



액세스 제어 정책

다음 주제에서는 액세스 제어 정책을 사용하는 방법에 대해 설명합니다.

- 액세스 제어 정책 구성 요소, 2 페이지
- 액세스 제어 정책 요구 사항 및 사전 요건, 4 페이지
- 액세스 제어 정책 관리, 4 페이지
- 시스템 생성 액세스 제어 정책, 5 페이지
- 기본 액세스 제어 정책 만들기, 5 페이지
- 액세스 제어 정책 수정, 6 페이지
- 액세스 제어 정책 상속 관리, 8 페이지
- 액세스 제어 정책에 대한 대상 디바이스 설정, 11 페이지
- 액세스 제어 정책용 로깅 설정, 12 페이지
- 액세스 제어 정책 고급 설정, 13 페이지
- 정책 적중 횟수 보기, 18 페이지
- 액세스 제어 정책 히스토리, 19 페이지

액세스 제어 정책 구성 요소

Simple Access Control Policy

Inspects all traffic with a balanced intrusion policy

Rules
Security Intelligence
HTTP Responses
Logging
Advanced

Filter by Device

▼ Search Rules

Name	Source Zones	Dest Zones	Source Netw...	Dest Netw...	VLAN Tags	Users	Appli...	S P
▼ Mandatory - Simple Access Control Policy (-)								
There are no rules in this section. Add Rule or Add Category								
▼ Default - Simple Access Control Policy (-)								
There are no rules in this section. Add Rule or Add Category								
Default Action								

이름 및 설명

각 액세스 제어 정책에는 고유한 이름이 있어야 합니다. 설명은 선택 사항입니다.

Inheritance Settings(상속 설정)

정책 상속을 사용하면 액세스 계층 제어 정책을 생성할 수 있습니다. 상위(또는 기본) 정책은 하위 항목에 대한 기본 설정을 정의하고 시행하며, 이는 특히 다중 도메인 구축에서 유용합니다.

정책 상속 설정을 통해 기본 정책을 선택할 수 있습니다. 현재 정책의 설정을 잠금 처리하여 하위 항목이 강제로 상속하도록 설정할 수도 있습니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

Policy Assignment(정책 할당)

각 액세스 제어 정책은 이를 사용하는 디바이스를 식별합니다. 각 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 다중 도메인 구축에서는 도메인의 모든 디바이스가 동일 한 기본 정책을 사용하도록 요구할 수 있습니다.

규칙

액세스 제어 규칙은 네트워크 트래픽 처리에 대한 세분화된 방법을 제공합니다. 액세스 제어 정책의 규칙은 상위 정책에서 상속된 규칙을 포함하여 1부터 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. 조건은 단순하거나 복잡할 수 있으며, 조건의 사용은 특정 라이선스에 따라 달라지는 경우가 많습니다.

기본 작업

기본 작업은 시스템이 다른 액세스 제어 구성에 의해 처리되지 않는 트래픽을 처리하고 기록하는 방법을 결정합니다. 기본 작업을 사용하여 추가 검사 없이 모든 트래픽을 차단하거나 신뢰할 수 있고, 침입 및 검색 데이터 트래픽을 검사할 수 있습니다.

액세스 제어 정책은 상위 정책에서 기본 작업을 상속할 수 있지만 이 상속을 적용할 수는 없습니다.

보안 인텔리전스

보안 인텔리전스는 악성 인터넷 콘텐츠에 대한 1차 방어선입니다. 이 기능을 사용하여 최신 IP 주소, URL, 도메인 이름 평판 인텔리전스에 따라 연결을 차단할 수 있습니다. 중요 리소스로 지속적으로 액세스할 수 있도록 차단 목록 항목을 사용자 지정 차단 안 함 목록 항목으로 재정의할 수 있습니다.

HTTP 응답

시스템이 사용자의 웹 사이트 요청을 차단하면 일반 시스템 제공 응답 페이지 또는 사용자 정의 페이지를 표시할 수 있습니다. 또한 사용자에게 경고하는 페이지를 표시할 수도 있지만 원래 요청한 사이트를 계속 진행할 수 있습니다.

로깅

액세스 제어 정책 로깅에 대한 설정을 통해 현재 액세스 제어 정책에 대한 기본 `syslog` 대상을 구성할 수 있습니다. 포함된 규칙 및 정책의 `syslog` 대상 설정이 사용자 정의 설정으로 명시적으로 무시되지 않는 한 설정은 액세스 제어 정책 및 포함된 모든 SSL, 사전 필터 및 침입 정책에 적용됩니다.

고급 액세스 제어 옵션

고급 액세스 제어 정책 설정은 일반적으로 약간의 변경이 필요하거나 변경이 필요하지 않습니다. 종종 기본 설정이 적합합니다. 수정할 수 있는 고급 설정에는 트래픽 사전 처리, SSL 검사, ID 및 다양한 성능 옵션이 포함됩니다.

관련 항목

[규칙 관리: 일반 특성](#)

액세스 제어 정책 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

액세스 제어 정책 관리




Firepower System을 사용하면 시스템에서 제공한 액세스 제어 정책을 편집하고 사용자 정의 액세스 제어 정책을 생성할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

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

단계 2 액세스 제어 정책 관리

- 복사- 복사 ()를 클릭합니다.
- 생성 - **New Policy**(새 정책)을 클릭합니다([기본 액세스 제어 정책 만들기, 5 페이지](#) 참조).
- 삭제- 삭제()를 클릭합니다.
- 구축 - **Deploy**(구축) > **Deployment**(구축)를 선택합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.
- 수정-수정()를 클릭합니다. [액세스 제어 정책 수정, 6 페이지](#)의 내용을 참조하십시오.
- 상속 - 정책의 계층 보기를 확장하기 위해 하위 계층이 포함된 정책 옆의 더하기 아이콘을 클릭합니다.

