



## CHAPTER 3

# Configuring Virtual Servers

---

This section provides an overview of server load balancing and procedures for configuring virtual servers for load balancing on an ACE appliance.

Topics include:

- [Load Balancing Overview, page 3-1](#)
- [Configuring Virtual Servers, page 3-2](#)
- [Managing Virtual Servers, page 3-47](#)
- [Configuring Secure KAL-AP, page 3-50](#)

## Load Balancing Overview

Server load balancing (SLB) is the process of deciding to which server a load-balancing device should send a client request for service. For example, a client request can consist of an HTTP GET for a Web page or an FTP GET to download a file. The job of the load balancer is to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Depending on the load-balancing algorithm or predictor that you configure, the ACE appliance performs a series of checks and calculations to determine the server that can best service each client request. The ACE appliance bases server selection on several factors, including the server with the fewest connections with respect to load, source or destination address, cookies, URLs, or HTTP headers.

The ACE Appliance Device Manager allows you to configure load balancing using:

- Virtual servers—See [Configuring Virtual Servers, page 3-2](#).
- Real servers—See [Configuring Real Servers, page 4-4](#).
- Server farms—See [Configuring Server Farms, page 4-10](#).
- Sticky groups—See [Configuring Sticky Groups, page 5-6](#).
- Parameter maps—See [Configuring Parameter Maps, page 6-6](#).

For information about SLB as configured and performed by the ACE appliance, see:

- [Configuring Virtual Servers, page 3-2](#)
- [Load-Balancing Predictors, page 4-2](#)
- [Real Servers, page 4-3](#)
- [Server Farms, page 4-3](#)

- [Configuring Health Monitoring, page 4-22](#)
- [TCL Scripts, page 4-22](#)
- [Configuring Sticky Groups, page 5-6](#)

## Configuring Virtual Servers

In a load-balancing environment, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. A virtual server is bound to physical services running on real servers in a server farm and uses IP address and port information to distribute incoming client requests to the servers in the server farm according to a specified load-balancing algorithm.

You use class maps to configure a virtual server address and definition. The load-balancing predictor algorithms (for example, round-robin, least connections, and so on) determine the servers to which the ACE sends connection requests.

For more information about virtual servers and the ACE Appliance Device Manager, see:

- [Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 3-2](#)
- [Using ACE Appliance Device Manager to Configure Virtual Servers, page 3-3](#)
- [Virtual Server Configuration Procedure, page 3-4](#)

## Understanding Virtual Server Configuration and ACE Appliance Device Manager

The ACE Appliance Device Manager Virtual Server configuration interface, an abstraction of the Modular Policy CLI, simplifies, reorders, and makes more atomic the configuration and deployment of a functional load-balancing environment. With simplification or abstraction, some constraints or limitations are necessarily introduced. This section identifies the constraints and framework used by ACE Appliance Device Manager for virtual server configuration.

In ACE Appliance Device Manager, a viable virtual server has the following attributes:

- A single Layer 3/Layer 4 match condition  
This means that you can specify only a single IP address (or single IP address range if a netmask is used), with only a single port (or port range). Having a single match condition greatly simplifies and aids virtual server configuration.
- A default Layer 7 action
- A Layer 7 policy map
- A Layer 3/Layer 4 class map
- A multi-match policy map, a class-map match, and an action

In addition:

- The virtual server multi-match policy map is associated with an interface or is global.
- The name of the virtual server is derived from the name of the Layer 3/Layer 4 class map.

[Example 3-1](#) shows the minimum configuration statements required for a virtual server.

**Example 3-1 Minimum Configuration Required for a Virtual Server**

```
class-map match-all Example_VIP
  2 match virtual-address 10.10.10.10 tcp eq www
policy-map type loadbalance first-match Example_VIP-l7slb
  class class-default
    forward
policy-map multi-match int10
  class Example_VIP
    loadbalance policy Example_VIP-l7slb

interface vlan 10
  ip address 192.168.65.37 255.255.255.0
  service-policy input int10
  no shutdown
```

Note also the following items regarding the ACE Appliance Device Manager and virtual servers:

- **Additional configuration options**  
The Virtual Server configuration screen allows you to configure additional items for a functional VIP. These items include server farms, sticky groups, real servers, probes, parameter maps, inspection, class maps, and inline match conditions. Because too many items on a screen can be overwhelming, not all configuration options appear on Virtual Server configuration screen, such as sticky statics or backup real servers. These options are available elsewhere in the ACE Appliance Device Manager interface instead of on the Virtual Server configuration screen.
- **Configuration options and roles**  
To support and maintain the separation of roles, some objects cannot be configured using the Virtual Server configuration screen. These objects include SSL certificates, SSL keys, NAT pools, interface IP addresses, and ACLs. Providing these options as separate configuration options in the ACE Appliance Device Manager interface ensures that a user who can view or modify virtual servers or aspects of virtual servers cannot create or delete virtual servers.

