

CHAPTER 7

Firewall Policy

The Firewall Policy feature lets you view and modify firewall configurations—access rules and **CBAC** inspection rules—in the context of the interfaces whose traffic they filter. Using a graphical representation of the router and its interfaces, you can choose different interfaces on the router and see whether an access rule or an inspection rule has been applied to that interface. You can also view the details of the rules displayed in the Edit Firewall Policy/ACL window.

Edit Firewall Policy/ACL

Use the Edit Firewall Policy/ACL window to view the access and inspection rules in a context that displays the interfaces the rules are associated with. Also use it to modify the access and inspection rules that are displayed.

Configure a Firewall Before Using the Firewall Policy Feature

Before using the Edit Firewall Policy/ACL window, you should perform the following tasks:

1. **Configure LAN and WAN interfaces.** You must configure the LAN and WAN interfaces before you can create a firewall. You can use the LAN and WAN wizards to configure connections for your router.
2. **Use the Firewall Wizard to configure a firewall and a DMZ.** The Firewall Wizard is the easiest way to apply access rules and inspection rules to the inside and outside interfaces you identify, and will allow you to configure a DMZ interface and specify the services that should be allowed onto the DMZ network.

3. **Come to the Firewall Policy window to edit the firewall policy you created.** After configuring LAN and WAN interfaces and creating a firewall, you can open this window and get a graphical representation of the policy in a traffic flow. You can view the access rule and inspection rule entries and make any necessary changes.

Use the Firewall Policy View Feature

After you have created the firewall, you can use the Firewall Policy View window to get a graphical view of the firewall in the context of the router interfaces, and to modify it if you need to.

For more information, click the action that you want to take:

- [Choose a Traffic Flow](#)
- [Examine the Traffic Diagram and Choose a Traffic Direction](#)
- [Make Changes to Access Rules](#)
- [Make Changes to Inspection Rules](#)

For a use case example, see [Firewall Policy Use Case Scenario](#).



Note

If the router is using a Cisco IOS image that does not support the Firewall feature set, only the Services area will be displayed, and you will only be able to create access control entries.

Apply Changes Button

Click to deliver changes you have made in this window to the router. If you leave the Edit Firewall Policy/ACL window without clicking **Apply Changes**, Cisco SDM displays a message indicating that you must either apply changes or discard them.

Discard Changes Button

Click to discard changes you have made in this window. This button does not let you remove changes that you have delivered to the router using the **Apply Changes** button.

Choose a Traffic Flow


Traffic flow refers to traffic that enters the router on a specified interface (the *from* interface) and exits the router on a specified interface (the *to* interface). The Cisco SDM traffic-flow display controls are located in a row at the top of the Edit Firewall Policy/ACL window.



Note

There must be at least two configured interfaces on the router. If there is only one, Cisco SDM will display a message telling you to configure an additional interface.

The following table defines the Cisco SDM traffic-flow display controls.

From	Choose the interface from which the traffic flow you are interested in originates. The firewall will protect the network connected to the From interface. The From drop-down list contains only interfaces with configured IP addresses.
To	Choose the interface out of which the traffic will leave the router. The To drop-down list contains only interfaces with configured IP addresses.
	Details button. Click to view details about the interface. Details such as IP address, encapsulation type, associated IPsec policy, and authentication type are provided.
Go button	Click to update the traffic-flow diagram with information about the interfaces you have chosen. The diagram is not updated until you click Go . The Go button is disabled if you have not chosen a From interface or a To interface, or if the From and To interfaces are the same.
View Option	Choose Swap From and To interface to swap the interfaces that you originally chose in the From and To drop-down lists. You can use the swap option if you want to create a firewall protecting both the network connected to the From interface and the network connected to the To interface. You can choose View all Access control lists in traffic flow when one access rule has been applied to the From interface and another access rule has been applied to the To interface for a traffic direction you have chosen. The entries of both access rules are displayed in another window.

Cisco SDM displays interfaces that have IP addresses in alphabetical order in both the **From** and **To** drop-down lists. By default, Cisco SDM chooses the first interface in the **From** list, and the second interface in the **To** list. Use the **From** and **To** drop-down lists to choose a different traffic flow. The chosen traffic flow is displayed in the traffic diagram below the traffic-flow display controls.

