Configuring Traffic Policies

Date: 1/26/11

Cisco Application Networking Manager helps you configure class maps and policy maps to provide a global level of classification for filtering traffic received by or passing through the ACE.

Note When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), enter an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you are using ANM with an ACE module or ACE appliance and you configure a named object at the ACE CLI, keep in mind that ANM does not support all of the special characters that the ACE CLI allows you to use when configuring a named object. If you use special characters that ANM does not support, you may not be able to import or manage the ACE using ANM.

This chapter includes the following sections:

Traffic Policy Overview

Cisco Application Networking Manager helps you configure class maps and policy maps to provide a global level of classification for filtering traffic received by or passing through the ACE. You create traffic policies and attach these policies to one or more VLAN interfaces associated with the ACE to apply feature-specific actions to the matching traffic. The ACE uses the individual traffic policies to implement functions such as:

- FTP command inspection
- IP normalization and fragment reassembly
- Network Address Translation (NAT)

- Optimization of HTTP traffic

- Protocol deep packet inspection

- Remote access using Secure Shell (SSH) or Telnet

- Secure Socket Layer (SSL) security services between a Web browser (the client) and the HTTP connection (the server)

- Server load balancing

- TCP termination, normalization, and reuse

Related Topics

- Class Map and Policy Map Overview, page 13-2

- Configuring Virtual Context Class Maps, page 13-6

- Configuring Virtual Context Policy Maps, page 13-31

Class Map and Policy Map Overview

You classify inbound network traffic destined to, or passing through, the ACE based on a series of flow match criteria specified by a class map. Each class map defines a traffic classification; that is, network traffic that is of interest to you. A policy map defines a series of actions (functions) that you want applied to a set of classified inbound traffic.

Class maps enable you to classify network traffic based on the following criteria:

- Layer 3 and Layer 4 traffic flow information—Source or destination IP address, source or destination port, virtual IP address, or IP protocol

- Layer 7 protocol information—HTTP cookie, HTTP URL, HTTP header, HTTP content, FTP request commands, RADIUS, RDP, RTSP, Skinny, or SIP

The policies that you can configure depend on the ACE you are configuring. Table 13-1 lists the available policies and the ACE devices that support them.

Table 13-1   Traffic Policies and ACE Device Support

Policy Map Type	Description	ACE Device	
		ACE Module	ACE Appliance
Layer 3/4 Management Traffic (First-Match)	Layer 3 and Layer 4 policy map for network management traffic received by the ACE	X	X
Layer 3/4 Network Traffic (First-Match)	Layer 3 and Layer 4 policy map for traffic passing through the ACE	X	X
Layer 7 Command Inspection - FTP (First-Match)	Layer 7 policy map for inspection of FTP commands	X	X
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Layer 7 policy map for inspection of HTTP packets	X	X
Layer 7 Deep Packet Inspection - SIP (All-Match)	Layer 7 policy map for inspection of SIP packets	X	X
Layer 7 Deep Packet Inspection - Skinny	Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)	X	X

Table 13-1   Traffic Policies and ACE Device Support (continued)

Policy Map Type	Description	ACE Device	
		ACE Module	ACE Appliance
Layer 7 HTTP Optimization (First-Match)	Layer 7 policy map for optimizing HTTP traffic		X
Layer 7 Server Load Balancing (First-Match)	Layer 7 policy map for HTTP server load balancing	X	X
Server Load Balancing - Generic (First-Match)	Generic Layer 7 policy map for server load balancing	X	X
Server Load Balancing - RADIUS (First-Match)	Layer 7 policy map for RADIUS server load balancing	X	X
Server Load Balancing - RDP (First-Match)	Layer 7 policy map for RDP server load balancing	X	X
Server Load Balancing - RTSP (First-Match)	Layer 7 policy map for RTSP server load balancing	X	X
Server Load Balancing - SIP (First-Match)	Layer 7 policy map for SIP server load balancing	X	X

The traffic classification process consists of the following three steps:

1. Creating a class map, which comprise a set of match criteria related to Layer 3 and Layer 4 traffic classifications or Layer 7 protocol classifications.

2. Creating a policy map, which refers to the class maps and identifies a series of actions to perform based on the traffic match criteria.

3. Activating the policy map and attaching it to a specific VLAN interface or globally to all VLAN interfaces associated with a context by configuring a virtual context global traffic policy to filter traffic received by the ACE.

The following overview topics describe the components that define a traffic policy:

- Class Maps, page 13-3
- Policy Maps, page 13-4
- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 13-5
- Applying a Policy Map Globally to All VLAN Interfaces, page 5-33

Class Maps

A class map defines each type of Layer 3 and Layer 4 traffic class and each Layer 7 protocol class. You create class maps to classify the traffic received and transmitted by the ACE as follows:

- Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE or network management traffic that can be received by the ACE.
- Layer 7 protocol-specific classes identify:
  - Server load-balancing traffic on generic, HTTP, RADIUS, RTSP, or SIP traffic
  - HTTP or SIP traffic for deep packet inspection
  - FTP traffic for inspection of commands

A traffic class contains the following components:

- Class map name
- Class map type
- One or more match conditions that define the match criteria for the class map
- Instructions on how the ACE evaluates match conditions when you specify more than one match statement in a traffic class (match-any, match-all)

The individual match conditions specify the criteria for classifying Layer 3 and Layer 4 network traffic as well as the Layer 7 server load balancing and application protocol-specific fields. The ACE evaluates the packets to determine whether they match the specified criteria. If a statement matches, the ACE considers that packet to be a member of the class and forwards the packet according to the specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class if one is specified.

The ACE allows you to configure two Layer 7 load-balancing class maps in a nested traffic class configuration to create a single traffic class. You can nest Layer 7 class maps to achieve complex logical expressions. The ACE restricts the nesting of class maps to two levels to prevent you from including one nested class map under a different class map.

Related Topics

Policy Maps

A policy map creates the traffic policy. The purpose of a traffic policy is to implement specific ACE functions associated with a traffic class. A traffic policy contains the following components:

- Policy map name
- Previously created traffic class map or, optionally, the class-default class map
- One or more of the individual Layer 3 and Layer 4 or Layer 7 policies that specify the actions to be performed by the ACE

A Layer 7 policy map is always associated within a Layer 3 and Layer 4 policy map to provide an entry point for traffic classification. Layer 7 policy maps are considered to be child policies and can only be nested under a Layer 3 and Layer 4 policy map. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface; a Layer 7 policy map cannot be directly applied on an interface. For example, to associate a Layer 7 load-balancing policy map, you nest the load-balancing policy map by using the Layer 3 and Layer 4 Policy map action type.

If none of the classifications specified in policy maps match, then the ACE executes the default actions specified against the class map configured with the Use Class Default option to use a default class map (if specified). All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. The Use Class Default feature has an implicit **match-any** match statement and is used to match any traffic classification.

The ACE supports flexible class map ordering within a policy map. The ACE executes only the actions for the first matching traffic classification, so the order of class maps within a policy map is very important. The policy lookup order is based on the security features of the ACE. The policy lookup order is implicit, irrespective of the order in which you configure policies on the interface.

The policy lookup order of the ACE is as follows:

1. Access control (permit or deny a packet)

2. Permit or deny management traffic

3. TCP/UDP connection parameters

4. Load balancing based on a virtual IP (VIP)

5. Application protocol inspection

6. Source NAT

7. Destination NAT

The sequence in which the ACE applies the actions for a specific policy is independent of the actions configured for a class map inside a policy.

Related Topics

- Class Map and Policy Map Overview, page 13-2

- Class Maps, page 13-3

- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 13-5

- Configuring Traffic Policies, page 13-1

- Configuring Virtual Context Policy Maps, page 13-31

Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps

Parameter maps allow you to combine related actions in a Layer 3 and Layer 4 policy map. For example, an HTTP parameter map provides a means of performing actions on traffic ingressing an ACE interface based on certain criteria such as HTTP header and cookie settings, server connection reuse, action to be taken when an HTTP header, cookie, or URL exceeds a configured maximum length, and so on.

The ACE uses policy maps to combine class maps and parameter maps into traffic policies and to perform certain configured actions on the traffic that matches the specified criteria in the policies.

See Table 9-1 for a list of the available parameter maps and the ACE devices that support them.

Related Topic

- Configuring Parameter Maps, page 9-1

- Class Map and Policy Map Overview, page 13-2

- Class Maps, page 13-3

- Policy Maps, page 13-4

Protocol Inspection Overview

Certain applications require special handling of the data portion of a packet as the packets pass through the ACE. Application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic passing through the ACE. Based on the specifications of the traffic policy, the ACE accepts or rejects the packets to ensure the secure use of applications and services.

For information about application protocol inspection as configured and performed by the ACE, see the related topics.

Related Topics

- Configuring Virtual Context Policy Maps, page 13-31
- Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 13-22
- Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 13-51
- Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 13-68

Configuring Virtual Context Class Maps

You can create a class map to classify the traffic received and transmitted by the ACE. For more information about class maps, see the "Class Maps" section on page 13-3.

> **Note** To delete a class map from a context, the class map must no longer be in use. To delete multiple class maps, none of the class maps must be in use. If you attempt to delete multiple class maps and one of the class maps is still in use, none of the class maps are deleted and a message appears stating that one of the class maps is in use. Remove the class map that is still in use from your selection, then click **Delete**. The selected class maps are removed.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2   In the Class Maps table, click **Add** to add a new class map, or choose an existing class map and click **Edit** to modify it.

Step 3   (Optional) Enter a class map identifier number.

The Name field contains an automatically incremented number for the class map. You can leave the number as it is or enter a different, unique number.

Step 4   In the Class Map Type field, choose the type of class map that you are creating.

The types that are available depend on the ACE that you are configuring. Table 13-2 lists the available class map types and the ACE devices that support them.

Table 13-2   ***Class Maps and ACE Device Support***

	ACE Devices	
Class Map	**ACE Module**	**ACE Appliance**
Layer 3/4 Management Traffic	X	X
Layer 3/4 Network Traffic	X	X
Layer 7 Command Inspection - FTP	X	X
Layer 7 Deep Packet Inspection - HTTP	X	X
Layer 7 Deep Packet Inspection - SIP	X	X
Layer 7 Server Load Balancing	X	X
Server Load Balancing - Generic	X	X
Server Load Balancing - RADIUS	X	X
Server Load Balancing - RTSP	X	X
Server Load Balancing - SIP	X	X

Step 5   In the Match Type field, choose the method to be used to evaluate multiple match statements when multiple match conditions exist:

  • **All**—A match exists only if all match conditions are satisfied. If you choose All, you can specify multiple types of match conditions.

  • **Any**—A match exists if at least one of the match conditions is satisfied. If you choose Any, you can specify only one type of match condition.

This field does not appear for Layer 7 Command Inspection - FTP class maps.

Step 6   In the Description field, enter a brief description for the class map.

Step 7   Do one of the following:

  • Click **Deploy Now** to deploy this configuration on the ACE and to configure match conditions for the class map. See Setting Match Conditions for Class Maps, page 13-8 for more information.

  • Click **Cancel** to exit the procedure without saving your entries and to return to the Class Maps table.

  • Click **Next** to deploy your entries and to configure another class map.

Related Topics

  • Information About Virtual Contexts, page 5-2

  • Deleting Class Maps, page 13-8

  • Setting Match Conditions for Class Maps, page 13-8

  • Configuring Virtual Context Policy Maps, page 13-31

Deleting Class Maps

You can delete a class map. To delete a class map from a context, the class map must no longer be in use. To delete multiple class maps, none of the class maps must be in use.

Assumption

The class map to be deleted is not being used.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2 In the Class Maps table, choose the class maps that you want to delete and click **Delete**.

A confirmation popup window appears, asking you to confirm the deletion.

If you attempt to delete multiple class maps and one of the class maps is still in use, none of the class maps are deleted and a message appears stating that one of the class map is in use. Remove the class map that is still in use from your selection, then click **Delete**. The Class Maps table refreshes and the deleted class maps no longer appear.

Step 3 Do one of the following:

- Click **OK** to confirm the deletion.
- Click **Cancel** to retain the class map and to return to the Class Maps table.

Related Topics

- Class Map and Policy Map Overview, page 13-2
- Configuring Virtual Context Class Maps, page 13-6

Setting Match Conditions for Class Maps

Table 13-3 lists the class maps available for all ACE devices and provides links to topics for setting match conditions:

Table 13-3   Class Maps Available for All ACE Devices

Class Map	Related Topic
Layer 3/Layer 4 management traffic	Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 13-12
Layer 3/Layer 4 network traffic	Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 13-9
Layer 7 FTP command inspection	Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 13-22
Layer 7 HTTP deep packet inspection	Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps, page 13-16
Layer 7 server load balancing	Setting Match Conditions for Layer 7 Server Load Balancing Class Maps, page 13-14

Table 13-3   Class Maps Available for All ACE Devices (continued)

Class Map	Related Topic
Generic server load balancing	Setting Match Conditions for Generic Server Load Balancing Class Maps, page 13-23
Layer 7 SIP deep packet inspection	Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps, page 13-29
RADIUS server load balancing	Setting Match Conditions for RADIUS Server Load Balancing Class Maps, page 13-24
RTSP server load balancing	Setting Match Conditions for RTSP Server Load Balancing Class Maps, page 13-26
SIP server load balancing	Setting Match Conditions for SIP Server Load Balancing Class Maps, page 13-27

Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps

You can match criteria for a Layer 3/Layer 4 network traffic class map on the ACE.

Assumption

You have configured a Layer 3/Layer 4 network traffic class map and want to establish match conditions.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2   In the Class Maps table, choose the Layer 3/4 network traffic class map that you want to set match conditions for.

The Match Condition table appears.

Step 3   In the Match Condition table, click **Add** to add match criteria, or choose the match condition you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4   In the Sequence Number field of the Match Condition configuration window, enter a value from 2 to 255.

Step 5   In the Match Condition Type field, choose the type of match condition to use for this class map and configure any match-specific attributes as described in Table 13-4.

Table 13-4   Layer 3/Layer 4 Network Traffic Class Map Match Conditions

Match Condition	Description
Access List	Access list that is the match type for this match condition. In the ACL field, choose the ACL to use as the match condition.
Any	Any Layer 3 or Layer 4 traffic passing through the ACE meets the match condition.

Table 13-4   *Layer 3/Layer 4 Network Traffic Class Map Match Conditions (continued)*

Match Condition	Description
Destination Address	Destination address that is the match type for this match condition. Do the following: **a.** In the Destination Address field, enter the destination IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **b.** In the Destination Netmask field, choose the subnet mask for the destination IP address.
Port	UDP or TCP port or range of ports that is the match type for this match condition. Do the following: **a.** In the Port Protocol field, choose TCP or UDP as the protocol to match. **b.** In the Port Operator field, choose the match criteria for the port. Choices are as follows: – **Any**—Any port using the selected protocol meets the match condition. – **Equal To**—Specific port using the protocol meets the match condition. – In the Port Number field, enter the port to be matched. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE is to include all ports. – **Range**—Port must be one of a range of ports to meet the match condition. Do the following: **1**. In the Lower Port Number field, enter the first port number in the port range for the match condition. **2**. In the Upper Port Number field, enter the last port number in the port range for the match condition. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE is to include all ports.
Source Address	Source IP address that is the match type for this match condition. Do the following: **a.** In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **b.** In the Source Netmask field, choose the subnet mask for the source IP address.

