

DetECCIÓN DE TRÁFICO DEL FLUJO DE DATOS DE VIDEO USANDO UN SISTEMA DE FIRESIGHT

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Detección del tráfico del flujo de datos de video](#)

[Usando los filtros de la aplicación](#)

[Tráfico de registración del flujo de datos de video](#)

Introducción

Para detectar el tráfico de video de su red, usted puede utilizar las funciones del control de acceso y la característica del Filtrado de URL de un sistema de FireSIGHT. Este documento describe cómo configurar un para este propósito del sistema de FireSIGHT.

Prerequisites

Requisitos

Las instrucciones en este documento requieren que una licencia del control y la licencia del filtro URL estén instaladas en el centro de administración de FireSIGHT.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Centro de administración de FireSIGHT
- Versión de software 5.2 o más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Detección del tráfico del flujo de datos de video

Usando los filtros de la aplicación

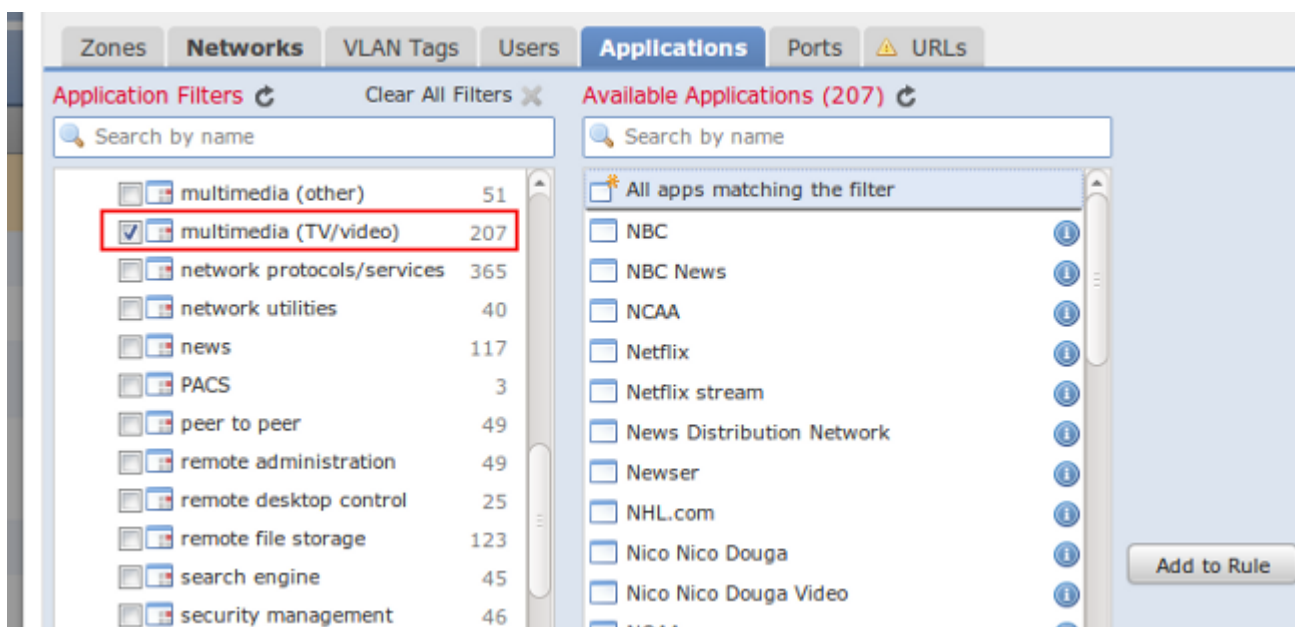
Las funciones de la directiva del control de acceso permiten que usted utilice Application type (Tipo de aplicación) como filtro para determinar si se bloquea, se confía en, o se examina el tráfico. Para detectar el tráfico del flujo de datos de video usando los filtros de la aplicación, siga los pasos abajo:

Paso 1: Cree una regla del control de acceso usando las zonas, las redes, y la acción apropiadas para su entorno.

