Managing Firewall Web Filter Rules

Web filter rules policies define policies for allowing or preventing web traffic based on the requested URL or the applet content of the traffic. For ASA, PIX, and FWSM devices, you can also filter FTP and HTTPS traffic.

How you configure web filter rules is different depending on whether the device uses ASA, PIX or FWSM software as opposed to Cisco IOS Software.

The following topics help you work with web filter rules:

Understanding Web Filter Rules

Web filter rules policies define policies for allowing or preventing web traffic based on the requested URL or the applet content of the traffic. For ASA, PIX, and FWSM devices, you can also filter FTP and HTTPS traffic.

Web, or URL, filtering allows you to control which web sites and web content your users have access to. For example, you might consider some types of content to create a hostile work environment for the people in your organization (for example, web sites that provide pornography). You might consider some web sites to be unsafe and a source of potential viral applications. Using web filter rules, you can block access to these objectionable or unsafe sites.

To filter web requests, you should install an external web filtering server, either Websense or SmartFilter (N2H2). For ASA, PIX, and FWSM devices, these external servers are required for URL, FTP, or HTTPS filtering. For IOS devices, you can also use these servers, but additionally you can create local lists of allowed (always allowed) or blocked (always denied) URLs. You configure the filtering servers in the web filter settings policy; see Configuring Settings for Web Filter Servers , on page 16.

Tip For IOS devices, you have the option of configuring web filtering using zone-based firewall rules instead of web filter rules, which allows you the additional option of using Trend Micro web filtering servers. For more information, see Managing Zone-based Firewall Rules.

Beside filtering requests based on URL, you can do some applet filtering, stripping out ActiveX or Java applets. You might want to do this to prevent applet downloads from sites you otherwise want to allow if you do not fully trust the site. You can configure your rules to block these applets from specific sites while allowing them from trusted sites.

The policies and procedures for configuring web filter rules differs based on the device type. See the following topics for more information:

- Configuring Web Filter Rules for ASA, PIX, and FWSM Devices , on page 2
- Configuring Web Filter Rules for IOS Devices , on page 11

Configuring Web Filter Rules for ASA, PIX, and FWSM Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX and FWSM features/functionality, it does not support any enhancements.

Web filter rules policies for ASA, PIX, and FWSM devices define how you want to handle HTTP, FTP, and HTTPS traffic. You can also filter ActiveX and Java applets. Web filter rules permit or deny traffic based on the Universal Resource Locator (URL) address in the web request. If you allow HTTP traffic in your access rules, you can subsequently deny (or drop) traffic if it is directed at an objectionable web or FTP site, or you can strip out ActiveX or Java applets from untrusted sources.

To configure web filtering rules for ASA, PIX, and FWSM devices:

1. Configure the rules that identify traffic that should be subject to filtering, and the traffic that should be exempt from filtering rules (see below for the procedure).
2. Configure web filter settings to identify the URL filtering server and other settings. For more information, see Configuring Settings for Web Filter Servers , on page 16.

Related Topics

- Understanding Web Filter Rules , on page 1
- Using Sections to Organize Rules Tables
- Adding and Removing Rules
- Editing Rules
- Enabling and Disabling Rules
- Moving Rules and the Importance of Rule Order
- Understanding Networks/Hosts Objects
- Understanding and Specifying Services and Service and Port List Objects

Step 1 Do one of the following to open the Web Filter Rules Page (ASA/PIX/FWSM) , on page 3:

- Device view—Select **Firewall** > **Web Filter Rules** from the Policy selector.

- Policy view—Select **Firewall > Web Filter Rules (PIX/FWSM/ASA)** from the Policy Type select. Select an existing policy or create a new one.

Step 2 Select the row after which you want to create the rule and click the **Add Row** button or right-click and select **Add Row**. This opens the Add and Edit PIX/ASA/FWSM Web Filter Rule Dialog Boxes , on page 6.

Tip If you do not select a row, the new rule is added at the end of the local scope. You can also select an existing row and edit either the entire row or specific cells. For more information, see Editing Rules.

Step 3 Configure the rule. Following are the highlights of what you typically need to decide. For specific information on configuring the fields, see Add and Edit PIX/ASA/FWSM Web Filter Rule Dialog Boxes , on page 6.

