

Service Policy

Service policies provide a consistent and flexible way to configure ASA 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. A service policy consists of multiple actions or rules applied to an interface or applied globally.

- About Service Policies, on page 1
- Guidelines for Service Policies, on page 7
- Defaults for Service Policies, on page 8
- Configure Service Policies, on page 9
- History for Service Policies, on page 15

About Service Policies

The following topics describe how service policies work.

The Components of a Service Policy

The point of service policies is to apply advanced services to the traffic you are allowing. Any traffic permitted by access rules can have service policies applied, and thus receive special processing, such as being redirected to a service module or having application inspection applied.

You can have these types of service policy:

- One global policy that gets applied to all interfaces.
- One service policy applied per interface. The policy can be a mix of classes for traffic going through the device and management traffic directed at the ASA interface rather than going through it,

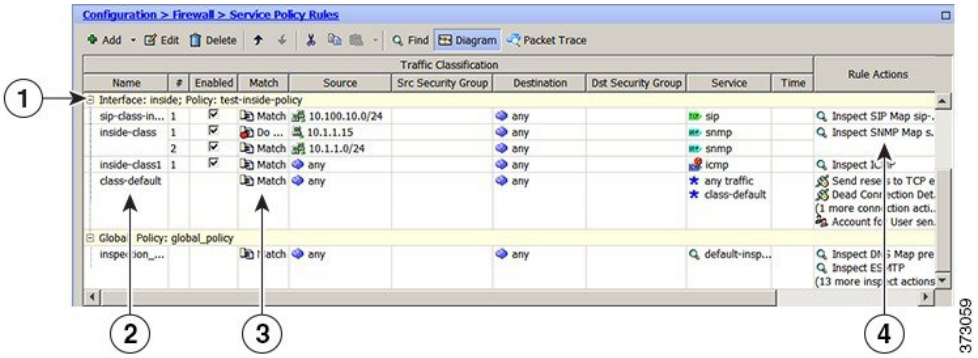
Each service policy is composed of the following elements:

1. Service policy map, which is the ordered set of rules, and is named on the **service-policy** command. In ASDM, the policy map is represented as a folder on the Service Policy Rules page.
2. Rules, each rule being a **class** command within the service policy map and the commands associated with the **class** command. In ASDM, each rule is shown on a separate row, and the name of the rule is the class name.

   The **class** command defines the traffic matching criteria for the rule.

The commands associated with class, such as **inspect**, **set connection timeout**, and so forth, define the services and constraints to apply to matching traffic. Note that inspect commands can point to inspection policy maps, which define actions to apply to inspected traffic. Keep in mind that inspection policy maps are not the same as service policy maps.

The following example compares how service policies appear in the CLI with how they appear in ASDM. Note that there is not a one-to-one mapping between the figure call-outs and lines in the CLI.



The following CLI is generated by the rules shown in the figure above.

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
```

```
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

Features Configured with Service Policies

The following table lists the features you configure using service policies.

Table 1: Features Configured with Service Policies

Feature	For Through Traffic?	For Management Traffic?	See:
Application inspection (multiple types)	**All** except RADIUS accounting	**RADIUS accounting** only	• Getting Started with Application Layer Protocol Inspection. • Inspection of Basic Internet Protocols. • Inspection for Voice and Video Protocols. • Inspection for Mobile Networks.
ASA FirePOWER (ASA SFR)	**Yes**	No	ASA FirePOWER Module.
NetFlow Secure Event Logging filtering	**Yes**	**Yes**	See the NetFlow implementation guide.
QoS input and output policing	**Yes**	No	Quality of Service.
QoS standard priority queue	**Yes**	No	Quality of Service.
TCP and UDP connection limits and timeouts, and TCP sequence number randomization	**Yes**	**Yes**	Connection Settings.
TCP normalization	**Yes**	No	Connection Settings.
TCP state bypass	**Yes**	No	Connection Settings.

Feature	For Through Traffic?	For Management Traffic?	See:
User statistics for Identity Firewall	**Yes**	**Yes**	See the **user-statistics** command in the command reference.

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 enters (or exits, depending on the feature) the interface to which you apply the policy map is affected. See the following table for the directionality of each feature.

