



CHAPTER 21

Configuring Service Policy Rules

This chapter describes how to enable service policy rules. Service policy rules define how specific types of application inspection are applied to different types of traffic that is received by the security appliance. You apply a specific rule to an interface or globally to every interface.

- [Service Policy Rules, page 21-1](#)
- [SUNRPC Server, page 21-34](#)

Service Policy Rules

Some applications require special handling by the security appliance and specific application inspection engines are provided for this purpose. Applications that require special application inspection engines are those that embed IP addressing information in the user data packet or open secondary channels on dynamically assigned ports. Application inspection is enabled by default for many protocols, while it is disabled for other protocols. In many cases, you can change the port on which the application inspection listens for traffic.

Application inspection engines work with NAT to help identify the location of embedded addressing information. This allows NAT to translate these embedded addresses and to update any checksum or other fields that are affected by the translation.

Service policy rules define how specific types of application inspection are applied to different types of traffic that is received by the security appliance. You apply a specific rule to an interface or globally to every interface.

Use traffic match criteria to define the set of traffic to which you want to apply application inspection. For example, TCP traffic with a port value of 23 might be classified as the Telnet traffic class. You can use the traffic class to change the default port for application inspection for protocols where this is permitted.

Multiple traffic match criteria can be assigned to a single interface, but a packet will only match the first criteria within a specific service policy rule.

Fields

- **Add**—Adds a new service policy rule. Choose the type of rule you want to add from the drop-down list.
- **Edit**—Edits a service policy rule.
- **Delete**—Deletes a service policy rule.
- **Move Up**—Moves a rule up. Rules are assessed in the order they appear in this table, so the order can matter if you have overlapping rules.

- Move Down—Moves a rule down.
- Cut—Cuts a rule.
- Copy—Copies the parameters of a rule so you can start a new rule with the same parameters using the Paste button.
- Paste—Opens an Add/Edit Rule dialog box with the copied or cut parameters of a rule prefilled. You can then make any modifications and add it to the table. The Paste button adds the rule above the selected rule. The Paste After item, available from the Paste drop-down list, adds the rule after the selected rule.
- Find—Filters the display to show only matching rules. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
 - Filter drop-down list—Choose the criteria to filter on, either Interface, Source, Destination, Service, or Rule Query. A rule query is a collection of multiple criteria that you can save and use repeatedly.
 - Filter field—For the Interface type, this field becomes a drop-down list so you can choose an interface name, or **All Interfaces**. For the Rule Query type, the drop-down list includes all defined rule queries. The Source and Destination types accept an IP address. You can type one manually, or browse for one by clicking the ... button and launching the Browse Address dialog box. The Service type accepts a TCP, UDP, TCP-UDP, ICMP, or IP protocol type. You can type one manually, or browse for one by clicking the ... button and launching the Browse Service Groups dialog box.
 - Filter—Runs the filter.
 - Clear—Clears the Filter field.
 - Rule Query—Opens the Rule Queries dialog box so you can manage named rule queries.
- Show Rule Flow Diagram—Shows the Rule Flow Diagram area under the rule table. This diagram shows the networks, type of traffic, interface name, direction of flow, and action.
- Packet Trace—Opens the Packet Tracer tool with the parameters pre-filled with the characteristics of the selected rule.

The following description summarizes the columns in the Service Policy Rules table. You can edit the contents of these columns by double-clicking on a table cell. Double-clicking on a column header sorts the table in ascending alphanumeric order, using the selected column as the sort key. If you right-click a rule, you see all of the options represented by the buttons above, as well as Insert and Insert After items. These items either insert a new rule before the selected rule (Insert) or after the selected rule (Insert After.)

- **Name**—Indicates the name of the rule.
- **No**—Indicates the order of evaluation for the rule.
- **Enabled**—Indicates whether the rule is enabled or disabled.
- **Match**—Indicates if the criteria are used to include (match) or exclude (do not match) traffic.
- **Source**—Lists the IP addresses that are subject to service policy when traffic is sent to the IP addresses listed in the Destination column.
- **Destination**—Lists the IP addresses that are subject to service policy when traffic is sent from the IP addresses listed in the Source column.
- **Service**—Shows the service or protocol specified by the rule.
- **Time**—Displays the time range during which the rule is applied.
- **Rule Actions**—Shows the actions applied by the rule.

- **Description**—The description you entered when you added the rule.

Modes

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

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

Service Policy

The **Service Policy** dialog box lets you add a new service policy rule, apply the rule to a specific interface, or apply the rule globally to all interfaces.

Fields

- **Create a service policy and apply to** area
 - **Interface**—Applies the rule to a specific interface. This selection is required if you want to match traffic based on the source or destination IP address using an access list.
 - **Interface**—Specifies the interface to which the rule applies.
 - **Policy Name**—Specifies the name of the interface service policy.
 - **Description**—Provides a text description of the policy.
 - **Global - applies to all interfaces**—Applies the rule to all interfaces. This selection is not compatible with matching traffic based on the source or destination IP address using an access list.
 - **Policy Name**—Specifies the name of the global service policy. Only one global service policy is allowed and it cannot be renamed.
 - **Description**—Provides a text description of the policy.

Modes

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

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

Edit Service Policy

The **Edit Service Policy** dialog box lets you change the description for the selected service policy.

Fields

- **Description**—Provides a text description of the service policy.

Modes

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

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

Traffic Classification Criteria

The **Traffic Classification** tab on the **Edit Service Policy Rule** screen lets you specify the criteria you want to use to match traffic to which the security policy rule applies.

Fields

- **Name**—Identifies the name of the traffic class.
- **Description (optional)**—Provides a text description of the new traffic class.
- **Traffic match criteria** area:
 - **Default Inspection Traffic**—Uses the criteria specified in the default inspection traffic policy.
 - **Source and Destination IP Address (uses ACL)**—Matches traffic based on the source and destination IP address, using an ACL. This selection is only available if you apply the rule to a specific interface using an Interface Service Policy.
 - **Tunnel Group**—Matches traffic based on the tunnel group.
 - **TCP or UDP Destination Port**—Matches traffic based on the TCP or UDP destination port.
 - **RTP Range**—Matches traffic based on a range of RTP ports.
 - **IP DiffServ CodePoints (DSCP)**—Matches traffic based on the Differentiated Services model of QoS.
 - **IP Precedence**—Matches traffic based on the IP precedence model of QoS.
 - **Any traffic**—Matches all traffic regardless of the traffic type.
- **Add rule to existing traffic class**—Adds the rule to the existing traffic class that is selected in the drop-down list.
- **Use class-default as the traffic class**—Specifies that the class-default traffic class is used when traffic does not match any other traffic class.