Table 13-4   *Layer 3/Layer 4 Network Traffic Class Map Match Conditions (continued)*

Match Condition	Description
Virtual Address	Virtual IP address that is the match type for this match condition. Do the following: **a.** In the Virtual IP Address field, enter the virtual server IP (VIP) address to match in dotted-decimal format, such as 192.168.11.1. **b.** In the Virtual IP Netmask field, choose the subnet mask for the virtual IP address. **c.** In the Virtual Address Protocol field, choose the protocol to be used for this match condition. For a list of protocols and their respective numbers, see Table 5-20. **Note** Depending on the protocol that you choose, such as TCP or UDP, additional fields appear. If they appear, enter the information described in the following steps. **d.** In the Port Operator field, choose the match criteria for the port: – **Any**—Any port using the selected protocol meets the match condition. – **Equal To**—A specific port using the protocol meets the match condition. – In the Port Number field, enter the port to be matched. Valid entries are from 0 to 65535. A value of 0 indicates that the ACE is to include all ports. – **Range**—The port must be one of a range of ports to meet the match condition. Valid entries are from 0 to 65535. A value of 0 indicates that the ACE is to include all ports. Do the following: **1**. In the Lower Port Number field, enter the first port number in the port range for the match condition. **2**. In the Upper Port Number field, enter the last port number in the port range for the match condition.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

Note   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- Configuring Traffic Policies, page 13-1

- Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 13-12

Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps

You can identify the network management protocols that can be received by the ACE.

Assumption

You have configured a Layer 3/Layer 4 network management class map and want to establish match conditions.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2   In the Class Maps table, choose the Layer 3/Layer 4 management class map that you want to set match conditions for.

The Match Condition table appears.

Step 3   In the Match Condition table, click **Add** to add match criteria, or choose the match conditions that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4   Enter the match conditions (see Table 13-5).

Table 13-5   Layer 3/Layer 4 Management Traffic Class Map Match Conditions

Field	Description
Sequence Number	Number from 2 to 255 as the line number. The number entered here does not indicate a priority or sequence for the match conditions.
Match Condition Type	Confirm that **Management** is selected. **Note** To change the type of match condition, you must delete the class map and add it again with the correct match type.

Table 13-5   Layer 3/Layer 4 Management Traffic Class Map Match Conditions (continued)

Field	Description
Management Protocol Type	Field that identifies the network management protocols that can be received by the ACE. Choose the allowed protocol for this match condition as follows: • **HTTP**—Specifies the Hypertext Transfer Protocol (HTTP). • **HTTPS**—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the ANM GUI on the ACE. • **ICMP**—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping. • **SNMP**—Specifies the Simple Network Management Protocol (SNMP). • **SSH**—Specifies a Secure Shell (SSH) connection to the ACE. • **TELNET**—Specifies a Telnet connection to the ACE. • **KAL-AP-UDP**—Specifies the KeepAlive Appliance Protocol over UDP. • **XML-HTTPS**—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE and a Network Management System (NMS). Communication is performed using port 10443. This option is available for ACE appliances only.
Traffic Type	Type of traffic: • **Any**—Any client source IP address meets the match condition. • **Source Address**—A specific source IP address is part of the match condition.
Source Address	Field that appears if Source Address is selected for Traffic Type. Enter the source IP address of the client in dotted-decimal notation, such as 192.168.11.1.
Source Netmask	Field that appears if Source Address is selected for Traffic Type. Choose the subnet mask for the source IP address.

Step 5   Do one of the following:

• Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

> **Note**   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

• Click **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.

• Click **Next** to deploy your entries and to configure additional match conditions.

Related Topics

• Configuring Traffic Policies, page 13-1

• Configuring Virtual Context Class Maps, page 13-6

• Configuring Real Servers, page 7-5

• Configuring Server Farms, page 7-22

    • Configuring Sticky Groups, page 8-7

Setting Match Conditions for Layer 7 Server Load Balancing Class Maps

You can set match conditions for Layer 7 server load balancing class maps.

Assumption

You have configured a load-balancing class map and want to establish the match conditions.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2 In the Class Maps table, choose the Layer 7 server load balancing class map you want to set match conditions for.

The Match Condition table appears.

Step 3 In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4 In the Sequence Number field, enter a value from 2 to 255 as the line number.

The number entered here does not indicate a priority or sequence for the match conditions.

Step 5 In the Match Condition Type field, choose the type of match to use and configure condition-specific attributes as described in Table 13-6.

Table 13-6   Layer 7 Server Load Balancing Class Map Match Conditions

Match Condition	Description
Class Map	Class map that is to be used to establish a match condition.
	In the Class Map field, choose the class map to apply to this match condition.
HTTP Content	Specific content contained within the HTTP entity-body that is used to establish a match condition.
	Do the following:
	a. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.
	b. In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255.

Table 13-6   *Layer 7 Server Load Balancing Class Map Match Conditions (continued)*

Match Condition	Description
HTTP Cookie	HTTP cookie that is to be used to establish a match condition. Do the following: **a.** In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **b.** In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. **c.** Check the Secondary Cookie Matching check box to instruct the ACE to use both the cookie name and the cookie value to satisfy this match condition. Uncheck this check box to indicate that the ACE is to use either the cookie name or the cookie value to satisfy this match condition.

HTTP Header	HTTP header that is to be used to establish a match condition.
	Do the following:
	
	a. In the Header Name field, specify the header to match in one of the following ways:
	
	   – To specify an HTTP header that is not one of the standard HTTP headers, click the first radio button, and enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
	
	   – To specify a standard HTTP header, click the second radio button, and choose an HTTP header from the list.
	
	b. In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string in quotes. See Table 13-34 for a list of the supported characters that you can use in regular expressions.

HTTP URL	Portion of an HTTP URL that is to be used to establish a match condition. Do the following: **a.** In the URL Expression field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following www.*hostname.domain*. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. **b.** In the Method Expression field, enter the HTTP method to match. Valid entries are method names entered as unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. You can enter either one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).
Source Address	Source IP address that is to be used to establish a match condition. Do the following: **a.** In the Source Address field, enter the source IP address of the client in dotted-decimal notation, such as 192.168.11.1. **b.** In the Source Netmask field, choose the subnet mask of the source IP address.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

    ✎

    Note   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps

You can configure a Layer 7 class map for deep packet inspection of HTTP traffic by the ACE. When these features are configured, the ACE performs a stateful deep packet inspection of the HTTP protocol and permits or restricts traffic based on the actions in the defined policy maps. You can configure the following security features as part of HTTP deep packet inspection to be performed by the ACE:

- Regular expression matching on name in an HTTP header, URL name, or content expressions in an HTTP entity body
- Content, URL, and HTTP header length checks
- MIME-type message inspection
- Transfer-encoding methods
- Content type verification and filtering
- Port 80 misuse by tunneling protocols
- RFC compliance monitoring and RFC method filtering

Use this procedure to configure a Layer 7 class map for deep packet inspection of HTTP traffic.

Assumption

You have configured a Layer 7 HTTP deep packet inspection class map and want to establish match conditions.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2   In the Class Maps table, choose the Layer 7 HTTP deep packet inspection class map that you want to set match conditions for.

The Match Condition table appears.

Step 3   In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4   In the Sequence Number field of the Match Condition configuration window, enter a value from 2 to 255 as the line number.

The number entered here does not indicate a priority or sequence for the match conditions.

Step 5   In the Match Condition Type field, choose the method that match decisions are to be made and configure condition-specific attributes as described in Table 13-7.

Table 13-7   Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions

Match Condition	Description
Content	Specific content contained within the HTTP entity-body that is to be used for protocol inspection decisions. Do the following: **a.** In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. **b.** In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255.

Table 13-7 **Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)**

Match Condition	Description
Content Length	Content parse length in an HTTP message that is to be used for protocol inspection decisions. Do the following: a. In the Content Length Operator field, choose the operand to use to compare content length as follows: – **Equal To**—The content length must equal the number in the Content Length Value (Bytes) field. – **Greater Than**—The content length must be greater than the number in the Content Length Value (Bytes) field. – **Less Than**—The content length must be less than the number in the Content Length Value (Bytes) field. – **Range**—The content length must be within the range specified in the Content Length Lower Value (Bytes) field and the Content Length Higher Value (Bytes) field. b. Enter values to apply for content length comparison as follows: – If you chose Equal To, Greater Than, or Less Than in the Content Length Operator field, the Content Length Value (Bytes) field appears. In the Content Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are from 0 to 4294967295. – If you chose Range in the Content Length Operator field, the Content Length Lower Value (Bytes) and the Content Length Higher Value (Bytes) fields appear. Do the following: **1**. In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value (Bytes) field. **2**. In the Content Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are from 0 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value (Bytes) field.
Header	Name and value in an HTTP header that are to be used for protocol inspection decisions. Do the following: a. In the Header field, choose one of the predefined HTTP headers to be matched, or choose HTTP Header to specify a different HTTP header. b. If you chose HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. c. In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.

Table 13-7   *Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)*

Match Condition	Description
Header Length	Length of the header in the HTTP message that is to be used for protocol inspection decisions. Do the following: **a.** In the Header Length Type field, specify whether HTTP header request or response messages are to be used for protocol inspection decisions as follows: – **Request**—HTTP header request messages are to be checked for header length. – **Response**—HTTP header response messages are to be checked for header length. **b.** In the Header Length Operator field, choose the operand to use to compare header length: – **Equal To**—The header length must equal the number in the Header Length Value (Bytes) field. – **Greater Than**—The header length must be greater than the number in the Header Length Value (Bytes) field. – **Less Than**—The header length must be less than the number in the Header Length Value (Bytes) field. – **Range**—The header length must be within the range specified in the Header Length Lower Value (Bytes) field and the Header Length Higher Value (Bytes) field. **c.** Enter values to apply for header length comparison as follows: – If you chose Equal To, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value (Bytes) field appears. In the Header Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are from 0 to 255. – If you chose Range in the Header Length Operator field, the Header Length Lower Value (Bytes) and the Header Length Higher Value (Bytes) fields appear. Do the following: **1**. In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value (Bytes) field. **2**. In the Header Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value (Bytes) field.
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types that are to be used for protocol inspection decisions. In the Header MIME Type field, choose the MIME message type to use for this match condition.
Port Misuse	Feature that specifies that the misuse of port 80 (or any other port running HTTP) is to be used for protocol inspection decisions. Choose the application category to use for this match condition: • **IM**—Instant messaging applications are to be used for this match condition. • **P2P**—Peer-to-peer applications are to be used for this match condition. • **Tunneling**—Tunneling applications are to be used for this match condition.

Table 13-7   Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
Request Method	Request method that is to be used for protocol inspection decisions.
	By default, ACEs allow all request and extension methods. This option allows you to configure class maps that define protocol inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods.
	Do the following:
	a. In the Request Method Type field, choose the type of compliance to be used for protocol inspection decision. Choices are as follows:
	– **Ext**—HTTP extension method is to be used for protocol inspection decisions.
	– **RFC**—Request method defined in RFC 2616 is to be used for protocol inspection decisions.
	Depending on your selection, the Ext Request Method field or the RFC Request Method field appears.
	b. In the Request Method field, choose the specific request method to be used.
Transfer Encoding	Field that appears when an HTTP transfer-encoding type is used for protocol inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient.
	In the Transfer Encoding field, choose the type of encoding that is to be checked:
	• **Chunked**—The message body is transferred as a series of chunks.
	• **Compress**—The encoding format that is produced by the UNIX file compression program compress.
	• **Deflate**—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951.
	• **Gzip**—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952.
	• **Identity**—The default (identity) encoding which does not require the use of transformation.
URL	URL name used for protocol inspection decisions.
	In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following www.*hostname.domain*. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html.

Table 13-7   *Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)*

Match Condition	Description
URL Length	URL length to be used for protocol inspection decisions. Do the following: **a.** In the URL Length Operator field, choose the operand to be used to compare URL length: – **Equal To**—The URL length must equal the number in the URL Length Value (Bytes) field. – **Greater Than**—The URL length must be greater than the number in the URL Length Value (Bytes) field. – **Less Than**—The URL length must be less than the number in the URL Length Value (Bytes) field. – **Range**—The URL length must be within the range specified in the URL Length Lower Value (Bytes) field and the URL Length Higher Value (Bytes) field. **b.** Enter values to apply for URL length comparison as follows: – If you chose Equal To, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value (Bytes) field appears. In the URL Length Value (Bytes) field, enter the value for comparison. Valid entries are from 1 to 65535 bytes. – If you chose Range in the URL Length Operator field, the URL Length Lower Value (Bytes) and the URL Length Higher Value (Bytes) fields appear. Do the following: **1**. In the URL Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value (Bytes) field. **2**. In the URL Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value (Bytes) field.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

    Note   If you click **Deploy Now**, the ACE drops the traffic, then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Policy Maps, page 13-31

- Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 13-9

- Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 13-12

Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps

You can set match conditions for a Layer 7 FTP command inspection class map.

Assumption

You have configured a Layer 7 FTP command inspection class map and want to establish match criteria.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2 In the Class Maps table, choose the Layer 7 FTP command inspection class map that you want to set match conditions for.

The Match Condition table appears.

Step 3 In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4 In the Sequence Number field of the Match Condition configuration window, enter a value from 2 to 255.

Step 5 In the Match Condition Type field, confirm that Request Method Name is selected as the match condition type for this class map.

Step 6 In the Request Method Name field, choose the FTP command to be inspected.

Table 13-8 identifies the FTP commands that can be inspected.

Table 13-8   FTP Commands for Inspection

FTP Command	Description
Appe	Append data to the end of the specified file on the remote host.
Cdup	Change to the parent of the current directory.
Dele	Delete the specified file.
Get	Copy the specified file from the remote host to the local system.
Help	List all available FTP commands.
Mkd	Create a directory using the specified path and directory name.
Put	Copy the specified file from the local system to the remote host.
Rmd	Remove the specified directory.
Rnfr	Rename a file, specifying the current file name. Used with **rnto**.
Rnto	Rename a file, specifying the new file name. Used with **rnfr**.
Site	Execute a site-specific command.
Stou	Store a file on the remote host and give it a unique name.
Syst	Query the remote host for operating system information.

Step 7 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

  ✎
  Note   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Setting Match Conditions for Generic Server Load Balancing Class Maps

You can set match conditions for a generic server load balancing class map.

Assumption

You have configured a generic server load balancing class map and want to establish match criteria.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2 In the Class Maps table, choose the generic server load balancing class map that you want to set match conditions for.

The Match Condition table appears.

