Configuring Filtering Services

This chapter describes how to use filtering services to provide greater control over traffic passing through the ASA and includes the following sections:

Information About Web Traffic Filtering

You can use web traffic filtering in two distinct ways:

- Filtering ActiveX objects or Java applets
- Filtering with an external filtering server

Instead of blocking access altogether, you can remove specific undesirable objects from web traffic, such as ActiveX objects or Java applets, that may pose a security threat in certain situations.

You can use web traffic filtering to direct specific traffic to an external filtering server, such an Secure Computing SmartFilter (formerly N2H2) or the Websense filtering server. You can enable long URL, HTTPS, and FTP filtering using either Websense or Secure Computing SmartFilter for web traffic filtering. Filtering servers can block traffic to specific sites or types of sites, as specified by the security policy.

Note URL caching will only work if the version of the URL server software from the URL server vendor supports it.

Because web traffic 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 web traffic filtering server, the time required for the initial connection may be noticeably slower when filtering traffic with an external filtering server.

(CLI) Configuring ActiveX Filtering

This section includes the following topics:

Information About ActiveX Filtering

ActiveX objects may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can disable ActiveX objects with ActiveX filtering.

ActiveX controls, formerly known as OLE or OCX controls, are components that you can insert in a web page or another application. These controls include custom forms, calendars, or any of the extensive third-party forms for gathering or displaying information. As a technology, ActiveX creates many potential problems for network clients including causing workstations to fail, introducing network security problems, or being used to attack servers.

The **filter activex** command blocks the HTML **object** commands by commenting them out within the HTML web page. ActiveX filtering of HTML files is performed by selectively replacing the <APPLET> and </APPLET>, and <OBJECT CLASSID> and </OBJECT> tags with comments. Filtering of nested tags is supported by converting top-level tags to comments.

Caution The **filter activex** command also blocks any Java applets, image files, or multimedia objects that are embedded in object tags.

If the <object> or </object> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the ASA cannot block the tag.

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command or for clientless SSL VPN traffic.

Licensing Requirements for ActiveX Filtering

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations for ActiveX Filtering

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Does not support IPv6.

Configuring ActiveX Filtering

To remove ActiveX objects in HTTP traffic that is passing through the ASA, enter the following command:

Command	Purpose
filter activex *port[-port] local_ip local_mask foreign_ip foreign_mask* **Example:** `ciscoasa# filter activex 80 0 0 0 0`	Removes ActiveX objects. To use this command, replace *port[-port]* with the TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The **http** or **url** literal can be used for port 80. You can specify a range of ports by using a hyphen between the starting port number and the ending port number. The local IP address and mask identify one or more internal hosts that are the source of the traffic to be filtered. The foreign address and mask specify the external destination of the traffic to be filtered.

Configuration Examples for ActiveX Filtering

You can set either address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts. You can use **0.0.0.0** for either mask (or in shortened form, **0**) to specify all masks. This command specifies that the ActiveX object blocking applies to HTTP traffic on port 80 from any local host and for connections to any foreign host.

The following example shows how to configure ActiveX filtering to block all outbound connections:

```
ciscoasa(config)# filter activex 80 0 0 0 0
```

The following example shows how to remove ActiveX filtering:

```
ciscoasa(config)# no filter activex 80 0 0 0 0
```

Feature History for ActiveX Filtering

Table 1: Feature History for ActiveX Filtering lists the release history for ActiveX Filtering. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 1: Feature History for ActiveX Filtering

Feature Name	Platform Releases	Feature Information
ActiveX filtering	7.0(1)	Filters specific undesirable objects from HTTP traffic, such as ActiveX objects, which may pose a security threat in certain situations.

Configuring Java Applet Filtering

This section includes the following topics:

Information About Java Applet Filtering

Java applets may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can remove Java applets with the **filter java** command.

Note Use the **filter activex** command to remove Java applets that are embedded in <object> tags.

The **filter java** command filters out Java applets that return to the ASA from an outbound connection. You still receive the HTML page, but the web page source for the applet is commented out so that the applet cannot execute. The **filter java** command does not filter clientless SSL VPN traffic.

Licensing Requirements for Java Applet Filtering

The following table shows the licensing requirements for Java applet filtering:

Table 2: Licensing Requirements

Model	License Requirement
License Requirement	Base License.

