Filtrado de URL en un ejemplo de la configuración del sistema de FireSIGHT

Contenido

Introducción

Este documento describe los pasos para configurar el Filtrado de URL en el sistema de FireSIGHT. La característica del Filtrado de URL en el centro de administración de FireSIGHT permite que usted escriba una condición en una regla del control de acceso para determinar el tráfico que atraviesa una red basada en las peticiones NON-cifradas URL por los host monitoreados.

Prerequisites

Requisitos

Este documento tiene algunos algunos requisitos específicos para la licencia del Filtrado de URL y el puerto.

Requisito de la licencia del Filtrado de URL

Un centro de administración de FireSIGHT requiere una licencia del Filtrado de URL para entrar en contacto la nube periódicamente para una actualización en la información del URL. Usted puede agregar la categoría y las condiciones reputación-basadas URL a las reglas del control de acceso sin un Filtrado de URL autorizan; no obstante usted no puede aplicar la directiva del control de acceso hasta que usted primero agregue una licencia del Filtrado de URL al centro de administración de FireSIGHT, después habilitelo en los dispositivos apuntados por la directiva.

Si expira una licencia del Filtrado de URL, el control de acceso gobierna con la categoría y las condiciones reputación-basadas URL paran el filtrar de los URL, y el centro de administración de

FireSIGHT entra en contacto no más el servicio de la nube. Sin una licencia del Filtrado de URL, los URL individuales o los grupos de URL se pueden fijar para permitir o para bloquear, pero los datos de la categoría o de la reputación URL no se pueden utilizar para filtrar el tráfico de la red.

Requisito del puerto

Un sistema de FireSIGHT utiliza los puertos 443/HTTPS y 80/HTTP para comunicar con el servicio de la nube. El puerto 443/HTTPS se debe abrir bidireccional, y el acceso entrante para virar 80/HTTP hacia el lado de babor se debe permitir en el centro de administración de FireSIGHT.

Componentes Utilizados

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

- Dispositivos de FirePOWER: 7000 Series, 8000 Series
- Dispositivo virtual del sistema de prevención de intrusiones de la última generación (NGIPS)
- Dispositivo de seguridad adaptante (ASA) FirePOWER
- Versión de software 5.2 de Sourcefire 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.

Configurar

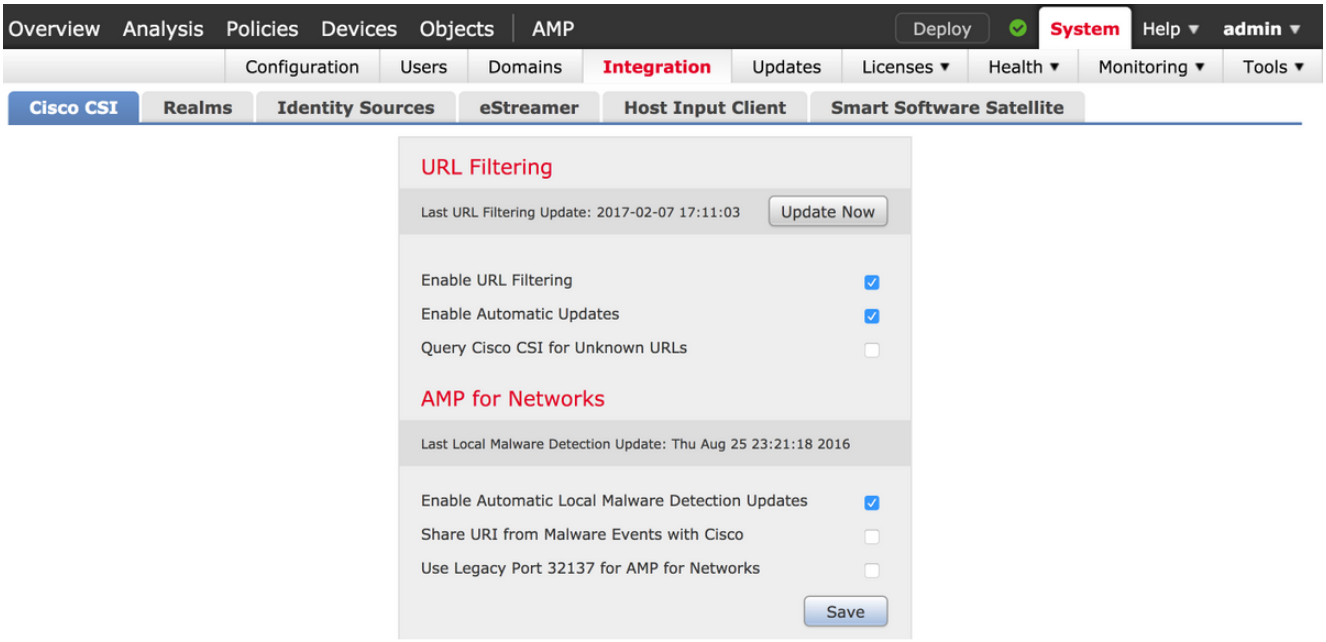
Filtrado de URL del permiso en el centro de administración de FireSIGHT

