



CHAPTER 27

Configuring Filter Rules

This chapter describes ways to filter web traffic to reduce security risks or prevent inappropriate use. This chapter includes the following sections:

- [URL Filtering, page 27-1](#)
- [Filter Rules, page 27-5](#)

URL Filtering

You can apply filtering to connection requests originating from a more secure network to a less secure network. Although you can use ACLs to prevent outbound access to specific content servers, managing usage this way is difficult because of the size and dynamic nature of the Internet. You can simplify configuration and improve security appliance performance by using a separate server running one of the following Internet filtering products:

- Websense Enterprise for filtering HTTP, HTTPS, and FTP.
- Secure Computing SmartFilter for filtering HTTP only. (Although some versions of Sentian support HTTPS, the security appliance only supports filtering HTTP with Sentian.)

Although security appliance performance is less affected when using an external server, users may notice longer access times to websites or FTP servers when the filtering server is remote from the security appliance.

When filtering is enabled and a request for content is directed through the security appliance, the request is sent to the content server and to the filtering server at the same time. If the filtering server allows the connection, the security appliance forwards the response from the content server to the originating client. If the filtering server denies the connection, the security appliance drops the response and sends a message or return code indicating that the connection was not successful.

If user authentication is enabled on the security appliance, then the security appliance also sends the user name to the filtering server. The filtering server can use user-specific filtering settings or provide enhanced reporting regarding usage.

This section includes the following topics:

- [Configuring URL Filtering, page 27-2](#)
- [URL Filtering Servers, page 27-2](#)
- [Advanced URL Filtering, page 27-4](#)

Configuring URL Filtering

To enable filtering with an external filtering server, perform the following steps:

-
- Step 1** Choose **Configuration > Firewall > URL Filter Servers** to specify an external filtering server. See [URL Filtering Servers, page 27-2](#).
 - Step 2** (Optional) Buffer responses from the content server. See [Advanced URL Filtering, page 27-4](#).
 - Step 3** (Optional) Cache content server addresses to improve performance. See [Advanced URL Filtering, page 27-4](#).
 - Step 4** Choose **Configuration > Firewall > Filter Rules** to configure filter rules. See [Filter Rules, page 27-5](#).
 - Step 5** Configure the external filtering server. For more information see the following websites:
 - <http://www.websense.com>
 - <http://www.securecomputing.com>
-

URL Filtering Servers

The URL Filtering Servers pane lets you specify the external filter server to use. You can identify up to four of the same type of filtering servers per context. In single mode a maximum of 16 of the same type of filtering servers are allowed. The security appliance uses the servers in order until a server responds. You can only configure a single type of server (Websense or Secure Computing SmartFilter) in your configuration.

**Note**

You must add the filtering server before you can configure filtering for HTTP, HTTPS, or FTP filtering rules.

Fields

The URL Filtering Server Type area includes the following fields:

- Websense—Enables the Websense URL filtering servers.
- Secure Computing SmartFilter—Enables the Secure Computing SmartFilter URL filtering server.
- Secure Computing SmartFilter Port—Specifies the Secure Computing SmartFilter port. The default is 4005.

The URL Filtering Servers area includes the following fields:

- Interface—Displays the interface connected to the filtering server.
- IP Address—Displays the IP address of the filtering server.
- Timeout—Displays the number of seconds after which the request to the filtering server times out.
- Protocol—Displays the protocol used to communicate with the filtering server.
- TCP Connections—Displays the maximum number of TCP connections allowed for communicating with the URL filtering server.
- Add—Adds a new filtering server, depending on whether you have selected Websense or Secure Computing SmartFilter. See the following topics for more information:

- [Add/Edit Parameters for Websense URL Filtering, page 27-3](#)
- [Add/Edit Parameters for Secure Computing SmartFilter URL Filtering, page 27-4](#)
- Insert Before—Adds a new filtering server in a higher priority position than the currently selected server.
- Insert After—Adds a new filtering server in a lower priority position than the currently selected server.
- Edit—Lets you modify parameters for the selected filtering server.
- Delete—Deletes the selected filtering server.