For example, to view traffic flow from a network connected to the router interface Ethernet 0 and exiting on the router interface Serial 0, follow these steps:

-
- Step 1** Choose Ethernet 0 in the **From** drop-down list.
 - Step 2** Choose Serial 0 in the **To** drop-down list.
 - Step 3** Click **Go**.
 - Step 4** To switch the interfaces in the **From** and **To** drop-down lists, choose **Swap From and To interface** from the View Option drop-down list.

Access rules applied to originating and returning traffic may be different. To learn more about how to switch between displaying originating and returning traffic in the traffic diagram, see [Examine the Traffic Diagram and Choose a Traffic Direction](#).

- Step 5** Click the **Details** button next to the **From** or **To** drop-down list to open a window showing an interface's IP address, IPSec policy, and other information.
-

To work with the traffic diagram, see [Examine the Traffic Diagram and Choose a Traffic Direction](#). To return to the main Firewall Policy window description see [Edit Firewall Policy/ACL](#).

Examine the Traffic Diagram and Choose a Traffic Direction

The traffic diagram displays the router with the chosen From and To interfaces (see [Choose a Traffic Flow](#) for more information). It also displays the types of rules applied for the chosen traffic flow, as well as the direction in which they have been applied.

Originating Traffic




Click to highlight the traffic flow that enters the router at the From interface and exits the router at the To interface. When this area is highlighted, you can see the details of rules applied in the direction of traffic flow.

Returning Traffic

Click to highlight the traffic flow that enters the router on the To interface and exits the router on the From interface. When this area is highlighted, you can see the details of rules applied to returning traffic.

Icons

Rules are represented by icons in the traffic flow:

	A filter symbol indicates that an access rule is being applied.
	A magnifying glass indicates that an inspection rule is being applied.
	<p>A firewall icon in the router indicates that a firewall has been applied to the Originating traffic flow. Cisco SDM displays a firewall icon if the following sets of criteria are met:</p> <ul style="list-style-type: none"> • There is an inspection rule applied to Originating traffic on the inbound direction of the From interface, and there is an access rule applied to the inbound direction of the To interface. • The access rule on the inbound direction of the To interface is an extended access rule, and contains at least one access rule entry. <p>No firewall icon is displayed when a firewall has been applied to Returning traffic. If the Firewall feature is available, but no firewall has been applied to the traffic flow, IOS Firewall: Inactive will be displayed underneath the traffic diagram.</p>

	Rules applied to Originating traffic are indicated by a right arrow. An icon on the From interface traffic line indicates the presence of a rule filtering traffic inbound to the router. An icon placed on the To interface traffic line indicates a rule filtering traffic outbound from the router. If you place the mouse over this icon, Cisco SDM will display the names of the rules that have been applied.
	Rules applied to Returning traffic are indicated by a left arrow. An icon on the To interface traffic line indicates the presence of a rule filtering traffic inbound to the router. An icon on the From interface traffic line indicates the presence of a rule filtering traffic outbound from the router. The names of the rules applied are displayed when you place the cursor over this icon.

**Note**

Although the icons are shown on a particular interface in the diagram, a firewall policy might contain access control entries that affect traffic not represented by the diagram. For example, an entry that contains the wildcard icon in the Destination column (see [Make Changes to Access Rules](#)) might apply to traffic exiting interfaces other than the one represented by the currently chosen To interface. The wildcard icon appears as an asterisk and stands for any network or host.


To make changes to an access rule, see [Make Changes to Access Rules](#). To return to the main Firewall Policy window description see [Edit Firewall Policy/ACL](#).

Make Changes to Access Rules

The policy panel shows the details of the rules applied to the chosen traffic flow. The Policy panel is updated when the From and To interfaces are chosen and when the Traffic Diagram is toggled between Originating Traffic focus and Returning Traffic focus.

The Policy panel is blank if an access rule that contains no entries has been associated with an interface. For example, if a rule name was associated with an interface using the CLI, but entries for the rule were not created, this panel would be blank. If the Policy Panel is blank, you can use the **Add** button to create entries for the rule.