- 가져오기/내보내기 - **Import/Export**(가져오기/내보내기)를 클릭합니다. 구성 가져오기 및 내보내기를 참조하십시오.
- 보고서- 보고서(📄)를 클릭합니다. 현재 정책 보고서 생성의 내용을 참조하십시오.

관련 항목

[만료된 정책](#)

시스템 생성 액세스 제어 정책

사용자 디바이스의 초기 설정에 따라 시스템 제공 정책에 다음이 포함될 수 있습니다.

- 기본 액세스 제어 - 추가 검사 없이 모든 트래픽을 차단합니다.
- 기본 침입 예방 - 모든 트래픽을 허용하지만 균형 보안 및 연결성 침입 정책과 기본 침입 변수 집합을 검사합니다.
- 기본 네트워크 검색 - 검색 데이터를 검사하는 동안 모든 트래픽을 허용하지만 침입과 익스플로잇은 허용하지 않습니다.

기본 액세스 제어 정책 만들기

신규 액세스 제어 정책을 만들 때 적어도 하나의 기본 작업을 선택해야 합니다.

대부분의 경우 기본 작업이 처리한 연결 기록은 처음으로 비활성화됩니다. 다중 도메인 구축 시 하위 정책을 생성하는 경우 예외가 발생합니다. 이 경우 시스템은 상속된 기본 작업의 기록 설정에 따라 연결 기록을 활성화합니다.

프로시저

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

단계 2 **New Policy**(새로운 정책)를 클릭합니다.

단계 3 고유한 **Name**(이름)을 입력하고, 필요한 경우 **Description**(설명)을 입력합니다.

단계 4 필요한 경우 기본 정책 선택 드롭다운 목록에서 기본 정책을 선택합니다.

도메인에 액세스 제어 정책이 강제 적용되는 경우 이 단계는 선택 사항이 아닙니다. 기본 정책으로는 강제 적용된 정책 또는 그 하위 정책 중 하나를 선택해야 합니다.

단계 5 초기 **Default Action**(기본 작업)을 지정합니다.

- 기본 정책을 선택한 경우 새 정책은 기본 작업을 상속합니다. 여기에서 변경할 수 없습니다.
- **Block all traffic**(모든 트래픽을 차단)은 **Access Control: Block All Traffic**(액세스 제어: 모든 트래픽을 차단) 기본 작업을 통해 정책을 생성합니다.

- **Intrusion Prevention**(침입 방지)은 기본 침입 변수 집합과 연결된 **Intrusion Prevention: Balanced Security and Connectivity**(침입 방지: 균형 잡힌 보안 및 연결성) 기본 작업을 통해 정책을 생성합니다.
- **Network Discovery**(네트워크 검색)을 선택하면 **Network Discovery Only**(네트워크 검색 전용) 기본 작업이 포함된 정책을 생성합니다.

팁 기본적으로 모든 트래픽을 신뢰하거나 기본 정책을 선택하지만 기본 작업을 상속하지 않을 경우 기본 작업을 나중에 변경할 수 있습니다.

단계 6 필요에 따라 정책을 구축할 **Available Devices**(사용 가능한 디바이스)를 선택하고 **Add to Policy**(정책에 추가)(또는 드래그 앤 드롭)을 클릭하여 선택한 디바이스를 추가합니다. 표시되는 디바이스의 범위를 좁히려면 **Search**(검색) 필드에 검색 문자열을 입력합니다.

이 정책을 즉시 구축하려는 경우 이 단계를 수행해야 합니다.

단계 7 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 필요한 경우, [액세스 제어 정책 수정, 6 페이지](#)의 설명에 따라 새 정책을 설정합니다.
- 선택적으로, 애플리케이션 및 URL 필터링이 TLS 1.3 지원 세션에서 예상대로 수행할 수 있도록 액세스 제어 정책의 고급 설정에서 TLS 서버 ID를 구성합니다. 자세한 내용은 [액세스 제어 정책 고급 설정, 13 페이지](#)을 참조해 주십시오.
- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

관련 항목

- [Access Control Policy Default Action](#)(액세스 제어 정책 기본 작업)
- [액세스 제어 정책에 대한 대상 디바이스 설정, 11 페이지](#)

액세스 제어 정책 수정

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장한 변경사항이 유지됩니다. 편의상 시스템에는 현재 각 정책을 수정하고 있는 사용자(있는 경우)에 대한 정보가 표시됩니다. 세션의 개인 정보를 보호하기 위해 정책 편집기에서 30분 동안 아무런 작업을 하지 않으면 경고가 표시됩니다. 60분이 지나면 시스템에서 변경사항을 삭제합니다.



참고 현재 도메인에서 생성된 액세스 제어 정책만 편집할 수 있습니다. 또한 상위 액세스 제어 정책에 의해 잠긴 설정은 편집할 수 없습니다.

프로시저

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

단계 2 편집하려는 액세스 제어 정책 옆에 있는 수정(✎)을 클릭합니다.

