

# FireSIGHT 시스템을 사용한 비디오 스트리밍 트래픽 탐지

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[비디오 스트리밍 트래픽 탐지](#)

[애플리케이션 필터 사용](#)

[비디오 스트리밍 트래픽 로깅](#)

## 소개

네트워크의 비디오 트래픽을 탐지하려면 FireSIGHT 시스템의 액세스 제어 기능 및 URL 필터링 기능을 사용할 수 있습니다. 이 문서에서는 이러한 목적으로 FireSIGHT 시스템을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서의 지침에 따라 FireSIGHT Management Center에 Control 라이선스 및 URL Filter 라이선스가 설치되어 있어야 합니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- FireSIGHT Management Center
- 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.

## 비디오 스트리밍 트래픽 탐지

## 애플리케이션 필터 사용

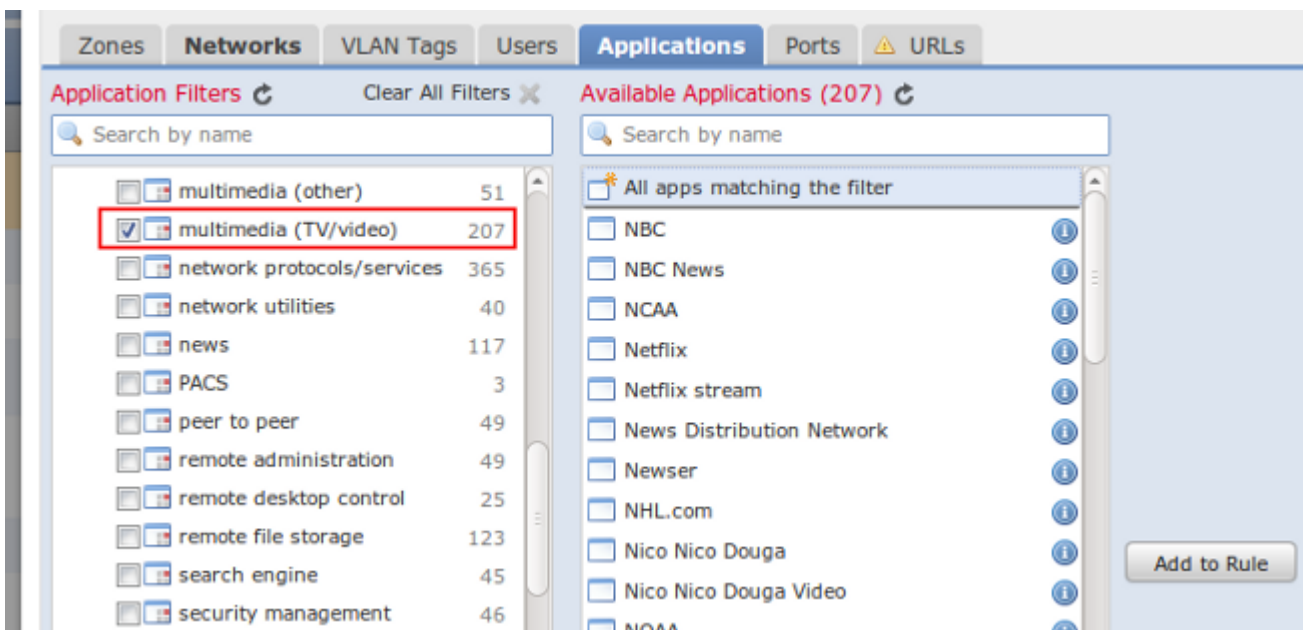
액세스 제어 정책 기능을 사용하면 애플리케이션 유형을 필터로 사용하여 트래픽을 차단, 신뢰 또는 검사할지 여부를 결정할 수 있습니다. 애플리케이션 필터를 사용하여 비디오 스트리밍 트래픽을 탐지하려면 다음 단계를 수행하십시오.

1단계: 환경에 적합한 영역, 네트워크 및 작업을 사용하여 액세스 제어 규칙을 생성합니다.

