



CHAPTER 22

Configuring Service Policy Rules

This chapter describes how to enable service policy rules. Service policies provide a consistent and flexible way to configure security appliance features. For example, you can use a service policy to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications.

This chapter includes the following sections:

- [Service Policy Overview, page 22-1](#)
- [Adding a Service Policy Rule for Through Traffic, page 22-6](#)
- [Adding a Service Policy Rule for Management Traffic, page 22-10](#)
- [Managing the Order of Service Policy Rules, page 22-13](#)
- [RADIUS Accounting Field Descriptions, page 22-14](#)

Service Policy Overview

This section describes how security policies work, and includes the following topics:

- [Supported Features, page 22-1](#)
- [Service Policy Elements, page 22-2](#)
- [Default Global Policy, page 22-2](#)
- [Feature Directionality, page 22-3](#)
- [Order in Which Multiple Feature Actions within a Rule are Applied, page 22-4](#)
- [Incompatibility of Certain Feature Actions, page 22-5](#)
- [Feature Matching Guidelines for Multiple Service Policies, page 22-5](#)

Supported Features

Security policies support the following features:

- QoS input policing
- TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization
- CSC

- Application inspection
- IPS
- QoS output policing
- QoS priority queue
- QoS traffic shaping, hierarchical priority queue
- NetFlow Secure Event Logging filtering

Service Policy Elements

Configuring a service policy consists of adding one or more service policy rules per interface or for the global policy. For each rule, you identify the following elements:

1. Identify the interface to which you want to apply the rule, or identify the global policy.
2. Identify the traffic to which you want to apply actions. You can identify Layer 3 and 4 through traffic.
3. Apply actions to the traffic class. You can apply multiple actions for each traffic class.

Default Global Policy

By default, the configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (a global policy). Not all inspections are enabled by default. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one. (An interface policy overrides the global policy.)

The default policy includes the following application inspections:

- DNS inspection for the maximum message length of 512 bytes
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP

Feature Directionality

Actions are applied to traffic bidirectionally or unidirectionally depending on the feature. For features that are applied bidirectionally, all traffic that enters or exits the interface to which you apply the policy map is affected if the traffic matches the class map for both directions.



Note

When you use a global policy, all features are unidirectional; features that are normally bidirectional when applied to a single interface only apply to the ingress of each interface when applied globally. Because the policy is applied to all interfaces, the policy will be applied in both directions so bidirectionality in this case is redundant.

For features that are applied unidirectionally, for example QoS priority queue, only traffic that exits the interface to which you apply the policy map is affected. See [Table 22-1](#) for the directionality of each feature.

Table 22-1 Feature Directionality

Feature	Single Interface Direction	Global Direction
Application inspection	Bidirectional	Ingress
CSC	Bidirectional	Ingress
IPS	Bidirectional	Ingress
NetFlow Secure Event Logging filtering	N/A	Ingress
QoS input policing	Ingress	Ingress
QoS output policing	Egress	Egress
QoS priority queue	Egress	Egress
QoS traffic shaping, hierarchical priority queue	Egress	Egress
TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization	Bidirectional	Ingress

Feature Matching Guidelines

See the following guidelines for how a packet matches rules for a given interface or for the global policy:

1. A packet can match only one rule for each feature type.
2. When the packet matches a rule for a feature type, the security appliance does not attempt to match it to any subsequent rules for that feature type.
3. If the packet matches a subsequent rule for a different feature type, however, then the security appliance also applies the actions for the subsequent rule, if supported. See the [“Incompatibility of Certain Feature Actions”](#) section on page 22-5 for more information about unsupported combinations.

For example, if a packet matches a rule for connection limits, and also matches a rule for application inspection, then both rule actions are applied.

If a packet matches a rule for HTTP inspection, but also matches another rule that includes HTTP inspection, then the second rule actions are not applied.

**Note**

Application inspection includes multiple inspection types, and each inspection type is a separate feature when you consider the matching guidelines above.

Order in Which Multiple Feature Actions within a Rule are Applied

The order in which different types of actions in a service policy are performed is independent of the order in which the actions appear in ASDM.

**Note**

NetFlow Secure Event Logging filtering is order-independent.