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

단계 3 기존 액세스 제어 정책을 편집합니다.

팁 여러 규칙을 Shift-클릭하거나 Control-클릭한 다음 마우스 오른쪽 버튼을 클릭하고 Edit(편집)을 선택하여 여러 규칙을 한 번에 편집할 수 있습니다. 대량 편집을 통해 규칙을 활성화 및 비활성화하고, 규칙 작업을 선택하고, 대부분의 검사 및 로깅 설정을 설정할 수 있습니다.

설정:

- 이름 및 설명 - 필드를 클릭하고 새 정보를 입력합니다.
- Default Action - **Default Action**(기본 작업) 드롭다운 목록에서 값을 선택합니다.
- Default Action Variable Set - **Intrusion Prevention**(침입 방지) 기본 작업과 관련된 변수 집합을 변경하려면 변수(📄)를 클릭합니다. 이때 나타나는 팝업 창에서 새로운 변수 집합을 선택하고 **OK**(확인)를 클릭합니다. 사용자는 또한 수정(✎)을 클릭하여 선택한 변수 집합을 새 창에서 수정할 수 있습니다. 자세한 내용은 [변수 관리](#)를 참고하십시오.
- Default Action Logging - 기본 작업에 의해 처리된 연결에 대한 로깅을 설정하려면 로깅(📄)을 클릭합니다. [정책 기본 작업으로 연결 로깅](#) 섹션을 참조하십시오.
- HTTP Responses - 시스템이 웹사이트 요청을 차단할 때 브라우저에 표시되는 내용을 지정하려면 **HTTP Responses(HTTP 응답)**를 클릭합니다. [HTTP 응답 페이지 선택](#) 섹션을 참조하십시오.
- Inheritance: Change Base Policy - 이 정책에 대한 기본 액세스 제어 정책을 변경하려면 **Inheritance Settings**(상속 설정)를 클릭합니다. [기본 액세스 제어 정책 선택, 9 페이지](#) 섹션을 참조하십시오.
- Inheritance: Lock Settings in Descendants - 이 정책의 설정을 하위 정책에 적용하려면 **Inheritance Settings**(상속 설정)를 클릭합니다. [하위 액세스 제어 정책의 설정 잠금, 10 페이지](#) 섹션을 참조하십시오.
- Policy Assignment: Targets - 이 정책의 대상이 되는 매니지드 디바이스를 식별하려면 **Policy Assignment**(정책 할당)를 클릭합니다. [액세스 제어 정책에 대한 대상 디바이스 설정, 11 페이지](#) 섹션을 참조하십시오.
- Policy Assignment: Required in Domains - 이 정책을 하위 도메인에 적용하려면 **Policy Assignment**(정책 할당)를 클릭합니다. [도메인에 액세스 제어 정책 필요, 10 페이지](#) 섹션을 참조하십시오.
- Rules - 액세스 제어 규칙을 관리하고 침입 및 파일 정책을 사용하여 악의적인 트래픽을 검사 및 차단하려면 **Rules**(규칙)를 클릭합니다. [액세스 제어 규칙 생성 및 수정](#) 섹션을 참조하십시오.
- Rule Conflicts - 규칙 충돌 경고를 표시하려면 **Show rule conflicts**(규칙 충돌 표시)를 활성화합니다. 이전 규칙이 항상 트래픽과 먼저 일치하므로 특정 규칙이 트래픽과 일치하지 않으면 충돌이

발생합니다. 규칙 충돌을 판별하는 것은 리소스가 많이 사용될 수 있기 때문에 표시하는 데 시간이 걸릴 수 있습니다. 자세한 내용은 [규칙 순서 지정 모범 사례](#)를 참고하십시오.

- **Security Intelligence** - 최신 평판 인텔리전스에 따라 즉시 연결을 차단하려면 **Security Intelligence**(보안 인텔리전스)를 클릭합니다. [보안 인텔리전스 설정](#) 섹션을 참조하십시오.
- **Advanced Options** - 사전 처리, SSL 검사, ID, 성능 및 기타 고급 옵션을 설정하려면 **Advanced**(고급)를 클릭합니다. [액세스 제어 정책 고급 설정, 13 페이지](#) 섹션을 참조하십시오.
- **Warnings** - 액세스 제어 정책(및 해당 하위 항목 및 관련 정책)의 경고 또는 오류 목록을 보려면 **Show Warnings**(경고 표시)를 클릭합니다. 경고 및 오류는 트래픽 분석 및 흐름에 악영향을 미치거나 정책 배포를 방해할 수 있는 구성을 표시합니다. 경고가 없는 경우, 경고 표시가 나타나지 않습니다. 규칙 충돌 경고를 표시하려면 **Show rule conflicts**(규칙 충돌 표시)를 활성화합니다.

단계 4 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

관련 항목

- [규칙 및 기타 정책 경고](#)
- [파일 및 침입 정책을 사용한 심층 검사](#)

액세스 제어 정책 상속 관리

시작하기 전에

상속이 어떻게 작동하는지 이해합니다. [액세스 제어 정책 상속](#) 및 하위 항목을 참조하십시오.

프로시저

단계 1 상속 설정을 변경하려는 액세스 제어 정책을 편집합니다. [액세스 제어 정책 수정, 6 페이지](#) 섹션을 참조하십시오.