Modes

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

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

Default Inspections

The **Default Inspections** dialog box lists the default port assignments that are used when you select the **Default Inspection Traffic** criteria on the **Traffic Classification Criteria** dialog box.

- **Service**—This lists the application inspection engine type.
- **Protocol**—This identifies whether the application inspection uses TCP or UDP for the transport protocol.
- **Port**—This identifies the port number used by the Default Inspection Traffic criteria.

Management Type Traffic Class and Action

The Management Class dialog box lets you configure the management traffic classification and define actions for the classified traffic.

Fields

- **Name**—Identifies the name of the traffic management class.
- **Description (optional)**—Provides a text description of the new traffic management class.
- **Match on Destination Port** area:
 - **Protocol**—Matches traffic based on the TCP or UDP destination port.
 - **Service**—Choose the = (equal) operator or range to specify a range of ports. Either type a number, or choose a well-known port name from the drop-down list. For a range, you must specify numbers.
- **Protocol Inspection area:**
 - **RADIUS Accounting Map**—Choose a **defined RADIUS accounting map** from the drop-down list.
- **Configure**—Opens the Select RADIUS Accounting Map dialog box to select a defined RADIUS accounting map or add a RADIUS accounting map or for fine control over inspection.

Modes

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

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

Select RADIUS Accounting Map

The Select RADIUS Accounting Map dialog box lets you select a defined RADIUS accounting map or define a new one.

Fields

- **Add**—Lets you add a new RADIUS accounting map.

Modes

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

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

Add RADIUS Accounting Policy Map

The Add RADIUS Accounting Policy Map dialog box lets you add the basic settings for the RADIUS accounting map.

Fields

- **Name**—Enter the name of the previously configured RADIUS accounting map.
- **Description**—Enter the description of the RADIUS accounting map, up to 100 characters in length.
- **Host Parameters tab**:
 - **Host IP Address**—Specify the IP address of the host that is sending the RADIUS messages.
 - **Key: (optional)**—Specify the key.
 - **Add**—Adds the host entry to the Host table.
 - **Delete**—Deletes the host entry from the Host table.
- **Other Parameters tab**:
 - **Attribute Number**—Specify the attribute number to validate when an Accounting Start is received.
 - **Add**—Adds the entry to the Attribute table.
 - **Delete**—Deletes the entry from the Attribute table.
 - **Send response to the originator of the RADIUS message**—Sends a message back to the host from which the RADIUS message was sent.
 - **Enforce timeout**—Enables the timeout for users.
- **Users Timeout**—Timeout for the users in the database (hh:mm:ss).

Modes

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

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

Using Default Inspection Traffic Criteria

The **fixup** command, which is available in PIX Firewall Version 6.3 and earlier releases, provided a simple, global policy for application inspection. The Modular Policy Framework provides a much more granular method of inspecting traffic. Modular Policy Framework lets you select the traffic for a specific application inspection and this can improve the performance of the security appliance. Performance is improved because the application inspection engine only inspects a limited amount of traffic.

To simplify enabling application inspection on the default ports, use the default inspection traffic criteria. When you specify the default inspection traffic criteria the security appliance selects traffic for application inspection on the well-known port for each protocol. [Table 21-1](#) lists the default port assignments for each protocol.

Table 21-1 Default Port Assignments

Protocol Name	Protocol	Source Port	Destination Port
ctiqbe	tcp	N/A	2748
dns	udp	53	53
esmtpt/smtpt	tcp	N/A	25
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
http	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
pptp	tcp	1723	1723
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sip	tcp, udp	N/A	5060
skinny	tcp	N/A	2000
sqlnet	tcp	N/A	1521
sunrpc	udp	111	111
tftp	udp	N/A	69
xdmcp	udp	177	177

When you select the default inspection traffic criteria, you can then enable each protocol on the **Protocol Inspection** tab of the **Rule Actions** screen. The protocol will be enabled on its default port. You can restrict inspection to a specific flow by using the **Source and destination IP address (uses ACL)** button and selecting specific criteria, such as **Source Host/Network** or **Destination Host/Network** from the **Service Policy Rule** screen.

**Note**

The default inspection traffic criteria override any port settings in the Protocol and Service group box. That means that you cannot change any of the default port assignments for any protocol when the default inspection traffic criteria are used.

The inspection_default security policy is a preconfigured global policy that enables application inspection using the default inspection traffic criteria. This global policy is enabled in the security appliance factory default configuration.

**Note**

When you specify the default inspection traffic as the traffic match criteria, only inspect rule actions can be applied in the security policy for the specified interface. Actions on the QoS and Connection Settings tabs cannot be applied.

Changing Default Ports for Application Inspection

The default inspection traffic criteria override any port settings in the Protocol and Service group box. That means that you cannot change any of the default port assignments for any protocol when the default inspection traffic criteria are used.

To change the default port assignment for any protocol, you must manually configure and enable each inspection engine.

To use Modular Policy Framework for changing the default port assignment for a protocol, perform the following steps:

-
- Step 1** Click **Service Policy Rules** on the **Security Policy** panel and then click **Add**.
The **Add Service Policy Rule Wizard - Service Policy** screen appears.
- Step 2** Create a service policy.
To create a security policy for a specific interface, on the **Create a service policy and apply to** group box, click the **Interface** radio button and select an available interface from the selection list.
To create a global security policy to be applied to all interfaces, on the **Create a service policy and apply to** group box, click the **Global** radio button.
- Step 3** Type a name of up to 40 characters in the **Policy Name** box and click **Next**.
The **Add Service Policy Rule Wizard - Traffic Classification Criteria** screen appears.
- Step 4** Click the **Source and destination IP address (uses ACL)** button.
- Step 5** Select the **Source Port** and **Destination Port** for the protocol in the **Protocol and Service** group box and click **Next**.
The **Add Service Policy Rule Wizard - Rule Actions** screen appears.
- Step 6** Click the checkbox for the protocol you want to enable and click **Finish**.
The new service policy is shown in the **Service Policy Rules** table on the **Security Policy** panel.