2단계: 애플리케이션 탭을 **선택합니다**. Application Filters(애플리케이션 필터) 섹션에서 여러 가지 가능한 선택을 찾을 수 있습니다.

3단계: 아래로 스크롤하여 **Application Filters**(애플리케이션 필터) 섹션으로 이동하면 **멀티미디어 (TV/비디오)**라는 필터와 200개 이상의 사용 가능한 애플리케이션이 있습니다. 한 번에 하나의 애플리케이션 또는 모든 애플리케이션을 선택할 수 있습니다. 이 필터의 모든 애플리케이션을 선택하려면 **All apps matching the filter**(필터와 일치하는 모든 앱)를 선택하고 **Add to Rule**(규칙에 추가) 버튼을 클릭합니다.

**팁:** 응용 프로그램을 이해하려면 각 응용 프로그램 오른쪽에 있는 정보 아이콘을 클릭합니다. 애플리케이션에 대해 설명하고 각 애플리케이션의 위험, 유형, 비즈니스 연관성 등을 제공합니다.



4단계: 또한 Application Filters(애플리케이션 필터) 섹션 아래에 있는 **Tags** 카테고리를 볼 수도 있습니다. **비디오 공유, 스트리밍 피드, 화상 회의, UDP 프로토콜, 멀티미디어(TV/비디오) 범주에 나열되지 않은 다른 응용 프로그램을 추가할 수 있는 웹캠 등 다양한 태그를 찾을 수 있습니다.**

5단계: 관리되는 디바이스에 액세스 제어 정책을 저장하고 다시 적용합니다.

**팁:** 새 애플리케이션 유형이 VDB(Vulnerability Data Base) 업데이트에 추가됩니다. VDB 버전을 최신 버전으로 유지하면 카테고리에 최근에 추가된 항목과 이전 애플리케이션을 탐지할 수 있습니다.

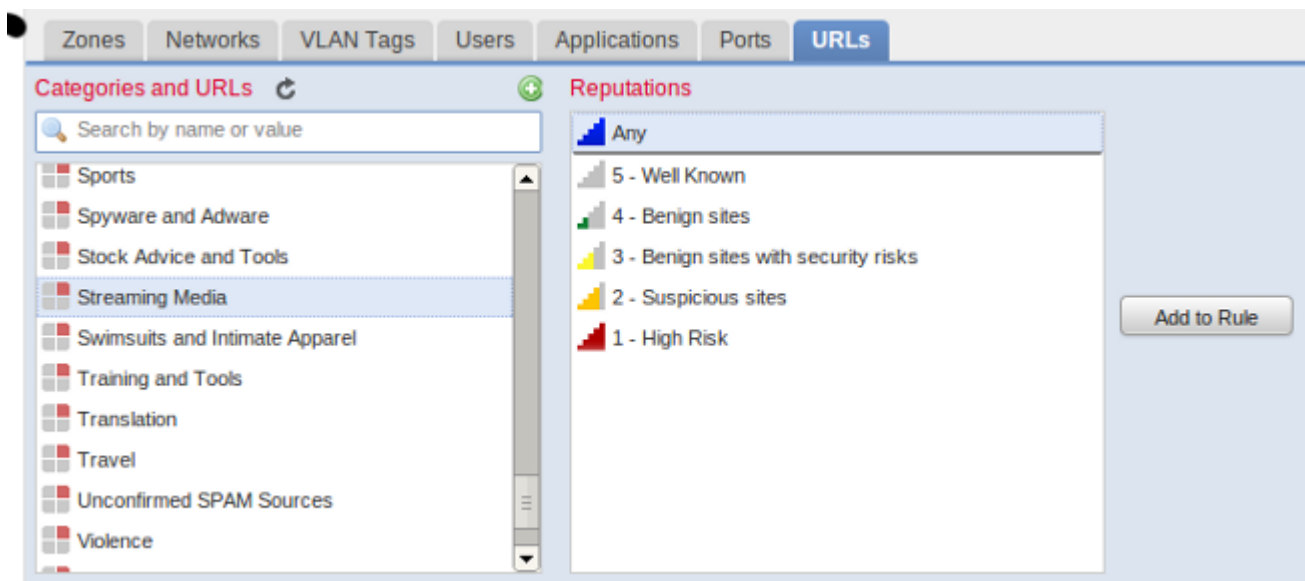
## URL 필터링 사용

URL 필터링을 사용하여 비디오 스트리밍 트래픽을 탐지할 수도 있습니다. 이렇게 하려면 액세스 제어 규칙을 추가할 때 다음 단계를 완료합니다.