Guidelines and Limitations for Java Applet Filtering

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Does not support IPv6.

Configuring Java Applet Filtering

To apply filtering to remove Java applets from HTTP traffic passing through the ASA, enter the following command:

Procedure

	Command or Action	Purpose
Step 1	**filter java** *port[-port] local_ip local_mask foreign_ip foreign_mask* **Example:** `ciscoasa# filter java 80 0 0 0 0`	Removes Java applets in HTTP traffic passing through the ASA. To use this command, replace *port*[*-port*] with the TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The **http** or **url** literal can be used for port 80. You can specify a range of ports by using a hyphen between the starting port number and the ending port number. The local IP address and mask identify one or more internal hosts that are the source of the traffic to be filtered. The foreign address and mask specify the external destination of the traffic to be filtered. You can set either address to **0**.0.0.0 (or in shortened form, 0) to specify all hosts. You can use **0**.0.0.0 for either mask (or in shortened form, 0) to specify all hosts. You can set either address to **0**.0.0.0 (or in shortened form, 0) to specify all hosts. You can use **0**.0.0.0 for either mask (or in shortened form, 0) to specify all hosts.

Configuration Examples for Java Applet Filtering

The following example specifies that Java applets are blocked on all outbound connections:

```
ciscoasa(config)# filter java 80 0 0 0 0
```

This command specifies that the Java applet blocking applies to web traffic on port 80 from any local host and for connections to any foreign host.

The following example blocks downloading of Java applets to a host on a protected network:

```
ciscoasa(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

This command prevents host 192.168.3.3 from downloading Java applets.

The following example removes the configuration for downloading Java applets to a host on a protected network:

```
ciscoasa(config)# no filter java http 192.168.3.3 255.255.255.255 0 0
```

This command allows host 192.168.3.3 to download Java applets.

Feature History for Java Applet Filtering

Table 1: Feature History for ActiveX Filtering lists the release history for Java applet filtering. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 3: Feature History for Java Applet Filtering

Feature Name	Platform Releases	Feature Information
Java applet filtering	7.0(1)	Filters specific undesirable objects from HTTP traffic, such as Java applets, which may pose a security threat in certain situations.

Filtering URLs and FTP Requests with an External Server

This section describes how to filter URLs and FTP requests with an external server and includes the following topics:

Information About 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 ASA performance by using a separate server running one of the following Internet filtering products:

- Websense Enterprise for filtering HTTP, HTTPS, and FTP.
- McAfee SmartFilter (formerly N2H2) for filtering HTTP, HTTPS, FTP, and long URL filtering.

  In long URLs, the URL in the Referer field might contain a “host:” text string, which could cause the HTTP GET header to be incorrectly parsed as containing the HTTP Host parameter. The ASA, however, correctly parses the Referer field even when it contains a “host:” text string and forwards the header to the McAfee SmartFilter server with the correct Referer URL.

  Note URL caching will only work if the version of the URL server software from the URL server vendor supports it.

  Although ASA performance is less affected when using an external server, you might notice longer access times to websites or FTP servers when the filtering server is remote from the ASA.

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

  If user authentication is enabled on the ASA, then the ASA also sends the username to the filtering server. The filtering server can use user-specific filtering settings or provide enhanced reporting about usage.

Licensing Requirements for URL Filtering

The following table shows the licensing requirements for URL filtering:

Table 4: Licensing Requirements

Model	License Requirement
All models	Base License.

Guidelines and Limitations for URL Filtering

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Does not support IPv6.

Identifying the Filtering Server

You can identify up to four filtering servers per context. The ASA uses the servers in order until a server responds. In single mode, a maximum of 16 of the same type of filtering servers are allowed. 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 or HTTPS.

CLI

Procedure

	Command or Action	Purpose
Step 1	Choose from the following options:	
Step 2	For Websense: `hostname(config)#` **url-server** (*if_name*) **host** *local_ip* [**timeout** *seconds*] [**protocol TCP** | **UDP version** [**1**|**4**] [**connections** *num_conns*]] **Example:** `ciscoasa(config)# url-server (perimeter) host 10.0.1.1 protocol TCP version 4`	Identifies the address of the filtering server. *if_name* is the name of the ASA interface connected to the filtering server (the default is inside). For the **vendor** {*secure-computing* | *n2h2*} option, use *secure-computing* as the vendor string; however, *n2h2* is acceptable for backward compatibility. When the configuration entries are generated, *secure-computing* is saved as the vendor string. The **host** *local_ip* option is the IP address of the URL filtering server. The **port** *number* option is the Secure Computing SmartFilter server port number of the filtering server; the ASA also listens for UDP replies on this port.

	Command or Action	Purpose
		Note The default port is 4005, which is used by the Secure Computing SmartFilter server to communicate to the ASA via TCP or UDP. For information about changing the default port, see the *Filtering by N2H2 Administrator's Guide*. The **timeout** *seconds* option is the number of seconds that the ASA should keep trying to connect to the filtering server. The **connections** *number* option is the number of tries to make a connection between the host and server. The example identifies a Websense filtering server with the IP address 10.0.1.1 on a perimeter interface of the ASA.Version 4, which is enabled in this example, is recommended by Websense because it supports caching.

Step 3	For Secure Computing SmartFilter (formerly N2H2):
	`hostname(config)#` **url-server** (*if_name*) **vendor** {*secure-computing* | *n2h2*} **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** [*connections number*] } | **UDP**]
	Example:
	`ciscoasa(config)# url-server (perimeter) vendor n2h2`
	`host 10.0.1.1`
	`ciscoasa(config)# url-server (perimeter) vendor n2h2`
	`host 10.0.1.2`
		The example identifies redundant Secure Computing SmartFilter servers that are both on a perimeter interface of the ASA.

ASDM

Step 1 In the ASDM main window, choose **Configuration** > **Firewall** > **URL Filtering Servers**.

Step 2 In the URL Filtering Server Type area, click one of the following options:

- **Websense**
- **Secure Computing SmartFilter**

Step 3 If you chose the second option, enter the Secure Computing SmartFilter port number if it is different than the default port number, which is 4005.

Step 4 In the URL Filtering Servers area, click **Add**.

If you chose the Websense option, the Add Parameters for Websense URL Filtering dialog box appears.

- Choose the interface on which the URL filtering server is connected from the drop-down list.
- Enter the IP address of the URL filtering server.
- Enter the number of seconds after which the request to the URL filtering server times out. The default is 30 seconds.

- In the Protocol area, to specify which TCP version to use to communicate with the URL filtering server, click one of the following radio buttons:
  - TCP 1
  - TCP 4
  - UDP 4
- Enter the maximum number of TCP connections allowed for communicating with the URL filtering server, and click **OK**.

The new Websense URL filtering server properties appear in the URL Filtering Servers pane. To change these properties, click **Edit**. To add more Websense URL filtering servers after you have added the first Websense URL filtering server, click **Add** or **Insert**. To remove a Websense URL filtering server, click **Delete**.

If you chose the Secure Computing SmartFilter URL Filtering option, the Add Parameters for Secure Computing SmartFilter URL Filtering dialog box appears.

- Choose the interface on which the URL filtering server is connected from the drop-down list.
- Enter the IP address of the URL filtering server.
- Enter the number of seconds after which the request to the URL filtering server times out. The default is 30 seconds.
- In the Protocol area, to specify which protocol type to use to communicate with the URL filtering server, click one of the following radio buttons:
  - TCP
  - UDP
- Enter the maximum number of TCP connections allowed for communicating with the URL filtering server, and click **OK**.

The new Secure Computing SmartFilter URL filtering server properties appear in the URL Filtering Servers pane. To change these properties, click **Edit**. To add more Secure Computing SmartFilter URL filtering servers after you have defined the first Secure Computing SmartFilter URL filtering server, click **Add** or **Insert**. To remove a Secure Computing SmartFilter URL filtering server, click **Delete**.

Configuring Additional URL Filtering Settings