Para habilitar el Filtrado de URL, complete estos pasos:

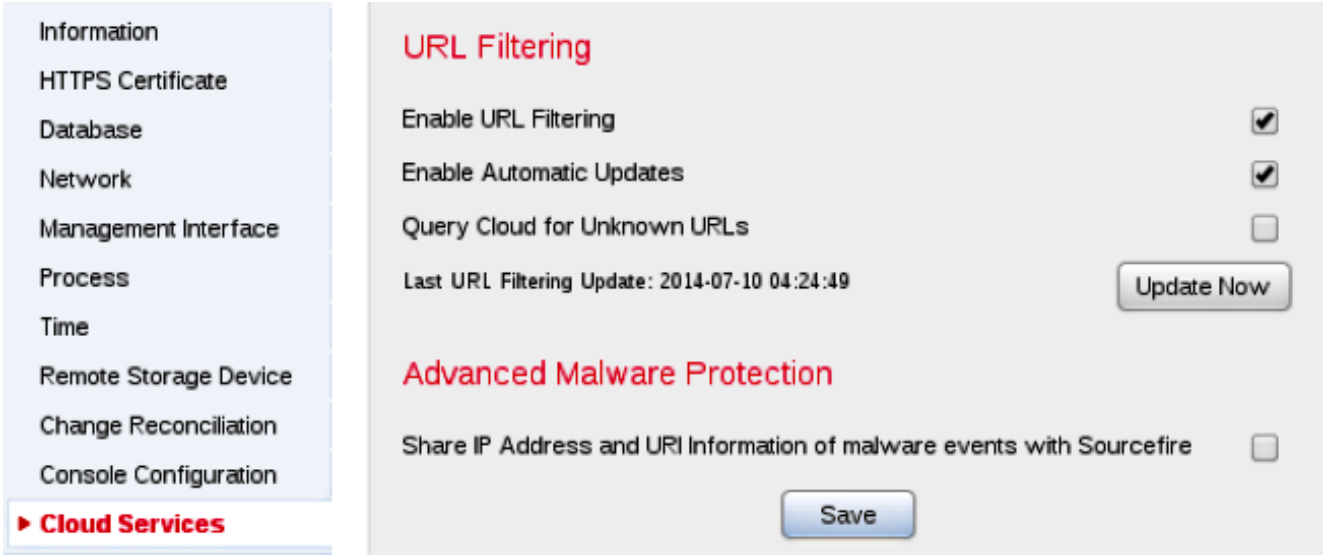
1. Registro en la interfaz del Web User del centro de administración de FireSIGHT.

2. La navegación es diferente basada en la versión de software que usted funciona con:

   En la versión 6.1.x, elija el **sistema > la integración > Cisco CSI**.



En la versión 5.x, elija el **sistema > el Local > la configuración**. Elija los **servicios de la nube**.



3. Marque la casilla de verificación del **Filtrado de URL del permiso** para habilitar el Filtrado de URL.
4. Opcionalmente, marque la casilla de verificación **automática de las actualizaciones del permiso** para habilitar las actualizaciones automáticas. Esta opción permite que el sistema entre en contacto el servicio de la nube en una base normal para obtener las actualizaciones a los datos URL en los conjuntos de los datos locales del dispositivo.