단계 2 정책 상속 관리:

- **Change Base Policy** - 이 정책에 대한 기본 액세스 제어 정책을 변경하려면 [기본 액세스 제어 정책 선택, 9 페이지](#)에 설명된 대로 **Inheritance Settings**(상속 설정)를 클릭합니다.
- **Lock Settings in Descendants** - 이 정책의 설정을 하위 정책에 적용하려면 [하위 액세스 제어 정책의 설정 잠금, 10 페이지](#)에 설명된 대로 **Inheritance Settings**(상속 설정)를 클릭합니다.
- **Required in Domains** - 이 정책을 하위 도메인에 적용하려면 [도메인에 액세스 제어 정책 필요, 10 페이지](#)에 설명된 대로 **Policy Assignment**(정책 할당)를 클릭합니다.

- **Inherit Settings from Base Policy** - 기본 액세스 제어 정책에서 설정을 상속하려면 **Security Intelligence**(보안 인텔리전스), **HTTP Responses(HTTP 응답)** 또는 **Advanced(고급)**을 클릭하고 기본 정책에서 액세스 제어 정책 설정 상속, 9 페이지의 지침에 따라 진행합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

기본 액세스 제어 정책 선택

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	Any(모든)	Any(모든)	Any(모든)	관리자/액세스 관리자/ 네트워크 관리자

하나의 액세스 제어 정책을 다른 정책에 대한 기본(상위)으로 사용할 수 있습니다. 잠금 해제된 설정을 변경할 수 있지만 기본적으로 하위 정책은 기본 정책에서 설정을 상속받습니다.

현재 액세스 제어 정책에 대한 기본 정책을 변경하면 시스템은 새 기본 정책에서 잠긴 설정으로 현재 정책을 갱신합니다.

프로시저

단계 1 액세스 컨트롤 정책 편집기에서 **Inheritance Settings**(상속 설정)를 클릭합니다.

단계 2 Select Base Policy(기본 정책 선택) 드롭다운 목록에서 정책을 선택합니다.

다중 도메인 구축의 경우 현재 도메인에서 액세스 제어 정책이 필요할 수 있습니다. 기본 정책으로 시행된 정책 또는 그 하위 항목 중 하나만 선택할 수 있습니다.

단계 3 Save(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

기본 정책에서 액세스 제어 정책 설정 상속

새 하위 정책은 기본 정책에서 많은 설정을 상속받습니다. 이 설정이 기본 정책에서 잠금 해제되어 있으면 재정의할 수 있습니다.

나중에 기본 정책의 설정을 다시 상속하면 시스템은 기본 정책의 설정을 표시하고 컨트롤을 흐릿하게 표시합니다. 하지만 시스템은 사용자가 변경한 내용을 저장하고 상속을 다시 사용하지 않도록 설정하면 복원합니다.

프로시저

-
- 단계 1 액세스 제어 정책 편집기에서 **Security Intelligence**(보안 인텔리전스), **HTTP Responses**(HTTP 응답) 또는 **Advanced**(고급)을 클릭합니다.
 - 단계 2 상속할 각 설정에 대해 **Inherit from base policy**(상속 정책에서 상속) 확인란을 선택합니다.
컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다.
 - 단계 3 **Save**(저장)를 클릭합니다.
-

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

하위 액세스 제어 정책의 설정 잠금

모든 하위 정책에 설정을 적용하려면 액세스 제어 정책에서 설정을 잠급니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

설정을 잠그면 시스템은 하위 정책에서 이미 적용된 재정의의 저장하므로 설정을 다시 해제하면 재정의의 복원할 수 있습니다.

프로시저

-
- 단계 1 액세스 컨트롤 정책 편집기에서 **Inheritance Settings**(상속 설정)를 클릭합니다.
 - 단계 2 **Child Policy Inheritance Settings**(하위 정책 상속 설정) 영역에서 잠그려는 설정을 선택합니다.
컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다.
 - 단계 3 **OK**(확인)를 클릭하여 상속 설정을 저장합니다.
 - 단계 4 **Save**(저장)를 클릭하여 액세스 제어 정책을 저장합니다.
-

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

도메인에 액세스 제어 정책 필요

도메인의 모든 디바이스가 동일한 기본 액세스 제어 정책 또는 그 하위 정책 중 하나를 사용하도록 요구할 수 있습니다.

시작하기 전에



- 전역 도메인 이외 하나 이상의 도메인을 구성합니다.

프로시저

단계 1 액세스 컨트롤 정책 편집기에서 **Policy Assignments**(정책 할당)를 클릭합니다.

단계 2 **Required on Domains**(도메인에 대한 필수 요소)를 클릭합니다.

단계 3 도메인 목록을 구축합니다.

- **Add**(추가) - 현재 액세스 제어 정책을 적용할 도메인을 선택한 다음 **Add**(추가)를 클릭하거나 선택한 도메인 목록으로 끌어다 놓습니다.
- **Delete**(삭제) - 리프 도메인 옆에 있는 삭제()을 클릭하거나 상위 도메인을 오른쪽 클릭하고 **Delete Selected**(선택 항목 삭제)를 선택합니다.
- **Search**(검색) - 검색 필드에 검색 문자열을 입력합니다. 지우기()을 클릭하여 검색 내용을 삭제합니다.

단계 4 **OK**(확인)를 클릭하여 도메인 적용 설정을 저장합니다.

단계 5 **Save**(저장)를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [권피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.


액세스 제어 정책에 대한 대상 디바이스 설정

액세스 제어 정책은 이를 사용하는 디바이스를 지정합니다. 각 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 다중 도메인 구축에서는 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다.