- Step 7** To enable another inspection engine, select the service policy and click **Add**.
The **Add Service Policy Rule Wizard - Service Policy** screen appears.
- Step 8** Click **Next**.
The **Add Service Policy Rule Wizard - Traffic Classification Criteria** screen appears.
- Step 9** Click **Create a new traffic class** and change the name of the traffic class, if necessary.
By default, the number at the end of the name for each traffic class is incremented as you add each new class.
- Step 10** Click **Source and destination IP address (uses ACL)**.
- Step 11** Click the **Traffic Match** tab.
- Step 12** Select the second port number for the protocol in the **Protocol and Service** group box and click **OK**.
The new access control entry is shown in the **Service Policy Rules** table on the **Security Policy** panel.
-

Configuring Application Inspection with Multiple Ports

To use Modular Policy Framework for changing the default port assignment for protocols that use more than one port, perform the following steps:

-
- Step 1** Click **Service Policy Rules** on the **Security Policy** panel and then click **Add**.
The **Add Service Policy Rule Wizard - Service Policy** screen appears.
- Step 2** Create a service policy.
To create a security policy for a specific interface, on the **Create a service policy and apply to** group box, click the **Interface** radio button and select an available interface from the selection list.
To create a global security policy to be applied to all interfaces, on the **Create a service policy and apply to** group box, click the **Global** radio button.
- Step 3** Type a name of up to 40 characters in the **Policy Name** box and click **Next**.
The **Add Service Policy Rule Wizard - Traffic Classification Criteria** screen appears.
- Step 4** Click the **Source and destination IP address (uses ACL)** button.
- Step 5** Select the first port number for the protocol in the **Protocol and Service** group box and click **Next**.
The **Add Service Policy Rule Wizard - Rule Actions** screen appears.
- Step 6** Define the rule action to apply to the specified traffic flow, using one of the following tabs:
- **Protocol Inspection**
 - **Connection Settings**
 - **QoS**
- Step 7** Click **Finish**.
The new service policy is shown in the **Service Policy Rules** table on the **Security Policy** panel.
- Step 8** Right-click the security policy on the Service Policy Rules table.
- Step 9** On the pop-up menu that appears, select **Insert After**.
The **Insert Service Policy Rule After** screen appears.

- Step 10** Click the **Traffic Match** tab.
- Step 11** Select the second port number for the protocol in the **Protocol and Service** group box and click **OK**.
The new access control entry is shown in the **Service Policy Rules** table on the **Security Policy** panel.

Source and Destination Address (This dialog is called “ACL” in other contexts)

(This dialog box is called **ACL** when editing a service policy rule)

This dialog box lets you identify the traffic to which a service policy rule applies based on the IP address or TCP/UDP port of the sending or receiving host. You can also use this dialog box to select a **Time Range** during which the policy rule is in effect.

Fields

- **Select an action**—Lets you specify whether the traffic must match or must not match the criteria specified on this dialog box.
- **Time Range** area
 - **Time Range**—Lets you select a named time range during which the policy rule is in effect.
 - **New**—Lets you access the **Add Time Range** dialog box. For more information, see [Add/Edit Time Range](#).
- **Source Host/Network** area
 - **IP Address**—Specifies that the source of the traffic is to be identified by IP address. When you select this button, the **Interface** drop-down list, **IP address** field, **. . .** button, and **Mask** drop-down list appear within the area.
 - **Name**—Specifies that the source of the traffic is to be identified by interface name. When you select this button, the **Name** drop-down list appears within the area.
 - **Group**—Specifies that the source of the traffic is to be identified by object groups. When you select this button, the **Interface** drop-down list and **Group** drop-down list appear within the area.
 - **Interface**—Specifies the name of the interface that the source of the traffic is on. This drop-down list appears only when the **IP Address** button or the **Group** button is selected.
 - **IP address**—Specifies the IP address used to identify the source of the traffic. This field appears only when the **IP Address** button is selected.
 - **. . .**—Lets you access the **Select host/network** dialog box, which lets you select a host or network from a preconfigured drop-down list. This button appears only when the **IP Address** button is selected.
 - **Mask**—Specifies the subnet mask for the address entered in the **IP address** field. This field appears only when the **IP Address** button is selected.
 - **Name**—Specifies the name of the interface that the source of the traffic is on. This drop-down list appears only when the **Name** button is selected.
 - **Group**—Specifies the object group that the source of the traffic is in. The items on the drop-down list is controlled by the **Network Object Groups** window. For more information about that window, see the [“Using Network Objects and Groups”](#) section on page 6-1. The **Group** drop-down list appears only when the **Group** button is selected.
- **Destination Host/Network** area

- **IP Address**—Specifies that the destination of the traffic is to be identified by IP address. When you select this button, the **Interface** drop-down list, **IP address** field, **. . .** button, and **Mask** drop-down list appear within the area.
- **Name**—Specifies that the destination of the traffic is to be identified by interface name. When you select this button, the **Name** drop-down list appears within the area.
- **Group**—Specifies that the destination of the traffic is to be identified by object groups. When you select this button, the **Interface** drop-down list and **Group** drop-down list appear within the area.
- **Interface**—Specifies the name of the interface that the destination of the traffic is on. This drop-down list appears only when the **IP Address** button or the **Group** button is selected.
- **IP address**—Specifies the IP address used to identify the destination of the traffic. This field appears only when the **IP Address** button is selected.
- **. . .**—Lets you access the **Select host/network** dialog box, which lets you select a host or network from a preconfigured drop-down list. This button appears only when the **IP Address** button is selected.
- **Mask**—Specifies the subnet mask for the address entered in the **IP address** field. This field appears only when the **IP Address** button is selected.
- **Name**—Specifies the name of the interface that the destination of the traffic is on. This drop-down list appears only when the **Name** button is selected.
- **Group**—Specifies the object group that the destination of the traffic is in. The items on the drop-down list is controlled by the **Network Object Groups** window. For more information about that window, see [“Using Network Objects and Groups” section on page 6-1](#). The **Group** drop-down list appears only when the **Group** button is selected.
- **Rule Flow Diagram**—Provides a graphic representation of how a specific filtering action is applied to traffic that is forwarded through the security appliance.
- **Protocol and Service area**
 - **TCP**—Matches traffic based on the TCP protocol or service.
 - **UDP**—Matches traffic based on the UDP protocol or service.
 - **ICMP**—Matches traffic based on the ICMP protocol value.
 - **IP**—Matches traffic based on the IP protocol value.
 - **Manage Service Groups**—Displays the **Manage Service Groups** dialog box, which lets you create and edit service groups. This button is available only when the TCP button is selected.
 - **Source Port**—Appears only when either the **TCP** or **UDP** radio button is selected.
 - Service**—Matches traffic based on the source port value.
 - Operator**—Specifies whether to identify a single port or a range of ports to match. When you select = (equal to), **not=** (not equal to), > (greater than), or < (less than) from the drop-down list, the **. . .** button appears, which lets you select a specific named port. When you select **range** from the drop-down list, two fields appear that let you enter the starting and ending ports in the range.
 - ...**—Displays the **Service** dialog box, which lets you select the named values for the TCP or UDP ports to match.
 - Service Group**—Matches traffic based on the source service group. To control the items on the drop-down list, use the **Manage Service Groups** button.
 - **Destination Port**—Appears only when either the **TCP** or **UDP** radio button is selected.

