



CHAPTER 20

Configuring Filter Rules

This section contains the following topics:

- [URL Filtering, page 20-1](#)
- [Filter Rules, page 20-5](#)

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.

General Procedure

The following summarizes the procedure for enabling filtering with an external filtering server.

- Step 1** Identify the filtering server.
- Step 2** (Optional) Buffer responses from the content server (optional).
- Step 3** (Optional) Cache content server addresses to improve performance (optional).
- Step 4** Configure filtering rules. See [Filter Rules](#).

Step 5 Configure the external filtering server. For more information refer to the following websites:

- <http://www.websense.com>
- <http://www.securecomputing.com>

You can identify up to four filtering servers per context. In single mode a maximum of 16 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

- **URL Filtering Server** area
 - **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.
 - **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**.
 - **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.
- **Apply**—Applies the changes to the running configuration.
- **Reset**—Removes any changes that have not been applied.
- **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

[Filter Rules](#)

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. Select 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. Select 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.
- **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** window 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 **Features > Configuration > Properties > URL Filtering** screen. For more information see [URL Filtering](#).

Benefits

The **Filter Rules** window 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 window.

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 **Add Filter Rule** dialog box for adding a new filtering rule.
- **Edit**—Displays the **Edit Filter Rule** dialog box for editing the selected filtering rule.
- **Delete**—Deletes the selected filtering rule.
- **MoveUp—Moves the filter rule up.**
- **MoveDown**—Moves the filter rule down.
- **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 on this button brings up an extended tool bar.
 - **Filter**—Lets you search by source, destination, source, action, or rule query, using the drop-down menu.
 - **...**—Lets you select the source of the filter, and brings up the Select Source dialog box.
 - **Filter**—Lets you input a filter.
 - **Clear**—Lets you clear a filter rule.
 - **Rule Query**—Lets you devise a query to search for a rule.
- Use the **Addresses** tab to select the source of the filter rule that you are choosing.
 - **Type**—Lets you select a source from the drop-down menu, selecting from All, Network Objects 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 select a predefined filter rule.
 - **Type**—Lets you select a source from the drop-down menu, selecting from All, Network Objects 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 select 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		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select Source

Use the Select Source dialog box to select the source of the filter rule that you are closing.

Fields

- Type—Lets you select a source from the drop-down menu, selecting from All, Network Objects, or Network Object Groups.
- Name—Lists the name(s) of the filter rule.
- IP Address—Lists the IP address of the filter rule(s).
- Netmask—Lists the netmask of the filter rule(s).
- Description (optional)—Lists descriptions for the filter rules.

Modes

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

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

Rule Query

Fields

- Name—Lets you enter the name of the filter rule for the query.
- Description (optional)—Lets you enter a description of the filter rule for the query.

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 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** screen. For more information see [URL Filtering](#).

Fields

- **Action**—Provides the following drop-down list of different filtering actions to apply:
 - 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

The **Rule Flow Diagram and the Filtering Option** area changes according to which filtering action you select.

- **Source** area
 - **IP Address**—Use the IP address to identify the traffic to which the filtering action applies.
 - ...—Opens the Browse Source Address dialog box.
 - **Netmask**—Specifies the Subnet mask used to identify the traffic to which the filtering action applies when **IP Address** is selected.
- **Destination** area
 - **IP Address**—Identifies the traffic to which the filtering action applies.
 - **Netmask**—Specifies the Subnet mask used to identify the traffic to which the filtering action applies when **IP Address** is selected.
- **Rule Flow Diagram** area —Provides a graphic representation of how a specific filtering action is applied to traffic that is forwarded through the security appliance.
- **ActiveX Filtering Option** area—This area appears only when you select the **Filter ActiveX** option from the drop-down list.
 - **ActiveX Filtering Option**—When you select the Filter ActiveX option from the drop-down list, this field appears and lets you specify the TCP/UDP port on which the security appliance listens for traffic to which the filtering action applies.
- **Java Filtering Option**—This area appears only when you select the **Filter Java** option from the drop-down list.

- **Java Filtering Option**—When you select the Filter Java option from the drop-down list, this field appears and lets you specify the TCP/UDP port on which the security appliance listens for traffic to which the filtering action applies.
- **HTTP Filtering Option**—This area appears only when you select the **Filter HTTP** option from the drop-down list.
 - **Filter HTTP on port(s)**—Specify the TCP/UDP port on which the security appliance listens for traffic to which the filtering action applies.
 - **Block connections to proxy server**—Prevent HTTP requests made through a proxy server.
 - **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.
 - **Truncate CGI requests by removing the CGI parameters**—The security appliance forwards only the CGI script location and the script name, without any parameters, to the filtering server.
- **HTTPS Filtering Option**—This area appears only when you select the **Filter HTTPS** option from the drop-down list.
 - **Filter HTTPS on port(s)**—specify the TCP/UDP port on which the security appliance listens for traffic to which the filtering action applies.
 - **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 Filtering Option**—This area appears only when you select the **Filter FTP** option from the drop-down list.
 - **Filter FTP on port(s)**—Specifies the TCP/UDP port on which the security appliance listens for traffic to which the filtering action applies.
 - **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 outbound traffic if absolute FTP path is not provided**—When enabled, FTP requests are dropped if they use a relative path name to the FTP directory.

Modes

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

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

Browse Source/Destination Address

Fields

- **Type**—Lets you select from one of the following types of sources: Network Objects or Network Object Groups.
- **Name**—Specifies the name used to identify the traffic to which the filtering action applies when the Name button is selected.
- **IP Address**—Specifies the IP address used to identify the traffic to which the filtering action applies.
- **Netmask**—Specifies the Subnet mask used to identify the traffic to which the filtering action applies when **IP Address** is selected.
- **Description (optional)**—Specifies a description for the filter.

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](#)

[URL Filtering](#)