CHAPTER 11

Configuring Traffic Policies

Date: 4/23/09

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. This section includes the following topics about traffic policies:

- Traffic Policy Overview, page 11-1
- Class Map and Policy Map Overview, page 11-2
- Configuring Virtual Context Class Maps, page 11-6
- Setting Match Conditions for Class Maps, page 11-8
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32
- Configuring Actions Lists, page 11-78

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 11-2
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

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 11-1 lists the available policies and the ACE devices that support them.

Table 11-1 Traffic Policies and ACE Device Support

		ACE Device			
Policy Map Type	**Description**	**ACE 1.0 Module**	**ACE 2.0 Module**	**ACE 4710 Appliance Running Image A1(8)**	**ACE 4710 Appliance Running Image A3(1.0)**
Layer 3/4 Management Traffic (First-Match)	Layer 3 and Layer 4 policy map for network management traffic received by the ACE	X	X	X	X
Layer 3/4 Network Traffic (First-Match)	Layer 3 and Layer 4 policy map for traffic passing through the ACE	X	X	X	X
Layer 7 Command Inspection - FTP (First-Match)	Layer 7 policy map for inspection of FTP commands	X	X	X	X
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Layer 7 policy map for inspection of HTTP packets	X	X	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	X

Table 11-1 Traffic Policies and ACE Device Support (continued)

Policy Map Type	Description	ACE Device			
		ACE 1.0 Module	ACE 2.0 Module	ACE 4710 Appliance Running Image A1(8)	ACE 4710 Appliance Running Image A3(1.0)
Layer 7 Server Load Balancing (First-Match)	Layer 7 policy map for HTTP server load balancing	X	X	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 11-3
- Policy Maps, page 11-4
- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 11-5
- Configuring Virtual Context Global Traffic Policies, page 3-26

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.

- 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

- Class Map and Policy Map Overview, page 11-2
- Policy Maps, page 11-4
- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 11-5
- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6

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 11-2
- Class Maps, page 11-3
- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 11-5
- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Policy Maps, page 11-30

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 7-1 for a list of the available parameter maps and the ACE devices that support them.

Related Topic

- Configuring Parameter Maps, page 7-1
- Class Map and Policy Map Overview, page 11-2
- Class Maps, page 11-3
- Policy Maps, page 11-4

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 11-30
- Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 11-21
- Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 11-47
- Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 11-62

Configuring Virtual Context Class Maps

Class maps are used to define each 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.

- 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)

Note To successfully 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 Click **Add** to add a new class map, or select an existing class map, then click **Edit** to modify it.

Step 3 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, select the type of class map you are creating.

The types that are available depend on the ACE that you are configuring. Table 11-2 lists the available class map types and the ACE devices that support them.

Table 11-2 Class Maps and ACE Module and Device Support

	ACE Modules and Devices			
Class Map	**ACE 1.0 Module**	**ACE 2.0 Module**	**ACE Appliance Running Image A1(8)**	**ACE Appliance Running Image A3(1.0)**
Layer 3/4 Management Traffic	X	X	X	X
Layer 3/4 Network Traffic	X	X	X	X
Layer 7 Command Inspection - FTP	X	X	X	X
Layer 7 Deep Packet Inspection - HTTP	X	X	X	X
Layer 7 Deep Packet Inspection - SIP		X		X
Layer 7 Server Load Balancing	X	X	X	X
Server Load Balancing - Generic		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, select the method to be used to evaluate multiple match statements when multiple match conditions exist:

- Any—A match exists if at least one of the match conditions is satisfied. If you select Any, you can specify only one type of match condition.
- All—A match exists only if all match conditions are satisfied. If you select All, you can specify multiple types of match conditions.

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 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 11-8 for more information.
- **Cancel** to exit the procedure without saving your entries and to return to the Class Maps table.
- **Next** to deploy your entries and to configure another class map.

Related Topics

- Using Virtual Contexts, page 3-1
- Deleting Class Maps, page 11-8

- Setting Match Conditions for Class Maps, page 11-8
- Configuring Virtual Context Policy Maps, page 11-30

Deleting Class Maps

To successfully 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 Select the class maps you want to delete, then click **Delete**. A 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 Click **OK** to confirm the deletion or **Cancel** to retain the class map and to return to the Class Maps table.

Related Topics

- Class Map and Policy Map Overview, page 11-2
- Configuring Virtual Context Class Maps, page 11-6

Setting Match Conditions for Class Maps

Table 11-3 lists the class maps available for all ACE devices and provides links to topics for setting match conditions:

Table 11-3 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 11-12
Layer 3/Layer 4 network traffic	Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 11-9
Layer 7 FTP command inspection	Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 11-21

Table 11-3 Class Maps Available for All ACE Devices (continued)

Class Map	Related Topic
Layer 7 HTTP deep packet inspection	Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps, page 11-16
Layer 7 server load balancing	Setting Match Conditions for Layer 7 Server Load Balancing Class Maps, page 11-14

Table 11-4 lists additional class maps that are available for ACE 2.0 modules and and the ACE 4710 A3(1.0) release, and provides links to topics for setting match conditions.

Table 11-4 Additional Class Maps for ACE 2.0 Modules and the ACE 4710 A3(1.0) Release

Class Map	Related Topic
Generic server load balancing	Setting Match Conditions for Generic Server Load Balancing Class Maps, page 11-22
Layer 7 SIP deep packet inspection	Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps, page 11-28
RADIUS server load balancing	Setting Match Conditions for RADIUS Server Load Balancing Class Maps, page 11-23
RTSP server load balancing	Setting Match Conditions for RTSP Server Load Balancing Class Maps, page 11-25
SIP server load balancing	Setting Match Conditions for SIP Server Load Balancing Class Maps, page 11-26

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

Use this procedure to specify the 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the Layer 3/4 network traffic 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer from 2 to 255.