Table 2: Feature Directionality

Feature	Single Interface Direction	Global Direction
Application inspection (multiple types)	Bidirectional	Ingress
ASA FirePOWER (ASA SFR)	Bidirectional	Ingress
NetFlow Secure Event Logging filtering	N/A	Ingress
QoS input policing	Ingress	Ingress
QoS output policing	Egress	Egress
QoS standard priority queue	Egress	Egress
TCP and UDP connection limits and timeouts, and TCP sequence number randomization	Bidirectional	Ingress
TCP normalization	Bidirectional	Ingress
TCP state bypass	Bidirectional	Ingress
User statistics for Identity Firewall	Bidirectional	Ingress

Feature Matching Within a Service Policy

A packet matches rules in a policy for a given interface according to the following rules:

1. A packet can match only one rule for an interface for each feature type.
2. When the packet matches a rule for a feature type, the ASA 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 ASA also applies the actions for the subsequent rule, if supported. See Incompatibility of Certain Feature Actions, on page 6 for more information about unsupported combinations.



Note Application inspection includes multiple inspection types, and most are mutually exclusive. For inspections that can be combined, each inspection is considered to be a separate feature.

Examples of Packet Matching

For example:

- If a packet matches a rule for connection limits, and also matches a rule for an application inspection, then both 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.
- If a packet matches a rule for HTTP inspection, but also matches another rule that includes FTP inspection, then the second rule actions are not applied because HTTP and FTP inspections cannot be combined.
- If a packet matches a rule for HTTP inspection, but also matches another rule that includes IPv6 inspection, then both actions are applied because the IPv6 inspection can be combined with any other type of inspection.

Order in Which Multiple Feature Actions 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 the table.

Actions are performed in the following order:

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



Note When a the ASA performs a proxy service (such as AAA) 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. Application inspections that can be combined with other inspections:
   a. IPv6
   b. IP options

c. WAAS

4. Application inspections that cannot be combined with other inspections. See Incompatibility of Certain Feature Actions, on page 6 for more information.
5. ASA FirePOWER (ASA SFR)
6. QoS output policing
7. QoS standard priority queue



Note NetFlow Secure Event Logging filtering and User statistics for Identity Firewall are order-independent.

Incompatibility of Certain Feature Actions

Some features are not compatible with each other for the same traffic. The following list might not include all incompatibilities; for information about compatibility of each feature, see the chapter or section for the feature:

- You cannot configure QoS priority queuing and QoS policing for the same set of traffic.
- Most inspections should not be combined with another inspection, so the ASA only applies one inspection if you configure multiple inspections for the same traffic. Exceptions are listed in Order in Which Multiple Feature Actions are Applied, on page 5.
- You cannot configure traffic to be sent to multiple modules.
- HTTP inspection is not compatible with ASA FirePOWER.



Note The Default Inspection Traffic traffic class, which is used in the default global policy, is a special CLI shortcut to match the default ports for all inspections. When used in a policy map, this class map 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 ASA, then the ASA applies the TFTP inspection; when TCP traffic for port 21 arrives, then the ASA applies the FTP inspection. So in this case only, you can configure multiple inspections for the same class map. Normally, the ASA does not use the port number to determine which inspection to apply, thus giving you the flexibility to apply inspections to non-standard ports, for example.

Feature Matching 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.

Guidelines for Service Policies

Inspection Guidelines

There is a separate topic that provides detailed guidelines for application inspection service policies. See Guidelines for Application Inspection.

IPv6 Guidelines

Supports IPv6 for the following features:

- Application inspection for several, but not all, protocols. For details, see Guidelines for Application Inspection.
- ASA FirePOWER
- NetFlow Secure Event Logging filtering
- SCTP state bypass
- TCP and UDP connection limits and timeouts, TCP sequence number randomization
- TCP normalization
- TCP state bypass
- User statistics for Identity Firewall

Class Map (Traffic Class) Guidelines

The maximum number of class maps (traffic classes) of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- Layer 3/4 class maps (for through traffic and management traffic).
- Inspection class maps
- Regular expression class maps
- **match** commands used directly underneath an inspection policy map

This limit also includes default class maps of all types, limiting user-configured class maps to approximately 235.

Service Policy Guidelines

- Interface service policies on ingress interfaces 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 normalization, then both FTP inspection and TCP normalization are applied to the interface. However,

if you have a global policy with FTP inspection, and an ingress interface policy with FTP inspection, then only the ingress interface policy FTP inspection is applied to that interface. If no ingress or global policy implements a feature, then an interface service policy on the egress interface that specifies the feature is applied.