Step 3 In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4 In the Sequence Number field of the Match Condition configuration window, enter a value from 2 to 255.

Step 5 In the Match Condition Type field, choose the match condition type for this class map and configure any match-specific criteria as described in Table 13-9.

Table 13-9 **Generic Server Load Balancing Class Map Match Conditions**

Match Condition	Description
Class Map	Class map that is used to establish a match condition. In the Class Map field, choose the class map to use for this match condition.
Layer 4 Payload	Generic data parsing that is used to establish a match condition. Do the following: **a.** In the Layer 4 Payload Regex field, enter the Layer 4 payload expression contained within the TCP or UDP entity body to use for this match condition. Valid entries are text strings with a maximum of 255 alphanumeric characters. See Table 13-34 for a list of the supported characters that you can use for matching string expressions. **b.** In the Layer 4 Payload Offset field, enter the absolute offset where the Layer 4 payload expression search starts. The offset starts at the first byte of the TCP or UDP body. Valid entries are from 0 to 999.
Source Address	Source IP address that is used to establish a match condition. Do the following: **a.** In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **b.** In the Source Netmask field, choose the subnet mask for the source IP address.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

> ✎
> **Note**   If you click **Deploy Now**, the ACE drops the traffic and then restarts it even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Setting Match Conditions for RADIUS Server Load Balancing Class Maps

You can set match conditions for a RADIUS server load balancing class map.

Assumption

You have configured a RADIUS server load balancing class map and want to establish match criteria.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2   In the Class Maps table, choose the RADIUS server load balancing class map that you want to set match conditions for.

The Match Condition table appears.

Step 3   In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4   In the Sequence Number field, enter a value from 2 to 255.

Step 5   In the Match Condition Type field, choose the match condition type for this class map and configure any match-specific criteria as described in Table 13-10.

Table 13-10   RADIUS Server Load Balancing Class Map Match Conditions

Match Condition	Description
Calling Station ID	Unique identifier of the calling station that is used to establish a match condition. In the RADIUS Calling Station ID field, enter the calling station identifier to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 13-34 for a list of the supported characters that you can use for matching string expressions.
User Name	Username that is used to establish a match condition. In the User Name field, enter the name to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 13-34 for a list of the supported characters that you can use for matching string expressions.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

    ✎

    Note   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Setting Match Conditions for RTSP Server Load Balancing Class Maps

You can set match conditions for a RTSP server load balancing class map.

Assumption

You have configured a RTSP server load balancing class map and want to establish match criteria.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2 In the Class Maps table, choose the RTSP server load balancing class map that you want to set match conditions for.

The Match Condition table appears.

Step 3 In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4 In the Sequence Number field, enter a value from 2 to 255.

Step 5 In the Match Condition Type field, choose the match condition type for this class map and configure any match-specific criteria as described in Table 13-11.

Table 13-11   *RTSP Server Load Balancing Class Map Match Conditions*

Match Condition	Description
Class Map	Class map that is used to establish a match condition. In the Class Map field, choose the class map to use for this match condition.
RTSP Header	Name and value in an RTSP header that is used to establish a match condition.
	Do the following
	a. In the Header Name field, specify the header in one of the following ways:
	– To specify an RTSP header that is not one of the standard RSTP headers, choose the first radio button and enter the RTSP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
	– To specify one of the standard RTSP headers, choose the second radio button and choose one of the RTSP headers from the list.
	b. In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the RTSP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.

Table 13-11   RTSP Server Load Balancing Class Map Match Conditions (continued)

Match Condition	Description
RTSP URL	URL or portion of a URL that is used to establish a match condition. Do the following: **a.** In the URL Expr field, enter a URL, or portion of a URL, to match. The ACE performs matching on whatever URL string appears after the RTSP method, regardless of whether the URL includes the host name. The ACE supports regular expressions for matching URL strings. See Table 13-34 for a list of the supported characters that you can use in regular expressions. **b.** In the Method field, enter the RTSP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can be either one of the standard RTSP method names (DESCRIBE, ANNOUNCE, GET_PARAMETER, OPTIONS, PAUSE, PLAY, RECORD, REDIRECT, SETUP, SET_PARAMETER, TEARDOWN) or a text string that must be matched exactly (for example, STINGRAY).
Source Address	Source IP address that is used to establish a match condition. Do the following: **a.** In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **b.** In the Source Netmask field, choose the subnet mask for the source IP address.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

✎
Note   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Setting Match Conditions for SIP Server Load Balancing Class Maps

You can set match conditions for a SIP server load balancing class map.

Assumption

You have configured a SIP server load balancing class map and want to establish match criteria.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2   In the Class Maps table, choose the SIP server load balancing class map that you want to set match conditions for.

The Match Condition table appears.

Step 3   In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4   In the Sequence Number field of the Match Condition configuration window, enter a value from 2 to 255.

Step 5   In the Match Condition Type field, choose the match condition type for this class map and configure any match-specific criteria as described in Table 13-12.

Table 13-12   **SIP Server Load Balancing Class Map Match Conditions**

Match Condition	Description
Class Map	Class map that is used to establish a match condition. In the Class Map field, choose the class map to use for this match condition.
SIP Header	SIP header name and value that are used to establish a match condition. Do the following: **a.** In the Header Name field, specify the header in one of the following ways: – To specify a SIP header that is not one of the standard SIP headers, choose the first radio button and enter the SIP header name in the Header Name field. Enter an unquoted text string with no spaces and a maximum of 64 characters. – To specify one of the standard SIP headers, choose the second radio button and choose one of the SIP headers from the list. **b.** In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the SIP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.
Source Address	Source IP address that is used to establish a match condition. Do the following: **a.** In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **b.** In the Source Netmask field, choose the subnet mask for the source IP address.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

  ✎

  Note   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps

You can set match conditions for a SIP deep packet inspection class map.

Assumption

You have configured a SIP deep packet inspection class map and want to establish match criteria.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Class Maps**.

The Class Maps table appears.

Step 2   In the Class Maps table, choose the SIP deep packet inspection class map that you want to set match conditions for.

The Match Condition table appears.

Step 3   In the Match Condition table, click **Add** to add match criteria, or choose the match condition that you want to modify and click **Edit**.

The Match Condition configuration window appears.

Step 4   In the Sequence Number field of the Match Condition configuration window, enter a value from 2 to 255.

Step 5   In the Match Condition Type field, choose the match condition type for this class map and configure any match-specific criteria as described in Table 13-13.

Table 13-13   Layer 7 SIP Deep Packet Inspection Class Map Match Conditions

Match Condition	Description
Called Party	Destination or called party in the URI of the SIP To header that is used to establish a match condition. In the Called Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 13-34 lists the supported characters that you can use for matching string expressions.
Calling Party	Source or calling party in the URI of the SIP From header that is used to establish a match condition. In the Calling Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 13-34 lists the supported characters that you can use for matching string expressions.
IM Subscriber	IM (instant messaging) subscriber that is used to establish a match condition. In the IM Subscriber field, enter a regular expression that identifies the IM subscriber for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 13-34 lists the supported characters that you can use for matching string expressions.
Message Path	Message coming from or transiting through certain SIP proxy servers that is used to establish a match condition. In the Message Path field, enter a regular expression that identifies the SIP proxy server for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 13-34 lists the supported characters that you can use for matching string expressions.
SIP Content Length	SIP message body length that is used to establish a match condition. Do the following: **a.** In the Content Operator field, confirm that Greater Than is selected. **b.** In the Content Length field, enter the maximum size of a SIP message body in bytes that the ACE is to allow without performing SIP protocol inspection. If a SIP message exceeds the specified value, the ACE performs SIP protocol inspection as defined in an associated policy map. Valid entries are from 0 to 65534 bytes.
SIP Content Type	Content type in the SIP message body that is used to establish a match condition. In the Content Type field, enter the a regular expression that identifies the content type in the SIP message body to use for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 13-34 lists the supported characters that you can use for matching string expressions.
SIP Request Method	SIP request method that is used to establish a match condition. In the Request Method field, choose the request method that is to be matched.

Table 13-13   *Layer 7 SIP Deep Packet Inspection Class Map Match Conditions (continued)*

Match Condition	Description
Third Party	Third party who is authorized to register other users on their behalf that is used to establish a match condition. In the Third Party Registration Entities field, enter a regular expression that identifies a privileged user authorized for third-party registrations for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 13-34 lists the supported characters that you can use for matching string expressions.
URI Length	SIP URI or user identifier that is used to establish a match condition. Do the following: **a.** In the URI Type field, choose the type of URI to use: – SIP URI—The calling party URI is used for this match condition. – Tel URI—A telephone number is used for this match condition. **b.** In the URI Operator field, confirm that Greater Than is selected. **c.** In the URI Length field, enter the maximum length of the SIP URI or Tel URI in bytes. Valid entries are integers from 0 to 254 bytes.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Match Condition table.

> **Note**   If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.

- Click **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Configuring Virtual Context Policy Maps

You can create policy maps for a context that establish traffic policy for the ACE. The purpose of a traffic policy is to implement specific ACE functions associated with a traffic class.

A traffic policy contains the following:

- A policy map name.
- A previously created traffic class map or, optionally, the class-default class map.

- One or more of the individual Layer 3/Layer 4 or Layer 7 policies that specify the actions to be performed by the ACE.

The ACE executes actions specified in a policy map on a first-match, multi-match, or all-match basis as follows:

- First-match—With a first-match policy map, the ACE executes only the action specified against the first classification that it matches. Layer 3/Layer 4 Management Traffic, Layer 7 Server Load Balancing, Layer 7 Command Inspection - FTP, and Layer 7 HTTP Optimization policy maps are first-match policy maps.

- Multi-match—With a multi-match policy map, the ACE executes all possible actions applicable for a specific classification. Layer 3/Layer 4 Network Traffic policy maps are multi-match policy maps.

- All-match—With an all-match policy map, the ACE attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request.

You can display a context's policy maps and their types in the Policy Maps table (Config > Virtual Contexts > *context* > Expert > Policy Maps.)

The types of policy maps that you can configure depend on the ACE device type. Table 13-14 lists the types of policy maps with brief descriptions and the ACE devices that support them.

Table 13-14   Policy Maps and ACE Device Support

Policy Map Type	Description	ACE Device	
		ACE Module	ACE Appliance
Layer 3/4 Management Traffic (First-Match)	Layer 3 and Layer 4 policy map for network management traffic received by the ACE	X	X
Layer 3/4 Network Traffic (First-Match)	Layer 3 and Layer 4 policy map for traffic passing through the ACE	X	X
Layer 7 Command Inspection - FTP (First-Match)	Layer 7 policy map for inspection of FTP commands	X	X
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Layer 7 policy map for inspection of HTTP packets	X	X
Layer 7 Deep Packet Inspection - SIP (All-Match)	Layer 7 policy map for inspection of SIP packets	X	X
Layer 7 Deep Packet Inspection - Skinny	Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)	X	X
Layer 7 HTTP Optimization (First-Match)	Layer 7 policy map for optimizing HTTP traffic		X
Layer 7 Server Load Balancing (First-Match)	Layer 7 policy map for HTTP server load balancing	X	X
Server Load Balancing - Generic	Generic Layer 7 policy map for server load balancing	X	X
Server Load Balancing - RADIUS (First-Match)	Layer 7 policy map for RADIUS server load balancing	X	X
Server Load Balancing - RDP (First-Match)	Layer 7 policy map for RDP server load balancing	X	X

Table 13-14   Policy Maps and ACE Device Support (continued)

		ACE Device	
Policy Map Type	**Description**	**ACE Module**	**ACE Appliance**
Server Load Balancing - RTSP (First-Match)	Layer 7 policy map for RTSP server load balancing	X	X
Server Load Balancing - SIP (First-Match)	Layer 7 policy map for SIP server load balancing	X	X

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, click **Add** to add a new policy map, or choose an existing policy map and click **Edit** to modify it.

Step 3   The Policy Map Name field contains an automatically incremented number for the policy map. Either leave the entry as it is or enter a different, unique number.

Step 4   In the Type field, choose the type of policy map to create. See Table 13-14 for a list of the policy maps and their availability for the different ACE models.

Step 5   In the Description field, enter a brief description of the policy map.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. To define rules and actions for the policy map, see Configuring Rules and Actions for Policy Maps, page 13-34.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.

- Click **Next** to deploy your entries and to configure another policy map.

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Rules and Actions for Policy Maps, page 13-34

Configuring Rules and Actions for Policy Maps

Table 13-15 lists the policy maps and related topics for setting rules and actions.

Table 13-15   Topic Reference for Policy Map Rules and Actions

Policy Map Type	Topic for Setting Rules and Actions
Layer 3/4 Management Traffic (First-Match)	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic, page 13-38
Layer 3/4 Network Traffic (First-Match)	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 13-40
Layer 7 Command Inspection - FTP (First-Match)	Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection, page 13-48
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 13-51
Layer 7 Deep Packet Inspection - SIP (All-Match)	Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 13-68
Layer 7 Deep Packet Inspection - Skinny	Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection, page 13-71
Layer 7 HTTP Optimization (First-Match)	Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 13-58
Layer 7 Server Load Balancing (First-Match)	Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 13-62
Server Load Balancing - Generic (First-Match)	Setting Policy Map Rules and Actions for Generic Server Load Balancing, page 13-34
Server Load Balancing - RADIUS (First-Match)	Setting Policy Map Rules and Actions for RADIUS Server Load Balancing, page 13-73
Server Load Balancing - RDP (First-Match)	Setting Policy Map Rules and Actions for RDP Server Load Balancing, page 13-75
Server Load Balancing - RTSP (First-Match)	Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 13-76
Server Load Balancing - SIP (First-Match)	Setting Policy Map Rules and Actions for SIP Server Load Balancing, page 13-79

Setting Policy Map Rules and Actions for Generic Server Load Balancing

You can configure the rules and actions for generic traffic received by the ACE.

Assumptions

This topic assumes the following:

- A generic traffic policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the generic traffic policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose the rule that you want to modify and click **Edit**.

The Rule window appears.

Step 4   In the Type field of the Rule window, configure rules using the information in Table 13-16.

Table 13-16   *Generic Server Load Balancing Policy Map Rules*

Option	Description
Class Map	Class map that is used for this traffic policy.
	Do the following:
	a. To use the class-default class map, check the Use Class Default check box.
	The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
	b. To use a previously created class map, do the following:
	1. Clear the Use Class Default check box.
	2. In the Class Map Name field, choose the class map to be used.