- Filtering and Type—Whether you are creating a rule that identifies traffic to be filtered (Filter) or exempted from an existing filter rule (Filter Except), and the type of filtering to be done:
  - URL—To filter traffic based on web address.
  - HTTPS—To filter web traffic to secure sites. This does not include SSL VPN traffic.
  - FTP—To filter FTP traffic.
  - ActiveX or Java—To remove ActiveX or Java applets. These options delete all entities within applet or object tags, so you might remove more than just ActiveX or Java applets.
- Source and Destination addresses—If the rule should apply no matter which addresses generated the traffic or their destinations, use “any” as the source or destination. If the rule is specific to a host or network, enter the addresses or network/host objects. For information on the accepted address formats, see Specifying IP Addresses During Policy Definition.
- Service—Primarily defines the port that should be monitored. You must specify some type of TCP service. Typically, you would use the pre-defined services HTTP, HTTPS, or FTP, which should be the same as the type of filtering you are performing, but you can specify any TCP port on your network that might contain the traffic to be filtered.
- Options—The options you want to include, if any. The main options of interest are whether you want to allow traffic if the filtering servers are unavailable, and whether you want to truncate long URLs or URLs that have parameters. Truncating URLs that have parameters is typically a good idea, because if you are going to drop a URL, it is not normally because of a parameter value.

Click **OK** when you are finished defining your rule.

Step 4 If you did not select the desired row before adding the rule, select the new rule and use the up and down arrow buttons to position the rule appropriately. Order is not as important for web filtering rules, however, because filter except rules always create exceptions to the related filter rule, whether they come before or after the filter rule. For more information, see Moving Rules and the Importance of Rule Order.

Web Filter Rules Page (ASA/PIX/FWSM)

Note From version 4.17, though Cisco Security Manager continues to support PIX and FWSM features/functionality, it does not support any enhancements.

Use the Web Filter Rules page for ASA, PIX, and FWSM devices to configure web, or URL, filtering rules. Web filtering is a type of HTTP inspection. If your access rules allow HTTP traffic, you can configure rules to apply server-based web filtering to prevent users from accessing undesirable web servers.

When you configure web filter rules, also configure web filter settings in the **Firewall > Settings > Web Filter** policy. The settings identify the web filtering server and contain other settings that control the overall functioning of the policy. You must configure a web filtering server for your URL, FTP, or HTTPS filter rules to be deployed. For more information, see Web Filter Settings Page , on page 17.

Tip Rules cannot overlap. For example, if you create two rules with the same, or overlapping, source, destination, and service, you cannot deploy them. Also, you should order any filter-except rules below the filter rule to which they are creating an exemption.

Navigation Path

To access the Web Filter Rules page for ASA, PIX, and FWSM devices, do one of the following:

- (Device view) Select an ASA, PIX, or FWSM device, then select **Firewall > Web Filter Rules** from the Policy selector.
- (Policy view) Select **Firewall > Web Filter Rules (PIX/FWSM/ASA)** from the Policy Type selector. Create a new policy or select an existing one.
- (

  Map view) Right-click an ASA, PIX, or FWSM device and select **Edit Firewall Policies > Web Filter Rules**.

Related Topics

- Understanding Web Filter Rules , on page 1
- Configuring Web Filter Rules for ASA, PIX, and FWSM Devices , on page 2
- Configuring Settings for Web Filter Servers , on page 16
- Adding and Removing Rules
- Editing Rules
- Using Sections to Organize Rules Tables
- Enabling and Disabling Rules
- Moving Rules and the Importance of Rule Order
- Filtering Tables

Field Reference

Table 1: Web Filter Rules Page (ASA, PIX, FWSM)

Element	Description
No.	The ordered rule number.
Source Destination	The source and destination addresses for the rule. The "any" address does not restrict the rule to specific hosts, networks, or interfaces. These addresses are IP addresses for hosts or networks, network/host objects, interfaces, or interface roles. Multiple entries are displayed as separate subfields within the table cell. See Understanding Networks/Hosts Objects.
Service	The services or service objects that specify the protocol and port of the traffic to which the rule applies. Multiple entries are displayed as separate subfields within the table cell. See Understanding and Specifying Services and Service and Port List Objects.
Type	The type of filtering action for the rule, either filtering the identified traffic, or exempting the identified traffic from filtering (Filter Except). For a full explanation, see Edit Web Filter Type Dialog Box , on page 9.
Options	Additional configuration options for the selected protocol, if any. For detailed descriptions, see Edit Web Filter Options Dialog Box , on page 10.
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects.
Description	The description of the rule, if any.
Last Ticket(s)	Shows the ticket(s) associated with last modification to the rule. You can click the ticket ID in the Last Ticket(s) column to view details of the ticket and to navigate to the ticket. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Ticket Management Page).
Query	Click this button to run a policy query, which can help you evaluate your rules and identify ineffective rules. See Generating Policy Query Reports
Find and Replace button (binoculars icon)	Click this button to search for various types of items within the table and to optionally replace them. See Finding and Replacing Items in Rules Tables.
Up Row and Down Row buttons (arrow icons)	Click these buttons to move the selected rules up or down within a scope or section. For more information, see Moving Rules and the Importance of Rule Order.
Add Row button	Click this button to add a rule to the table after the selected row using the Add and Edit PIX/ASA/FWSM Web Filter Rule Dialog Boxes , on page 6. If you do not select a row, the rule is added at the end of the local scope. For more information about adding rules, see Adding and Removing Rules.
Edit Row button	Click this button to edit the selected rule. You can also edit individual cells. For more information, see Editing Rules.