Step 5 In the Match Condition Type field, select the type of match condition to use for this class map and configure any match-specific attributes as described in Table 11-5.

Table 11-5 Layer 3/Layer 4 Network Traffic Class Map Match Conditions

Match Condition	Description
Access List	An access list is the match type for this match condition. In the ACL field, select the ACL to use as the match condition.
Any	Any Layer 3 or Layer 4 traffic passing through the ACE meets the match condition.
Destination Address	The destination address is the match type for this match condition. 1. In the Destination Address field, enter the destination IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Destination Netmask field, select the subnet mask for the destination IP address.
Port	A UDP or TCP port or range of ports is the match type for this match condition. 1. In the Port Protocol field, select TCP or UDP as the protocol to match. 2. In the Port Operator field, select 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 integers 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. a. In the Lower Port Number field, enter the first port number in the port range for the match condition. b. 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.

Table 11-5 Layer 3/Layer 4 Network Traffic Class Map Match Conditions (continued)

Match Condition	Description
Source Address	The source IP address is the match type for this match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.
Virtual Address	A virtual IP address is the match type for this match condition. 1. 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. 2. In the Virtual IP Netmask field, select the subnet mask for the virtual IP address. 3. In the Virtual Address Protocol field, select the protocol to be used for this match condition. For a list of protocols and their respective numbers, see Table 3-12. 4. Depending on the protocol that you select, such as TCP or UDP, additional fields appear. If they appear, enter the information described in the following steps. 5. In the Port Operator field, select 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 integers 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 integers from 0 to 65535. A value of 0 indicates that the ACE is to include all ports. a. In the Lower Port Number field, enter the first port number in the port range for the match condition. b. In the Upper Port Number field, enter the last port number in the port range for the match condition.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- Configuring Traffic Policies, page 11-1
- Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 11-12
- Setting Match Conditions for Layer 7 Server Load Balancing Class Maps, page 11-14

- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Virtual Context Class Maps, page 11-6

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

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the Layer 3/Layer 4 management 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 select the match conditions you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 Enter the match conditions (see Table 11-6).

Table 11-6 Layer 3/Layer 4 Management Traffic Class Map Match Conditions

Field	Description
Sequence Number	Enter an integer 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 11-6 Layer 3/Layer 4 Management Traffic Class Map Match Conditions (continued)

Field	Description
Management Protocol Type	This field identifies the network management protocols that can be received by the ACE. Select the allowed protocol for this match condition: • 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. This option is available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. • 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	Select the 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	This field 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	This field appears if Source Address is selected for Traffic Type. Select the subnet mask for the source IP address.

Step 5 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Real Servers, page 5-4
- Configuring Server Farms, page 5-12
- Configuring Sticky Groups, page 6-7

Setting Match Conditions for Layer 7 Server Load Balancing Class Maps

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer 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, select the type of match to use and configure condition-specific attributes as described in Table 11-7.

Table 11-7 Layer 7 Server Load Balancing Class Map Match Conditions

Match Condition	Description
Class Map	A class map is to be used to establish a match condition. In the Class Map field, select the class map to apply to this match condition.
HTTP Content	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Specific content contained within the HTTP entity-body is used to establish a match condition. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. 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 integers from 1 to 255.

Table 11-7 Layer 7 Server Load Balancing Class Map Match Conditions (continued)

Match Condition	Description
HTTP Cookie	An HTTP cookie is to be used to establish a match condition. 1. 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. 2. 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. 3. Select the Secondary Cookie Matching check box to indicate that the ACE is to use both the cookie name and the cookie value to satisfy this match condition. Clear 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	An HTTP header is to be used to establish a match condition. 1. 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, select 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 select an HTTP header from the list. 2. 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 11-35 for a list of the supported characters that you can use in regular expressions.
HTTP URL	A portion of an HTTP URL is to be used to establish a match condition. 1. 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. 2. 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	The source IP address is to be used to establish a match condition. 1. In the Source Address field, enter the source IP address of the client in dotted-decimal notation, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask of the source IP address.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- Using Virtual Contexts, page 3-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

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

The ANM allows you to create Layer 7 class maps and policy maps to be used for HTTP deep packet inspection 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the Layer 7 HTTP deep packet inspection 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer 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, select the method by which match decisions are to be made and configure condition-specific attributes as described in Table 11-8.

Table 11-8 Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions

Match Condition	Description
Content	Specific content contained within the HTTP entity-body is to be used for protocol inspection decisions. **1.** In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. **2.** 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 integers from 1 to 255.
Content Length	The content parse length in an HTTP message is to be used for protocol inspection decisions. **1.** In the Content Length Operator field, select the operand to use to compare content length: – 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. **2.** Enter values to apply for content length comparison: – If you select 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 integers from 0 to 4294967295. – If you select Range in the Content Length Operator field, the Content Length Lower Value (Bytes) and the Content Length Higher Value (Bytes) fields appear: a. In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value (Bytes) field. b. In the Content Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value (Bytes) field.

Table 11-8 Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
Header	The name and value in an HTTP header are to be used for protocol inspection decisions. 1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header. 2. If you select 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. 3. 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 11-35 for a list of the supported characters that you can use in regular expressions.
Header Length	The length of the header in the HTTP message is to be used for protocol inspection decisions. 1. In the Header Length Type field, specify whether 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. 2. In the Header Length Operator field, select 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. 3. Enter values to apply for header length comparison: – If you select 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 integers from 0 to 255. – If you select Range in the Header Length Operator field, the Header Length Lower Value (Bytes) and the Header Length Higher Value (Bytes) fields appear: a. In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value (Bytes) field. b. In the Header 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 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 are to be used for protocol inspection decisions. In the Header MIME Type field, select the MIME message type to use for this match condition.