Table 13-16   Generic Server Load Balancing Policy Map Rules (continued)

Option	Description		
Match Condition	Match condition is used for this traffic policy.		
	Match Condition Name	Enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.	
	Match Condition Type	Layer 4 Payload	Layer 4 payload data that is used for the network matching criteria. Do the following: **a.** In the Layer 4 Payload RegexMatch Condition field, enter a Layer 4 payload expression that is contained within the TCP or UDP entity body. Valid entries are strings containing 1 to 255 alphanumeric characters. Table 13-34 lists the supported characters that you can use for matching string expressions. **b.** In the Layer 4 Payload Offset field, enter the absolute offset in the data where the Layer 4 payload expression search string starts. The offset starts at the first byte of the TCP or UDP body. Valid entries are from 0 to 999.
		Source Address	Client source host IP address and subnet mask that are used for the network traffic matching criteria. Do the following: **a.** In the Source IP Address field, enter the source IP address of the client in dotted-decimal notation. **b.** In the Source Netmask field, choose the subnet mask for the source IP address.
Insert Before	**a.** Indicate whether this rule is to precede another rule for this policy map: – **N/A**—This option is not configured. – **False**—This rule is not to precede another rule in this policy map. – **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears. **b.** If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.		

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. Continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

✎

Note   If you chose the Insert Before option described in Table 13-16 and specified True, perform the
following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.

2. In the Rule table, choose the newly added rule.

When the window refreshes, an empty action list appears.

Step 6   In the Action table, click **Add** to add an entry or choose an existing entry to modify and click **Edit**.

Step 7   In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 8   In the Action Type field, configure actions for this rule using the information in Table 13-17.

Table 13-17   Generic Server Load Balancing Policy Map Actions

Action	Description
Drop	Field that instructs the ACE to discard packets that match this policy map. In the Action Log field, specify whether or not the dropped packets are to be logged in the software: • **N/A**—This option is not configured. • **False**—Dropped packets are not to be logged in the software. • **True**—Dropped packets are to be logged in the software.
Forward	Field that instructs the ACE to forward the traffic that matches this policy map to its destination.
Reverse Sticky	Feature that applies only to the ACE module version 3.0(0)A2(1.1), ACE appliance version A4(1.0), or later releases of either device type. Reverse IP stickiness is an enhancement to regular stickiness and is used mainly in FWLB. It ensures that multiple distinct connections that are opened by hosts at both ends (client and server) are load-balanced and stuck to the same firewall. Reverse stickiness applies to such protocols as FTP, RTSP, SIP, and so on where there are separate control channels and data channels opened by the client and the server, respectively. For complete details about reverse stickiness, see the *Release Note for the Cisco Application Control Engine Module (Software Version 3.0(0)A2(X))*. In the Sticky Group field, choose an existing IP netmask sticky group that you want to associate with reverse IP stickiness.
Server Farm	Serverfarm that the ACE is to load balance client requests for content. Do the following: **a.** In the Server Farm field, choose the server farm for this policy map action. **b.** In the Backup Server Farm field, choose the backup server farm for this action. **c.** Check the **Sticky Enabled** check box to indicate that the backup server farm is sticky. Uncheck this check box if the backup server farm is not sticky. **d.** Check the **Aggregate State Enabled** check box to indicate that the operational state of the backup server farm is taken into consideration when evaluating the state of the load-balancing class in a policy map. Uncheck this check box to indicate that the operational state of the backup server farm is not taken into consideration when evaluating the state of the load-balancing class in a policy map.

Table 13-17   Generic Server Load Balancing Policy Map Actions (continued)

Action	Description
Server Farm-NAT	Dynamic NAT that the ACE is to apply to traffic for this policy map. Do the following: **a.** In the NAT Pool ID field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are from 1 to 2147483647. For information about configuring NAT pools, see "Configuring Virtual Context BVI Interfaces" section on page 11-13. **b.** In the VLAN ID field, choose the VLAN to use for NAT. Valid entries are from 1 to 4094. **c.** In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.
Set-IP-TOS	IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte that the ACE is to set. After the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. In the IP TOS Rewrite Value field, enter the IP DSCP value. Valid entries are from 0 to 255.
Sticky Group	Sticky group that you want to associate with reverse stickiness.
Sticky Server Farm	Sticky server farm that the ACE is to load balance client requests for content. In the Sticky Group field, choose the sticky server farm that is to be used for requests that match this policy map.

Step 9 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

Related Topics

- Configuring Traffic Policies, page 13-1

- Configuring Virtual Context Class Maps, page 13-6

- Configuring Virtual Context Policy Maps, page 13-31

- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic

You can configure the rules and actions for IP management traffic received by the ACE.

Assumptions

This topic assumes the following:

- A network management policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1   Choose **Config > Virtual Contexts > *context* > Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the Layer 3/Layer 4 management traffic policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose the rule that you want to modify and click **Edit**.

The Rule window appears.

Step 4   In the Type field of the Rule window, confirm that classmap is selected.

Step 5   (Optional) To use the class-default class map, check the Use Class Default check box.

Step 6   (Optional) To use a previously created class map for this rule, do the following:

   a.   Uncheck the Use Class Default check box.

   b.   In the Class Map Name field, choose the class map to be used.

   c.   In the Insert Before field, specify whether this rule is to precede another rule in this policy map:

   –   **N/A**—This option is not configured.

   –   **False**—This rule is not to precede another rule in this policy map.

   –   **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears

   d.   If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Step 7   Do one of the following:

   •   Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The Action table appears. To define actions for this rule, continue with Step 8.

   •   Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.

   •   Click **Next** to deploy your entries and to configure another rule.

   ✎

   Note   If you chose the Insert Before option in Step 6 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

   1. Click the Rule tab to refresh the Rule table.

   2. In the Rule table, choose the newly added rule.

   When the window refreshes, an empty action list appears.

Step 8   In the Action table, click **Add** to add an action or choose an existing action, and click **Edit** to modify it.

The Action configuration window appears.

Step 9   In the Id field of the Action configuration window, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 10 In the Action Type field, confirm that Management Permit is selected to indicate that this action permits or denies network management traffic.

Step 11 In the Action field, specify the action that is to occur:

- **Deny**—The ACE is to deny network management traffic when this rule is met.

- **Permit**—The ACE is to accept network management traffic when this rule is met.

Step 12 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

Related Topics

- Configuring Virtual Context Class Maps, page 13-6

- Configuring Virtual Context Policy Maps, page 13-31

- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic

You can configure rules and actions for Layer 3/Layer 4 traffic other than network management traffic.

Assumptions

This topic assumes the following:

- You have configured a Layer 3/Layer 4 policy map.

- A class map has been defined if you do not want to use the class-default class map.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2 In the Policy Maps table, choose the Layer 3/Layer 4 network traffic policy map that you want to set rules and actions for.

The Rule table appears.

Step 3 In the Rule table, click **Add** to add a new rule, or choose the rule that you want to modify and click **Edit**.

The Rule configuration window appears.

Step 4 In the Type field of the Rule configuration window, confirm that Class Map is selected.

Step 5 (Optional) To use the class-default class map, check the Use Class Default check box.

Step 6 (Optional) To use a previously created class map for this rule, do the following:

  a. Uncheck the Use Class Default check box.

  b. In the Class Map Name field, choose the class map to be used.

    c. In the Insert Before field, indicate whether or not this rule is to precede another rule in this policy map:

       – **N/A**—This option is not configured.

       – **False**—This rule is not to precede another rule in this policy map.

       – **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.

    d. If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Step 7 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action field appears. To configure actions for this rule, continue with Step 8.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.

- Click **Next** to deploy your entries and to configure another rule.

> **Note** If you chose the Insert Before option in Step 6 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:
>
> **1.** Click the Rule tab to refresh the Rule table.
>
> **2.** In the Rule table, choose the newly added rule.
>
> When the window refreshes, an empty action list appears.

Step 8 In the Action field, click Edit. The Action table appears.

Step 9 In the Action table, click **Add** to add an action or choose an existing action and click **Edit** to modify it.

The Action configuration window appears.

Step 10 In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 11 In the Action Type field, choose the type of action to be taken for this rule and configure the related attributes. See Table 13-18.

Table 13-18   Layer 3/Layer 4 Network Traffic Policy Map Actions

Action	Description/Steps
Appl-Parameter-DNS	DNS parameter map that contains DNS-related actions that is to be implemented for this rule.
	In the Parameter Map field, specify the name of the DNS parameter map to use.
Appl-Parameter-Generic	Generic parameter map that is to be implemented for this rule.
	In the Parameter Map field, specify the name of the generic parameter map to use.
Appl-Parameter-HTTP	HTTP parameter map that contains HTTP-related actions that is to be implemented for this rule.
	In the Parameter Map field, specify the name of the HTTP parameter map to use.
Appl-Parameter-RTSP	RTSP parameter map that contains RTSP-related actions that is to be implemented for this rule.
	In the Parameter Map field, specify the name of the RTSP parameter map to use.

Table 13-18   Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
Appl-Parameter-SIP	SIP parameter map that contains SIP-related actions that is to be implemented for this rule. In the Parameter Map field, specify the name of the SIP parameter map to use.
Appl-Parameter-Skinny	Skinny parameter map that contains Skinny-related actions that is to be implemented for this rule. In the Parameter Map field, specify the name of the Skinny parameter map to use.
Connection	Connection parameter map that contains TCP/IP connection-related commands that pertain to normalization and termination that is to be implemented for this rule. In the Connection Parameter Maps field, choose the Connection parameter map that is to be used.
HTTP Optimize	Option that appears for ACE appliances only. In the HTTP Optimization Policy field, choose the HTTP optimization policy map to use.
Inspect	Application inspection that is to be implemented for this rule. Do the following: **a.** In the Inspect Type field, choose the protocol that is to be inspected. **b.** Provide any protocol-specific information. Table 13-19 describes the available options for application inspection actions.
KAL-ap-Primary-Out-of-Service	Feature that is supported only for ACE module software version A2(3.1), ACE appliance software version A4(1.0), and later versions of either device type. This feature enables the ACE to notify a Global Site Selector (GSS) that the primary server farm is down when the backup server farm is in use. By default, when you configure a redirect server farm as a backup server farm on the ACE and the primary server farm fails, the backup server farm redirects client requests to another data center; however, the VIP remains in the INSERVICE state. When you configure the ACE to communicate with a GSS, it provides information for server availability. When a backup server is in use after the primary server farm is down, this feature enables the ACE to inform the GSS that the VIP for the primary server farm is out of service by returning a load value of 255. The GSS recognizes that the primary server farm is down and sends future DNS requests with the IP address of the other data center.

Table 13-18   ***Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)***

Action	Description/Steps
KAL-AP-TAG	Feature that is supported only for the ACE module software version A2(2.0), ACE appliance software version A4(1.0), and later versions for both device types. The KAL-AP-TAG feature allows the Cisco Global Site Selector (GSS) proprietary KAL-AP protocol to extract load and availability information from the ACE when a firewall is positioned between the GSS and the ACE. This feature allows you to configure a tag (name) per VIP for a maximum of 4096 tags on an ACE. This feature does not replace the tag per domain feature. For more information about this feature, see the *Release Note for the Cisco Application Control Engine Module (Software Version A2(2.0))* or the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide* (Software Version A2(3.0)), the Configuring Health Monitoring chapter.
	Note The KAL-AP-TAG selection is not available for the class-default class map.
	In the KAL-AP-Tag Name field, enter the name as an unquoted text string with no spaces and a maximum of 76 alphanumeric characters.
	The following scenarios are not supported and will result in an error:
	• You cannot configure a tag name for a VIP that already has a tag configuration as part of a different policy configuration.
	• You cannot associate the same tag name with more than one VIP.
	• You cannot associate the same tag name with a domain and a VIP.
	• You cannot assign two different tags to two different Layer 3 class maps that have the same VIP, but different port numbers. The KAL-AP protocol considers these class maps to have the same VIP and calculates the load for both Layer 3 rules together when the GSS queries the VIP.

Table 13-18   Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
NAT	Network address translation (NAT) that the ACE is to use for this rule.
	Do the following:
	a. In the NAT Mode field, choose the type of NAT to be used:
	– **Dynamic NAT**—NAT is to translate local addresses to a pool of global addresses. Continue with Step c.
	– **Static NAT**—NAT is to translate each local address to a fixed global address. Continue with Step b.
	b. If you chose Static NAT, do the following:
	1. In the Static Mapped Address field, enter the IP address to use for static NAT translation. This entry establishes the globally unique IP address of a host as it appears to the outside world. The policy map performs the global IP address translation for the source IP address specified in the ACL (as part of the class-map traffic classification).
	2. In the Static Mapped Netmask field, choose the subnet mask to apply to the static mapped address.
	3. In the NAT Protocol field, choose the protocol to use for NAT. Choices are as follows:
	- **N/A**—This attribute is not set.
	- **TCP**—The ACE is to use TCP for NAT.
	- **UDP**—The ACE is to use UDP for NAT.
	4. In the Static Port field, enter the TCP or UDP port to use for static port redirection. Valid entries are from 0 to 65535.
	5. In the VLAN Id field, choose the VLAN to use for NAT.
	c. If you chose Dynamic NAT, do the following:
	1. In the NAT Pool Id field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are from 1 to 2147483647. See the "Configuring Virtual Context BVI Interfaces" section on page 11-13.
	2. In the VLAN Id field, choose the VLAN to use for NAT.
	Note For dynamic NAT, ACE allows you to associate a non-configured NAT pool ID to the dynamic NAT action. However, the ANM will not discover the dynamic NAT action when the NAT pool ID is not configured. You must associate the configured NAT pool ID to the dynamic NAT action for ANM discovery to complete successfully.
Policymap	Layer 7 server load-balancing policy map that the ACE is to associate with this Layer 3/Layer 4 policy map.
	In the Policy Map field, choose the Layer 7 policy map.
SSL-Proxy	SSL proxy server service that defines the SSL parameters that the ACE is to use during the handshake and subsequent SSL session.
	Do the following:
	a. In the SSL Proxy field, choose the SSL proxy server service to use in the handshake and subsequent SSL session when the ACE engages with an SSL client.
	b. In the SSL Proxy Type field, confirm that Server is selected to indicate that the ACE is to be configured so that it is recognized as an SSL server.

Table 13-18   *Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)*

Action	Description/Steps
UDP-Fast-Age	Option that appears for ACE modules only. The ACE is to close the connection immediately after sending a response to the client, thereby enabling per-packet load balancing for UDP traffic.
VIP-Advertise	Option that appears for ACE modules release only. The ACE is to advertise the IP address of a virtual server as the host route. Do the following: **a.** In the Active field, check the checkbox if you want the ACE to advertises the IP address of the virtual server as the host route only if there is at least one active real server in the server farm. ✎ **Note** Uncheck the Active field check box if you want the ACE to always advertises the IP address of the virtual server whether there is any active real server associated with the VIP. **b.** If you check the Active field check box, in the Metric Distance field, enter the administrative distance to include in the routing table. Valid entries are from 1 to 254.
VIP-ICMP-Reply	VIP is to send an ICMP ECHO-REPLY response to ICMP requests. Do the following: **a.** In the Active field, check the checkbox to instruct the ACE to reply to an ICMP request only if the configured VIP is active. If the VIP is not active and the active option is specified, the ACE discards the ICMP request and the request times out. **b.** In the Primary Inservice field, check the checkbox to instruct the ACE to reply to an ICMP ping only if the primary server farm state is UP, regardless of the state of the backup server farm. If this option is enabled and the primary server farm state is DOWN, the ACE discards the ICMP request and the request times out.
VIP-In-Service	VIP is to be enabled for server load-balancing operations.