**Related Topics**

- [Configuring Virtual Servers, page 3-2](#)
- [Using ACE Appliance Device Manager to Configure Virtual Servers, page 3-3](#)
- [Virtual Server Configuration Procedure, page 3-4](#)

## Using ACE Appliance Device Manager to Configure Virtual Servers

It is important to understand the following when using the ACE Appliance Device Manager to configure virtual servers:

- **Virtual server configuration screens**  
The ACE Appliance Device Manager Virtual Server configuration screens are designed to aid you in configuring virtual servers by presenting configuration options that are relevant to your choices. For example, the protocols that you select in the Properties configuration subset determine the other configuration subsets that appear.
- **Use the virtual server configuration method that suits you**

The ACE Appliance Device Manager Virtual Server configuration screens simplify the process of creating, modifying, and deploying virtual servers by displaying those options that you are most likely to use. In addition, as you specify attributes for a virtual server, such as protocols, the interface refreshes with related configuration options, such as Protocol Inspection or Application Acceleration and Optimization, thereby speeding virtual server configuration and deployment.

While Virtual Server configuration screens remove some configuration complexities, they have a few constraints that the Expert configuration options do not. If you are comfortable using the CLI, you can use the Expert options (such as **Config > Virtual Contexts > context > Expert > Class Map or Policy** or **Config > Virtual Contexts > context > Load Balancing > Parameter Map**) to configure more complex attributes of virtual servers, traffic policies, and parameter maps.

- **Synchronizing virtual server configurations**

When you use the CLI to change a virtual context's configuration on the ACE appliance, the ACE Appliance Device Manager periodically polls the CLI (approximately once every two minutes) for configuration changes. When it detects an out-of-band configuration change in a context, the changes are applied to the configuration maintained by ACE Appliance Device Manager. The status bar at the bottom of the ACE Appliance Device Manager indicates a summary count of the contexts in the various synchronization states

If you configure a virtual server using the CLI and then use the CLI Sync option (**Config > Virtual Contexts > CLI Sync**) to manually synchronize configurations, the configuration that appears in the ACE Appliance Device Manager for the virtual server might not display all configuration options for that virtual server. The configuration that appears in the ACE Appliance Device Manager depends on a number of items, such as the protocols configured in class maps or the rules defined for policy maps.

For example, if you configure a virtual server on the CLI that includes a class map that can match any protocol, you will not see the virtual server Application Acceleration and Optimization configuration subset in the ACE Appliance Device Manager.

- **Modifying shared objects**

Modifying an object that is used by multiple virtual servers, such as a server farm, real server, or parameter map, could impact the other virtual servers. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying objects used by multiple virtual servers.

#### Related Topics

- [Configuring Virtual Servers, page 3-2](#)
- [Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 3-2](#)
- [Virtual Server Configuration Procedure, page 3-4](#)

## Virtual Server Configuration Procedure

Use this procedure to add virtual servers to the ACE Appliance Device Manager for load-balancing purposes.

#### Assumptions

- Depending on the protocol to be used for the virtual server, parameter maps need to be defined.
- For SSL service, SSL certificates, keys, chain groups, and parameter maps must be configured.

## Procedure

- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, then click **Edit** to modify it. The Virtual Server configuration screen appears with a number of configuration subsets. The subsets that you see depend on whether you use the Basic View or the Advanced View and configuration entries you make in the Properties subset. Change views by using the View object selector at the top of the configuration pane.

[Table 3-1](#) identifies and describes virtual server configuration subsets with links to related topics for configuration information.

