

Ejemplo de Configuración de Filtrado de URL en un Sistema FireSIGHT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Requisito de licencia de filtrado de URL](#)

[Requisito de puerto](#)

[Componentes Utilizados](#)

[Configurar](#)

[Habilitar el filtrado de URL en FireSIGHT Management Center](#)

[Aplicación de la licencia de filtrado de URL en un dispositivo administrado](#)

[Exclusión de un sitio específico de una categoría de URL bloqueada](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos para configurar el filtrado de URL en el sistema FireSIGHT. La función de filtrado de URL de FireSIGHT Management Center permite escribir una condición en una regla de control de acceso para determinar el tráfico que atraviesa una red en función de las solicitudes de URL no cifradas de los hosts supervisados.

Prerequisites

Requirements

Este documento contiene algunos requisitos específicos para la licencia de filtrado de URL y el puerto.

Requisito de licencia de filtrado de URL

FireSIGHT Management Center requiere una licencia de filtrado de URL para ponerse en contacto con la nube periódicamente para obtener información actualizada sobre URL. Puede agregar condiciones de URL basadas en la categoría y la reputación a las reglas de control de acceso sin una licencia de filtrado de URL; sin embargo, no podrá aplicar la política de control de acceso hasta que no agregue primero una licencia de filtrado de URL a FireSIGHT Management Center y, a continuación, la habilite en los dispositivos de destino de la política.

Si vence una licencia de filtrado de URL, las reglas de control de acceso con condiciones de URL basadas en categoría y reputación dejan de filtrar URL y FireSIGHT Management Center deja de ponerse en contacto con el servicio en la nube. Sin una licencia de filtrado de URL, se pueden

establecer URL individuales o grupos de URL para permitir o bloquear, pero la categoría de URL o los datos de reputación no se pueden utilizar para filtrar el tráfico de red.

Requisito de puerto

Un sistema FireSIGHT utiliza los puertos 443/HTTPS y 80/HTTP para comunicarse con el servicio en la nube. El puerto 443/HTTPS debe abrirse bidireccionalmente y se debe permitir el acceso entrante al puerto 80/HTTP en FireSIGHT Management Center.

Componentes Utilizados

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

- Appliances FirePOWER: Serie 7000, Serie 8000
- Dispositivo virtual NGIPS (sistema de prevención de intrusiones de última generación)
- Appliance de seguridad adaptable (ASA) FirePOWER
- Software Sourcefire versión 5.2 o posterior

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.