- You can only apply one global policy. For example, you cannot create a global policy that includes feature set 1, and a separate global policy that includes feature set 2. All features must be included in a single policy.
- When you make service policy changes to the configuration, all *new* connections use the new service policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. Output for the **show** command will not include data about the old connections.

  For example, if you remove a QoS service policy from an interface, then add a modified version, then the **show service-policy** command only displays QoS counters associated with new connections that match the new service policy; existing connections on the old policy no longer show in the command output.

  To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. Use the **clear conn** or **clear local-host** commands.

Defaults for Service Policies

The following topics describe the default settings for service policies and the Modular Policy Framework.

Default Service Policy Configuration

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 for a particular feature.)

The default policy includes the following application inspections:

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC

- SIP
- NetBios
- TFTP
- IP Options

Default Class Maps (Traffic Classes)

The configuration includes a default Layer 3/4 class map (traffic class) that the ASA uses in the default global policy called Default Inspection Traffic; it matches the default inspection traffic. This class, which is used in the default global policy, is a special shortcut to match the default ports for all inspections.

When used in a policy, this class 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 ASA, then the ASA applies the TFTP inspection; when TCP traffic for port 21 arrives, then the ASA applies the FTP inspection. So in this case only, you can configure multiple inspections for the same class map. Normally, the ASA does not use the port number to determine which inspection to apply, thus giving you the flexibility to apply inspections to non-standard ports, for example.

Another class map that exists in the default configuration is called class-default, and it matches all traffic. This class map appears at the end of all Layer 3/4 policy maps and essentially tells the ASA to not perform any actions on all other traffic. If you use the class-default class (the Any traffic class in ASDM), use it for broader purposes like enabling TCP sequence randomization, TTL decrement, or any other optional attribute changes. Do not use it for inspection, or it can cause traffic disruptions. Some features are only available for class-default.

Configure Service Policies

Configuring a service policy consists of adding one or more service policy rules per interface or for the global policy. ASDM uses a wizard to take you through the process of creating a service policy. For each rule, you identify the following elements:

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

After you create a policy, you can add rules, move, edit, or delete rules or policies. The following topics explain how to configure service policies.

Add a Service Policy Rule for Through Traffic

To add a service policy rule for through traffic, use the Add Service Policy Rule wizard. You will be asked to choose the scope of the policy, for a specific interface or global:

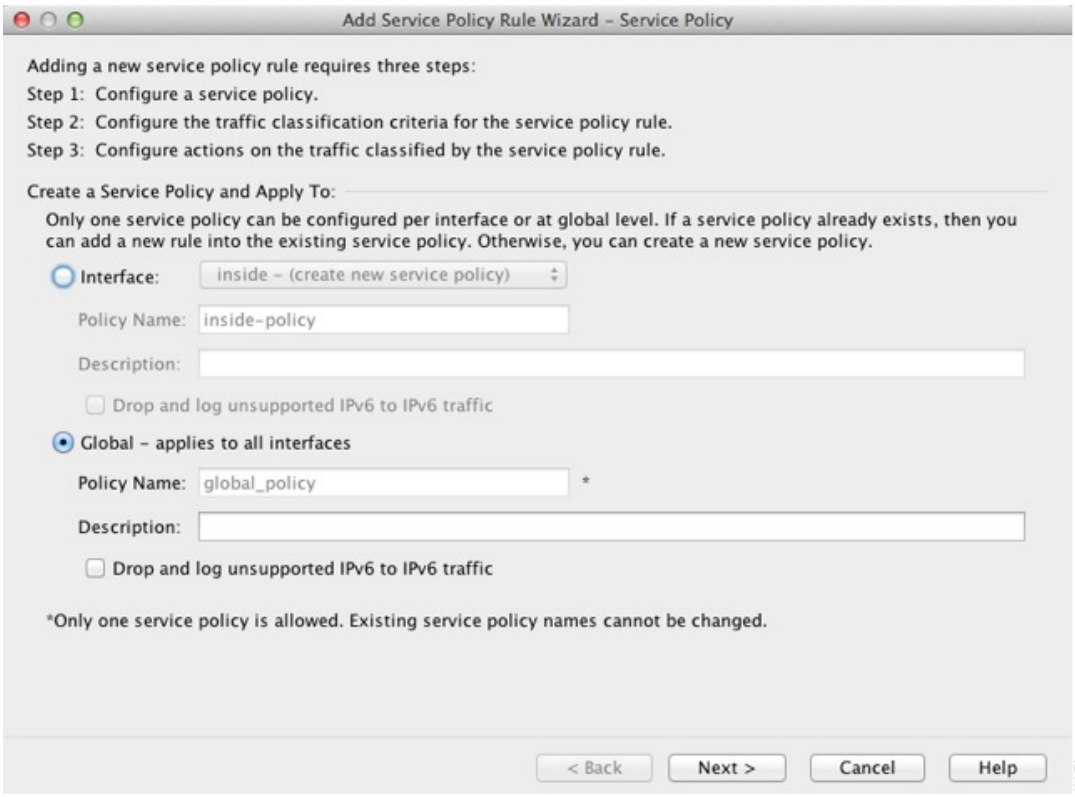
- Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with FTP inspection, and an interface policy with TCP connection limits, then both FTP inspection and TCP connection limits are applied to the interface. However, 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.

