



## 액세스 제어 규칙

다음 주제에서는 액세스 제어 규칙을 구성하는 방법을 설명합니다.

- 액세스 제어 규칙 소개, 1 페이지
- 액세스 제어 규칙 요구 사항 및 사전 요건, 6 페이지
- 액세스 제어 규칙 범주 추가, 7 페이지
- 액세스 제어 규칙 생성 및 수정, 7 페이지
- 액세스 제어 규칙 활성화 및 비활성화, 9 페이지
- 하나의 액세스 제어 정책에서 다른 정책으로 액세스 제어 규칙 복사, 10 페이지
- 사전 필터 정책으로 액세스 제어 규칙 이동, 10 페이지
- 액세스 제어 규칙 포지셔닝, 13 페이지
- 액세스 제어 규칙 작업, 14 페이지
- 액세스 제어 규칙 코멘트, 17 페이지
- 액세스 컨트롤 규칙 기록, 18 페이지

## 액세스 제어 규칙 소개

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

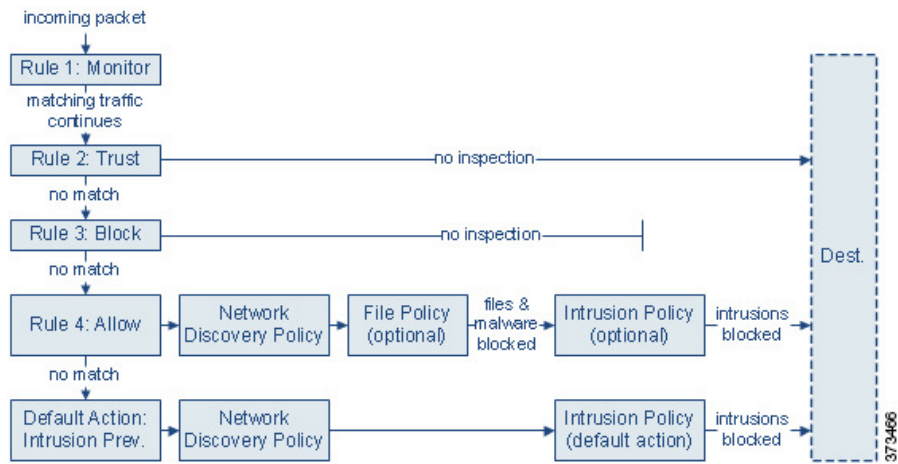


**참고** 8000 시리즈 단축 경로 지정, 보안 인텔리전스 필터링, SSL 검사, 사용자 식별, 일부 디코딩 및 전처리하는 액세스 컨트롤 규칙이 네트워크 트래픽을 평가하기 전에 수행됩니다.

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, 14 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 작업**은 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.

SSL 검사 구성에서 암호화 트래픽의 통과를 허용하는 경우 또는 SSL 검사를 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 **Rules(규칙)** 탭에서는 현재 정책의 액세스 제어 규칙을 추가, 편집, 분류, 검색, 필터링, 이동, 활성화, 비활성화, 삭제하고 그 밖의 방식으로 관리할 수 있습니다. 검색 표시줄을 사용하여 액세스 제어 정책 규칙 목록을 필터링합니다. 필터 기준과 일치하는 규칙 목록 및 현재 액세스 제어 정책의 모든 규칙을 전환하려면 **Toggle(전환)**을 클릭합니다.

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()
- 침입 정책()
- 파일 정책()
- 로깅()
- 코멘트()
- 경고()
- 오류()
- 중요 정보()

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

규칙을 생성하거나 편집하려면 액세스 제어 규칙 편집기를 사용합니다. 다음 작업을 수행할 수 있습니다.

- 편집기의 상단에서 규칙의 이름, 상태, 위치 및 작업과 같은 기본 속성을 구성합니다.
- 편집기 하단의 왼쪽 탭을 사용하여 조건을 추가합니다.
- 편집기 하단의 오른쪽 탭을 사용하여 검사 및 로깅 옵션을 구성하고 규칙에 코멘트를 추가합니다. 편의를 위해, 사용자가 어떤 탭에 있든 편집기에는 규칙의 검사 및 로깅 옵션이 나열됩니다.