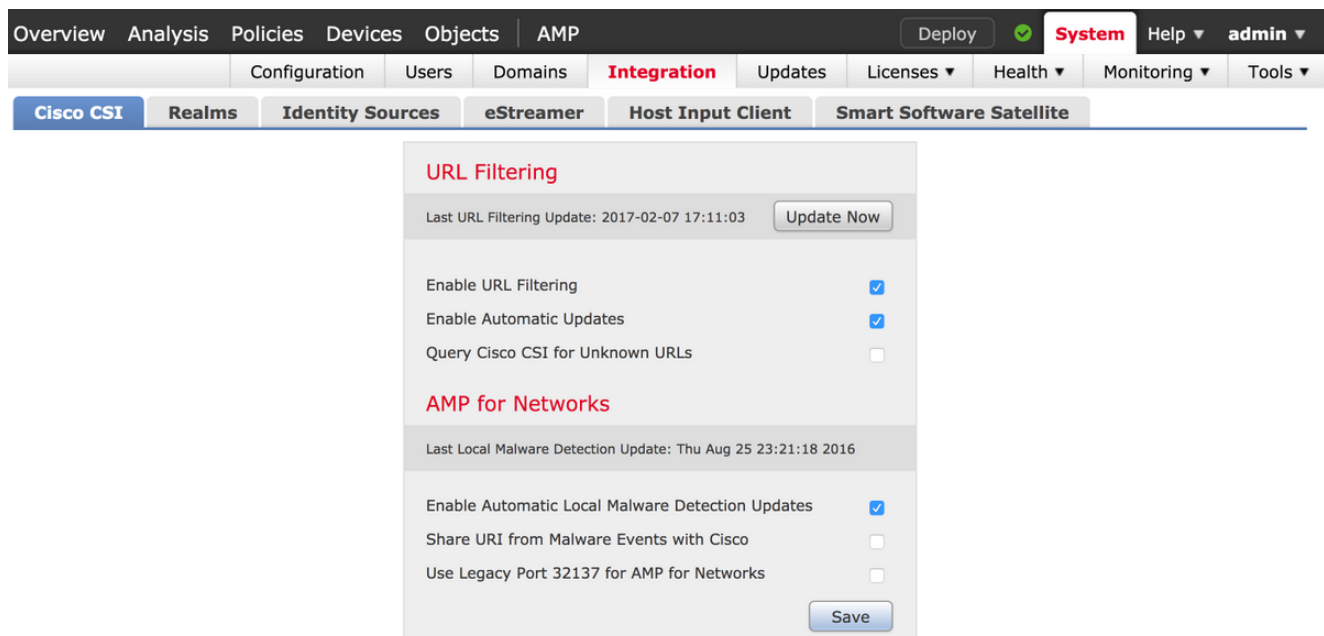
Configurar

Habilitar el filtrado de URL en FireSIGHT Management Center

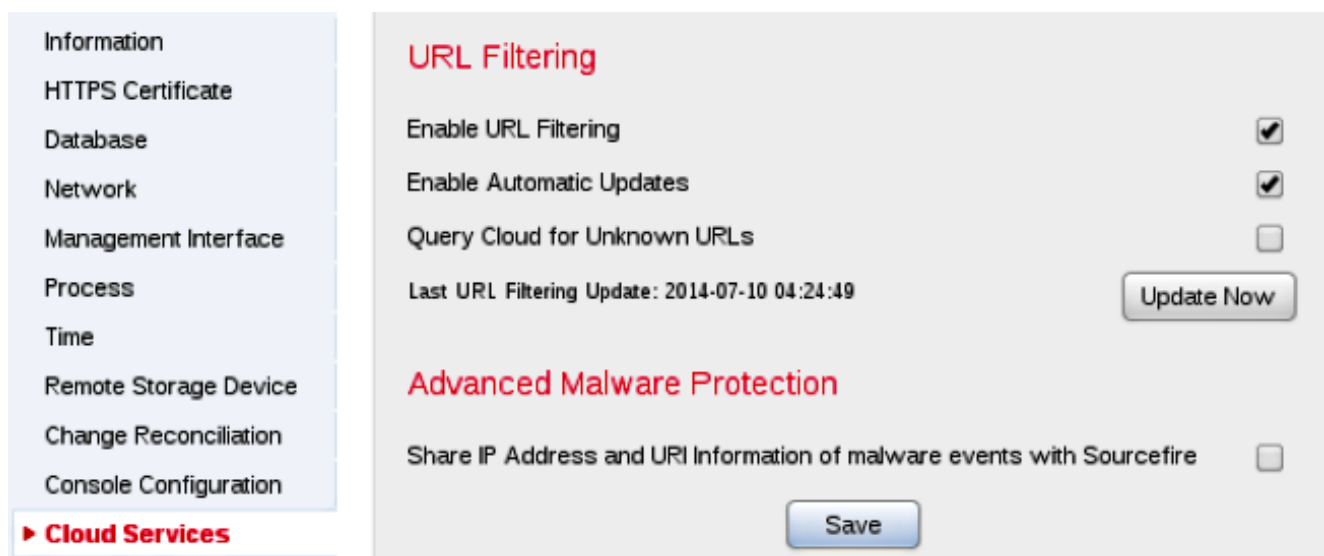
Para habilitar el filtrado de URL, siga estos pasos:

1. Inicie sesión en la interfaz de usuario web de FireSIGHT Management Center.
2. La navegación es diferente según la versión de software que ejecute:

En la versión 6.1.x, elija **System > Integration > Cisco CSI**.



En la versión 5.x, elija **System > Local > Configuration**. Elija **Cloud Services**.



3. Marque la casilla de verificación **Enable URL Filtering** para habilitar el filtrado de URL.
4. Opcionalmente, marque la casilla de verificación **Enable Automatic Updates** para habilitar las actualizaciones automáticas. Esta opción permite al sistema ponerse en contacto con el servicio en la nube de forma regular para obtener actualizaciones de los datos de URL de los conjuntos de datos locales del dispositivo.

Nota: Aunque el servicio en la nube suele actualizar sus datos una vez al día, si activa las actualizaciones automáticas, obliga a FireSIGHT Management Center a comprobar cada 30 minutos para asegurarse de que la información siempre está actualizada. Aunque las actualizaciones diarias suelen ser pequeñas, si han transcurrido más de cinco días desde la última actualización, la descarga de los nuevos datos de filtrado de URL puede tardar hasta 20 minutos. Una vez descargadas las actualizaciones, es posible que la actualización en sí tarde hasta 30 minutos.