You can perform the following actions in this pane:

- Advanced—Displays advanced filtering parameters, including buffering caching, and long URL support.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

[Advanced URL Filtering, page 27-4](#)

[Filter Rules, page 27-5](#)

Add/Edit Parameters for Websense URL Filtering

- Interface—Specifies the interface on which the URL filtering server is connected.
- IP Address—Specifies the IP address of the URL filtering server.
- Timeout—Specifies the number of seconds after which the request to the filtering server times out.
- Protocol area
 - TCP 1—Uses TCP Version 1 for communicating with the Websense URL filtering server.
 - TCP 4—Uses TCP Version 4 for communicating with the Websense URL filtering server.
 - UDP 4—Uses UDP Version 4 for communicating with the Websense URL filtering server.
- TCP Connections—Specifies the maximum number of TCP connections allowed for communicating with the URL filtering server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Parameters for Secure Computing SmartFilter URL Filtering

- Interface—Specifies the interface on which the URL filtering server is connected.
- IP Address—Specifies the IP address of the URL filtering server.
- Timeout—Specifies the number of seconds after which the request to the filtering server times out.
- Protocol area
 - TCP—Uses TCP for communicating with the Secure Computing SmartFilter URL filtering server.
 - UDP—Uses UDP for communicating with the Secure Computing SmartFilter URL filtering server.

TCP Connections—Specifies the maximum number of TCP connections allowed for communicating with the URL filtering server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Advanced URL Filtering

Fields

URL Cache Size area

After a user accesses a site, the filtering server can allow the security appliance to cache the server address for a certain amount of time, as long as every site hosted at the address is in a category that is permitted at all times. Then, when the user accesses the server again, or if another user accesses the server, the security appliance does not need to consult the filtering server again.



Note Requests for cached IP addresses are not passed to the filtering server and are not logged. As a result, this activity does not appear in any reports.

- Enable caching based on—Enables caching based on the specified criteria.
 - Destination Address—Caches entries based on the URL destination address. Choose this mode if all users share the same URL filtering policy on the Websense server.

- Source/Destination Address—Caches entries based on both the source address initiating the URL request as well as the URL destination address. Choose this mode if users do not share the same URL filtering policy on the server.
- Cache size—Specifies the size of the cache.

URL Buffer Size area

When a user issues a request to connect to a content server, the security appliance sends the request to the content server and to the filtering server at the same time. If the filtering server does not respond before the content server, the server response is dropped. This delays the web server response from the point of view of the web client because the client must reissue the request.

By enabling the HTTP response buffer, replies from web content servers are buffered and the responses are forwarded to the requesting client if the filtering server allows the connection. This prevents the delay that might otherwise occur.

- Enable buffering—Enables request buffering.
 - Number of 1550-byte buffers—Specifies the number of 1550-byte buffers. Valid values are from 1 to 128.
- Long URL Support area

By default, the security appliance considers an HTTP URL to be a long URL if it is greater than 1159 characters. For Websense servers, you can increase the maximum length allowed.

- Use Long URL—Enables long URLs for Websense filtering servers.
- Maximum Long URL Size—Specifies the maximum URL length allowed, up to a maximum of 4 KB.
- Memory Allocated for Long URL—Specifies the memory allocated for long URLs.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Filter Rules

The Filter Rules pane displays configured filter rules and provides options for adding new filter rules or modifying existing rules. A filter rule specifies the type of filtering to apply and the kind of traffic to which it should be applied.



Note

Before you can add an HTTP, HTTPS, or FTP filter rule, you must enable a URL filtering server. To enable a URL filtering server, use the Configuration > Firewall > URL Filtering Servers pane. For more information, see [URL Filtering, page 27-1](#).

Benefits

The Filter Rules pane provides information about the filter rules that are currently configured on the security appliance. It also provides buttons that you can use to add or modify the filter rules and to increase or decrease the amount of detail shown in the pane.

Filtering allows greater control over any traffic that your security policy allows to pass through the security appliance. Instead of blocking access altogether, you can remove specific undesirable objects from HTTP traffic, such as ActiveX objects or Java applets, that may pose a security threat in certain situations. You can also use URL filtering to direct specific traffic to an external filtering server, such as Secure Computing SmartFilter or Websense. These servers can block traffic to specific sites or types of sites, as specified by your security policy.

Because URL filtering is CPU-intensive, using an external filtering server ensures that the throughput of other traffic is not affected. However, depending on the speed of your network and the capacity of your URL filtering server, the time required for the initial connection may be noticeably slower for filtered traffic.