Table 13-19   Layer 3/Layer 4 Network Traffic Policy Map Application Inspection Options

Option	Description
DNS	Domain Name System (DNS) query inspection is to be implemented. DNS requires application inspection so that DNS queries will not be subject to the generic UDP handling based on activity timeouts. Instead, the UDP connections associated with DNS queries and responses are torn down as soon as a reply to a DNS query has been received. The ACE performs the reassembly of DNS packets to verify that the packet length is less than the configured maximum length. In the DNS Max. Length field, enter the maximum length of a DNS reply in bytes. Default for all modules and ACE 4710 devices is 512. Valid range for ACE 1.0 modules is 64 to 65535, and for all other supported modules and ACE 4710 devices, 64 to 65535.
FTP	FTP inspection is to be implemented. The ACE inspects FTP packets, translates the address and port embedded in the payload, and opens up secondary channel for data. **a.** In the Parameter Map field, specify a previously created parameter map used to define parameters for FTP inspection. **b.** In the FTP Strict field, specify whether or not the ACE is to check for protocol RFC compliance and prevent Web browsers from sending embedded commands in FTP requests: – **N/A**—This attribute is not set. – **False**—The ACE is not to check for RFC compliance or prevent Web browsers from sending embedded commands in FTP requests. – **True**—The ACE is to check for RFC compliance and prevent Web browsers from sending embedded commands in FTP requests. **c.** If you chose True, in the FTP Inspect Policy field, choose the Layer 7 FTP command inspection policy to be implemented for this rule.
HTTP	Enhanced Hypertext Transfer Protocol (HTTP) inspection is to be performed on HTTP traffic. The inspection checks are based on configured parameters in an existing Layer 7 policy map and internal RFC compliance checks performed by the ACE. By default, the ACE allows all request methods. Do the following: **a.** In the HTTP Inspect Policy field, choose the HTTP inspection policy map to be implemented for this rule. If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 protocol fixup actions and internal RFC compliance checks. **b.** In the URL Logging field, specify whether or not Layer 3 and Layer 4 traffic is to be monitored: – **N/A**—This attribute is not set. – **False**—Layer 3 and Layer 4 traffic is not to be monitored. – **True**—Layer 3 and Layer 4 traffic is to be monitored. When enabled, this function logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed.

Table 13-19   Layer 3/Layer 4 Network Traffic Policy Map Application Inspection Options (continued)

Option	Description
ICMP	Internet Control Message Protocol (ICMP) payload inspection is to be performed. ICMP inspection allows ICMP traffic to have a "session" so that it can be inspected similarly to TCP and UDP traffic. In the ICMP Error field, specify whether or not the ACE is to perform name address translation on ICMP error messages: • **N/A**—This attribute is not set. • **False**—The ACE is not to perform NAT on ICMP error messages. • **True**—The ACE is to perform NAT on ICMP error messages. When enabled, the ACE creates translation sessions for intermediate or endpoint nodes that send ICMP error messages based on the NAT configuration. The ACE overwrites the packet with the translated IP addresses.
ILS	Internet Locator Service (ILS) protocol inspection is to be implemented.
RTSP	Real Time Streaming Protocol (RTSP) packet inspection is to be implemented. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. The ACE monitors Setup and Response (200 OK) messages in the control channel established using TCP port 554 (no UDP support). In the Parameter Map field, choose a previously defined parameter map used to define parameters for RTSP inspection.
SIP	SIP protocol inspection is to be implemented. SIP is used for call handling sessions and instant messaging. The ACE inspects signaling messages for media connection addresses, media ports, and embryonic connections. The ACE also uses NAT to translate IP addresses that are embedded in the user-data portion of the packet. Do the following: **a.** In the Parameter Map field, specify a previously created parameter map used to define parameters for SIP inspection. **b.** In the SIP Inspect Policy field, choose a previously created Layer 7 SIP inspection policy map to implement packet inspection of Layer 7 SIP application traffic. If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.
Skinny	Cisco Skinny Client Control Protocol (SCCP) protocol inspection is to be implemented. The SCCP is a Cisco proprietary protocol that is used between Cisco CallManager and Cisco VOiP phones. The ACE uses NAT to translate embedded IP addresses and port numbers in SCCP packet data. Do the following: **a.** In the Parameter Map field, specify a previously created connection parameter map used to define parameters for Skinny inspection. **b.** In the Skinny Inspect Policy field, choose a previously created Layer 7 Skinny inspection policy map to implement packet inspection of Layer 7 Skinny application traffic. If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.

Step 12   Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another Action.

Related Topics

- Configuring Traffic Policies, page 13-1

- Configuring Virtual Context Class Maps, page 13-6

- Configuring Virtual Context Policy Maps, page 13-31

Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection

You can add rules and actions for Layer 7 FTP command inspection policy maps.

File Transfer Protocol (FTP) inspection inspects FTP sessions for address translation in a message, dynamic opening of ports, and stateful tracking of request and response messages. Each specified FTP command must be acknowledged before the ACE allows a new command. Command filtering allows you to restrict specific commands by the ACE. When the ACE denies a command, it closes the connection.

The FTP command inspection process, as performed by the ACE:

- Prepares a dynamic secondary data connection. The channels are allocated in response to a file upload, a file download, or a directory listing event and must be prenegotiated. The port is negotiated through the PORT or PASV commands.

- Tracks the FTP command-response sequence. The ACE performs the command checks listed below. If you specify the FTP Strict field in a Layer 3 and Layer 4 policy map, the ACE tracks each FTP command and response sequence for the anomalous activity outlined below. The FTP Strict parameter is used in conjunction with a Layer 7 FTP policy map (nested within the Layer 3 and Layer 4 policy map) to deny certain FTP commands or to mask the server reply for SYST command.

> ✎
>
> **Note**   The use of the FTP Strict parameter may affect FTP clients that do not comply with the RFC standards.

  - Truncated command—Checks the number of commas in the PORT and PASV reply command against a fixed value of five. If the value is not five, the ACE assumes that the PORT command is truncated and issues a warning message and closes the TCP connection.

  - Incorrect command—Checks the FTP command to verify if it ends with <CR><LF> characters, as required by RFC 959. If the FTP command does not end with those characters, the ACE closes the connection.

  - Size of RETR and STOR commands—Checked the size of the RETR and STOR commands against a fixed constant of 256. If the size is greater, the ACE logs an error message and closes the connection.

  - Command spoofing—Verifies that the PORT command is always sent from the client. If a PORT command is sent from the server, the ACE denies the TCP connection.

- Reply spoofing—Verifies that the PASV reply command (227) is always sent from the server. If a PASV reply command is sent from the client, the ACE denies the TCP connection. This denial prevents a security hole when the user executes "227 xxxxx a1, a2, a3, a4, p1, p2."

- Invalid port negotiation—Checks the negotiated dynamic port value to verify that it is greater than 1024 (port numbers in the range from 2 to 1024 are reserved for well-known connections). If the negotiated port falls in this range, the ACE closes the TCP connection.

- Command pipelining—Checks the number of characters present after the port numbers in the PORT and PASV reply command against a constant value of 8. If the number of characters is greater than 8, the ACE closes the TCP connection.

- Translates embedded IP addresses in conjunction with NAT. FTP command inspection translates the IP address within the application payload. Refer to RFC 959 for background details.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the Layer 7 FTP command inspection policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose an existing rule and click **Edit** to modify it.

The Rule configuration window appears.

Step 4   In the Type field of the Rule configuration window, configure rules using the information in Table 13-20.

Table 13-20   Layer 7 FTP Command Inspection Policy Map Rules

Option	Description
Class Map	Class map to use for this traffic policy.
	Do the following:
	a. To use the class-default class map, check the Use Class Default check box.
	The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
	b. To use a previously created class map, do the following:
	1. Clear the Use Class Default check box.
	2. In the Class Map Name field, choose the class map to be used.

Table 13-20   *Layer 7 FTP Command Inspection Policy Map Rules (continued)*

Option	Description
Match Condition	Match condition to use for this traffic policy. Do the following: **a.** In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **b.** In the Match Condition Type field, confirm that Request Method Name is selected. **c.** In the Request Method Name field, choose the FTP command to be inspected for this rule. Table 13-8 describes the FTP commands that can be inspected.
Insert Before	Order of the rules in the policy map. Do the following: **a.** Specify whether or not this rule is to precede another rule for this policy map. Choices are as follows: – **N/A**—This option is not configured. – **False**—This rule is not to precede another rule in this policy map. – **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears. **b.** If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. Continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.

- Click **Next** to deploy your entries and to configure another rule.

✎

Note   If you chose the Insert Before option described in Table 13-20 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.

2. In the Rule table, choose the newly added rule.

When the window refreshes, an empty action list appears.

Step 6   In the Action table, click **Add** to add an entry, or choose an existing entry and click **Edit** to modify it.

The Action configuration window appears.

Step 7   In the Id field of the Action configuration window, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 8   In the Action Type field, specify the action to be taken for this rule:

- **Deny**—The ACE is to deny the specified FTP command when this rule is met.

- **Mask Reply**—The ACE is to mask the reply to the FTP **syst** command by filtering sensitive information from the command output. The action applies to the FTP **syst** command only.

Step 9   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action for this rule.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31

Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection

You can add rules and actions for Layer 7 HTTP deep packet inspection policy maps.

The ACE performs a stateful deep packet inspection of the HTTP protocol. Deep packet inspection is a special case of application inspection where the ACE examines the application payload of a packet or a traffic stream and makes decisions based on the content of the data. During HTTP deep inspection, the main focus of the application inspection process is on HTTP attributes such as HTTP header, URL, and to a limited extent, the payload. User-defined regular expressions can also be used to detect "signatures" in the payload.

You define policies to permit or deny the traffic, or to send a TCP reset message to the client or server to close the connection.

The security features covered by HTTP application inspection include:

- RFC compliance monitoring and RFC method filtering
- Content, URL, and HTTP header length checks
- Transfer-encoding methods
- Content type verification and filtering
- Port 80 misuse

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the Layer 7 deep packet inspection policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose an existing rule and click **Edit** to modify it.

The Rule configuration window appears.

Step 4   In the Type field of the Rule configuration window, configure rules using the information in Table 13-21.

Table 13-21   *Layer 7 HTTP Deep Packet Inspection Policy Map Rules*

Option	Description

Class Map	Class map to use for this traffic policy.
	
	Do the following:
	
	a. To use the class-default class map, check the Use Class Default check box.
	
	The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
	
	b. To use a previously created class map, do the following:
	
	    1. Clear the Use Class Default check box.
	
	    2. In the Class Map Name field, choose the class map to be used.

Match Condition	Match condition to use for this traffic policy. Do the following: **a.** In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **b.** In the Match Condition Type field, choose the method by which match decisions are to be made and their corresponding conditions. See Table 13-22 for information about these selections.

Insert Before	Order of the rules in the policy map.
	
	Do the following:
	
	a. Specify whether or not this rule is to precede another rule for this policy map. Choices are as follows:
	
	   – **N/A**—This option is not configured.
	
	   – **False**—This rule is not to precede another rule in this policy map.
	
	   – **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.
	
	b. If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Table 13-22   Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions

Match Condition	Description
Content	Content contained within the HTTP entity-body that is used for protocol inspection decisions. Do the following: **a.** In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. **b.** In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255 bytes.
Content Length	Content parse length in an HTTP message that is used for protocol inspection decisions. Do the following: **a.** In the Content Length Operator field, choose the operand to be used to compare content length: – **Equal To**—Content length must equal the number in the Content Length Value (Bytes) field. – **Greater Than**—Content length must be greater than the number in the Content Length Value (Bytes) field. – **Less Than**—Content length must be less than the number in the Content Length Value (Bytes) field. – **Range**—Content length must be within the range specified in the Content Length Lower Value (Bytes) field and the Content Length Higher Value (Bytes) field. **b.** Enter values to apply for content length comparison as follows: – If you chose Equal To, Greater Than, or Less Than in the Content Length Operator field, the Content Length Value (Bytes) field appears. In the Content Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are from 0 to 4294967295. – If you chose Range in the Content Length Operator field, the Content Length Lower Value (Bytes) and the Content Length Higher Value (Bytes) fields appear: **1**. In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value (Bytes) field. **2**. In the Content Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are from 1 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value (Bytes) field.
Content Type Verification	Match command that verifies the content MIME-type messages with the header MIME-type. This inline match command limits the MIME-types in HTTP messages allowed through the ACE. It verifies that the header MIME-type value is in the internal list of supported MIME-types and the header MIME-type matches the actual content in the data or entity body portion of the message. If they do not match, the ACE performs the specified Layer 7 policy map action.

Table 13-22   *Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)*

Match Condition	Description
Header	Name and value in an HTTP header that are used for protocol inspection decisions. Do the following: **a.** In the Header field, choose one of the predefined HTTP headers to be matched, or choose HTTP Header to specify a different HTTP header. **b.** If you chose HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **c.** In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.

Header Length	Length of the header in the HTTP message that is used for protocol inspection decisions.
	
	Do the following:
	
	a. In the Header Length Type field, specify whether or not HTTP header request or response messages are to be used for protocol inspection decisions:
	
	   – **Request**—HTTP header request messages are to be checked for header length.
	
	   – **Response**—HTTP header response messages are to be checked for header length.
	
	b. In the Header Length Operator field, choose the operand to be used to compare header length:
	
	   – **Equal To**—The header length must equal the number in the Header Length Value (Bytes) field.
	
	   – **Greater Than**—The header length must be greater than the number in the Header Length Value (Bytes) field.
	
	   – **Less Than**—The header length must be less than the number in the Header Length Value (Bytes) field.
	
	   – **Range**—The header length must be within the range specified in the Header Length Lower Value (Bytes) field and the Header Length Higher Value (Bytes) field.
	
	c. Enter values to apply for header length comparison as follows:
	
	   – If you chose Equal To, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value (Bytes) field appears. In the Header Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are from 0 to 255.
	
	   – If you chose Range in the Header Length Operator field, the Header Length Lower Value (Bytes) and the Header Length Higher Value (Bytes) fields appear.
	
	   Do the following:
	
	   1. In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value (Bytes) field.
	
	   2. In the Header Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value (Bytes) field.

Table 13-22   *Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)*

Match Condition	Description
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types that are used for protocol inspection decisions. In the Header MIME Type field, choose the MIME message type to be used for this match condition.
Port Misuse	Misuse of port 80 (or any other port running HTTP) that is used for protocol inspection decisions. In the Port Misuse field, choose the application category to be used for this match condition: • **IM**—Instant messaging applications are to be used for this match condition. • **P2P**—Peer-to-peer applications are to be used for this match condition. • **Tunneling**—Tunneling applications are to be used for this match condition.

