# SDM: Filtrado de URL en el ejemplo de la configuración del router del Cisco IOS

## Contenido



## Introducción

Este documento demuestra cómo configurar el filtrado URL en un router Cisco IOS. El filtrado URL proporciona mayor control sobre el tráfico que atraviesa el router Cisco IOS. El Filtrado de URL se soporta en las versiones deL Cisco IOS en la versión 12.2(11)YU y posterior.

**Nota:** Porque el Filtrado de URL es Uso intensivo de la CPU, el uso de un servidor de filtrado externo se asegura de que la producción del otro tráfico no sea afectada. De acuerdo con la velocidad de su red y la capacidad de su servidor del Filtrado de URL, el tiempo requerido para la conexión inicial puede ser perceptiblemente más lento cuando el tráfico se filtra con un servidor de filtrado externo.

## prerrequisitos

### Restricciones para el Filtrado de URL del Websense del Firewall

**Requisito del servidor Websense:** Para habilitar esta característica, usted debe tener por lo menos un servidor Websense; , solamente prefieren a dos o más servidores Websense. Aunque no haya límite al número de servidores Websense que usted puede tener, y usted puede configurar tantos

servidores como usted desea, sólo un servidor puede ser activo en cualquier momento — el servidor primario. Las peticiones de las operaciones de búsqueda URL se envían solamente al servidor primario.

**Restricción del soporte del Filtrado de URL:** Este soportes de característica solamente un en un momento activo del esquema del Filtrado de URL. (Antes de que usted habilite el Filtrado de URL del Websense, usted debe asegurarse siempre de que no haya otro esquema del Filtrado de URL configurado, por ejemplo el N2H2.)

**Restricción del nombre de usuario:** Esta característica no pasa la información del nombre de usuario y del grupo al servidor Websense, pero el servidor Websense puede trabajar para las directivas basadas en el usuario porque tiene otro mecanismo para permitir al nombre de usuario para corresponder a una dirección IP.

### Componentes Utilizados

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

- Cisco 2801 Router con el Software Release 12.4(15)T de Cisco IOS®
- Versión 2.5 del (SDM) del administrador de dispositivo Security de Cisco

**Nota:** Refiera a la configuración básica del router usando el SDM para permitir que al router configure el SDM.

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.

### Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Antecedentes

La característica del Filtrado de URL del Websense del Firewall permite a su Firewall Cisco IOS (también conocido como [CSIS] del Cisco Secure Integrated Software) para obrar recíprocamente con el software del Filtrado de URL del Websense. Esto permite que usted prevenga el acceso del usuario a los sitios web especificados en base de una cierta directiva. El Firewall Cisco IOS trabaja con el servidor Websense para saber si un URL determinado puede ser permitido o ser negado (bloqueado).

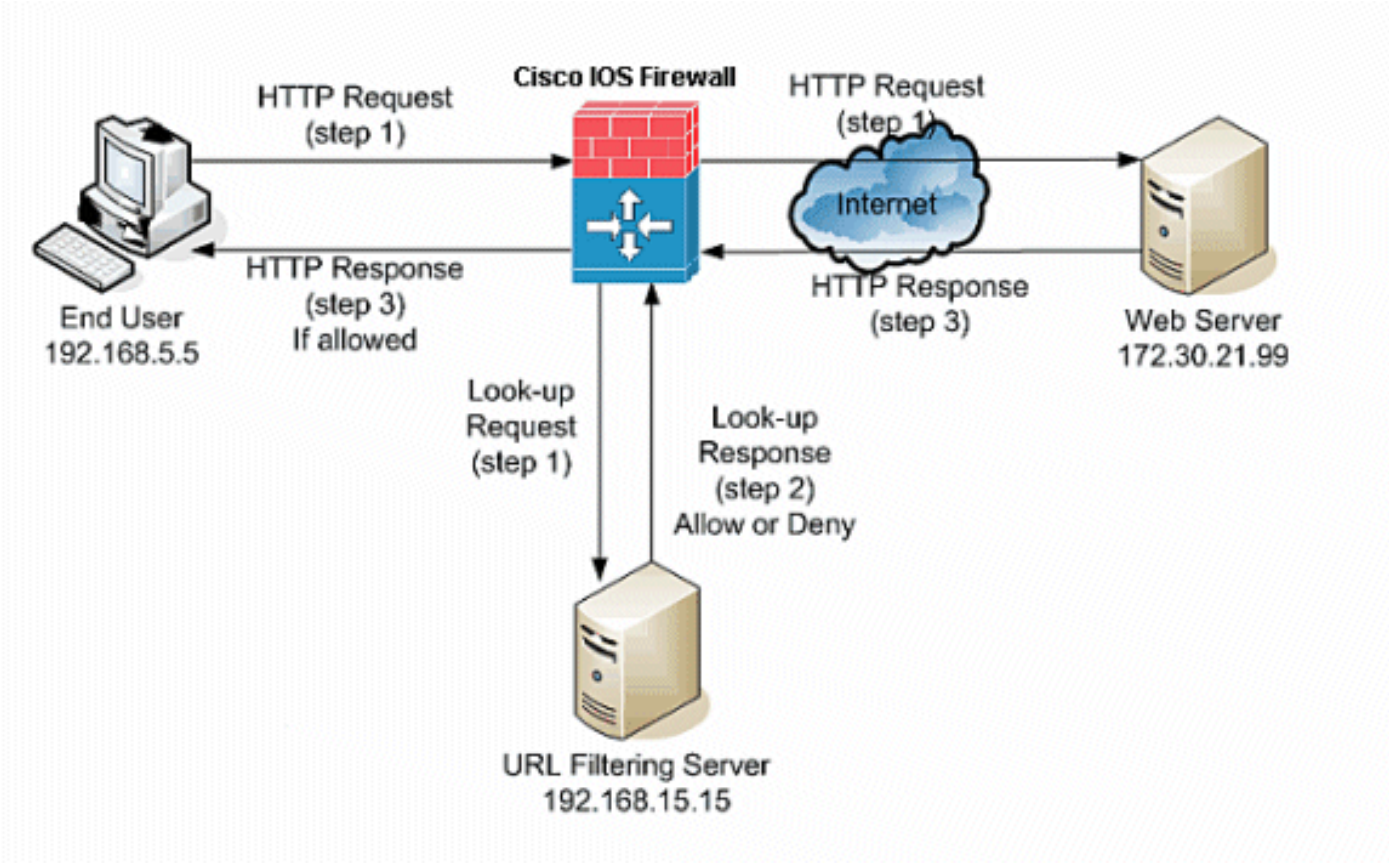
## Configure al router con el CLI

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:




En este ejemplo, el servidor del Filtrado de URL está situado en la red interna. Los usuarios finales situados dentro de la red intentan acceder al servidor Web situado fuera de la red sobre Internet.