Element	Description
Delete Row button	Click this button to delete the selected rule.

Add and Edit PIX/ASA/FWSM Web Filter Rule Dialog Boxes

Note From version 4.17, though Cisco Security Manager continues to support PIX and FWSM features/functionality, it does not support any enhancements.

Use the Add and Edit PIX/ASA/FWSM Web Filter Rule dialog boxes to configuring web filtering rules for these types of devices.

Navigation Path

From the Web Filter Rules Page (ASA/PIX/FWSM) , on page 3, click the **Add Row** button or select a row and click the **Edit Row** button.

Related Topics

- Configuring Web Filter Rules for ASA, PIX, and FWSM Devices , on page 2
- Understanding Web Filter Rules , on page 1
- Configuring Settings for Web Filter Servers , on page 16

Field Reference

Table 2: Add and Edit PIX/ASA/FWSM Web Filter Rule Dialog Boxes

Element	Description
Enable Rule	Whether to enable the rule, which means the rule becomes active when you deploy the configuration to the device. Disabled rules are shown overlain with hash marks in the rule table. For more information, see Enabling and Disabling Rules.
Filtering	The type of rule you are defining: • Filter—The rule filters the identified type of traffic between source and destination. • Filter Except—The rule creates an exemption to a filter rule. The identified traffic between the source and destination is not filtered.

Element	Description
Type	The type of traffic that should be filtered (or exempted from filtering) for this rule. For filtering that uses an external server, consult the documentation for your version of the server to determine if it supports that type of filtering. Configure the filtering server on the Web Filter Settings Page , on page 17. • URL—HTTP traffic. Filtering is done using an external filtering server. • HTTPS—HTTPS traffic. This does not include traffic associated with an SSL VPN. Filtering is done using an external filtering server. • Java—Remove Java applets from HTTP traffic if they are identified on applet tags. The rule does not remove Java applets from SSL VPN traffic. If the applet tag spans packets, or the code in the tags is larger than the MTU, the Java applet is not removed. • ActiveX—Remove ActiveX or Java applets from HTTP traffic. The rule removes any item within object or applet tags, which might also remove images and multimedia objects. The rule might not remove applets from SSL VPN traffic. If the object tag spans packets, or the code in the tags is larger than the MTU, the object is not removed. • FTP—FTP traffic. Filtering is done using an external filtering server.
Sources Destinations	The source or destination of the traffic. You can enter more than one value by separating the items with commas. You can enter any combination of the following address types to define the source or destination of the traffic. For more information, see Specifying IP Addresses During Policy Definition. • Network/host object. Enter the name of the object or click **Select** to select it from a list. You can also create new network/host objects from the selection list. • Host IP address, for example, 10.10.10.100. • Network address, including subnet mask, in either the format 10.10.10.0/24 or 10.10.10.0/255.255.255.0. • A range of IP addresses, for example, 10.10.10.100-10.10.10.200. • An IP address pattern in the format 10.10.0.10/255.255.0.255, where the mask is a discontiguous bit mask (see Contiguous and Discontiguous Network Masks for IPv4 Addresses).