1단계:URLs 탭을 선택합니다.

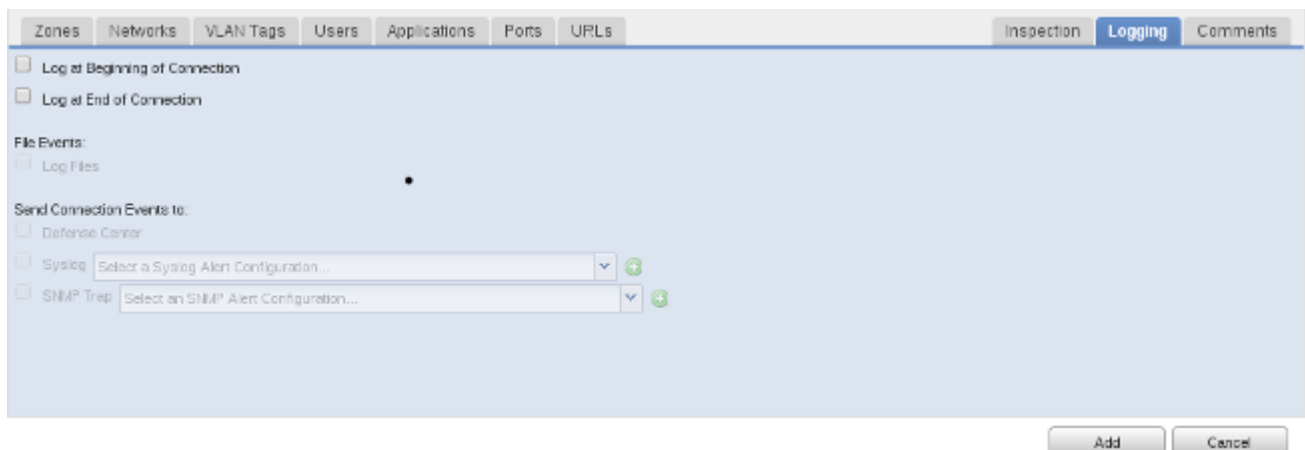
2단계:스트리밍 미디어 범주를 선택합니다.그런 다음 관심 있는 미디어의 평판 레벨을 Well Known(잘 알려진)에서 High Risk(고위험)로 선택할 수 있습니다. 이를 통해 정기적으로 업데이트해야 하는 URL 필터링 데이터베이스에 새 URL이 추가되면 새로운 비디오 스트리밍 트래픽을 탐지할 수 있습니다.

3단계:규칙을 추가한 후 액세스 제어 정책을 저장하고 관리되는 디바이스에 다시 적용합니다.



## 비디오 스트리밍 트래픽 로깅

애플리케이션 또는 URL 필터를 구성했으면 로깅을 활성화하여 이러한 연결을 추적할 수 있습니다. 이렇게 하려면 Logging 탭을 선택합니다.



비디오 스트리밍 트래픽을 차단하도록 Access Control 규칙을 구성하는 경우 **Log at Beginning of Connection**을 선택하여 연결을 로깅합니다.규칙에서 네트워크에서 사용 중인 비디오 스트리밍 유형 및 연결 기간에 대한 정보를 생성하려면 **Log at End of Connection**을 선택합니다.

**참고:**UDP 애플리케이션은 연결이 없으므로 소스와 대상 간의 추가 UDP 트래픽 없이 1시간이 지날 때까지 UDP 세션이 완료된 것으로 간주되지 않습니다.