CHAPTER 12

Configuring Traffic Policies

This chapter describes how to configure traffic policies. ACE Appliance Device 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 appliance. You create traffic policies and attach these policies to one or more VLAN interfaces associated with the ACE appliance to apply feature-specific actions to the matching traffic. The ACE appliance uses the individual traffic policies to implement functions such as:

- Remote access using Secure Shell (SSH) or Telnet
- Server load balancing
- Network Address Translation (NAT)
- Optimization of HTTP traffic
- HTTP deep packet inspection, application protocol inspection, FTP command inspection, Skinny Client Control Protocol (SCCP) deep packet inspection, or SIP inspection
- Secure Socket Layer (SSL) security services between a Web browser (the client) and the HTTP connection (the server)
- TCP termination, normalization, and reuse
- IP normalization and fragment reassembly

Note When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

Related Topics

- Class Map and Policy Map Overview, page 12-2
- Configuring Virtual Context Class Maps, page 12-8
- Setting Match Conditions for Class Maps, page 12-10
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36
- Configuring Actions Lists, page 12-90

Class Map and Policy Map Overview

You classify inbound network traffic destined to, or passing through, the ACE appliance 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, IP protocol and port, or management protocol
- Layer 7 protocol information—HTTP cookie, HTTP URL, HTTP header, HTTP content, FTP request commands, RADIUS, RDP, RTSP, Skinny, or SIP

Table 12-1 lists the available policies for the ACE.

Table 12-1 Traffic Policies

Policy Map	Description
Layer 3/4 Management Traffic (First-Match)	Layer 3 and Layer 4 policy map for network management traffic received by the ACE
Layer 3/4 Network Traffic (First-Match)	Layer 3 and Layer 4 policy map for traffic passing through the ACE
Layer 7 Command Inspection - FTP (First-Match)	Layer 7 policy map for inspection of FTP commands
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Layer 7 policy map for inspection of HTTP packets
Layer 7 Deep Packet Inspection - SIP (All-Match)	Layer 7 policy map for inspection of SIP packets
Layer 7 Deep Packet Inspection - Skinny	Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)
Layer 7 HTTP Optimization (First-Match)	Layer 7 policy map for optimizing HTTP traffic
Layer 7 Server Load Balancing (First-Match)	Layer 7 policy map for HTTP server load balancing
Server Load Balancing - Generic (First-Match)	Generic Layer 7 policy map for server load balancing
Server Load Balancing - HTTPS[1] (First-Match)	Layer 7 policy map for HTTPS server load balancing
Server Load Balancing - RADIUS (First-Match)	Layer 7 policy map for RADIUS server load balancing
Server Load Balancing - RDP (First-Match)	Layer 7 policy map for RDP server load balancing
Server Load Balancing - RTSP (First-Match)	Layer 7 policy map for RTSP server load balancing

1. This option is not available for ACE NPE software image.

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 appliance.

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

- Class Maps, page 12-3
- Policy Maps, page 12-4
- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5
- Application Protocol Inspection Overview, page 12-5
- Configuring Virtual Context Global Traffic Policies, page 4-28

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 appliance.

- Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE appliance or network management traffic that can be received by the ACE appliance.
- Layer 7 protocol-specific classes identify server load balancing based on HTTP traffic, deep inspection of HTTP traffic, or the inspection of FTP commands by the ACE appliance.

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 appliance evaluates match conditions when you specify more than one match statement in a traffic class (match-any, match-all)

The ACE supports a system-wide maximum of 8192 class maps.

The individual match conditions specify the criteria for classifying Layer 3 and Layer 4 network traffic as well as the Layer 7 HTTP server load balancing and application protocol-specific fields. The ACE appliance evaluates the packets to determine whether they match the specified criteria. If a statement matches, the ACE appliance 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 appliance allows you to configure two Layer 7 HTTP load-balancing class maps in a nested traffic class configuration to create a single traffic class. You can perform Layer 7 class map nesting to achieve complex logical expressions. The ACE appliance 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 12-2
- Policy Maps, page 12-4
- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5

- Application Protocol Inspection Overview, page 12-5
- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8

Policy Maps

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

- Policy map name
- Previously created traffic class map or, optionally, the 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 appliance

The ACE appliance supports a system-wide maximum of 4096 policy maps.

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 appliance 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 appliance supports flexible class map ordering within a policy map. The ACE appliance 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 appliance. 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 appliance 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 appliance 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 12-2
- Policy Maps, page 12-4

- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5
- Application Protocol Inspection Overview, page 12-5
- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Policy Maps, page 12-34

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 received by the ACE appliance 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 appliance 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 8-1 for a list of available ACE appliance parameter maps.

Related Topics

- Configuring Parameter Maps, page 8-1
- Class Map and Policy Map Overview, page 12-2
- Class Maps, page 12-3
- Policy Maps, page 12-4
- Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5
- Application Protocol Inspection Overview, page 12-5

Application 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.

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

You can configure the ACE to perform application protocol inspection, sometimes referred to as an application protocol “fixup” for applications that do the following:

- Embed IP addressing information in the data packet including the data payload.
- Open secondary channels on dynamically assigned ports.

You may require the ACE to perform application inspection of Domain Name System (DNS), FTP (File Transfer Protocol), H.323, HTTP, Internet Control Message Protocol (ICMP), Internet Locator Service (ILS), Real-Time Streaming Protocol (RTSP), Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP) as a first step before passing the packets to the destination server. For HTTP, the ACE performs deep packet inspection to statefully monitor the HTTP protocol and permit or deny

traffic based on user-defined traffic policies. HTTP deep packet inspection focuses mainly on HTTP attributes such as the HTTP header, the URL, and the payload. For FTP, the ACE performs FTP command inspection for FTP sessions, allowing you to restrict specific commands by the ACE.

Application inspection helps you to identify the location of the embedded IP addressing information in the TCP or UDP flow. This inspection allows the ACE to translate embedded IP addresses and to update any checksum or other fields that are affected by the translation.

Translating IP addresses embedded in the payload of protocols is especially important for NAT (explicitly configured by the user) and server load balancing (an implicit NAT).

Application inspection also monitors TCP or UDP sessions to determine the port numbers for secondary channels. Some protocols open secondary TCP or UDP ports to improve performance. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application protocol inspection function monitors these sessions, identifies the dynamic port assignments, and permits data exchange on these ports for the duration of the session.

Table 12-2 describes the application inspection protocols supported by the ACE, the default TCP or UDP protocol and port, and whether the protocol is compatible with Network Address Translation (NAT) and Port Address Translation (PAT).

Table 12-2 Application Inspection Support

Application Protocol	Transport Protocol	Port	NAT/PAT Support	Enabled by Default	Standards [1]	Comments/Limitations
DNS	UDP	Src—Any Dest—53	NAT	No	RFC 1123	Inspects DNS packets destined to port 53. You can specify the maximum length of the DNS packet to be inspected.
FTP	TCP	Src—Any Dest—21	Both	No	RFC 959	Inspects FTP packets, translates address and port embedded in the payload, and opens up a secondary channel for data.
FTP strict	TCP	Src—Any Dest—21	Both	No	RFC 959	The FTP Strict field allows the ACE appliance to track each FTP command and response sequence, and also prevents an FTP client from determining valid usernames that are supported on an FTP server.
HTTP	TCP	Src—Any Dest—80	Both	No	RFC 2616	Inspects HTTP packets.
ICMP	ICMP	Src—N/A Dest—N/A	Both	No	—	Allows ICMP traffic to have a “session” so that it can be inspected similarly to TCP and UDP traffic.