Service Area Header Fields


Firewall Feature Availability	If the Cisco IOS image that the router is using supports the Firewall feature, this field contains the value Available .
Access Rule	The name or number of the access rule whose entries are being displayed.
Inspection Rule	The name of the inspection rule whose entries are being displayed.
	This icon appears when an access rule has been associated with an interface, but no access rule of that name or number has been created. Cisco SDM informs you that the policy has no effect unless there is at least one access rule entry.

Service Area Controls

The following table describes the controls found in the Service Area.

Add button	Click to add an access rule entry. Specify whether you want to add the entry before or after the entry currently chosen. Then, create the entry in the Add an Entry window. Remember that the order of entries is important. Cisco SDM displays the Extended entry dialog when you add an entry from the Edit Firewall Policy/ACL window. To add a standard rule entry, go to Additional Tasks > ACL Editor > Access Rules .
Edit button	Click to edit a chosen access rule entry. Although you can only add extended rule entries in the Edit Firewall Policy/ACL window, you are not prevented from editing a standard rule entry that has already been applied to a chosen interface.












Cut button	Click to remove a chosen access rule entry. The entry is placed on the clipboard and can be pasted to another position in the list, or it can be pasted to another access rule. If you want to reorder an entry, you can cut the entry from one location, choose an entry before or after the location that you want for the cut entry, and click Paste . The Paste context menu allows you to place the entry before or after the entry you chose.
Copy button	Choose a rule entry and click to put the rule entry on the clipboard.
Paste button	Click to paste an entry on the clipboard to the chosen rule. You will be prompted to specify whether you want to paste the entry before or after the currently chosen entry. If Cisco SDM determines that an identical entry already exists in the access rule, it displays the Add an Extended Rule Entry window so that you can modify the entry. Cisco SDM does not allow duplicate entries in the same access rule.
Interface drop-down list	If the chosen traffic flow (Originating or Returning) contains an access rule on both the From interface and the To interface, you can use this list to toggle between the two rules.
 Apply Firewall	If the chosen traffic flow does not have a firewall applied, you can apply a firewall by choosing Originating traffic and clicking the Apply Firewall button. By default, clicking Apply Firewall will associate an Cisco SDM-default inspection rule to the inbound direction of the From interface, and will associate an access rule to the inbound direction of the To interface that denies traffic. If the Cisco IOS image that the router is using does not support the Firewall feature, this button is disabled. For example, to apply a firewall that protects the network connected to the Ethernet 0 interface from traffic entering the Ethernet 1 interface, choose Ethernet 0 from the From drop-down list, and Ethernet 1 from the To drop-down list. Then click Apply Firewall . If you want to apply a firewall that protects the network connected to the Ethernet 1 interface from traffic entering the Ethernet 0 interface, go to Additional Tasks > ACL Editor > Access Rules .

Service area buttons are disabled if the rule is read-only. A rule is read-only when it contains syntax that Cisco SDM does not support. Read-only rules are indicated by this icon: .

If there is an existing standard rule that filters the returning traffic flow to which you are applying the firewall, Cisco SDM informs you that it will convert the standard access rule to an extended rule.

Service Area Entry Fields

The following table describes the icons and other data in the Service Area entries.

Field	Description	Icons	Meaning
Action	Whether the traffic will be permitted or denied		Permit source traffic
			Deny source traffic
Source/ Destination	Network or host address, or any host or network.		The address of a network
			The address of a host
			Any network or host
Service	Type of service filtered.		Examples: TCP, EIGRP, UDP, GRE. See IP Services .
			Examples: Telnet, http, FTP. See TCP Services .
			Examples: SNMP, bootpc, RIP. See UDP Services .
			Internet Group Management Protocol (IGMP).
			Examples: echo-reply, host-unreachable. See ICMP Message Types .
Log	Whether or not denied traffic is logged.		Log denied traffic. To configure logging for firewalls see Firewall Log .

Field	Description	Icons	Meaning
Option	Options configured using the CLI	No icons.	
Description	Any description provided.	No icons	

To make changes to inspection rules, see [Make Changes to Inspection Rules](#). To return to the main Firewall Policy window description see [Edit Firewall Policy/ACL](#).