After you have accessed a website, the filtering server can allow the ASA to cache the server address for a certain period of time, as long as each website hosted at the address is in a category that is permitted at all times. When you access the server again, or if another user accesses the server, the ASA does not need to consult the filtering server again to obtain the server address.

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.

This section describes how to configure additional URL filtering settings and includes the following topics:

Buffering the Content Server Response

When you issue a request to connect to a content server, the ASA 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 behavior delays the web server response for the web client, because the web 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 behavior prevents the delay that might otherwise occur.

CLI

Procedure

	Command or Action	Purpose
Step 1	**url-block block** *block-buffer-limit* **Example:** `ciscoasa# url-block 3000`	Enables buffering of responses for HTTP or FTP requests that are pending a response from the filtering server. Replaces *block-buffer* with the maximum number of HTTP responses that can be buffered while awaiting responses from the URL server. **Note** Buffering of URLs longer than 3072 bytes is not supported.
Step 2	**url-block mempool-size** *memory-pool-size* **Example:** `ciscoasa# url-block mempool-size 5000`	Configures the maximum memory available for buffering pending URLs (and for buffering long URLs). Replaces *memory-pool-size* with a value from 2 to 10240 for a maximum memory allocation of 2 KB to 10 MB.

ASDM

Step 1 In the URL Filtering Servers pane, click **Advanced** to display the Advanced URL Filtering dialog box.

Step 2 In the URL Buffer Size area, check the **Enable buffering** check box.

Step 3 Enter the number of 1550-byte buffers. Valid values range from 1 to 128.

Step 4 Click **OK** to close this dialog box.

Caching Server Addresses

After you access a website, the filtering server can allow the ASA to cache the server address for a certain period of time, as long as each website hosted at the address is in a category that is permitted at all times. When you access the server again, or if another user accesses the server, the ASA 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. You can accumulate Websense run logs before using the **url-cache** command.

CLI

Procedure

	Command or Action	Purpose
Step 1	**url-cache dst | src_dst** *size* **Example:** `ciscoasa## url-cache src_dst 100`	Replaces *size* with a value for the cache size within the range from 1 to 128 (KB). Uses the **dst** keyword to cache entries based on the URL destination address. Choose this option if all users share the same URL filtering policy on the Websense server. Uses the **src_dst** keyword to cache entries based on both the source address initiating the URL request as well as the URL destination address. Choose this option if users do not share the same URL filtering policy on the Websense server.

ASDM

Step 1 In the URL Filtering Servers pane, click **Advanced** to display the Advanced URL Filtering dialog box.

Step 2 In the URL Cache Size area, check the **Enable caching based on** check box to enable caching according to the specified criteria.

Step 3 Click one of the following radio buttons:

- Destination Address—This option caches entries according to the URL destination address. Choose this setting if all users share the same URL filtering policy on the Websense server.
- Source/Destination Address—This option caches entries according to both the source address that initiates the URL request and the URL destination address. Choose this setting if users do not share the same URL filtering policy on the server.

Step 4 Enter the cache size within the range from 1 to 128 (KB).

Step 5 Click **OK** to close this dialog box.

Filtering HTTP URLs

This section describes how to configure HTTP filtering with an external filtering server and includes the following topics:

(CLI) Enabling HTTP Filtering

You must identify and enable the URL filtering server before enabling HTTP filtering. When the filtering server approves an HTTP connection request, the ASA allows the reply from the web server to reach the

originating client. If the filtering server denies the request, the ASA redirects you to a block page, indicating that access was denied.

To enable HTTP filtering, enter the following command:

Procedure

	Command or Action	Purpose
Step 1	**filter url** [**http** | *port* [*-port*] *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**proxy-block**] **Example:** `ciscoasa# filter url http 80 allow proxy-block`	Replaces *port*[*-port*] with one or more port numbers if a different port than the default port for HTTP (80) is used. Replaces *local_ip* and *local_mask* with the IP address and subnet mask of a user or subnetwork making requests. Replaces *foreign_ip* and *foreign_mask* with the IP address and subnet mask of a server or subnetwork responding to requests. The **allow** option causes the ASA to forward HTTP traffic without filtering when the primary filtering server is unavailable. Use the **proxy-block** command to drop all requests to proxy servers.

Enabling Filtering of Long HTTP URLs

By default, the ASA considers an HTTP URL to be a long URL if it is greater than 1159 characters. You can increase the maximum length allowed.

CLI

Procedure

	Command or Action	Purpose
Step 1	**url-block url-size** *long-url-size* **Example:** `ciscoasa# url-block url-size 3`	Replaces the *long-url-size* with the maximum size in KB for each long URL being buffered. For Websense servers, this is a value from 2 to 4 for a maximum URL size from 2 KB to 4 KB; for Secure Computing SmartFilter servers, this is a value between 2 and 3 for a maximum URL size from 2 KB to 3 KB. The default value is 2.

ASDM

Step 1 In the URL Filtering Servers pane, click **Advanced** to display the Advanced URL Filtering dialog box.

Step 2 In the Long URL Support area, check the **Use Long URL** check box to enable long URLs for filtering servers.

Step 3 Enter the maximum URL length allowed, up to a maximum of 4 KB.

Step 4 Enter the memory allocated for long URLs in KB.

Step 5 Click **OK** to close this dialog box.

(CLI) Truncating Long HTTP URLs

By default, if a URL exceeds the maximum permitted size, then it is dropped. To avoid this occurrence, truncate a long URL by entering the following command:

Procedure

	Command or Action	Purpose
Step 1	**filter url** [**longurl-truncate** | **longurl-deny** | **cgi-truncate**] **Example:** `ciscoasa# filter url longurl-truncate`	The **longurl-truncate** option causes the ASA to send only the hostname or IP address portion of the URL for evaluation to the filtering server when the URL is longer than the maximum length permitted. Use the **longurl-deny** option to deny outbound URL traffic if the URL is longer than the maximum permitted. Use the **cgi-truncate** option to truncate CGI URLs to include only the CGI script location and the script name without any parameters. Many long HTTP requests are CGI requests. If the parameters list is very long, waiting and sending the complete CGI request, including the parameter list, can use up memory resources and affect ASA performance.

(CLI) Exempting Traffic from Filtering

To exempt traffic from filtering, enter following command:

Procedure

	Command or Action	Purpose

Step 1	**filter url except** *source_ip source_mask dest_ip dest_mask*
	Example:
	`ciscoasa(config)# filter url http 0 0 0 0`
	`ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0`
		Exempts specific traffic from filtering.
		The example shows how to cause all HTTP requests to be forwarded to the filtering server, except for those from 10.0.2.54.

(CLI) Filtering HTTPS URLs