프로시저

단계 1 액세스 컨트롤 정책 편집기에서 **Policy Assignments**(정책 할당)를 클릭합니다.

단계 2 **Targeted Devices**(대상 디바이스)에 대상 목록을 만듭니다.

- **Add**(추가) - 하나 이상의 **Available Devices**(사용 가능한 디바이스)를 선택한 다음 **Add to Policy**(정책에 추가)를 클릭하거나 **Selected Devices**(선택한 디바이스) 목록으로 드래그 앤 드롭합니다.
- **Delete**(삭제) - 단일 디바이스 옆에 있는 삭제()을 클릭하거나 여러 디바이스를 선택하고 오른쪽 클릭한 다음 **Delete Selected**(선택 항목 삭제)를 선택합니다.

- Search(검색) - 검색 필드에 검색 문자열을 입력합니다. 지우기(✕)을 클릭하여 검색 내용을 삭제합니다.

Impacted Devices(영향을 받는 디바이스)에서 시스템은 할당된 액세스 제어 정책이 현재 정책의 하위 디바이스를 나열합니다. 현재 정책의 변경 사항은 이러한 디바이스에 영향을 줍니다.

단계 3 필요에 따라 **Required on Domains**(도메인에 대한 필수 요소)를 클릭하여 선택한 하위 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다. [도메인에 액세스 제어 정책 필요, 10 페이지](#)의 내용을 참조하십시오.

단계 4 **OK**(확인)를 클릭하여 대상 디바이스 설정을 저장합니다.

단계 5 **Save**(저장)를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

액세스 제어 정책용 로깅 설정

액세스 제어 정책 로깅에 대한 설정을 통해 현재 액세스 제어 정책에 대한 기본 **syslog** 대상 및 **syslog** 알림을 구성할 수 있습니다. 포함된 규칙 및 정책의 **syslog** 대상 설정이 사용자 정의 설정으로 명시적으로 무시되지 않는 한 설정은 액세스 제어 정책 및 포함된 모든 **SSL**, 사전 필터 및 침입 정책에 적용됩니다.

기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화됩니다.

기본 **Syslog** 설정

Send using specific syslog alert(특정 **syslog** 알림을 사용하여 전송): 이 옵션을 선택하면 **Syslog 알림 응답 생성**의 지침에 따라 구성된 대로 선택한 **syslog** 알림을 기반으로 이벤트가 전송됩니다. 목록에서 **syslog** 알림을 선택하거나 이름, 로깅 호스트, 포트, 기능 및 심각도를 지정하여 **syslog** 알림을 추가할 수 있습니다. 자세한 내용은 [침입 시스템 로그 알림에 대한 시설 및 Severities\(심각도\)](#)를 참조하십시오. 이 옵션은 모든 디바이스에 적용할 수 있습니다.

FTD 6.3 이상: 디바이스에 구축된 **FTD Platform Settings** 정책에 구성된 **syslog** 설정 사용: 이 옵션을 선택하고 심각도를 선택하면 선택한 심각도와 함께 연결 또는 침입 이벤트가 플랫폼 설정에서 구성된 **syslog** 수집기로 전송됩니다. 이 옵션을 사용하면 플랫폼 설정에서 구성하고 액세스 제어 정책의 설정을 다시 사용하여 **syslog** 구성을 통합할 수 있습니다. 이 섹션에서 선택한 심각도는 모든 연결 및 침입 이벤트에 적용됩니다. 기본 심각도는 **ALERT**입니다.

이 옵션은 Firepower Threat Defense 디바이스 6.3 이상에만 적용됩니다.




참고 두 옵션을 선택하는 경우 옵션의 동작이 변경됩니다. 동적 요약 섹션에는 선택 결과가 표시됩니다.

File and Malware Settings(파일 및 악성코드 설정)는 일반적으로 **syslog** 메시지를 보내는 페이지 위쪽의 옵션을 선택한 후에만 적용됩니다.

액세스 제어 정책 고급 설정

고급 액세스 제어 정책 설정은 일반적으로 약간의 변경이 필요하거나 변경이 필요하지 않습니다. 기본 설정은 대부분의 배포에 적합합니다. 액세스 제어 정책의 여러 고급 사전 처리 및 성능 옵션은 [침입 규칙 업데이트](#)에 설명된 규칙 업데이트에 의해 수정될 수 있습니다.

보기 아이콘(보기 ())이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy**(기본 정책에서 상속)의 선택을 취소하여 수정을 활성화합니다.



주의 트래픽 검사를 일시적으로 중단하는 **Snort** 프로세스를 재시작하는 고급 설정 수정 목록은 [구축 또는 활성화 시 Snort 프로세스를 재시작하는 키프그레이션을 확인하세요](#). 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 [Snort® 재시작 트래픽 동작](#)을 참고하십시오.

일반 설정

옵션	설명
연결 이벤트에 저장하고자 하는 최대 URL 문자	사용자가 요청한 각 URL에 저장하는 문자 수를 사용자 정의하려면 긴 URL의 로깅 제한 을 참고하십시오. 사용자가 최초 차단을 건너뛴 후 웹사이트를 다시 차단하기 전에 걸린 시간을 맞춤화하려면, 차단된 웹사이트의 사용자 우회 시간 제한 설정 를 참고하십시오.
인터랙티브 차단을 허용하여 다음 시간(초) 동안 차단 바이패스	차단된 웹사이트의 사용자 우회 시간 제한 설정 의 내용을 참조하십시오.
DNS 트래픽에 대한 평판 시행 활성화	이 기능은 릴리스 6.7 에서 실험적으로 제공됩니다. 따라서 예상대로 작동하지 않을 수 있습니다. 프로덕션 환경에서는 사용하지 마십시오. Enable this option(이 옵션 활성화) 활성화됩니다. 자세한 내용 및 추가 지침은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타) 및 하위 주제를 참조하십시오.