Table 11-8 Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
Port Misuse	The misuse of port 80 (or any other port running HTTP) is to be used for protocol inspection decisions. Select 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.
Request Method	The request method 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. 1. In the Request Method Type field, select 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. Depending on your selection, the Ext Request Method field or the RFC Request Method field appears. 2. In the Request Method field, select the specific request method to be used.
Transfer Encoding	An HTTP transfer-encoding type is to be 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, select 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.

Table 11-8 Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
URL	URL names are to be 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 is to be used for protocol inspection decisions. 1. In the URL Length Operator field, select 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. 2. Enter values to apply for URL length comparison: – If you select 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 select Range in the URL Length Operator field, the URL Length Lower Value (Bytes) and the URL Length Higher Value (Bytes) fields appear: a. 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. b. 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 Click:

- **Deploy Now** to deploy this configuration on the ACE.

  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.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Policy Maps, page 11-30
- Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 11-9

- Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 11-12
- Setting Match Conditions for Layer 7 Server Load Balancing Class Maps, page 11-14
- Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 11-21

Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the Layer 7 FTP command inspection 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer 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, select the FTP command to be inspected. Table 11-9 identifies the FTP commands that can be inspected.

Table 11-9 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 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

Setting Match Conditions for Generic Server Load Balancing Class Maps

Note Generic server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the generic 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer from 2 to 255.

Step 5 In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in Table 11-10.

Table 11-10 Generic Server Load Balancing Class Map Match Conditions

Match Condition	Description
Class Map	A class map is used to establish a match condition. In the Class Map field, select the class map to use for this match condition.
Layer 4 Payload	Generic data parsing is used to establish a match condition. 1. 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 11-35 for a list of the supported characters that you can use for matching string expressions. 2. 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 integers from 0 to 999.
Source Address	A source IP address is used to establish a match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

Setting Match Conditions for RADIUS Server Load Balancing Class Maps

Note RADIUS server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the RADIUS 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer from 2 to 255.

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

Table 11-11 RADIUS Server Load Balancing Class Map Match Conditions

Match Condition	Description
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 11-35 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 11-35 for a list of the supported characters that you can use for matching string expressions.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

Setting Match Conditions for RTSP Server Load Balancing Class Maps

Note RTSP server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the RTSP 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer from 2 to 255.

Step 5 In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in Table 11-12.

Table 11-12 RTSP Server Load Balancing Class Map Match Conditions

Match Condition	Description
Class Map	A class map is used to establish a match condition. In the Class Map field, select the class map to use for this match condition.
RTSP Header	The name and value in an RTSP header are used to establish a match condition. 1. 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, select 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, select the second radio button and select one of the RTSP headers from the list. 2. 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 11-35 for a list of the supported characters that you can use in regular expressions.

Table 11-12 RTSP Server Load Balancing Class Map Match Conditions (continued)

Match Condition	Description
RTSP URL	A URL or portion of a URL is used to establish a match condition. 1. 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 11-35 for a list of the supported characters that you can use in regular expressions. 2. 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	The source IP address is used to establish a match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

Setting Match Conditions for SIP Server Load Balancing Class Maps

Note SIP server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the SIP 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer from 2 to 255.

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

Table 11-13 SIP Server Load Balancing Class Map Match Conditions

Match Condition	Description
Class Map	A class map is used to establish a match condition. In the Class Map field, select the class map to use for this match condition.
SIP Header	A SIP header name and value are used to establish a match condition. 1. 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, select 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, select the second radio button and select one of the SIP headers from the list. 2. 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 11-35 for a list of the supported characters that you can use in regular expressions.
Source Address	The source IP address is used to establish a match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

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

Note SIP deep packet inspection class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 In the Class Maps table, select the SIP deep packet inspection 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 select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.

Step 4 In the Sequence Number field, enter an integer from 2 to 255.

Step 5 In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in Table 11-14.

Table 11-14 Layer 7 SIP Deep Packet Inspection Class Map Match Conditions

Match Condition	Description
Called Party	The destination or called party in the URI of the SIP To header 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 11-35 lists the supported characters that you can use for matching string expressions.
Calling Party	The source or calling party in the URI of the SIP From header 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 11-35 lists the supported characters that you can use for matching string expressions.

Table 11-14 Layer 7 SIP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
IM Subscriber	An IM (instant messaging) subscriber 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 11-35 lists the supported characters that you can use for matching string expressions.
Message Path	A message coming from or transiting through certain SIP proxy servers 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 11-35 lists the supported characters that you can use for matching string expressions.
SIP Content Length	The SIP message body length is used to establish a match condition. 1. In the Content Operator field, confirm that Greater Than is selected. 2. 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 integers from 0 to 65534 bytes.
SIP Content Type	The content type in the SIP message body 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 11-35 lists the supported characters that you can use for matching string expressions.
SIP Request Method	A SIP request method is used to establish a match condition. In the Request Method field, select the request method that is to be matched.
Third Party	A third party who is authorized to register other users on their behalf 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 11-35 lists the supported characters that you can use for matching string expressions.
URI Length	A SIP URI or user identifier is used to establish a match condition. 1. In the URI Type field, select 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. 2. In the URI Operator field, confirm that Greater Than is selected. 3. 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 Click:

- **Deploy Now** to deploy this configuration on the ACE and to 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.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

Configuring Virtual Context Policy Maps

Policy maps 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:

- 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:

- 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 view 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 11-15 lists the types of policy maps with brief descriptions and the ACE devices that support them.