Request Method	Request method that is used for protocol inspection decisions. By default, ACEs allow all request and extension methods. This option allows you to configure class maps that define protocol inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods.
	
	a. In the Request Method Type field, choose the type of compliance to be used for protocol inspection decision:
	
	   – **Ext**—An HTTP extension method is to be used for protocol inspection decisions.
	
	   – **RFC**—A request method defined in RFC 2616 is to be used for protocol inspection decisions.
	
	b. In the Request Method field, choose the specific request method to be used.

Strict HTTP	Internal compliance checks that are performed to verify that a message is compliant with the HTTP RFC standard, RFC 2616. If the HTTP message is not compliant, the ACE performs the specified Layer 7 policy map action.
Transfer Encoding	HTTP transfer-encoding type that is used for protocol inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient. In the Transfer Encoding field, choose the type of encoding that is to be checked: • **Chunked**—Message body is transferred as a series of chunks. • **Compress**—Encoding format that is produced by the UNIX file compression program compress. • **Deflate**—.zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951. • **Gzip**—Encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952. • **Identity**—Default (identity) encoding which does not require the use of transformation.

Table 13-22   Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)

Match Condition	Description
URL	URL names are used for protocol inspection decisions. In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following www.*hostname.domain*. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html.
URL Length	URL length that is used for protocol inspection decisions.
	Do the following:
	a. In the URL Length Operator field, choose the operand to be used to compare URL length:
	– **Equal To**—URL length must equal the number in the URL Length Value (Bytes) field.
	– **Greater Than**—URL length must be greater than the number in the URL Length Value (Bytes) field.
	– **Less Than**—URL length must be less than the number in the URL Length Value (Bytes) field.
	– **Range**—URL length must be within the range specified in the URL Length Lower Value (Bytes) field and the URL Length Higher Value (Bytes) field.
	b. Enter values to apply for URL length comparison as follows:
	– If you chose Equal To, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value (Bytes) field appears. In the URL Length Value (Bytes) field, enter the value for comparison. Valid entries are from 1 to 65535 bytes.
	– If you chose Range in the URL Length Operator field, the URL Length Lower Value (Bytes) and the URL Length Higher Value (Bytes) fields appear.
	Do the following:
	1. In the URL Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value (Bytes) field.
	2. In the URL Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value (Bytes) field.

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. To define actions for this rule, continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.

- Click **Next** to deploy your entries and to configure another rule.

> **Note**   If you chose the Insert Before option described in Table 13-21 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:
>
> **1**. Click the Rule tab to refresh the Rule table.
>
> **2.** In the Rule table, choose the newly added rule.
>
> When the window refreshes, an empty action list appears.

Step 6   In the Action table, click **Add** to add a new action, or choose an existing action and click **Edit** to modify it.

The Action configuration window appears.

Step 7   In the Id field of the Action configuration window, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 8   In the Action Type field, choose the action to be taken for this rule:

- **Permit**—The HTTP traffic is to be allowed if it meets the match criteria.
- **Reset**—The HTTP traffic is to be denied if it meets the match criteria. A TCP reset message is sent to the client or server to close the connection.

Step 9   In the Action Log field, specify whether or not the action taken is to be logged:

- **N/A**—This option is not configured.
- **False**—Dropped packets are not to be logged in the software.
- **True**—Dropped packets are to be logged in the software.

Step 10   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.
- Click **Next** to configure another action for this policy map and rule.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31
- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization

> **Note**   HTTP optimization policy maps are available for ACE appliances only.

You can add rules and actions for Layer 7 HTTP optimization policy maps.

Assumptions

This topic assumes the following:

- An action list has been configured. See Configuring an HTTP Optimization Action List, page 14-3 for more information.
- A class map has been defined if you are not using the class-default class map. See Configuring Virtual Context Class Maps, page 13-6 for more information.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the Layer 7 HTTP optimization policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose an existing rule and click **Edit** to modify it.

The Rule configuration window appears.

Step 4   In the Type field of the Rule configuration window, configure rules using the information in Table 13-23.

Table 13-23   Layer 7 HTTP Optimization Policy Map Rules

Option	Description
Class Map	Class map to use for this traffic policy.
	Do the following:
	a. To use the class-default class map, check the Use Class Default check box.
	The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
	b. To use a previously created class map, do the following:
	1. Uncheck the Use Class Default check box.
	2. In the Class Map Name field, choose the class map to be used.

Table 13-23   *Layer 7 HTTP Optimization Policy Map Rules (continued)*

Option	Description
Match Condition	Match condition to use for this traffic policy.
	Do the following:
	a. In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
	b. In the Match Condition Type field, choose the method by which match decisions are to be made and their corresponding conditions. See Table 13-24 for information about these selections.
Insert Before	Order of the rules in the policy map.
	Do the following:
	a. Specify whether or not this rule is to precede another rule for this policy map:
	– **N/A**—This option is not configured.
	– **False**—This rule is not to precede another rule in this policy map.
	– **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.
	b. If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Table 13-24   Layer 7 HTTP Optimization Policy Map Match Conditions

Match Condition	Procedure
Cookie	HTTP cookie that is to be used to establish a match condition. Do the following: **a.** In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **b.** In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. **c.** In the Secondary Cookie field, check the checkbox to specify that the ACE is to use either the cookie name or the cookie value to satisfy this match condition. Uncheck this check box to indicate that the ACE is to use either the cookie name or the cookie value to satisfy this match condition.
Header	HTTP header that is to be used to establish a match condition. Do the following: **a.** In the Header field, choose one of the predefined HTTP headers to be matched, or choose HTTP Header to specify a different HTTP header. **b.** If you chose HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **c.** In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.
HTTP URL	Portion of an HTTP URL that is to be used to establish a match condition. Do the following: **a.** In the URL Expression field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following www.*hostname.domain*. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. **b.** In the Method Expression field, enter the HTTP method to match. Valid entries are method names entered as unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. You can enter either one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. To define actions for this rule, continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to configure another rule.

> **Note** If you chose the Insert Before option described in Table 13-23 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:
>
> **1**. Click the Rule tab to refresh the Rule table.
>
> **2**. In the Rule table, choose the newly added rule.
>
> When the window refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add a new action, or choose an existing action and click **Edit** to modify it.

The Action configuration window appears.

Step 7 In the Id field of the Action configuration window, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 8 In the Action Type field, confirm that Action List is selected.

Step 9 In the Action List field, choose the action list to apply to this policy map and rule.

Step 10 In the Optimization Parameter Map field, choose the optimization parameter map to apply to this policy map and rule.

Step 11 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.
- Click **Next** to deploy your entries and to configure another action for this rule.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31
- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic

You can set rules and actions for Layer 7 server load-balancing policy maps.

Assumptions

This topic assumes the following:

- You have configured a load-balancing policy map and want to establish the corresponding rules and actions.
- If you want to configure an SSL proxy action, you have configured SSL proxy service for this context.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the load-balancing policy map you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose an existing rule and **Edit** to modify it.

The Rule configuration window appears.

Step 4   In the Type field of the Rule configuration window, configure rules using the information in Table 13-25.

Table 13-25   Layer 7 Server Load Balancing Policy Map Rules

Option	Description
Class Map	Class map to use for this traffic policy. Do the following: **a.** To use the class-default class map, check the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic. **b.** To use a previously created class map, do the following: **1**. Clear the Use Class Default check box. **2**. In the Class Map Name field, choose the class map to be used.
Match Condition	Match condition to use for this traffic policy. Do the following: **a.** In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **b.** In the Match Condition Type field, choose the method by which match decisions are to be made and their corresponding conditions. See Table 13-26 for information about these selections.

Insert Before	Order of the rules in the policy map.
	
	 Do the following:
	
	 a. Specify whether or not this rule is to precede another rule for this policy map. Choices are as follows:
	
	    – **N/A**—This option is not configured.
	
	    – **False**—This rule is not to precede another rule in this policy map.
	
	    – **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.
	
	 b. If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Table 13-26   Layer 7 Server Load Balancing Policy Map Match Conditions

Match Condition	Description
HTTP Content	Option that appears for ACE modules only. Specific content contained within the HTTP entity-body is used to establish a match condition.
	Do the following:
	a. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.
	b. In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255.
HTTP Cookie	HTTP cookies are to be used for this match condition.
	Do the following:
	a. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
	b. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 13-34 lists the supported characters that you can use for matching string expressions.
HTTP Header	HTTP header and a corresponding value are to be used for this match condition.
	Do the following:
	a. In the Header Name field, specify the header to match in one of the following ways:
	– To specify an HTTP header that is not one of the standard HTTP headers, choose the first radio button, then enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
	– To specify a standard HTTP header, click the second radio button, then choose an HTTP header from the list.
	b. In the Header Value (Bytes) field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces, enclose the entire string in quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.

Table 13-26   Layer 7 Server Load Balancing Policy Map Match Conditions (continued)

Match Condition	Description
HTTP URL	Rule that performs regular expression matching against the received packet data from a particular connection based on the HTTP URL string.
	Do the following:
	a. In the URL Expression field, enter a URL, or portion of a URL, to match. Valid entries are URL strings from 1 to 255 alphanumeric characters. Include only the portion of the URL following www.*hostname.domain* in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. To match the www.anydomain.com portion, the URL string can take the form of a URL regular expression. The ACE supports regular expressions for matching URL strings. See Table 13-34 for a list of the supported characters that you can use in regular expressions.
	b. In the Method Expression field, enter the HTTP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).
Source Address	Client source IP address that is used to establish match conditions.
	Do the following:
	a. In the Source IP Address field, enter the source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).
	b. In the Source Netmask field, enter the subnet mask of the IP address. Enter the netmask in dotted-decimal notation (for example, 255.255.255.0). The default is 255.255.255.255.

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. To define the actions for this rule, continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to configure another rule.

Note   If you chose the Insert Before option described in Table 13-25 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.

2. In the Rule table, choose the newly added rule.

When the window refreshes, an empty action list appears.

Step 6   In the Action table, click **Add** to add a new action, or choose an existing action and click **Edit** to modify it.

Step 7   In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 8   In the Action Type field, choose the action to be taken and configure any action-specific attributes as described in Table 13-27.

Table 13-27   Layer 7 Server Load Balancing Policy Map Actions

Action	Description
Action	Action that the ACE is to implement for the rule. In the Action List field, choose an action list to associate with this rule.
Compress	Option that appears for ACE appliances (all versions) and ACE modules version A4(1.0) and later. The ACE is to compress packets that match this policy map. This option is available only when you associate an HTTP-type class map with a policy map.
	In the Compress Method field, specify the method that the ACE is to use to compress packets:
	• **Deflate**—Indicates that the ACE is to use the DEFLATE compression method when the client browser supports both the DEFLATE and GZIP compression methods.
	• **Gzip**—Indicates that ACE is to use the GZIP compression method when the client browser supports both the DEFLATE and GZIP compression methods.
Drop	Field that instructs the ACE to discard packets that match the rule. In the Action Log field, specify whether or not the dropped packets are to be logged in the software:
	• **N/A**—This option is not configured.
	• **False**—Dropped packets are not to be logged in the software.
	• **True**—Dropped packets are to be logged in the software.
Forward	Field that instructs the ACE to forward requests that match this policy map without load balancing the requests.
Insert-HTTP	Field that instructs the ACE to insert an HTTP header for Layer 7 load balancing for requests that match this policy map. This option allows the ACE to identify a client whose IP address has been translated using NAT by inserting a generic header and string value in the client HTTP request.
	Do the following:
	a. In the HTTP Header Name field, enter the name of the generic field in the HTTP header. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
	b. In the HTTP Header Value field, enter the value to be inserted into the HTTP header. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces, enclose the entire string in quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.
Reverse Sticky	Feature that applies only to the ACE module version 3.0(0)A2(1.1), ACE appliance version A4(1.0), or later releases of either device type. Reverse IP stickiness is an enhancement to regular stickiness and is used mainly in firewall load balancing (FWLB). It ensures that multiple distinct connections that are opened by hosts at both ends (client and server) are load-balanced and stuck to the same firewall. Reverse stickiness applies to such protocols as FTP, RTSP, SIP, and so on where there are separate control channels and data channels opened by the client and the server, respectively. For complete details about reverse stickiness, see the *Release Note for the Cisco Application Control Engine Module (Software Version 3.0(0)A2(X))*.
	In the Sticky Group field, choose the name of a an existing IP netmask sticky group that you want to associate with reverse IP stickiness.

Table 13-27   Layer 7 Server Load Balancing Policy Map Actions (continued)

Action	Description
Server Farm	Field that instructs the ACE to load balance client requests for content to a server farm. Do the following: **a.** In the Server Farm field, choose the server farm to which requests for content are to be sent. **b.** In the Backup Server Farm field, choose the backup server farm to which requests for content are to be sent. Choose **N/A** to indicate that no backup server farm is to be used. **c.** Choose the Sticky Enabled check box to indicate that the sticky group associated with this policy and applied to the primary server farm is applied to the backup server farm. Clear the Sticky Enabled check box to indicate that the sticky group associated with this policy and applied to the primary server farm in that policy is not applied to the backup server farm. **d.** Choose the Aggregate State Enabled check box to indicate that the operational state of the backup server farm is taken into consideration when evaluating the state of the load-balancing class in a policy map. Clear this check box to indicate that the operational state of the backup server farm is not taken into consideration when evaluating the state of the load-balancing class in a policy map.
Server Farm-NAT	Option that appears for ACE modules only. The ACE is to apply dynamic NAT to traffic for this policy map. Do the following: **a.** In the NAT Pool ID field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are from 1 to 2147483647. For information on configuring NAT pools, see Configuring Virtual Context BVI Interfaces, page 11-13. **b.** In the VLAN ID field, choose the VLAN to use for NAT. Valid entries are from 1 to 4094. **c.** In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.
Set IP-TOS	Set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. After the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. In the IP TOS Rewrite Value (Bytes) field, enter the IP DSCP value. Valid entries are from 0 to 255.
SSL-Proxy	SSL proxy client service that defines the SSL parameters that the ACE is to use during the handshake and subsequent SSL session. Do the following: **a.** In the SSL Proxy field, choose the SSL proxy service to be used for this action. **b.** In the SSL Proxy Type field, confirm that Client is selected to indicate that the ACE is to be configured so that it is recognized as an SSL client.
Sticky-Server Farm	Field that instructs the ACE to load balance requests that match this policy to a sticky server farm. In the Sticky Group field, choose the sticky server farm that is to be used for requests that match this policy map.

Step 9   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31
- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection

You can configure the rules and actions for a SIP deep packet inspection policy map.

Assumptions

This topic assumes the following:

- A SIP deep packet inspection policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1   Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the SIP deep packet inspection policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose the rule that you want to modify and click **Edit**.

The Rule window appears.

Step 4   In the Type field of the Rule window, configure rules using the information in Table 13-28.

