URL Filtering

URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on information contained in an URL list. You can maintain a local URL list on the router, and you can use URL lists stored on Websense or Secure Computing URL filter list servers. URL filtering is enabled by configuring an Application Security policy that enables it.

Even if no Application Security policy is configured on the router, you can still maintain a local URL list and an URL filter server list that can be used for URL filtering when a policy is created that enables it.

This chapter contains the following sections:

- URL Filtering Window
- Local URL List
- URL Filter Servers

For more information on URL filtering, go to the following link:

Firewall Websense URL Filtering

To learn how URL filtering policies are used, click URL Filtering Precedence.
URL Filtering Window

This window displays the global settings for URL filtering on the router. You can maintain the local URL list and the URL filter server list in the Additional Tasks screens or in the Application Security windows. The Global settings for URL filtering can only be maintained from this Additional Tasks window. Use the Edit Global Settings button to change these values.

For a description of each setting that appears in this window, Click Edit Global Settings.

See the introductory information in URL Filtering for a description of the URL filtering features that Cisco SDM provides.

Edit Global Settings

Edit URL filtering global settings in this window.

Note

Logging must be enabled for the router to report URL filter alerts, audit trail messages, and system messages pertaining to the URL filter server.

Allow Mode

Check this box to enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list. When the router is in allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.

URL Filter Alert

Check this box to enable the router to log URL filtering alert messages. URL filtering alert messages report events such as an URL filtering server going down, or an HTTP request containing an URL that is too long for a lookup request. This option is disabled by default.
Audit Trail

Check this box to enable the router to maintain an audit trail in the log. The router will record URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.

URL Filter Server Log

Check this box to enable the router to record system messages that pertain to the URL filter server in the log. This option is disabled by default.

Cache Size

You can set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status. The default size of this cache is 5000 bytes. The range is from 0 bytes to 2147483647. The cache is cleared every 12 hours.

Maximum buffered HTTP requests

You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.

Maximum buffered HTTP responses

You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.

General Settings for URL Filtering

Name the URL filter, specify what the router is to do when it detects a match, and configure log and cache size parameters. You can also specify a source interface if you do not want the URL filtering parameter map to apply to all router interfaces.
URL Filter Name

Enter a name that will convey how this URL filter is configured or used. For example if you specify a source interface of FastEthernet 1, you might enter the name fa1-parmap. If the filter uses a Websense URL filter server at IP address 192.128.54.23, you might enter websense23-parmap as the name.

Allow Mode

Check this box to enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list. When the router is in allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.

URL Filter Alert

Check this box to enable the router to log URL filtering alert messages. URL filtering alert messages report events such as an URL filtering server going down, or an HTTP request containing an URL that is too long for a lookup request. This option is disabled by default.

Audit Trail

Check this box to enable the router to maintain an audit trail in the log. The router will record URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.

URL Filter Server Log

Check this box to enable the router to record system messages that pertain to the URL filter server in the log. This option is disabled by default.

Cache Size

You can set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status. The default size of this cache is 5000 bytes. The range is from 0 bytes to 2147483647. The cache is cleared every 12 hours.
Maximum Buffered HTTP Requests

You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.

Maximum Buffered HTTP Responses

You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.

Advanced

The Advanced box allows you to choose the source interface. Choose the interface from the Source Interface list.

Local URL List

If the Cisco IOS image on the router supports URL filtering but does not support Zone-based Policy Firewall (ZPF), you can maintain one local URL list on the router. This list is used by all Application Security policies in which URL filtering is enabled. Cisco IOS images of release 12.4(9)T and later support all the ZPF features that SDM supports. In a ZPF configuration, a local URL list can be created for each URL filtering parameter map.

You can use Cisco SDM to create list entries and you can import entries from a list stored on your PC. When a local URL list is used in combination with URL filter servers, local entries are used first. See URL Filtering Precedence for more information.

Maintaining the Local URL List

You can use Cisco SDM to maintain a local URL list by adding and deleting entries one-by-one, and by importing an URL list from your PC and specifying what you want Cisco SDM to do with each entry. Use the Add and the Delete buttons to manage specific entries in the list on the router, and click the Import URL List button to import an URL list from your PC.
If an entry is deleted from the local list and the router is configured to use URL filtering servers, entries that match ones that you are deleting from the local list may exist on those servers.

Use the **Delete All** button to delete all entries on the router. If no local list is configured on the router, the router must rely on the configured URL filter servers. If you want to retrieve the URL list you are deleting at a later time, use the **Export URL List** button to save the URL list to your PC before deleting all the entries. When you save an URL list to your PC the list is given a .CSV extension.

**Importing URL Lists from your PC**

Click the **Import URL List** button to import an URL list from your PC to the router. The URL list that you select must have a .txt or .CSV extension. After you select the list on your PC, Cisco SDM displays a dialog that allows you to specify what you want to do with each entry in the list. See **Import URL List** for more information.