Service—Matches traffic based on the destination port value.

Operator—Specifies whether to identify a single port or a range of ports to match. When you select = (equal to), **not=** (not equal to), > (greater than), or < (less than) from the drop-down list, the . . . button appears, which lets you select a specific named port. When you select **range** from the drop-down list, two fields appear that let you enter the starting and ending ports in the range.

...—Displays the **Service** dialog box, which lets you select the named values for the TCP or UDP ports to match.

Service Group—Matches traffic based on the destination service group. To control the items on the drop-down list, use the **Manage Service Groups** button.

- **ICMP Type**—Appears only when the **ICMP** radio button is selected.

ICMP type—Lets you enter the ICMP type of the traffic.

...—Displays the **Service** dialog box, which lets you select ICMP types from a preconfigured drop-down list.

- **IP Protocol**—Appears only when the **IP** radio button is selected.

IP protocol—Lets you enter the IP protocol of the traffic.

...—Displays the **Service** dialog box, which lets you select an IP protocol from a preconfigured drop-down list.

Modes

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

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

Destination Port

The **Destination Port** dialog box appears when you select **TCP or UDP destination port** in the **Traffic Match Criteria** dialog box, or choose the corresponding tab when editing a service policy rule. This dialog box lets you identify the traffic to which a service policy rule applies based on the TCP or UDP destination port.

Fields

- **TCP**—Matches traffic based on the TCP port used by the destination.
- **UDP**—Matches traffic based on the UDP port used by the destination.
- **Operator**—Specifies whether to identify a single port or a range of ports to match.

When you select = (equals sign) from the drop-down list, the . . . button appears, which lets you select a specific named port.

When you select **range** from the drop-down list, two fields appear that let you enter the starting and ending ports in the range.

- **...**—Displays the **Service** dialog box, which lets you select the named values for the TCP or UDP ports to match.

Modes

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

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

RTP Ports

The **RTP Ports** dialog box appears when you select **RTP range** on the **Traffic Match Criteria** dialog box, or choose the corresponding tab when editing a service policy rule. This dialog box lets you identify the traffic to which a service policy rule applies based on a range of RTP ports.

- **RTP Port Range**—Specifies the starting and ending ports within the range of RTP ports to be used for matching traffic. RTP port numbers should be between 2000 and 65535. The maximum number of RTP ports in a range is 16383.

Modes

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

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

IP Precedence

The **IP Precedence** dialog box appears when you select **IP Precedence** on the **Traffic Match Criteria** dialog box, or choose the corresponding tab when editing a service policy rule. This dialog box lets you identify the traffic to which a service policy rule applies based on the IP precedence.

Fields

- **Available IP Precedence**—Lists the available IP Precedence values that you can use to match traffic. IP Precedence is one model for assigning QoS priorities to IP traffic.
- **Add**—Adds the selected IP Precedence value to the Match on IP Precedence list.
- **Delete**—Removes the selected IP Precedence value from the Match on IP Precedence list.
- **Match On IP Precedence**—Lists the IP Precedence values that have been selected to match traffic.

Modes

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

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

IP DiffServ CodePoints (DSCP)

The **IP DiffServ Code Points (DSCP)** dialog box lets you match traffic based on the values assigned for Differentiated Services model of QoS. DiffServ defines two sets of DSCP values: EF and AF.

Fields

- **Expedited Forwarding (EF)**—Provides a single DSCP value (101110) that gives marked packets the highest level of service from the network. EF is commonly considered most appropriate for Voice over IP (VoIP).
- **Assured Forwarding (AF)**—Provides four classes, each with three drop precedence levels.

You can select named DSCP values from the selection drop-down list, or enter a numeric value.

- **Named DSCP Values**—Lists named DSCP values that you can select as match criteria. Select the values that you want to match and choose **Add**.
- **Enter DSCP value (0-63)**—Specifies a numeric DSCP value.
- **Add**—Adds a selected DSCP value to the Match on DSCP table.
- **Delete**—Removes a selected DSCP value from the Match on DSCP table.
- **Match on DSCP**—Lists the DSCP values that have been selected as match criteria.
- **Enter DSCP value (0-63)**—Uses a numeric value as the criteria for matching.

Modes

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

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

Rule Actions > Protocol Inspection Tab

The **Protocol Inspection** tab lets you enable or disable the different types of application inspection available. To view or change the configuration for a specific application inspection type, choose **Configure**, which lets you select a map name to use for the protocol. To configure a map see [Configuring Inspect Maps, page 6-28](#).

Fields

- **CTIQBE**—Enables application inspection for the CTIQBE protocol.
- **DCERPC**—Enables application inspection for the DCERPC protocol.

- Configure—Displays the **Select DCERPC Map** dialog box, which lets you select a map name to use for this protocol.
- **DNS**—Enables application inspection for the DNS protocol.
 - Configure—Displays the **Select DNS Map** dialog box, which lets you select a map name to use for this protocol.
- **ESMTP**—Enables application inspection for the ESMTP protocol.
 - Configure—Displays the **Select ESMTP Map** dialog box, which lets you select a map name to use for this protocol.
- **FTP**—Enables application inspection for the FTP protocol.
 - Configure—Displays the **Select FTP Map** dialog box, which lets you select a map name to use for this protocol.
- **GTP**—Enables application inspection for the GTP protocol.
 - Configure—Displays the **Select GTP Map** dialog box, which lets you select a map name to use for this protocol.



Note GTP inspection is not available without a special license.

- **H323 H225**—Enables application inspection for the H323 H225 protocol.
 - Configure—Displays the **Select H323 H225 Map** dialog box, which lets you select a map name to use for this protocol.
- **H323 RAS**—Enables application inspection for the H323 RAS protocol.
 - Configure—Displays the **Select H323 RAS Map** dialog box, which lets you select a map name to use for this protocol.
- **HTTP**—Enables application inspection for the HTTP protocol.
 - Configure—Displays the **Select HTTP Map** dialog box, which lets you select a map name to use for this protocol.
- **ICMP**—Enables application inspection for the ICMP protocol.
- **ICMP Error**—Enables application inspection for the ICMP Error protocol.
- **ILS**—Enables application inspection for the ILS protocol.
- **IM**—Enables application inspection for the IM protocol.
 - Configure—Displays the **Select IM Map** dialog box, which lets you select a map name to use for this protocol.
- **IPSec-Pass-Thru**—Enables application inspection for the IPSec protocol.
 - Configure—Displays the **Select IPSec Map** dialog box, which lets you select a map name to use for this protocol.
- **MGCP**—Enables application inspection for the MGCP protocol.
 - Configure—Displays the **Select MGCP Map** dialog box, which lets you select a map name to use for this protocol.
- **NETBIOS**—Enables application inspection for the NetBIOS protocol.
 - Configure—Displays the **Select NETBIOS Map** dialog box, which lets you select a map name to use for this protocol.