   Note: Aunque el servicio de la nube ponga al día típicamente sus datos una vez por el día, si usted habilita automático lo pone al día fuerza el centro de administración de FireSIGHT a marcar cada 30 minutos para aseegurarse que la información es siempre actual. Aunque las actualizaciones diarias tiendan a ser pequeñas, si ha sido más de cinco días desde la actualización más reciente, los nuevos datos del Filtrado de URL pudieron tomar hasta 20 minutos para descargar. Una vez que se han descargado las actualizaciones, puede ser que tome hasta 30 minutos para realizar la actualización sí mismo.

5. Opcionalmente, marque la **nube de la interrogación para los URL desconocidos** para la casilla de verificación desconocida URL para preguntar el servicio de la nube para los URL

desconocidos. Esta opción permite que el sistema pregunte la nube de Sourcefire cuando alguien en su red monitoreada intenta hojear a un URL que no esté en el conjunto de los datos locales. Si la nube no conoce la categoría o la reputación de un URL, o si el centro de administración de FireSIGHT no puede entrar en contacto la nube, el URL no hace juego las reglas del control de acceso con la categoría o las condiciones reputación-basadas URL.

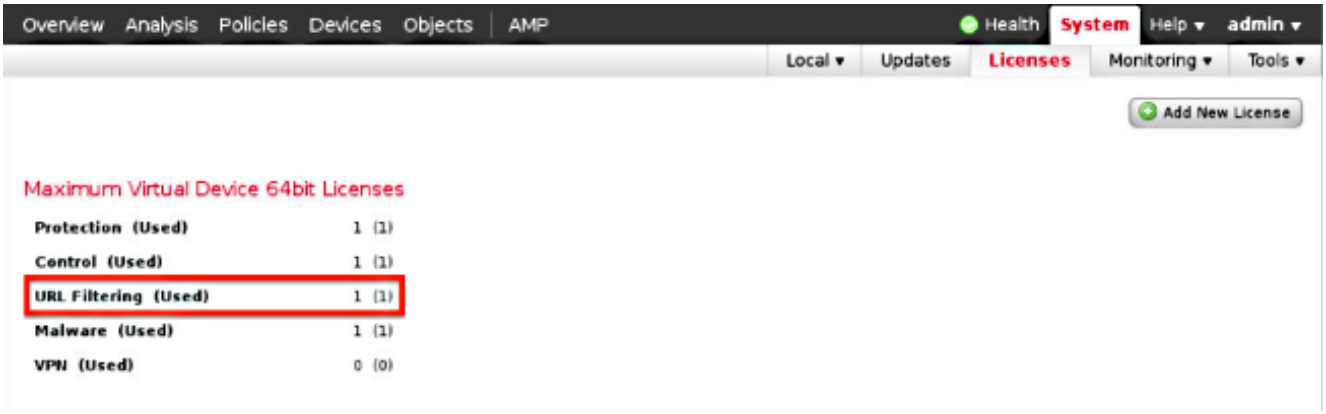
Note: Usted no puede asignar las categorías o las reputaciones a los URL manualmente. Inhabilite esta opción si usted no quisiera que sus URL uncategorized fueran catalogados por la nube de Sourcefire, por ejemplo, por las razones de la aislamiento.

6. Click **Save**. Se guardan las configuraciones del Filtrado de URL.

Note: De acuerdo con la longitud del tiempo puesto que el Filtrado de URL era último habilitado, o si éste está la primera vez usted ha habilitado el Filtrado de URL, un centro de administración de FireSIGHT extrae los datos del Filtrado de URL del servicio de la nube.

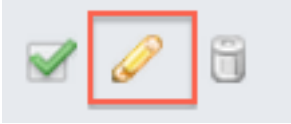
Aplique la licencia del Filtrado de URL en un dispositivo administrado

1. Marque si la licencia del Filtrado de URL está instalada en el centro de administración de FireSIGHT. Vaya a la página del **sistema > de las licencias** para encontrar una lista de licencias.

