视频流流量的检测使用FireSIGHT系统

目录

简介

为了检测您的网络视频流量，您能使用FireSIGHT系统的访问控制功能和URL过滤功能。本文描述如何为此配置FireSIGHT系统。

先决条件

要求

关于本文的说明要求控制许可证和URL过滤许可证在FireSIGHT管理中心安装。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- FireSIGHT管理中心
- 软件版本5.2或以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

检测视频流流量

使用应用程序过滤器

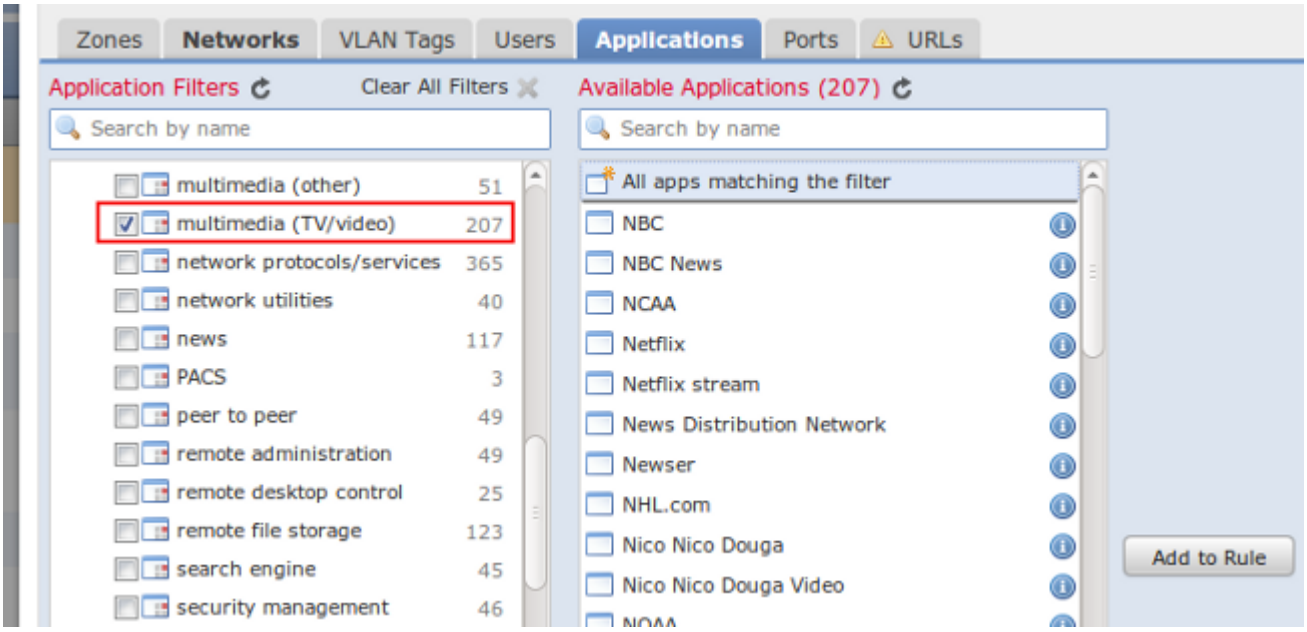
访问控制策略功能允许您使用应用类型作为过滤器确定流量应该是否阻塞，被信任或者被检查。使用应用程序过滤器，为了检测视频流流量，请遵从下面步骤：

步骤 1：使用适当的区域、网络和行为您的环境的，创建访问控制规则。

步骤 2：选择**Applications选项**。您将查找在**应用程序过滤器**部分的许多可能的选择。

步骤 3：移下来到**应用程序过滤器**部分，您将查找过滤器被命名**多媒体(TV/video)**，与200可用的应用程序。您能每次选择一应用程序或者所有应用程序。为了选择在此过滤器的所有应用程序，选择**匹配过滤器的所有apps**和单击**添加规定**按钮。

> **提示**：为了帮助是每应用程序权利的您了解应用程序，请点击*info图标*。它描述应用程序并且提供您每应用程序风险、类型、企业相关性等等。



步骤 4：您可以也希望查看在**应用程序过滤器**部分下的**标记**类别。您将查找多种标记例如**共享视频**，**放出源**、**视频会议**、**UDP协议**和**网络摄影**您会想要添加在**多媒体的**所有其他应用程序的**(TV/video)**类别未列出。