- **PPTP**—Enables application inspection for the PPTP protocol.
- **RSH**—Enables application inspection for the RSH protocol.
- **RTSP**—Enables application inspection for the RTSP protocol.
- **SCCP SKINNY**—Enables application inspection for the Skinny protocol.
 - **Configure**—Displays the **Select SCCP (Skinny) Map** dialog box, which lets you select a map name to use for this protocol.
- **SIP**—Enables application inspection for the SIP protocol.
 - **Configure**—Displays the **Select SIP Map** dialog box, which lets you select a map name to use for this protocol.
- **SNMP**—Enables application inspection for the SNMP protocol.
 - **Configure**—Displays the **Select SNMP Map** dialog box, which lets you select a map name to use for this protocol.
- **SQLNET**—Enables application inspection for the SQLNET protocol.
- **SUNRPC**—Enables application inspection for the SunRPC protocol.
- **TFTP**—Enables application inspection for the TFTP protocol.
- **XDMCP**—Enables application inspection for the XDMCP protocol.

Modes

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

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

For More Information

[Configuring Inspect Maps](#)

Inspect command pages for each protocol in the *Cisco ASA 5500 Series Command Reference*

Select DCERPC Map

The **Select DCERPC Map** dialog box lets you select or create a new **DCERPC** map. A **DCERPC** map lets you change the configuration values used for **DCERPC** application inspection. The **Select DCERPC Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No DCERPC map for inspection**—Specifies no DCERPC map.
- **Select a DCERPC map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Configure DNS**Fields**

Maximum DNS packet length (default 512)—Changes the maximum packet length for DNS messages that are allowed to pass through the security appliance.

Modes

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

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

Select DNS Map

The **Select DNS Map** dialog box lets you select or create a new **DNS** map. A **DNS** map lets you change the configuration values used for **DNS** application inspection. The **Select DNS Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No DNS map for inspection**—Specifies no **DNS** map.
- **Select a DNS map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select ESMTP Map

The **Select ESMTP Map** dialog box lets you select or create a new **ESMTP** map. An **ESMTP** map lets you change the configuration values used for **ESMTP** application inspection. The **Select ESMTP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No ESMTP map for inspection**—Specifies no **ESMTP** map.
- **Select an ESMTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select FTP Map

The **Select FTP Map** dialog box lets you enable strict FTP application inspection, select an FTP map, or create a new FTP map. An FTP map lets you change the configuration values used for FTP application inspection. The **Select FTP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **FTP Strict (prevent web browsers from sending embedded commands in FTP requests)**—Enables strict FTP application inspection, which causes the security appliance to drop the connection when an embedded command is included in an FTP request.
- **No FTP map for inspection**—Specifies no FTP map.
- **Select an FTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select GTP Map

The **Select GTP Map** dialog box lets you select or create a new GTP map. A GTP map lets you change the configuration values used for GTP application inspection. The Select GTP Map table provides a list of previously configured maps that you can select for application inspection.



Note GTP inspection requires a special license. If you try to enable GTP application inspection on a security appliance without the required license, the security appliance displays an error message.

Fields

- **No GTP map for inspection**—Specifies no GTP map.
- **Select an GTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select H.323 Map

The **Select H.323 Map** dialog box lets you select or create a new **H.323** map. An **H.323** map lets you change the configuration values used for **H.323** application inspection. The Select **H.323** Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No H.323 map for inspection**—Specifies no **H.323** map.
- **Select an H.323 map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select HTTP Map

The **Select HTTP Map** dialog box lets you select or create a new HTTP map. An HTTP map lets you change the configuration values used for HTTP application inspection. The Select HTTP Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No HTTP map for inspection**—Specifies no HTTP map.
- **Select an HTTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select IM Map

The **Select IM Map** dialog box lets you select or create a new IM map. An IM map lets you change the configuration values used for IM application inspection. The Select IM Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No IM map for inspection**—Specifies no IM map.
- **Select an IM map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select IPSec-Pass-Thru Map

The **Select IPSec-Pass-Thru** dialog box lets you select or create a new IPSec map. An IPSec map lets you change the configuration values used for IPSec application inspection. The Select IPSec Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No IPSec map for inspection**—Specifies no IPSec map.
- **Select an IPSec map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select MGCP Map

The **Select MGCP Map** dialog box lets you select or create a new MGCP map. An MGCP map lets you change the configuration values used for MGCP application inspection. The Select MGCP Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No MGCP map for inspection**—Specifies no MGCP map.
- **Select an MGCP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select NETBIOS Map

The **Select NETBIOS Map** dialog box lets you select or create a new NetBIOS map. A NetBIOS map lets you change the configuration values used for NetBIOS application inspection. The Select NetBIOS Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No IM map for inspection**—Specifies no NetBIOS map.
- **Select a NetBIOS map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.

- Add—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select SCCP (Skinny) Map

The **Select SCCP (Skinny) Map** dialog box lets you select or create a new **SCCP (Skinny)** map. An **SCCP (Skinny)** map lets you change the configuration values used for **SCCP (Skinny)** application inspection. The **Select SCCP (Skinny) Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No SCCP (Skinny) map for inspection**—Specifies no **SCCP (Skinny)** map.
- **Select an SCCP (Skinny) map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- Add—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select SIP Map

The **Select SIP Map** dialog box lets you select or create a new **SIP** map. A **SIP** map lets you change the configuration values used for **SIP** application inspection. The **Select SIP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No SIP map for inspection**—Specifies no **SIP** map.
- **Select a SIP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- Add—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Select SNMP Map

The **Select SNMP Map** dialog box lets you select or create a new SNMP map. An SNMP map lets you change the configuration values used for SNMP application inspection. The Select SNMP Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **No SNMP map for inspection**—Specifies no SNMP map.
- **Select an SNMP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

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

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

Rule Actions > Intrusion Prevention Tab

The **Intrusion Prevention** tab lets you configure the Intrusion Prevention (IPS) action to take within a policy map for a traffic class. This window appears only if Intrusion Prevention System hardware is installed in the security appliance.

Fields

- **Enable IPS for this traffic flow**—Enables or disables intrusion prevention for this traffic flow. When this check box is selected, the other parameters on this window become active.
- **Mode**—Configures the operating mode for intrusion prevention
 - **Inline Mode**—Selects Inline Mode, in which a packet is directed to IPS. The packet might be dropped as a result of the IPS operation.
 - **Promiscuous Mode**—Selects Promiscuous Mode, in which IPS operates on a duplicate of the original packet. The original packet cannot be dropped.
- **If IPS card fails, then**—Configures the action to take if the IPS card becomes inoperable.
 - **Permit traffic**—Permit traffic if the IPS card fails
 - **Close traffic**—Block traffic if the IPS card fails.