Estos pasos se completan en la petición del usuario para el servidor Web:

1. El usuario final hojea a una página en el servidor Web, y el navegador envía un pedido de HTTP.
2. Después de que el Firewall Cisco IOS reciba esta petición, él adelante la petición al servidor Web. Extrae simultáneamente el URL y envía una petición de las operaciones de búsqueda al servidor del Filtrado de URL.
3. Después de que el servidor del Filtrado de URL reciba la petición de las operaciones de búsqueda, marca su base de datos para determinar si al permit or deny el URL. Vuelve un estatus del permit or deny con una respuesta de las operaciones de búsqueda al Firewall de Cisco IOS®.
4. El Firewall de Cisco IOS® recibe esta respuesta de las operaciones de búsqueda y realiza una de estas funciones:Si la respuesta de las operaciones de búsqueda permite el URL, envía el HTTP de respuesta al usuario final.Si la respuesta de las operaciones de búsqueda niega el URL, el servidor del Filtrado de URL reorienta al usuario a su propio servidor Web interno, que visualiza un mensaje que describa la categoría bajo la cual se bloquea el URL. Después de eso, la conexión se reajusta en los ambos extremos.

## Identifique al servidor de filtrado

Usted necesita identificar el direccionamiento del servidor de filtrado con el comando del **servidor del proveedor del urlfilter del IP**. Usted debe utilizar la forma apropiada de este comando basado en el tipo de servidor de filtrado que usted utiliza.

**Nota:** Usted puede configurar solamente un tipo único de servidor, Websense o N2H2, en su configuración.

### Websense

El Websense es un software de filtración de tercera persona que puede filtrar los pedidos de HTTP en base de estas directivas:

- nombre del host de destino
- IP Address de destino
- palabras claves
- Nombre de usuario

El software mantiene una base de datos URL de más de 20 millones de sitios ordenados en más de 60 categorías y subcategorías.

El comando del **servidor del proveedor del urlfilter del IP** señala el servidor que ejecuta la aplicación del Filtrado de URL N2H2 o del Websense. Para configurar un servidor del vendedor para el Filtrado de URL, utilice el comando del **servidor del proveedor del urlfilter del IP** en el modo de configuración global. Para quitar un servidor de su configuración, no utilice la ninguna forma de este comando. Éste es el sintaxis del comando del **servidor del proveedor del urlfilter del IP**:

```
hostname(config)# ip urlfilter server vendor {websense | n2h2} ip-address [port port-number]
[timeout seconds] [retransmit number] [outside] [vrf vrf-name]
```

Substituya el `IP address` por la dirección IP del servidor Websense. Substituya los `segundos` por el número de segundos que el escudo de protección IOS deba continuar para intentar conectar con el servidor de filtrado.

Por ejemplo, para configurar a un solo servidor de filtrado del Websense para el Filtrado de URL, publique este comando:

```
hostname(config)#
   ip urlfilter server vendor websense 192.168.15.15
```

## Configure la política de filtrado

**Nota:** Usted debe identificar y habilitar el servidor del Filtrado de URL antes de que usted habilite el Filtrado de URL.

### HTTP largo truncado URL

Para permitir que el filtro URL trunque los URL largos al servidor, utilice el comando **truncado del urlfilter del IP** en el modo de configuración global. Para inhabilitar la opción que trunca, no utilice la ninguna forma de este comando. Este comando se soporta en la versión deL Cisco IOS 12.4(6)T y posterior.

`urlfilter del IP truncado {script-parámetros | el nombre de host}` es el sintaxis de este comando.

**script-parámetros:** Solamente el URL hasta las opciones del script se envía. Por ejemplo, si el URL entero es `http://www.cisco.com/dev/xxx.cgi?when=now`, sólo el URL con `http://www.cisco.com/dev/xxx.cgi` se envía (si la longitud soportada máximo URL no se excede).

**Nombre de host:** Solamente se envía el nombre de host. Por ejemplo, si el URL entero es `http://www.cisco.com/dev/xxx.cgi?when=now`, sólo se envía `http://www.cisco.com`.

Si se configuran los script-parámetros y las palabras claves ambas del nombre de host, la palabra clave de los script-parámetros toma la precedencia sobre la palabra clave del nombre de host. Si se configuran ambas palabras claves y se truncan los parámetros URL del script y se excede la longitud soportada máximo URL, el URL se trunca hasta el nombre de host.

**Nota:** Si se configuran los script-parámetros y el nombre de host de las palabras claves, deben estar en las líneas aparte como se muestra abajo. No pueden ser combinados en una línea.

**Nota:** `script-parámetros truncados del urlfilter del IP`

**Nota:** `nombre de host truncado del urlfilter del IP`

## Configuración para el router que funciona con la versión deL Cisco IOS 12.4

Esta configuración incluye los comandos descritos en este documento:

**Configuración para el router que funciona con la versión deL Cisco IOS 12.4**

```
R3#show running-config : Saved version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec service password-encryption ! hostname R3
! ! !--- username cisco123 privilege 15 password 7
104D000A061843595F ! aaa session-id common ip subnet-
zero ! ! ip cef ! ! ip ips sdf location
flash://128MB.sdf ip ips notify SDEE ip ips po max-
events 100 !--- use the ip inspect name command in
global configuration mode to define a set of inspection
rules. This Turns on HTTP inspection. The urlfilter
keyword associates URL filtering with HTTP inspection.
ip inspect name test http urlfilter !--- use the ip
urlfilter allow-mode command in global configuration
mode to turn on the default mode (allow mode) of the
filtering algorithm. ip urlfilter allow-mode on !--- use
the ip urlfilter exclusive-domain command in global
configuration mode to add or remove a domain name to or
from the exclusive domain list so that the firewall does
not have to send lookup requests to the vendor server.
Here we have configured the IOS firewall to permit the
URL www.cisco.com without sending any lookup requests to
the vendor server. ip urlfilter exclusive-domain permit
www.cisco.com !--- use the ip urlfilter audit-trail
command in global configuration mode to log messages
into the syslog server or router. ip urlfilter audit-
trail !--- use the ip urlfilter urlf-server-log command
in global configuration mode to enable the logging of
system messages on the URL filtering server. ip
urlfilter urlf-server-log !--- use the ip urlfilter
server vendor command in global configuration mode to
configure a vendor server for URL filtering. Here we
have configured a websense server for URL filtering ip
urlfilter server vendor websense 192.168.15.15 no ftp-
```

```
server write-enable ! ! !--- Below is the basic
interface configuration on the router interface
FastEthernet0 ip address 192.168.5.10 255.255.255.0 ip
virtual-reassembly !--- use the ip inspect command in
interface configuration mode to apply a set of
inspection rules to an interface. Here the inspection
name TEST is applied to the interface FastEthernet0. ip
inspect test in duplex auto speed auto ! interface
FastEthernet1 ip address 192.168.15.1 255.255.255.0 ip
virtual-reassembly duplex auto speed auto ! interface
FastEthernet2 ip address 10.77.241.109 255.255.255.192
ip virtual-reassembly duplex auto speed auto ! interface
FastEthernet2 no ip address ! interface Vlan1 ip address
10.77.241.111 255.255.255.192 ip virtual-reassembly ! ip
classless ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65 ! ! !---
Configure the below commands to enable SDM access to the
cisco routers ip http server ip http authentication
local no ip http secure-server ! ! line con 0 line aux 0
line vty 0 4 privilege level 15 transport input telnet
ssh ! end
```

# Configure al router con el SDM

## Configuración de SDM del router

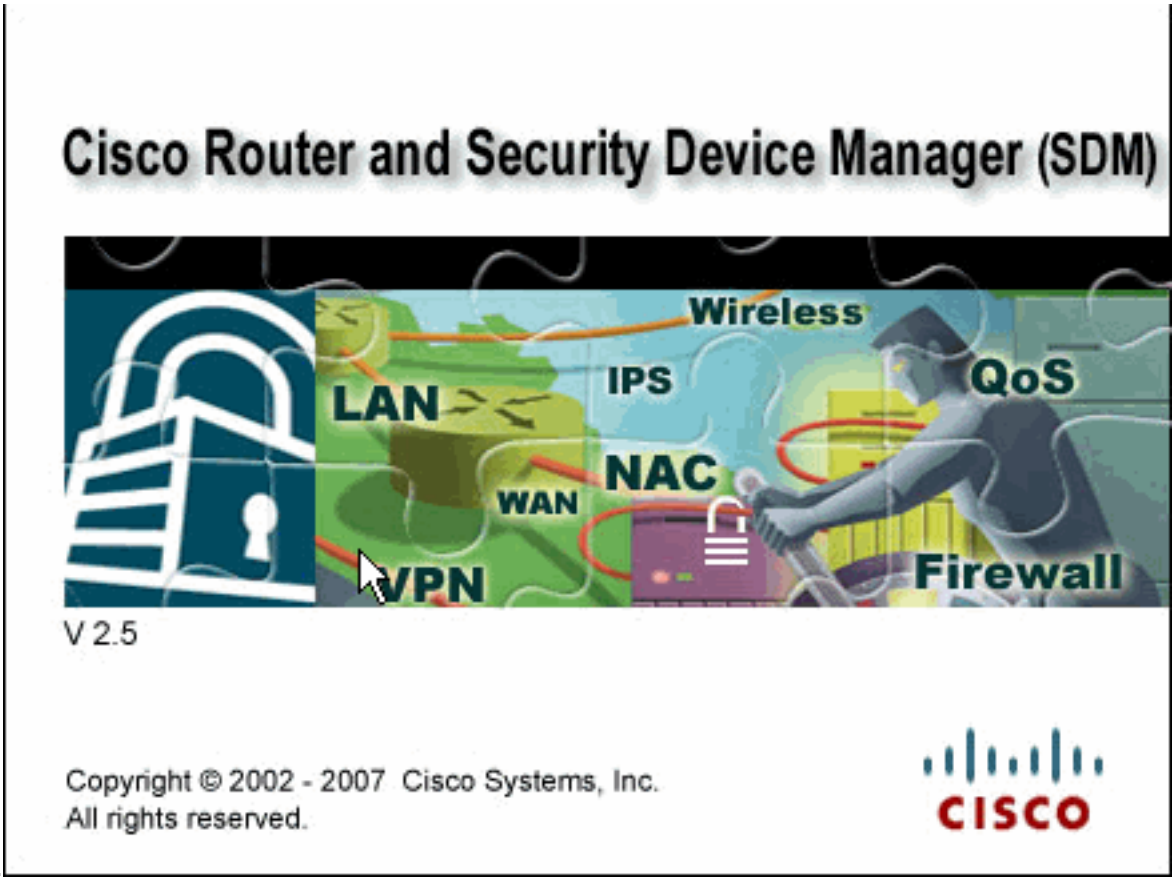
Complete estos pasos para configurar el Filtrado de URL en el router del Cisco IOS:

**Nota:** Para configurar el Filtrado de URL con el SDM, utilice el **comando ip inspect name** en el modo de configuración global de definir un conjunto de las reglas del examen. Esto gira el examen HTTP. La palabra clave del urlfilter asocia el Filtrado de URL al examen HTTP. Entonces el nombre del examen configurado se puede asociar a la interfaz en la cual la filtración debe ser hecha, por ejemplo:

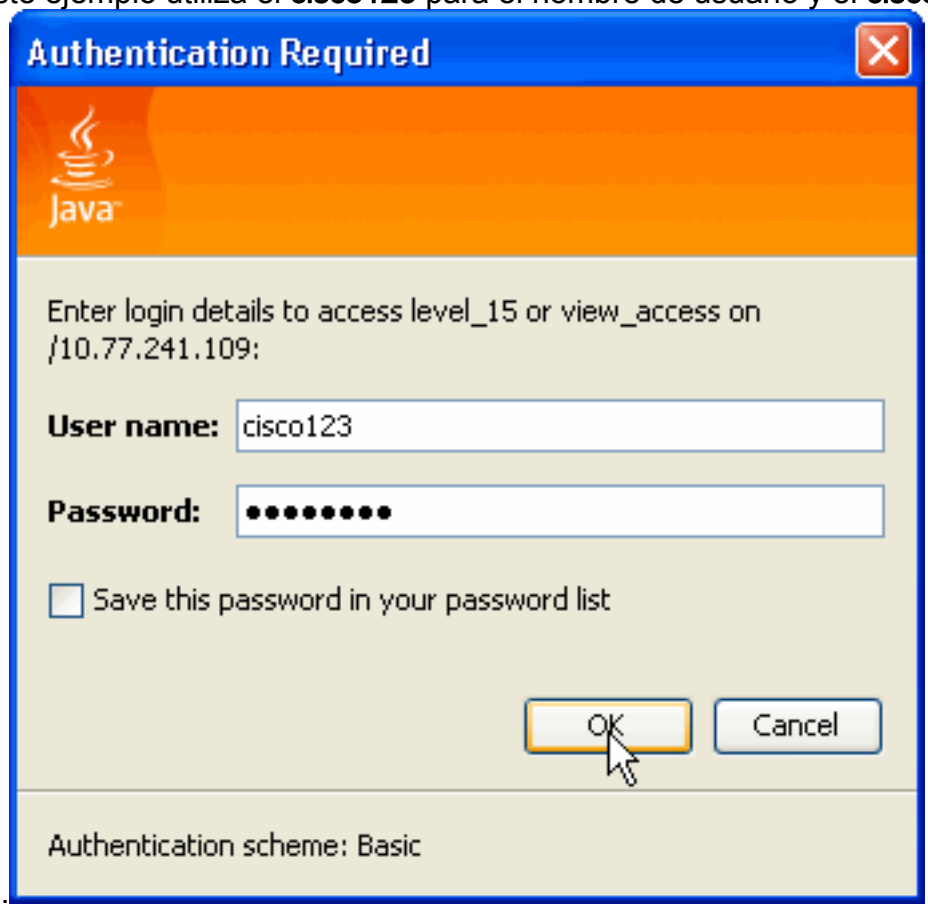
```
hostname(config)#ip inspect
   name test http urlfilter
```

1. Abra su hojeador y ingrese los **<IP_Address de https:// de la interfaz del router que se ha configurado para el SDM Access>** para acceder el SDM en el router.Aseegurese autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad de certificados SSL. Nombre de usuario predeterminado y la contraseña son ambos espacio en blanco.El router presenta esta ventana para permitir la descarga de la aplicación del SDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en los subprogramas

java.

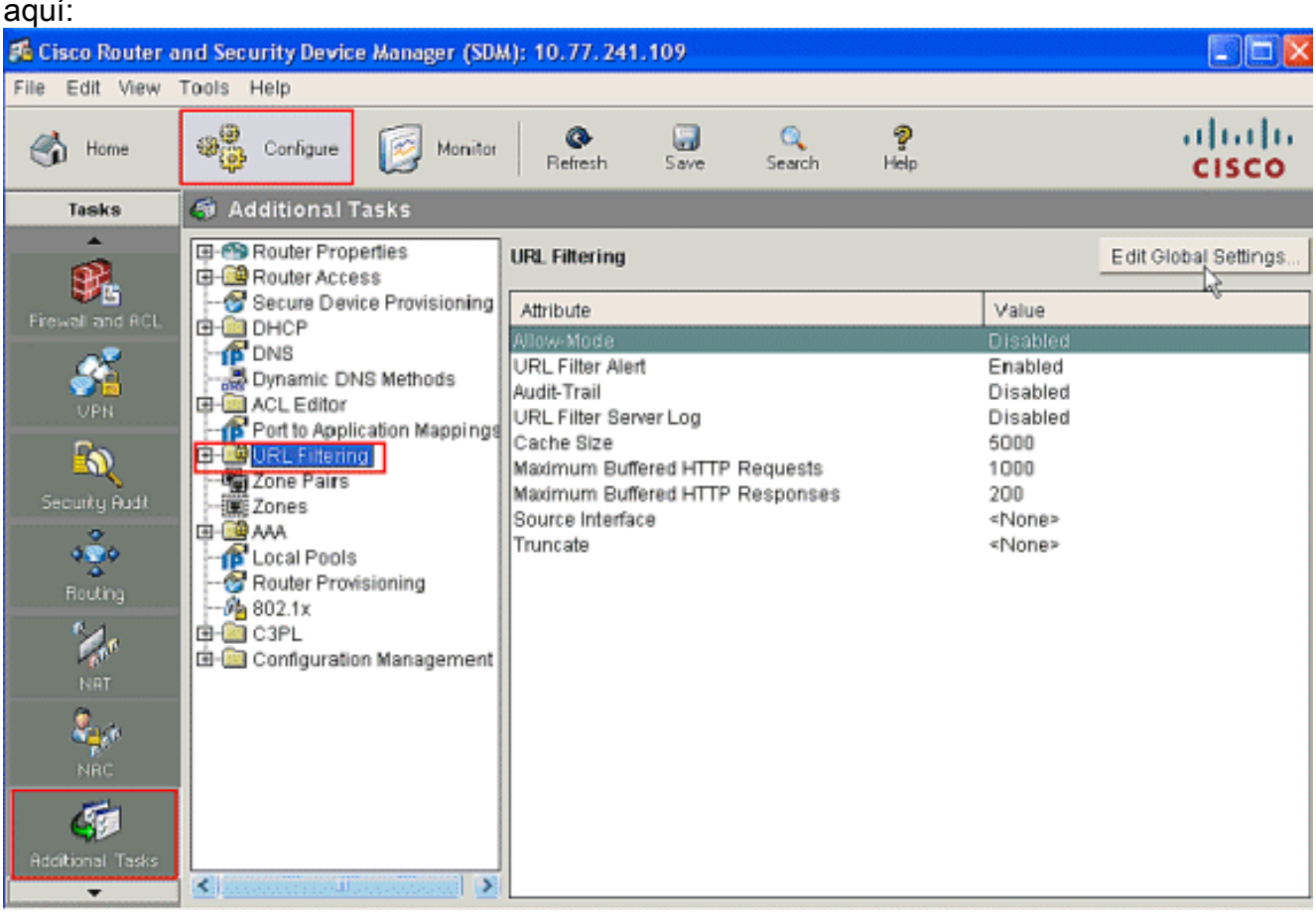



2. La descarga del SDM ahora comienza. Una vez que las descargas del lanzador del SDM, completan los pasos ordenados por los prompts para instalar el software y funcionar con el lanzador del SDM de Cisco.
3. Ingrese el **nombre de usuario y contraseña**, si usted especificó uno, y haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza el **cisco123** para el nombre de usuario y el **cisco123** como la contraseña.