Table 11-15 Policy Maps and ACE Device Support

		ACE Modules and Device			
Policy Map Type	**Description**	**ACE 1.0 Module**	**ACE 2.0 Module**	**ACE Appliance Running Image A1(8)**	**ACE Appliance Running Image A3(1.0)**
Layer 3/4 Management Traffic (First-Match)	Layer 3 and Layer 4 policy map for network management traffic received by the ACE	X	X	X	X
Layer 3/4 Network Traffic (First-Match)	Layer 3 and Layer 4 policy map for traffic passing through the ACE	X	X	X	X
Layer 7 Command Inspection - FTP (First-Match)	Layer 7 policy map for inspection of FTP commands	X	X	X	X
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Layer 7 policy map for inspection of HTTP packets	X	X	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	X
Layer 7 Server Load Balancing (First-Match)	Layer 7 policy map for HTTP server load balancing	X	X	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
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

Use this procedure to create a policy map for a virtual context.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 Click **Add** to add a new policy map, or select an existing policy map, then 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 Type, select the type of policy map to create. See Table 11-15 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 Click:

- **Deploy Now** to deploy this configuration on the ACE. To define rules and actions for the policy map, see Configuring Rules and Actions for Policy Maps, page 11-32.
- **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- **Next** to deploy your entries and to configure another policy map.

Related Topics

- Using Virtual Contexts, page 3-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Rules and Actions for Policy Maps, page 11-32

Configuring Rules and Actions for Policy Maps

Table 11-16 lists the policy maps and related topics for setting rules and actions.

Table 11-16 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 11-37
Layer 3/4 Network Traffic (First-Match)	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 11-38
Layer 7 Command Inspection - FTP (First-Match)	Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection, page 11-45
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 11-47
Layer 7 Deep Packet Inspection - SIP (All-Match)	Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 11-62
Layer 7 Deep Packet Inspection - Skinny	Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection, page 11-64
Layer 7 HTTP Optimization (First-Match)	Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 11-53
Layer 7 Server Load Balancing (First-Match)	Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 11-56
Server Load Balancing - Generic (First-Match)	Setting Policy Map Rules and Actions for Generic Server Load Balancing, page 11-33

Table 11-16 Topic Reference for Policy Map Rules and Actions

Policy Map Type	Topic for Setting Rules and Actions
Server Load Balancing - RADIUS (First-Match)	Setting Policy Map Rules and Actions for RADIUS Server Load Balancing, page 11-66
Server Load Balancing - RDP (First-Match)	Setting Policy Map Rules and Actions for RDP Server Load Balancing, page 11-68
Server Load Balancing - RTSP (First-Match)	Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 11-70
Server Load Balancing - SIP (First-Match)	Setting Policy Map Rules and Actions for SIP Server Load Balancing, page 11-73

Setting Policy Map Rules and Actions for Generic Server Load Balancing

Note Generic server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

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

Assumptions

- 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 Select **Config > Virtual Contexts** > ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the generic traffic 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-17.

Table 11-17 Generic Server Load Balancing Policy Map Rules

<table>
<tr><th>Option</th><th colspan="3">Description</th></tr>
<tr><td>Class Map</td><td colspan="3">A class map is used for this traffic policy.
1. 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 <b>match any</b> statement that enables it to match all traffic.
2. To use a previously created class map:
a. Clear the Use Class Default check box.
b. In the Class Map Name field, select the class map to be used.</td></tr>
<tr><td rowspan="4">Match Condition</td><td colspan="3">A match condition is used for this traffic policy.</td></tr>
<tr><td>Match Condition Name</td><td colspan="2">Enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</td></tr>
<tr><td rowspan="2">Match Condition Type</td><td>Layer 4 Payload</td><td>Layer 4 payload data is used for the network matching criteria.
1. 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 11-35 lists the supported characters that you can use for matching string expressions.
2. 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 integers from 0 to 999.</td></tr>
<tr><td>Source Address</td><td>A client source host IP address and subnet mask are used for the network traffic matching criteria.
1. In the Source IP Address field, enter the source IP address of the client in dotted-decimal notation.
2. In the Source Netmask select the subnet mask for the source IP address.</td></tr>
<tr><td>Insert Before</td><td colspan="3">1. 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.
2. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.</td></tr>
</table>

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

Note If you selected the Insert Before option described in Table 11-17 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add an entry or select an existing entry to modify, then 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 11-18.

Table 11-18 Generic Server Load Balancing Policy Map Actions

Action	Description
Drop	The ACE is to discard packets that match this policy map. In the Action Log field, specify whether 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	The ACE is to forward the traffic that match this policy map to its destination.
Reverse Sticky	This feature applies only to the ACE module software version 3.0(0)A2(1.1) or higher. 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, select an existing IP netmask sticky group that you want to associate with reverse IP stickiness.

Table 11-18 Generic Server Load Balancing Policy Map Actions (continued)

Action	Description
Server Farm	The ACE is to load balance client requests for content to a server farm. 1. In the Server Farm field, select the server farm for this policy map action. 2. In the Backup Server Farm field, select the backup server farm for this action. 3. Check the Sticky Enabled check box to indicate that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky. 4. 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. 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.
Sticky Group	Select the name of an existing sticky group that you want to associate with reverse stickiness.
Sticky Server Farm	The ACE is to load balance client requests for content to a sticky server farm. In the Sticky Group field, select the sticky server farm that is to be used for requests that match this policy map.
Set-IP-TOS	The ACE is to set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. Once 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 integers from 0 to 255.
Server Farm-NAT	The ACE is to apply dynamic NAT to traffic for this policy map. 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 integers from 1 to 2147483647. For information on configuring NAT pools, see Configuring VLAN Interface NAT Pools, page 9-10. 2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 1 to 4094. 3. In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.

Step 9 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

- Configuring Rules and Actions for Policy Maps, page 11-32

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

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

Assumptions

- 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 Select **Config > Virtual Contexts** > ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the Layer 3/Layer 4 management traffic 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

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

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

Step 6 To use a previously created class map for this rule:

a. Clear the Use Class Default check box.

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

c. In the Insert Before field, indicate 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.

d. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 7 Click:

- **Deploy Now** to deploy this configuration on the ACE. The Action table appears. To define actions for this rule, continue with Step 8.
- **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 8 In the Action table, click **Add** to add an action or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.