Table 12-2 Application Inspection Support (continued)

Application Protocol	Transport Protocol	Port	NAT/PAT Support	Enabled by Default	Standards [1]	Comments/Limitations
ICMP error	ICMP	Src—N/A Dest—N/A	NAT	No	—	The ICMP Error field supports NAT of ICMP error messages. When you enable ICMP error inspection, the ACE appliance creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The ACE appliance overwrites the packet with the translated IP addresses.
ILS	TCP	Src—Any Dest—389	NAT	No	RFC 2251 (LDAPv3) Includes support for RFC 1777 (LDAPv2)	Referral requests and responses are not supported. Users in multiple directories are not unified. Single users having multiple identities in multiple directories cannot be recognized by NAT.
RTSP	TCP	Src—Any Dest—554	NAT	No	RFC 2326, RFC 2327, RFC 1889	Inspects RTSP packets and translates the payload according to NAT rules. The ACE opens up the secondary channels for audio and video. Not all the RTSP methods (packet types) specified in the RFC are supported.
SCCP	TCP	Src—Any Dest—2000	NAT	No	—	The ACE does not support PAT with SCCP.
SIP	TCP and UDP	Src—Any Dest—5060	NAT	No	RFC 2543, RFC 3261, RFC 3265, RFC 3428	The ACE does not support PAT with SIP.

1. The ACE is in compliance with these standards, but it does not enforce compliance on packets being inspected. For example, FTP commands are supposed to be in a particular order, but the ACE does not enforce the order.

For background information about application protocol inspection as performed by the ACE appliance, see the *Security Guide, Cisco ACE Application Control Engine*.

Related Topics

- Configuring Virtual Context Policy Maps, page 12-34
- Setting Match Conditions for Class Maps, page 12-10
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

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 appliance.

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

A traffic class contains:

- A class map name
- One or more match commands that define the match criteria for the class map
- Instructions on how the ACE appliance evaluates match commands when there is more than one match command in a traffic class

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, and then click **Delete**. The selected class maps are removed.

Procedure

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

Step 2 Click **Add** to add a new class map, or select an existing class map, and 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 (Table 12-3).

Table 12-3 Class Maps Types

Class Map	Related Topic
Layer 3/4 Management Traffic	Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14
Layer 3/4 Network Traffic	Setting Match Conditions for Class Maps, page 12-10
Layer 7 Command Inspection - FTP	Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 12-30
Layer 7 Deep Packet Inspection - HTTP	Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps, page 12-25
Layer 7 Deep Packet Inspection - SIP	Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps, page 12-31
Layer 7 Server Load Balancing	Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16
Server Load Balancing - Generic	Setting Match Conditions for Generic Server Load Balancing Class Maps, page 12-19
Server Load Balancing - RADIUS	Setting Match Conditions for RADIUS Server Load Balancing Class Maps, page 12-20
Server Load Balancing - RTSP	Setting Match Conditions for RTSP Server Load Balancing Class Maps, page 12-21
Server Load Balancing - SIP	Setting Match Conditions for SIP Server Load Balancing Class Maps, page 12-23

Step 5 For all selections except Layer 7 Command Inspection - FTP, in the Match Type field, select the method the ACE appliance is to use to evaluate multiple match statements when multiple match conditions exist in the class map:

- Match-any—Indicates that the class map is a match if at least one of the match conditions listed in the class map is satisfied.
- Match-all—Indicates that the class map is a match only if all match conditions listed in the class map are satisfied.

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

Step 7 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to configure match conditions for this class map. See Setting Match Conditions for Class Maps, page 12-10 for more information.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Class Maps table.
- Click **Next** to save your entries and to configure another class map.

Related Topics

- Configuring Virtual Contexts, page 4-1
- Deleting Class Maps, page 12-10
- Setting Match Conditions for Class Maps, page 12-10

- Configuring Virtual Context Policy Maps, page 12-34

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 Choose **Config > Virtual Contexts >** ***context*** **> Expert > Class Maps**. The Class Maps table appears.

Step 2 Select the class maps you want to delete, and then click **Delete**.

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, and then click **Delete**. The Class Maps table refreshes and the deleted class maps no longer appear.

Related Topics

- Class Map and Policy Map Overview, page 12-2
- Configuring Virtual Context Class Maps, page 12-8

Setting Match Conditions for Class Maps

Table 12-4 lists the class maps available for the ACE and provides links to topics for setting match conditions:

Table 12-4 Class Maps and Match Conditions

Class Map	Related Topic
Layer 3/4 Management Traffic	Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14
Layer 3/4 Network Traffic	Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 12-11
Layer 7 Command Inspection - FTP	Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 12-30
Layer 7 Deep Packet Inspection - HTTP	Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps, page 12-25
Layer 7 Deep Packet Inspection - SIP	Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps, page 12-31
Layer 7 Server Load Balancing	Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16

Table 12-4 Class Maps and Match Conditions (continued)

Class Map	Related Topic
Server Load Balancing - Generic	Setting Match Conditions for Generic Server Load Balancing Class Maps, page 12-19
Server Load Balancing - RADIUS	Setting Match Conditions for RADIUS Server Load Balancing Class Maps, page 12-20
Server Load Balancing - RTSP	Setting Match Conditions for RTSP Server Load Balancing Class Maps, page 12-21
Server Load Balancing - SIP	Setting Match Conditions for SIP Server Load Balancing Class Maps, page 12-23

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 appliance.

Assumption

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

Procedure

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

Step 2 In the Class Maps table, select the Layer 3/4 network traffic class map you want to set match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.

Step 3 In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and 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 be used for this class map and configure any match-specific attributes as described in Table 12-5.

Table 12-5 Layer 3/Layer 4 Network Traffic Class Map Match Condition Attributes

Match Condition Type	Description
Access List	Indicates that an access list is the match type for this match condition. In the Extended ACL field, select the ACL to use as the match condition.
Any	Indicates that any Layer 3 or Layer 4 traffic passing through the ACE appliance meets the match condition.
Anyv6	This option appears for Device Manager software Version A5(1.2) and later only. Any Layer 3 or Layer 4 IPv6 traffic passing through the ACE meets the match condition.

Table 12-5 Layer 3/Layer 4 Network Traffic Class Map Match Condition Attributes (continued)

Match Condition Type	Description
Destination Address	Indicates that a destination address is the match type for this match condition. **1.** For the IP Address Type, select either IPv4 or IPv6 for the address type. **2.** In the Destination Address field, enter the destination IP address for this match condition in the format based on the address type (IPv4 or IPv6). **3.** For an IPv4 destination address, in the Destination Netmask field, select the subnet mask of the IP address. For an IPv6 destination address, in the Destination Prefix-length field, enter the prefix length for the address.
Port	Indicates that 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 be matched. **2.** In the Port Operator field, select the match criteria for the port: – Any—Indicates that any port using the selected protocol meets the match condition. – Equal To—Indicates that 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 appliance is to include all ports. – Range—Indicates that 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 appliance is to include all ports.
Portv6	This option appears for Device Manager software Version A5(1.2) and later only. UDP or TCP port or range of ports for IPv6 traffic that is the match type for this match condition. For port configuration information, see Port.

Table 12-5 Layer 3/Layer 4 Network Traffic Class Map Match Condition Attributes (continued)

Match Condition Type	Description
Source Address	Indicates that a source IP address is the match type for this match condition. 1. For the IP Address Type, select either IPv4 or IPv6 for the address type. 2. In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6). 3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.
Virtual Address	Indicates that a virtual IP address is the match type for this match condition. 1. For the IP Address Type, select either IPv4 or IPv6 for the address type. 2. In the Virtual Address field, enter the virtual IP address for this match condition in the format based on the address type (IPv4 or IPv6). 3. For an IPv4 virtual address, in the Virtual Netmask field, select the subnet mask of the IP address. For an IPv6 virtual address, in the Virtual Prefix-length field, enter the prefix length for the address. 4. 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 4-18. Depending on the protocol that you select, 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—Indicates that any port using the selected protocol meets the match condition. – Equal To—Indicates that 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 appliance is to include all ports. – Range—Indicates that 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 appliance 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 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.

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

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14
- Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Virtual Context Class Maps, page 12-8

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 appliance.

Assumption

You have configured a network management class map and want to establish the match conditions.

