FireSIGHT 시스템 컨피그레이션의 URL 필터링 예

목차

소개

이 문서에서는 FireSIGHT 시스템에서 URL 필터링을 구성하는 단계에 대해 설명합니다. FireSIGHT Management Center의 URL 필터링 기능을 사용하면 모니터링되는 호스트의 비암호화 URL 요청을 기반으로 네트워크를 통과하는 트래픽을 결정하기 위해 액세스 제어 규칙에 조건을 쓸 수 있습니다.

사전 요구 사항

요구 사항

이 문서에는 URL 필터링 라이센스 및 포트에 대한 몇 가지 특정 요구 사항이 있습니다.

URL 필터링 라이센스 요구 사항

FireSIGHT Management Center에서 URL 정보 업데이트를 위해 클라우드에 정기적으로 연결하려면 URL 필터링 라이센스가 필요합니다. URL 필터링 라이센스 없이 액세스 제어 규칙에 카테고리 및 평판 기반 URL 조건을 추가할 수 있습니다. 그러나 먼저 FireSIGHT Management Center에 URL 필터링 라이센스를 추가한 다음 정책 대상 디바이스에서 활성화해야 액세스 제어 정책을 적용할 수 있습니다.

URL Filtering 라이센스가 만료되면 카테고리 및 평판 기반 URL 조건의 액세스 제어 규칙이 URL 필터링을 중지하며, FireSIGHT Management Center에서 더 이상 클라우드 서비스에 연결하지 않습니다. URL 필터링 라이센스가 없으면 개별 URL 또는 URL 그룹을 허용하거나 차단하도록 설정할 수 있지만, URL 카테고리 또는 평판 데이터를 사용하여 네트워크 트래픽을 필터링할 수는 없습니다.

포트 요구 사항

FireSIGHT 시스템은 클라우드 서비스와 통신하기 위해 포트 443/HTTPS 및 80/HTTP를 사용합니다. 포트 443/HTTPS를 양방향으로 열어야 하며, 포트 80/HTTP에 대한 인바운드 액세스를 FireSIGHT Management Center에서 허용해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- FirePOWER 어플라이언스: 7000 시리즈, 8000 시리즈
- NGIPS(Next Generation Intrusion Prevention System) 가상 어플라이언스
- ASA(Adaptive Security Appliance) FirePOWER
- Sourcefire 소프트웨어 버전 5.2 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

