

SDM: URL Filtering on Cisco IOS Router Configuration Example

Document ID: 110318

Introduction

Prerequisites

- Restrictions for Firewall Websense URL Filtering
- Components Used
- Conventions

Background Information

Configure the Router with the CLI

- Network Diagram
- Identify the Filtering Server
- Configure the Filtering Policy
- Configuration for Router that runs Cisco IOS version 12.4

Configure the Router with SDM

- Router SDM Configuration

Verify

Troubleshoot

- Error Messages

Related Information

Introduction

This document demonstrates how to configure URL Filtering on a Cisco IOS Router. URL Filtering provides greater control over the traffic that passes through the Cisco IOS Router. URL Filtering is supported in Cisco IOS versions in version 12.2(11)YU and later.

Note: Because URL filtering is CPU-intensive, the use of an external filtering server ensures that the throughput of other traffic is not affected. Based on the speed of your network and the capacity of your URL filtering server, the time required for the initial connection can be noticeably slower when traffic is filtered with an external filtering server.

Prerequisites

Restrictions for Firewall Websense URL Filtering

Websense Server Requirement: In order to enable this feature, you must have at least one Websense server, but two or more Websense servers are preferred. Although there is no limit to the number of Websense servers you can have, and you can configure as many servers as you wish, only one server can be active at any given time the primary server. URL look-up requests are sent only to the primary server.

URL Filtering Support Restriction: This feature supports only one active URL filtering scheme at a time. (Before you enable Websense URL filtering, you must always ensure that there is not another URL filtering scheme configured, such as N2H2.)

Username Restriction: This feature does not pass the username and group information to the Websense server, but the Websense server can work for user-based policies because it has another mechanism to enable the username to correspond to an IP address.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2801 router with Cisco IOS® Software Release 12.4(15)T
- Cisco Security Device Manager (SDM) Version 2.5

Note: Refer to Basic Router Configuration using SDM in order to allow the router to be configured by SDM.

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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The Firewall Websense URL Filtering feature enables your Cisco IOS firewall (also known as Cisco Secure Integrated Software [CSIS]) to interact with the Websense URL filtering software. This allows you to prevent user access to specified websites on the basis of some policy. The Cisco IOS firewall works with the Websense server to know whether a particular URL can be allowed or denied (blocked).