Procedure

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

Step 2 In the Class Maps table, select the Layer 3/Layer 4 management class map you want to set match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.

Step 3 In the Match Condition table, click **Add** to add match criteria, or select the match conditions you want to modify, and then click **Edit**. The Match Condition configuration screen appears.

Step 4 Enter the match conditions (see Table 12-6).

Table 12-6 Management 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	Select **Management** to confirm that this is for Layer 3/Layer 4 management traffic. **Note** To change the type of match condition, you must delete the class map and add it again with the correct match type.
Management Protocol Type	This field identifies the network management protocols that can be received by the ACE appliance. Select the allowed protocol for this match condition: • HTTP—Specifies the Hypertext Transfer Protocol (HTTP). • HTTPS—Specifies the Hypertext Transfer Protocol Secure (HTTPS) for connectivity with the ACE Appliance Device Manager GUI on the ACE appliance. Communication is performed using port 443. • ICMP—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping. • ICMPv6—Specifies the Internet Control Message Protocol version 6 (ICMPv6). • KALAP UDP—Specifies the KeepAlive Appliance Protocol over UDP. • SNMP—Specifies the Simple Network Management Protocol (SNMP). • SSH—Specifies a Secure Shell (SSH) connection to the ACE appliance. • TELNET—Specifies a Telnet connection to the ACE appliance. • XML-HTTPS—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS). Communication is performed using port 10443.
Traffic Type	Select the type of traffic: • Any—Indicates that any client source IP address meets the match condition. • Source Address—Indicates that 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. For ICMPv6, enter a complete IPv6 address.
Source Netmask	This field appears if Source Address is selected for Traffic Type. Select the subnet mask for the source IP address.
Source Prefix-length	This field appears if ICMPv6 is selected for the Management Protocol Type and Source Address is selected for Traffic Type. Enter the prefix length for the source IPv6 address.

Step 5 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.

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

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Real Servers, page 6-5
- Configuring Server Farms, page 6-18
- Configuring Sticky Groups, page 7-11

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 Choose **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. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.

Step 3 In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and 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 12-7.

Table 12-7 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	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	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 Matching check box, do one of the following: – Clear the check box to indicate that the cookie being defined is a primary cookie. – Check the check box to indicate that the cookie being defined is a secondary cookie. You can specify the delimiters for cookies in a URL string by using an HTTP parameter map (see the "Configuring HTTP Parameter Maps" section on page 8-2).
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, and 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, and 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 12-33 for a list of the supported characters that you can use in regular expressions.

Table 12-7 Layer 7 Server Load Balancing Class Map Match Conditions (continued)

Match Condition	Description
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. For the IP Address Type, select either IPv4 or IPv6 for the address type. 2. In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6). 3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.

Step 6 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.

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

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

Related Topics

- Using Virtual Contexts, page 4-2
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34

Setting Match Conditions for Generic Server Load Balancing Class Maps

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 Choose **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, and 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 12-8.

Table 12-8 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 12-33 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. For the IP Address Type, select either IPv4 or IPv6 for the address type. 2. In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6). 3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.

Step 6 Do the following:

- 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.

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

Related Topics

- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34

Setting Match Conditions for RADIUS Server Load Balancing Class Maps

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 Choose **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, and 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 12-9.

Table 12-9 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 12-33 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 12-33 for a list of the supported characters that you can use for matching string expressions.

Step 6 Do the following:

- 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.

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

Related Topics

- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34

Setting Match Conditions for RTSP Server Load Balancing Class Maps

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 Choose **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, and 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 12-10.

Table 12-10 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 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 12-33 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 to establish a match condition. 1. In the URL Expression 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 12-33 for a list of the supported characters that you can use in regular expressions. 2. In the Method Expression 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 Do the following:

- 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.

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

Related Topics

- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34

Setting Match Conditions for SIP Server Load Balancing Class Maps

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 Choose **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, and 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 12-11.

Table 12-11 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 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 12-33 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. For the IP Address Type, select either IPv4 or IPv6 for the address type. 2. In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6). 3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.

Step 6 Do the following:

- 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.

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

Related Topics

- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34

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

The ACE Appliance Device Manager allows you to create Layer 7 class maps and policy maps to be used for HTTP deep packet inspection by the ACE appliance. When these features are configured, the ACE appliance 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 ACE appliances:

- 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 deep packet inspection class map and want to establish match conditions.

Procedure

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

Step 2 In the Class Maps table, select the Layer 7 HTTP deep packet inspection class map you want to set match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.

Step 3 In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and 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 12-12.

Table 12-12 HTTP Protocol Inspection Match Condition Types

Match Condition Type	Description
Content	Specific content contained within the HTTP entity-body is to be used for application 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 application inspection decisions. **1.** In the Content Length Operator field, select the operand to be used to compare content length: – Equal To—Indicates that the content length must equal the number in the Content Length Value (Bytes) field. – Greater Than—Indicates that the content length must be greater than the number in the Content Length Value (Bytes) field. – Less Than—Indicates that the content length must be less than the number in the Content Length Value (Bytes) field. – Range—Indicates that 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: 1. In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are 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. 2. In the Content Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are 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 12-12 HTTP Protocol Inspection Match Condition Types (continued)

Match Condition Type	Description
Header	The name and value in an HTTP header are to be used for application 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 be matched. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **3.** In the Header Value 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 appliance 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 12-33 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 application inspection decisions. **1.** In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: – Request—Indicates that HTTP header request messages are to be checked for header length. – Response—Indicates that 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—Indicates that the header length must equal the number in the Header Length Value (Bytes) field. – Greater Than—Indicates that the header length must be greater than the number in the Header Length Value (Bytes) field. – Less Than—Indicates that the header length must be less than the number in the Header Length Value (Bytes) field. – Range—Indicates that 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: 1. In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are 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. 2. In the Header Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are 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 12-12 HTTP Protocol Inspection Match Condition Types (continued)

Match Condition Type	Description
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types are to be used for application inspection decisions. In the Header MIME Type field, select the MIME message type to use for this match condition.
Port Misuse	The misuse of port 80 (or any other port running HTTP) is to be used for application inspection decisions. Indicate the application category to use for this match condition: • IM—Indicates that instant messaging applications are to be used for this match condition. • P2P—Indicates that peer-to-peer applications are to be used for this match condition. • Tunneling—Indicates that tunneling applications are to be used for this match condition.
Request Method	The request method is to be used for application inspection decisions. By default, ACE appliances allow all request and extension methods. This option allows you to configure class maps that define application 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 application inspection decision: – Ext—Indicates that an HTTP extension method is to be used for application inspection decisions. **Note** The list of available HTTP extension methods from which to choose varies depending on the version of software installed in the ACE. – RFC—Indicates that a request method defined in RFC 2616 is to be used for application 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 application 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 12-12 HTTP Protocol Inspection Match Condition Types (continued)

Match Condition Type	Description
URL	URL names are to be used for application 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 application inspection decisions. **1.** In the URL Length Operator field, select the operand to be used to compare URL length: – Equal To—Indicates that the URL length must equal the number in the URL Length Value (Bytes) field. – Greater Than—Indicates that the URL length must be greater than the number in the URL Length Value (Bytes) field. – Less Than—Indicates that the URL length must be less than the number in the URL Length Value (Bytes) field. – Range—Indicates that 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: 1. In the URL Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value (Bytes) field. 2. In the URL Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value (Bytes) field.

Step 6 Do the following:

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

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

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

Related Topics

- Configuring Virtual Context Policy Maps, page 12-34
- Setting Match Conditions for Class Maps, page 12-10
- Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14
- Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16
- Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 12-30

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 command inspection class map and want to establish match criteria.

Procedure

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

Step 2 In the Class Maps table, select the Layer 7 FTP command inspection class map that you want to configure match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.

Step 3 In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and 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 Request Method Name 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 12-13 identifies the FTP commands that can be inspected.

Table 12-13 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.
Cele	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**.