Actions are performed in the following order:

1. QoS input policing
2. TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization

**Note**

When a the security appliance performs a proxy service (such as AAA or CSC) or it modifies the TCP payload (such as FTP inspection), the TCP normalizer acts in dual mode, where it is applied before and after the proxy or payload modifying service.

3. CSC
4. Application inspection (multiple types)

The order of application inspections applied when a class of traffic is classified for multiple inspections is as follows. Only one inspection type can be applied to the same traffic. WAAS inspection is an exception, because it can applied along with other inspections for the same traffic. See the [“Incompatibility of Certain Feature Actions” section on page 22-5](#) for more information.

- a. CTIQBE
- b. DNS
- c. FTP
- d. GTP
- e. H323
- f. HTTP
- g. ICMP
- h. ICMP error
- i. ILS
- j. MGCP
- k. NetBIOS
- l. PPTP
- m. Sun RPC
- n. RSH
- o. RTSP

- p. SIP
- q. Skinny
- r. SMTP
- s. SNMP
- t. SQL*Net
- u. TFTP
- v. XDMCP
- w. DCERPC
- x. Instant Messaging



Note RADIUS accounting is not listed because it is the only inspection allowed on management traffic. WAAS is not listed because it can be configured along with other inspections for the same traffic.

- 5. IPS
- 6. QoS output policing
- 7. QoS standard priority queue
- 8. QoS traffic shaping, hierarchical priority queue

Incompatibility of Certain Feature Actions

Some features are not compatible with each other for the same traffic. For example, most inspections should not be combined with another inspection, so the security appliance only applies one inspection if you configure multiple inspections for the same traffic. In this case, the feature that is applied is the higher priority feature in the list in the [“Order in Which Multiple Feature Actions within a Rule are Applied”](#) section on page 22-4.

For information about compatibility of each feature, see the chapter or section for your feature.



Note

The Default Inspection Traffic traffic classification, which is used in the default global policy, is a special shortcut to match the default ports for all inspections. When used in a rule, this traffic classification ensures that the correct inspection is applied to each packet, based on the destination port of the traffic. For example, when UDP traffic for port 69 reaches the security appliance, then the security appliance applies the TFTP inspection; when TCP traffic for port 21 arrives, then the security appliance applies the FTP inspection. So in this case only, you can configure multiple inspections for the same rule. Normally, the security appliance does not use the port number to determine the inspection applied, thus giving you the flexibility to apply inspections to non-standard ports, for example.

Feature Matching Guidelines for Multiple Service Policies

For TCP and UDP traffic (and ICMP when you enable stateful ICMP inspection), service policies operate on traffic flows, and not just individual packets. If traffic is part of an existing connection that matches a feature in a policy on one interface, that traffic flow cannot also match the same feature in a policy on another interface; only the first policy is used.

For example, if HTTP traffic matches a policy on the inside interface to inspect HTTP traffic, and you have a separate policy on the outside interface for HTTP inspection, then that traffic is not also inspected on the egress of the outside interface. Similarly, the return traffic for that connection will not be inspected by the ingress policy of the outside interface, nor by the egress policy of the inside interface.

For traffic that is not treated as a flow, for example ICMP when you do not enable stateful ICMP inspection, returning traffic can match a different policy map on the returning interface. For example, if you configure IPS inspection on the inside and outside interfaces, but the inside policy uses virtual sensor 1 while the outside policy uses virtual sensor 2, then a non-stateful Ping will match virtual sensor 1 outbound, but will match virtual sensor 2 inbound.

Adding a Service Policy Rule for Through Traffic

To add a service policy rule for through traffic, perform the following steps:

Step 1 From the Configuration > Firewall > Service Policy Rules pane, click **Add**.

The Add Service Policy Rule Wizard - Service Policy dialog box appears.



Note When you click the Add button, and not the small arrow on the right of the Add button, you add a through traffic rule by default. If you click the arrow on the Add button, you can choose between a through traffic rule and a management traffic rule.

Step 2 In the Create a Service Policy and Apply To area, click one of the following options:

- **Interface.** This option applies the service policy to a single interface. Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with FTP inspection, and an interface policy with TCP connection limits, then both FTP inspection and TCP connection limits are applied to the interface. However, if you have a global policy with FTP inspection, and an interface policy with FTP inspection, then only the interface policy FTP inspection is applied to that interface.
 - a. Choose an interface from the drop-down list.