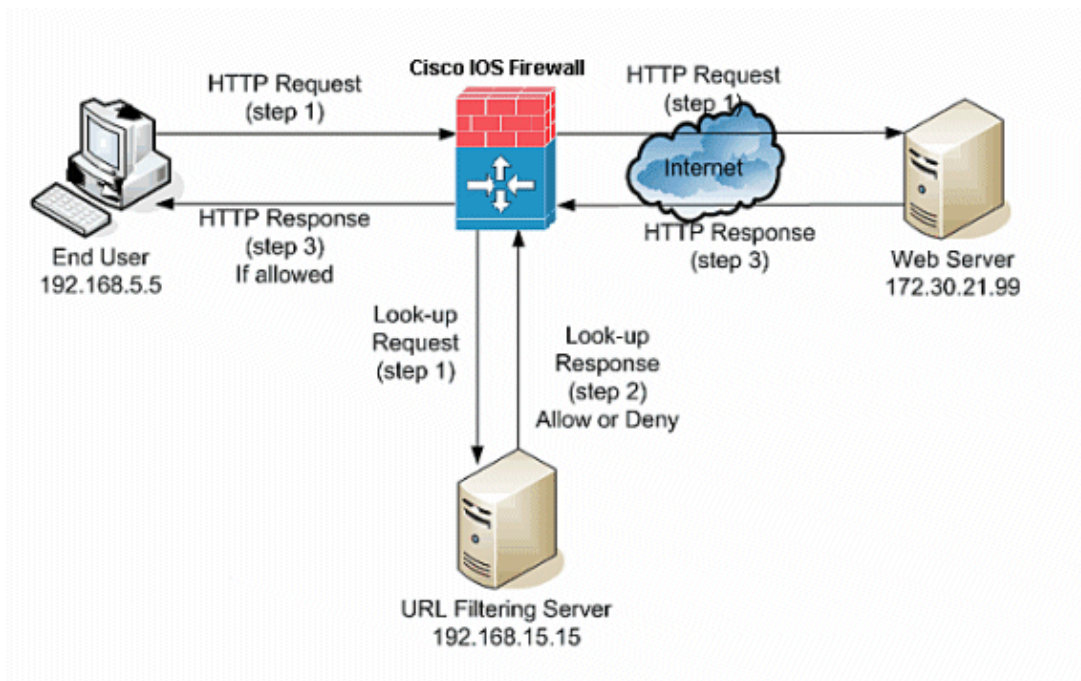
Configure the Router with the CLI

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



In this example, the URL filtering server is located in the inside network. End users located inside the network try to access the web server located outside the network over the Internet.

These steps are completed at the user request for the web server:

1. The end user browses to a page on the web server, and the browser sends an HTTP request.
2. After the Cisco IOS Firewall receives this request, it forwards the request to the web server. It simultaneously extracts the URL and sends a look-up request to the URL filtering server.
3. After the URL filtering server receives the look-up request, it checks its database in order to determine whether to permit or deny the URL. It returns a permit or deny status with a look-up response to the Cisco IOS® firewall.
4. The Cisco IOS® firewall receives this look-up response and performs one of these functions:
 - ◆ If the look-up response permits the URL, it sends the HTTP response to the end user.
 - ◆ If the look-up response denies the URL, the URL filtering server redirects the user to its own internal web server, which displays a message that describes the category under which the URL is blocked. Thereafter, the connection is reset on both ends.

Identify the Filtering Server

You need to identify the address of the filtering server with the **ip urlfilter server vendor** command. You must use the appropriate form of this command based on the type of filtering server you use.

Note: You can only configure a single type of server, either Websense or N2H2, in your configuration.

Websense

Websense is a third-party filtering software that can filter HTTP requests on the basis of these policies:

- destination hostname
- destination IP address
- keywords
- user name

The software maintains a URL database of more than 20 million sites organized into more than 60 categories and subcategories.

The **ip urlfilter server vendor** command designates the server that runs the N2H2 or Websense URL filtering application. In order to configure a vendor server for URL filtering, use the **ip urlfilter server vendor** command in global configuration mode. In order to remove a server from your configuration, use the no form of this command. This is the syntax of the **ip urlfilter server vendor** command:

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

Replace `ip-address` with the IP address of the websense server. Replace `seconds` with the number of seconds that the IOS Firewall must continue to try to connect to the filtering server.

For example, in order to configure a single Websense filtering server for URL filtering, issue this command:

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

Configure the Filtering Policy

Note: You must identify and enable the URL filtering server before you enable URL filtering.

Truncate Long HTTP URLs

In order to allow the URL filter to truncate long URLs to the server, use the **ip urlfilter truncate** command in global configuration mode. In order to disable the truncating option, use the no form of this command. This command is supported in Cisco IOS version 12.4(6)T and later.

`ip urlfilter truncate {script-parameters | hostname}` is the syntax of this command.

script-parameters: Only the URL up to the script options is sent. For example, if the entire URL is `http://www.cisco.com/dev/xxx.cgi?when=now`, only the URL through `http://www.cisco.com/dev/xxx.cgi` is sent (if the maximum supported URL length is not exceeded).

Hostname: Only the hostname is sent. For example, if the entire URL is `http://www.cisco.com/dev/xxx.cgi?when=now`, only `http://www.cisco.com` is sent.

If the `script-parameters` and `hostname` keywords are both configured, the `script-parameters` keyword takes precedence over the `hostname` keyword. If both keywords are configured and the script parameters URL is truncated and the maximum supported URL length is exceeded, the URL is truncated up to the hostname.

Note: If both keywords `script-parameters` and `hostname` are configured, they must be on separate lines as shown below. They cannot be combined in one line.