Table 12-13 FTP Commands for Inspection (continued)

FTP Command	Description
Site	Execute a site-specific command.
Stou	Store a file on the remote host and give it a unique name.
Syst	Query the remote host for operating system information.

Step 7 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.

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

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

Related Topics

- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34

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

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 Choose **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, and 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 12-14.

Table 12-14 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 12-33 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 12-33 lists the supported characters that you can use for matching string expressions.
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 12-33 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 12-33 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 12-33 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.

Table 12-14 Layer 7 SIP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
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 12-33 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 Do the following:

- 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.

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

Related Topics

- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34

Configuring Virtual Context Policy Maps

Policy maps establish traffic policy for the ACE appliance. The purpose of a traffic policy is to implement specific ACE appliance functions associated with a traffic class. A traffic policy contains:

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

The ACE appliance 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 appliance 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 appliance 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 appliance 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 12-15 lists the types of policy maps with brief descriptions.

Table 12-15 Policy Maps

Policy Map	Description	Related Topic
Layer 3/4 Management Traffic (First-Match)	Layer 3 and Layer 4 policy map for network management traffic received by the ACE	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic, page 12-45
Layer 3/4 Network Traffic (Multi-Match)	Layer 3 and Layer 4 policy map for traffic passing through the ACE	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 12-37
Layer 7 Command Inspection - FTP (First-Match)	Layer 7 policy map for inspection of FTP commands	Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection, page 12-79
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Layer 7 policy map for inspection of HTTP packets	Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 12-73
Layer 7 Deep Packet Inspection - SIP (All-Match)	Layer 7 policy map for inspection of SIP packets	Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 12-82
Layer 7 Deep Packet Inspection - Skinny	Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)	Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection, page 12-84

Table 12-15 Policy Maps (continued)

Policy Map	Description	Related Topic
Layer 7 HTTP Optimization (First-Match)	Layer 7 policy map for optimizing HTTP traffic	Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 12-86
Layer 7 Server Load Balancing (First-Match)	Layer 7 policy map for HTTP server load balancing	Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46
Server Load Balancing - Generic (First-Match)	Generic Layer 7 policy map for server load balancing	Setting Policy Map Rules and Actions for Generic Server Load Balancing, page 12-54
Server Load Balancing - HTTPS (First-Match)	Layer 7 policy map for HTTPS server load balancing **Note** The SLB HTTPS (First-Match) option is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).	Setting Policy Map Rules and Actions for HTTPS Server Load Balancing, page 12-58
Server Load Balancing - RADIUS (First-Match)	Layer 7 policy map for RADIUS server load balancing	Setting Policy Map Rules and Actions for RADIUS Server Load Balancing, page 12-63
Server Load Balancing - RDP (First-Match)	Layer 7 policy map for RDP server load balancing	Setting Policy Map Rules and Actions for RDP Server Load Balancing, page 12-71
Server Load Balancing - RTSP (First-Match)	Layer 7 policy map for RTSP server load balancing	Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 12-65
Server Load Balancing - SIP (First-Match)	Layer 7 policy map for SIP server load balancing	Setting Policy Map Rules and Actions for SIP Server Load Balancing, page 12-68

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

Procedure

Step 1 Choose **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, and 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 12-15 for a list of policy maps.

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

Step 6 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. To define rules and actions for this policy map, see Configuring Rules and Actions for Policy Maps, page 12-36.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save your entries and to configure another policy map.

Related Topics

- Using Virtual Contexts, page 4-2
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Real Servers, page 6-5
- Configuring Server Farms, page 6-18
- Configuring Sticky Groups, page 7-11

Configuring Rules and Actions for Policy Maps

Table 12-16 lists the policy maps and related topics for setting rules and actions.

Table 12-16 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 12-45
Layer 3/4 Network Traffic (First-Match)	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 12-37
Layer 7 Command Inspection - FTP (First-Match)	Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection, page 12-79
Layer 7 Deep Packet Inspection - HTTP (All-Match)	Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 12-73
Layer 7 Deep Packet Inspection - SIP (All-Match)	Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 12-82
Layer 7 Deep Packet Inspection - Skinny	Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection, page 12-84
Layer 7 HTTP Optimization (First-Match)	Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 12-82
Layer 7 Server Load Balancing (First-Match)	Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46
Server Load Balancing - Generic (First-Match)	Setting Policy Map Rules and Actions for Generic Server Load Balancing, page 12-54

Table 12-16 Topic Reference for Policy Map Rules and Actions (continued)

Policy Map Type	Topic for Setting Rules and Actions
Server Load Balancing - HTTPS (First-Match)	Setting Policy Map Rules and Actions for HTTPS Server Load Balancing, page 12-58 **Note** The SLB HTTPS (First Match) feature does not apply to the ACE NPE software version (see the"Information About the ACE No Payload Encryption Software Version" section on page 1-2).
Server Load Balancing - RADIUS (First-Match)	Setting Policy Map Rules and Actions for RADIUS Server Load Balancing, page 12-63
Server Load Balancing - RDP (First-Match)	Setting Policy Map Rules and Actions for RDP Server Load Balancing, page 12-71
Server Load Balancing - RTSP (First-Match)	Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 12-65
Server Load Balancing - SIP (First-Match)	Setting Policy Map Rules and Actions for SIP Server Load Balancing, page 12-68

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

Use this procedure to configure the 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 or class-default-v6 class map.

Procedure

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

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

Step 3 In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule configuration screen appears.

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

Step 5 In the Use Class Map field:

- For an IPv6 default class map, select the class-default radio button.
- For an IPv6 default class map, select the class-default-v6 radio button.
- For a previously created class map, go to the next step.

Step 6 To use a previously created class map for this rule, perform the following

a. In the Use Class Map field, select the others radio button.

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—Indicates that this option is not configured.

– False—Indicates that this rule is not to precede another rule in this policy map.

– True—Indicates that 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 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to define actions for this rule (see Step 8).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save 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 To add an action for this rule, click **Add** in the Action table, or select an existing action, and 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, select the type of action to be taken for this rule, and then configure the related attributes. See Table 12-17.

Table 12-17 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	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-RDP	An RDP parameter map containing RDP-related actions is to be implemented for this rule. In the Parameter Map field, specify the name of the RDP parameter map to use.

Table 12-17 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
Appl-Parameter-RTSP	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.
Appl-Parameter-SIP	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	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	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 12-18 describes the available options for application inspection actions.

Table 12-17 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.** For the IP Address Type, select either IPv4 or IPv6 for the address type. **b.** In the Static Mapped v4 or v6 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). **c.** For an IPv4 address, in the Static Mapped Netmask field, select the subnet mask to apply to the static mapped address. For an IPv6 address, in the Static Mapped Prefix-length field, enter the prefix length for the static mapped address. **d.** 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. **e.** 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. **f.** 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 and Displaying NAT Utilization, page 10-32. **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.

Table 12-17 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
Kal-ap-Primary-Out-of-Service	Enables the ACE to notify the Global Site Selector (GSS) that the primary server farm is down when the backup server farm is in use. By default, when you configure a redirect server farm as a backup server farm on the ACE and the primary server farm fails, the backup server farm redirects the client requests to another data center. However, the VIP remains in the INSERVICE state. When you configure the ACE to communicate with a Global Site Selector (GSS), it provides information for server availability. When a backup server is in use after the primary server farm is down, this feature enables the ACE to inform the GSS that the VIP for the primary server farm is out of service by returning a load value of 255. The GSS recognizes that the primary server farm is down and sends future DNS requests with the IP address of the other data center.
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	**Note** The SSL-Proxy option is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). 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.
UDP-Fast-Age	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-ICMP-Reply	A VIP is to send an ICMP ECHO-REPLY response to ICMP requests. 1. In the Active field, click the check box 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 check box 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.