Table 13-28   *Layer 7 SIP Deep Packet Inspection Policy Map Rules*

Option	Description
Class Map	Class map to use for this traffic policy. Do the following: **a.** To use the class-default class map, check the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic. **b.** To use a previously created class map, do the following: **1.** Uncheck the Use Class Default check box. **2.** In the Class Map Name field, choose the class map to be used.
Match Condition	Match condition to use for this traffic policy. Do the following: **a.** In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **b.** In the Match Condition Type field, choose the type of match condition to use for this policy map and configure any type-specific options using the information in Table 6-10.
Insert Before	Order of the rules in the policy map. Do the following: **a.** Specify whether or not this rule is to precede another rule for this policy map: – **N/A**—This option is not configured. – **False**—This rule is not to precede another rule in this policy map. – **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears. **b.** If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. Continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to add another rule.

> **Note**   If you chose the Insert Before option described in Table 13-28 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:
>
> **1.** Click the Rule tab to refresh the Rule table.
>
> **2.** In the Rule table, choose the newly added rule.
>
> When the window refreshes, an empty action list appears.

Step 6   In the Action table, click **Add** to add an entry or choose an existing entry to modify and click **Edit**.

Step 7   In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 8   In the Action Type field, choose the action to be taken for this rule:

- **Drop**—The SIP traffic is to be dropped if it meets the specified match criteria.
- **Permit**—The SIP traffic is to be allowed if it meets the specified match criteria.
- **Reset**—The SIP traffic is to be denied if it meets the specified match criteria. A TCP reset message is sent to the client or server to close the connection.

Step 9   In the Action Log field, specify whether the action taken is to be logged:

- **N/A**—This option is not configured.
- **False**—Dropped packets are not to be logged in the software.
- **True**—Dropped packets are to be logged in the software.

Step 10   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to deploy your entries and to configure another action.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31
- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection

You can configure the rules and actions for a Skinny Client Control Protocol (SCCP) deep packet inspection policy map.

Assumptions

This topic assumes the following:

- A Skinny deep packet inspection policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2 In the Policy Maps table, choose the Skinny deep packet inspection policy map that you want to set rules and actions for.

The Rule table appears.

Step 3 In the Rule table, click **Add** to add a new rule, or choose the rule you want to modify, then click **Edit**.

The Rule window appears.

Step 4 In the Type field of the Rule window, confirm that Match Condition is selected.

Step 5 In the Match Condition Name field, enter a name for this match condition.

Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

Step 6 In the Match Condition Type field, confirm that Message ID is selected.

Step 7 In the Message ID Operator field, specify whether of not the match criteria is for a single message identifier or for a range of message identifiers:

- **Equal To**—A single message identifier is used for this match condition.

  In the Message ID Value field, enter the numerical identifier of a SCCP message. Valid entries are from 0 to 65535.

- **Range**—A range of message identifiers is used for this match condition.

  Do the following:

  a. In the Message ID Low Range Value field, enter the lowest numerical identifier of a range of SCCP messages. Valid entries are from 0 to 65535.

  b. In the Message ID High Range Value field, enter the highest numerical identifier of a range of SCCP messages. Valid entries are integers from 0 to 65535, and the value in this field must equal or be greater than the value in the Message ID Low Range Value field.

Step 8 In the Insert Before field, specify whether or not this rule is to precede another rule in this policy map:

- **N/A**—This option is not configured.

- **False**—This rule is not to precede another rule in this policy map.

- **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.

Step 9   If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Step 10   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. To define the actions for this rule, continue with Step 11.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to configure another rule.

✎
Note   If you chose the Insert Before option in Step 8 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:
1. Click the Rule tab to refresh the Rule table.

2. In the Rule table, choose the newly added rule.

When the window refreshes, an empty action list appears.

Step 11   In Action table, click **Add** to add a new action, or choose an existing action and click **Edit** to modify it.

The Action configuration window appears.

Step 12   In the ID field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 13   In the Action Type field, confirm that Reset is selected.

Step 14   In the Action Log field, specify whether the action taken is to be logged:

- **N/A**—This option is not configured.

- **False**—Dropped packets are not to be logged in the software.

- **True**—Dropped packets are to be logged in the software.

Step 15   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31
- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for RADIUS Server Load Balancing

You can configure the rules and actions for RADIUS traffic received by the ACE.

Assumptions

This topic assumes the following:

- A RADIUS server load balancing traffic policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1   Choose **Config > Virtual Contexts > ** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the RADIUS server load balancing policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose the rule you want to modify and click **Edit**.

The Rule window appears.

Step 4   In the Type field of the Rule window, configure rules using the information in Table 13-29.

Table 13-29   RADIUS Server Load Balancing Policy Map Rules

Option	Description
Class Map	Class map to use for this traffic policy.
	Do the following:
	a. To use the class-default class map, check the Use Class Default check box.
	The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
	b. To use a previously created class map, do the following:
	1. Uncheck the Use Class Default check box.
	2. In the Class Map Name field, choose the class map to be used.

Table 13-29   RADIUS Server Load Balancing Policy Map Rules (continued)

Option	Description
Match Condition	Match condition to use for this traffic policy. Do the following: **a.** In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **b.** In the Match Condition Type field, choose the type of match condition to use for this policy map: – **Calling Station ID**—A unique identifier of the calling station is used to establish a match condition. In the RADIUS Calling Station ID field, enter the calling station identifier to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 13-34 for a list of the supported characters that you can use for matching string expressions. – **User Name**—A username is used to establish a match condition. In the User Name field, enter the name to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 13-34 for a list of the supported characters that you can use for matching string expressions.
Insert Before	Order of the rules in the policy map. Do the following: **a.** Indicate whether this rule is to precede another rule for this policy map: – **N/A**—This option is not configured. – **False**—This rule is not to precede another rule in this policy map. – **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears. **b.** If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. To enter actions for this rule, continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to configure another rule.

✎

Note   If you chose the Insert Before option described in Table 13-29 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.

2. In the Rule table, choose the newly added rule.

When the window refreshes, an empty action list appears.

Step 6   In the Action table, click **Add** to add an entry or choose an existing entry to modify and click **Edit**.

Step 7 In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 8 In the Action Type field, configure actions for this rule using the information in Table 13-17.

Step 9 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

Related Topics

- Configuring Traffic Policies, page 13-1

- Configuring Virtual Context Class Maps, page 13-6

- Configuring Virtual Context Policy Maps, page 13-31

- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for RDP Server Load Balancing

Use this procedure to configure the rules and actions for RDP traffic received by the ACE.

Assumptions

This topic assumes the following:

- An RDP server load balancing traffic policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1 Choose **Config > Virtual Contexts > *context* > Expert > Policy Maps**.

The Policy Maps table appears.

Step 2 In the Policy Maps table, choose the RDP server load balancing policy map that you want to set rules and actions for.

The Rule table appears.

Step 3 In the Rule table, click **Add** to add a new rule.

The Rule window appears.

Step 4 In the Type field of the Rule window, confirm that Class Map is selected.

Step 5 Check the Use Class Default check box.

✎

Note You can only use the default class map (Class Default) with an RDP server load balancing policy map.

The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. The class-default class map has an implicit **match any** statement that enables it to match all traffic.

Step 6 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. To enter actions for this rule, continue with Step 7.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to configure another rule.

Step 7 In the Action table, click **Add** to add an entry, or choose an existing entry to modify and click **Edit**.

Step 8 In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 9 In the Action Type field, configure actions for this rule using the information in Table 13-17.

Step 10 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31
- Configuring Rules and Actions for Policy Maps, page 13-34

Setting Policy Map Rules and Actions for RTSP Server Load Balancing

You can configure the rules and actions for RTSP traffic received by the ACE.

Assumptions

This topic assumes the following:

- An RTSP server load balancing traffic policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Expert > Policy Maps**.

The Policy Maps table appears.

Step 2 In the Policy Maps table, choose the RTSP server load balancing policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose the rule that you want to modify and click **Edit**.

The Rule window appears.

Step 4   In the Type field of the Rule window, configure rules using the information in Table 13-30.

Table 13-30   ***RTSP Server Load Balancing Policy Map Rules***

Option	Description
Class Map	Class map to use for this traffic policy.
	Do the following:
	a. To use the class-default class map, check the Use Class Default check box.
	The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
	b. To use a previously created class map, do the following:
	1. Uncheck the Use Class Default check box.
	2. In the Class Map Name field, choose the class map to be used.
Match Condition	Match condition to use for this traffic policy.
	Do the following:
	a. In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
	b. In the Match Condition Type field, choose the type of match condition to use for this policy map and configure any type-specific options using the information in Table 13-31.
Insert Before	Order of the rules in the policy map.
	Do the following:
	a. Indicate whether or not this rule is to precede another rule for this policy map:
	– **N/A**—This option is not configured.
	– **False**—This rule is not to precede another rule in this policy map.
	– **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.
	b. If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Table 13-31   RTSP Policy Map Match Conditions

Match Condition	Description

RTSP Header	RTSP header information that is used for matching criteria.
	
	Do the following:
	
	a. In the Header Name field, specify the header to match in one of the following ways:
	
	  – To specify an RTSP header that is not one of the standard RTSP headers, choose the first radio button, then enter the RTSP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
	
	  – To specify a standard RTSP header, click the second radio button, then choose an RTSP header from the list.
	
	b. In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the RTSP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.

RTSP URL	URL or portion of a URL that is used for match criteria. Do the following: **a.** In the URL Expr field, enter a URL, or portion of a URL, to match. The ACE performs matching on whatever URL string appears after the RTSP method, regardless of whether the URL includes the host name. The ACE supports regular expressions for matching URL strings. See Table 13-34 for a list of the supported characters that you can use in regular expressions. **b.** In the Method Expr field, enter the RTSP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can be either one of the standard RTSP method names (DESCRIBE, ANNOUNCE, GET_PARAMETER, OPTIONS, PAUSE, PLAY, RECORD, REDIRECT, SETUP, SET_PARAMETER, TEARDOWN) or a text string that must be matched exactly (for example, STINGRAY).
Source Address	Source IP address that is used for match criteria. Do the following: **a.** In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **b.** In the Source Netmask field, choose the subnet mask for the source IP address.

Step 5   In the Insert Before field, indicate whether or not this rule is to precede another rule for this policy map:

- **N/A**—This option is not configured.
- **False**—This rule is not to precede another rule in this policy map.
- **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.

Step 6   If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Step 7   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears. Continue with Step 8.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to add another rule.

✏️

Note   If you chose the Insert Before option in Table 13-31 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

   1. Click the Rule tab to refresh the Rule table.

   2. In the Rule table, choose the newly added rule.

   When the window refreshes, an empty action list appears.

Step 8   In the Action table, click **Add** to add an entry, or choose an existing entry to modify and click **Edit**.

Step 9   In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 10   In the Action Type field, configure actions for this rule using the information in Table 13-17.

Step 11   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

Related Topics

Setting Policy Map Rules and Actions for SIP Server Load Balancing

You can configure the rules and actions for SIP traffic received by the ACE.

Assumptions

This topic assumes the following:

- A SIP server load balancing traffic policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

Step 1   Choose **Config > Virtual Contexts > *context* > Expert > Policy Maps**.

The Policy Maps table appears.

Step 2   In the Policy Maps table, choose the SIP server load balancing policy map that you want to set rules and actions for.

The Rule table appears.

Step 3   In the Rule table, click **Add** to add a new rule, or choose the rule that you want to modify and click **Edit**.

The Rule window appears.

Step 4   In the Type field of the Rule window, configure rules using the information in Table 13-32.

Table 13-32   SIP Server Load Balancing Policy Map Rules

Option	Description
Class Map	Class map to use for this traffic policy.
	Do the following:
	a. To use the class-default class map, check the Use Class Default check box.
	The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
	b. To use a previously created class map:
	1. Uncheck the Use Class Default check box.
	2. In the Class Map Name field, choose the class map to be used.
Match Condition	Match condition to use for this traffic policy.
	Do the following:
	a. In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
	b. In the Match Condition Type field, choose the type of match condition to use for this policy map and configure any type-specific options using the information in Table 13-33.
Insert Before	Order of the rules in the policy map.
	Do the following:
	a. Indicate whether or not this rule is to precede another rule for this policy map. Choices are as follows:
	– **N/A**—This option is not configured.
	– **False**—This rule is not to precede another rule in this policy map.
	– **True**—This rule is to precede another rule in this policy map. The Insert Before Policy Rule field appears.
	b. If you chose True, in the Insert Before Policy Rule field, choose the rule that you want the current rule to precede.

Table 13-33   SIP Server Load Balancing Policy Map Match Conditions

Match Condition	Description

SIP Header	SIP header information that is used for matching criteria.
	
	Do the following:
	
	a. In the Header Name field, specify the header to match in one of the following ways:
	
	   – To specify a SIP header that is not one of the standard SIP headers, choose the first radio button, then enter the SIP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
	
	   – To specify a standard SIP header, click the second radio button, then choose an SIP header from the list.
	
	b. In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the SIP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.

Source Address	Source IP address is used for match criteria. Do the following: **a.** In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **b.** In the Source Netmask field, choose the subnet mask for the source IP address.

Step 5   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. The window refreshes and the Action table appears so you can enter actions for this rule. Continue with Step 6.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

- Click **Next** to deploy your entries and to add another rule.

Step 6   In the Action table, click **Add** to add an entry, or choose an existing entry to modify and click **Edit**.

Step 7   In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 8   In the Action Type field, configure actions for this rule using the information in Table 13-17.

Step 9   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- Click **Next** to deploy your entries and to configure another action.

✎

Note   If you chose the Insert Before option in Table 13-32 and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.

2. In the Rule table, choose the newly added rule.

When the window refreshes, an empty action list appears.

Related Topics

Special Characters for Matching String Expressions

Table 13-34 identifies the special characters that can be used in matching string expressions.

Table 13-34   Special Characters for Matching String Expressions

Convention	Description
.	One of any character.
.*	Zero or more of any character.
\.	Period (escaped).
\xhh	Non-printable character.
[*charset*]	Match any single character from the range.
[^charset]	Do not match any character in the range. All other characters represent themselves.
()	Expression grouping.
expr1 | expr2	OR of expressions.
(expr)*	0 or more of expression.
(expr)+	1 or more of expression.
.\a	Alert (ASCII 7).
.\b	Backspace (ASCII 8).
.\f	Form-feed (ASCII 12).
.\n	New line (ASCII 10).
.\r	Carriage return (ASCII 13).
.\t	Tab (ASCII 9).
.\v	Vertical tab (ASCII 11).
.\0	Null (ASCII 0).
.\\	Backslash.
.\x##	Any ASCII character as specified in two-digit hexadecimal notation.

Related Topics

- Configuring Traffic Policies, page 13-1
- Configuring Virtual Context Class Maps, page 13-6
- Configuring Virtual Context Policy Maps, page 13-31
- Configuring Rules and Actions for Policy Maps, page 13-34

Configuring Actions Lists

An action list is a named group of actions that you associate with a Layer 7 policy map. The ACE supports the following types action lists:

- An HTTP optimization action list groups a series of individual application acceleration and optimization operations that you want the ACE to perform. The HTTP optimization action list is associated with a Layer 7 HTTP optimization policy map (see the "Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization" section on page 13-58).