If you choose an interface that already has a policy, then the wizard lets you add a new service policy rule to the interface.
 - b. If it is a new service policy, enter a name in the Policy Name field.
 - c. (Optional) Enter a description in the Description field.
- **Global - applies to all interfaces.** This option applies the service policy globally to all interfaces. By default, a global policy exists that includes a service policy rule for default application inspection. See the [“Default Global Policy”](#) section on page 22-2 for more information. You can add a rule to the global policy using the wizard.

Step 3 Click **Next**.

The Add Service Policy Rule Wizard - Traffic Classification Criteria dialog box appears.

Step 4 Click one of the following options to specify the traffic to which to apply the policy actions:

- **Create a new traffic class.** Enter a traffic class name in the Create a new traffic class field, and enter an optional description.

Identify the traffic using one of several criteria:

- **Default Inspection Traffic**—The class matches the default TCP and UDP ports used by all applications that the security appliance can inspect.

This option, which is used in the default global policy, is a special shortcut that when used in a rule, ensures that the correct inspection is applied to each packet, based on the destination port of the traffic. For example, when UDP traffic for port 69 reaches the security appliance, then the security appliance applies the TFTP inspection; when TCP traffic for port 21 arrives, then the security appliance applies the FTP inspection. So in this case only, you can configure multiple inspections for the same rule (See the [“Incompatibility of Certain Feature Actions” section on page 22-5](#) for more information about combining actions). Normally, the security appliance does not use the port number to determine the inspection applied, thus giving you the flexibility to apply inspections to non-standard ports, for example.

See the [“Default Inspection Policy” section on page 24-3](#) for a list of default ports. The security appliance includes a default global policy that matches the default inspection traffic, and applies common inspections to the traffic on all interfaces. Not all applications whose ports are included in the Default Inspection Traffic class are enabled by default in the policy map.

You can specify a Source and Destination IP Address (uses ACL) class along with the Default Inspection Traffic class to narrow the matched traffic. Because the Default Inspection Traffic class specifies the ports and protocols to match, any ports and protocols in the access list are ignored.

- **Source and Destination IP Address (uses ACL)**—The class matches traffic specified by an extended access list. If the security appliance is operating in transparent firewall mode, you can use an EtherType access list.



Note When you create a new traffic class of this type, you can only specify one access control entry (ACE) initially. After you finish adding the rule, you can add additional ACEs by adding a new rule to the same interface or global policy, and then specifying **Add rule to existing traffic class** on the Traffic Classification dialog box (see below).

- **Tunnel Group**—The class matches traffic for a tunnel group to which you want to apply QoS. You can also specify one other traffic match option to refine the traffic match, excluding Any Traffic, Source and Destination IP Address (uses ACL), or Default Inspection Traffic.
- **TCP or UDP Destination Port**—The class matches a single port or a contiguous range of ports.



Tip For applications that use multiple, non-contiguous ports, use the Source and Destination IP Address (uses ACL) to match each port.

- **RTP Range**—The class map matches RTP traffic.
- **IP DiffServ CodePoints (DSCP)**—The class matches up to eight DSCP values in the IP header.
- **IP Precedence**—The class map matches up to four precedence values, represented by the TOS byte in the IP header.
- **Any Traffic**—Matches all traffic.
- **Add rule to existing traffic class.** If you already have a service policy rule on the same interface, or you are adding to the global service policy, this option lets you add an ACE to an existing access list. You can add an ACE to any access list that you previously created when you chose the Source and Destination IP Address (uses ACL) option for a service policy rule on this interface. For this traffic class, you can have only one set of rule actions even if you add multiple ACEs. You can add

multiple ACEs to the same traffic class by repeating this entire procedure. See the “[Managing the Order of Service Policy Rules](#)” section on page 22-13 for information about changing the order of ACEs.