Element	Description
Services	The services that define the port number of the traffic to act on. You can enter more than one value by separating the items with commas. The service must use TCP. Your specification defines the port that you want filtered (the service name has no meaning). For example, if you want to filter port 80, use the HTTP service object. If HTTP traffic on your network uses a different port, specify TCP/port number (for example, TCP/8080). You can enter TCP by itself to filter all ports. You can enter any combination of service objects and service types (which are typically a protocol and port combination). If you type in a service, you are prompted as you type with valid values. You can select a value from the list and press Enter or Tab. For complete information on how to specify services, see Understanding and Specifying Services and Service and Port List Objects.
Allow traffic if URL Filter Server unavailable (URL, FTP, HTTPS only)	Whether to permit unfiltered traffic on outbound connections if all of the URL filtering servers are unavailable. If you do not select this option, all affected outbound traffic (HTTP, FTP, or HTTPS) is blocked until at least one filtering server becomes available.
Block connection to HTTP Proxy Server (URL only)	Whether to prevent users from connecting to an HTTP proxy server.
Truncate CGI request by removing CGI parameters (URL only)	When a URL has a parameter list starting with a question mark (?), such as a CGI script, whether to truncate the URL sent to the filtering server by removing all characters after and including the question mark.
Block outbound requests if absolute FTP path is not provided (FTP only)	Whether to prevent interactive FTP sessions that do not provide the entire directory path when the user tries to change directories.
Long URL (URL only)	How to handle URLs that are longer than the maximum allowed by the filtering server: 4 KB for Websense, 3 KB for Smartfilter (N2H2). Many times, long URLs are due to parameter lists, and you can use the **Truncate CGI request by removing CGI parameters** option to handle those URLs. For other long URLs, select from the following options: • Drop—Drop the long URL request. • Truncate—Truncate the URL request to only the hostname or IP address portion of the URL. • Deny—Deny the URL request.

Element	Description
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects.
Description	An optional description of the rule (up to 1024 characters).

Edit Web Filter Type Dialog Box

Use the Edit Web Filter Type dialog box to edit the type of filtering to be done by a web filter rule for ASA, PIX, and FWSM devices.

Navigation Path

Right-click the Type cell in a web filter rule for ASA/PIX/FWSM (on the Web Filter Rules Page (ASA/PIX/FWSM) , on page 3) and select **Edit Web Filter Type**. You can edit the type for one row at a time.

Field Reference

Table 3: Edit Web Filter Type Dialog Box

Element	Description
Filtering	The type of rule you are defining: • Filter—The rule filters the identified type of traffic between source and destination. • Filter Except—The rule creates an exemption to a filter rule. The identified traffic between the source and destination is not filtered.
Type	The type of traffic that should be filtered (or exempted from filtering) for this rule. For filtering that uses an external server, consult the documentation for your version of the server to determine if it supports that type of filtering. Configure the filtering server on the Web Filter Settings Page , on page 17. • URL—HTTP traffic. Filtering is done using an external filtering server. • HTTPS—HTTPS traffic. This does not include traffic associated with an SSL VPN. Filtering is done using an external filtering server. • Java—Remove Java applets from HTTP traffic if they are identified on applet tags. The rule does not remove Java applets from SSL VPN traffic. If the applet tag spans packets, or the code in the tags is larger than the MTU, the Java applet is not removed. • ActiveX—Remove ActiveX or Java applets from HTTP traffic. The rule removes any item within object or applet tags, which might also remove images and multimedia objects. The rule might not remove applets from SSL VPN traffic. If the object tag spans packets, or the code in the tags is larger than the MTU, the object is not removed. • FTP—FTP traffic. Filtering is done using an external filtering server.

Edit Web Filter Options Dialog Box

Use the Edit Web Filter Options dialog box to edit the filtering options defined for a web filter rule for ASA, PIX, and FWSM devices.

The options displayed on this dialog box differ depending on the type of filtering configured for the rule. For some types, there are no options and the dialog box is empty. The reference table below includes all possible options.

Navigation Path

Right-click the Options cell in a web filter rule for ASA/PIX/FWSM (on the Web Filter Rules Page (ASA/PIX/FWSM) , on page 3) and select **Edit Web Filter Type**. You can edit the type for one row at a time.

Field Reference

Table 4: Edit Web Filter Options Dialog Box

Element	Description
Allow traffic if URL Filter Server unavailable (URL, FTP, HTTPS only)	Whether to permit unfiltered traffic on outbound connections if all of the URL filtering servers are unavailable. If you do not select this option, all affected outbound traffic (HTTP, FTP, or HTTPS) is blocked until at least one filtering server becomes available.
Block connection to HTTP Proxy Server (URL only)	Whether to prevent users from connecting to an HTTP proxy server.
Truncate CGI request by removing CGI parameters (URL only)	When a URL has a parameter list starting with a question mark (?), such as a CGI script, whether to truncate the URL sent to the filtering server by removing all characters after and including the question mark.
Block outbound requests if absolute FTP path is not provided (FTP only)	Whether to prevent interactive FTP sessions that do not provide the entire directory path when the user tries to change directories.
Long URL (URL only)	How to handle URLs that are longer than the maximum allowed by the filtering server: 4 KB for Websense, 3 KB for Smartfilter (N2H2). Many times, long URLs are due to parameter lists, and you can use the **Truncate CGI request by removing CGI parameters** option to handle those URLs. For other long URLs, select from the following options: • Drop—Drop the long URL request. • Truncate—Truncate the URL request to only the hostname or IP address portion of the URL. • Deny—Deny the URL request.