**참고** 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.

관련 항목

- [액세스 제어 규칙 구성 요소, 4 페이지](#)
- [예: 맞춤형 사용자 역할 및 액세스 제어](#)
- [맞춤형 사용자 역할 생성](#)
- [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 규칙의 모든 탭에 지정된 조건을 전부 충족해야 합니다. 예를 들어, Applications(애플리케이션) 탭에서 HTTPS는 지정하지 않고 HTTP를 지정하는 경우, URLs 탭의 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, 7 페이지](#)
- [규칙 조건 유형](#)
- [액세스 제어 규칙 작업, 14 페이지](#)
- [파일 및 침입 정책을 사용한 심층 검사](#)
- [연결 로깅 모범 사례](#)
- [액세스 제어 규칙 코멘트, 17 페이지](#)

**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(필수)** 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.



**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 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

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

## 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** **OK**(확인)를 클릭합니다.

**단계 5** **Save**를 클릭하여 정책을 저장합니다.

### 다음에 수행할 작업

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

## 액세스 제어 규칙 생성 및 수정

능동적으로 사용 중인 액세스 제어 규칙을 수정한다면, 구축 시 설정된 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.



Firepower Threat Defense의 경우에는 설정된 연결을 FTD **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.

프로시저

단계 1 액세스 제어 정책 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하려면 **Add Rule**(규칙 추가)을 클릭합니다.
- 기존 규칙을 수정하려면 수정(✎)을 클릭합니다.
- 여러 규칙을 편집하려면 규칙 범위를 Shift 키를 누른 상태에서 클릭하거나 편집할 여러 규칙을 Ctrl 키를 누른 상태에서 마우스 오른쪽 버튼을 클릭하고 옵션을 선택합니다.

규칙 옆에 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 설정하거나 기본값을 승인합니다.

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

- Enabled(활성화) — 규칙이 **Enabled**(활성화) 상태인지 여부를 지정합니다.
- Position(위치) — 규칙 위치를 지정합니다(액세스 제어 규칙 순서, 5 페이지 참조).
- Action(작업) — 규칙 **Action**(작업)을 선택합니다(액세스 제어 규칙 작업, 14 페이지 참조).

참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. 방화벽 인터페이스에 적용된 액세스 규칙에는 사용할 수 없습니다.

- Time Range(시간 범위) — (FTD 디바이스에서만 지원됨) 규칙을 적용할 수 있는 날짜와 시간을 추가하거나 선택합니다. 자세한 내용은 [시간 범위 개체 생성](#) 섹션을 참조하십시오.
- Conditions(조건) — 추가할 조건에 해당하는 항목을 클릭합니다. 자세한 내용은 [규칙 조건 유형](#)의 내용을 참조하십시오.
- Deep Inspection(심층 검사)—Allow and Interactive Block(허용 및 인터랙티브 차단) 규칙의 경우, 침입 정책(🛡) 또는 파일 정책(📁)을 클릭하여 규칙의 **Inspection**(검사) 옵션을 설정합니다. 옵션이 흐리게 표시되면, 규칙에 해당 유형의 정책이 선택되지 않은 것입니다. 자세한 내용은 [액세스 제어의 이해](#)를 참조하십시오.
- Logging(로깅) — 로깅(📄)을 클릭하여 **Logging**(로깅) 옵션을 지정합니다. 옵션이 흐리게 표시되면, 규칙에 연결 로깅이 비활성화된 것입니다. 자세한 내용은 [연결 로깅 모범 사례](#)를 참조하십시오.



- **Comments(코멘트)** — 코멘트 열의 번호를 클릭하여 **Comments(코멘트)**를 추가합니다. 번호는 규칙에 이미 포함된 코멘트의 수를 나타냅니다. 자세한 내용은 [액세스 제어 규칙 코멘트, 17 페이지](#)를 참조하십시오.

단계 4 규칙을 저장합니다.