- Global service policies provide default services to all interfaces. Unless overridden by an interface-specific policy, the global services are applied. By default, a global policy exists that includes a service policy rule for default application inspection. You can add a rule to the global policy using the wizard.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Service Policy Rules**, and click **Add** or **Add** > **Add Service Policy Rule**.



Step 2 In the Create a Service Policy and Apply To area:

a) Choose whether the policy applies to a specific **Interface** or **Global** to all interfaces.
b) If you select Interface, choose the name of the interface. If the interface already has a policy, then you are adding a rule to the existing policy.
c) If the interface does not already have a service policy, enter the name of the new policy.
d) (Optional) Enter a description for the policy.
e) (Optional) Check the **Drop and log unsupported IPv6 to IPv6 traffic** option to generate a syslog (767001) for IPv6 traffic that is dropped by application inspections that do not support IPv6 traffic. By default, syslogs are not generated.
f) Click **Next**.

Step 3 On the Traffic Classification Criteria page, choose one of the following options to specify the traffic to which to apply the policy actions and click **Next**.

- **Create a new traffic class**. Enter a traffic class name and 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 ASA can inspect. When you click **Next**, you are shown the services and ports defined by this class.

    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 more information, see Default Class Maps (Traffic Classes), on page 9.

    See Default Inspections and NAT Limitations for a list of default ports. The ASA 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 class (which uses an ACL) 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 ACL are ignored.

  - **Source and Destination IP Address (uses ACL)**—The class matches traffic specified by an extended ACL. When you click **Next**, you are prompted for the attributes of the access control entry, and the wizard builds the ACL. Optionally, you can select an existing ACL.

    When defining the ACE, 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.

    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** (see below).

  - **Tunnel Group**—The class matches traffic for a tunnel group (connection profile) 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.

    When you click **Next**, you are prompted to select the tunnel group (you can create a new one if necessary). To police each flow, check **Match flow destination IP address**. All traffic going to a unique IP destination address is considered a flow.

  - **TCP or UDP or SCTP Destination Port**—The class matches a single port or a contiguous range of ports. When you click **Next**, you are prompted to choose the protocol and enter the port number; click **...** to choose one already defined in ASDM.

    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. When you click **Next**, you are prompted to enter an RTP port range, between 2000 and 65534. The maximum number of ports in the range is 16383.
- **IP DiffServ CodePoints (DSCP)**—The class matches up to eight DSCP values in the IP header. When you click **Next**, you are prompted to select or enter the desired values (move them into the Match on DSCP list).
- **IP Precedence**—The class map matches up to four precedence values, represented by the TOS byte in the IP header. When you click **Next**, you are prompted for the values.
- **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 ACL. You can add an ACE to any ACL 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. When you click **Next**, you are prompted for the attributes of the access control entry.
- **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 ASA and placed at the end of the policy. If you do not apply any actions to it, it is still created by the ASA, 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 4 If you selected a traffic matching criteria that requires additional configuration, enter the desired parameters and click **Next**.

Step 5 On the Rule Actions page, configure one or more rule actions. See Features Configured with Service Policies, on page 3 for a list of features and actions that you can apply, with pointers to additional details.

Step 6 Click **Finish**.

Add a Service Policy Rule for Management Traffic

To add a service policy rule for traffic directed to the ASA for management purposes, use the Add Service Policy Rule wizard. You will be asked to choose the scope of the policy, for a specific interface or global:

- 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.

- Global service policies provide default services to all interfaces. Unless overridden by an interface-specific policy, the global services are applied. By default, a global policy exists that includes a service policy rule for default application inspection. You can add a rule to the global policy using the wizard.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Service Policy Rules**, and click **Add** or **Add** > **Add Management Service Policy Rule**.