Make Changes to Inspection Rules

The Applications area appears if the Cisco IOS image running on the router supports [CBAC](#) Inspection rules. The Applications area displays the inspection rule entries that are filtering the traffic flow, and is updated whenever a new traffic flow is chosen. The inspection rule that affects the chosen direction of traffic is displayed.

The Applications area will display one of the following for **Originating traffic**:

- The inspection rule that is applied to the inbound direction of the From interface, if one exists.
- The inspection rule that is applied to the outbound direction of the To interface, if the inbound direction of the From interface has no inspection rule applied.

Swap From and To Interfaces to Bring Other Rules into View

Inspection rules applied to **Returning traffic** are not displayed. You can display an inspection rule applied to **Returning traffic** by choosing **Swap From and To interfaces** in the View Options menu. You can also view inspection rules that are not displayed in the Edit Firewall Policy/ACL window by going to the Application Security window in the Firewall and ACL task.



This icon appears when two inspection rules are found in the chosen traffic direction. Cisco SDM also displays a warning dialog, giving you the opportunity to dissociate one of the inspection rules from the interface.

Application Area Controls

The following is a list of Application area controls:

Add—Click to add an inspection rule. If there is no inspection rule, you can add the Cisco SDM default inspection rule, or you can create and add a custom inspection rule. If you add the Cisco SDM default inspection rule to a traffic flow with no inspection rule, it will be associated with the inbound traffic to the From interface. You can add an entry for a specific application whether or not an inspection rule already exists.

Edit—Click to edit a chosen entry.

Delete—Click to delete a chosen entry.

Global Settings—Click to display a dialog box that enables you to set global timeouts and thresholds.

Summary—Click to display the application or protocol name and a description for each entry.

Detail—Click to display the application or protocol name, description, alert status, audit trail status, and timeout settings for each entry.

Application Area entry fields

The following list describes the Application area entry fields:

Application Protocol—Displays the name of the application or protocol. For example, **vdolive**.

Alert—Indicates whether or not an alert is on (default) or off.

Audit Trail—Indicates whether or not audit trail is on or off (default).

Timeout—Displays how long, in seconds, the router waits before blocking return traffic for this protocol or application.

Description—Displays a short description. For example, **VDOLive protocol**.

To return to the main Firewall Policy window description see [Edit Firewall Policy/ACL](#).

Add *App-Name* Application Entry

Use this window to add an application entry that you want the Cisco IOS firewall to inspect.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value for the protocol or application.

Add *rpc* Application Entry

Add a Remote Procedure Call (RPC) program number in this window, and specify Alert, Audit, Timeout, and Wait time settings.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Program Number

Enter a single program number in this field.

Wait Time

You can optionally specify how many minutes to allow subsequent RPC connections from the same source to be made to the same destination address and port. The default wait time is zero minutes.

Add Fragment application entry

In this window, you can add a fragment entry to an inspection rule that you are configuring in the Edit Firewall Policy/ACL window, and you can specify Alert, Audit, and Timeout settings. A fragment entry sets the maximum number of unreassembled packets that the router should accept before dropping them.

Alert Action

Choose one of the following:

- **default(on)**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default(off)**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Range (optional)

Enter the maximum number of unreassembled packets the router should accept before dropping them. The range can have a value between 50 and 10000.

Add or Edit http Application Entry

Use this window to add an http application to the inspection rule.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Hosts/network for Java applet download

The source hosts or networks whose applet traffic is to be inspected. Multiple hosts and networks can be specified.

Click **Add** to display the Java Applet Blocking window in which you can specify a host or network.

Click **Delete** to remove an entry from the list.

Java Applet Blocking

Use this window to specify whether Java applets from a specified network or host should be permitted or denied.

Action

Choose one of the following:

- **Do Not Block (Permit)**—Permit Java applets from this network or host.
- **Block (Deny)**—Deny Java applets from this network or host.

Host/Network

Specify the network or the host.

Type

Choose one of the following:

- **A Network**—If you choose this, provide a network address in the IP address field. Note that the wildcard mask enables you to enter a network number that may specify multiple subnets.
- **A Host Name or IP Address**—If you choose this, provide a host IP address or host name in the next field.
- **Any IP address**—If you choose this, the action you specified is to apply to any host or network.