Table 12-17 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

Action	Description/Steps
VIP-In-Service	A VIP is to be enabled for server load-balancing operations.
KAL-AP-TAG	The KAL-AP-TAG feature allows the Cisco Global Site Selector (GSS) proprietary KAL-AP protocol to extract load and availability information from the ACE when a firewall is positioned between the GSS and the ACE. This feature allows you to configure a tag (name) per VIP for a maximum of 4,096 tags on an ACE. This feature does not replace the tag per domain feature. For more information about this feature, see the Configuring Health Monitoring chapter in the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*. **Note** The KAL-AP-TAG selection is not available for the class-default class map. In the KAL-AP-Tag Name field, enter the name as an unquoted text string with no spaces and a maximum of 76 alphanumeric characters. The following scenarios are not supported and will result in an error: • You cannot configure a tag name for a VIP that already has a tag configuration as part of a different policy configuration. • You cannot associate the same tag name with more than one VIP. • You cannot associate the same tag name with a domain and a VIP. • You cannot assign two different tags to two different Layer 3 class maps that have the same VIP, but different port numbers. The KAL-AP protocol considers these class maps to have the same VIP and calculates the load for both Layer 3 rules together when the GSS queries the VIP.

Table 12-18 Policy Map Application Inspection Options

Inspection Option	Description
DNS	Indicates that 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 appliance 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. Valid entries are integers from 512 to 65535.
FTP	Indicates that FTP inspection is to be implemented. The ACE appliance inspects FTP packets, translates the address and port embedded in the payload, and opens up secondary channel for data. **1.** 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 appliance is to check for protocol RFC compliance and prevent Web browsers from sending embedded commands in FTP requests: – N/A—Indicates that this attribute is not set. – False—Indicates that the ACE appliance is not to check for RFC compliance or prevent Web browsers from sending embedded commands in FTP requests. – True—Indicates that the ACE appliance 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	Indicates that 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 appliance. By default, the ACE appliance 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 appliance 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—Indicates that this attribute is not set. – False—Indicates that Layer 3 and Layer 4 traffic is not to be monitored. – True—Indicates that 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 12-18 Policy Map Application Inspection Options (continued)

Inspection Option	Description
ICMP	Indicates that 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 appliance is to perform name address translation on ICMP error messages: • N/A—Indicates that this attribute is not set. • False—Indicates that the ACE appliance is not to perform NAT on ICMP error messages. • True—Indicates that the ACE appliance is to perform NAT on ICMP error messages. When enabled, the ACE appliance creates translation sessions for intermediate or endpoint nodes that send ICMP error messages based on the NAT configuration. The ACE appliance overwrites the packet with the translated IP addresses.
ILS	Internet Locator Service (ILS) protocol inspection is to be implemented.
RTSP	Indicates that 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 appliance monitors Setup and Response (200 OK) messages in the control channel established using TCP port 554 (no UDP support).
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. 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. 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 11 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

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 appliance.

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 or class-default-v6 class map.

Procedure

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

Step 2 In the Policy Maps table, select the Layer 3/Layer 4 management traffic policy map you want to set rules and actions for, and then select the **Rule** tab. 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, and then click **Edit**. The Rule screen appears.

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

Step 5 In the Use Class Map field:

- For an IPv4 default class map, select the class-default radio button.
- For an IPv6 default class map, select the class-default-v6 radio button.
- For a previously created class map, go to the next step.

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

a. In the Use Class Map field, select the others radio button.

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—Indicates that this option is not configured.
- False—Indicates that this rule is not to precede another rule in this policy map.
- True—Indicates that 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 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with Step 8.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save 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 To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

Step 9 In the Action configuration screen:

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

b. In the Action Type field, select **Mgmt-permit** to indicate that this action permits or denies network management traffic.

c. In the Action field, specify the action that is to occur:

- Deny—Indicates that the ACE appliance is to deny network management traffic when this rule is met.
- Permit—Indicates that the ACE appliance is to accept network management traffic when this rule is met.

Step 10 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

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.
- If you want to insert, rewrite, and delete HTTP headers, ensure that an HTTP header modify action list has been configured. See Configuring an HTTP Header Modify Action List, page 12-90 for more information.

Procedure

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

Step 2 In the Policy Maps table, select the load-balancing policy map you want to set rules and actions for, and then select the Rule tab. The Rule table appears.

Step 3 In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.

Step 4 Select the type of rule to be used:

- Class Map—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions. If you select this rule type, continue with Step 5.
- Match Condition—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions. If you select this rule type, continue with Step 6.

Step 5 If you select Class Map, either check the Use Class Default check box to use a default class map or specify 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.

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

- N/A—Indicates that this option is not configured.
- False—Indicates that this rule is not to precede another rule in this policy map.
- True—Indicates that 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 6 For match conditions:

a. In the Match Condition Name field enter a name for the match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

b. In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 12-19 for information about these selections.

Table 12-19 Policy Match Condition Types

Match Condition	Description
HTTP Content	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 4000.
HTTP Cookie	Indicates that HTTP cookies are to be used for this rule. If you select this method: 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 appliance supports regular expressions for matching string expressions. Table 12-33 lists the supported characters that you can use for matching string expressions.
HTTP Header	Indicates that the HTTP header and a corresponding value are to be used for this rule. If you select this method: 1. In the 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 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 appliance 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 12-33 for a list of the supported characters that you can use in regular expressions.
HTTP URL	Indicates that this rule is to perform regular expression matching against the received packet data from a particular connection based on the HTTP URL string. If you select this method: 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 appliance supports regular expressions for matching URL strings. See Table 12-33 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 64 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).

Table 12-19 Policy Match Condition Types (continued)

Match Condition	Description
Source Address	Indicates that this rule is to use a client source IP address to establish match conditions. If you select this method: 1. For the IP Address Type, select either IPv4 or IPv6 for the address type. 2. In the Source IP Address field, enter the source IP address of the client in the format based on the address type (IPv4 or IPv6). 3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.

Table 12-19 Policy Match Condition Types (continued)

Match Condition	Description
SSL	Defines load balancing decisions based on the specific SSL cipher or cipher strength. **Note** The SSL option is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). Enables the ACE to load balance client traffic to different server farms based on the SSL encryption level negotiated with the ACE during SSL termination. If you select this method: **1.** In the SSL Cipher Match Type field, select the match type. Options include: – Equal To—Specifies an SSL cipher for the load balancing decision. – Less Than—Specifies SSL cipher strength for the load balancing decision. **2.** If you selected Equal To, in the Cipher Name field specify an SSL cipher for the load balancing decision. The possible values are as follows: – RSA_EXPORT1024_WITH_DES_CBC_SHA – RSA_EXPORT1024_WITH_RC4_56_MD5 – RSA_EXPORT1024_WITH_RC4_56_SHA – RSA_EXPORT_WITH_DES40_CBC_SHA – RSA_EXPORT_WITH_RC4_40_MD5 – RSA_WITH_3DES_EDE_CBC_SHA – RSA_WITH_AES_128_CBC_SHA – RSA_WITH_AES_256_CBC_SHA – RSA_WITH_DES_CBC_SHA – RSA_WITH_RC4_128_MD5 – RSA_WITH_RC4_128_SHA **3.** If you selected Less Than, in the Specify Minimum Cipher Strength field specify a non-inclusive minimum SSL cipher bit strength. For example, if you specify a cipher strength value of 128, any SSL cipher that was no greater than 128 would hit the traffic policy. If the SSL cipher was 128-bit or greater, the connection would miss the policy. The possible values are as follows: – 56—56-bit strength – 128—128-bit strength – 168—168-bit strength – 256—256-bit strength

Step 7 For specific class maps and match conditions, in the Insert Before field, indicate whether this rule is to precede another defined policy rule:

- N/A—Indicates that this option is not applicable.
- False—Indicates that this rule is not to precede another defined policy rule.
- True—Indicates that this rule is to precede another policy rule.

  If you select True, in the Insert Before Policy Rule field, select the policy rule that this rule is to precede.