옵션	설명
정책 적용 중에 트래픽 검사	<p>특정 설정이 Snort 프로세스 재시작을 필요로 하지 않는 경우 구축 설정을 변경할 때 트래픽을 검사하려면 정책 적용 중 트래픽 검사가 기본 값(활성화)로 설정되어 있는지 확인해야 합니다.</p> <p>이 옵션이 활성화된 경우 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그 레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 시나리오를 참조하십시오.</p>

관련 정책

고급 설정을 사용해 액세스 제어와 하위 정책(SSL, ID,)을 연결하려면 [액세스 제어에 다른 정책 연결, 16 페이지](#)를 참조하십시오.

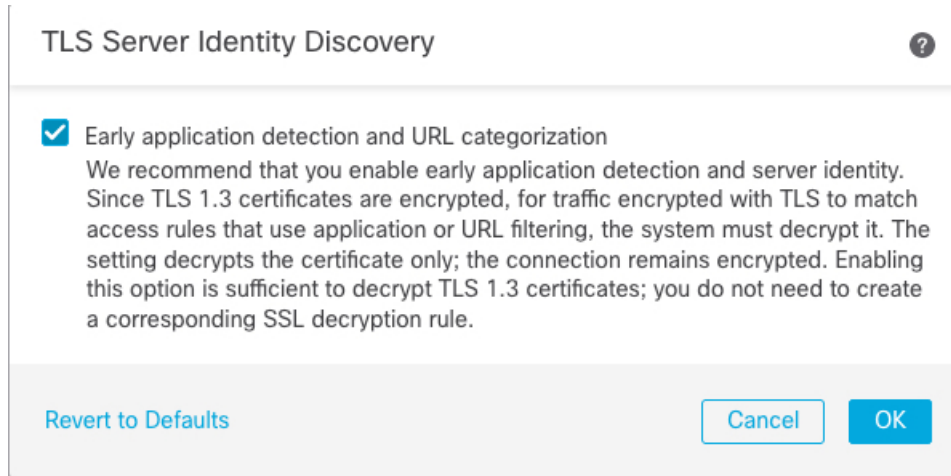
TLS 서버 ID 검색

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.

다음과 같은 경우, TLS 서버 ID 검색이라고 하는 기능을 활성화할 수 있습니다.

- SSL 정책을 액세스 제어 정책과 연결
- 액세스 제어 정책에 대한 고급 설정 설정

새 액세스 제어 정책을 생성하면 **Advanced(고급)** 탭에 기능 활성화를 고려해야 한다는 경고가 표시됩니다. 다음 그림과 같이 제어 항목을 Enabled(활성화됨)로 이동하면 경고 메시지에서 이를 확인할 수 있습니다.



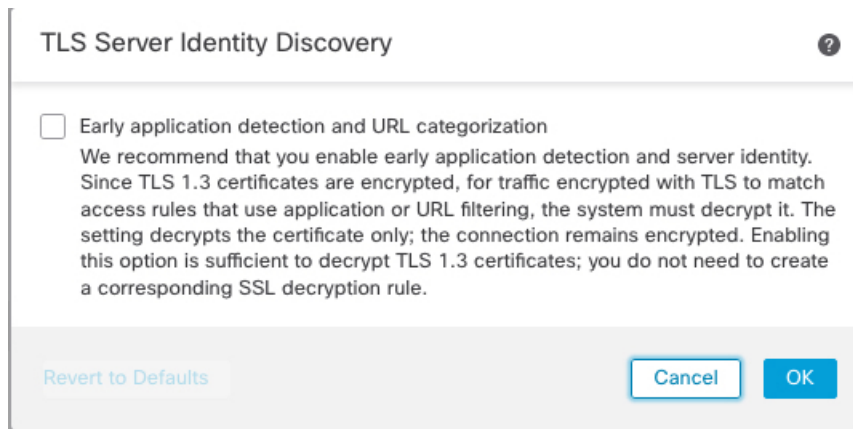
애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.



참고

- TLS 서버 ID 검색은 하드웨어 플랫폼에 따라 성능을 저하시킬 수 있습니다.
- TLS 서버 ID 검색은 인라인 탭 모드 또는 패시브 모드 구축에서 지원되지 않습니다.

다음 그림에는 액세스 제어 정책의 고급 설정에서 TLS 서버 ID 검색을 활성화하는 예가 나와 있습니다.



네트워크 분석 및 침입 정책

고급 네트워크 분석 및 침입 정책을 설정하면 다음을 수행할 수 있습니다.

- 시스템이 트래픽을 검사하는 방법을 정확히 결정하기 전에 통과해야 하는 패킷을 검사하는 데 사용되는 침입 정책 및 관련 변수 세트를 지정합니다.
- 다양한 사전 처리 옵션을 제어하는 액세스 제어 정책의 기본 네트워크 분석 정책을 변경합니다.