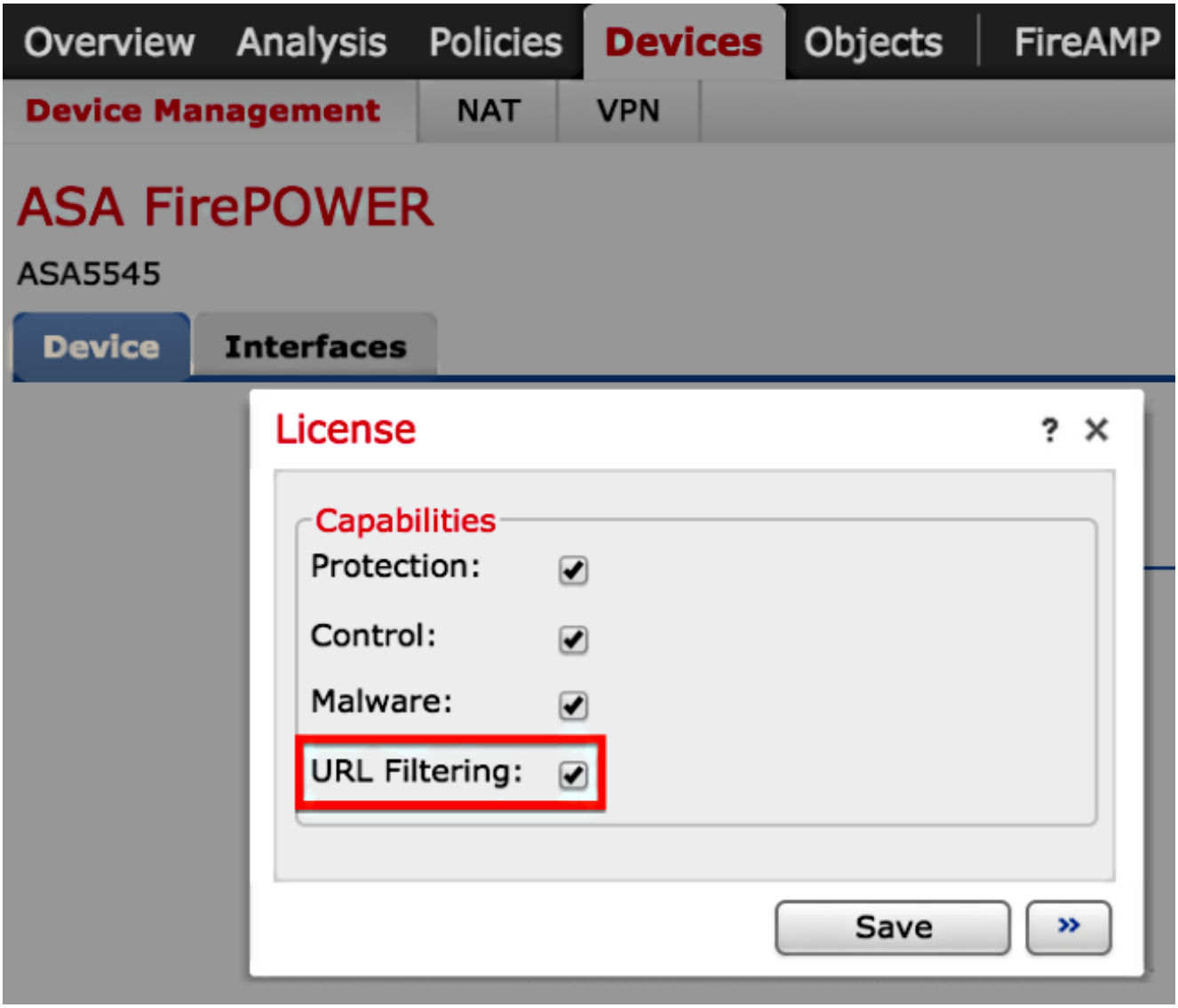


2. Vaya a la página de los **dispositivos > de la Administración de dispositivos**, y verifique si la licencia del Filtrado de URL se aplica en el dispositivo que monitorea el tráfico.