You must identify and enable the URL filtering server before enabling HTTPS filtering.

Note Websense and Secure Computing Smartfilter currently support HTTPS; older versions of the Secure Computing SmartFilter (formerly N2H2) do not support HTTPS filtering.

Because HTTPS content is encrypted, the ASA sends the URL lookup without directory and filename information. When the filtering server approves an HTTPS connection request, the ASA allows the completion of SSL connection negotiation and allows the reply from the web server to reach the originating client. If the filtering server denies the request, the ASA prevents the completion of SSL connection negotiation. The browser displays an error message, such as “The Page or the content cannot be displayed.”

Note The ASA does not provide an authentication prompt for HTTPS, so you must authenticate with the ASA using HTTP or FTP before accessing HTTPS servers.

To enable HTTPS filtering, enter the following command:

Procedure

	Command or Action	Purpose
Step 1	**filter https** *port* [*-port*] *localIP local_mask foreign_IP foreign_mask* [**allow**] **Example:** `ciscoasa# filter https 443 0 0 0 0 0 0 0 0 allow`	Enables HTTPS filtering. Replaces *port*[*-port*] with a range of port numbers if a different port than the default port for HTTPS (443) is used. Replaces *local_ip* and *local_mask* with the IP address and subnet mask of a user or subnetwork making requests. Replaces *foreign_ip* and *foreign_mask* with the IP address and subnet mask of a server or subnetwork responding to requests. The **allow** option causes the ASA to forward HTTPS traffic without filtering when the primary filtering server is unavailable.

(CLI) Filtering FTP Requests

You must identify and enable the URL filtering server before enabling FTP filtering.

Note Websense and Secure Computing Smartfilter currently support FTP; older versions of Secure Computing SmartFilter (formerly known as N2H2) did not support FTP filtering.

When the filtering server approves an FTP connection request, the ASA allows the successful FTP return code to reach the originating client. For example, a successful return code is "250: CWD command successful." If the filtering server denies the request, the FTP return code is changed to show that the connection was denied. For example, the ASA changes code 250 to "550 Requested file is prohibited by URL filtering policy."

To enable FTP filtering, enter the following command:

Procedure

	Command or Action	Purpose
Step 1	**filter ftp** *port* [*-port*] *localIP local_mask foreign_IP foreign_mask* [**allow**] [**interact-block**] **Example:** `ciscoasa# filter ftp 21 0 0 0 0 0 0 0 0 allow`	Enables FTP filtering. Replaces *port*[*-port*] with a range of port numbers if a different port than the default port for FTP (21) is used. Replaces *local_ip* and *local_mask* with the IP address and subnet mask of a user or subnetwork making requests.

	Command or Action	Purpose
		Replaces *foreign_ip* and *foreign_mask* with the IP address and subnet mask of a server or subnetwork responding to requests. The **allow** option causes the ASA to forward HTTPS traffic without filtering when the primary filtering server is unavailable. Use the **interact-block** option to prevent interactive FTP sessions that do not provide the entire directory path. An interactive FTP client allows you to change directories without typing the entire path. For example, you might enter **cd ./files** instead of **cd /public/files**.

(ASDM) Configuring Filtering Rules

Before you can add an HTTP, HTTPS, or FTP filter rule, you must enable a URL filtering server. To enable a URL filtering server, choose **Configuration** > **Firewall** > **URL Filtering Servers**.

To configure filtering rules, perform the following steps:

Step 1 From the ASDM main window, choose **Configuration** > **Firewall** > **Filter Rules**.

Step 2 In the toolbar, click **Add** to display the types of filter rules that are available to add from the following list:

- Add Filter ActiveX Rule
- Add Filter Java Rule
- Add Filter HTTP Rule
- Add Filter HTTPS Rule
- Add Filter FTP Rule

Step 3 If you chose Add Filter ActiveX Rule, specify the following settings:

- Click one of the following radio buttons: **Filter ActiveX** or **Do not filter ActiveX**.
- Enter the source of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any source address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Source dialog box. Choose a host or address from the drop-down list.

- Enter the destination of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any destination address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Destination dialog box. Choose a host or address from the drop-down list.
- Identify the service of the traffic to which the filtering action applies. To identify the service, enter one of the following:
  - *tcp/port*—The port number can range 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.

    >—Greater than. For example, >tcp/2000.

    - —Range. For example, tcp/2000-3000.
  - Enter a well-known service name, such as HTTP or FTP.
  - Click the ellipses to display the Browse Service dialog box. Choose a service from the drop-down list.
- Click **OK** to close this dialog box.
- Click **Apply** to save your changes.

Step 4 If you chose Add Filter Java Rule, specify the following settings:

- Click one of the following radio buttons: **Filter Java** or **Do not filter Java**.
- Enter the source of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any source address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Source dialog box. Choose a host or address from the drop-down list.
- Enter the destination of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any destination address.
  - Enter a hostname.

- 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**.
- Click the ellipses to display the Browse Destination dialog box. Choose a host or address from the drop-down list.

- Identify the service of the traffic to which the filtering action applies. To identify the service, enter one of the following:
  - *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.

    >—Greater than. For example, >tcp/2000.

    - —Range. For example, tcp/2000-3000.
  - Enter a well-known service name, such as HTTP or FTP.
  - Click the ellipses to display the Browse Service dialog box. Choose a service from the drop-down list.

- Click **OK** to close this dialog box.
- Click **Apply** to save your changes.

Step 5 If you chose Add Filter HTTP Rule, specify the following settings:

- Click one of the following radio buttons: **Filter HTTP** or **Do not filter HTTP**.
- Enter the source of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any source address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Source dialog box. Choose a host or address from the drop-down list.

- Enter the destination of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any destination address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Destination dialog box. Choose a host or address from the drop-down list.

- Identify the service of the traffic to which the filtering action applies. To identify the service, enter one of the following:
  - *tcp/port*—The port number can range 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.

    >—Greater than. For example, >tcp/2000.

    - —Range. For example, tcp/2000-3000.
  - Enter a well-known service name, such as HTTP or FTP.
  - Click the ellipses to display the Browse Service dialog box. Choose a service from the drop-down list.
- Choose the action to take when the URL exceeds the specified size from the drop-down list.