- **Use an existing traffic class.** If you created a traffic class used by a rule on a different interface, you can reuse the traffic class definition for this rule. Note that if you alter the traffic class for one rule, the change is inherited by all rules that use that traffic class. If your configuration includes any **class-map** commands that you entered at the CLI, those traffic class names are also available (although to view the definition of the traffic class, you need to create the rule).
- **Use class default as the traffic class.** This option uses the class-default class, which matches all traffic. The class-default class is created automatically by the security appliance and placed at the end of the policy. If you do not apply any actions to it, it is still created by the security appliance, but for internal purposes only. You can apply actions to this class, if desired, which might be more convenient than creating a new traffic class that matches all traffic. You can only create one rule for this service policy using the class-default class, because each traffic class can only be associated with a single rule per service policy.

Step 5 Click **Next**.

Step 6 The next dialog box depends on the traffic match criteria you chose.



Note The Any Traffic option does not have a special dialog box for additional configuration.

- **Default Inspections**—This dialog box is informational only, and shows the applications and the ports that are included in the traffic class.
- **Source and Destination Address**—This dialog box lets you set the source and destination addresses:
 - Click Match or Do Not Match.**
The Match option creates a rule where traffic matching the addresses have actions applied. The Do Not Match option exempts the traffic from having the specified actions applied. For example, you want to match all traffic in 10.1.1.0/24 and apply connection limits to it, except for 10.1.1.25. In this case, create two rules, one for 10.1.1.0/24 using the Match option and one for 10.1.1.25 using the Do Not Match option. Be sure to arrange the rules so that the Do Not Match rule is above the Match rule, or else 10.1.1.25 will match the Match rule first.
 - In the Source field, enter the source IP address, or click the ... button to choose an IP address that you already defined in ASDM.
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
Enter **any** to specify any source address.
Separate multiple addresses by a comma.
 - In the Destination field, enter the destination IP address, or click the ... button to choose an IP address that you already defined in ASDM.
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
Enter **any** to specify any destination address.
Separate multiple addresses by a comma.
 - In the Service field, enter an IP service name or number for the destination service, or click the ... button to choose a service.

If you want to specify a TCP or UDP port number, or an ICMP service number, enter *protocollport*. For example, enter TCP/8080.

By default, the service is IP.

Separate multiple services by a comma.

- e. (Optional) Enter a description in the Description field.
- f. (Optional) To specify a source service for TCP or UDP, click the **More Options** area open, and enter a TCP or UDP service in the Source Service field.

The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.

- g. (Optional) To make the rule inactive, click the **More Options** area open, and uncheck **Enable Rule**.

This setting might be useful if you do not want to remove the rule, but want to turn it off.

- h. (Optional) To set a time range for the rule, click the **More Options** area open, and from the Time Range drop-down list, choose a time range.

To add a new time range, click the ... button. See the “[Configuring Time Ranges](#)” section on page 19-15 for more information.

This setting might be useful if you only want the rule to be active at predefined times.

- Tunnel Group—Choose a tunnel group from the Tunnel Group drop-down list, or click **New** to add a new tunnel group. See the “[IPSec Remote Access Connection Profiles](#)” section on page 35-49 for more information.

To police each flow, check **Match flow destination IP address**. All traffic going to a unique IP destination address is considered a flow.

- Destination Port—Click **TCP** or **UDP**.

In the Service field, enter a port number or name, or click ... to choose one already defined in ASDM.

- RTP Range—Enter an RTP port range, between 2000 and 65534. The maximum number of port sin the range is 16383.
- IP DiffServ CodePoints (DSCP)—In the DSCP Value to Add area, choose a value from the **Select Named DSCP Values** or enter a value in the **Enter DSCP Value (0-63)** field, and click **Add**.

Add additional values as desired, or remove them using the **Remove** button.

- IP Precedence—From the Available IP Precedence area, choose a value and click **Add**.

Add additional values as desired, or remove them using the **Remove** button.

Step 7 Click **Next**.

The Add Service Policy Rule - Rule Actions dialog box appears.

Step 8 Configure one or more rule actions according to the following sections:

- [Chapter 24, “Configuring Application Layer Protocol Inspection.”](#)
- [“Configuring Connection Settings” section on page 27-6](#)
- [Chapter 25, “Configuring QoS.”](#)
- [Chapter 28, “Configuring IPS.”](#)
- [Chapter 29, “Configuring Trend Micro Content Security.”](#)
- [Chapter 24, “Configuring MMP Inspection for a TLS Proxy”](#)

Step 9 Click **Finish**.