IP Address/Wildcard Mask

Enter a network address and then the wildcard mask to specify how much of the network address must match exactly.

For example, if you entered a network address of 10.25.29.0 and a wildcard mask of 0.0.0.255, any Java applet with a source address containing 10.25.29 would be filtered. If the wildcard mask were 0.0.255.255, any Java applet with a source address containing 10.25 would be filtered.

Host Name/IP

This field appears if you chose **A Host Name or IP Address** as Type. If you enter a host name, ensure that there is a DNS server on the network that can resolve the host name to an IP address.

Cisco SDM Warning: Inspection Rule

This window is displayed when Cisco SDM finds two inspection rules have been configured for a direction in a traffic flow. For example, you might have one inspection rule applied to traffic inbound on the From interface, and another applied to traffic outbound on the To interface. Two inspection rules may not harm the functioning of the router, but they may be unnecessary. Cisco SDM allows you to keep the inspection rules the way they are, to remove the inspection rule on the From interface, or to remove the inspection rule on the To interface.

- **Do not make any change**—Cisco SDM will not remove either inspection rule.

- **Keep inspection rule *name* on <interface-name> inbound, and dissociate inspection rule *name* on <interface-name> outbound**—Cisco SDM will keep one inspection rule, and dissociate the rule from the other interface.
- **Keep inspection rule *name* on <interface-name> outbound and dissociate inspection rule *name* on <interface-name> inbound**—Cisco SDM will keep one inspection rule, and dissociate the rule from the other interface.

Before you make a selection and click **OK**, you may want to click **Cancel**, then determine if you need to add entries to the inspection rule you want to retain. You can add entries by using the **Add** button in the Application area toolbar in the Edit Firewall Policy/ACL window.

Cisco SDM Warning: Firewall

This window appears when you click **Apply Firewall** in the Edit Firewall Policy/ACL window. It lists the interfaces to which it will apply a rule, and describes the rule that it will apply.

Example:

```
SDM will apply firewall configuration to the following interfaces:  
Inside (Trusted) Interface: FastEthernet 0/0  
* Apply inbound default SDM Inspection rule  
* Apply inbound ACL. Anti-spoofing, broadcast, local loopback, etc.).  
  
Outside (Untrusted) Interface: Serial 1/0  
* Apply inbound access list to deny returning traffic.
```

Click **OK** to accept these changes, or click **Cancel** to stop the application of the firewall.

Edit Firewall Policy

The Edit Firewall Policy window provides a graphical view of the firewall policies on the router and enables you to add ACLs to policies without leaving the window. Read the procedures in the sections that follow to see how to view the information in this window and add rules.

Things You Must do Before Viewing Information in this Window

This window is empty if no [zone](#), [zone-pairs](#), or [policy maps](#) have been configured. Create a basic configuration containing these elements by going to **Configure > Firewall and ACL > Create Firewall** and completing the Advanced Firewall wizard. After you have done this, you can create additional zones, zone pairs and policies as needed by going to **Configure > Additional Tasks > Zones** to configure zones, and to **Additional Tasks > Zone Pairs** to configure additional zone pairs. To create the policy maps that the zone pairs are to use, go to **Configure > Additional Tasks > C3PL**. Click the **Policy Map** branch to display additional branches which enable you to create policy maps and the class maps that define traffic for the policy maps.

Expanding and Collapsing the Display of a Policy

When the display of a policy is collapsed, only the policy name and the source and destination zones are displayed. To expand the display of the policy to show the rules that make up the policy, click the + button to the left of the policy name. An expanded view of a firewall policy might look similar to the following:

ID	Traffic Classification			Action	Rule Options
	Source	Destination	Service		
clients-servers-policy (clients to servers)					
1	any	any	tcp	Permit Firewall	
			udp		
			icmp		
2	Unmatched Traffic			Drop	

The policy named clients-servers-policy contains two [ACLs](#). The rule with the ID 1 permits [TCP](#), [UDP](#), and [ICMP](#) traffic from any source to any destination. The rule with the ID 2 drops any unmatched traffic.