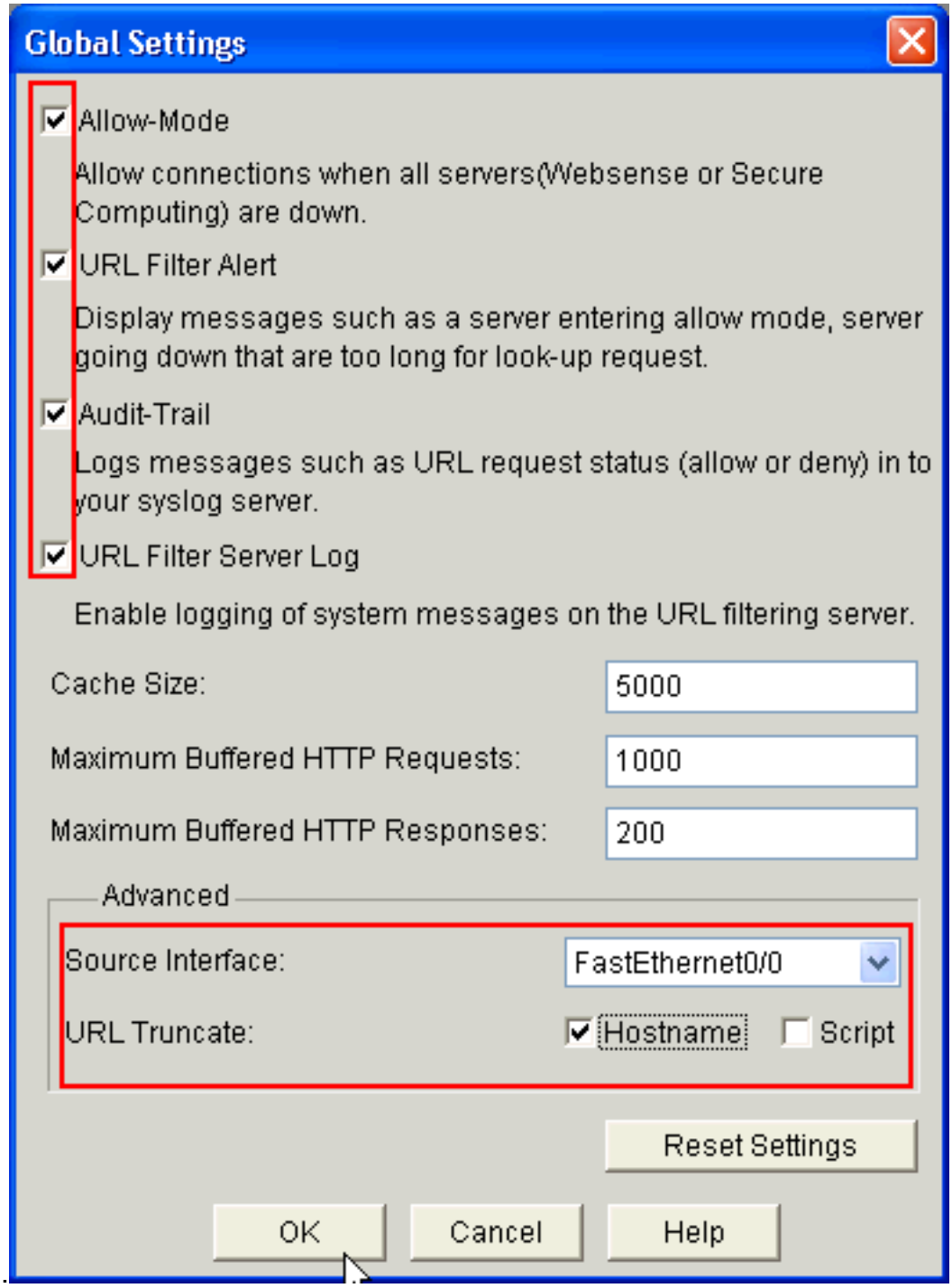



4. Elija las **tareas de Configuration->Additional** y haga clic el **Filtrado de URL** en el Home Page

del SDM. Entonces haga clic **editan las configuraciones globales**, como se muestra aquí:

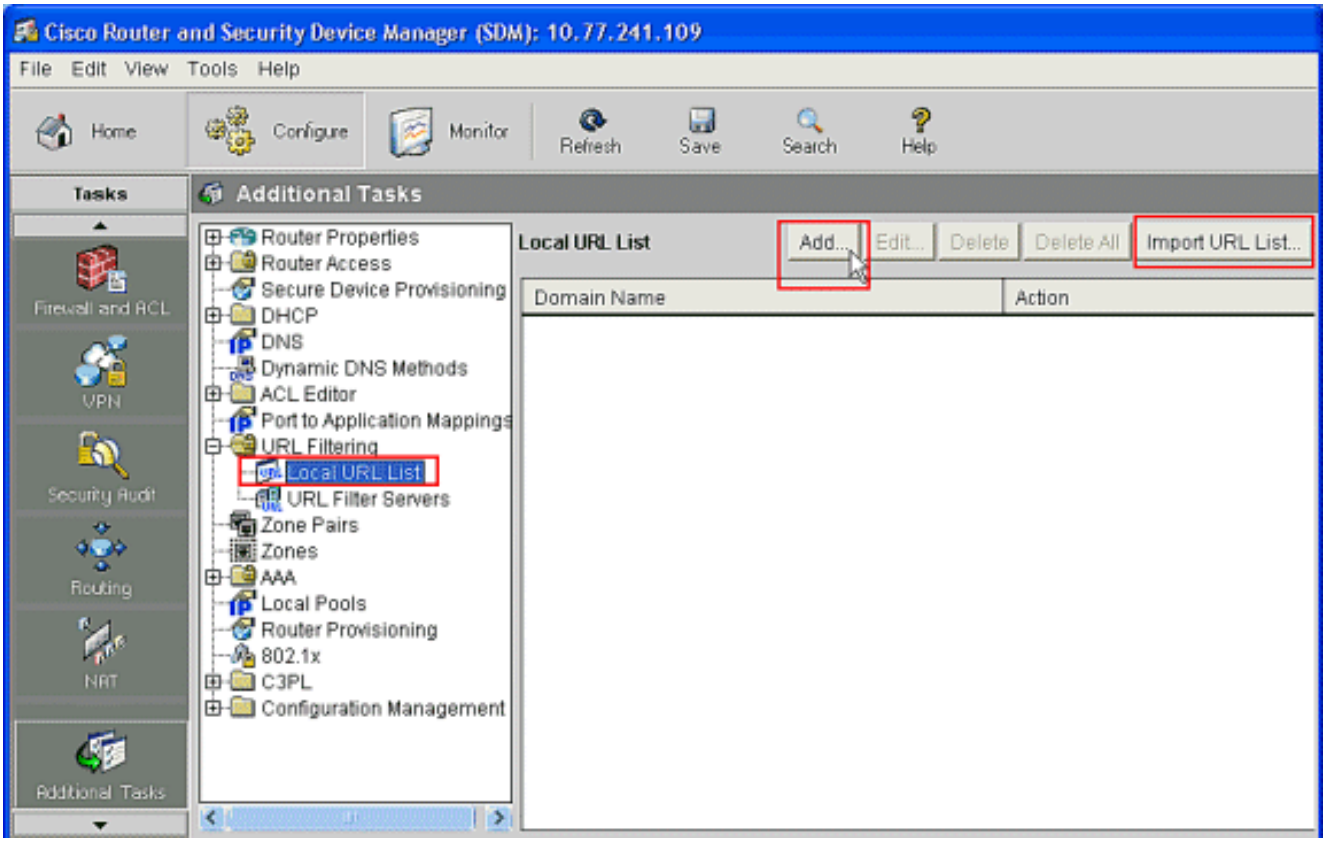



5. En la nueva ventana que aparece, habilite los parámetros requeridos para el Filtrado de URL, tal como **alerta Permitir-MODE, del filtro URL, Auditoría-ensayo** y **registro del servidor del Filtrado de URL**. Marque las casillas de verificación al lado de cada los parámetros como se muestra. Ahora proporcione la información del **tamaño de la memoria caché** y del **buffer HTTP**. También proporcione la **interfaz de origen** y el URL método truncado bajo sección **avanzada** como se muestra para permitir que el filtro URL trunque los URL largos al servidor. (Aquí el parámetro del truncamiento se elige como **nombre de host**.) Ahora haga clic la

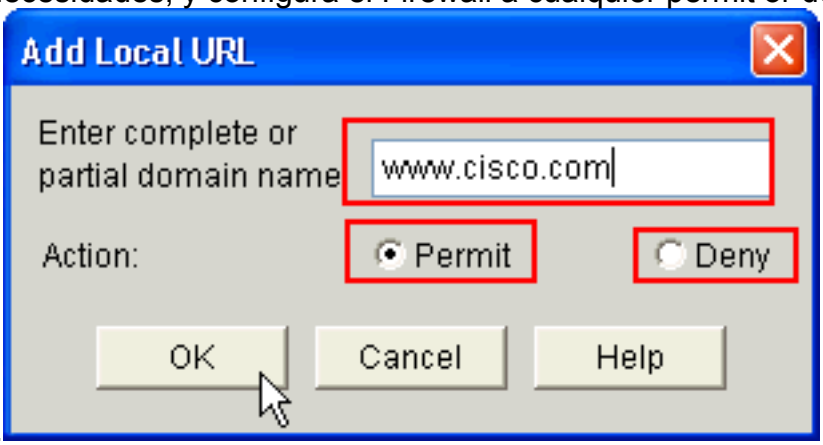



**AUTORIZACIÓN.**

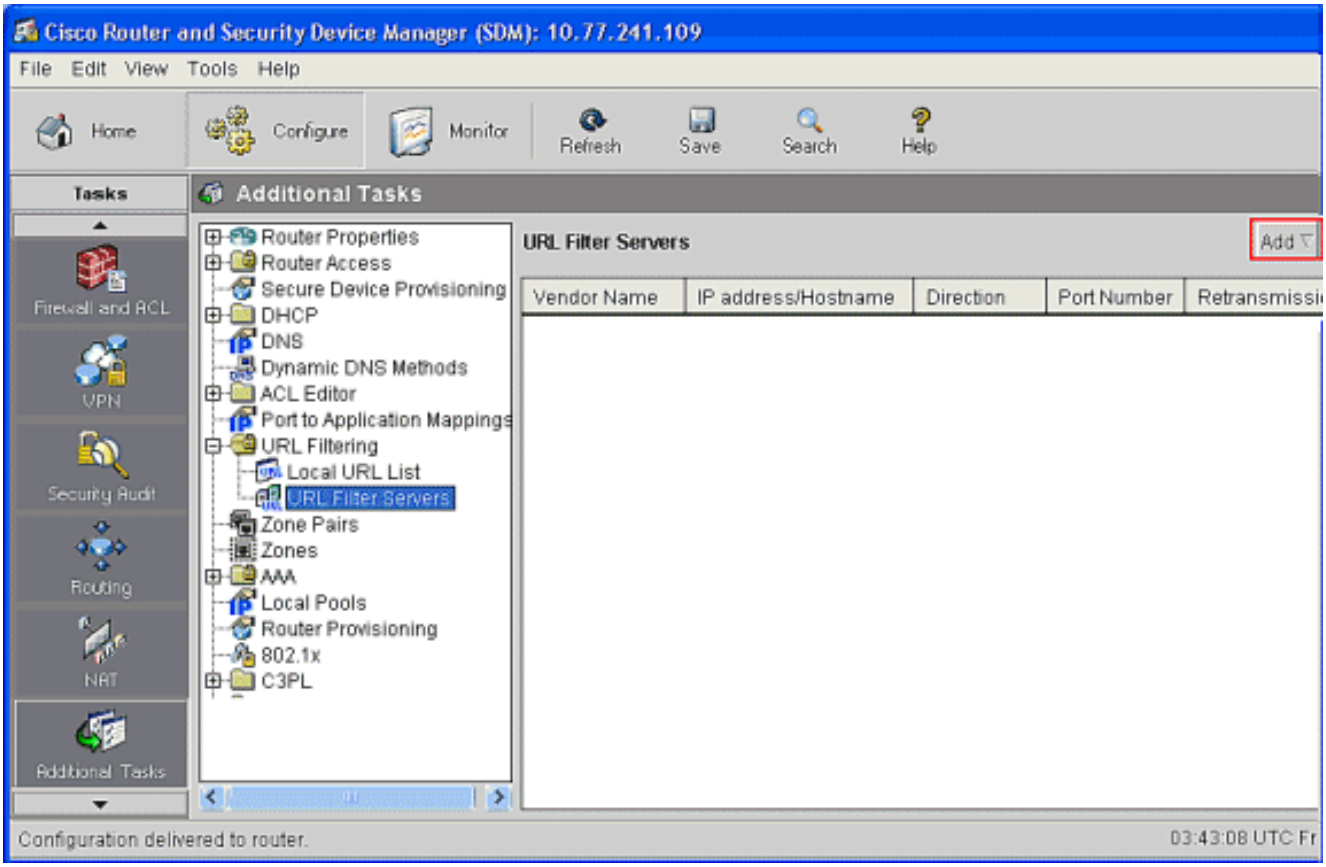
6. Ahora elija la opción **local de la lista url** situada bajo tecleo de cuadro del **Filtrado de URL agregan** para agregar el Domain Name y configurar el Firewall al permit or deny que el Domain Name agregó. Usted puede también elegir la **lista url de importación de la** opción si la lista de URL necesarios es presente como archivo. La opción es la suya para elegir el **agregar URL** o las opciones de la **lista url de la importación** basadas en el requisito y la Disponibilidad de la lista
url.