Step 2 In the Create a Service Policy and Apply To area:

a) Choose whether the policy applies to a specific **Interface** or **Global** to all interfaces.
b) If you select Interface, choose the name of the interface. If the interface already has a policy, then you are adding a rule to the existing policy.
c) If the interface does not already have a service policy, enter the name of the new policy.
d) (Optional) Enter a description for the policy.
e) Click **Next**.

Step 3 On the Traffic Classification Criteria page, choose one of the following options to specify the traffic to which to apply the policy actions and click **Next**.

- **Create a new traffic class**. Enter a traffic class name and 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 ACL. When you click **Next**, you are prompted for the attributes of the access control entry, and the wizard builds the ACL. Optionally, you can select an existing ACL.

    When defining the ACE, 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.

  - **TCP or UDP or SCTP Destination Port**—The class matches a single port or a contiguous range of ports. When you click **Next**, you are prompted to choose the protocol and enter the port number; click **...** to choose one already defined in ASDM.

    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 ACL. You can add an ACE to any ACL 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. When you click **Next**, you are prompted for the attributes of the access control entry.

- **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 4 If you selected a traffic matching criteria that requires additional configuration, enter the desired parameters and click **Next**.

Step 5 On the Rule Actions page, configure one or more rule actions.

- 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 Features Configured with Service Policies, on page 3 for more information.
- To configure connection settings, see Configure Connection Settings for Specific Traffic Classes (All Services).

Step 6 Click **Finish**.

Manage 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 ASA 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 ASA 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.

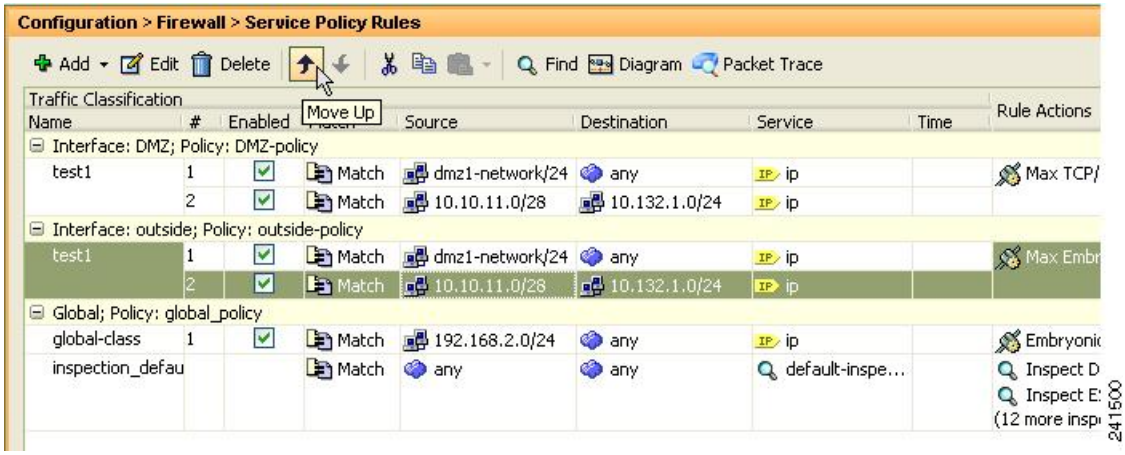
If your rule includes an ACL with multiple ACEs, then the order of ACEs also affects the packet flow. The ASA tests the packet against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an ACL 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:

Procedure

Step 1 On 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** button.



Note
If you rearrange ACEs in an ACL 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**.

History for Service Policies

Feature Name	Releases	Description
Modular Policy Framework	7.0(1)	Modular Policy Framework was introduced.
Management class map for use with RADIUS accounting traffic	7.2(1)	The management class map was introduced for use with RADIUS accounting traffic. The following commands were introduced: **class-map type management**, and **inspect radius-accounting**.
Inspection policy maps	7.2(1)	The inspection policy map was introduced. The following command was introduced: **class-map type inspect**.
Regular expressions and policy maps	7.2(1)	Regular expressions and policy maps were introduced to be used under inspection policy maps. The following commands were introduced: **class-map type regex**, **regex**, **match regex**.
Match any for inspection policy maps	8.0(2)	The **match any** keyword was introduced for use with inspection policy maps: traffic can match one or more criteria to match the class map. Formerly, only **match all** was available.