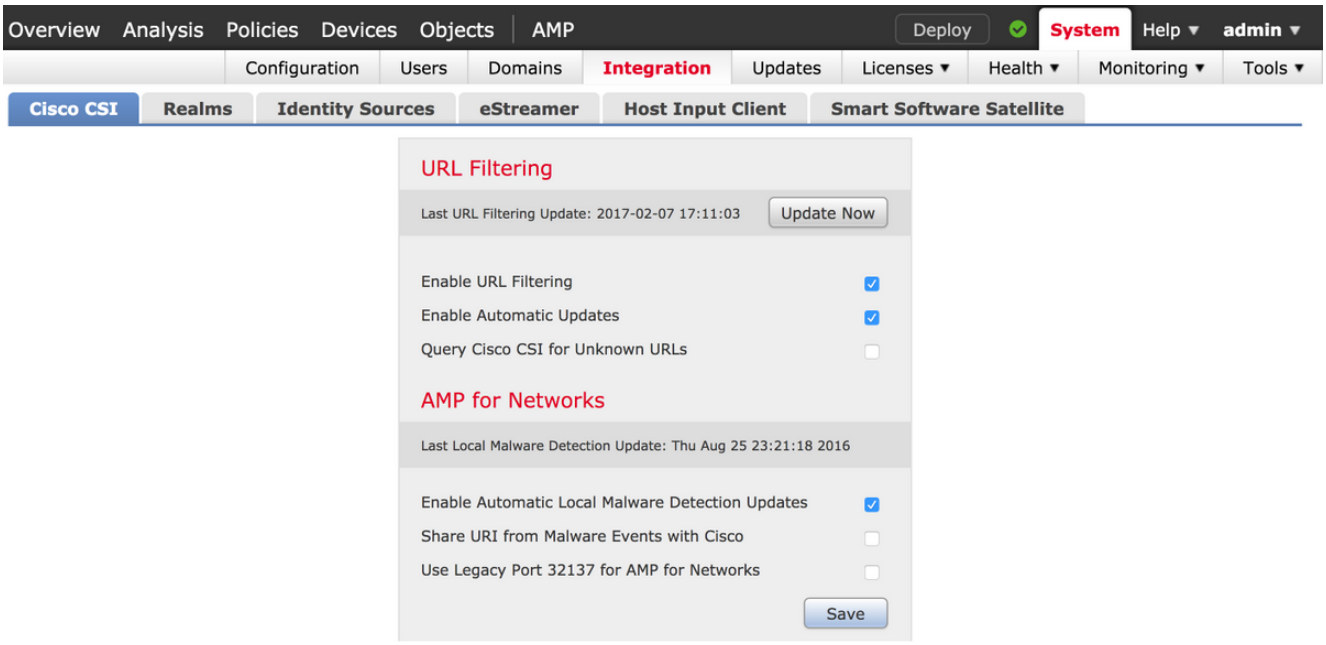
구성

FireSIGHT Management Center에서 URL 필터링 활성화

URL 필터링을 활성화하려면 다음 단계를 완료하십시오.

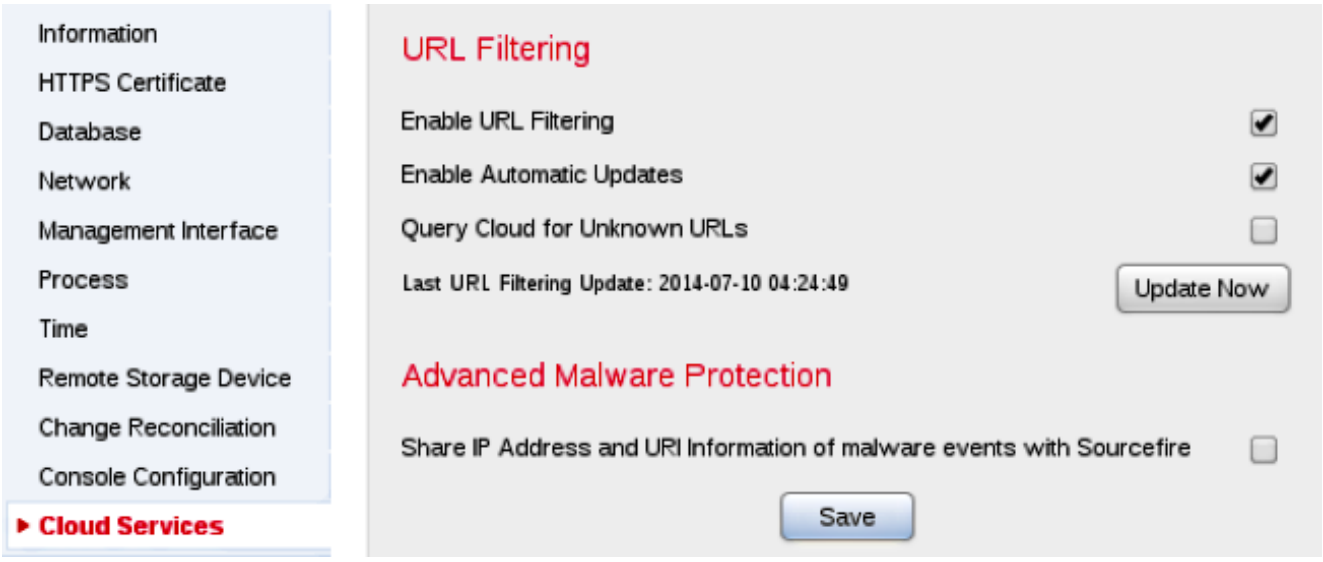
1. FireSIGHT Management Center의 웹 사용자 인터페이스에 로그인합니다.
2. 탐색은 실행하는 소프트웨어 버전에 따라 다릅니다.

   버전 6.1.x에서 **System > Integration > Cisco CSI를 선택합니다**.



   버전 5.x에서 **System > Local > Configuration**을 선택합니다. **Cloud Services(클라우드 서비스**

)**를** 선택합니다.