Adding a Service Policy Rule for Management Traffic

You can create a service policy for traffic directed to the security appliance for management purposes. This type of security policy can perform RADIUS accounting inspection and connection limits. This section includes the following topics:

- [RADIUS Accounting Inspection Overview, page 22-10](#)
- [Configuring a Service Policy Rule for Management Traffic, page 22-10](#)

RADIUS Accounting Inspection Overview

One of the well known problems is the over-billing attack in GPRS networks. The over-billing attack can cause consumers anger and frustration by being billed for services that they have not used. In this case, a malicious attacker sets up a connection to a server and obtains an IP address from the SGSN. When the attacker ends the call, the malicious server will still send packets to it, which gets dropped by the GGSN, but the connection from the server remains active. The IP address assigned to the malicious attacker gets released and reassigned to a legitimate user who will then get billed for services that the attacker will use.

RADIUS accounting inspection prevents this type of attack using by ensuring the traffic seen by the GGSN is legitimate. With the RADIUS accounting feature properly configured, the security appliance tears down a connection based on matching the Framed IP attribute in the Radius Accounting Request Start message with the Radius Accounting Request Stop message. When the Stop message is seen with the matching IP address in the Framed IP attribute, the security appliance looks for all connections with the source matching the IP address.

You have the option to configure a secret pre-shared key with the RADIUS server so the security appliance can validate the message. If the shared secret is not configured, the security appliance does not need to validate the source of the message and will only check that the source IP address is one of the configured addresses allowed to send the RADIUS messages.

Configuring a Service Policy Rule for Management Traffic

To add a service policy rule for management traffic, perform the following steps:

- Step 1** From the Configuration > Firewall > Service Policy Rules pane, click the down arrow next to Add.
- Step 2** Choose **Add Management Service Policy Rule**.
The Add Management Service Policy Rule Wizard - Service Policy dialog box appears.
- Step 3** In the Create a Service Policy and Apply To area, click one of the following options:
- **Interface**. This option applies the service policy to a single interface. Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with RADIUS accounting inspection, and an interface policy with connection limits, then

both RADIUS accounting and connection limits are applied to the interface. However, if you have a global policy with RADIUS accounting, and an interface policy with RADIUS accounting, then only the interface policy RADIUS accounting is applied to that interface.

- a. Choose an interface from the drop-down list.

If you choose an interface that already has a policy, then the wizard lets you add a new service policy rule to the interface.

- b. If it is a new service policy, enter a name in the Policy Name field.
 - c. (Optional) Enter a description in the Description field.
- **Global - applies to all interfaces.** This option applies the service policy globally to all interfaces. By default, a global policy exists that includes a service policy rule for default application inspection. See the [“Default Global Policy” section on page 22-2](#) for more information. You can add a rule to the global policy using the wizard.

Step 4 Click **Next**.

The Add Management Service Policy Rule Wizard - Traffic Classification Criteria dialog box appears.

Step 5 Click one of the following options to specify the traffic to which to apply the policy actions:

- **Create a new traffic class.** Enter a traffic class name in the Create a new traffic class field, and enter an optional description.

Identify the traffic using one of several criteria:

- **Source and Destination IP Address (uses ACL)**—The class matches traffic specified by an extended access list. If the security appliance is operating in transparent firewall mode, you can use an EtherType access list.



Note

When you create a new traffic class of this type, you can only specify one access control entry (ACE) initially. After you finish adding the rule, you can add additional ACEs by adding a new rule to the same interface or global policy, and then specifying **Add rule to existing traffic class** on the Traffic Classification dialog box (see below).

- **TCP or UDP Destination Port**—The class matches a single port or a contiguous range of ports.



Tip

For applications that use multiple, non-contiguous ports, use the Source and Destination IP Address (uses ACL) to match each port.