- Check the **Allow outbound traffic if URL server is not available check box** to connect without URL filtering being performed. When this check box is unchecked, you cannot connect to Internet websites if the URL server is unavailable.
- Check the **Block users from connecting to an HTTP proxy server check box to** prevent HTTP requests made through a proxy server.
- Check the **Truncate CGI parameters from URL sent to URL server** check box to have the ASA forward only the CGI script location and the script name, without any parameters, to the filtering server.
- Click **OK** to close this dialog box.
- Click **Apply** to save your changes.

Step 6 If you chose Add Filter HTTPS Rule, specify the following settings:

- Click one of the following radio buttons: **Filter HTTPS** or **Do not filter HTTPS**.
- Enter the source of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any source address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Source dialog box. Choose a host or address from the drop-down list.
- Enter the destination of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any destination address.
  - Enter a hostname.
  - 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**.

- Click the ellipses to display the Browse Destination dialog box. Choose a host or address from the drop-down list.

- Identify the service of the traffic to which the filtering action applies. To identify the service, enter one of the following:
  - *tcp/port*—The port number can range 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.

    >—Greater than. For example, >tcp/2000.

    - —Range. For example, tcp/2000-3000.
  - Enter a well-known service name, such as HTTP or FTP.
  - Click the ellipses to display the Browse Service dialog box. Choose a service from the drop-down list.

- Check the **Allow outbound traffic if URL server is not available check box** to connect without URL filtering being performed. When this check box is unchecked, you cannot connect to Internet websites if the URL server is unavailable.
- Click **OK** to close this dialog box.
- Click **Apply** to save your changes.

Step 7 If you chose Add Filter FTP Rule, specify the following settings:

- Click one of the following radio buttons: **Filter FTP** or **Do not filter FTP**.
- Enter the source of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any source address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Source dialog box. Choose a host or address from the drop-down list.

- Enter the destination of the traffic to which the filtering action applies. To enter the source, choose from the following options:
  - Enter **any** to indicate any destination address.
  - Enter a hostname.
  - 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**.
  - Click the ellipses to display the Browse Destination dialog box. Choose a host or address from the drop-down list.

- Identify the service of the traffic to which the filtering action applies. To identify the service, enter one of the following:
  - *tcp/port*—The port number can range 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.

    >—Greater than. For example, >tcp/2000.

    - —Range. For example, tcp/2000-3000.
  - Enter a well-known service name, such as http or ftp.
  - Click the ellipses to display the Browse Service dialog box. Choose a service from the drop-down list.
- Check the **Allow outbound traffic if URL server is not available check box** to connect without URL filtering being performed. When this check box is unchecked, you cannot connect to Internet websites if the URL server is unavailable.
- Check the **Block interactive FTP sessions (block if absolute FTP path is not provided)** check box to drop FTP requests if they use a relative path name to the FTP directory.
- Click **OK** to close this dialog box.
- Click **Apply** to save your changes.

Step 8 To modify a filtering rule, select it and click **Edit** to display the Edit Filter Rule dialog box for the specified filtering rule.

Step 9 Make the required changes, then click **OK** to close this dialog box.

Step 10 Click **Apply** to save your changes.

(ASDM) Filtering the Rule Table

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 to display the Filter toolbar.

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 composed of source, destination, service, and rule type information.

Step 3 For Source, Destination, Source or Destination, and Service filters, perform the following steps:

a. Enter the string to match using one of the following methods:

1. Type the source, destination, or service name in the adjacent field.
2. Click the ellipses to open a Browse dialog box from which you can choose existing services, IP addresses, or host names.

b. Choose the match criteria from the drop-down list. Choose **is** for exact string matches or **contains** for partial string matches.

Step 4 For Rule Type filters, choose the rule type from the list.

Step 5 For Query filters, click **Define Query**. To define queries, see the (ASDM) Defining Queries.

Step 6 To apply the filter to the rule table, click **Filter**.

Step 7 To remove the filter from the rule table and display all rule entries, click **Clear**.

Step 8 To show the packet trace for the selected rule, click **Packet Trace**.

Step 9 To show and hide the selected rule diagram, click **Diagram**.

Step 10 To remove a filter rule and place it elsewhere, click **Cut**.

Step 11 To copy a filter rule, click **Copy**. Then to move the copied filter rule elsewhere, click **Paste**.

Step 12 To delete a selected filter rule, click **Delete**.

(ASDM) Defining Queries

To define queries, perform the following steps:

Step 1 Enter the IP address or hostname of the source. Choose **is** for an exact match or choose **contains** for a partial match. Click the ellipses to display the Browse Source dialog box. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them with commas.

Step 2 Enter the IP address or hostname of the destination. Choose **is** for an exact match or choose **contains** for a partial match. Click the ellipses to display the Browse Destination dialog box. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them with commas.

Step 3 Enter the IP address or hostname of the source or destination. Choose **is** for an exact match or choose **contains** for a partial match. Click the ellipses to display the Browse Source dialog box. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them with commas.

Step 4 Enter the protocol, port, or name of a service. Choose **is** for an exact match or choose **contains** for a partial match. Click the ellipses to display the Browse Service dialog box. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them with commas.

Step 5 Choose the rule type from the drop-down list.

Step 6 Click **OK** to close this dialog box.

After you click **OK**, the filter is immediately applied to the rule table. To remove the filter, click **Clear**.

(CLI) Monitoring Filtering Statistics

To monitor filtering statistics, enter one of the following commands:

Command	Purpose
show url-server	Shows information about the URL filtering server.
show url-server statistics	Shows URL filtering statistics.
show url-block	Shows the number of packets held in the url-block buffer and the number (if any) dropped because of exceeding the buffer limit or retransmission.
show url-block block statistics	Shows the URL block statistics.
show url-cache stats	Shows the URL cache statistics.
show perfmon	Shows URL filtering performance statistics, along with other performance statistics.
show filter	Shows the filtering configuration.

The following is sample output from the **show url-server** command:

```
ciscoasa# show url-server
url-server (outside) vendor n2h2 host 128.107.254.202 port 4005 timeout 5 protocol TCP
```

The following is sample output from the **show url-server statistics** command:

```
ciscoasa# show url-server statistics
Global Statistics:
--------------------
URLs total/allowed/denied 13/3/10
URLs allowed by cache/server 0/3
URLs denied by cache/server 0/10
HTTPSs total/allowed/denied 138/137/1
HTTPSs allowed by cache/server 0/137
HTTPSs denied by cache/server 0/1
FTPs total/allowed/denied 0/0/0
FTPs allowed by cache/server 0/0
FTPs denied by cache/server 0/0
Requests dropped 0
Server timeouts/retries 0/0
Processed rate average 60s/300s 0/0 requests/second
Denied rate average 60s/300s 0/0 requests/second
Dropped rate average 60s/300s 0/0 requests/second
Server Statistics:
--------------------
10.125.76.20 UP
Vendor websense
Port 15868
Requests total/allowed/denied 151/140/11
Server timeouts/retries 0/0
```

```
Responses received 151
Response time average 60s/300s 0/0
URL Packets Sent and Received Stats:
------------------------------------
Message Sent Received
STATUS_REQUEST 1609 1601
LOOKUP_REQUEST 1526 1526
LOG_REQUEST 0 NA
Errors:
-------
RFC noncompliant GET method 0
URL buffer update failure 0
```

The following is sample output from the show url-block command:

```
ciscoasa# show url-block
url-block url-mempool 128
url-block url-size 4
url-block block 128
```

The following is sample output from the **show url-block block statistics** command:

```
ciscoasa# show url-block block statistics
URL Pending Packet Buffer Stats with max block 128
----------------------------------------------------
Cumulative number of packets held: 896
Maximum number of packets held (per URL): 3
Current number of packets held (global): 38
Packets dropped due to
exceeding url-block buffer limit: 7546
HTTP server retransmission: 10
Number of packets released back to client: 0
```

The following is sample output from the **show url-cache stats** command:

```
ciscoasa# show url-cache stats
URL Filter Cache Stats
----------------------
Size : 128KB
Entries : 1724
In Use : 456
Lookups : 45
Hits : 8
This shows how the cache is used.
```

The following is sample output from the **show perfmon** command:

```
ciscoasa# show perfmon
PERFMON STATS:     Current    Average
Xlates               0/s        0/s
Connections          0/s        2/s
TCP Conns            0/s        2/s
UDP Conns            0/s        0/s
URL Access           0/s        2/s
URL Server Req       0/s        3/s
TCP Fixup            0/s        0/s
TCPIntercept         0/s        0/s
HTTP Fixup           0/s        3/s
FTP Fixup            0/s        0/s
AAA Authen           0/s        0/s
AAA Author           0/s        0/s
AAA Account          0/s        0/s
```

The following is sample output from the **show filter** command:

```
ciscoasa# show filter
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

Feature History for URL Filtering

Table 5: Feature History for URL Filtering lists the release history for URL filtering. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 5: Feature History for URL Filtering

Feature Name	Platform Releases	Feature Information
URL filtering	7.0(1)	Filters URLs based on an established set of filtering criteria.