3. URL 필터링을 **활성화하려면** Enable URL Filtering 확인란을 선택합니다.
4. 선택적으로, 자동 **업데이트를** 활성화하려면 Enable Automatic Updates 확인란을 선택합니다. 이 옵션을 사용하면 시스템이 어플라이언스의 로컬 데이터 세트에서 URL 데이터에 대한 업데이트를 얻기 위해 정기적으로 클라우드 서비스에 연결할 수 있습니다.

   참고: 일반적으로 클라우드 서비스는 하루에 한 번 데이터를 업데이트하지만, 자동 업데이트를 활성화하면 FireSIGHT Management Center에서 정보가 항상 최신 상태인지 확인하기 위해 30분마다 확인해야 합니다. 일일 업데이트가 적은 편이지만, 마지막 업데이트 이후 5일 이상 지난 경우 새 URL 필터링 데이터를 다운로드하는 데 최대 20분이 소요될 수 있습니다. 업데이트가 다운로드되면 업데이트 자체를 수행하는 데 최대 30분이 소요될 수 있습니다.

5. 선택적으로, 클라우드 서비스**에 알 수 없는 URL**을 쿼리하려면 Query Cloud for Unknown URLs for Unknown URLs 확인란을 선택합니다. 이 옵션을 사용하면 모니터링되는 네트워크의 사용자가 로컬 데이터 집합에 없는 URL로 이동하려고 할 때 시스템에서 Sourcefire 클라우드를 쿼리할 수 있습니다. 클라우드가 URL의 카테고리 또는 평판을 알지 못하거나 FireSIGHT Management Center가 클라우드에 연결할 수 없는 경우, URL이 카테고리 또는 평판 기반 URL 조건과 함께 액세스 제어 규칙과 일치하지 않습니다.

   참고: URL에 카테고리 또는 평판을 수동으로 할당할 수 없습니다. 예를 들어 프라이버시의 이유로 분류되지 않은 URL을 Sourcefire 클라우드에서 카탈로그화하지 않으려면 이 옵션을 비활성화합니다.

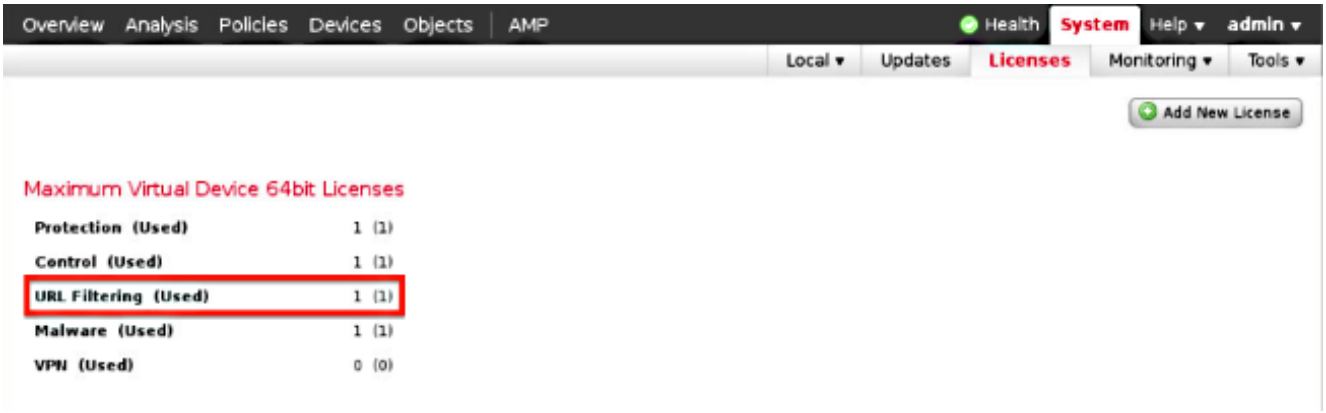
6. 저장을 **클릭합니다**. URL 필터링 설정이 저장됩니다.

   참고: URL 필터링이 마지막으로 활성화된 이후의 시간 또는 URL 필터링을 처음 활성화한 경우, FireSIGHT Management Center는 클라우드 서비스에서 URL 필터링 데이터를 검색합니다.