- **Add rule to existing traffic class.** If you already have a service policy rule on the same interface, or you are adding to the global service policy, this option lets you add an ACE to an existing access list. You can add an ACE to any access list that you previously created when you chose the Source and Destination IP Address (uses ACL) option for a service policy rule on this interface. For this traffic class, you can have only one set of rule actions even if you add multiple ACEs. You can add multiple ACEs to the same traffic class by repeating this entire procedure. See the [“Managing the Order of Service Policy Rules” section on page 22-13](#) for information about changing the order of ACEs.
- **Use an existing traffic class.** If you created a traffic class used by a rule on a different interface, you can reuse the traffic class definition for this rule. Note that if you alter the traffic class for one rule, the change is inherited by all rules that use that traffic class. If your configuration includes any **class-map** commands that you entered at the CLI, those traffic class names are also available (although to view the definition of the traffic class, you need to create the rule).

Step 6 Click **Next**.

Step 7 The next dialog box depends on the traffic match criteria you chose.

- Source and Destination Address—This dialog box lets you set the source and destination addresses:
 - a. Click **Match** or **Do Not Match**.

The Match option creates a rule where traffic matching the addresses have actions applied. The Do Not Match option exempts the traffic from having the specified actions applied. For example, you want to match all traffic in 10.1.1.0/24 and apply connection limits to it, except for 10.1.1.25. In this case, create two rules, one for 10.1.1.0/24 using the Match option and one for 10.1.1.25 using the Do Not Match option. Be sure to arrange the rules so that the Do Not Match rule is above the Match rule, or else 10.1.1.25 will match the Match rule first.
 - b. In the Source field, enter the source IP address, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any source address.

Separate multiple addresses by a comma.
 - c. In the Destination field, enter the destination IP address, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any destination address.

Separate multiple addresses by a comma.
 - d. In the Service field, enter an IP service name or number for the destination service, or click the ... button to choose a service.

If you want to specify a TCP or UDP port number, or an ICMP service number, enter *protocol/port*. For example, enter TCP/8080.

By default, the service is IP.

Separate multiple services by a comma.
 - e. (Optional) Enter a description in the Description field.
 - f. (Optional) To specify a source service for TCP or UDP, click the **More Options** area open, and enter a TCP or UDP service in the Source Service field.

The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
 - g. (Optional) To make the rule inactive, click the **More Options** area open, and uncheck **Enable Rule**.

This setting might be useful if you do not want to remove the rule, but want to turn it off.
 - h. (Optional) To set a time range for the rule, click the **More Options** area open, and from the Time Range drop-down list, choose a time range.

To add a new time range, click the ... button. See the “[Configuring Time Ranges](#)” section on [page 19-15](#) for more information.

This setting might be useful if you only want the rule to be active at predefined times.
- Destination Port—Click **TCP** or **UDP**.

In the Service field, enter a port number or name, or click ... to choose one already defined in ASDM.

Step 8 Click **Next**.

The Add Management Service Policy Rule - Rule Actions dialog box appears.

Step 9 To configure RADIUS accounting inspection, choose an inspect map from the RADIUS Accounting Map drop-down list, or click **Configure** to add a map.

See the [“RADIUS Accounting Field Descriptions”](#) section on page 22-14 for more information.

Step 10 To configure maximum connections, enter one or more of the following values in the 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.

Step 11 Click **Finish**.

Managing the Order of Service Policy Rules

The order of service policy rules on an interface or in the global policy affects how actions are applied to traffic. See the following guidelines for how a packet matches rules in a service policy:

- A packet can match only one rule in a service policy for each feature type.
- When the packet matches a rule that includes actions for a feature type, the security appliance does not attempt to match it to any subsequent rules including that feature type.
- If the packet matches a subsequent rule for a different feature type, however, then the security appliance also applies the actions for the subsequent rule.

For example, if a packet matches a rule for connection limits, and also matches a rule for application inspection, then both rule actions are applied.

If a packet matches a rule for application inspection, but also matches another rule that includes application inspection, then the second rule actions are not applied.