Step 8 Do the following:

- Click **Deploy Now** to deploy the configuration on the ACE appliance. The Action table appears below the Rule table. To define the actions for this rule, continue with Step 9.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to save 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 a new action for this rule, or select an existing action, and then click **Edit** to modify it.

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 tab in the Action Type field, select the action to be taken and configure any action-specific attributes as described in Table 12-20.

Table 12-20 Policy Map Actions for Load Balancing

Action	Description
Action	Indicates that the ACE appliance is to use an HTTP header modify action list to insert, rewrite, or delete HTTP headers. It can also be used to configure the SSL URL rewrite function The Action List drop down appears, listing the configured HTTP header modify action lists (see the "Configuring an HTTP Header Modify Action List" section on page 12-90). Make a selection from this list. If necessary, click **Add** to add a new HTTP header modify action list, or select an existing action list, and then click **Edit** to modify it.
Compress	Indicates that the ACE appliance 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 appliance is to use to compress packets: • Deflate—Indicates that the ACE appliance is to use the DEFLATE compression method when the client browser supports both the DEFLATE and GZIP compression methods. • Gzip—Indicates that ACE appliance is to use the GZIP compression method when the client browser supports both the DEFLATE and GZIP compression methods. This is the default setting.
Drop	Indicates that the ACE appliance 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	Indicates that the ACE appliance is to forward requests that match this policy map without load balancing the requests.
Insert-HTTP	Indicates that the ACE appliance is to insert an HTTP header for Layer 7 load balancing for requests that match this policy map. This option allows the ACE appliance 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 appliance 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 12-33 for a list of the supported characters that you can use in regular expressions.

Table 12-20 Policy Map Actions for Load Balancing (continued)

Action	Description
Reverse Sticky	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 *Server Load-Balancing Guide, Cisco ACE Application Control Engine*. In the Sticky Group field, choose the name of an existing IPv4 IP netmask or IPv6 prefix sticky group that you want to associate with reverse IP stickiness.
Server Farm	Indicates that the ACE appliance 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. Leave this field blank to indicate that no backup server farm is to be used. 3. Check 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. 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.
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 and Displaying NAT Utilization, page 10-32. 2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 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.

Table 12-20 Policy Map Actions for Load Balancing (continued)

Action	Description
SSL-Proxy	**Note** The SSL-Proxy action is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). Indicates that the ACE appliance is to use an SSL proxy client service to define the SSL parameters the ACE appliance is to use during the handshake and subsequent SSL session. 1. In the SSL Proxy field, select the SSL proxy server service to be used for this action. 2. In the SSL Proxy Type field, select Client to indicate that the ACE appliance is to be configured so that it is recognized as an SSL client.
Sticky-Server Farm	Indicates that 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 12 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Setting Policy Map Rules and Actions for Generic Server Load Balancing

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 Choose **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, and then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 12-21.

Table 12-21 Generic Server Load Balancing Policy Map Rules

Option	Description
Class Map	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 **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.

Table 12-21 Generic Server Load Balancing Policy Map Rules (continued)

Option	Description		
Match Condition	A match condition is used for this traffic policy.		
	Match Condition Name	Enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.	
	Match Condition Type	Layer 4 Payload	Layer 4 payload data 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 12-33 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.
		Source Address	A client source host IPv4 address and subnet mask, or IPv6 address and prefix length are used for the network traffic matching criteria. **1.** For the IP Address Type, select either IPv4 or IPv6 for the address type. **2.** In the Source IP Address field, enter the source IP address of the client in the format based on the address type (IPv4 or IPv6). **3.** For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.
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 Do the following:

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

Note If you selected the Insert Before option 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, and 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 12-22.

Table 12-22 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.
Forward	The ACE is to forward the traffic that match this policy map to its destination.
Reverse Sticky	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 *Server Load-Balancing Guide, Cisco ACE Application Control Engine*. In the Sticky Group field, choose an existing IPv4 IP netmask or IPv6 prefix sticky group that you want to associate with reverse IP stickiness.
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.

Table 12-22 Generic Server Load Balancing Policy Map Actions (continued)

Action	Description
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 and Displaying NAT Utilization, page 10-32. 2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 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.
Sticky Group	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.

Step 9 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Setting Policy Map Rules and Actions for HTTPS Server Load Balancing

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

Note The HTTPS server load balancing feature does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

Assumptions

- An HTTPS traffic policy map has been configured.

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

Procedure

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

Step 2 In the Policy Maps table, select the HTTPS 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, and then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 12-21.

Table 12-23 HTTPS Server Load Balancing Policy Map Rules

Option	Description	
Class Map	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 **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	A match condition is used for this traffic policy.	
	Match Condition Name	Enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

Table 12-23 HTTPS Server Load Balancing Policy Map Rules (continued)

Option	Description		
	Match Condition Type	Source Address	A client source host IPv4 address and subnet mask, or IPv6 address and prefix length are used for the network traffic matching criteria. **1.** For the IP Address Type, select either **IPv4** or **IPv6** for the address type. **2.** In the Source IP Address field, enter the source IP address of the client in the format based on the address type (IPv4 or IPv6). **3.** For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.
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 Do the following:

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

Note If you selected the Insert Before option 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, and 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 12-22.

Table 12-24 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 by choosing one of the following options: • **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	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 *Server Load-Balancing Guide, Cisco ACE Application Control Engine*. In the Sticky Group field, choose an existing IPv4 IP netmask or IPv6 prefix sticky group that you want to associate with reverse IP stickiness.

Table 12-24 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.
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 and Displaying NAT Utilization, page 10-32. 2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 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.
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 group to be used for requests that match this policy map. ACE displays all stick groups configured on the virtual context; however, only the following sticky types are applicable for a load balancing policy map: IP Netmask, IPv6 Prefix, and SSL. ACE displays an error message if you choose an incorrect sticky type.

Step 9 Do one of the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Setting Policy Map Rules and Actions for RADIUS Server Load Balancing

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 Choose **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, and then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 12-25.

Table 12-25 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 12-33 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 12-33 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 Do the following:

- 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.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to configure another rule.

Note If you selected the Insert Before option 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, and 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 12-22.

Step 9 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Setting Policy Map Rules and Actions for RTSP Server Load Balancing

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 Choose **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, and then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 12-26.

Table 12-26 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 12-27.
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 12-27 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 12-33 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 Expression 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 12-33 for a list of the supported characters that you can use in regular expressions. **2.** In the Method Expression 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.** For the IP Address Type, select either IPv4 or IPv6 for the address type. **2.** In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6). **3.** For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the 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 Do the following:

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

Note If you selected the Insert Before option in Step 5 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, and 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 12-22.

Step 10 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Setting Policy Map Rules and Actions for SIP Server Load Balancing

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 Choose **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, and then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 12-28.

Table 12-28 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 12-29.
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 12-29 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, and 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, and 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 12-33 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. The source IP address is used to establish a match condition. 1. For the IP Address Type, select either IPv4 or IPv6 for the address type. 2. In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6). 3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address. For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.

Step 5 Do the following:

- 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.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to add another rule.

Note If you selected the Insert Before option in Step 4 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, and 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 12-22.

Step 9 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Setting Policy Map Rules and Actions for RDP Server Load Balancing

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

Assumptions

- An RDP server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

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

Step 2 In the Policy Maps table, 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, and 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 Do the following:

- 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.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to configure another rule.

Note If you 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, and 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 12-22.

Step 12 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

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

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

Procedure

Step 1 Choose **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, and then select the Rule tab. You can select multiple policy maps (hold down the Shift key while selecting entries) and apply common rules and actions to them.

Step 3 In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.

Step 4 In the Type field, select the type of rule to be used:

- Class Map—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions. Continue with Step 5.
- Match Condition—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions. Continue with Step 7.

Step 5 For class maps, check the Use Class Default check box to use the class-default class map, or clear the check box to use a previously created class map.

Step 6 If you clear the Use Class Default check box:

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

b. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.