Paso 2: Seleccione la lengüeta de las **aplicaciones**. Usted encontrará muchas selecciones posibles en la sección de los **filtros de la aplicación**.

Paso 3: Navegue hacia abajo a los **filtros** sección de la **aplicación**, usted encontrará un filtro nombrado los **multimedia (TV/video)**, con sobre 200 aplicaciones disponibles. Usted puede seleccionar un en un momento de la aplicación, o todas las aplicaciones. Para seleccionar todas las aplicaciones en este filtro, seleccionar **todos los apps que corresponden con el filtro** y el tecleo **agregue para gobernar el botón**.

Tip: Para ayudarle a entender las aplicaciones, haga clic en el *icono de información* que correcto de cada aplicación. Describe la aplicación y provee de usted los riesgos, los tipos, la importancia del negocio, el etc. de cada aplicación.



Paso 4: Usted puede también desear ver la categoría de las **etiquetas** que está bajo sección de los **filtros de la aplicación**. Usted encontrará las diversas etiquetas tales como **video de la parte**, **fluyendo la alimentación**, la **videoconferencia**, el **protocolo UDP**, y el **webcam** para cualquier otra aplicación que usted quisiera agregar que no fue enumerado en la categoría de las **multimedias (TV/video)**.

Paso 5: Salve y reaplique la directiva del control de acceso a sus dispositivos administrados.

Tip: Agregan a los tipos de nueva aplicación en las actualizaciones de la base de datos de la vulnerabilidad (VDB). La custodia de su corriente de la versión VDB permite que usted detecte la mayoría de las adiciones recientes a las categorías así como a las más viejas aplicaciones.

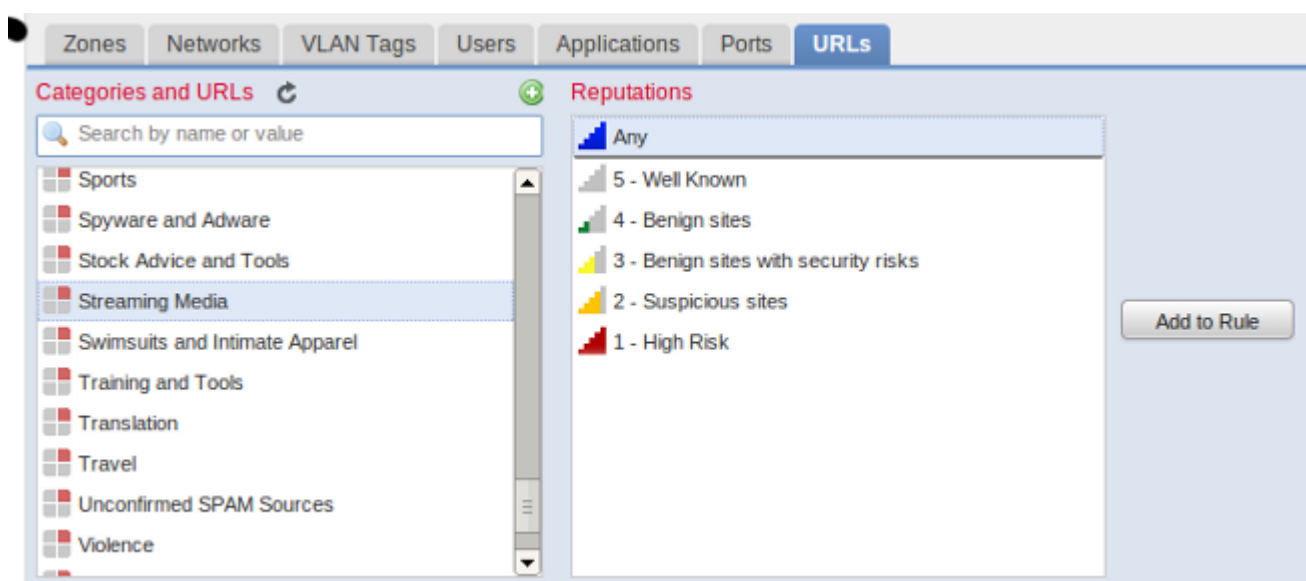
Usando el Filtrado de URL

Usted puede también detectar el tráfico del flujo de datos de video usando el Filtrado de URL. Para hacer eso, complete los pasos siguientes cuando usted está agregando una regla del control de acceso:

Paso 1: Seleccione la lengüeta **URL**.

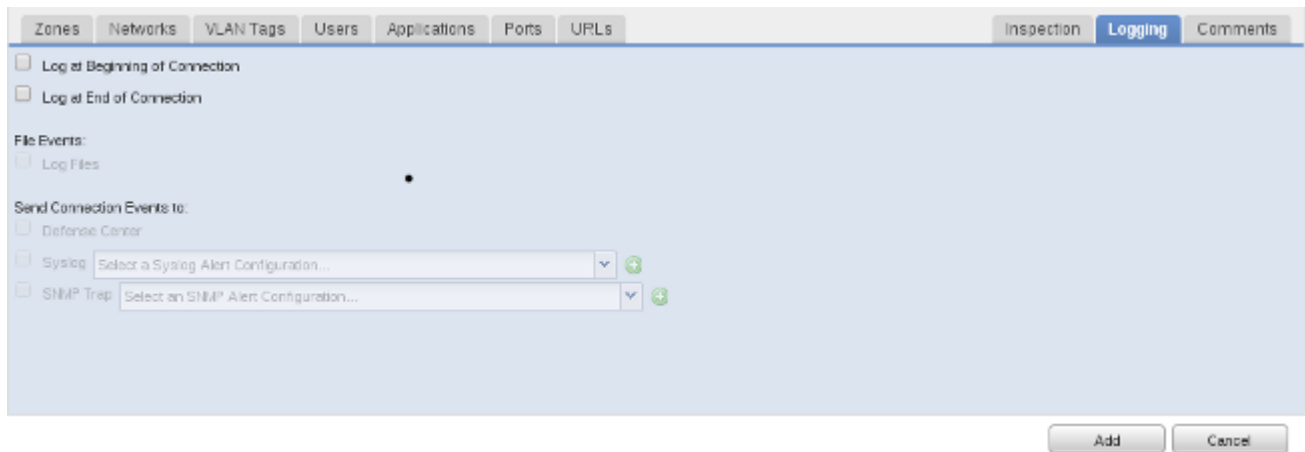
Paso 2: Elija la categoría de los **medios de flujo continuo**. Usted puede entonces seleccionar la **reputación** llana de los media que usted se refiere a, de **bien conocido al alto riesgo**. Esto permite que usted detecte el nuevo tráfico del flujo de datos de video mientras que los nuevos URL se agregan a la base de datos del Filtrado de URL que usted debe poner al día regularmente.

Paso 3: Después de agregar las reglas, salve la directiva del control de acceso y reapliquela a sus dispositivos administrados.



Tráfico de registración del flujo de datos de video

Una vez que usted ha configurado la aplicación o los filtros URL, usted puede permitir al registro para seguir estas conexiones. Para hacer eso, seleccione la lengüeta del **registro**.



Si usted configura una regla del control de acceso para bloquear el tráfico del flujo de datos de video, seleccione el **registro al principio de la conexión** para registrar las conexiones. Si usted quisiera que la regla generara la información en el tipo de flujo de datos de video funcionando en su red y la duración de las conexiones, seleccione el **registro en el extremo de la conexión**.

Note: Las aplicaciones UDP están sin conexión, así que no consideran a las Sesiones UDP completas hasta que una hora pase sin el tráfico adicional UDP entre la fuente y el destino.