Configuring Web Filter Rules for IOS Devices

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any enhancements.

Web filter rules policies for IOS devices define how you want to handle HTTP traffic. The web filter rules are a type of inspection rule that permits or denies traffic based on the Universal Resource Locator (URL) address in the web request. If you allow HTTP traffic on an interface in your access rules, you can subsequently deny (or drop) traffic if it is directed at an objectionable web site.

To configure web filtering rules for IOS devices:

1. Configure the interfaces that should filter web traffic (see below for the procedure).
2. Configure the local web filtering list to identify web sites that should always be permitted or denied (see below for the procedure).
3. Configure web filter settings to identify the URL filtering server and other settings. For more information, see Configuring Settings for Web Filter Servers , on page 16.

Tip You can also configure web filtering as a zone based firewall rule. For more information, see Adding Zone-Based Firewall Rules.

Related Topics

- Understanding Web Filter Rules , on page 1
- Understanding Interface Role Objects
- Understanding Networks/Hosts Objects

Step 1 Do one of the following to open the Web Filter Rules Page (IOS) , on page 12:

- Device view—Select **Firewall** > **Web Filter Rules** from the Policy selector.
- Policy view—Select **Firewall** > **Web Filter Rules (IOS)** from the Policy Type select. Select an existing policy or create a new one.

Step 2 Configure the interfaces on which you will filter HTTP traffic. Create rules for each interface on which you will enable filtering:

a) Select the Web Filter Rules tab if it is not already selected and do one of the following to open the IOS Web Filter Rule and Applet Scanner Dialog Box , on page 14:

- To create a new rule, right-click inside the work area and select **Add Row**.
- To edit an existing rule, right-click the rule and select **Edit Row**.

b) Identify the interface for which this rule applies. You can either enter the interface name or click **Select** to select it or an interface role from the list. Also configure the following:

- Traffic direction with respect to the interface—Typically, you want to select **In** so that undesired traffic is dropped before the device spends more time processing the packet.
- J

  ava applet scanning—If you enable web filtering on an interface, Java applets are inspected, which can affect performance. Typically, you want to enable Java applet scanning so that you can identify permitted and denied sources and avoid the scanning of denied applets. If you want to configure both permitted and denied sources for an interface, you must configure two rules for the interface.

c) Click **OK** to add the rule to the web filtering rules table.

Step 3 (Optional) Configure the list of exclusive domains, which define the local filtering list. This list is applied before web requests are sent to the external web filtering server (defined on the Web Filter Settings Page , on page 17). If you know there are web sites that you will always permit (such as your organization's web site) or deny, configure them in the local list. Configure as many rules as needed to define the complete list.

a) Click the **Exclusive Domains** tab and do one of the following to open the IOS Web Filter Exclusive Domain Name Dialog Box , on page 15.

- To create a new rule, right-click inside the work area and select **Add Row**.
- To edit an existing rule, right-click the rule and select **Edit Row**.

b) Select whether you are permitting or denying the specified domains, and enter the domain names or host IP addresses. You can enter either full domain names (the names of specific web sites) or partial names (for entire domains you want to treat the same way).

c) Click **OK** to add your exclusive domain rule to the policy.

Web Filter Rules Page (IOS)

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any enhancements.

Use the Web Filter Rules page for IOS devices to configure web, or URL, filtering rules. Web filtering is a type of HTTP inspection. If your access rules allow HTTP traffic on an interface, you can configure rules to apply local and server-based web filtering to prevent users from accessing undesirable web servers.

When you configure web filter rules, also configure web filter settings in the **Firewall > Settings > Web Filter** policy. The settings identify the web filtering server and contain other settings that control the overall functioning of the policy. For example, you can use the settings policy to allow all web traffic if the filtering server becomes unavailable. For more information, see Web Filter Settings Page , on page 17.

Tip You can also configure web filtering as a zone based firewall rule. For more information, see Zone-based Firewall Rules Page.