단계 5 **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

시간 기반 규칙을 구축할 경우, 정책이 할당된 디바이스의 표준 시간대를 지정합니다. [정책 애플리케이션에 대한 디바이스 표준 시간대 구성](#)의 내용을 참조하십시오.

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

관련 항목

[액세스 제어 규칙 순서에 대한 모범 사례](#)

## 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.



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

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.

시작하기 전에

계속하기 전에 다음 사항에 유의하십시오.

- 주석을 제외한 복사된 규칙의 모든 설정은 붙여 넣은 버전으로 유지됩니다. 그러나 소스 액세스 제어 정책을 언급하는 새로운 주석이 복사된 규칙에 추가됩니다.

프로시저

단계 1 액세스 제어 정책 편집기에서 마우스 왼쪽 버튼을 클릭하여 복사할 규칙을 선택합니다.

팁 여러 규칙을 선택하려면 키보드에서 Ctrl(컨트롤) 키를 사용합니다.

단계 2 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Copy to**(복사 대상) > **Another policy**(다른 정책)를 선택합니다.

단계 3 **Access Policy**(액세스 정책) 드롭 다운 목록에서 대상 액세스 제어 정책을 선택합니다.

단계 4 **Place Rules**(규칙 배치) 드롭 다운 목록에서 복사한 규칙을 배치할 위치를 선택합니다.

- **Default**(기본값) 섹션에서 마지막 규칙 집합으로 배치하려면 **At the bottom**(맨 아래)(**Default**(기본) 섹션 내)를 선택합니다.
- **Mandatory**(의무) 섹션에서 첫번째 규칙 집합으로 배치하려면 **At the top**(맨 위)(**Mandatory**(의무) 섹션 내)를 선택합니다.

단계 5 **Copy**(복사)를 클릭합니다.

다음에 수행할 작업

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

## 사전 필터 정책으로 액세스 제어 규칙 이동

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

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
차단	Block(차단)
Block with Reset(차단 후 재설정)	Block(차단)
인터랙티브 차단(Block)	Block(차단)
재설정 인터랙티브 차단(Block)	Block(차단)
신입	Fastpath(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.
Block(차단)	<ul style="list-style-type: none"> <li>• Log at Beginning of Connection(연결 시작 시 로깅)</li> <li>• 이벤트 뷰어</li> <li>• Syslog 서버</li> <li>• SNMP 트랩</li> </ul>

액세스 제어 규칙 작업	사전 필터 규칙에서 활성화된 로깅 구성
Block with Reset(차단 후 재설정)	<ul style="list-style-type: none"> <li>• Log at Beginning of Connection(연결 시작 시 로깅)</li> <li>• 이벤트 뷰어</li> <li>• Syslog 서버</li> <li>• SNMP 트랩</li> </ul>
인터랙티브 차단(Block)	<ul style="list-style-type: none"> <li>• Log at Beginning of Connection(연결 시작 시 로깅)</li> <li>• 이벤트 뷰어</li> <li>• Syslog 서버</li> <li>• SNMP 트랩</li> </ul>
재설정 인터랙티브 차단(Block)	<ul style="list-style-type: none"> <li>• Log at Beginning of Connection(연결 시작 시 로깅)</li> <li>• 이벤트 뷰어</li> <li>• Syslog 서버</li> <li>• SNMP 트랩</li> </ul>
신입	<ul style="list-style-type: none"> <li>• Log at Beginning of Connection(연결 시작 시 로깅)</li> <li>• Log at End of Connection(연결 종료 시 로깅)</li> <li>• 이벤트 뷰어</li> <li>• Syslog 서버</li> <li>• SNMP 트랩</li> </ul>

- 기본 사전 필터 정책에는 규칙을 사용할 수 없으므로 액세스 제어 규칙을 기본 사전 필터 정책으로 이동할 수 없습니다.
- 소스 정책에서 규칙을 이동하는 동안 다른 사용자가 해당 규칙을 수정하면 FMC에 메시지가 표시됩니다. 페이지를 새로 고침 후 프로세스를 계속 진행할 수 있습니다.

프로시저

단계 1 액세스 제어 정책 편집기에서 마우스 왼쪽 버튼을 클릭하여 이동할 규칙을 선택합니다.