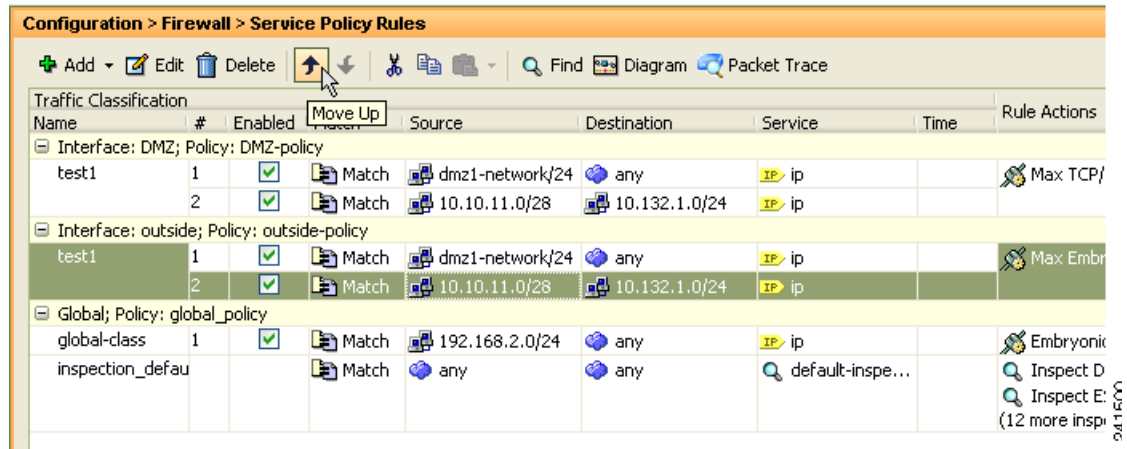
If your rule includes an access list with multiple ACEs, then the order of ACEs also affects the packet flow. The FWSM tests the packet against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an access list that explicitly permits all traffic, no further statements are ever checked.

To change the order of rules or ACEs within a rule, perform the following steps:

Step 1 From the Configuration > Firewall > Service Policy Rules pane, choose the rule or ACE that you want to move up or down.

Step 2 Click the Move Up or Move Down cursor (see [Figure 22-1](#)).

Figure 22-1 Moving an ACE



Note If you rearrange ACEs in an access list that is used in multiple service policies, then the change is inherited in all service policies.

Step 3 When you are done rearranging your rules or ACEs, click **Apply**.

RADIUS Accounting Field Descriptions

This section lists RADIUS accounting field descriptions, and includes the following topics:

- [Select RADIUS Accounting Map, page 22-14](#)
- [Add RADIUS Accounting Policy Map, page 22-15](#)
- [RADIUS Inspect Map, page 22-16](#)
- [RADIUS Inspect Map Host, page 22-16](#)
- [RADIUS Inspect Map Other, page 22-17](#)

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
•	•	•	•	—

RADIUS Inspect Map

The RADIUS pane lets you view previously configured RADIUS application inspection maps. A RADIUS map lets you change the default configuration values used for RADIUS application inspection. You can use a RADIUS map to protect against an overbilling attack.

Fields

- Name—Enter the name of the inspect map, up to 40 characters in length.
- Description—Enter the description of the inspect map, up to 200 characters in length.
- RADIUS Inspect Maps—Table that lists the defined RADIUS inspect maps. The defined inspect maps are also listed in the RADIUS area of the Inspect Maps tree.
- Add—Adds the new RADIUS inspect map to the defined list in the RADIUS Inspect Maps table and to the RADIUS area of the Inspect Maps tree. To configure the new RADIUS map, select the RADIUS entry in Inspect Maps tree.
- Delete—Deletes the application inspection map selected in the RADIUS Inspect Maps table and from the RADIUS area of the Inspect Maps tree.

Modes

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

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

RADIUS Inspect Map Host

The RADIUS Inspect Map Host Parameters pane lets you configure the host parameter settings for the inspect map.

Fields

- Name—Shows the name of the previously configured RADIUS accounting map.
- Description—Enter the description of the RADIUS accounting map, up to 200 characters in length.
- Host Parameters—Lets you configure host parameters.
 - 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.

Modes

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

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

RADIUS Inspect Map Other

The RADIUS Inspect Map Other Parameters pane lets you configure additional parameter settings for the inspect map.

Fields

- Name—Shows the name of the previously configured RADIUS accounting map.
- Description—Enter the description of the RADIUS accounting map, up to 200 characters in length.
- Other Parameters—Lets you configure additional parameters.
 - 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).
 - Enable detection of GPRS accounting—Enables detection of GPRS accounting. This option is only available when GTP/GPRS license is enabled.
 - Validate Attribute—Attribute information.
 - 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.

Modes

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

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