관리되는 디바이스에 URL 필터링 라이센스 적용

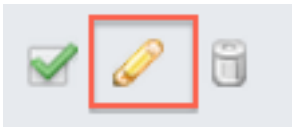
1. URL 필터링 라이센스가 FireSIGHT Management Center에 설치되어 있는지 확인합니다. 라

이센스 목록을 찾으려면 **System > Licenses** 페이지로 이동합니다.

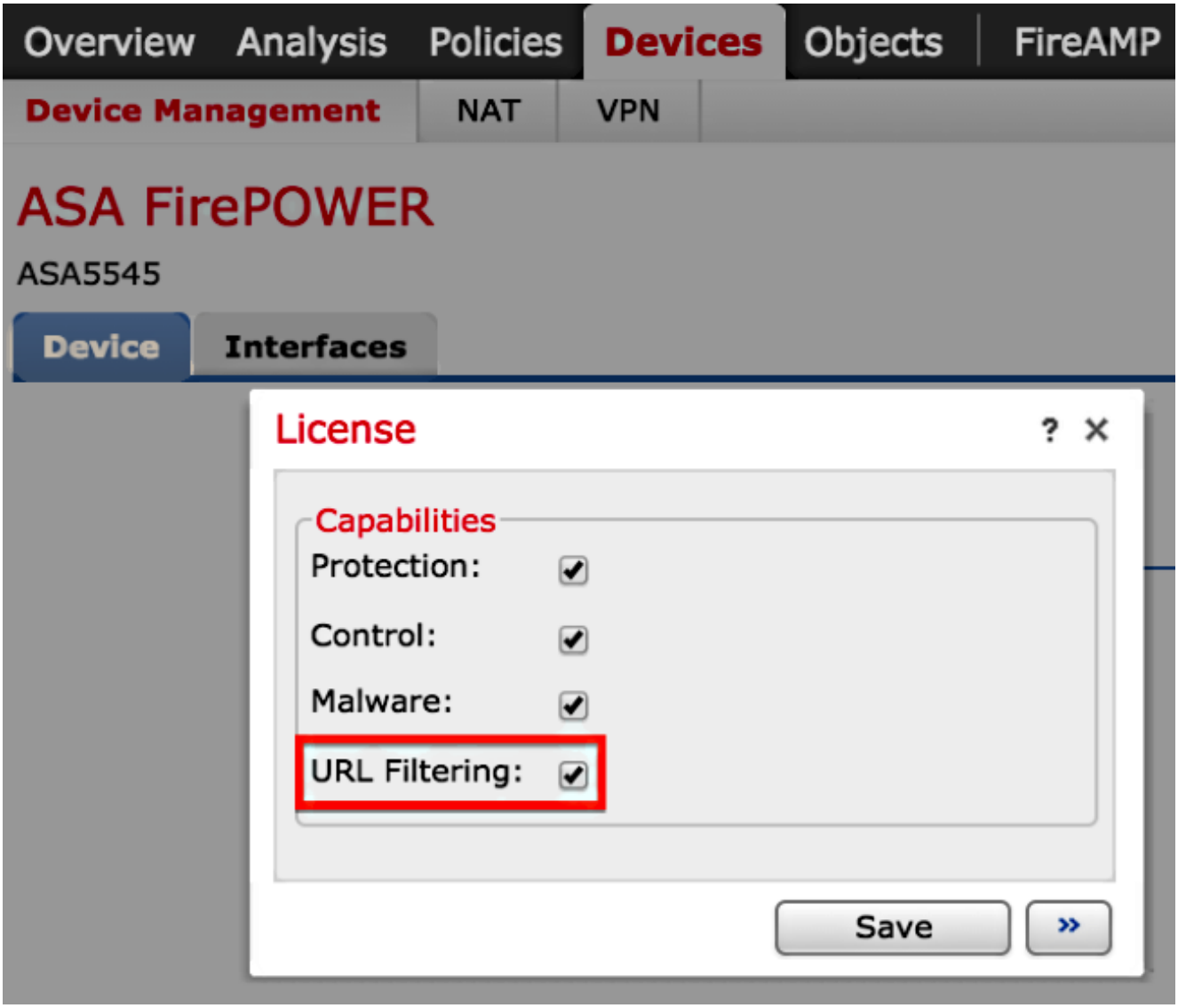


2. Devices(디바이스) **> Device Management(디바이스 관리)** 페이지로 이동하여 트래픽을 모니터링하는 디바이스에 URL Filtering 라이센스가 적용되었는지 확인합니다.

3. 디바이스에 URL 필터링 라이센스가 적용되지 않은 경우 설정을 수정하려면 **연필** 아이콘을 클릭합니다. 아이콘은 디바이스 이름 옆에 있습니다.