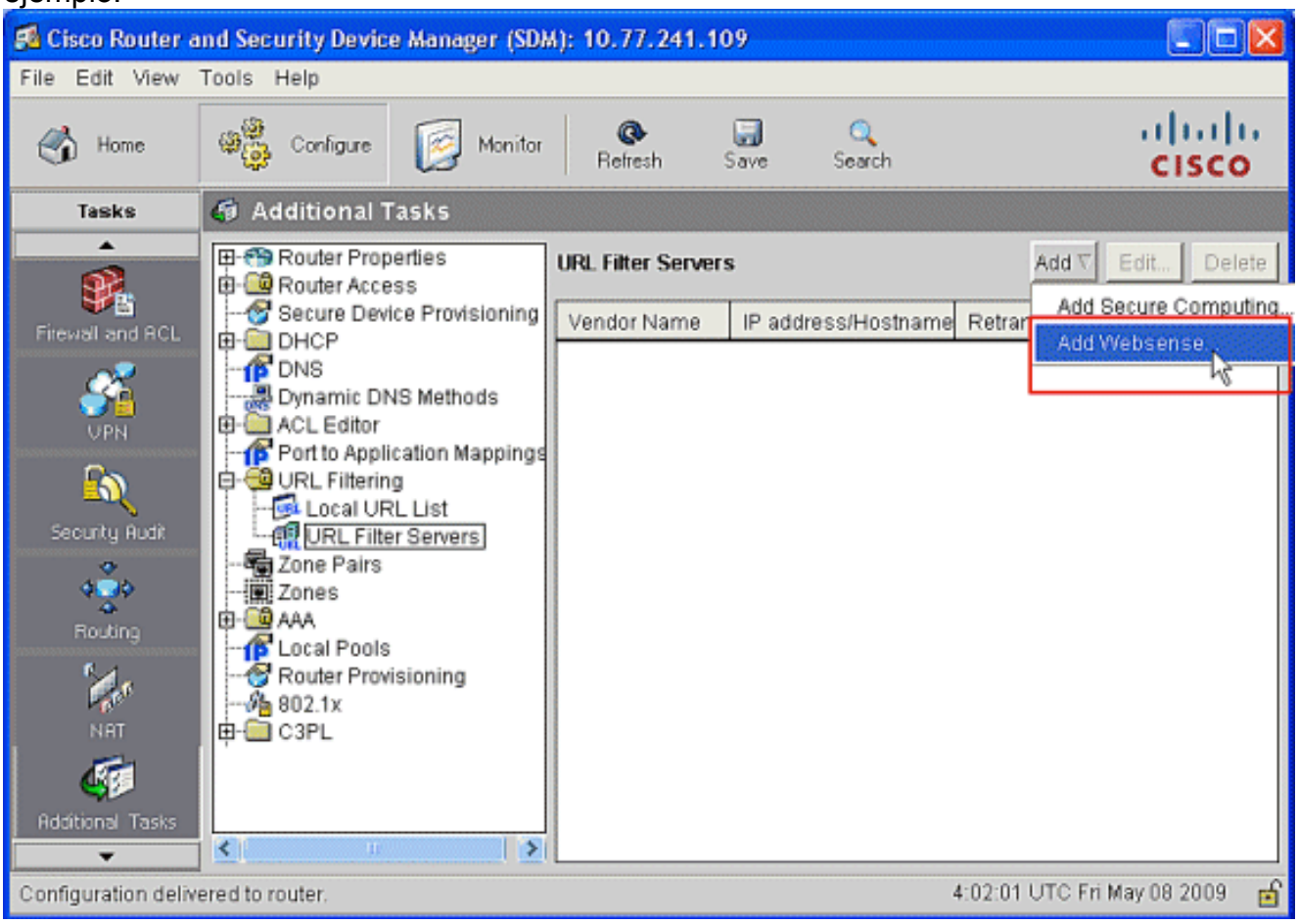

7. En este ejemplo, el tecleo **agrega** para agregar el URL y para configurar el escudo de protección IOS al permit or deny el URL como sea necesario. Ahora una nueva ventana titulada **AGREGA EL URL local** se abre en cuál tiene que proporcionar el Domain Name y decidir el usuario si al permit or deny el URL. Haga clic el botón de radio al lado de la opción del permit or deny como se muestra. Aquí el Domain Name es **www.cisco.com**, y el usuario **permite el URL www.cisco.com**. De la misma manera, usted puede hacer clic **agrega**, agrega tantos URL según las necesidades, y configura el Firewall a cualquier permit or deny que basaron en el requisito.




8. Elija la **selección de servidores del filtro URL** situada bajo lengueta del **Filtrado de URL**, como se muestra. El tecleo **agrega** para agregar el Filtrado de URL Nombre del servidor que realiza la función del Filtrado de URL.