**Table 3-1 Virtual Server Configuration Subsets**

Configuration Subset	Description	Related Topics
Properties	This subset allows you to specify basic virtual server characteristics, such as the virtual server name, IP address, protocol, port, and VLANs.	<a href="#">Configuring Virtual Server Properties, page 3-7</a>
SSL Termination	This subset appears when TCP is the selected protocol and Other or HTTPS is the application protocol.  This subset allows you to configure the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients.	<a href="#">Configuring Virtual Server SSL Termination, page 3-13</a>
Protocol Inspection	This subset appears in the Advanced View for: <ul style="list-style-type: none"> <li>TCP with FTP, HTTP, HTTPS, RTSP, or SIP</li> <li>UDP with DNS or SIP</li> </ul> This subset appears in the Basic view for TCP with FTP.  This subset allows you to configure the virtual server so that it can verify protocol behavior and identify unwanted or malicious traffic passing through the ACE appliance on selected application protocols.	<a href="#">Configuring Virtual Server Protocol Inspection, page 3-14</a>
L7 Load-Balancing	This subset appears only in the Advanced View for: <ul style="list-style-type: none"> <li>TCP with Generic, HTTP, HTTPS, RTSP, or SIP</li> <li>UDP with Generic, RADIUS, or SIP</li> </ul> This subset allows you to configure Layer 7 load-balancing options, including SSL initiation.	<a href="#">Configuring Virtual Server Layer 7 Load Balancing, page 3-23</a>

**Table 3-1 Virtual Server Configuration Subsets (continued)**

Configuration Subset	Description	Related Topics
Default L7 Load-Balancing Action	This subset allows you to establish the default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions.  It also allows you to configure SSL initiation. SSL initiation appears only in the Advanced View.	<a href="#">Configuring Virtual Server Default Layer 7 Load Balancing, page 3-40</a>
Application Acceleration and Optimization	This subset appears only in the Advanced View and when HTTP or HTTPS is the selected application protocol.  This subset allows you to configure application acceleration and optimization options for HTTP or HTTPS traffic.	<a href="#">Configuring Application Acceleration and Optimization, page 3-42</a>
NAT	This subset appears in the Advanced View only.  This subset allows you to set up Name Address Translation (NAT) for the virtual server.	<a href="#">Configuring Virtual Server NAT, page 3-46</a>

**Step 3** When you finish configuring virtual server properties, click:

- **Deploy Now** to deploy the configuration on the ACE appliance.
- **Cancel** to exit the procedure without saving your entries and to return to the Virtual Servers table.

**Related Topic**

- [Configuring Virtual Servers, page 3-2](#)
- [Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 3-2](#)
- [Using ACE Appliance Device Manager to Configure Virtual Servers, page 3-3](#)
- [Shared Objects and Virtual Servers, page 3-6](#)
- [Role Mapping in ACE Appliance Device Manager, page 13-18](#)

## Shared Objects and Virtual Servers

A shared object is one that is used by multiple virtual servers. Examples of shared objects are:

- Action lists
- Class maps
- Parameter maps
- Real servers
- Server farms
- SSL services

- Sticky groups

Because these objects are shared, modifying an object's configuration in one virtual server can impact other virtual servers that use the same object.

### Configuring Shared Objects

ACE Appliance Device Manager offers the following options for shared objects in virtual server configuration screens (**Config > Virtual Contexts > context > Load Balancing > Virtual Servers**):

- View—Click **View** to review the object's configuration. The screen refreshes with read-only fields and the following three buttons.
- Cancel—Click **Cancel** to close the read-only view and to return to the previous screen.
- Edit—Click **Edit** to modify the selected object's configuration. The screen refreshes with fields that can be modified, except for the Name field which remains read-only.



---

**Note** Before changing a shared object's configuration, make sure you understand the effect of the changes on other virtual servers using the same object. As an alternative, consider using the Duplicate option instead.

---

- Duplicate—Click **Duplicate** to create a new object with the same configuration as the selected object. The screen refreshes with configurable fields. In the Name field, enter a unique name for the new object, then modify the configuration as desired. This option allows you to create a new object without impacting other virtual servers using the same object.

### Deleting Virtual Servers with Shared Objects

If you create a virtual server and include shared objects in its configuration, deleting the virtual server does not delete the associated shared objects. This ensures that other virtual servers using the same shared objects are not impacted.