Modes

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

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

Rule Actions > CSC Scan Tab

The **CSC Scan** tab lets you whether the Content Security and Control (CSC) SSM scans traffic identify by the current traffic class. This window appears only if a CSC SSM is installed in the security appliance.

The CSC SSM scans only HTTP, SMTP, POP3, and FTP traffic. If your service policy selects traffic that includes other protocols in addition to these four, packets for other protocols are passed through the CSC SSM without being scanned.

To reduce the load on the CSC SSM, configure the service policy rules that send packets to the CSC SSM to select only HTTP, SMTP, POP3, or FTP packets.

Fields

- **Enable CSC scan for this traffic flow**—Enables or disables use of the CSC SSM for this traffic flow. When this check box is selected, the other parameters on this window become active.
- **If CSC card fails, then**—Configures the action to take if the CSC SSM becomes inoperable.
 - **Permit traffic**—Permit traffic if the CSC SSM fails
 - **Close traffic**—Block traffic if the CSC SSM fails.

Modes

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

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

For More Information

[Managing the CSC SSM](#)

Rule Actions > Connection Settings Tab

The **Connection Settings** tab lets you configure maximum connections, embryonic connections, and sequence number randomizing for TCP packets on a host or network. You can also configure connection timeouts and TCP normalization.

Fields

- **Maximum Connections** area
 - **TCP & UDP Connections**—Specifies the maximum number of simultaneous TCP and UDP connections for all clients in the traffic class, up to 65,536. The default is **0** for both protocols, which means the maximum possible connections are allowed.
 - **Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is **0**, which means the maximum embryonic connections. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.
 - **Per Client Connections**—Specifies the maximum number of simultaneous TCP and UDP connections for each client. When a new connection is attempted by a client that already has opened the maximum per-client number of connections, the security appliance rejects the connection and drops the packet.
 - **Per Client Embryonic Connections**—Specifies the maximum number of simultaneous TCP embryonic connections for each client. When a new TCP connection is requested by a client that already has the maximum per-client number of embryonic connections open through the security appliance, the security appliance proxies the request to the TCP Intercept feature, which prevents the connection.
- **Randomize Sequence Number**—Sets the state of the Randomize Sequence Number feature to enabled or disabled. Disable this feature only if another inline security appliance is also randomizing sequence numbers and the result is scrambling the data. Each TCP connection has two Initial Sequence Numbers: one generated by the client and one generated by the server. The security appliance randomizes the ISN that is generated by the host/server on the higher security interface. At least one of the ISNs must be randomly generated so that attackers cannot predict the next ISN and potentially hijack the session.
- **TCP Timeout** area
 - **Connection Timeout**—Specifies the idle time until a connection slot is freed. Enter 0:0:0 to disable timeout for the connection. This duration must be at least 5 minutes. The default is **1 hour**.
 - **Send reset to TCP endpoints before timeout**—Specifies that the security appliance should send a TCP reset message to the endpoints of the connection before freeing the connection slot.
 - **Embryonic Connection Timeout**—Specifies the idle time until an embryonic connection slot is freed. Enter 0:0:0 to disable timeout for the connection. The default is **30 seconds**.
 - **Half Closed Connection Timeout**—Specifies the idle time until a half closed connection slot is freed. Enter 0:0:0 to disable timeout for the connection. This duration must be at least 5 minutes. The default is **10 minutes**.
- **TCP Normalization** area
 - **Use TCP Map**—Selects whether TCP normalization is enabled or not. Enable this feature to use TCP maps.
 - **TCP Map**—Selects an existing TCP map.
 - **New**—Adds a new TCP map.

- **Edit**—Edits an existing TCP map.

Modes

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

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

Rule Actions > QoS Tab

The **QoS** tab lets you configure priority queuing, policing, or traffic shaping.



Note

If a service policy is applied or removed from an interface that has existing connections, the QoS policy is not applied or removed from the traffic stream. To apply or remove the QoS policy for such connections, you must clear (that is, drop) the connections and reestablish them.

Supported QoS Features

The security appliance supports the following QoS features:

- **Policing**—To prevent individual flows from hogging the network bandwidth, you can limit the maximum bandwidth used per flow. See the [“Policing Overview” section on page 21-27](#) for more information.
- **Priority queuing**—For critical traffic that cannot tolerate latency, such as voice over IP (VoIP), you can identify traffic for low latency queuing (LLQ) so that it is always transmitted at a minimum rate. See the [“Priority Queueing Overview” section on page 21-27](#) for more information.
- **Traffic shaping**—If you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the [“Traffic Shaping Overview” section on page 21-28](#) for more information.

What is a Token Bucket?

A token bucket is used to manage a device that regulates the data in a flow. For example, the regulator might be a traffic policer or a traffic shaper. A token bucket itself has no discard or priority policy. Rather, a token bucket discards tokens and leaves to the flow the problem of managing its transmission queue if the flow overdrives the regulator.

A token bucket is a formal definition of a rate of transfer. It has three components: a burst size, an average rate, and a time interval. Although the average rate is generally represented as bits per second, any two values may be derived from the third by the relation shown as follows:

$$\text{average rate} = \text{burst size} / \text{time interval}$$

Here are some definitions of these terms:

- **Average rate**—Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.

- **Burst size**—Also called the Committed Burst (Bc) size, it specifies in bits or bytes per burst how much traffic can be sent within a given unit of time to not create scheduling concerns. (For traffic shaping, it specifies bits per burst; for policing, it specifies bytes per burst.)
- **Time interval**—Also called the measurement interval, it specifies the time quantum in seconds per burst.

In the token bucket metaphor, tokens are put into the bucket at a certain rate. The bucket itself has a specified capacity. If the bucket fills to capacity, newly arriving tokens are discarded. Each token is permission for the source to send a certain number of bits into the network. To send a packet, the regulator must remove from the bucket a number of tokens equal in representation to the packet size.

If not enough tokens are in the bucket to send a packet, the packet either waits until the bucket has enough tokens (in the case of traffic shaping) or the packet is discarded or marked down (in the case of policing). If the bucket is already full of tokens, incoming tokens overflow and are not available to future packets. Thus, at any time, the largest burst a source can send into the network is roughly proportional to the size of the bucket.

Note that the token bucket mechanism used for traffic shaping has both a token bucket and a data buffer, or queue; if it did not have a data buffer, it would be a policer. For traffic shaping, packets that arrive that cannot be sent immediately are delayed in the data buffer.