3. Si la licencia del Filtrado de URL no se aplica en un dispositivo, haga clic el icono del **lápiz** para editar las configuraciones. El icono está situado al lado del Nombre del dispositivo.



4. Usted puede habilitar la licencia del Filtrado de URL en un dispositivo de la lengueta de los **dispositivos**.



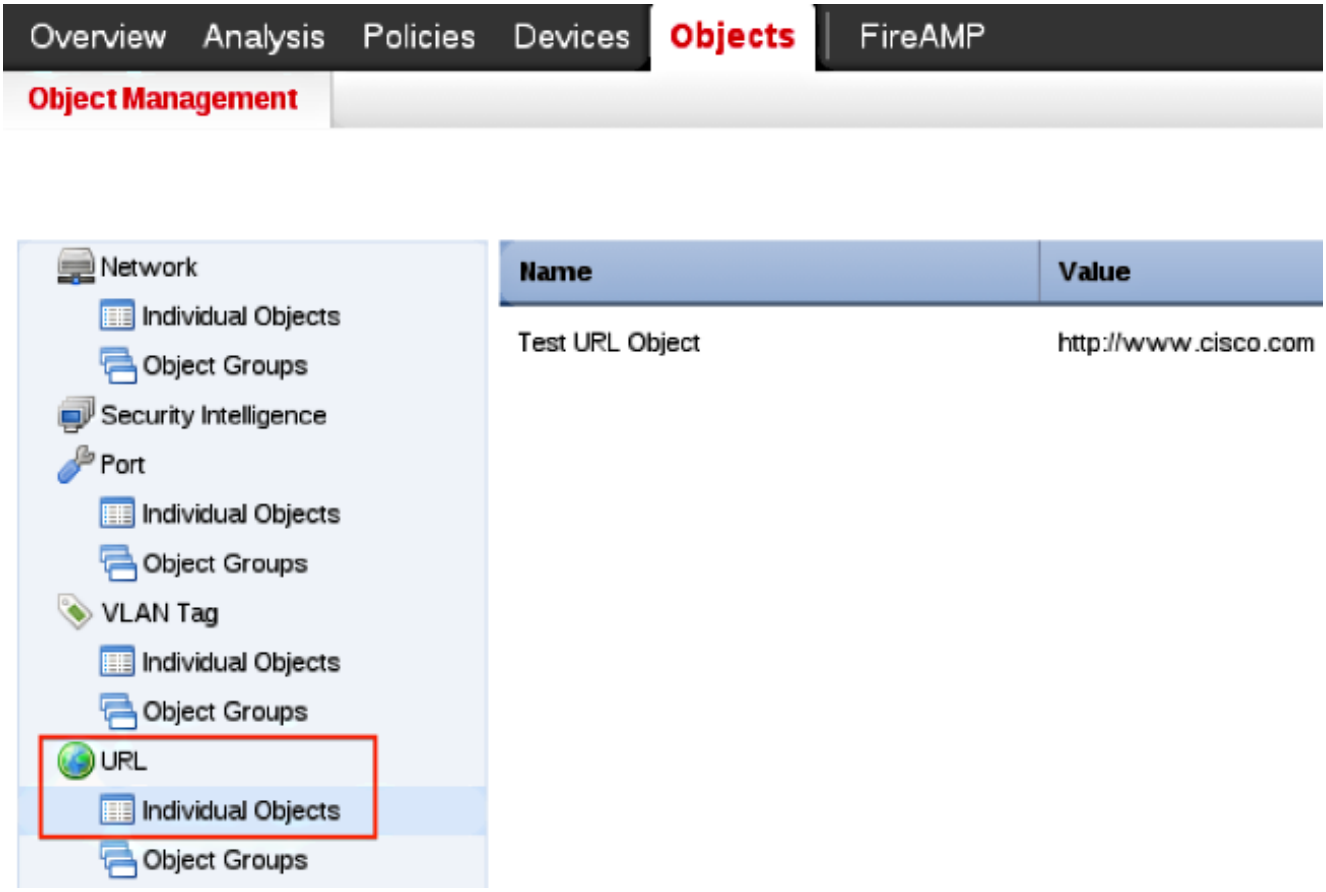
5. Después de que usted habilite una licencia y salve sus cambios, usted también debe hacer clic **aplica los cambios** para aplicar la licencia en su dispositivo administrado.