Step 9 In the Id field, 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 Click:

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

Related Topics

- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

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

Use this procedure to configure rules and actions for Layer 3/Layer 4 traffic other than network management traffic.

Assumptions

- 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the Layer 3/Layer 4 network traffic 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 select the rule you want to modify, then click **Edit**. The Rule configuration screen appears.

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

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

Step 6 To use a previously created class map for this rule:

a. Clear the Use Class Default check box.

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

c. In the Insert Before field, indicate 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.

d. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 7 Click:

- **Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action field appears. To configure actions for this rule, continue with Step 8.
- **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

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

Step 9 Click **Add** to add an action or select an existing action, then click **Edit** to modify it. The Action configuration screen 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, select the type of action to be taken for this rule, then configure the related attributes. See Table 11-19.

Table 11-19 Layer 3/Layer 4 Network Traffic Policy Map Actions

Action	Description/Steps
Appl-Parameter-DNS	A DNS parameter map containing DNS-related actions 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	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. A generic parameter map 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	An HTTP parameter map containing HTTP-related actions 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	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. An RTSP parameter map containing RTSP-related actions is to be implemented for this rule. In the Parameter Map field, specify the name of the RTSP parameter map to use.

Table 11-19 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
Appl-Parameter-SIP	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. A SIP parameter map containing SIP-related actions 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	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. A Skinny parameter map containing Skinny-related actions is to be implemented for this rule. In the Parameter Map field, specify the name of the Skinny parameter map to use.
Connection	A connection parameter map containing TCP/IP connection-related commands that pertain to normalization and termination is to be implemented for this rule. In the Connection Parameter Maps field, select the Connection parameter map that is to be used.
HTTP Optimize	This option appears for ACE appliances only. In the HTTP Optimization Policy field, select the HTTP optimization policy map to use.
Inspect	Application inspection is to be implemented for this rule. **1.** In the Inspect Type field, select the protocol that is to be inspected. **2.** Provide any protocol-specific information. Table 11-20 describes the available options for application inspection actions.

Table 11-19 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
NAT	The ACE is to implement network address translation (NAT) for this rule. **1.** In the NAT Mode field, select the type of NAT to be used: – Dynamic NAT—NAT is to translate local addresses to a pool of global addresses. Continue with Step 3. – Static NAT—NAT is to translate each local address to a fixed global address. Continue with Step 2. **2.** If you select Static NAT, do the following: **a.** 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). **b.** In the Static Mapped Netmask field, select the subnet mask to apply to the static mapped address. **c.** In the NAT Protocol field, select the protocol to use for NAT: - 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. **d.** In the Static Port field, enter the TCP or UDP port to use for static port redirection. Valid entries are integers from 0 to 65535. **e.** In the VLAN Id field, select the VLAN to use for NAT. **3.** If you select Dynamic NAT, 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 integers from 1 to 2147483647. See Configuring VLAN Interface NAT Pools, page 9-10. **b.** In the VLAN Id field, select 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	The ACE is to associate a Layer 7 server load-balancing policy map with this Layer 3/Layer 4 policy map. In the Policy Map field, select the Layer 7 policy map to associate with this Layer 3/Layer 4 policy map.
SSL-Proxy	The ACE is to use an SSL proxy server service to define the SSL parameters the ACE is to use during the handshake and subsequent SSL session. **1.** In the SSL Proxy field, select the SSL proxy server service to use in the handshake and subsequent SSL session when the ACE engages with an SSL client. **2.** 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 11-19 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
UDP-Fast-Age	This option appears for ACE 2.0 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	This option appears for ACE modules release only. The ACE is to advertise the IP address of a virtual server as the host route. **1.** In the Active field, click 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** Leave the Active field unchecked 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. **2.** If you click the Active field, in the Metric Distance field, enter the administrative distance to include in the routing table. Valid entries are integers from 1 to 254.
VIP-ICMP-Reply	A VIP is to send an ICMP ECHO-REPLY response to ICMP requests. **1.** In the Active field, click 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. **2.** In the Primary Inservice field, click 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	A VIP is to be enabled for server load-balancing operations.

Table 11-20 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. 1. For ACE 2.0 modules and the ACE 4710 A3(1.0) release only, in the Parameter Map field, specify a previously created parameter map used to define parameters for FTP inspection. 2. In the FTP Strict field, indicate whether 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. 3. If you select True, in the FTP Inspect Policy field, select 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. 1. In the HTTP Inspect Policy field, select 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. 2. In the URL Logging field, indicate whether 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 11-20 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 it can be inspected similarly to TCP and UDP traffic. In the ICMP Error field, indicate whether 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). For ACE 2.0 modules and the ACE 4710 A3(1.0) release only, in the Parameter Map field, select a previously defined parameter map used to define parameters for RTSP inspection.
SIP	SIP protocol inspection is 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. 1. For ACE 2.0 modules and the ACE 4710 A3(1.0) release only, in the Parameter Map field, specify a previously created parameter map used to define parameters for SIP inspection. 2. In the SIP Inspect Policy field, select 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 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. 1. For ACE 2.0 modules and the ACE 4710 A3(1.0) release only, in the Parameter Map field, specify a previously created connection parameter map used to define parameters for Skinny inspection. 2. In the Skinny Inspect Policy field, select 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 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

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

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.

Use this procedure to add rules and actions for Layer 7 FTP command inspection policy maps.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the Layer 7 FTP command inspection 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 select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-21.

Table 11-21 Layer 7 FTP Command Inspection Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: 1. 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. 2. To use a previously created class map: a. Clear the Use Class Default check box. b. In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: 1. 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. 2. In the Match Condition Type field, confirm that Request Method Name is selected. 3. In the Request Method Name field, select the FTP command to be inspected for this rule. Table 11-9 describes the FTP commands that can be inspected.
Insert Before	1. 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. 2. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 5 Click:

- **Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action table appears. Continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.