Note: `ip urlfilter truncate script-parameters`

Note: `ip urlfilter truncate hostname`

Configuration for Router that runs Cisco IOS version 12.4

This configuration includes the commands described in this document:

Configuration for Router that runs Cisco IOS Version 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 the Router with SDM

Router SDM Configuration

Complete these steps in order to configure URL filtering on the Cisco IOS Router:

Note: In order to configure URL Filtering with SDM, 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. Then the inspection name configured can be mapped to the interface on which the filtering is to be done, for example:

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

1. Open your browser and enter **https://<IP_Address of the interface of the Router that has been configured for SDM Access>** to access the SDM on the Router.

Make sure to authorize any warnings your browser gives you related to the SSL certificate authenticity. The default username and password are both blank.

The router presents this window to allow the download of the SDM application. This example loads the application onto the local computer and does not run in a Java applet.

Cisco Router and Security Device Manager (SDM)



V 2.5

Copyright © 2002 - 2007 Cisco Systems, Inc.
All rights reserved.



2. The SDM download starts now. Once the SDM Launcher downloads, complete the steps directed by the prompts in order to install the software and run the Cisco SDM Launcher.
3. Enter the **Username** and **Password**, if you specified one, and click **OK**.

This example uses the **cisco123** for the username and **cisco123** as the password.

Authentication Required

Java

Enter login details to access level_15 or view_access on /10.77.241.109:

User name: cisco123

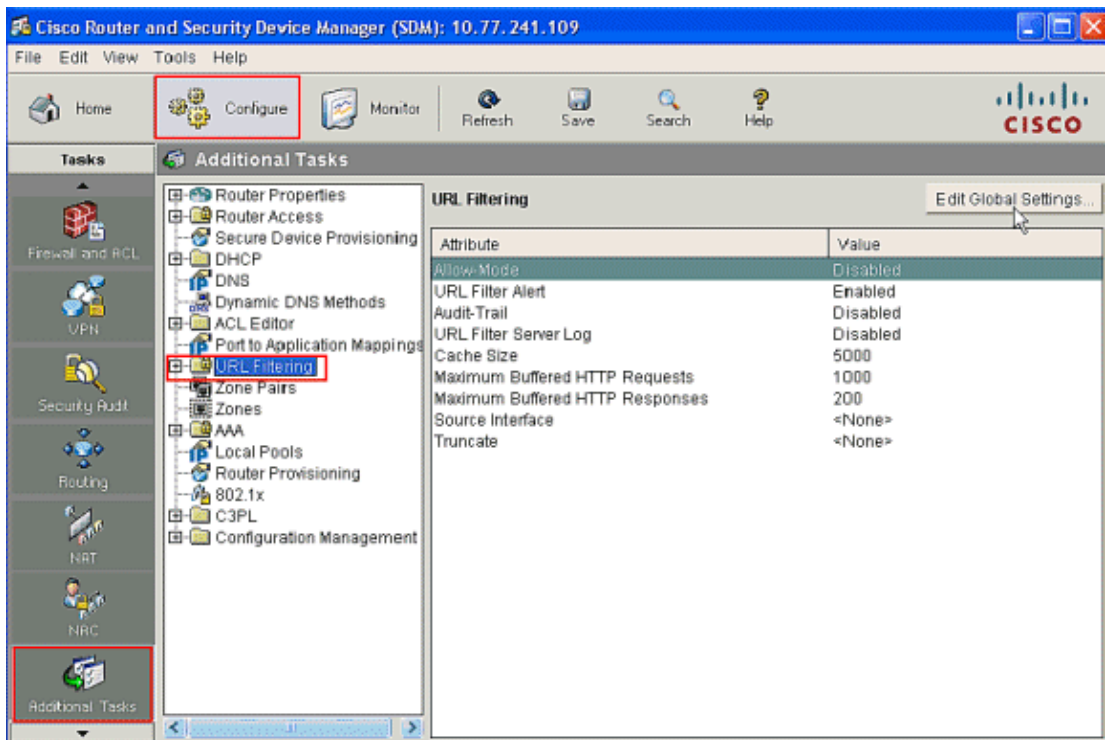
Password: cisco123

Save this password in your password list

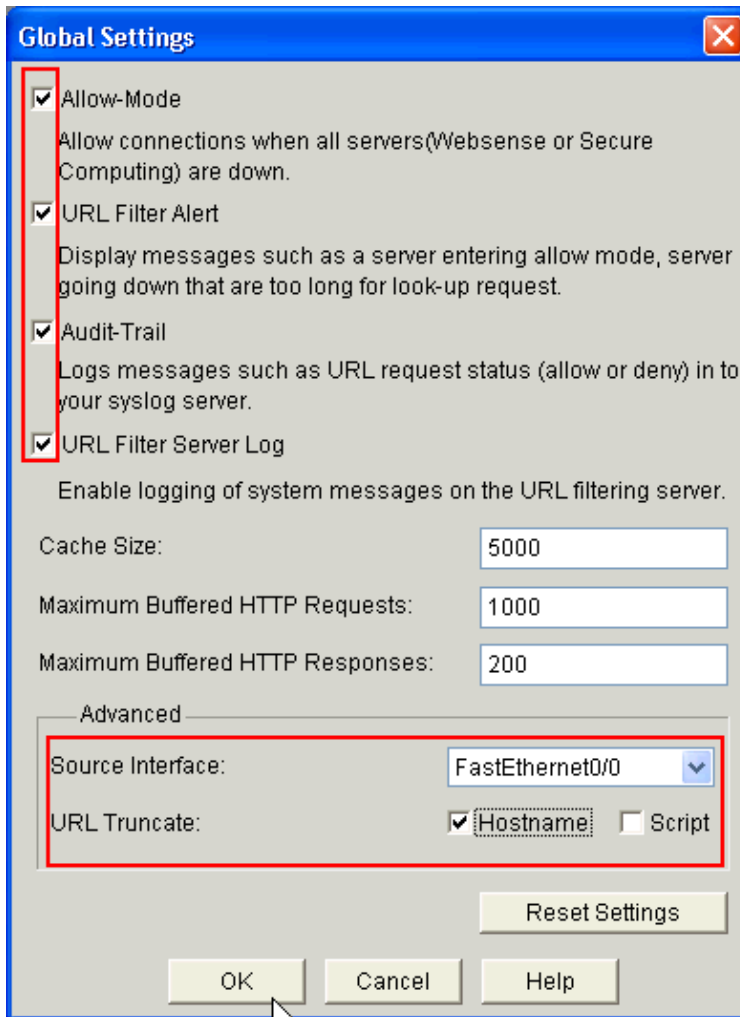
OK Cancel

Authentication scheme: Basic

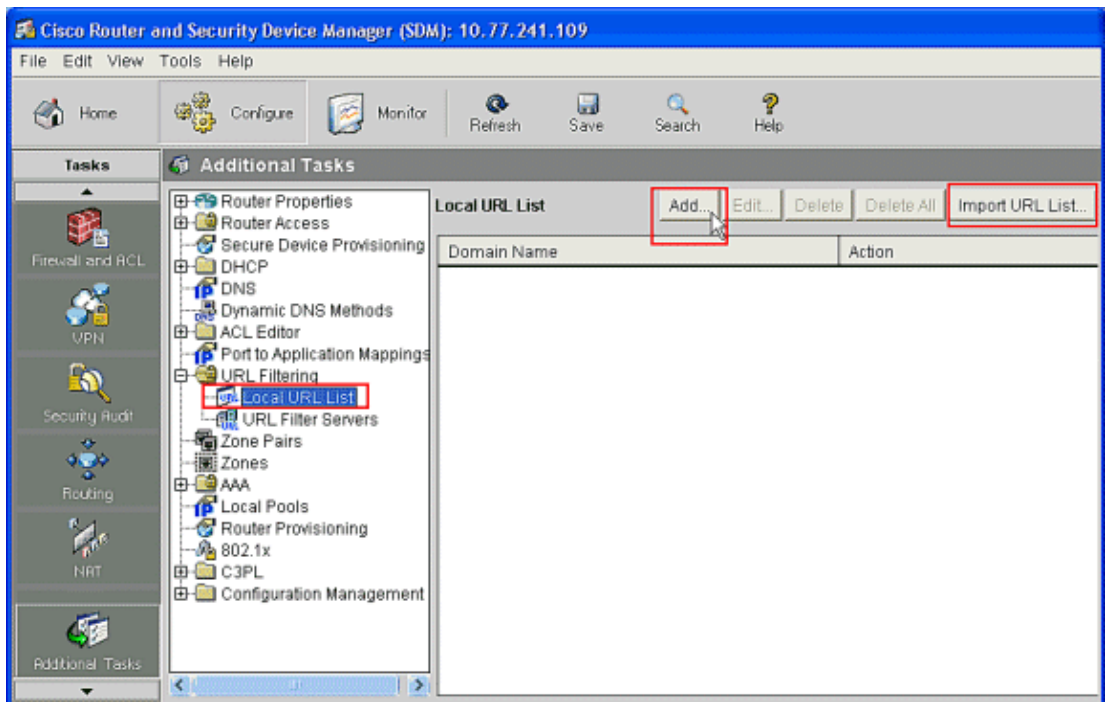
4. Choose **Configuration**→**Additional Tasks** and click **URL Filtering** on the SDM home page. Then click **Edit Global Settings**, as shown here:



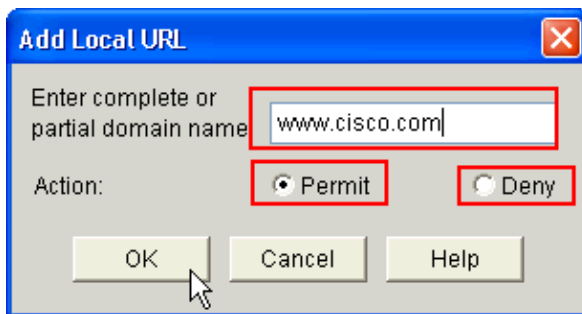
5. In the new window that appears, enable the parameters required for URL filtering, such as **Allow-Mode**, **URL Filter Alert**, **Audit-Trial** and **URL Filtering Server Log**. Check the check boxes next to each parameters as shown. Now provide the **Cache Size** and **HTTP Buffer** information. Also provide the **Source Interface** and **URL Truncate** method under the **Advanced** section as shown to allow the URL filter to truncate long URLs to the server. (Here the Truncation parameter is chosen as **Hostname**.) Now click **OK**.



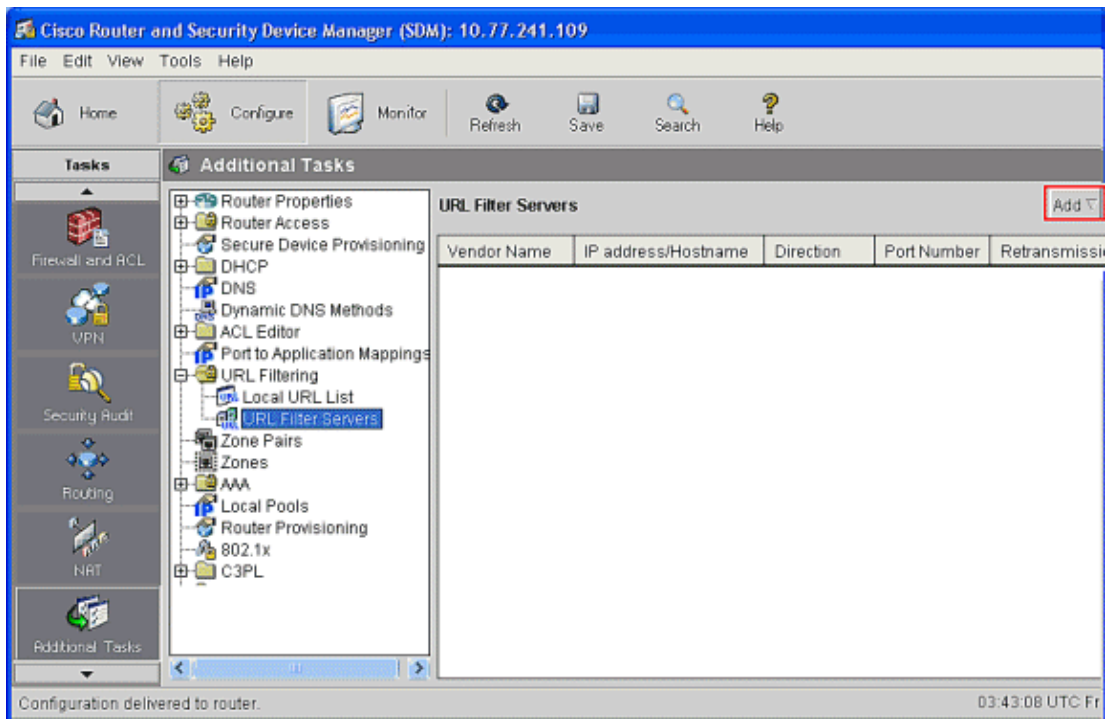
6. Now choose the **Local URL List** option located under the **URL Filtering** tab. Click **Add** in order to add the domain name and configure the firewall to permit or deny the domain name added. You can also choose the option **Import URL List** if the list of URLs needed are present as a file. The choice is yours to choose either the **Add URL** or the **Import URL List** options based on the requirement and availability of the URL list.



