

Configuring Service Policy Rules

This chapter describes how to enable service policy rules. Service policies provide a consistent and flexible way to configure FWSM 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, page 22-5](#)
- [Managing the Order of Service Policy Rules, page 22-8](#)

Service Policy Overview

A service policy is made up of one or more service policy rules. 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 22-2](#)
- [Feature Matching Guidelines, page 22-3](#)
- [Order in Which Multiple Feature Actions Within a Rule are Applied, page 22-3](#)
- [Incompatibility of Certain Feature Actions, page 22-4](#)
- [Feature Matching Guidelines for Multiple Service Policies, page 22-4](#)

Supported Features

Service policies support the following features:

- Connection settings
- Application inspection (multiple types)

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
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP

Feature Directionality

Actions are applied to traffic bidirectionally or unidirectionally depending on whether the service policy is applied to an interface or globally. For a service policy that is applied to an interface, all features are bidirectional; 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. 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.

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 FWSM 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 FWSM also applies the actions for the subsequent rule, if supported. See the [“Incompatibility of Certain Feature Actions” section on page 22-4](#) 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. Actions are performed in the following order:

1. Connection settings
2. 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. See the [“Incompatibility of Certain Feature Actions” section on page 22-4](#) 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

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 FWSM 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.

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 FWSM, then the FWSM applies the TFTP inspection; when TCP traffic for port 21 arrives, then the FWSM applies the FTP inspection. So in this case only, you can configure multiple inspections for the same rule. Normally, the FWSM 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 connection limits on the inside and outside interfaces, but the inside policy sets the maximum connections to 2000 while the outside policy sets the maximum connections to 3000, then a non-stateful Ping might be denied at a lower level if it is outbound than if it is inbound.

Adding a Service Policy Rule

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.

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 FWSM 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 FWSM, then the FWSM applies the TFTP inspection; when TCP traffic for port 21 arrives, then the FWSM 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 22-4](#) for more information about combining actions). Normally, the FWSM 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 23-3](#) for a list of default ports. The FWSM 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 or 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 FWSM 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) option to match each port.

- **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 22-8 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 FWSM and placed at the end of the policy. If you do not apply any actions to it, it is still created by the FWSM, 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:

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 19-13 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 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 23, “Configuring Application Layer Protocol Inspection.”](#)
 - [“Configuring Connection Settings and TCP State Bypass” section on page 26-1](#)
 - [“Using PISA to Permit or Deny Application Types” section on page 26-5](#)
- Step 9** 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 FWSM 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 FWSM 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**.