For traffic shaping, a token bucket permits burstiness but bounds it. It guarantees that the burstiness is bounded so that the flow will never send faster than the token bucket capacity, divided by the time interval, plus the established rate at which tokens are placed in the token bucket. See the following formula:

(token bucket capacity in bits / time interval in seconds) + established rate in bps = maximum flow speed in bps

This method of bounding burstiness also guarantees that the long-term transmission rate will not exceed the established rate at which tokens are placed in the bucket.

Policing Overview

Policing is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that no one traffic flow can take over the entire resource. When traffic exceeds the maximum rate, the security appliance drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

Priority Queueing Overview

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The security appliance supports two types of priority queueing:

- **Standard priority queueing**—Standard priority queueing uses an LLQ priority queue on an interface (see the “[Priority Queue](#)” section on page 25-1), while all other traffic goes into the “best effort” queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size. You can also fine-tune the maximum number of packets allowed into the transmit queue. These options let you control the latency and robustness of the priority queueing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- **Hierarchical priority queueing**—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used. See the following guidelines about hierarchical priority queueing:

- Priority packets are always queued at the head of the shape queue so they are always transmitted ahead of other non-priority queued packets.
- Priority packets are never dropped from the shape queue unless the sustained rate of priority traffic exceeds the shape rate.
- For IPsec-encrypted packets, you can only match traffic based on the DSCP or precedence setting.
- IPsec-over-TCP is not supported for priority traffic classification.

Traffic Shaping Overview

Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

- Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic.
- Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to be transmitted, including all the possible overhead such as the IPsec header and L2 header.
- The shaped traffic includes both through-the-box and from-the-box traffic.
- The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the Burst Size value. See the [“What is a Token Bucket?”](#) section on page 21-26.
- When bursty traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queuing, see the [“Priority Queue”](#) section on page 25-1):
 - The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200-milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.
 - When the queue limit is reached, packets are tail-dropped.
 - Certain critical keep-alive packets such as OSPF Hello packets are never dropped.
 - The time interval is derived by $time_interval = burst_size / average_rate$. The larger the time interval is, the burstier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

Average Rate = 1000000

Burst Size = 1000000

In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay-sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

How QoS Features Interact

You can configure each of the QoS features alone if desired for the security appliance. Often, though, you configure multiple QoS features on the security appliance so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + Policing (for the rest of the traffic).
You cannot configure priority queuing and policing for the same set of traffic.

- Traffic shaping (for all traffic on an interface) + Hierarchical priority queueing (for a subset of traffic).

You cannot configure traffic shaping and standard priority queueing for the same interface; only hierarchical priority queueing is allowed. For example, if you configure standard priority queueing for the global policy, and then configure traffic shaping for a specific interface, the feature you configured last is rejected because the global policy overlaps the interface policy.

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the security appliance does not restrict you from configuring this.

DSCP and DiffServ Preservation

- DSCP markings are preserved on all traffic passing through the security appliance.
- The security appliance does not locally mark/re-mark any classified traffic, but it honors the Expedited Forwarding (EF) DSCP bits of every packet to determine if it requires “priority” handling and will direct those packets to the LLQ.
- DiffServ marking is preserved on packets when they traverse the service provider backbone so that QoS can be applied in transit (QoS tunnel pre-classification).

Fields

- Enable Priority for this flow (not available for class-default)—Enables low latency queueing (LLQ) for this flow. Priority queueing requires a priority queue to be enabled for each interface. If this service policy rule is for an individual interface, ASDM automatically creates the priority queue for the interface (**Configuration > Properties > Priority Queue**; for more information, see the [“Priority Queue” section on page 25-1](#)). If this rule is for the global policy, then you need to manually add the priority queue to one or more interfaces *before* you configure the service policy rule. You cannot configure a separate priority queueing rule on the same interface for which you configure a traffic shaping rule; you can, however, configure priority queueing for a subset of shaped traffic under the traffic shaping rule (see the “Enable traffic shaping” option below). You also cannot configure priority queueing for the global policy if you also enable traffic shaping on any interfaces.
- Enable traffic shaping (only available for class-default)—Enables traffic shaping for all traffic on the interface. If you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem can be a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate, called traffic shaping. You cannot configure a separate traffic shaping rule on the same interface for which you configure a priority queueing rule (see the “Enable Priority for this flow” option above); you can, however, configure priority queueing for a subset of shaped traffic under the traffic shaping rule (see the “Enforce priority to selected shape traffic” below). You also cannot configure traffic shaping for the global policy if you also enable priority queueing on any interfaces.
 - Average Rate—Sets the average rate of traffic in bits per second over a given fixed time period, between 64000 and 154400000. Specify a value that is a multiple of 8000.
 - Burst Size—Sets the average burst size in bits that can be transmitted over a given fixed time period, between 2048 and 154400000. Specify a value that is a multiple of 128. If you do not specify the Burst Size, the default value is equivalent to 4-milliseconds of traffic at the specified Average Rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = $1000000 * 4/1000 = 4000$.
 - Enforce priority to selected shape traffic—You can configure priority queueing for a subset of the traffic for which you enable traffic shaping. Click **Configure** to identify the traffic that you want to prioritize. For this type of priority queueing, you do *not* need to create a priority queue

on an interface (**Configuration > Properties > Priority Queue**). To avoid out-of-order IPSec packets that are not within the anti-replay window, see **Configuration > VPN > IPSec > IPSec Rules > Enable Anti-replay window size** in the “IPSec Rules” section on page 26-13.

- **Enable policing**—Enables policing of traffic in the input or output direction. Typically, if you enable policing, you do not also enable traffic shaping for the same traffic.
 - **Direction**—Select to enable policing in either the input or output direction.
 - **Committed Rate**—The rate limit for this traffic flow; this is a value in the range 8000-2000000000, specifying the maximum speed (bits per second) allowed.
 - **Conform Action**—The action to take when the rate is less than the conform-burst value. Values are transmit or drop.
 - **Exceed Action**—Take this action when the rate is between the conform-rate value and the conform-burst value. Values are transmit or drop.
 - **Burst Rate**—A value in the range 1000-512000000, specifying the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value.



Note The Enable Policing check box merely enforces the maximum speed and burst rate, forcing them to the conforming rate value. It does not enforce the conform-action or the exceed-action specification if these are present.

Modes

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

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

Edit Class Map

The **Edit Class Map** dialog box lets you add or edit the description of a class map.

Fields

- **Description**—Add or change the name of the class map description.

Modes

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

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

Edit Rule

The **Edit Rule** dialog box lets you modify an existing rule.