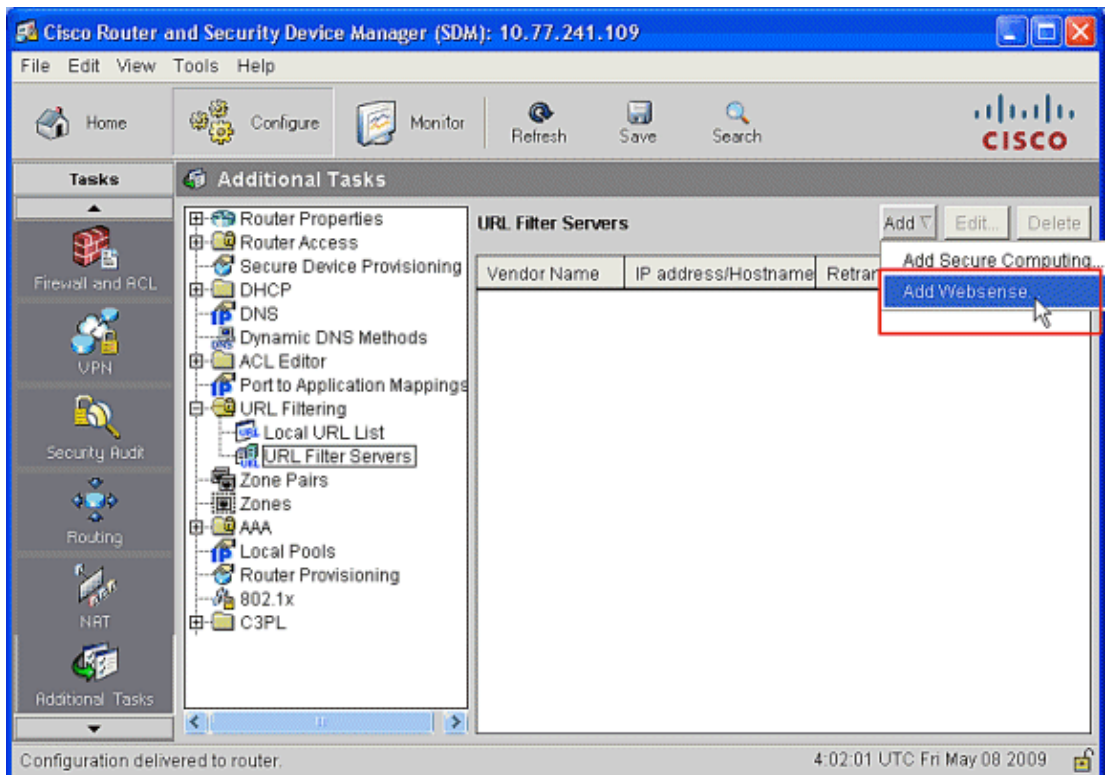
7. In this example, click **Add** to add the URL and configure the IOS Firewall to permit or deny the URL as required. Now a new window entitled **ADD Local URL** opens in which the user has to provide the domain name and decide whether to permit or deny the URL. Click the radio button next to the Permit or Deny option as shown. Here the domain name is **www.cisco.com**, and the user **permits** the **URL www.cisco.com**. In the same way, you can click **Add**, add as many URLs as needed, and configure the firewall to either permit or deny them based on the requirement.



