



CHAPTER 23

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 23-1](#)
- [Adding a Service Policy Rule for Through Traffic, page 23-4](#)
- [Adding a Service Policy Rule for Management Traffic, page 23-10](#)

Service Policy Overview

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

- [Supported Features, page 23-1](#)
- [Service Policy Elements, page 23-2](#)
- [Default Global Policy, page 23-2](#)

Supported Features

Security policies support the following features:

- TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization
- CSC
- Application inspection
- IPS
- QoS input policing
- QoS output policing
- QoS priority queue

Service Policy Elements

Configuring a service policy consists of the following elements:

1. Create the service policy by identifying the interface to which you want to apply the policy, or by configuring a global policy. You can only have one service policy per interface, and one global service policy.
2. Identify the traffic to which you want to apply actions. You can identify Layer 3 and 4 through traffic or Layer 3 and 4 management traffic. You can identify multiple traffic classes for each service policy.
3. Apply actions to each 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 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 23-1](#) for the directionality of each feature.

Table 23-1 Feature Directionality

Feature	Single Interface Direction	Global Direction
TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization	Bidirectional	Ingress
CSC	Bidirectional	Ingress
Application inspection	Bidirectional	Ingress
IPS	Bidirectional	Ingress
QoS input policing	Ingress	Ingress
QoS output policing	Egress	Egress
QoS priority queue	Egress	Egress

Feature Matching Guidelines for Rules in a Service Policy

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.

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.

Order in Which Multiple Feature Actions are Applied

Actions within a rule are performed in the following order:

- 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.

- CSC
- Application inspection
- IPS
- QoS input policing
- QoS output policing
- QoS priority queue

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. The interface policy overrides the global policy.
 - 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 23-2 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.

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 to match, any ports 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.
- **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.
- **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 using the class-default class, because each traffic class can only be associated with a single rule.

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 8-14](#) 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 [“Add IPSec Remote Access Connection and Add SSL VPN Access Connection” section on page 32-61](#) 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](#)
- [“QoS Tab Field Information” section on page 28-2](#)
- [Chapter 39, “Configuring IPS.”](#)
- [Chapter 40, “Configuring Trend Micro Content Security.”](#)

Step 9 Click **Finish**.

Edit Service Policy

The Edit Service Policy dialog box lets you edit the description of the service policy.

Fields

- **Name**—Shows the name of the service policy.
- **Applied To**—Shows what the service policy applies to.
- **Description**—Enter the description of the service policy, up to 100 characters in length.

Modes

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

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

Edit Service Policy Rules

The Edit Service Policy Rules dialog box lets you edit the settings for the service policy.

Fields

- Traffic Match Criteria—Lets you edit the traffic class settings.
 - Default Inspection Traffic—The class matches the default TCP and UDP ports used by all applications that the security appliance can inspect.

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 to match, any ports 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.
 - 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.
- ACL tab—Lets you set the source and destination addresses:
 - Action—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.

- Source—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.

- Destination—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.

- Service—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.

- Description—(Optional) Enter a description.
- More Options—(Optional) To specify a source service for TCP or UDP, 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.

Enable Rule—(Optional) To make the rule inactive, uncheck Enable Rule. This setting might be useful if you do not want to remove the rule, but want to turn it off.

- Time Range—(Optional) To set a time range for the rule, choose a time range.

To add a new time range, click the ... button. See the “[Configuring Time Ranges](#)” section on [page 8-14](#) for more information.

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

Modes

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

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

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 23-10](#)
- [Configuring a Service Policy Rule for Management Traffic, page 23-10](#)

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. The interface policy overrides the global policy.
 - 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 23-2 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 Enter a traffic class name in the Create a new traffic class field, and enter an optional description.

Step 6 Identify the traffic using one of the following 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.
- 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.

Step 7 Click **Next**.

Step 8 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 *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 8-14](#) 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 9 Click **Next**.

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

Step 10 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 23-13](#) for more information.

Step 11 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.
- **Per Client Connections**—Specifies the maximum number of simultaneous TCP and UDP connections for each client. When a new connection is attempted by a client that already has opened the maximum per-client number of connections, the security appliance rejects the connection and drops the packet.
- **Per Client Embryonic Connections**—Specifies the maximum number of simultaneous TCP embryonic connections for each client. When a new TCP connection is requested by a client that already has the maximum per-client number of embryonic connections open through the security appliance, the security appliance proxies the request to the TCP Intercept feature, which prevents the connection.

Step 12 Click **Finish**.

RADIUS Accounting Field Descriptions

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

- [Select RADIUS Accounting Map, page 23-13](#)
- [Add RADIUS Accounting Policy Map, page 23-13](#)
- [RADIUS Inspect Map, page 23-14](#)
- [RADIUS Inspect Map Host, page 23-15](#)
- [RADIUS Inspect Map Other, page 23-15](#)

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
•	•	•	•	—