4. Devices 탭에서 디바이스에 URL Filtering 라이센스를 활성화할 **수** 있습니다.



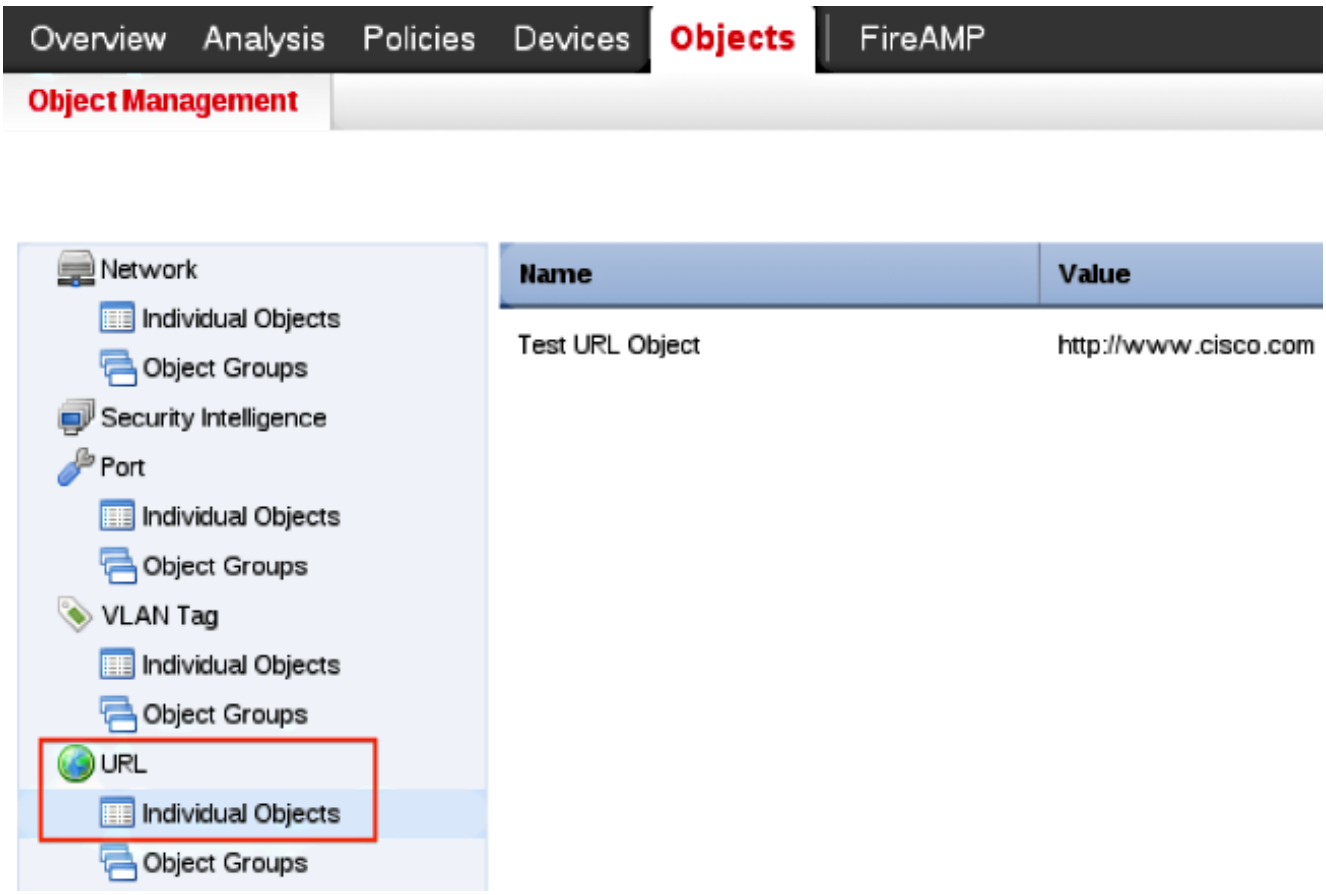
5. 라이센스를 활성화하고 변경 사항을 저장한 후, 관리되는 디바이스에 **라이센스**를 적용하려면 Apply Changes(변경 사항 적용)를 클릭해야 합니다.