팁 여러 규칙을 선택하려면 키보드에서 Ctrl(컨트롤) 키를 사용합니다.

단계 2 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Move to another policy**(다른 정책으로 이동)를 선택합니다.

단계 3 **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 4 **Move**(이동)를 클릭합니다.

다음에 수행할 작업

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

## 액세스 제어 규칙 포지셔닝

액세스 제어 정책 내에서 기존 규칙을 이동할 수 있습니다. 카테고리에 규칙을 추가하거나 카테고리로 규칙을 이동하면 시스템은 해당 규칙을 카테고리 마지막에 배치합니다.



팁 여러 규칙을 선택한 다음 마우스 오른쪽 버튼 메뉴를 사용하여 잘라 붙여 넣으면 한 번에 여러 규칙을 이동할 수 있습니다.

시작하기 전에

[액세스 제어 규칙 순서에 대한 모범 사례](#)에서 규칙 순서 지침을 검토합니다.

프로시저

단계 1 액세스 제어 규칙 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하는 경우, **Insert**(삽입) 드롭다운 목록을 사용합니다.
- 기존 규칙을 수정하는 경우, **Move**(이동)를 클릭합니다.

단계 2 규칙을 이동하거나 삽입할 곳을 선택합니다.

- **into Mandatory**(필수로) 또는 **into Default**(기본으로)를 선택합니다.
- **into Category**(카테고리로)를 선택한 다음 사용자 정의 카테고리를 선택합니다.

- **above rule**(규칙 위) 또는 **below rule**(규칙 아래)를 선택한 다음 적절한 규칙 번호를 입력합니다.

단계 3 **Save**(저장)를 클릭합니다.

단계 4 **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

## 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 않았습니. 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 검사](#)을 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.

관련 항목

[모니터링된 연결에 대한 로깅](#)

## 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.

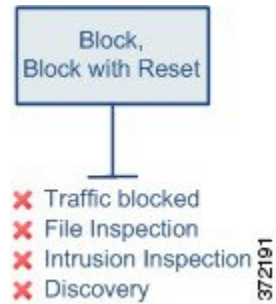


관련 항목

[신뢰할 수 있는 연결에 대한 로깅](#)

## 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 차단](#)를 참고하십시오.

관련 항목

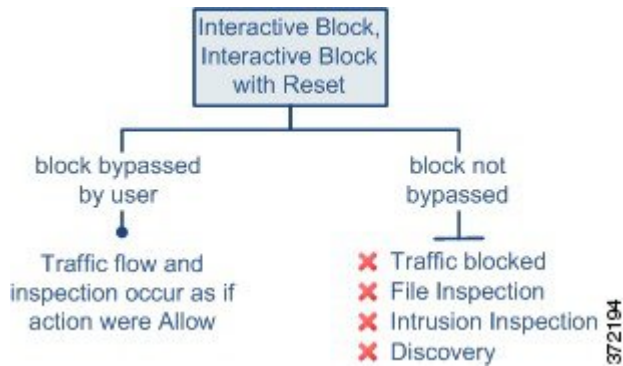
[차단된 연결에 대한 로깅](#)

[HTTP 응답 페이지 정보](#)

## 액세스 제어 규칙 인터랙티브 차단 작업

자세한 내용은 [HTTP 응답 페이지 및 인터랙티브 차단](#)를 참고하십시오.





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 차단](#)를 참고하십시오.

관련 항목

- [허용된 연결에 대한 로깅](#)
- [TLS/SSL 규칙 차단 작업](#)