5. De manera opcional, marque la casilla de verificación **Consultar URL desconocidas en la nube** para URL desconocidas para consultar al servicio en la nube las URL desconocidas. Esta opción permite que el sistema consulte la nube de Sourcefire cuando alguien de la red

supervisada intente acceder a una URL que no está en el conjunto de datos local. Si la nube no conoce la categoría o la reputación de una URL, o si FireSIGHT Management Center no puede ponerse en contacto con la nube, la URL no cumple las reglas de control de acceso con las condiciones de URL basadas en la categoría o la reputación.

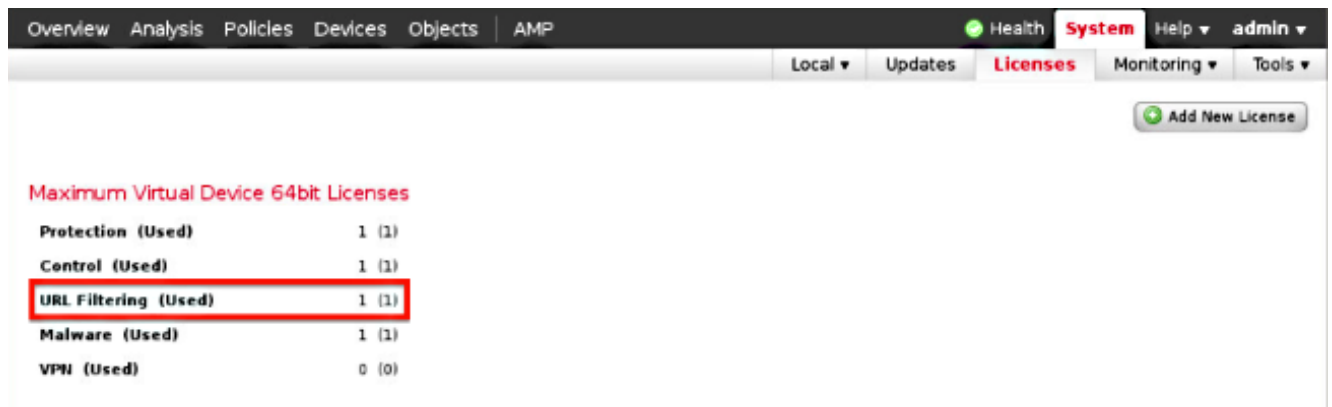
Nota: No puede asignar categorías o reputaciones a las URL manualmente. Desactive esta opción si no desea que la nube de Sourcefire catalogue las URL no categorizadas, por ejemplo, por motivos de privacidad.

6. Click **Save**. Se guarda la configuración de filtrado de URL.

Nota: En función del tiempo transcurrido desde que se habilitó el filtrado de URL por última vez, o si es la primera vez que ha habilitado el filtrado de URL, un FireSIGHT Management Center recupera los datos del filtrado de URL del servicio en la nube.

Aplicación de la licencia de filtrado de URL en un dispositivo administrado

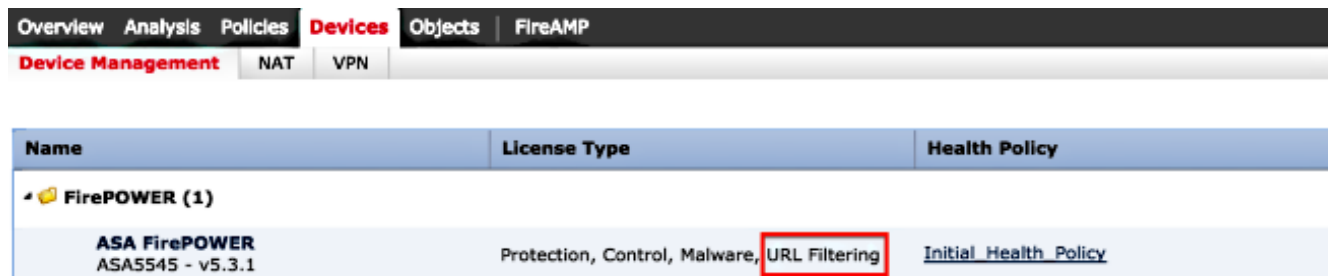
1. Compruebe si la licencia de filtrado de URL está instalada en FireSIGHT Management Center. Vaya a la página **System > Licenses** para encontrar una lista de licencias.