- 사전 처리 옵션을 특정 보안 영역, 네트워크, VLAN에 맞춰 조정하기 위해 맞춤형 네트워크 분석 규칙과 네트워크 분석 정책을 사용합니다.

자세한 내용은 [네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정](#)를 참고하십시오.

위협 방어 서비스 정책

특정 트래픽 클래스에 서비스를 적용하기 위해 위협 방어 서비스 정책을 사용할 수 있습니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 컨피그레이션을 만드는 서비스 정책을 사용할 수 있습니다. 이 정책은 Firepower Threat Defense 디바이스에만 적용되며 다른 디바이스 유형에 대해서는 무시됩니다. 서비스 정책 규칙은 액세스 제어 규칙 이후에 적용됩니다. 자세한 내용은 [Threat Defense Service 정책](#)를 참고하십시오.

파일 및 악성코드 설정

[파일 및 악성코드 탐지 성능 및 저장 조정](#)은 파일 컨트롤 및 AMP for Networks 에 대한 성능 옵션과 관련된 정보를 제공합니다.

Intelligent Application Bypass Settings(IAB(Intelligent Application Bypass) 설정)

IAB(Intelligent Application Bypass)는 트래픽이 검사 성능 및 플로우 임계값 조합을 초과하는 경우 건너뛴 애플리케이션이나 우회할 테스트를 지정하는 전문가 레벨 컨피그레이션입니다. 자세한 내용은 [IAB\(Intelligent Application Bypass\)](#)를 참고하십시오.

전송/네트워크 레이어 전처리 설정

고급 전송 및 네트워크 전처리 설정은 액세스 제어 정책을 배포하는 모든 네트워크, 영역 및 VLAN에 글로벌로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다. 자세한 내용은 [고급 전송/네트워크 전처리기 설정](#)를 참고하십시오.

탐지 향상 설정

고급 탐지 개선 설정을 통해 적응형 프로파일을 사용하여 호스트 운영 체제에 따라 수동 구축에서 패킷 프래그먼트 및 TCP 스트림 리어셈블리를 개선할 수 있습니다. 자세한 내용은 [적응형 프로파일](#)을 참고하십시오.

성능 설정 및 대기 시간 기반 성능 설정

[침입 방지 성능 조정 정보](#)는 시도된 침입의 트래픽을 분석할 때 시스템 성능 향상에 관한 정보를 제공합니다.

레이턴시 기반 성능 설정 관련 정보는 [패킷 및 침입 규칙 레이턴시 임계값 구성](#)을 참조하십시오.

액세스 제어에 다른 정책 연결

액세스 제어 정책의 고급 설정을 사용하여 다음 각각의 하위 정책 중 하나를 액세스 제어 정책과 연결합니다.

- SSL 정책 — SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security)로 암호화된 애플리케이션 레이어 프로토콜 트래픽을 모니터링, 암호 해독, 차단하거나 허용합니다.



주의 SSL 정책을 추가 또는 제거하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 [Snort® 재시작 트래픽 동작](#)을 참고하십시오.

- ID 정책 — 영역 및 트래픽과 관련된 인증 방법에 따라 사용자 인증을 수행합니다.

시작하기 전에

SSL 정책을 액세스 제어 정책과 연결하기 전에 [액세스 제어 정책 고급 설정, 13 페이지](#)에서 TLS 서버 ID 검색에 대한 정보를 검토합니다.

프로시저

단계 1 액세스 제어 정책 편집기에서 **Advanced Settings**(고급 설정)를 클릭합니다.

단계 2 해당하는 **Policy Settings**(정책 설정) 영역에서 수정(✎)을 클릭합니다.

보기 아이콘(보기 (👁))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy**(기본 정책에서 상속)의 선택을 취소하여 수정을 활성화합니다.

단계 3 드롭다운 목록에서 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, 표시된 편집 내용을 클릭하여 정책을 수정할 수 있습니다.

단계 4 **OK**(확인)를 클릭합니다.

단계 5 **Save**(저장)를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

관련 항목

[Snort® 재시작 시나리오](#)

정책 적중 횟수 보기

적중 횟수는 정책 규칙이 일치하는 연결을 트리거한 횟수를 나타냅니다. 이 정보를 사용하여 규칙의 효과를 식별할 수 있습니다. 적중 횟수 정보는 액세스 제어 및 FTD 디바이스에 적용되는 사전 필터 규칙에만 사용할 수 있습니다. 지원되는 정책의 경우 적중 횟수 정보는 정책에 대해 설정된 기본 작업에 대해서도 표시됩니다.



참고

- Firepower Threat Defense 디바이스가 리부팅되면 모든 적중 횟수 정보가 재설정됩니다.
- 디바이스에서 구축이나 작업이 진행 중일 때 적중 횟수 정보를 얻을 수 없습니다.

프로시저

- 단계 1** 액세스 제어 또는 사전 필터 정책 페이지로 이동합니다.
- 단계 2** 적중 횟수 정보를 확인하려는 정책을 클릭합니다.
- 단계 3** 정책 페이지의 오른쪽 상단에서 **Analyze Hit Counts**(적중 횟수 분석)를 클릭합니다.
- 단계 4** Hit Count(적중 횟수) 페이지에서 **Select a device**(디바이스 선택) 드롭다운 목록에서 디바이스를 선택합니다.