Exclusión de un sitio específico de la categoría bloqueada URL

El centro de administración de FireSIGHT no permite que usted tenga un grado local de los URL que reemplazan los grados proporcionados Sourcefire predeterminados de la categoría. Para lograr esta tarea, usted debe utilizar una directiva del control de acceso. Estas instrucciones describen cómo utilizar un objeto URL en una regla del control de acceso para excluir un sitio específico de una categoría del bloque.

1. Vaya a los **objetos > a la** página de la **Administración del objeto**.

2. **Elija los objetos individuales** para el URL, y haga clic el botón del **agregar URL**. La ventana de los **objetos URL** aparece.

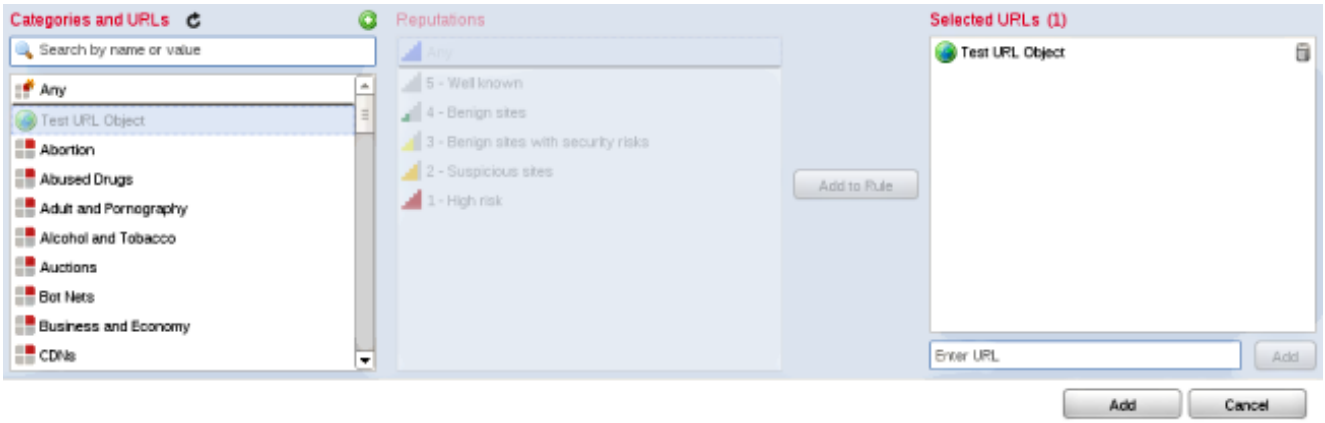


3. Después de que usted salve los cambios, elija las **directivas > el control de acceso** y haga clic el icono del **lápiz** para editar la directiva del control de acceso.

4. El tecleo **agrega la regla**.

5. Agregue su objeto URL a la regla con la acción de la **permit** y póngalo sobre la regla de la

categoría URL, para evaluar su acción de la regla primero.



6. Después de que usted agregue la regla, haga clic la **salvaguardia y apliqúese**. Guarda los nuevos cambios y aplica la directiva del control de acceso a los dispositivos manejados.

Verificación

Para la información Verify o del Troubleshooting, refiera a los **problemas del Troubleshooting con el Filtrado de URL en el** artículo del **sistema de FireSIGHT** conectado en la sección de información relacionada.

Troubleshooting

Para la información Verify o del Troubleshooting, refiera a los **problemas del Troubleshooting con el Filtrado de URL en el** artículo del **sistema de FireSIGHT** conectado en la sección de información relacionada.

Información Relacionada

- Problemas del Troubleshooting con el Filtrado de URL en el sistema de FireSIGHT
- Soporte Técnico y Documentación - Cisco Systems