Fields

- No—Numeric identifier of the rule. Rules are applied in numeric order.
- Source—Source host or network to which the filtering action applies.
- Destination—Destination host or network to which the filtering action applies.
- Service—Identifies the protocol or service to which the filtering action applies.
- Action—Type of filtering action to apply.
- Options—Indicates the options that have been enabled for the specific action.
- Add—Displays the types of filter rules you can add. Clicking the rule type opens the Add Filter Rule dialog box for the specified filter rule type.
 - Add Filter ActiveX Rule
 - Add Filter Java Rule
 - Add Filter HTTP Rule
 - Add Filter HTTPS Rule
 - Add Filter FTP Rule
- Edit—Displays the Edit Filter Rule dialog box for editing the selected filtering rule.
- Delete—Deletes the selected filtering rule.
- Cut—Lets you to cut a filter rule and place it elsewhere.
- Copy—Lets you copy a filter rule.
- Paste—Lets you paste a filter rule elsewhere.
- Find—Lets you search for a filter rule. Clicking this button brings up an extended toolbar. See [Filtering the Rule Table, page 27-9](#) for more information.
- Rule Diagram—Toggles the display of the Rule Diagram.
- Packet Trace—Launches the Packet Tracer utility.
- Use the Addresses tab to choose the source of the filter rule that you are choosing.
 - Type—Lets you choose a source from the drop-down list, selecting from All, IP Address Objects, IP Names, or Network Object groups.
 - Name—Lists the name(s) of the filter rule.

- Add—Lets you add a filter rule.
- Edit—Lets you edit a filter rule.
- Delete—Lets you delete a filter rule.
- Find—Lets you find a filter rule.
- Use the Services tab to choose a predefined filter rule.
 - Type—Lets you choose a source from the drop-down list, selecting from All, IP Address Objects, IP Names, or Network Object groups.
 - Name—Lists the name(s) of the filter rule.
 - Edit—Lets you edit a filter rule.
 - Delete—Lets you delete a filter rule.
 - Find—Lets you find a filter rule.
- Use the Time Ranges to choose a time range for the filter rule.
 - Add—Add—Lets you add a time range for the filter rule.
 - Edit—Lets you edit a time range for the filter rule.
 - Delete—Lets you delete a time range for a filter rule.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	—

Add/Edit Filter Rule

Use the Add Filter Rule dialog box to specify the interface on which the rule applies, to identify the traffic to which it applies, or to configure a specific type of filtering action.



Note

Before you can add an HTTP, HTTPS, or FTP filter rule, you must enable a URL filtering server. To enable a URL filtering server, use the Features > Configuration > Properties > URL Filtering window. For more information, see [URL Filtering](#).

Fields

- Action—Provides the following drop-down list of different filtering actions to apply (the actions displayed depend upon the type of filter rule being created or edited):
 - Filter ActiveX
 - Do not filter ActiveX
 - Filter Java Applet
 - Do not filter Java Applet

- Filter HTTP (URL)
- Do not filter HTTP (URL)
- Filter HTTPS
- Do not filter HTTPS
- Filter FTP
- Do not filter FTP
- Source—Enter the source of the traffic to which the filtering action applies. You can enter the source in one of the following ways:
 - any—Enter “any” (without quotation marks) to indicate any source address.
 - *name*—Enter a hostname.
 - *address/mask*—Enter an IP address and optional network mask. You can express the netmask in CIDR or dotted decimal notation. For example, you can enter 10.1.1.0/24 or 10.1.1.0/255.255.255.0.
 - ...—Opens the Browse Source dialog box. You can choose a host or address from the drop-down list.
- Destination—Identifies the destination of the traffic to which the filtering action applies. You can enter the destination in one of the following ways:
 - any—Enter “any” (without quotation marks) to indicate any destination address.
 - *name*—Enter a hostname.
 - *address/mask*—Enter an IP address and optional network mask. You can express the netmask in CIDR or dotted decimal notation. For example, you can enter 10.1.1.0/24 or 10.1.1.0/255.255.255.0.
 - ...—Opens the Browse Destination dialog box. You can choose a host or address from the drop-down list.
- Service —Identifies the service of the traffic to which the filtering action applies. You can enter the destination in one of the following ways:
 - *tcp/port*—The port number can be from 1 to 65535. Additionally, you can use the following modifiers with the TCP service:
 - !—Not equal to. For example, !=tcp/443
 - <—Less than. For example, <tcp/2000.
 - >—Great than. For example, >tcp/2000.
 - —Range. For example, tcp/2000-3000.
 - *name*—Enter a well-known service name, such as http or ftp.
 - ...—Opens the Browse Service dialog box. You can choose a service from the drop-down list.
- HTTP Options—This area appears only for HTTP filter rules.
 - When URL exceeds maximum permitted size—Choose the action to take when the URL exceeds the specified size. You can choose to truncate the URL or block the traffic.
 - Allow outbound traffic if URL server is not available—When enabled, if the URL filtering server is down or connectivity is interrupted to the security appliance, users will be able to connect without URL filtering being performed. If this is disabled, users will not be able to connect to Internet websites when the URL server is unavailable.