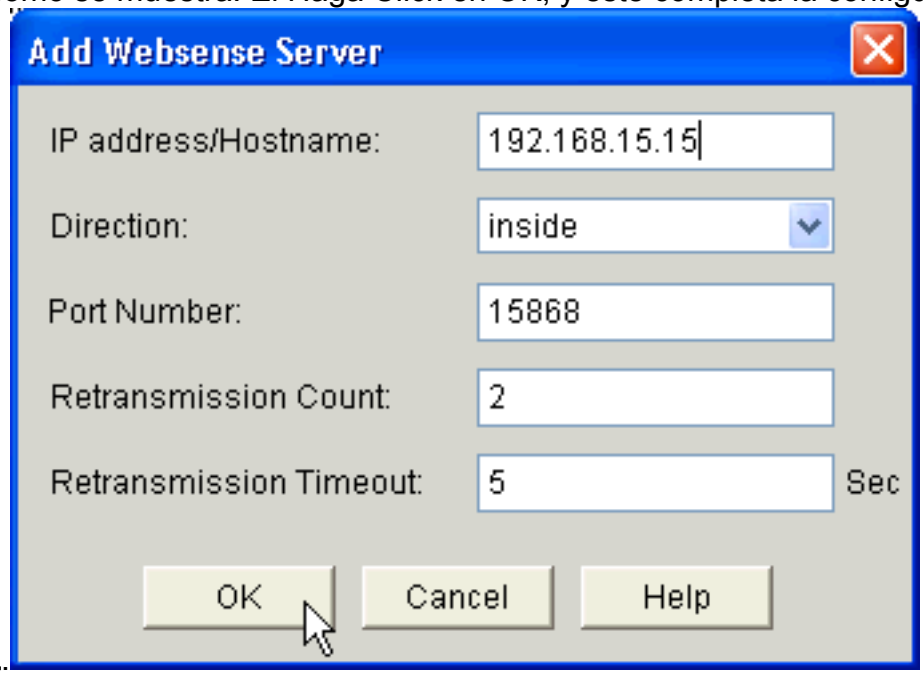



9. Después de que usted tecleo **agregue**, elija al servidor de filtrado como **Websense** como se muestra abajo puesto que utilizan al servidor de filtrado del Websense en este ejemplo.




10. En esto **agregue la** ventana del **servidor Websense**, proporcione la **dirección IP del** servidor Websense junto con la **dirección** en la cual el filtro funciona y **número del puerto,** (el número del puerto predeterminado para el servidor Websense es **15868**). También

proporcione la **cuenta de la retransmisión** y los **valores de agotamiento del tiempo de la retransmisión**, como se muestra. El Haga Click en OK, y éste completa la configuración del Filtrado de URL.




# Verificación

Utilice los comandos en esta sección para ver la información del Filtrado de URL. Usted puede utilizar estos comandos para verificar su configuración.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

- muestre las estadísticas del urlfilter del IP — Demostraciones información y estadísticas sobre el servidor de filtradoPor ejemplo:`Router# show ip urlfilter statistics URL filtering statistics ================ Current requests count:25 Current packet buffer count(in use):40 Current cache entry count:3100 Maxever request count:526 Maxever packet buffer count:120 Maxever cache entry count:5000 Total requests sent to URL Filter Server: 44765 Total responses received from URL Filter Server: 44550 Total requests allowed: 44320 Total requests blocked: 224`
- muestre el caché del urlfilter del IP — Visualiza el número máximo de entradas que se puedan ocultar en la tabla de caché, el número de entradas, y los IP Address de destino que se ocultan en la tabla de caché cuando usted utiliza el comando cache del urlfilter del IP de la demostración en el modo EXEC privilegiado
- muestre los config del filtro del urlfilter del IP — Muestra la configuración de filtraciónPor ejemplo:`hostname#show ip urlfilter config URL filter is ENABLED Primary Websense server configurations ==================================== Websense server IP address Or Host Name: 192.168.15.15 Websense server port: 15868 Websense retransmission time out: 6 (in seconds) Websense number of retransmission: 2 Secondary Websense servers configurations ========================================= None Other configurations ==================== Allow Mode: ON System Alert: ENABLED Audit Trail: ENABLED Log message on Websense server: ENABLED Maximum number of cache entries: 5000 Maximum number of packet buffers: 200 Maximum outstanding requests: 1000`

# Troubleshooting

## Mensajes de error

`%URLF-3-SERVER_DOWN: La conexión al servidor 10.92.0.9 del filtro URL es abajo` — presentaciones del mensaje de este LOG_ERR-type del nivel tres cuando va un UFS configurado abajo. Cuando sucede esto, el Firewall marcará al servidor configurado como secundario e intentará criar a uno de los otros servidores secundarios y marcar ese servidor como el servidor primario. Si no hay otro servidor configurado, el Firewall ingresará permite el modo y visualiza el mensaje `URLF-3-ALLOW_MODE`.

`%URLF-3-ALLOW_MODE: La conexión a todos los servidores del filtro URL está abajo y PERMITE EL MODE está apagada` — las presentaciones del mensaje de este tipo LOG_ERR cuando todos los UFS están abajo, y el sistema ingresa permiten el modo.

**Nota:** Siempre que el sistema entre permita el modo (todos los servidores del filtro están abajo), un temporizador señal de mantenimiento periódico se acciona que intente abrir una conexión TCP y traer para arriba un servidor.

`%URLF-5-SERVER_UP: La conexión a un servidor 10.92.0.9 del filtro URL se hace; el sistema está volviendo de PERMITE EL MODE` — las presentaciones del mensaje de este LOG_NOTICE-type cuando los UFS se detectan como ascendente y las devoluciones del sistema del modo de la permit.

`¿%URLF-4-URL_TOO_LONG:URL demasiado de largo (más de 3072 bytes), posiblemente un paquete falso?` — Presentaciones del mensaje de este LOG_WARNING-type cuando el URL en una petición de las operaciones de búsqueda es demasiado largo; cualquier URL que 3K se cae más de largo.

`%URLF-4-MAX_REQ: El número de petición pendiente excede el límite máximo <1000>` — se caen las presentaciones del mensaje de este LOG_WARNING-type cuando el número de peticiones pendientes en el sistema excede el límite máximo, y todas piden más lejos.

# Información Relacionada

- Cisco IOS Firewall
- Filtrado de URL del Websense del Firewall
- Guía de configuración de la Seguridad de Cisco IOS, versión 12.4-Support
- Soporte Técnico y Documentación - Cisco Systems