- An HTTP header modify action list performs the following operations:

  – Groups a series of individual functions to insert, rewrite, or delete HTTP headers.

  – Configures the SSL URL rewrite function.

  – Inserts SSL session parameters, client certificate fields, and server certificate fields into the HTTP requests that the ACE receives over the connection.

  The HTTP header action list is associated with a Layer 7 server load-balancing policy map (see the "Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic" section on page 13-62).

Table 13-35 lists the action lists that you can configure using the ACE.

Table 13-35   Action Lists

Action List	Topic
Optimization Action List	Configuring an HTTP Optimization Action List, page 14-3
HTTP Header Modify Action List	Configuring an HTTP Header Modify Action List, page 13-84

Configuring an HTTP Header Modify Action List

An HTTP header modify action list groups a series of individual functions to insert, rewrite, or delete HTTP headers. It can also be used to configure the SSL URL rewrite function.

This section includes the following topics:

- Configuring HTTP Header Insertion, Deletion, and Rewrite, page 13-84

- Configuring SSL URL Rewrite, page 13-87

- Configuring SSL Header Insertion, page 13-88

Configuring HTTP Header Insertion, Deletion, and Rewrite

You can configure an HTTP header modify action list that inserts, rewrites, or deletes HTTP headers.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Expert > HTTP Header Modify Action Lists**.

- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Expert > HTTP Header Modify Action Lists**.

The HTTP Header Modify Action Lists table appears.

Step 2   In the HTTP Header Modify Action Lists table, click **Add** to add a new action list, or choose an existing action list and click **Edit** to modify it.

Step 3   For a new action list, in the Action List Name field, enter a unique name for the action list.

Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters. Click **Deploy Now** when completed to save the configuration and display the editing tabs.

Step 4   Click the **Header Action** tab.

The Header Action table appears.

Step 5   In the Header Action table, click **Add** to add a new entry to the table.

The Header Action configuration window appears. Enter the required information as shown in Table 13-36.

Table 13-36   Header Action Configuration Window Fields

Header Action Field	Description / Action
Operator	HTTP header modify action that the ACE is to take in an HTTP request from a client, a response from a server, or both. Choices are as follows: • **Delete**—Deletes an HTTP header in a request from a client, in a response from a server, or both. • **Insert**—Insert a header name and value in an HTTP request from a client, a response from a server, or both. When the ACE uses Network Address Translation (NAT) to translate the source IP address of a client to a VIP, servers need a way to identify that client for the TCP and IP return traffic. To identify a client whose source IP address has been translated using NAT, you can instruct the ACE to insert a generic header and string value of your choice in the client HTTP request. • **Rewrite**—Rewrite an HTTP header in request packets from a client, response packets from a server, or both.

Table 13-36   Header Action Configuration Window Fields (continued)

Header Action Field	Description / Action
Direction	HTTP header modify action that the ACE is to take with respect to the selected operator (Insert, Delete, or Rewrite). Choices are as follows: **Insert:** • **Both**—Specifies that the ACE insert an HTTP header in both HTTP request packets and response packets. • **Request**—Specifies that the ACE insert an HTTP header only in HTTP request packets from clients. • **Response**—Specifies that the ACE insert an HTTP header only in HTTP response packets from servers. **Delete:** • **Both**—Specifies that the ACE delete the header in both HTTP request packets and response packets. • **Request**—Specifies that the ACE delete the header only in HTTP request packets from clients. • **Response**—Specifies that the ACE delete the header only in HTTP response packets from servers. **Rewrite:** • **Both**—Specifies that the ACE rewrite an HTTP header string in both HTTP request packets and response packets. • **Request**—Specifies that the ACE rewrite an HTTP header string only in HTTP request packets from clients. • **Response**—Specifies that the ACE rewrite an HTTP header string only in HTTP response packets from servers.
Header Name	Identifier of an HTTP header. Enter an unquoted text string with a maximum of 255 alphanumeric characters.
Header Value	Value of the HTTP header that you want to insert or replace in request packets, response packets, or both. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can also use the following dynamic replacement strings: • **%is**—Inserts the source IP address in the HTTP header • **%id**—Inserts the destination IP address in the HTTP header • **%ps**—Inserts the source port in the HTTP header • **%pd**—Inserts the destination port in the HTTP header The ACE supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.
Replace	Pattern string that you want to substitute for the header value regular expression. For dynamic replacement of the first and second parenthesized expressions from the header value, use %1 and %2, respectively.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **OK** to save your entries. This option appears for configuration building blocks.

- Click **Cancel** to exit this procedure without saving your entries.

- Click **Next** to save your entries.

Related Topics

- Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 13-62, Table 13-27

Configuring SSL URL Rewrite

You can configure an HTTP header modify action list that performs SSL URL rewrite.

When a client sends encrypted traffic to the ACE in an SSL termination configuration, the ACE terminates the SSL traffic and then sends clear text to the server. Because the server is unaware of the encrypted traffic flowing between the client and the ACE, the server may return to the client a URL in the Location header of HTTP redirect responses (301: Moved Permanently or 302: Found) in the form http://www.cisco.com instead of https://www.cisco.com. In this case, the client makes a request to the unencrypted insecure URL, even though the original request was for a secure URL. Because the client connection changes to HTTP, the requested data may not be available from the server using a clear text connection.

To solve this problem, the ACE provides SSLURL rewrite, which changes the redirect URL from http:// to https:// in the Location response header from the server before sending the response to the client. By using URL rewrite, you can avoid nonsecure HTTP redirects. All client connections to the web server will be SSL, ensuring the secure delivery of HTTPS content back to the client. The ACE uses regular expression matching to determine whether the URL needs rewriting. If a Location response header matches the specified regular expression, the ACE rewrites the URL. In addition, the ACE provides parameters to add or change the SSL and the clear port numbers.

Procedure

Step 1   Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Expert > HTTP Header Modify Action Lists**.

- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Expert > HTTP Header Modify Action Lists**.

The HTTP Header Modify Action Lists table appears.

Step 2   In the HTTP Header Modify Action Lists table, click **Add** to add a new action list, or choose an existing action list and click **Edit** to modify it.

Step 3   For a new action list, in the Action List Name field enter a unique name for the action list.

Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters. Click **Deploy Now** when completed to save the configuration and display the editing tabs.

Step 4   Click the **SSL Action** tab.

The SSL Action table appears.

Step 5   In the SSL Action table, click **Add** to add a new entry to the SSL Action table.

The SSL Action configuration window appears. Enter the required information as shown in Table 13-37.

Table 13-37   SSL Action Configuration Window Fields

Header Action Field	Description / Action
URL Expression	Field that specifies the rewriting of the URL in the Location response header based on a URL regular expression match. If the URL in the Location header matches the URL regular expression string that you specify, the ACE rewrites the URL from http:// to https:// and rewrites the port number. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. Alternatively, you can enter a text string with spaces if you enclose the entire string in quotation marks (").
	The location regex that you enter must be a pure URL (for example, www\.cisco\.com) with no port or path designations. To match a port, use the SSL Port and Clear Port parameters. If you need to match a path, use the HTTP header rewrite feature to rewrite the string. For information about the HTTP header rewrite feature, see the "Configuring HTTP Header Insertion, Deletion, and Rewrite" section on page 13-84.
	The ACE supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See Table 13-34 for a list of the supported characters that you can use in regular expressions.
SSL Port	SSL port number from which the ACE translates a clear port number before sending the server redirect response to the client. Enter a value from 1 to 65535. The default is 443.
Clear Port	Clear port number to which the ACE translates the SSL port number before sending a server redirect response to the client. Enter a value from 1 to 65535. The default is 80.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **OK** to save your entries. This option appears for configuration building blocks.

- Click **Cancel** to exit this procedure without saving your entries.

- Click **Next** to save your entries.

Related Topics

- Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 13-62, Table 13-27

Configuring SSL Header Insertion

Note   This option is available only for the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of either device type.

You can configure an HTTP header modify action list that performs SSL header insertion.

When a client sends encrypted traffic to the ACE in an SSL termination configuration, the ACE terminates the SSL traffic and then sends clear text to the server, which is unaware of the encrypted traffic flowing between the client and the ACE. Using an action list associated with a Layer 7 HTTP load-balancing policy map, you can instruct the ACE to perform SSL HTTP header insertion. The ACE provides the server with the following SSL session information by inserting HTTP headers into the HTTP requests that it receives over the connection:

- Session Parameters—SSL session parameters that the ACE and client negotiate during the SSL handshake.

- Server Certificate Fields—Information regarding the SSL server certificate that resides on the ACE.

- Client Certificate Fields—Information regarding the SSL client certificate that the ACE retrieves from the client when you configure the ACE to perform client authentication.

Note To prevent HTTP header spoofing, the ACE deletes any incoming HTTP headers that match one of the headers that it is going to insert into the HTTP request.

By default, the ACE inserts the SSL header information into the first HTTP request only that it receives over the connection. When the ACE and client need to renegotiate their connection, the ACE updates the HTTP header information that it send to the server to reflect the new session parameters. You can also instruct the ACE to insert the session information into every HTTP request that it receives over the connection by creating an HTTP parameter map with either the **Header Modify Per-Request** or **HTTP Persistence Rebalance** options enabled (see the "Configuring HTTP Parameter Maps" section on page 9-9).

Note The maximum amount of data that the ACE can insert is 512 bytes. The ACE truncates the data if it exceeds this limit.

Procedure

Step 1   Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Expert > HTTP Header Modify Action Lists**.

- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Expert > HTTP Header Modify Action Lists**.

The HTTP Header Modify Action Lists table appears.

Step 2   In the HTTP Header Modify Action Lists table, do one of the following:

- To add a new action list, click **Add**. In the Action List Name field, enter a unique name for the action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters. Click **Deploy Now** when completed to save the configuration and display the editing tabs.

- To edit an existing action list, choose the action list and click **Edit** to display the editing tabs.

Step 3   Click the **SSL Header Insert** tab.

The SSL Header Insert table appears.

Step 4   In the SSL Header Insert table, click **Add** to add a new entry to the SSL Header Insert table.

The SSL Header Insert configuration window appears. Enter the required information as shown in Table 13-38.

Table 13-38   ***SSL Action Configuration Window Fields***

Header Action Field	Description / Action
Request	Type of SSL header information to insert into the HTTP request: • **Client-Certificate**—Information about the client certificate that the ACE retrieves from the client. • **Server-Certificate**—Information about the server certificate that resides on the ACE. • **Session**—Information about the session parameters that the ACE and client negotiated during the SSL handshake.
Algorithm	Field that appears only when the Request field is set to either Client-Certificate or Server-Certificate. Specify the following certificate field information to insert into the HTTP request: • **Authority-Key-Id**—X.509 authority key identifier. • **Basic-Constraints**—X.509 basic constraints. • **Certificate-Version**—X.509 certificate version. • **Data-Signature-Algorithm**—X.509 hashing and encryption method. • **Fingerprint-SHA1**—SHA1 hash of the certificate. • **Issuer**—X.509 certificate issuer's distinguished name. • **Issuer-CN**—X.509 certificate issuer's common name. • **Not-After**—Date after which the certificate is not valid. • **Not-Before**—Date before which the certificate is not valid. • **Public-Key-Algorithm**—Algorithm used for the public key. • **RSA-Exponent**—Public RSA exponent. • **RSA-Modulus**—RSA algorithm modulus. • **RSA-Modulus-Size**—Size of the RSA public key. • **Serial-Number**—Certificate serial number. • **Signature**—Certificate signature. • **Signature-Algorithm**—Certificate signature algorithm. • **Subject**—X.509 subject's distinguished name. • **Subject-CN**—X.509 subject's common name. • **Subject-Key-Id**—X.509 subject key identifier. For more information, see the *Cisco Application Control Engine Module SSL Configuration Guide*.

Table 13-38   *SSL Action Configuration Window Fields (continued)*

Header Action Field	Description / Action

CipherKey	Field that appears only when the Request field is set to Session. Indicate the following session parameters to insert into the HTTP request:
	
	• **Cipher-Key-Size**—Symmetric cipher key size.
	
	• **Cipher-Name**—Symmetric cipher suite name.
	
	• **Cipher-Use-Size**—Symmetric cipher use size.
	
	• **Id**—SSL Session ID. The default is 0.
	
	• **Protocol-Version**—Version of SSL or TLS.
	
	• **Step-Up**—Use of SGC or StepUp cryptography to increase the level of security by using 128-bit encryption.
	
	• **Verify-Result**—SSL session verify result. Possible values are as follows:
	
	  – ok—The SSL session is established.
	
	  – certificate is not yet valid—The client certificate is not yet valid.
	
	  – certificate is expired—The client certificate has expired.
	
	  – bad key size—The client certificate has a bad key size.
	
	  – invalid not before field—The client certificate notBefore field is in an unrecognized format.
	
	  – invalid not after field—The client certificate notAfter field is in an unrecognized format.
	
	  – certificate has unknown issuer—The client certificate issuer is unknown.
	
	  – certificate has bad signature—The client certificate contains a bad signature.
	
	  – certificate has bad leaf signature—The client certificate contains a bad leaf signature.
	
	  – unable to decode issuer public key—The ACE is unable to decode the issuer public key.
	
	  – unsupported certificate—The client certificate is not supported.
	
	  – certificate revoked— The client certificate has been revoked.
	
	  – internal error—An internal error exists.
	
	For more information, see the *Cisco Application Control Engine Module SSL Configuration Guide*.

Value	Field that appears only when the Request field is set to either Client-Certificate or Server-Certificate. Choose one of the following options: • **N/A**—Specifies that the selected algorithm or cipher key is inserted without adding a prefix to it or renaming it. • **Prefix**—Enables you to specify a prefix string to place before the specified certificate or session field name. For example, if you specify the prefix Acme-SSL for the SSL session field name Cipher-Name, then the field name becomes Acme-SSL-Session-Cipher-Name. • **Rename**—Enables you to specify a new name for the specified certificate or session field name.
Prefix	Field that appears only when the Value field is set to Prefix. Enter a quoted text string to place before the specified certificate or session field name. The maximum combined number of prefix string and field name characters that the ACE permits is 32.
Rename	Field that appears only when the Value field is set to Rename. Enter a new name to the specified certificate or session field name. The name must be an unquoted text string with no spaces. The maximum number of field name string characters that the ACE permits is 32.

Step 5   Repeat Step 4 for each certificate field or session parameter that you want the ACE to insert.

Step 6   Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- Click **OK** to save your entries. This option appears for configuration building blocks.

- Click **Cancel** to exit this procedure without saving your entries.

- Click **Next** to deploy your entries and to add another entry to the SSL Header Insert table.

Related Topics

- Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 13-62, Table 13-27