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

Note If you selected the Insert Before option described in Table 11-21 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it. The Action configuration screen appears.

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, 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 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30

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

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

Use this procedure to add rules and actions for Layer 7 HTTP deep packet inspection policy maps.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select 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 select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-22.

Table 11-22 Layer 7 HTTP Deep Packet Inspection Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: **1.** 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. **2.** To use a previously created class map: **a.** Clear the Use Class Default check box. **b.** In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: **1.** 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. **2.** In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 11-23 for information about these selections.
Insert Before	**1.** 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. **2.** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-23 Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions

Match Condition	Description
Content	Specific content contained within the HTTP entity-body is used for protocol inspection decisions. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. 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	The content parse length in an HTTP message is used for protocol inspection decisions. 1. In the Content Length Operator field, select the operand to be used to compare content length: – 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. 2. Enter values to apply for content length comparison: – If you select 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 integers from 0 to 4294967295. – If you select Range in the Content Length Operator field, the Content Length Lower Value (Bytes) and the Content Length Higher Value (Bytes) fields appear: **a.** In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value (Bytes) field. **b.** In the Content 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 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value (Bytes) field.
Content Type Verification	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 11-23 Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)

Match Condition	Description
Header	The name and value in an HTTP header are used for protocol inspection decisions. 1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header. 2. If you select 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. 3. 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 11-35 for a list of the supported characters that you can use in regular expressions.
Header Length	The length of the header in the HTTP message is used for protocol inspection decisions. 1. In the Header Length Type field, specify whether 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. 2. In the Header Length Operator field, select 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. 3. Enter values to apply for header length comparison: – If you select 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 integers from 0 to 255. – If you select Range in the Header Length Operator field, the Header Length Lower Value (Bytes) and the Header Length Higher Value (Bytes) fields appear: **a.** In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value (Bytes) field. **b.** In the Header 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 255. The number in this field must be greater than the number entered in the Header Length Lower Value (Bytes) field.

Table 11-23 Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)

Match Condition	Description
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types are used for protocol inspection decisions. In the Header MIME Type field, select the MIME message type to be used for this match condition.
Port Misuse	The misuse of port 80 (or any other port running HTTP) is used for protocol inspection decisions. In the Port Misuse field, select 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	The request method 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. 1. In the Request Method Type field, select 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. 2. In the Request Method field, select the specific request method to be used.
Strict HTTP	Internal compliance checks 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	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, select 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.

Table 11-23 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 is used for protocol inspection decisions. 1. In the URL Length Operator field, select 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. 2. Enter values to apply for URL length comparison: – If you select 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 select Range in the URL Length Operator field, the URL Length Lower Value (Bytes) and the URL Length Higher Value (Bytes) fields appear: **a.** 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. **b.** 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 5 Click:

- **Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action table appears. To define actions for this rule, continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected the Insert Before option described in Table 11-22 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add a new action, or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.

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, select 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 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 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization

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

Use this procedure to add rules and actions for Layer 7 HTTP optimization policy maps.

Assumptions

- An action list has been configured. See Configuring an HTTP Optimization Action List, page 12-3 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 11-6 for more information.

Procedure

Step 1 Select **Config** > **Virtual Contexts** > ***context*** > **Expert** > **Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the Layer 7 HTTP optimization 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 select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-24.

Table 11-24 Layer 7 HTTP Optimization Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: **1.** 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. **2.** To use a previously created class map: **a.** Clear the Use Class Default check box. **b.** In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: **1.** 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. **2.** In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 11-25 for information about these selections.
Insert Before	**1.** 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. **2.** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-25 Layer 7 HTTP Optimization Policy Map Match Conditions

Match Condition	Procedure
Cookie	An HTTP cookie is to be used to establish a match condition. 1. 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. 2. 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. 3. In the Secondary Cookie field, click the checkbox to ACE is to use either the cookie name or the cookie value to satisfy this match condition. Clear 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	An HTTP header is to be used to establish a match condition. 1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header. 2. If you select 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. 3. 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 11-35 for a list of the supported characters that you can use in regular expressions.
HTTP URL	A portion of an HTTP URL is to be used to establish a match condition. 1. 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. 2. 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 Click:

- **Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action table appears. To define actions for this rule, continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected the Insert Before option described in Table 11-24 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add a new action, or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.

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, confirm that Action List is selected.

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

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

Step 11 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

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

Use this procedure to set rules and actions for Layer 7 server load-balancing policy maps.

Assumptions

- 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 Select **Config > Virtual Contexts >** ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select 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 select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-26.

Table 11-26 Layer 7 Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: **1.** 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. **2.** To use a previously created class map: **a.** Clear the Use Class Default check box. **b.** In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: **1.** 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. **2.** In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 11-27 for information about these selections.
Insert Before	**1.** 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. **2.** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-27 Layer 7 Server Load Balancing Policy Map Match Conditions

Match Condition	Description
HTTP Content	This option appears for ACE 2.0 modules only. Specific content contained within the HTTP entity-body is used to establish a match condition. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. 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 integers from 1 to 255.
HTTP Cookie	HTTP cookies are to be used for this match condition. 1. 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. 2. 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 11-35 lists the supported characters that you can use for matching string expressions.
HTTP Header	The HTTP header and a corresponding value are to be used for this match condition. 1. 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, select 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 select an HTTP header from the list. 2. 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 11-35 for a list of the supported characters that you can use in regular expressions.

Table 11-27 Layer 7 Server Load Balancing Policy Map Match Conditions (continued)

Match Condition	Description
HTTP URL	This rule is to perform regular expression matching against the received packet data from a particular connection based on the HTTP URL string. 1. 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 11-35 for a list of the supported characters that you can use in regular expressions. 2. 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	A client source IP address is used to establish match conditions. 1. 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). 2. 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 Click:

- **Deploy Now** to deploy the configuration on the ACE. The screen refreshes and the Action table appears. To define the actions for this rule, continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected the Insert Before option described in Table 11-26 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add a new action, or select an existing action, then 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, select the action to be taken and configure any action-specific attributes as described in Table 11-28.