Navigation Path

To access the Web Filter Rules page for IOS devices, do one of the following:

- (Device view) Select an IOS device and select **Firewall** > **Web Filter Rules** from the Policy selector.
- (Policy view) Select **Firewall** > **Web Filter Rules (IOS)** from the Policy Type selector. Create a new policy or select an existing one.
- (Map view) Right-click an IOS device and select **Edit Firewall Policies** > **Web Filter Rules**.

Related Topics

- Understanding Web Filter Rules , on page 1
- Configuring Web Filter Rules for IOS Devices , on page 11
- Managing Firewall Web Filter Rules, on page 1

Field Reference

Table 5: Web Filter Rules Page (IOS)

Element	Description
Web Filter Rules tab	The URL filtering rules defined for the policy. Each rule shows the interface on which it is defined, whether the rule is applied to incoming or outgoing traffic, and the permitted or denied Java applet sources if Java applet scanning is enabled. You might have more than one rule for an interface if you configure both a permit and deny list for Java applet scanning. • To add a rule, click the Add Row button and fill in the IOS Web Filter Rule and Applet Scanner Dialog Box , on page 14. • To edit a rule, select it and click the Edit Row button. • To delete a rule, select it and click the Delete Row button.
Exclusive Domains tab	The local web filter list. This list is checked before web requests are sent to the filtering server and applies to all interfaces on which you configure web filtering. If you know there are specific domains that you will always allow (such as your organization's own domain name), or disallow, you can list them here. By configuring a local filter list, you can improve performance because the device does not need to wait for a response from the filtering server. • To add a domain, click the Add Row button and fill in the IOS Web Filter Exclusive Domain Name Dialog Box , on page 15. • To edit a domain, select it and click the Edit Row button. • To delete a domain, select it and click the Delete Row button.

IOS Web Filter Rule and Applet Scanner Dialog Box

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any enhancements.

Use the IOS Web Filter Rule and Applet Scanner dialog box to create web filtering rules for IOS devices.

Navigation Path

To open this dialog box, select the Web Filter Rules tab on the Web Filter Rules Page (IOS) , on page 12, click **Add Row** to create a new rule, or select a row and click **Edit Row** to edit an existing rule.

Related Topics

- Configuring Web Filter Rules for IOS Devices , on page 11
- Understanding Web Filter Rules , on page 1

Field Reference

Table 6: IOS Web Filter Rule and Applet Scanner Dialog Box

Element	Description
Enable Web Filtering	Whether to enable the web filtering rule.
Interface	The interface or interface role to which the rule is assigned. Enter the name of the interface or the interface role, or click **Select** to select the interface or role from a list, or to create a new role. An interface must already be defined to appear on the list. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. See Understanding Interface Role Objects.
Traffic Direction	The direction of the traffic to which this rule applies: • In—Packets entering an interface. • Out—Packets exiting an interface.
Java Applet Scanning Enable Java Applet Scanner	If you select **Enable Java Applet Scanning**, the device checks for the presence of Java applets in HTTP traffic coming from web servers to internal hosts. If a Java applet is present and the web server (applet source) is in the list of permitted sources, the Java applet is left unmodified in the HTTP traffic. Otherwise, the Java applets are removed from HTTP pages. **Tip** When you enable web filtering, Java applets are inspected, which can affect performance. By enabling the Java applet scanner, you can identify a list of permitted or denied sources and avoid inspection for those applets. Even if you do not want to deny any sources, enable scanning and permit the **any** source.

Element	Description
Permit Traffic Applet Sources	The list of permitted or denied source addresses for Java applets. To configure a list of permitted or denied sources: • Select either **Permit from Specified Sources** or **Deny from Specified Sources**. If you want to create both a permit and deny list, create two separate web filter rules. If you do not configure a permit list, all sources are denied. • Enter the list of permitted or denied addresses in the **Applet Sources** field. The list can include host IP addresses, network addresses, address ranges, or network/host objects, but cannot include domain names. Separate multiple addresses with commas. For more information on entering addresses, see Specifying IP Addresses During Policy Definition.

IOS Web Filter Exclusive Domain Name Dialog Box

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any enhancements.

Use the IOS Web Filter Exclusive Domain Name dialog box to configure local web filtering rules for IOS devices. You can create a list of permitted or denied domain names or IP addresses. The device checks this list before forwarding web requests to your web filtering server.

Using local filtering saves the wait time for getting a response from the server when a user requests a web site that you know you will either always permit or always deny.