The screenshot shows the 'Licenses' page in the FireSIGHT Management Center. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'System' tab is active, and the 'Licenses' sub-tab is selected. A table displays the license usage for various features:

Maximum Virtual Device 64bit Licenses	
Protection (Used)	1 (1)
Control (Used)	1 (1)
URL Filtering (Used)	1 (1)
Malware (Used)	1 (1)
VPN (Used)	0 (0)

2. Vaya a la página **Devices > Device Management**, y verifique si la licencia de filtrado de URL se aplica en el dispositivo que monitorea el tráfico.



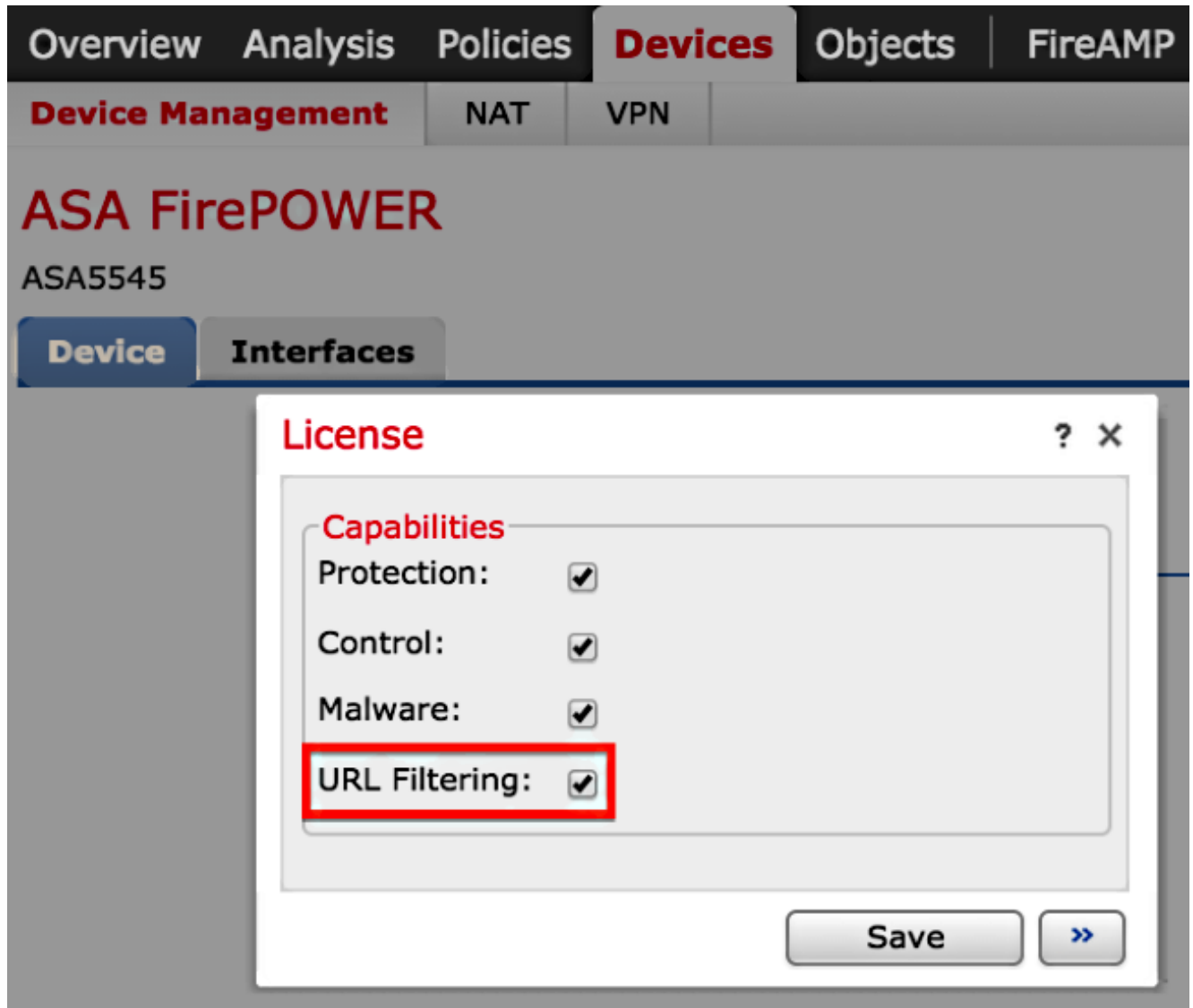
The screenshot shows the 'Device Management' page in the FireSIGHT Management Center. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Device Management' sub-tab is selected. A table displays the license information for the devices:

Name	License Type	Health Policy
FirePOWER (1)		
ASA FirePOWER ASA5545 - v5.3.1	Protection, Control, Malware, URL Filtering	Initial Health Policy

3. Si la licencia de filtrado de URL no se aplica en un dispositivo, haga clic en el icono del **lápiz** para editar la configuración. El icono se encuentra junto al nombre del dispositivo.