Table 11-28 Layer 7 Server Load Balancing Policy Map Actions

Action	Description
Action	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. The ACE is to implement an action list for the rule. In the Action List field, select an action list to associate with this rule.
Compress	**Note** This option appears for ACE appliances. 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	The ACE is to discard packets that match the rule. In the Action Log field, specify whether 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	The ACE is to forward requests that match this policy map without load balancing the requests.
Insert-HTTP	The ACE is 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. 1. 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. 2. 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 11-35 for a list of the supported characters that you can use in regular expressions.
Reverse Sticky	This feature applies only to the ACE module software version 3.0(0)A2(1.1) or higher. 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, select the name of a an existing IP netmask sticky group that you want to associate with reverse IP stickiness.

Table 11-28 Layer 7 Server Load Balancing Policy Map Actions (continued)

Action	Description
Server Farm	The ACE is to load balance client requests for content to a server farm. 1. In the Server Farm field, select the server farm to which requests for content are to be sent. 2. In the Backup Server Farm field, select the backup server farm to which requests for content are to be sent. Select **N/A** to indicate that no backup server farm is to be used. 3. Select 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. 4. Select 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	This option appears for ACE 2.0 modules only. The ACE is to apply dynamic NAT to traffic for this policy map. 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 integers from 1 to 2147483647. For information on configuring NAT pools, see Configuring VLAN Interface NAT Pools, page 9-10. 2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 1 to 4094. 3. In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.
Set IP-TOS	The ACE is to set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. Once 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 integers from 0 to 255.
SSL-Proxy	The ACE is to use an SSL proxy client service to define the SSL parameters the ACE is to use during the handshake and subsequent SSL session. 1. In the SSL Proxy field, select the SSL proxy service to be used for this action. 2. 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	Requests matching this policy map be load balanced to a sticky server farm. In the Sticky Group field, select the sticky server farm that is to be used for requests that match this policy map.

Step 9 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

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

Note SIP deep packet inspection policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for a SIP deep packet inspection policy map.

Assumptions

- 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 Select **Config > Virtual Contexts** **>** ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the SIP deep packet inspection 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-29.

Table 11-29 Layer 7 SIP Deep Packet Inspection Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: **1.** 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. **2.** To use a previously created class map: **a.** Clear the Use Class Default check box. **b.** In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: **1.** 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. **2.** In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in Table 4-10.
Insert Before	**1.** 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. **2.** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to add another rule.

Note If you selected the Insert Before option described in Table 11-29 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add an entry or select an existing entry to modify, then 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, select 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 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

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

Note Skinny deep packet inspection policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for a Skinny Client Control Protocol (SCCP) deep packet inspection policy map.

Assumptions

- 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 Select **Config > Virtual Contexts** > *context* > **Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the Skinny deep packet inspection 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Type field, 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, indicate whether 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 integers from 0 to 65535.

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

  a. In the Message ID Low Range Value field, enter the lowest numerical identifier of a range of SCCP messages. Valid entries are integers 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, indicate 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.

Step 9 If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 10 Click:

- **Deploy Now** to deploy the configuration on the ACE. The screen refreshes and the Action table appears. To define the actions for this rule, continue with Step 11.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 11 In Action table, click **Add** to add a new action, or select an existing action, then click **Edit** to modify it. The Action configuration screen 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 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

Setting Policy Map Rules and Actions for RADIUS Server Load Balancing

Note RADIUS server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

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

Assumptions

- 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 Select **Config > Virtual Contexts** **>** ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the RADIUS server 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-30.

Table 11-30 RADIUS Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: **1.** 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. **2.** To use a previously created class map: **a.** Clear the Use Class Default check box. **b.** In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: **1.** 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. **2.** In the Match Condition Type field, select 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 11-35 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 11-35 for a list of the supported characters that you can use for matching string expressions.
Insert Before	**1.** 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. **2.** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. To enter actions for this rule, continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected the Insert Before option described in Table 11-30 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add an entry or select an existing entry to modify, then 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 11-18.

Step 9 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

Setting Policy Map Rules and Actions for RDP Server Load Balancing

Note RDP server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

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

Assumptions

- 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 Select **Config > Virtual Contexts** > *context* > **Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the RDP server 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

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

Step 5 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.

Step 6 To use a previously created class map:

a. Clear the Use Class Default check box.

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

Step 7 In the Insert Before field, 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.

  If you select True in the Insert Before field, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 8 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. To enter actions for this rule, continue with Step 9.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

Note If you selected the Insert Before option in Step 7 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 9 In the Action table, click **Add** to add an entry or select an existing entry to modify, then click **Edit**.

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

Step 11 In the Action Type field, configure actions for this rule using the information in Table 11-18.

Step 12 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

Setting Policy Map Rules and Actions for RTSP Server Load Balancing

Note RTSP server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

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

Assumptions

- 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 Select **Config > Virtual Contexts** > ***context*** **> Expert > Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the RTSP server 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-31.

Table 11-31 RTSP Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: 1. 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. 2. To use a previously created class map: a. Clear the Use Class Default check box. b. In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: 1. 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. 2. In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in Table 11-32.
Insert Before	1. 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. 2. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-32 RTSP Policy Map Match Conditions

Match Condition	Description
RTSP Header	RTSP header information is used for matching criteria. **1.** 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, select 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 select an RTSP header from the list. **2.** 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 11-35 for a list of the supported characters that you can use in regular expressions.
RTSP URL	A URL or portion of a URL is used for match criteria. **1.** 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 11-35 for a list of the supported characters that you can use in regular expressions. **2.** 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	The source IP address is used for match criteria. **1.** In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. **2.** In the Source Netmask field, select the subnet mask for the source IP address.