Navigation Path

To open this dialog box, select the Exclusive Domains tab on the Web Filter Rules Page (IOS) , on page 12, click **Add Row** to create a new rule, or select a row and click **Edit Row** to edit an existing rule.

Related Topics

- Configuring Web Filter Rules for IOS Devices , on page 11>
- Understanding Web Filter Rules , on page 1

Field Reference

Table 7: IOS Web Filter Exclusive Domain Name Dialog Box

Element	Description
Traffic	Whether you want to permit access to the listed web sites or deny access to them.

Element	Description
Domain Name	The domain names or host IP addresses of web sites that you are permitting or denying. Separate multiple entries with commas. For domain names, you can enter a full or partial name. For example, cisco.com covers all web servers on the cisco.com domain, whereas www.cisco.com specifies only the www web server.

Configuring Settings for Web Filter Servers

Use the Web Filter settings policy to configure the web filter servers and other settings to use with your web filter rules policy. You can use Websense or Smartfilter (N2H2) filtering servers, or no external servers (for IOS devices).

You must install and configure the web filter servers as directed by the documentation for the server before configuring and deploying this policy. Security Manager cannot confirm that the servers exist or that they are configured correctly.

Tip These settings work only with the web filter rules policy. The web servers you configure here are not used with zone based firewall rules policies that configure web content filtering.

Related Topics

- Understanding Web Filter Rules , on page 1
- Configuring Web Filter Rules for ASA, PIX, and FWSM Devices , on page 2
- Configuring Web Filter Rules for IOS Devices , on page 11

Step 1 Do one of the following to open the Web Filter Settings Page , on page 17:

- (Device view) Select **Firewall** > **Settings** > **Web Filter** from the Policy selector.
- (Policy view) Select **Firewall** > **Settings** > **Web Filter** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Select the type of web filtering server you use in the **Web Filter Server Type** field, and then add the servers to the table of web filtering servers. If you have more than one server, add them in priority order; the first server in the list is the primary server.

- To add a server, click the Add Row button and fill in the Web Filter Server Configuration Dialog Box , on page 20.
- To edit a server, select it and click the Edit Row button.
- To delete a server, select it and click the Delete Row button.

Step 3 The bottom half of the settings policy includes device-specific options that you can also configure. For specific information on each setting, see Web Filter Settings Page , on page 17. The following is an overview of the settings:

- IOS devices—The most interesting setting is **Allow Traffic when Servers Unreachable**, which determines whether you allow any web connections if the filtering servers are unavailable. If you do not select this option, all web traffic is cut off if the servers go offline for any reason.

The remaining settings configure logging and cache size options.

- ASA, PIX, FWSM devices—These options configure the cache size and buffer limits used with the filtering servers. You can also control whether the cached responses include both source and destination (if you have different filtering policies per user) or destination only (one policy for all), as configured in the filtering server.

Web Filter Settings Page

Use the Web Filter settings page to configure the web filter servers and other settings to use with your web filter rules policy.

You must install and configure the web filter servers as directed by the documentation for the server before configuring and deploying this policy. Security Manager cannot confirm that the servers exist or that they are configured correctly.

Tip These settings work only with the web filter rules policy. The web servers you configure here are not used with zone based firewall rules policies that configure web content filtering.

Navigation Path

To access the Web Filter settings page, do one of the following:

- (Device view) Select a device, then select **Firewall > Settings > Web Filter** from the Policy selector.
- (Policy view) Select **Firewall > Settings > Web Filter** from the Policy Type selector. Create a new policy or select an existing one.
- (Map view) Right-click a device and select **Edit Firewall Settings > Web Filter**.

Related Topics

- Understanding Web Filter Rules , on page 1
- Configuring Settings for Web Filter Servers , on page 16
- Configuring Web Filter Rules for ASA, PIX, and FWSM Devices , on page 2
- Configuring Web Filter Rules for IOS Devices , on page 11

