Обнаружение трафика потока видеосигналов Использование системы FireSIGHT

Содержание

Введение

Для обнаружения видеотрафика сети можно использовать функциональность Управления доступом и функцию Фильтрации URL-адресов Системы FireSIGHT. Этот документ описывает, как настроить Систему FireSIGHT для этой цели.

Предварительные условия

Требования

Инструкции по этому документу требуют, чтобы лицензия Контроля и лицензия Фильтра URL были установлены на Центре управления FireSIGHT.

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Центр управления FireSIGHT
- Версия программного обеспечения 5.2 или позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Обнаружение трафика потока видеосигналов

Использование фильтров приложения

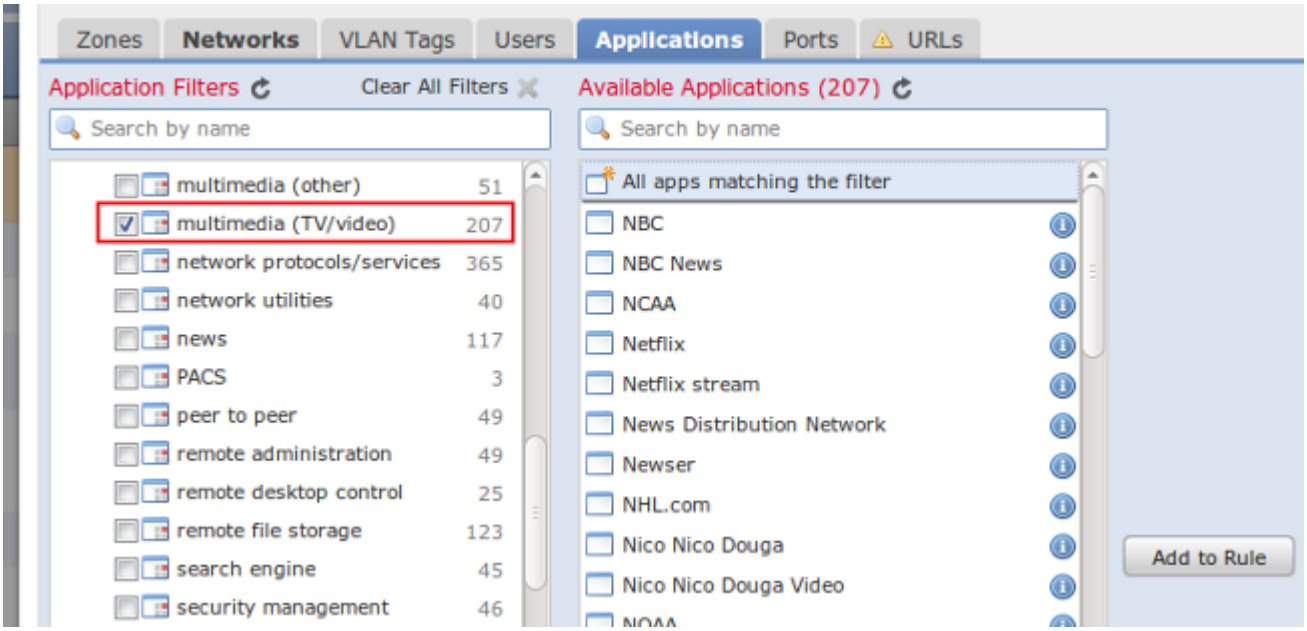
Функциональность Политики контроля доступа позволяет вам использовать тип приложения в качестве фильтра, чтобы определить, нужно ли трафик заблокировать, доверять или осмотреть. Для обнаружения трафика потока видеосигналов с помощью Фильтров Приложения выполните действия ниже:

Шаг 1: Создайте правило Управления доступом с помощью соответствующих Зон, Сетей и Действия для среды.

Шаг 2: Выберите вкладку **Applications**. Вы найдете много возможных выборов в разделе **Фильтров Приложения**.

Шаг 3: Прокрутите вниз к разделу **Фильтров Приложения**, вы найдете фильтр названным **мультимедиа (TV/ВИДЕО)** с более чем 200 доступными приложениями. Можно выбрать одно приложение за один раз или все приложения. Для выбора всех приложений в этом фильтре выберите **All apps matching фильтр** и **нажмите Add к** кнопке **Rule**.

> **Совет:** Чтобы помочь вам понимать приложения, щелкните *по Информационному* значку, который является правильным из каждого приложения. Это описывает приложение и предоставляет вам риски, типы, бизнес-уместность, и т.д. каждого приложения.



Шаг 4. : Можно также хотеть просмотреть категорию **Меток**, которая находится под разделом **Фильтров Приложения**. Вы найдете различные метки, такие как **общее видео**, **передавая потоком канал**, **видеоконференцсвязь**, **протокол UDP** и **веб-камеру** для любых других приложений, требуется добавить, что не были перечислены в **мультимедиа (TV/ВИДЕО)** категория.

Шаг 5. : Сохраните и повторно примените Политику контроля доступа к своим управляемым

устройствам.

> **Совет:** Типы нового приложения добавлены в обновлениях Базы данных уязвимости (VDB). Держание в курсе вашей версии VDB позволяет вам обнаруживать новые добавления к категориям, а также более старым приложениям.