Step 5 In the Insert Before field, 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.

  If you select True in the Insert Before field, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 6 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with Step 7.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to add another rule.

Note If you selected the Insert Before option in Table 11-32 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 7 In the Action table, click **Add** to add an entry or select an existing entry to modify, then 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 11-18.

Step 10 Click:

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

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

Setting Policy Map Rules and Actions for SIP Server Load Balancing

Note SIP server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

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

Assumptions

- 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 Select **Config** > **Virtual Contexts** > ***context*** > **Expert** > **Policy Maps**. The Policy Maps table appears.

Step 2 In the Policy Maps table, select the SIP server 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 select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 11-33.

Table 11-33 SIP Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: **1.** 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. **2.** To use a previously created class map: **a.** Clear the Use Class Default check box. **b.** In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: **1.** 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. **2.** In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in Table 11-34.
Insert Before	**1.** 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. **2.** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-34 SIP Server Load Balancing Policy Map Match Conditions

Match Condition	Description
SIP Header	SIP header information is used for matching criteria. 1. 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, select 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 select an SIP header from the list. 2. 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 11-35 for a list of the supported characters that you can use in regular expressions.
Source Address	The source IP address is used for match criteria. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears so you can enter actions for this rule. Continue with Step 6.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to add another rule.

Step 6 In the Action table, click **Add** to add an entry or select an existing entry to modify, then 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 11-18.

Step 9 Click:

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

Note If you selected the Insert Before option in Table 11-33 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, select the newly added rule.

When the screen refreshes, an empty action list appears.

Related Topics

- Configuring Traffic Policies, page 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

Special Characters for Matching String Expressions

Table 11-35 identifies the special characters that can be used in matching string expressions.

Table 11-35 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 11-1
- Configuring Virtual Context Class Maps, page 11-6
- Configuring Virtual Context Policy Maps, page 11-30
- Configuring Rules and Actions for Policy Maps, page 11-32

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 11-53).
- 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. 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 11-56).

Table 11-36 lists the action lists that you can configure using the ACE.

Table 11-36 Action Lists

Action List	Topic
Optimization Action List	Configuring an HTTP Optimization Action List, page 12-3
HTTP Header Modify Action List	Configuring an HTTP Header Modify Action List, page 11-78

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 procedure includes the following topics:

Configuring HTTP Header Insertion, Deletion, and Rewrite, page 11-78

Configuring SSL URL Rewrite, page 11-81

Configuring HTTP Header Insertion, Deletion, and Rewrite

Use this procedure to configure an HTTP header modify action list that inserts, rewrites, or deletes HTTP headers.

Procedure

Step 1 Select the item to configure:

- To configure a virtual context, select **Config > Devices >** ***context*** **> Expert > HTTP Header Modify Action List**. The HTTP Header Modify Action Lists table appears.
- To configure a configuration building block, select **Config > Global > All Building Blocks >** *building_block* **> Expert > HTTP Header Modify Action List**.

Step 2 Click **Add** to add a new HTTP header modify action list, or select an existing action list, then click **Edit** to modify it.

Step 3 For a new action list, in the Action List Name field enter a unique name for the HTTP header modify action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.

Step 4 Select the Header Action tab. The Header Action table appears.

Step 5 Click **Add** to add a new entry to the Header Action table. The Header Action configuration screen appears. Enter the required information as shown in Table 11-37.

Table 11-37 Header Action Configuration Screen Fields

Header Action Field	Description / Action
Operator	Select the HTTP header modify action the ACE is to take in an HTTP request from a client, a response from a server, or both: • 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 11-37 Header Action Configuration Screen Fields (continued)

Header Action Field	Description / Action
Direction	Select the HTTP header modify action the ACE is to take with respect to the selected operator (Insert, Delete, or Rewrite): **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	Specifies the 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 11-35 for a list of the supported characters that you can use in regular expressions.
Replace	Specifies the 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 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **OK** to save your entries. This option appears for configuration building blocks.
- **Cancel** to exit this procedure without saving your entries.
- **Next** to save your entries.

Related Topics

- Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 11-56, Table 11-28

Configuring 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.

Use this procedure to configure an HTTP header modify action list that performs SSL URL rewrite.

Procedure

Step 1 Select the item to configure:

- To configure a virtual context, select **Config > Devices >** ***context*** **> Expert > HTTP Header Modify Action List**. The HTTP Header Modify Action Lists table appears.
- To configure a configuration building block, select **Config > Global > All Building Blocks >** *building_block* **> Expert > HTTP Header Modify Action List**.

Step 2 Click **Add** to add a new HTTP header modify action list, or select an existing action liClick **Add** to add a new HTTP header modify action list, or select an existing action list, then click **Edit** to modify it.

Step 3 For a new action list, in the Action List Name field enter a unique name for the HTTP header modify action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.

Step 4 Select the SSL Action tab. The SSL Action table appears.

Step 5 Click **Add** to add a new entry to the SSL Action table. The SSL Action configuration screen appears. Enter the required information as shown in Table 11-38.

Table 11-38 SSL Action Configuration Screen Fields

Header Action Field	Description / Action
URL Expression	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 11-78. 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 11-35 for a list of the supported characters that you can use in regular expressions.
SSL Port	Specifies the SSL port number from which the ACE translates a clear port number before sending the server redirect response to the client. Enter an integer from 1 to 65535. The default is 443.
Clear Port	Specifies the clear port number to which the ACE translates the SSL port number before sending a server redirect response to the client. Enter an integer from 1 to 65535. The default is 80.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **OK** to save your entries. This option appears for configuration building blocks.
- **Cancel** to exit this procedure without saving your entries.
- **Next** to save your entries.

Related Topics

- Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 11-56, Table 11-28