- N/A—Indicates that this option is not configured.
- False—Indicates that this rule is not to precede another rule in this policy map.
- True—Indicates that this rule is to precede another rule in this policy map.

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

Step 7 For match conditions:

a. In the Match Condition Name field enter a name for the match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

b. In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 12-30 for information about these selections.

Table 12-30 HTTP Deep Packet Inspection Match Types

Match Condition Type	Description
Content	Specific content contained within the HTTP entity-body is used for application 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 4000 bytes.
Content Length	The content parse length in an HTTP message is used for application inspection decisions. **1.** In the Content Length Operator field, select the operand to be used to compare content length: – Equal To—Indicates that the content length must equal the number in the Content Length Value (Bytes) field. – Greater Than—Indicates that the content length must be greater than the number in the Content Length Value (Bytes) field. – Less Than—Indicates that the content length must be less than the number in the Content Length Value (Bytes) field. – Range—Indicates that 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: 1. In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are 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. 2. In the Content Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are 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 appliance. 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 appliance performs the specified Layer 7 policy map action. **Note** Content Type Verification is only available an inline match condition. Because this Layer 7 HTTP deep inspection match criteria cannot be combined with other match criteria, it appears as an inline match condition.

Table 12-30 HTTP Deep Packet Inspection Match Types (continued)

Match Condition Type	Description
Header	The name and value in an HTTP header are used for application 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 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 appliance 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 12-33 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 application inspection decisions. **1.** In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: – Request—Indicates that HTTP header request messages are to be checked for header length. – Response—Indicates that 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—Indicates that the header length must equal the number in the Header Length Value (Bytes) field. – Greater Than—Indicates that the header length must be greater than the number in the Header Length Value (Bytes) field. – Less Than—Indicates that the header length must be less than the number in the Header Length Value (Bytes) field. – Range—Indicates that 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: 1. In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are 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. 2. In the Header Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are 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 12-30 HTTP Deep Packet Inspection Match Types (continued)

Match Condition Type	Description
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types are used for application 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 application inspection decisions. Indicate the application category to be used for this match condition: • IM—Indicates that instant messaging applications are to be used for this match condition. • P2P—Indicates that peer-to-peer applications are to be used for this match condition. • Tunneling—Indicates that tunneling applications are to be used for this match condition.
Request Method	The request method is used for application inspection decisions. By default, ACE appliances allow all request and extension methods. This option allows you to configure class maps that define application 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 application inspection decision: – Ext—Indicates that an HTTP extension method is to be used for application inspection decisions. – RFC—Indicates that a request method defined in RFC 2616 is to be used for application 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.
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 appliance performs the specified Layer 7 policy map action. **Note** Strict HTTP is only available an inline match condition. Because this Layer 7 HTTP deep inspection match criteria cannot be combined with other match criteria, it appears as an inline match condition.

Table 12-30 HTTP Deep Packet Inspection Match Types (continued)

Match Condition Type	Description
Transfer Encoding	An HTTP transfer-encoding type is used for application 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.
URL	URL names are used for application 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 application inspection decisions. **1.** In the URL Length Operator field, select the operand to be used to compare URL length: – Equal To—Indicates that the URL length must equal the number in the URL Length Value (Bytes) field. – Greater Than—Indicates that the URL length must be greater than the number in the URL Length Value (Bytes) field. – Less Than—Indicates that the URL length must be less than the number in the URL Length Value (Bytes) field. – Range—Indicates that 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: 1. In the URL Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value (Bytes) field. 2. In the URL Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value (Bytes) field.

Step 8 In the Insert Before field, specify whether this rule is to precede another rule in this policy map:

- N/A—Indicates that this attribute is not set.
- False—Indicates that this rule is not to precede another rule in the policy map.
- True—Indicates that this rule is to precede another rule in the policy map.

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

Step 10 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with Step 11.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save 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 To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

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

Step 13 In the Action Type field, select the action to be taken for this rule:

- Permit—Indicates that the specified HTTP traffic is to be allowed if it meets the specified HTTP deep packet inspection match criteria.
- Reset—Indicates that the specified HTTP traffic is to be denied. A TCP reset message is sent to the client or server to close the connection.

Step 14 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

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 Choose **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, and then select the Rule tab. You can select multiple policy maps (hold down the Shift key while selecting entries) and apply common rules and actions to them.

Step 3 In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.

Step 4 In the Type field, select the type of rule to be used:

- Class Map—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions.
- Match Condition—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions.

Step 5 For class maps, check the Use Class Default check box to use the class-default class map, or clear the check box to use a previously created class map.

Step 6 If you clear the Use Class Default check box:

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

b. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.

- N/A—Indicates that this option is not configured.
- False—Indicates that this rule is not to precede another rule in this policy map.
- True—Indicates that this rule is to precede another rule in this policy map.

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

Step 7 For match conditions:

a. In the Match Condition Name field enter a name for the match condition for this rule. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

b. In the Match Condition Type field, select Request Method Name as the match condition type for this rule.

c. In the Request Method Name field, select the FTP command to be inspected for this rule. Table 12-13 describes the FTP commands that can be inspected.

Step 8 In the Insert Before field, specify whether this rule is to precede another rule in this policy map:

- N/A—Indicates that this attribute is not set.
- False—Indicates that this rule is not to precede another rule in the policy map.
- True—Indicates that this rule is to precede another rule in the policy map.

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

Step 10 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with Step 11.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save 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 To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

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

Step 13 In the Action Type field, specify the action to be taken for this rule:

- Deny—Indicates that the ACE appliance is to deny the specified FTP command when this rule is met.
- Mask Reply—Indicates that the ACE appliance 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 14 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

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

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 Choose **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, and then click **Edit**. The Rule screen appears.

Step 4 In the Type field, configure rules using the information in Table 12-31.

Table 12-31 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 5-7.
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 Do the following:

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

Note If you selected the Insert Before option 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, and 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 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

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

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 Choose **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, and 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 Do the following:

- 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.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to configure another rule.

Note If you 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, and 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 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization

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

Assumptions

- An HTTP optimization action list has been configured. See Configuring an HTTP Optimization Action List, page 13-3 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 12-8 for more information.

Procedure

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

Step 2 In the Policy Maps table, select the Layer 7 HTTP optimization policy map you want to set rules and actions for, and then select the Rule tab. You can select multiple policy maps (hold down the Shift key while selecting entries) and apply common rules and actions to them.

Step 3 In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.

Step 4 In the Type field, select the type of rule to be used:

- Class Map—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions.
- Match Condition—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions.

Step 5 For class maps, check the Use Class Default check box to use the class-default class map, or clear the check box to use a previously created class map.

Step 6 If you clear the Use Class Default check box:

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

b. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.

- N/A—Indicates that this option is not configured.
- False—Indicates that this rule is not to precede another rule in this policy map.
- True—Indicates that this rule is to precede another rule in this policy map.

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

Step 7 For match conditions:

a. In the Match Condition Name field, enter a name for the match condition for this rule. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

b. In the Match Condition Type field, select the type of match condition to use and configure condition-specific options as described in Table 12-32.

Table 12-32 Layer 7 HTTP Optimization Match Condition Types

Match Condition Type	Procedure
Cookie	Indicates that 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 check box, do one of the following: – Clear the check box to indicate that the cookie being defined is a primary cookie. – Check the check box to indicate that the cookie being defined is a secondary cookie. You can specify the delimiters for cookies in a URL string by using an HTTP parameter map (see the "Configuring HTTP Parameter Maps" section on page 8-2).
Header	Indicates that 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 appliance 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 12-33 for a list of the supported characters that you can use in regular expressions.
HTTP URL	Indicates that 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 64 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 8 In the Insert Before field, specify whether this rule is to precede another rule in this policy map:

- N/A—Indicates that this attribute is not set.
- False—Indicates that this rule is not to precede another rule in the policy map.
- True—Indicates that this rule is to precede another rule in the policy map.