4. Puede habilitar la licencia de filtrado de URL en un dispositivo desde la pestaña **Devices**.



5. Después de habilitar una licencia y guardar los cambios, también debe hacer clic en **Apply Changes** para aplicar la licencia en el dispositivo administrado.

 **You have unapplied changes**

 **Apply Changes**

Exclusión de un sitio específico de una categoría de URL bloqueada

FireSIGHT Management Center no permite tener una clasificación local de URL que sustituya a las clasificaciones de categoría predeterminadas proporcionadas por Sourcefire. Para realizar esta tarea, debe utilizar una directiva de control de acceso. Estas instrucciones describen cómo utilizar un objeto URL en una regla de control de acceso para excluir un sitio específico de una categoría de bloque.

1. Vaya a la página **Objects > Object Management**.
2. **Elija Objetos individuales** para URL y haga clic en el botón **Agregar URL**. Aparece la ventana

URL Objects.

URL Objects



Name:

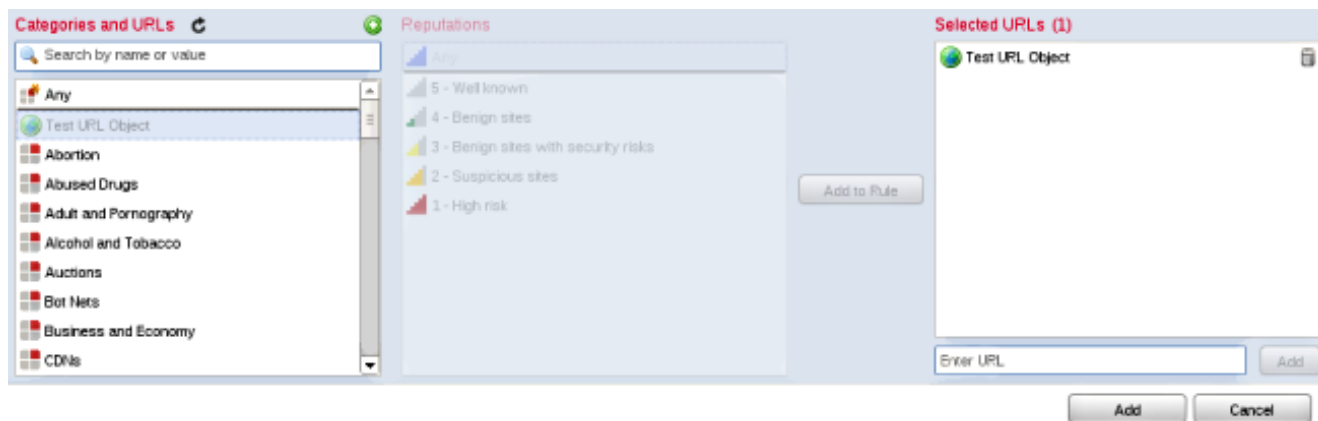
URL:

Overview Analysis Policies Devices **Objects** FireAMP

Object Management

Name	Value
Test URL Object	http://www.cisco.com

- Después de guardar los cambios, elija **Policies > Access Control** y haga clic en el icono del lápiz para editar la política de Access Control.
- Haga clic en **Agregar regla**.
- Agregue el objeto URL a la regla con la acción **Permitir** y colóquelo sobre la regla Categoría de URL, de modo que su acción de regla se evalúe primero.



6. Después de agregar la regla, haga clic en **Guardar y aplicar**. Guarda los nuevos cambios y aplica la directiva de control de acceso a los dispositivos administrados.

Verificación

Para obtener información sobre la verificación o solución de problemas, consulte el artículo **Solución de problemas con el filtrado de URL en el sistema FireSIGHT** vinculado en la sección Información relacionada.

Troubleshoot

Para obtener información sobre verificación o solución de problemas, consulte la **Solución de problemas de filtrado de URL en el sistema FireSIGHT** artículo vinculado en la sección Información relacionada.

Información Relacionada

- [Solución de problemas de filtrado de URL en el sistema FireSIGHT](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).