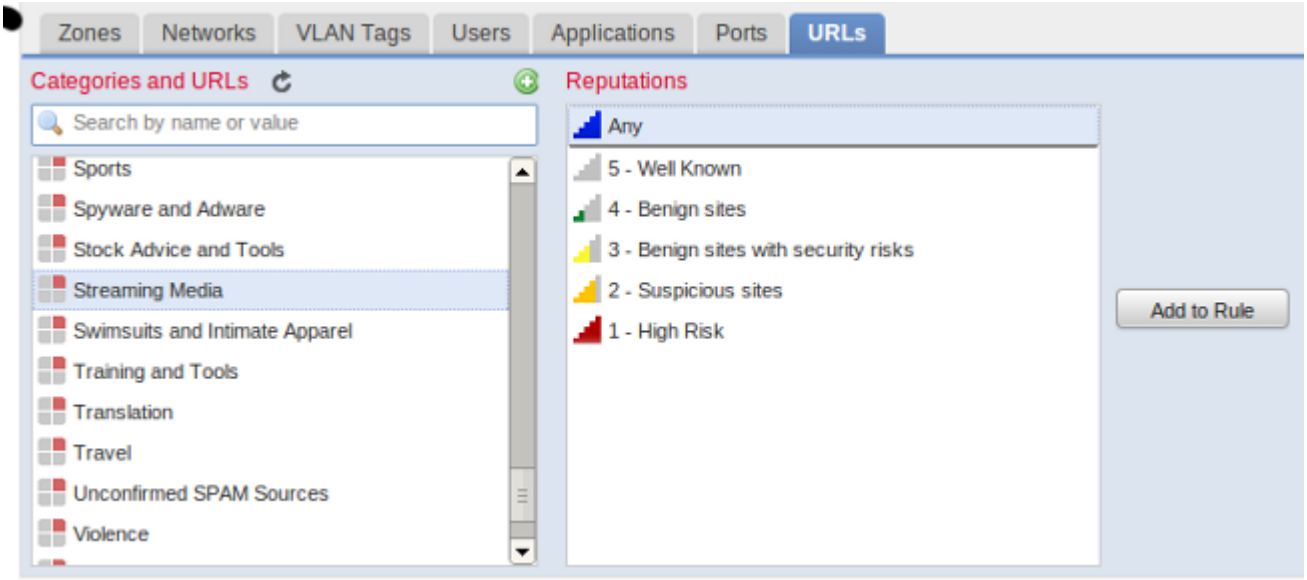
Использование фильтрации URL-адресов

Можно также обнаружить трафик потока видеосигналов при помощи фильтрации URL-адресов. Чтобы сделать это, завершите следующие шаги, когда вы добавите правило Управления доступом:

Шаг 1: Выберите вкладку **URL**.

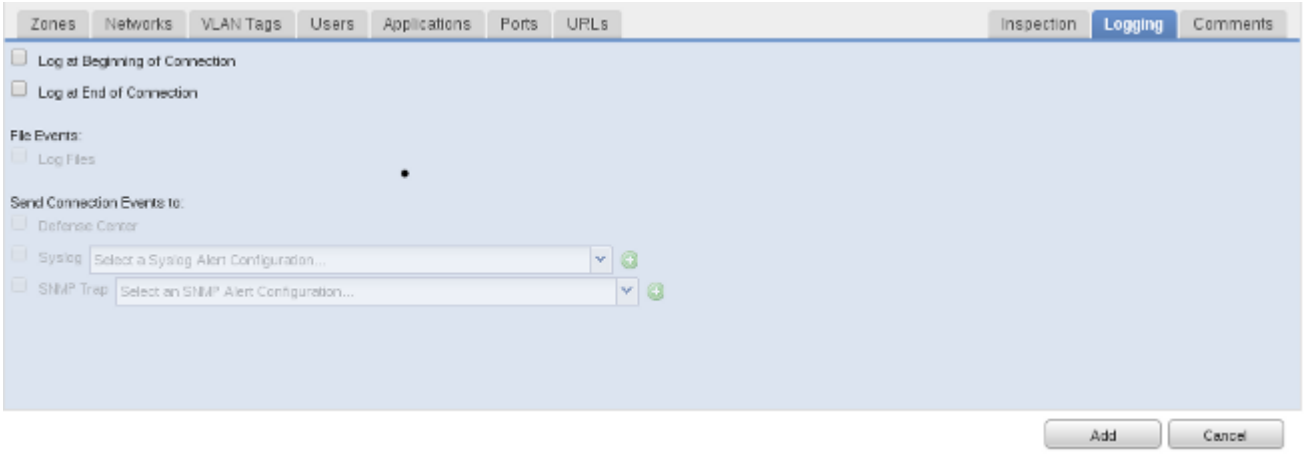
Шаг 2: Выберите **Потоковую медиа-данные** категорию. Можно тогда выбрать уровень **Репутации** сред, которые вы обеспокоены в от **Известного** до **Высокого риска**. Это позволяет вам обнаруживать новый трафик потока видеосигналов, поскольку новые URL добавлены к базе данных Фильтрации URL-адресов, которую необходимо регулярно обновлять.

Шаг 3: После добавления правил сохраните Политику контроля доступа и повторно примените его к своим управляемым устройствам.



Трафик потока видеосигналов Регистрации

Как только вы настроили Приложение или фильтры URL, вы можете enable logging для отслеживания этих соединений. Чтобы сделать это, выберите вкладку **Logging**.



При настройке правила Управления доступом заблокировать трафик потока видеосигналов выберите **Log at Beginning of Connection** для регистрации соединений. Если вы хотите правило генерировать информацию о типе потока видеосигналов в использовании в вашей сети и продолжительности соединений, выберите **Log at End of Connection**.

> **Примечание:** Приложения UDP без установления соединения, таким образом, сеансы UDP не считают завершенными до проходов часа без дальнейшего трафика UDP между источником и назначением.