참고 이 디바이스에 대한 적중 횟수를 생성하는 것이 처음이 아닌 경우 드롭다운 상자 옆에 마지막으로 조회된 적중 횟수 정보가 표시됩니다. 또한 **Last Deployed**(마지막 구축) 시간을 확인하여 최근 정책 변경 내용을 확인합니다.
- 단계 5** 적중 횟수 데이터를 얻으려면 현재 **Fetch Current Hit Count**(현재 적중 횟수 검색)를 클릭합니다.

선택한 디바이스에 대한 적중 횟수 정보에 처음 액세스하는 것이 아니라면, **Fetch Current Hit Count**(현재 적중 횟수 검색) 대신 **Refresh**(새로 고침)가 표시됩니다. 최신 적중 횟수 정보를 얻으려면 **Refresh**(새로 고침)를 클릭하십시오.
- 단계 6** (선택 사항) 톱니바퀴(⚙️)와 함께 **Filter Rules/Policy**(필터 규칙/정책) 상자 또는 **Filter by**(필터 기준) 및 **In Last**(마지막) 드롭다운 상자를 사용하여 테이블 내의 테이블 및 목록을 사용자 지정합니다.

Filter by(필터 기준) 드롭다운 상자는 중요한 규칙을 식별하는 데 도움이 되는 **Hit Rules**(적중 규칙) 및 **Never Hit Rules**(적중 실패 규칙)와 같은 중요한 필터 옵션을 제공합니다. **In Last**(마지막) 드롭다운 상자에서는 사전 설정된 기간을 기준으로 규칙을 필터링하는 옵션을 제공합니다.
- 단계 7** (선택 사항) 규칙 이름을 클릭하여 편집하거나 마지막 열의 보기(👁️)을 클릭하여 규칙 세부 정보를 봅니다.

규칙 이름을 클릭하면 편집할 수 있는 정책 페이지에서 규칙 이름이 강조 표시됩니다.

참고 액세스 제어 정책 페이지에서 Hit Count(적중 횟수) 페이지에 액세스한 경우 사전 필터 규칙을 보거나 편집할 수 없으며 그 반대의 경우도 마찬가지입니다.

- 단계 8** (선택 사항) 규칙을 오른쪽 클릭하고 **Clear Hit Count**(적중 횟수 지우기)를 선택하여 규칙의 적중 횟수 정보를 지웁니다.

여러 규칙의 적중 횟수 정보를 지우려면 **Ctrl** 버튼을 사용하여 여러 규칙을 선택하고, 선택한 규칙 중 하나를 마우스 오른쪽 버튼으로 클릭한 후 **Clear Hit Count**(적중 횟수 지우기)를 선택하면 됩니다.

참고 적중 횟수 정보를 지우면 적중 횟수가 0으로 설정되며, 이 변경 사항은 취소할 수 없습니다.
- 단계 9** (선택 사항) 페이지의 왼쪽 하단에 있는 **Generate CSV**(CSV 생성)를 클릭하여 페이지의 세부 정보에 대한 CSV 보고서를 생성합니다.
- 단계 10** **Close**(닫기)를 클릭하여 **Policy**(정책) 페이지로 돌아갑니다.

액세스 제어 정책 히스토리

기능	버전	세부 사항
DNS 필터링	6.7(실험)	<p>URL 필터링이 활성화 및 구성된 경우 범주 및 평판 필터링 효율성을 개선하기 위한 새 옵션이 각 새 액세스 제어 정책에 대해 사용할 수 있습니다.</p> <p>중요! 이는 실험적인 기능이며 예상대로 작동하지 않을 수 있습니다. 프로덕션 환경에서는 사용하지 마십시오.</p> <p>자세한 내용은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타) 및 하위 항목을 참조하십시오.</p> <p>수정된 화면 : 액세스 제어 정책의 Advanced(고급) 탭에 General Settings(일반 설정) : Enable reputation enforcement on DNS traffic(DNS 트래픽에서 평판 시행 활성화) 아래에 새 옵션이 있습니다.</p> <p>지원되는 플랫폼: 전체</p>

기능	버전	세부 사항
TLS 서버 ID 검색	6.7	<p>클라이언트가 TLS 1.3 지원 서버에 연결할 때 URL 및 애플리케이션 조건을 평가하도록 액세스 제어 정책을 활성화합니다. TLS 서버 ID 검색을 사용하면 트래픽 암호 해독 없이 이러한 조건을 평가할 수 있습니다.</p> <p>참고: 이 기능을 활성화하면 매니지드 디바이스 모델에 따라 성능에 영향을 줍니다.</p> <p>수정된 화면: 액세스 제어 정책의 고급 탭 페이지에 새로운 옵션이 추가되었습니다.</p> <ul style="list-style-type: none"> • Advanced(고급) 탭에 경고가 표시됩니다. 슬라이더를 오른쪽으로 이동하면 TLS 서버 ID 검색이 활성화됩니다. • Advanced(고급) 탭 페이지의 새로운 옵션: TLS Server Identity Discovery(TLS 서버 ID 검색)
새로운 보안 인텔리전스 범주	--	<p>다음 범주는 6.6 릴리스 시점에 도입되었지만 6.6에만 해당되지는 않습니다.</p> <ul style="list-style-type: none"> • banking_fraud • high_risk • ioc • link_sharing • 발생하는 것만은 아님 • newly_seen • 스파이웨어 <p>신규/수정된 페이지: Access control policy(액세스 제어 정책) > Security Intelligence(보안 인텔리전스) 탭</p> <p>지원되는 플랫폼: FMC</p>