- Block users from connecting to an HTTP proxy server—Prevent HTTP requests made through a proxy server.
- **Truncate CGI parameters from URL sent to URL server**—The security appliance forwards only the CGI script location and the script name, without any parameters, to the filtering server.
- **HTTPS Options**—This area appears only when you choose the **Filter HTTPS** option from the drop-down list.
 - **Allow outbound traffic if URL server is not available**—When enabled, if the URL filtering server is down or connectivity is interrupted to the security appliance, users will be able to connect without URL filtering being performed. If this is disabled, users will not be able to connect to Internet websites when the URL server is unavailable.
- **FTP Options**—This area appears only when you choose the **Filter FTP** option from the drop-down list.
 - **Allow outbound traffic if URL server is not available**—When enabled, if the URL filtering server is down or connectivity is interrupted to the security appliance, users will be able to connect without URL filtering being performed. If this is disabled, users will not be able to connect to Internet websites when the URL server is unavailable.
 - **Block interactive FTP sessions (block if absolute FTP path is not provided)**—When enabled, FTP requests are dropped if they use a relative pathname to the FTP directory.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	—

Filtering the Rule Table

It can be difficult to find a specific rule if your rule table includes a lot of entries. You can apply a filter to the rule table to show only the rules specified by the filter. To filter the rule table, perform the following steps:

-
- Step 1** Click **Find** on the toolbar. The Filter toolbar appears.
- Step 2** Choose the type of filter from the filter drop-down list:
- **Source**—Displays rules based on the specified source address or hostname.
 - **Destination**—Displays rules based on the specified destination address or hostname.
 - **Source or Destination**—Displays rules based on the specified source or destination address or hostname.
 - **Service**—Displays rules based on the specified service.
 - **Rule Type**—Displays rules based on the specified rule type.
 - **Query**—Displays rules based on a complex query comprise of source, destination, service, and rule type information.

- Step 3** For Source, Destination, Source or Destination, and Service filters, perform the following steps:
- a. Choose the match criteria from the drop-down list. Choose “is” (without the quotes) for exact string matches or choose “contains” for partial string matches.
 - b. Enter the string to match using one of the following methods:
 - Type the source, destination, or service name into the condition field.
 - Click ... to open a browse dialog from which you can choose existing services, IP addresses, or hostnames.
- Step 4** For Rule Type filter, choose the rule type from the list.
- Step 5** For Query filters, click **Define Query** and configure the complex query. For more information about configuring the complex query, see [Browse Source/Destination/Service, page 27-11](#).
- Step 6** To apply the filter to the rule table, click **Filter**.
- Step 7** To clear the filter from the rule table and display all rule entries, click **Clear**.
-

Define Query

The Define Query dialog box lets you define a rule table filter based on multiple criteria, such as source, destination, service, and rule type.

Once you create the query and click OK, the filter is immediately applied to the rule table. You can clear the filter by clicking **Clear**.

Fields

- Source—IP address or hostname of the source. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them by commas (,).
- Destination—IP address or hostname of the destination. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them by commas (,).
- Source or Destination—IP address or hostname of the source or destination. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them by commas (,).
- Service—The protocol/port or name of a service. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify multiple services by separating them by commas (,).
- Rule Type—Choose the rule type from the drop-down list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

[Filtering the Rule Table, page 27-9](#)

Browse Source/Destination/Service

The Browse Source/Destination/Service dialog box lets you choose from existing IP address, name, or service objects.

Fields

- Add—Click to add a new IP address, name, or service object.
- Edit—Click to edit an existing IP address, name, or service object.
- Filter/Clear—Enter a string by which to filter the information shown in the dialog box. Click Filter to apply the filter to the information shown in the dialog box. Click Clear to remove the filter and display all objects.
- Type—Organizes the objects shown into types, such as IP Names, IP Address Objects, and so on.
- Name—The name of the object. For services, it is the service name. For IP Address objects, it is the IP address, for IP name objects, it is the hostname.
- IP Address—The IP address of the address object.
- Netmask—The network mask of the address object.
- Protocol—The network protocol used by the service (such as tcp, udp, or icmp).
- Source Ports—The source port used by the service.
- Destination Ports—The destination port used by the service.
- ICMP Type—The ICMP type (for example 9, which is a router advertisement).
- Description (optional)—Specifies a description for the object.
- Source/Destination/Service button—Click this to add the address or service object to the filter rule or query.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information[Filter Rules, page 27-5](#)[URL Filtering, page 27-1](#)