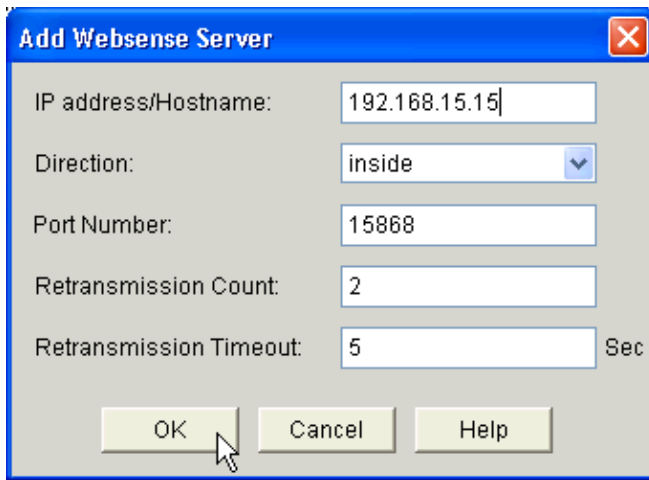
8. Choose the **URL Filter Servers** option located under the **URL Filtering** tab, as shown. Click **Add** in order to add the URL Filtering Server name that performs the URL Filtering function.



9. After you click **Add**, choose the filtering server as **Websense** as shown below since the Websense Filtering Server is used in this example.



10. In this **Add Websense Server** window, provide the **IP address** of the Websense server along with **Direction** in which filter works and **Port Number**, (The default port number for the Websense Server is **15868**). Also provide the **Retransmission Count** and **Retransmission Timeout** values, as shown. Click **OK**, and this completes the **URL Filtering** configuration.



Verify

Use the commands in this section in order to view URL filtering information. You can use these commands in order to verify your configuration.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

- **show ip urlfilter statistics** Shows information and statistics about the filtering server

For example:

```
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
```

- **show ip urlfilter cache** Displays the maximum number of entries that can be cached into the cache table, the number of entries, and the destination IP addresses that are cached into the cache table when you use the show ip urlfilter cache command in privileged EXEC mode
- **show ip urlfilter filter config** Shows the filtering configuration

For example:

```
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
```

Troubleshoot

Error Messages

`%URLF-3-SERVER_DOWN`: Connection to the URL filter server 10.92.0.9 is down. This level three LOG_ERR-type message displays when a configured UFS goes down. When this happens, the firewall will mark the configured server as secondary and try to bring up one of the other secondary servers and mark that server as the primary server. If there is no other server configured, the firewall will enter allow mode and display the `URLF-3-ALLOW_MODE` message.

`%URLF-3-ALLOW_MODE`: Connection to all URL filter servers are down and ALLOW MODE is OFF. This LOG_ERR type message displays when all UFSs are down, and the system enters allow mode.

Note: Whenever the system goes into allow mode (all filter servers are down), a periodic keep-alive timer is triggered that attempts to open a TCP connection and bring up a server.

`%URLF-5-SERVER_UP`: Connection to an URL filter server 10.92.0.9 is made; the system is returning from ALLOW MODE. This LOG_NOTICE-type message displays when the UFSs are detected as up and the system returns from the allow mode.

`%URLF-4-URL_TOO_LONG`: URL too long (more than 3072 bytes), possibly a fake packet? This LOG_WARNING-type message displays when the URL in a look-up request is too long; any URL longer than 3K is dropped.

`%URLF-4-MAX_REQ`: The number of pending request exceeds the maximum limit <1000>. This LOG_WARNING-type message displays when the number of pending requests in the system exceeds the maximum limit, and all further requests are dropped.

Related Information

- [Cisco IOS Firewall](#)
 - [Firewall Websense URL Filtering](#)
 - [Cisco IOS Security Configuration Guide, Release 12.4-Support](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