Fields

- **Select an action**—Determines the action type of the new rule. Select either permit or deny from the Select an action drop-down list.
 - Permit—Permits all matching traffic.
 - Deny—Denies all matching traffic.
- **Apply to traffic**—Determines which type of traffic to which the rule is applied.
 - Incoming to source interface—Selects incoming traffic to the source interface.
 - Outgoing from destination interface—Selects outgoing traffic from the destination interface.
- **Syslog**—Shows whether syslog is enabled or not.
- **More Options**—Enables logging for the access list and sets logging options. The **More Options** button lets you set logging options. This button allows you to:
 - Use default logging behavior.
 - Enable logging for the rule.
 - Disable logging for the rule.
 - Set the level and interval for permit and deny logging. This option checks the **Enable Logging** check box.
See **Log Options** for more information. Also, see **Advanced Access Rule Configuration** to set global logging options.
- **Time Range**—Select a time range defined for this rule from the drop-down list.
- **New**—Create a new time range for this rule. See **Add Time Range**.
- **Source and Destination Host/Network IP Address**—Choose this button to identify the networks by IP address.
 - **Interface**—The interface on which the host or network resides.
 - **IP address**—The IP address of the host or network.
 - **Browse**—Lets you select an existing host or network by choosing the options under the **Select Host/Network** window to populate the **Name**, **Interface**, **IP address**, and **Mask** fields with the properties of the selected host or network.
 - **Mask**—The subnet mask of the host or network
- **Name**—Choose this button to identify the networks by name. To name hosts/networks, see the **Network Objects/Groups** tab.
The name of the host or network. If you choose this option, and reopen the rule to edit it, the button selection reverts to IP Address, and the named host/network IP address information appears in the fields.
- **Group**—Choose this button to identify a group of networks and hosts that you grouped together on the **Network Objects/Groups** tab.
 - **Interface**—The interface connected to the hosts and networks in the group.
 - **Group**—The group name.

- **Protocol and Service: TCP and UDP buttons**—Selects the TCP/UDP protocol for the rule. The **Source Port** and **Destination Port** areas allow you to specify the ports that the access list uses to match packets.
 - **Source Port Service**—Choose this option to specify a port number, a range of ports, or a well-known service name from a drop-down list of services, such as HTTP or FTP.
 - **Source Port Service**—The operator drop-down list specifies how the access list matches the port. Choose one of the following operators:
 - = —Equals the port number.
 - **not =** —Does not equal the port number.
 - > —Greater than the port number.
 - < —Less than the port number.
 - **range**—Equal to one of the port numbers in the range.
 - **Source Port Service**—Specifies port number, a range of ports, or a well-known service name from a drop-down list of services, such as HTTP or FTP. The browse button displays the Service dialog box, which lets you select a TCP or UDP service from a preconfigured drop-down list.
 - **Source Port Service Group**—Choose this option to specify a service group from the Service Group drop-down list,
- **Protocol and Service: ICMP**—Specifies the ICMP type for the rule in the ICMP type field. The **Browse** button displays the **Service** dialog box, which lets you select an ICMP type from a preconfigured drop-down list.
- **Protocol and Service: IP**—Specifies the IP protocol for the rule in the IP protocol field. The **Browse** button displays the Protocols dialog box, which lets you select an IP protocol from a preconfigured drop-down list.
- **Manage Service Groups**—Manages service groups. Service groups allow you to identify multiple non-contiguous port numbers that you want the access list to match. For example, if you want to filter HTTP, FTP, and port numbers 5, 8, and 9, you can define a service group that includes all these ports. Without service groups, you would have to create a separate rule for each port.
 You can create service groups for TCP, UDP, and TCP-UDP. A service group with the TCP-UDP protocol contains services, ports, and ranges that might use either the TCP or UDP protocol. See **Manage Service Groups** for more information.
- **Description**—(Optional) Enter a description of the access rule.

Modes

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

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

Edit Service Policy Rule > Traffic Classification Tab

The **Traffic Classification** tab lets you specify the criteria you want to use to match traffic to which the security policy rule applies.

Fields

- **Description**—Specifies a description for the traffic classification.
- **Default Inspection Traffic**—Uses the criteria specified in the default inspection traffic policy.
- **Source and destination IP address (uses ACL)**—Matches traffic based on the source and destination IP address, using an access control list. This selection is only available if you apply the rule to a specific interface using an Interface Service Policy.
- **Tunnel Group**—Matches traffic based on the tunnel group.
- **TCP or UDP destination port**—Matches traffic based on the TCP or UDP destination port.
- **RTP range**—Matches traffic based on a range of RTP ports.
- **IP DiffServ CodePoints (DSCP)**—Matches traffic based on the Differentiated Services model of QoS.
- **IP Precedence**—Matches traffic based on the IP precedence model of QoS.
- **Any traffic**—Matches all traffic regardless of the traffic type.

Modes

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

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

Tunnel Group

The **Tunnel Group** dialog box lets you identify the traffic to which a service policy rule applies based on the tunnel group.

Fields

- **Tunnel Group**—Selects the tunnel group for which to match traffic.
- **New**—Displays the **Add Tunnel Group** window, on which you can configure a new tunnel group.
- **Match flow destination IP address**—Adds the requirement to match the flow destination IP address, as well as the tunnel group.

Modes

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

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

SUNRPC Server

The **SUNRPC Server** window shows which SunRPC services can traverse the security appliance and their specific timeout, on a per server basis.

Fields

- **Interface**—Displays the interface on which the SunRPC server resides.
- **IP address**—Displays the IP address of the SunRPC server.
- **Mask**—Displays the subnet mask of the IP Address of the SunRPC server.
- **Service ID**—Displays the SunRPC program number, or service ID, allowed to traverse the security appliance.
- **Protocol**—Displays the SunRPC transport protocol (TCP or UDP).
- **Port**—Displays the SunRPC protocol port range.
- **Timeout**—Displays the idle time after which the access for the SunRPC service traffic is closed.

Modes

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

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

Add/Edit SUNRPC Service

The **Add/Edit SUNRPC Service** dialog box lets you specify what SunRPC services are allowed to traverse the security appliance and their specific timeout, on a per-server basis.

Fields

- **Interface Name**—Specifies the interface on which the SunRPC server resides.
- **Protocol**—Specifies the SunRPC transport protocol (TCP or UDP).
- **IP address**—Specifies the IP address of the SunRPC server.
- **Port**—Specifies the SunRPC protocol port range.
- **Mask**—Specifies the subnet mask of the IP Address of the SunRPC server.
- **Timeout**—Specifies the idle time after which the access for the SunRPC service traffic is closed. Format is HH:MM:SS.
- **Service ID**—Specifies the SunRPC program number, or service ID, allowed to traverse the security appliance.

Modes

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

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