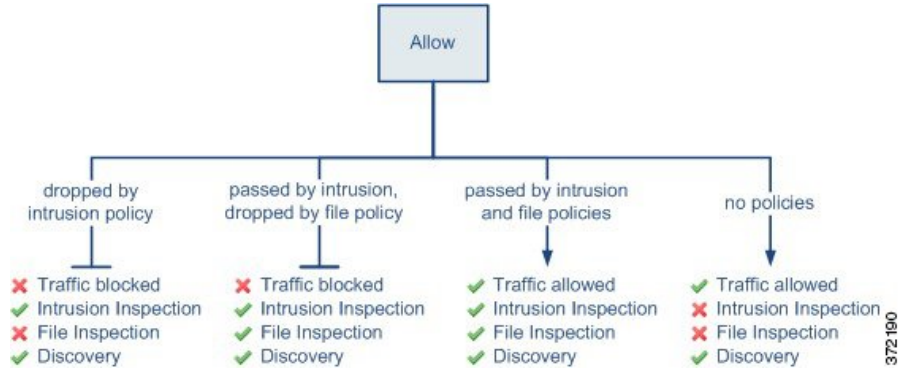
## 액세스 제어 규칙 허용 작업

**Allow**(허용) 작업은 일치하는 트래픽이 통과하도록 허용하지만 ID 요건과 속도 제한은 계속 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. AMP for Networks 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.

관련 항목

[허용된 연결에 대한 로깅](#)

## 액세스 제어 규칙 코멘트

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. [규칙 검색](#)의 내용을 참조하십시오.

관련 항목

[액세스 제어 정책 환경설정](#)

## 액세스 제어 규칙에 설명 추가

프로시저

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

단계 2 **New Comment**(새 코멘트)를 클릭합니다.

단계 3 코멘트를 입력하고 **OK**(확인)를 클릭합니다. 규칙을 저장할 때까지 이 코멘트를 수정하거나 삭제할 수 있습니다.

단계 4 **Save**(저장)를 클릭합니다.

단계 5 **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

## 액세스 컨트롤 규칙 기록

기능	버전	세부 사항
액세스 제어 규칙 코멘트 검색	6.7	이제 <b>Search Rules</b> (검색 규칙) 표시줄에 코멘트를 검색할 수 있는 옵션이 제공됩니다.  신규/수정된 페이지: <b>Access control rules</b> (액세스 제어 규칙) 페이지, <b>Search Rules</b> (검색 규칙) 텍스트 입력 필드  지원되는 플랫폼: FMC
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: <b>Access control policy</b> (액세스 제어 정책) 페이지 - 선택한 규칙에 대해 마우스 오른쪽 버튼을 클릭하면 복사 및 이동에 대한 추가 옵션이 제공됩니다.  지원되는 플랫폼: FMC

기능	버전	세부 사항
액세스 제어 규칙에서 특정 설정 대량 편집	6.6	<p>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.</p> <p>신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지</p> <p>지원되는 플랫폼: FMC</p>
설정된 규칙에 대한 향상된 검색	6.6	<p>설정된 규칙에 대한 검색을 개선했습니다.</p> <p>신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지</p> <p>지원되는 플랫폼: FMC</p>
규칙 애플리케이션의 시간 범위	6.6	<p>적용할 규칙에 대해 절대적이거나 반복되는 시간 또는 시간 범위를 지정할 수 있습니다. 규칙은 트래픽을 처리하는 디바이스의 표준 시간대에 따라 적용됩니다.</p> <p>신규/수정된 페이지:</p> <ul style="list-style-type: none"> <li>• Access Control Add Rule(액세스 제어 규칙 추가) 페이지의 새로운 옵션</li> <li>• 매니지드 디바이스의 표준 시간대를 지정하기 위한 <b>Devices</b>(디바이스) &gt; <b>Platform Settings</b>(플랫폼 설정) &gt; <b>FTD</b> 페이지의 관련 새 옵션</li> </ul> <p>지원되는 플랫폼: FTD 디바이스 전용</p>

기능	버전	세부 사항
<p>Access control rules(액세스 제어 규칙) 페이지에서 개체 세부 사항 보기</p>	<p>pre-6.6</p>	<p>규칙 목록 또는 규칙 설정 대화 상자에 서 개체에 대한 정보를 보려면 개체를 마우스 오른쪽 버튼으로 클릭합니다.</p> <p>신규/수정된 페이지: <b>Policies(정책)</b> &gt; <b>Access Control(액세스 제어)</b> &gt; <b>Access Control(액세스 제어)</b> 및 <b>Add Rule(규칙 추가)</b> 페이지</p> <p>지원되는 플랫폼: FMC</p>