Detection of Video Streaming Traffic Using a FireSIGHT System

Document ID: 118018

Contributed by Nazmul Rajib, Douglas Loss, Cisco TAC Engineer.
Jul 22, 2014

Contents

Introduction
Prerequisites
Requirements
Components Used
Detecting Video Streaming Traffic

Using Application Filters
Logging Video Streaming Traffic

Introduction

In order to detect the video traffic of your network, you can use the Access Control functionality and URL Filtering feature of a FireSIGHT System. This document describes how to configure a FireSIGHT System for this purpose.

Prerequisites

Requirements

The instructions on this document requires that a Control license and URL Filter license are installed on the FireSIGHT Management Center.

Components Used

The information in this document is based on these hardware and software versions:

- FireSIGHT Management Center
- Software Version 5.2 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Detecting Video Streaming Traffic

Using Application Filters

An Access Control policy functionality allows you to use application type as a filter to determine if traffic

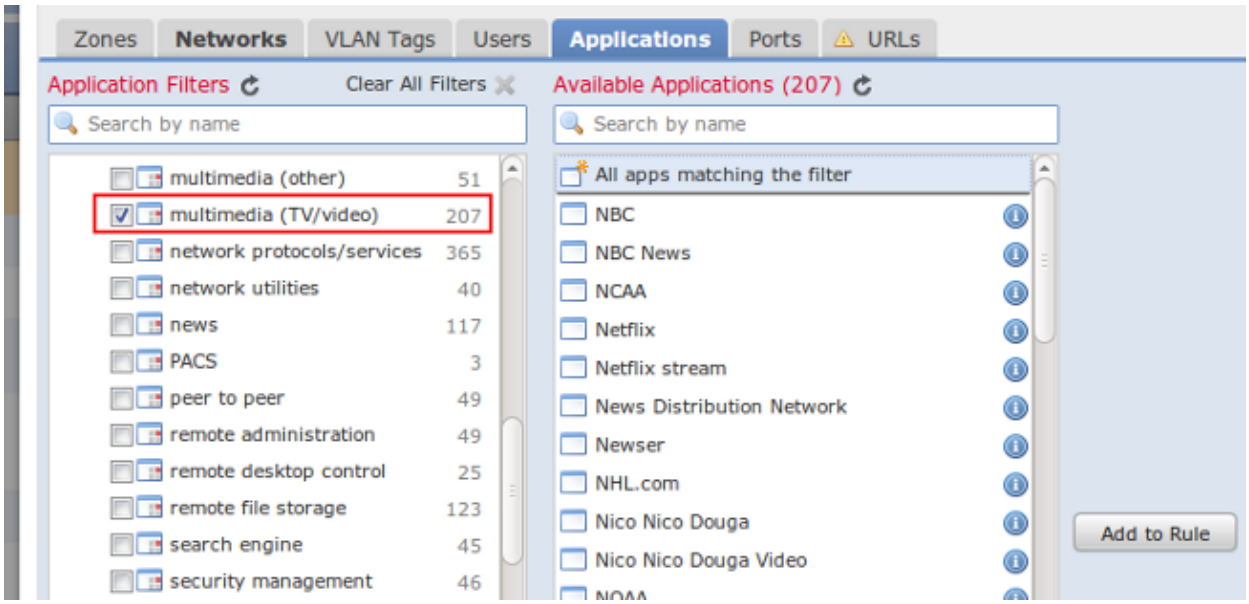
should be blocked, trusted, or inspected. In order to detect video streaming traffic using Application Filters, follow the steps below:

Step 1: Create an Access Control rule using the appropriate Zones, Networks, and Action for your environment.

Step 2: Select the ***Applications*** tab. You will find many possible selections in the ***Application Filters*** section.

Step 3: Scroll down to the ***Application Filters*** section, you will find a filter named ***multimedia (TV/video)***, with over 200 available applications. You can select one application at a time, or all of the applications. In order to select all the applications in this filter, select ***All apps matching the filter*** and click ***Add to Rule*** button.

Tip: In order to help you understand the applications, click on the *Info* icon which is right of each application. It describes the application and provides you with the risks, types, business relevancy, etc. of each application.



Step 4: You may also wish to view the ***Tags*** category which is under the ***Application Filters*** section. You will find various tags such as ***share video***, ***streaming feed***, ***video conferencing***, ***UDP protocol***, and ***webcam*** for any other applications you would like to add that weren't listed in the ***multimedia (TV/video)*** category.

Step 5: Save and reapply the Access Control policy to your managed devices.

Tip: New application types are added in Vulnerability Data Base (VDB) updates. Keeping your VDB version current allows you to detect the most recent additions to the categories as well as older applications.