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

Step 9 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with Step 10.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to save 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 10 To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

Step 11 In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 12 In the Action Type field, select Action-list to indicate that an HTTP optimization action list is to be employed when the match criteria are met.

Step 13 In the Action List field, select the HTTP optimization action list to apply to this policy map and rule.

If necessary, click **Add** to add a new HTTP optimization action list, or select an existing action list, and then click **Edit** to modify it.

Step 14 In the Optimization Parameter Map field, select the optimization parameter map to apply to this policy map and rule.

Step 15 Do the following:

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

Related Topics

- Configuring Traffic Policies, page 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Rules and Actions for Policy Maps, page 12-36

Special Characters for Matching String Expressions

Table 12-33 identifies the special characters that can be used in matching string expressions. Use parenthesized expressions for dynamic replacement using %1 and %2 in the replacement pattern.

Note When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

Table 12-33 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 12-1
- Configuring Virtual Context Class Maps, page 12-8
- Configuring Virtual Context Policy Maps, page 12-34
- Configuring Real Servers, page 6-5

- Configuring Server Farms, page 6-18
- Configuring Sticky Groups, page 7-11

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 12-86).
- An HTTP header modify action list performs the following operations:
  - Groups a series of individual functions to insert, rewrite, or delete HTTP headers.
  - Configures the SSL URL rewrite function.
  - Inserts SSL session parameters, client certificate fields, and server certificate fields into the HTTP requests that the ACE receives over the connection.

  The HTTP header action list is associated with a Layer 7 server load-balancing policy map (see the "Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic" section on page 12-46).

Table 12-34 lists the action lists that you can configure using the ACE.

Table 12-34 Action Lists

Action List	Topic
Optimization Action List	Configuring an HTTP Optimization Action List, page 13-3
HTTP Header Modify Action List	Configuring an HTTP Header Modify Action List, page 12-90

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 12-91
- Configuring SSL URL Rewrite, page 12-94
- Configuring SSL Header Insertion, page 12-96

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 Choose **Config > Virtual Contexts > *context* > Expert > Action Lists > HTTP Header Modify Action Lists**.

The HTTP Header Modify Action List table appears.

Step 2 Do one of the following:

- To edit an existing action list, choose the action list and click the **Edit** icon. The Edit HTTP Header Modify Action List window appears.
- To create a new action list, do the following:

  a. Click the **Add** icon. The New HTTP Header Modify Action List window appears.

  b. 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.

  c. Click **Deploy Now**. The Edit HTTP Header Modify Action List window appears.

Step 3 (Optional) To rewrite the URL pathname in HTTP requests, do the following:

a. From the URL Expression field, enter the regular expression of the URL in the incoming request to match.

b. From the Replace field, enter the replacement URL string.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
- **%u**—Inserts the URL path string from the request
- **%h**—Inserts the hostname from the request host header

Step 4 (Optional) Content Rewrite Response String provides the capability to rewrite configured regex patterns in the HTTP response:

a. The HTTP Content Rewrite feature provides the capability on the ACE module to re-write configured HTTP content in the HTTP response data.

b. The HTTP content ‘Rewrite response replace’ feature provides the capability on the ACE module to replace configured HTTP content in the HTTP response data.

Step 5 Select the Header Action tab. The Header Action table appears.

Step 6 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 12-35.

Table 12-35 Header Action Configuration Screen Fields

Header Action Field	Description / Action
Operator	Select the HTTP header modify action the ACE appliance 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 12-35 Header Action Configuration Screen Fields (continued)

Header Action Field	Description / Action
Direction	Select the HTTP header modify action the ACE appliance 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 appliance 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 12-33 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 7 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to save your entries.

Related Topics

- Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46, Table 12-20

Configuring SSL URL Rewrite

Note The SSL URL rewrite feature does not apply to the ACE NPE software image (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

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 Choose **Config > Virtual Contexts >** ***context*** **> Expert > Action Lists > HTTP Header Modify Action Lists**. The HTTP Header Modify Action List table appears.

Step 2 Click **Add** to add a new HTTP header modify action list, or select an existing action list, and 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 12-36.

Table 12-36 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 12-91. The ACE appliance 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 12-33 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 Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to save your entries.

Related Topics

- Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46, Table 12-20

Configuring SSL Header Insertion

Note The SSL Header Insertion feature does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

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

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

- Session Parameters—SSL session parameters that the ACE and client negotiate during the SSL handshake.
- Server Certificate Fields—Information regarding the SSL server certificate that resides on the ACE.
- Client Certificate Fields—Information regarding the SSL client certificate that the ACE retrieves from the client when you configure the ACE to perform client authentication.

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

By default, the ACE inserts the SSL header information into the first HTTP request only that it receives over the connection. When the ACE and client need to renegotiate their connection, the ACE updates the HTTP header information that it send to the server to reflect the new session parameters. You can also instruct the ACE to insert the session information into every HTTP request that it receives over the connection by creating an HTTP parameter map with either the **Header Modify Per-Request** or **HTTP Persistence Rebalance** options enabled (see the "Configuring HTTP Parameter Maps" section on page 8-2).

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

Procedure

Step 1 Choose **Config** > **Virtual Contexts** > *context* > **Expert** > **HTTP Header Modify Action Lists**.

The HTTP Header Modify Action Lists table appears.

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

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

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

The SSL Header Insert table appears.

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

The SSL Header Insert configuration window appears. Enter the required information as shown in Table 12-37.

Table 12-37 SSL Header Insert Configuration Window Fields

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

Table 12-37 SSL Header Insert Configuration Window Fields (continued)

Header Action Field	Description / Action
CipherKey	This field appears only when the Request field is set to Session. Select the following session parameters to insert into the HTTP request: • Cipher-Key-Size—Symmetric cipher key size. • Cipher-Name—Symmetric cipher suite name. • Cipher-Use-Size—Symmetric cipher use size. • Id—SSL Session ID. The default is 0. • Protocol-Version—Version of SSL or TLS. • Step-Up—Use of SGC or StepUp cryptography to increase the level of security by using 128-bit encryption. • Verify-Result—SSL session verify result. Possible values are as follows: – ok—The SSL session is established. – certificate is not yet valid—The client certificate is not yet valid. – certificate is expired—The client certificate has expired. – bad key size—The client certificate has a bad key size. – invalid not before field—The client certificate notBefore field is in an unrecognized format. – invalid not after field—The client certificate notAfter field is in an unrecognized format. – certificate has unknown issuer—The client certificate issuer is unknown. – certificate has bad signature—The client certificate contains a bad signature. – certificate has bad leaf signature—The client certificate contains a bad leaf signature. – unable to decode issuer public key—The ACE is unable to decode the issuer public key. – unsupported certificate—The client certificate is not supported. – certificate revoked— The client certificate has been revoked. – internal error—An internal error exists. For more information, see the *SSL Guide, Cisco ACE Application Control Engine*.
Value	This field appears only when the Request field is set to either Client-Certificate or Server-Certificate. Choose one of the following options: • N/A—Specifies that the selected algorithm or cipher key is inserted without adding a prefix to it or renaming it. • Prefix—Enables you to specify a prefix string to place before the specified certificate or session field name. For example, if you specify the prefix Acme-SSL for the SSL session field name Cipher-Name, then the field name becomes Acme-SSL-Session-Cipher-Name. • Rename—Enables you to specify a new name for the specified certificate or session field name.
Prefix	This field appears only when the Value field is set to Prefix. Enter a quoted text string to place before the specified certificate or session field name. The maximum combined number of prefix string and field name characters that the ACE permits is 32.
Rename	This field appears only when the Value field is set to Rename. Enter a new name to the specified certificate or session field name. The name must be an unquoted text string with no spaces. The maximum number of field name string characters that the ACE permits is 32.

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

Step 6 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **OK** to save your entries. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the SSL Header Insert table.

Related Topics

- Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 12-65, Table 12-20