Field Reference

Table 8: Web Filter Page

Element	Description
Web Filter Server Type	The type of web filter server you are using: • None—You are not using web filter servers. • Websense—You use Websense servers. • Secure Computing SmartFilter/N2H2—You use Smartfilter servers. If you select this option, you can specify the server port to use for communication in the **Port** field. **Tip** If you change this setting, you are prompted to remove the existing list of servers from the table. Clicking **Yes** does not clear the table. The prompt is to remind you that the list might contain the wrong type of servers.
Web Filter Servers table	The servers that the device should use for web filtering. Enter the servers in priority order; the device uses the first one in the list until it fails to respond, and moves to the next server in the list until it gets a response. If you select None for filter type, this list is ignored. • To add a server, click the **Add Row** button and fill in the Web Filter Server Configuration Dialog Box , on page 20. • To edit a server, select it and click the **Edit Row** button. • To delete a server, select it and click the **Delete Row** button.
IOS Specific Settings	
Allow Traffic when Servers Unreachable	Whether the device should allow web traffic if the web filter servers are not responding. If you do not select this option, all web access is prevented until the servers come back online. If you allow web traffic when the servers are down, the web requests are not filtered and access to all web servers is allowed.
Enable Alerts	Whether to generate stateful packet inspection alert messages on the console.
Enable Audit Trail	Whether audit trail messages are logged to the syslog server or router.
Enable Web Filter Server Logging	Whether to send system messages to the URL filtering server for logging. The device sends a log request immediately after the URL lookup request. The log request contains the URL, hostname, source IP address, and the destination IP address. The server records the log request into its own log server so you can view this information as necessary.
Cache Size	The maximum number of destination IP addresses (and their authorization status) that can be cached in the device. The default value is 5000. When the cache reaches 80% full, the device starts removing older inactive entries.

Element	Description
Maximum Requests	The maximum number of outstanding requests that can exist at any given time. If the specified number is exceeded, new requests are dropped. The default is 1000.
Packet Buffer	The maximum number of HTTP responses that can be stored in the packet buffer of the device while it waits for the web filter server to allow or deny the request. The device drops responses when the maximum is reached. The default (and maximum) value is 200. When users make web requests, the device simultaneously sends the request to the web site and to the web filtering server. If the response from the web site is received before the server provides a permit or deny response, the device keeps the request in the packet buffer until it gets a response from the server. The response is removed from the buffer when the server responds or if the device determines that the server is unavailable and you also selected **Allow Traffic when Servers Unreachable**.
PIX/ASA/FWSM Specific Settings	
Cache Match Criteria	How to cache web requests: • Source and Destination—Cache entries are based on both the address initiating the request and the destination web address. Select this mode if users do not share the same filtering policy on the filtering server. • Destination—Cache entries are based on the destination web address. Select this mode if all users share the same filtering policy on the filtering server.
URL Buffer Memory (ASA 7.2+, PIX 7.2+ only.)	The size of the URL buffer memory pool in KB. Values are 2 to 10240.
Maximum Allowed URL Size (ASA 7.2+, PIX 7.2+ only.)	The maximum allowed URL size in KB for each URL being buffered. The possible values differ depending on server type: • Websense—From 2 to 4. • Smartfilter (N2H2)—2 or 3.
Cache Size	The size of the cache, in KB, for storing responses from the filtering server. Values are 1 to 128. Caching stores URL access privileges in memory on the security appliance. When a host requests a connection, the security appliance first looks in the URL cache for matching access privileges instead of forwarding the request to the Websense server.
URL Block Buffer Limit	The size of the buffer for storing web server responses while waiting for a filtering decision from the filtering server. The values are 1 to 128, which specifies the number of 1550-byte blocks.

Web Filter Server Configuration Dialog Box

Use the Web Filter Server Configuration dialog box to configure the external web filter servers you want to use with your Web Filter Rules policies. You can configure Websense or Smartfilter (N2H2) servers.

Navigation Path

From the Web Filter Settings Page , on page 17, click **Add Row** beneath the Web Filter Servers table, or select a row and click **Edit Row**.

Related Topics

- Configuring Settings for Web Filter Servers , on page 16
- Understanding Web Filter Rules , on page 1

Table 9: Web Filter Server Configuration Dialog Box

Element	Description
Common	
IP Address	The IP address of the web filter server.
Timeout	The length of time, in seconds, that the device will wait for a response from the web filter server. The default is 5 seconds. If the request times out, the device tries the next server, if you configure more than one.
PIX/ASA/FWSM Specific Settings	
Interface	The network interface where the authentication server resides, for example, FastEthernet0. If not specified, the default is inside. Enter the name of the interface or the interface role that identifies it, or click **Select** to select the interface or role from a list, or to create a new role. An interface must already be defined to appear on the list.
Protocol	The protocol to use when communicating with the web filtering server. Select the option for which the server is configured: • TCP (version 1) • TCP version 4 • UDP version 4
Connection Number	(Optional) The maximum number of TCP connections allowed between the device and the server.
IOS Specific Settings	
Retransmit	The number of times the device will retransmit a request when the server does not respond. The default value is two times.

Element	Description
Port	The port number that the server listens on. The default port is 15868.