### Related Topics

- [Managing Virtual Servers, page 3-47](#)
- [Configuring Virtual Server Properties, page 3-7](#)
- [Configuring Virtual Server SSL Termination, page 3-13](#)
- [Configuring Virtual Server Protocol Inspection, page 3-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 3-23](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 3-40](#)
- [Configuring Application Acceleration and Optimization, page 3-42](#)

## Configuring Virtual Server Properties

Use this procedure to configure virtual server properties.

### Procedure

- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.

**Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, then click **Edit** to modify it. The Virtual Server configuration screen appears. The Properties configuration subset is open by default. The fields that you see in the Properties configuration subset depend on whether you are using Advanced View or Basic View:

- To configure Advanced View properties, continue with [Step 3](#).
- To configure Basic View properties, continue with [Step 4](#).

**Step 3** To configure virtual server properties in the Advanced View, enter the information in [Table 3-2](#).

**Table 3-2** Virtual Server Properties – Advanced View

Field	Description
VIP Name	Enter the name for the virtual server.
VIP IP	Enter the IP address for the virtual server.
Netmask	Select the subnet mask to apply to the virtual server IP address.
Protocol	<p>Select the protocol the virtual server supports:</p> <ul style="list-style-type: none"> <li>• Any—Indicates the virtual server is to accept connections using any IP protocol.</li> <li>• TCP—Indicates that the virtual server is to accept connections that use TCP.</li> <li>• UDP—Indicates that the virtual server is to accept connections that use UDP.</li> </ul> <p><b>Note</b> This field is read-only if you are editing an existing virtual server. The Device Manager does not allow changes between protocols that require a change to the Layer 7 server load-balancing policy map. You need to delete the virtual server and create a new one with the desired protocol.</p>

**Table 3-2 Virtual Server Properties – Advanced View (continued)**

Field	Description
Application Protocol	<p>This field appears if TCP or UDP is selected. Select the application protocol to be supported by the virtual server.</p> <p><b>Note</b> This field is read-only if you are editing an existing virtual server. The Device Manager does not allow changes between protocols that require a change to the Layer 7 server load-balancing policy map. You need to delete the virtual server and create a new one with the desired application protocol.</p> <p>For TCP, the options are:</p> <ul style="list-style-type: none"> <li>• Other—Any protocol other than those specified.</li> <li>• HTTP—Hyper Text Transfer Protocol</li> <li>• HTTPS—HTTP over SSL</li> </ul> <p>If you select HTTPS, the SSL Termination configuration subset appears. See <a href="#">Configuring Virtual Server SSL Termination, page 3-13</a>.</p> <ul style="list-style-type: none"> <li>• FTP—File Transfer Protocol</li> <li>• RTSP—Real Time Streaming Protocol</li> <li>• RDP—Remote Desktop Protocol</li> <li>• Generic—Generic protocol parsing</li> <li>• SIP—Session Initiation Protocol</li> </ul> <p>For UDP, the options are:</p> <ul style="list-style-type: none"> <li>• Other—Any protocol other than those specified.</li> <li>• RTSP—Real Time Streaming Protocol</li> <li>• DNS—Domain Name System</li> <li>• RADIUS—Remote Authentication Dial-In User Service</li> <li>• Generic—Generic protocol parsing</li> <li>• SIP—Session Initiation Protocol</li> </ul> <p>If you select any specific application protocol, the Protocol Inspection configuration subset appears. See <a href="#">Configuring Virtual Server Protocol Inspection, page 3-14</a>.</p>
Port	<p>This field appears for any specified protocol.</p> <p>Enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as <b>10-20</b>. Enter <b>0</b> (zero) to indicate all ports.</p> <p>For a complete list of protocols and ports, see the Internet Assigned Numbers Authority available at <a href="http://www.iana.org/numbers.html">www.iana.org/numbers.html</a>.</p>
All VLANs	<p>Select the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.</p>

Table 3-2 Virtual Server Properties – Advanced View (continued)