**Add or Edit Local URL**

Use this window to add or edit an URL entry for the local URL list on the router. Enter a full domain name or a partial domain name and choose whether to **Permit** or **Deny** requests for this URL.

If you enter a full domain name, such as www.somedomain.com, all requests that include that domain name, such as www.somedomain.com/news or www.somedomain.com/index will be permitted or denied based on the setting you choose in this dialog. These requests will not be sent to the URL filtering servers that the router is configured to use.

If you enter a partial domain name, such as .somedomain.com, all requests that end with that string, such as www.somedomain.com/products or wwwin/somedomain.com/eng will be permitted denied based on the setting you choose in this dialog. These requests will not be sent to the URL filtering servers that the router is configured to use.
Import URL List

This dialog allows you to examine the URL list you are importing from your PC to the router and specify what you want to do with each entry. If an URL entry in this dialog is not already present on the router, you can add it to the list on the router by clicking Append. If an URL entry is already present on the router but you want to replace it with the entry in this dialog, click Replace.

All boxes in the Import column are checked by default. If there are entries that you do not want to be sent to the router, uncheck the box next to those entries. If you want to remove the checks from all the boxes, click Unselect All. Clicking Select All places checkmarks in all the boxes.

Append adds any checked entry to the URL list that is not already present in the list. If you attempt to add an entry that is already in the URL list, it will not be added even if the action specified for the domain in the entry is different from the action that is already in the list.

Use the Replace button to specify a different action for an entry that is already in the router’s URL list. If the entry you checked is not already in the router’s list, Replace has no effect.

URL Filter Servers

The router can send HTTP requests to URL filtering servers that are capable of storing much larger URL lists than the router can store. If the router is configured with an URL filter server list, the router sends requests that do not match entries in the local list to the URL filter server it has a connection to, and permits or denies the request based on the response it receives from the server. When the server that the router is connected to goes down, the router contacts the next server in the list until it establishes a connection.

Lists on URL filter servers can be used along with local URL lists. Click URL Filtering Precedence to learn how the router uses both of these resources.

Click Add, and choose either Secure Computing or Websense to specify the type of server that you are adding.

Note: Cisco IOS software can only use one type of URL filtering server, and does not allow you to add a server to the list if it is of a different type. For example, if an URL filter server list containing Websense servers is configured on the router, you...
will receive an error message if you attempt to add an Secure Computing server to the list. If the URL filter server list currently contains one type of server and you want to change to the other type, you must delete all the server entries in the list before adding an entry of the new type.

This window displays the configuration for each URL filter server in the list. See Add or Edit an URL Filter Server for a description of each configuration value.

Add or Edit an URL Filter Server

Specify the information for the Websense or Secure Computing URL filter server.

IP Address/Hostname

Enter the IP address or the hostname for the server. If you enter a hostname, the router must have a connection to a DNS server in order to resolve the hostname to an IP address.

Direction

Choose **Inside** if the URL filter server is part of the inside network. This is usually one of the networks that the router LAN interfaces connect to. Choose **Outside** if the router is in the outside network. This is usually one of the networks that the router WAN interfaces connect to. The default value is **Inside**.

Port Number

Automatically contains the default port number for the type of URL filter server you are adding. If you are adding a Websense server, the default value is 15868. If you are adding an Secure Computing server, the default value is 4005. Change this number to the number of the port that the server listens on if that number is different from the default. This field accepts values from 1 to 65535.

Retransmission Count

Optional field. Enter the number of times that you want the router to attempt to retransmit the request if no response arrives from the server. The default value is 2 times. This field accepts values from 1 to 10.
Chapter 35  URL Filtering

Retransmission Timeout

Optional field. Enter the number of seconds that the router should wait for a response from the server before retransmitting the request. The default value is 5 seconds.

URL Filtering Precedence

URL filtering must be enabled by going to Configure > Firewall and ACL > Application Security > URL Filtering and clicking Enable URL filtering. This can only be done when an Application security policy is configured on the router.

When URL filtering is enabled, the router determines how to handle an HTTP request as follows:

- If the URL in the request matches an entry in the local URL list on the router, the router permits or denies the request based on that entry.
- If the URL in the request does not match any entry in the local URL list, the router passes the HTTP request to the URL filtering server to which it has a connection. It permits or denies the request based on the information that the server returns.
- If allow mode is disabled, and the router cannot establish a connection with an URL filter server, the router denies the request. Allow mode is disabled by default.
- If allow mode is enabled and the router cannot establish a connection with an URL filter server, the router permits the request. Allow mode can be enabled in the Edit Global Settings dialog.

Only one URL list and one URL filter server list can be configured on the router. All configured Application Security policies use the same URL list and URL filter server list. These lists can be maintained in the Application Security windows, or by going to Additional Tasks > URL Filtering. If all Application Security policies are deleted, the URL list and URL filter server list can still be maintained in the Additional Tasks windows. However, the router does not perform URL filtering unless URL filtering is enabled in an Application Security policy.