步骤 5：保存并且重新应用访问控制策略到您的受管理设备。

> **提示**：新应用类型在漏洞数据库(VDB)更新被添加。保持您的VDB版本当前允许您检测最最近的新增内容到类别以及更旧的应用程序。

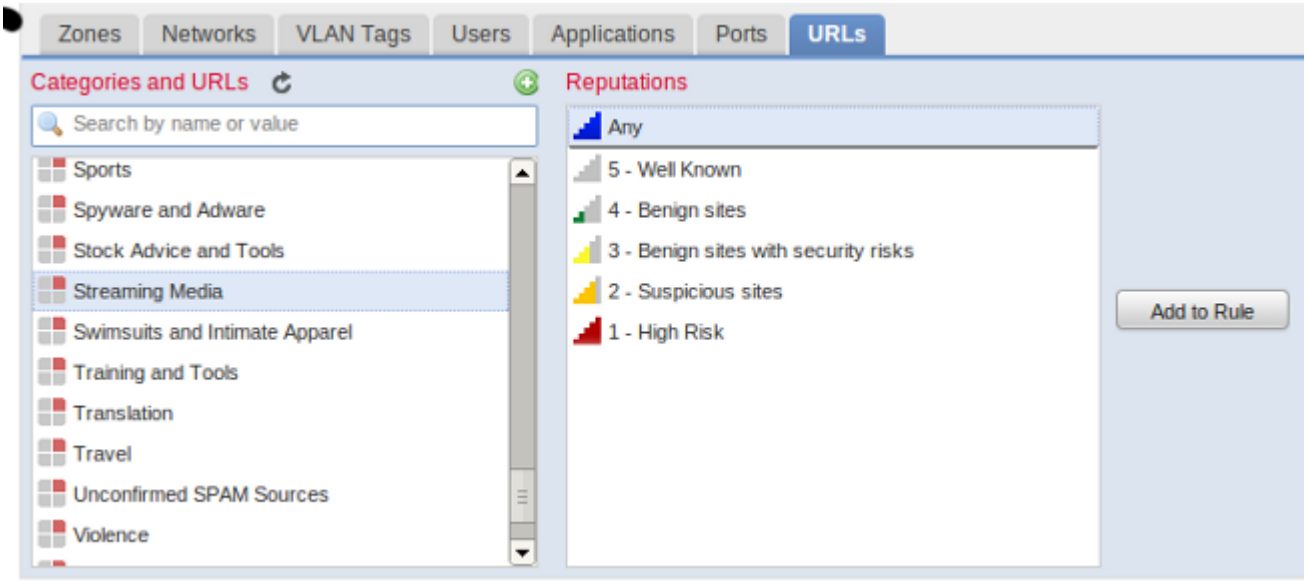
使用URL过滤

通过使用URL过滤，您能也检测视频流流量。 当您增加访问控制规则时，要执行那，请完成以下步骤：

步骤 1：选择**URL**选项卡。

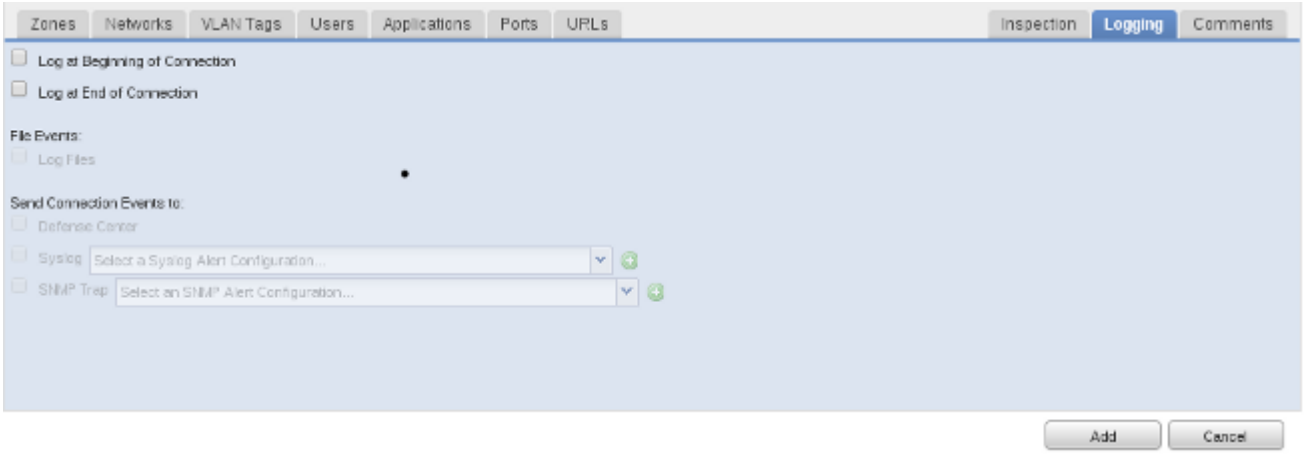
步骤 2：选择**流媒体**类别。您能然后选择**名誉**您关注的级媒体，从**著名的**到**高危险**。 这允许您检测新建的视频流流量和新的URL被添加到您应该定期更新的URL过滤数据库。

步骤 3：在增加规则以后，请保存访问控制策略并且重新应用它到您的受管理设备。



记录的视频流流量

一旦配置应用程序或URL过滤器，您能跟踪这些连接的启用日志。要执行那，请选择**Logging选项**。



如果配置访问控制规则阻塞视频流流量，请选择**日志在连接开始**记录连接。如果想要规则生成关于视频流种类的信息在使用中在您的网络和连接的持续时间，请选择**日志在连接结束时**。

> **Note**:UDP应用程序无连接，因此UDP会话没有被认为完整，直到一个小时通过没有进一步UDP流量在源和目的之间。