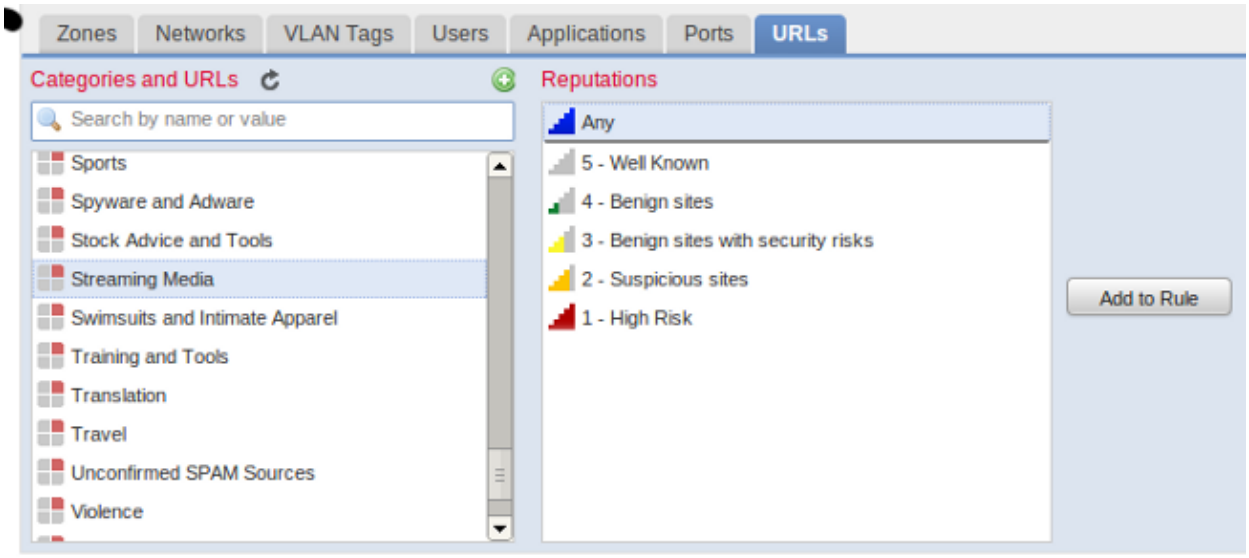
Using URL Filtering

You can also detect video streaming traffic by using URL filtering. To do that, complete the following steps when you are adding an Access Control rule:

Step 1: Select the ***URLs*** tab.

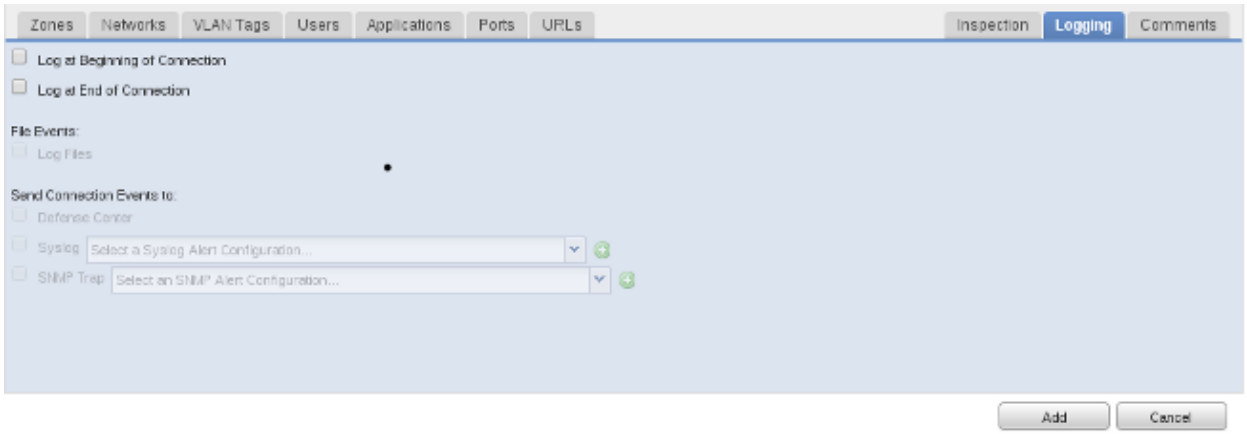
Step 2: Choose the ***Streaming Media*** category. You can then select the ***Reputation*** level of the media you're concerned with, from ***Well Known*** to ***High Risk***. This allows you to detect new video streaming traffic as new URLs are added to the URL Filtering database which you should update regularly.

Step 3: After adding the rules, save the Access Control policy and reapply it to your managed devices.



Logging Video Streaming Traffic

Once you have configured the Application or URL filters, you can enable logging to track these connections. To do that, select the ***Logging*** tab.



If you configure an Access Control rule to block video streaming traffic, select ***Log at Beginning of Connection*** to log the connections. If you want the rule to generate information on the type of video streaming in use on your network and the duration of the connections, select ***Log at End of Connection***.

Note: UDP applications are connection−less, so the UDP sessions aren't considered complete until one hour passes with no further UDP traffic between the source and destination.

Updated: Jul 22, 2014 Document ID: 118018