차단된 URL 카테고리에서 특정 사이트 제외

FireSIGHT Management Center에서는 기본 Sourcefire 제공 카테고리 등급을 재정의하는 URL의 로컬 등급을 설정할 수 없습니다. 이 작업을 수행하려면 액세스 제어 정책을 사용해야 합니다. 이 지침은 특정 사이트를 차단 범주에서 제외하기 위해 액세스 제어 규칙에서 URL 객체를 사용하는 방법에 대해 설명합니다.

1. Objects(개체) **> Object Management(개체 관리)** 페이지로 이동합니다.

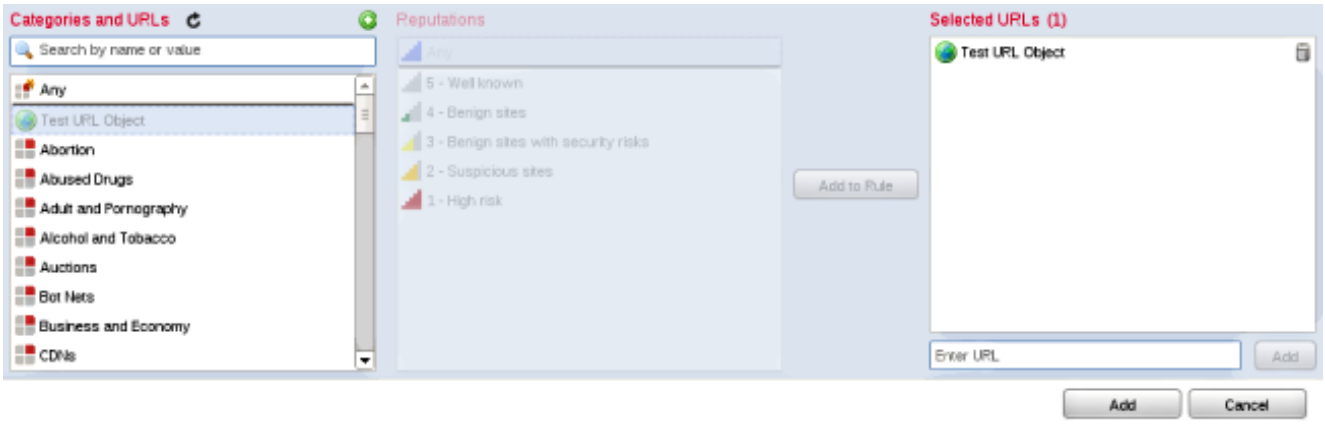
2. **Individual Objects** for URL을 선택하고 Add **URL(URL 추가) 버튼**을 클릭합니다. **URL Objects(URL 개체)** 창이 나타납니다.



3. 변경 사항을 저장한 후 Policies(정책) **> Access Control(액세스 제어)**을 선택하고 **연필** 아이콘을 클릭하여 액세스 제어 정책을 수정합니다.

4. Add **Rule(규칙 추가)**을 **클릭합니다**.

5. Allow(허용) 작업이 있는 규칙에 URL **객체**를 추가하고 URL Category(URL 카테고리) 규칙 위에 놓으면 규칙 작업이 먼저 평가됩니다.



6. 규칙을 추가한 후 Save and Apply**를 클릭합니다**. 새 변경 사항을 저장하고 액세스 제어 정책을 관리되는 어플라이언스에 적용합니다.

다음을 확인합니다.

정보 확인 또는 문제 해결에 대한 내용은 Related Information(관련 정보) 섹션에서 연결된 **Troubleshoot Issues with URL Filtering on FireSIGHT System(FireSIGHT 시스템에서 URL 필터링 관련 문제** 해결) 문서를 참조하십시오.

문제 해결

확인 또는 문제 해결 정보는 **FireSIGHT 시스템의 URL 필터링 문제 해결** 관련 정보 섹션에서 링크된 기사

관련 정보

- FireSIGHT 시스템의 URL 필터링 문제 해결
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.