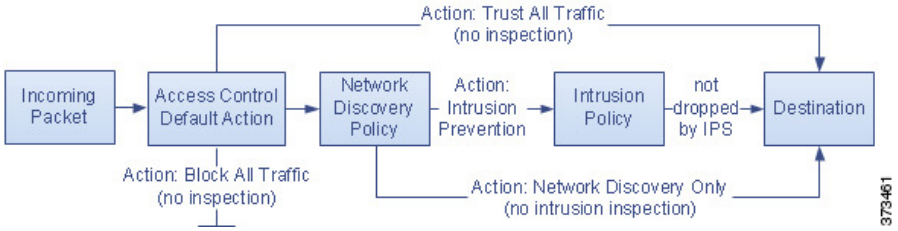
다음 표는 각 기본 작업에 의해 처리된 트래픽에서 수행할 수 있는 검사 유형을 나열합니다.

표 *1:* 액세스 제어 정책 기본 작업

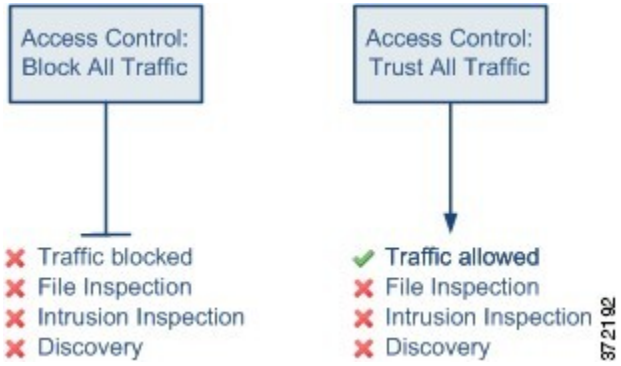
기본 작업	트래픽에 미치는 영향	검사 유형 및 정책
액세스 제어: 모든 트래픽 차단	추가 검사 없이 차단	없음
액세스 제어: 모든 트래픽 신뢰	신뢰(추가 검사 없이 최종 대상에서 허용)	없음
침입 방지	허용. 사용자가 지정한 침입 정책에 의해 통과된 경우	지정된 침입 정책 및 관련 변수 집합을 사용한 침입 및 네트워크 검색 정책을 사용한 검색
네트워크 검색 한정	허용	네트워크 검색 정책을 사용한 검색만 해당

기본 작업	트래픽에 미치는 영향	검사 유형 및 정책
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.

관련 항목

제한된 구축에 대한 성능 고려 사항

정책 기본 작업으로 연결 로깅

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 AMP for Networks 기능을 제어합니다.

  자세한 내용은 파일 정책 및 악성코드 보호를 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

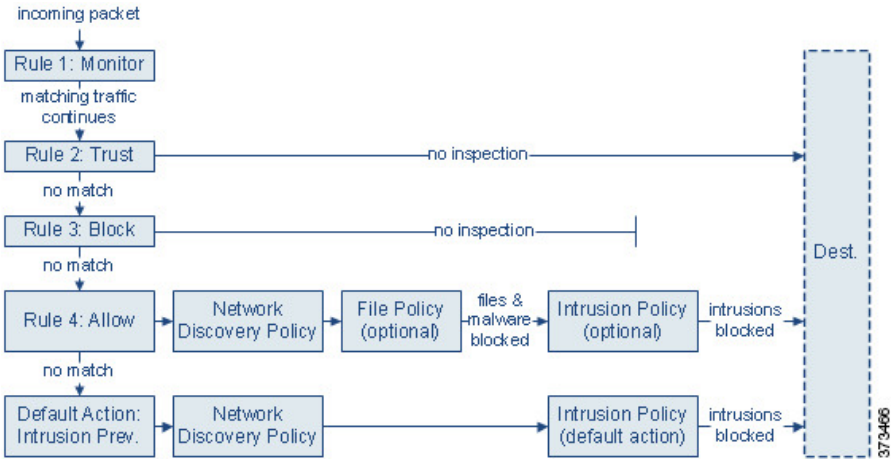
참고 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

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 AMP for Networks 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.

- **AMP for Networks** 및 파일 제어**:** 파일 정책 - 검색에 의해 트래픽이 검사된 후 시스템은 트래픽에서 금지된 파일과 악성코드를 검사할 수 있습니다. AMP for Networks 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.

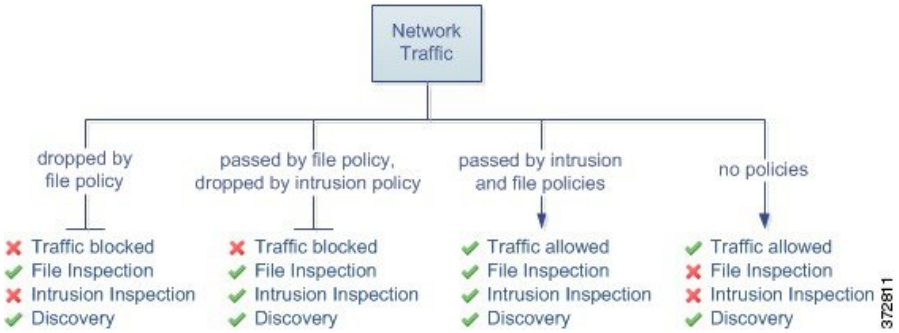
참고 트래픽이 침입 방지 또는 네트워크 검색 한정 기본 작업에 의해 허용된 경우 검색 데이터 및 침입은 검사할 수 있지만, 금지된 파일 또는 악성코드는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 없습니다.

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 Firepower 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.

관련 항목

액세스 제어 정책 상속 관리
보안 인텔리전스 차단 목록
HTTP 응답 페이지 및 인터랙티브 차단
액세스 제어 정책 고급 설정
액세스 제어 정책용 로깅 설정