Adding a New Rule to a Policy

To add a new rule to a policy, complete the following steps:

-
- Step 1** Click anywhere in the display for that policy, and click the **+ Add** button.
- To insert a rule for new traffic in the order that you want it select an existing rule, click the **+ Add** button, and choose **Insert** or **Insert After**. The Insert and Insert After options are also available from a context menu that you display by right-clicking on an existing rule.
 - Choosing **Rule for New Traffic** automatically places the new rule at the top of the list.
 - Choosing **Rule for Existing Traffic** allows you to select an existing class map and modify it. It automatically places the new rule at the top of the list.
- Step 2** Complete the displayed dialog. Click [Add a New Rule](#) for more information.
-

Reordering Rules within a Policy

If a policy contains more than one rule that permits traffic, you can reorder them by selecting a rule and clicking the **Move Up** button or the **Move Down** button. The Move Up button is disabled if you selected a rule that is already at the top of the list, or if you selected the Unmatched Traffic rule. The Move Down button is disabled if you selected a rule that is already at the bottom of the list.

You can also use the Cut and the Paste buttons to reorder rules. To remove a rule from its current position, select it and click **Cut**. To place the rule in a new position, select an existing rule, click **Paste**, and choose **Paste** or **Paste After**.

The Move Up, Move Down, Cut, Paste, and Paste After operations are also available from the context menu displayed when you right-click on a rule.

Copying and Pasting a Rule

Copying and pasting a rule is very useful if one policy contains a rule that can be used with few or no modifications in another policy.

To copy a rule, select a rule and click the **Copy** button or right-click the rule and choose **Copy**. To paste the rule to a new location, click **Paste** and choose **Paste** or **Paste After**. The Paste and Paste After buttons are also available from the context menu. When you paste a rule to a new location, the [Add a New Rule](#) dialog is displayed so you can make changes to the rule if you need to.

Displaying the Rule Flow Diagram

Click anywhere in a firewall policy and click Rule Diagram to display the Rule Flow Diagram for that policy. The Rule Flow Diagram displays the source zone on the right of the router icon, and the destination zone on the left of the icon.

Applying Your Changes

To send your changes to the router, click **Apply Changes** at the bottom of the screen.

Discarding Your Changes

To discard changes that you have made but have not sent to the router, click **Discard Changes** at the bottom of the screen.

Add a New Rule

Define a traffic flow and specify protocols to inspect in the Add a Rule window. Complete the following steps to add a new rule.

-
- Step 1** In the Source and Destination field, specify that the traffic is flowing between a network and another network by choosing **Network**, or that the traffic is flowing between entities that may be networks or may be individual hosts by choosing **Any**.
 - Step 2** Enter a name for the traffic flow in the Traffic Name field.
 - Step 3** Click **Add** next to the Source Network and Destination Network columns and add source and destination network addresses. You can add multiple entries for the source and destination networks, and you can edit an existing entry by selecting it and clicking **Edit**.
 - Step 4** Reorder an entry if necessary by selecting it and clicking **Move Up** or **Move Down**. The Move Up button is disabled when the selected entry is already at the top of the list. The Move Down button is disabled when the selected entry is already at the bottom of the list.
 - Step 5** Enter a name that describes the protocols or services that you are identifying for inspection in the Service Name field.

- Step 6** Add a service by clicking on a branch in the tree in the left-hand column, choosing the service, and clicking **Add>>**. Click the **+** icon next to a branch to display to display the available services of that type. To remove a service from the right-hand column, select it and click **<<Remove**.
- Step 7** Specify how you want the traffic handled by choosing **Permit Firewall**, **Permit ACL**, or **Drop** in the Action field. If you choose **Permit Firewall**, you can click **Advanced** and choose a menu item if you want to further define the action, such as inspecting the protocols that you chose in the service box. See the following help topics for more information:
- [Application Inspection](#)
 - [URL Filter](#)
 - [Quality of Service](#)
 - [Inspect Parameter](#)
- Step 8** If you chose **Drop** as the action, you can click **Log** to have the event logged.
- Step 9** Click **OK** to close this dialog and send the changes to the router.
-

Add Traffic

Use the Add Traffic dialog to create a source and destination address entry for a rule.

Action

Use the Include or the Exclude option to specify whether you want the rule to apply to the traffic exchanged between the source and destination addresses.

Choose **Include** to include this traffic in the rule.

Choose **Exclude** to have this traffic excluded from the rule.

Source Host/Network and Destination Host/Network

Specify the source and the destination of the traffic in these fields.

Type

Choose one of the following values:

- Any IP Address—Choose if you do now want to limit the source or destination traffic to any host or network.
- A Network—Choose if you want to specify a network address as the source or destination, and specify the network address in the IP Address and Wildcard Mask fields.
- A Host Name or IP Address—Choose if you want to specify the name or IP address of a host. Then, specify the host in the Host Name/IP field.

IP Address

Enter the network address. This field is displayed when you choose **A Network** in the Type field.

Wildcard Mask

Enter the wildcard mask that specifies the bits that are used for the network address. For example, if the network address is 192.168.3.0, specify 0.0.0.255 as the mask. This field is displayed when you choose **A Network** in the Type field.

Host Name/IP

Enter the name or the IP address of a host in this field. If you enter a name, the router must be able to contact a DNS server to resolve the name to an IP address. This field is displayed when you choose **A Host Name or IP Address** in the Type field.

Application Inspection

Configure deep packet inspection for any of the applications or protocols listed in this screen by checking the box next to the application or protocol, clicking the button to the right of the field, and choosing **Create** or **Select** from the context menu. Choose **Create** to configure a new policy map. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.

For example, to create a new policy map for Instant Messaging, check the box next to IM, click the button next to the IM field, and choose **Create**. Then, create the policy map in the Configure Deep Packet Inspection dialog.

URL Filter

Add an URL filter by choosing an existing URL filter from the URL Filter Name list, or by clicking **Create New** and making a new URL filter in the dialogs displayed. The settings for the URL filter that you chose or created are summarized in this dialog.

Quality of Service

You can drop traffic that exceeds a specified rate per second, the [police rate](#), and drop traffic that exceeds a specified burst value. The police rate can be a value between 8,000 and 2,000,000,000 bits per second. The [burst rate](#) can be a value between 1,000 and 512,000,000 bytes.

Inspect Parameter

Specify an existing [parameter map](#) in the Inspect Parameter window by choosing a parameter map in the Inspect Parameter Map list, or click **Create New** to create a new parameter map to apply to the rule for the policy you are modifying. The details of the parameter map that you specify are displayed in the Preview box.

To learn about parameter maps, click [Timeouts and Thresholds for Inspect Parameter Maps and CBAC](#).

Select Traffic

Select a class map that specifies the traffic that you want to add to the policy. To view more information about a particular class map, select the class map and click **View Details**.

When you click **OK**, the Add a New Rule dialog is displayed, with the information in the class map that you chose. You can make additional changes to the class map or leave it unchanged. If you do make changes, you can change the name of the class map if you do not want your changes to apply to other policies that use the original class map.

Delete Rule

This dialog is displayed when you delete a rule that contains a [class map](#) or [ACL](#) that you might want to delete along with the rule or keep for use in other rules.

Automatically delete class maps and ACLs used by this rule

Click this option to remove the class maps and ACLs that are part of this rule. They will be removed from the router configuration and not be available for use by other rules.

I will delete the unused class maps and ACLs later

Click this option to remove the rule but retain the class maps and ACLs. You can keep them for use in other parts of the firewall configuration.

View Details

Click **View Details** to display the names of the class maps and ACLs that are associated with the rule you are deleting. The dialog expands to show the details. When you click View Details, the button name becomes Hide Details.

Hide Details

Click **Hide Details** to close the details portion of the dialog. When you click Hide Details, the button name becomes View Details.

Manually Deleting Class Maps

To manually delete a class map, complete the following steps.

-
- Step 1** Go to **Configure > Additional Tasks > C3PL > Class Maps**.
 - Step 2** Click the node for the type of class map that you are deleting.
 - Step 3** Select the name of the class map that was displayed in the View Details window and click **Delete**.
-

Manually Deleting ACLs

To manually delete a class map, complete the following steps.

-
- Step 1** Go to **Configure > Additional Tasks > ACL Editor**.
 - Step 2** Click the node for the type of ACL that you are deleting.
 - Step 3** Select the name or number of the ACL that was displayed in the View Details window and click **Delete**.
-