Field	Description
VLAN	<p>This field appears if the All VLANs check box is cleared.</p> <p>In the Available Items list, select the VLANs to use for incoming traffic, then click <b>Add to Selection</b>. The items appear in the Selected Items list.</p> <p>To remove VLANs, select them in the Selected Items lists, then click <b>Remove from Selection</b>. The items appear in the Available Items list.</p> <p><b>Note</b> You cannot change the VLAN for a virtual server once it is specified. Instead, you need to delete the virtual server and create a new one with the desired VLAN.</p>
HTTP Parameter Map	<p>This field appears if HTTP or HTTPS is the selected application protocol.</p> <p>Select an existing HTTP parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See <a href="#">Shared Objects and Virtual Servers, page 3-6</a> for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the HTTP Parameter Map configuration pane appears. Configure the HTTP parameter map as described in <a href="#">Table 6-5</a>.</li> </ul>
Connection Parameter Map	<p>This field appears if TCP is the selected protocol.</p> <p>Select an existing connection parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See <a href="#">Shared Objects and Virtual Servers, page 3-6</a> for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the Connection Parameter Map configuration pane appears. Configure the connection parameter map as described in <a href="#">Table 6-2</a>.</li> </ul>
RTSP Parameter Map	<p>This field appears if RTSP is the selected application protocol over TCP.</p> <p>Select an existing RTSP parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See <a href="#">Shared Objects and Virtual Servers, page 3-6</a> for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the RTSP Parameter Map configuration pane appears. Configure the RTSP parameter map as described in <a href="#">Table 6-8</a>.</li> </ul>
Generic Parameter Map	<p>This field appears if Generic is the selected application protocol over TCP or UDP.</p> <p>Select an existing Generic parameter map or click <b>*New*</b> to create a new one.</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See <a href="#">Shared Objects and Virtual Servers, page 3-6</a> for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the Generic Parameter Map configuration pane appears. Configure the Generic parameter map as described in <a href="#">Table 6-4</a>.</li> </ul>

**Table 3-2** *Virtual Server Properties – Advanced View (continued)*

Field	Description
ICMP Reply	Indicate how the virtual server is to respond to ICMP ECHO requests: <ul style="list-style-type: none"> <li>• None—Indicates that the virtual server is not to send ICMP ECHO-REPLY responses to ICMP requests.</li> <li>• Active—Indicates that the virtual server is to send ICMP ECHO-REPLY responses only if the configured VIP is active.</li> <li>• Always—Indicates that the virtual server is always to send ICMP ECHO-REPLY responses to ICMP requests.</li> </ul>
Status	Indicate whether the virtual server is to be in service or out of service: <ul style="list-style-type: none"> <li>• In-Service—Enables the virtual server for load-balancing operations.</li> <li>• Out-of-Service—Disables the virtual server for load-balancing operations.</li> </ul>

**Step 4** To configure virtual server properties in the Basic View, enter the information in [Table 3-3](#).

**Table 3-3** *Virtual Server Properties – Basic View*

Field	Description
VIP Name	Enter the name for the virtual server.
VIP IP	Enter the IP address for the virtual server.
Protocol	Select the protocol that the virtual server supports: <ul style="list-style-type: none"> <li>• Any—Indicates that the virtual server is to accept connections using any IP protocol.</li> <li>• TCP—Indicates that the virtual server is to accept connections that use TCP.</li> <li>• UDP—Indicates that the virtual server is to accept connections that use UDP.</li> </ul>

**Table 3-3 Virtual Server Properties – Basic View (continued)**

Field	Description
Application Protocol	<p>Select the application protocol to be supported by the virtual server.</p> <p>For TCP, the options are:</p> <ul style="list-style-type: none"> <li>• Other—Any protocol other than those specified.</li> <li>• HTTP—Hyper Text Transfer Protocol</li> <li>• HTTPS—HTTP over SSL</li> </ul> <p>If you select HTTPS, the SSL Termination configuration subset appears. See <a href="#">Configuring Virtual Server SSL Termination, page 3-13</a>.</p> <ul style="list-style-type: none"> <li>• FTP—File Transfer Protocol</li> <li>• RTSP—Real Time Streaming Protocol</li> <li>• RDP—Remote Desktop Protocol</li> <li>• Generic—Generic protocol parsing</li> <li>• SIP—Session Initiation Protocol</li> </ul> <p>For UDP, the options are:</p> <ul style="list-style-type: none"> <li>• Other—Any protocol other than those specified.</li> <li>• RTSP—Real Time Streaming Protocol</li> <li>• DNS—Domain Name System</li> <li>• RADIUS—Remote Authentication Dial-In User Service</li> <li>• Generic—Generic protocol parsing</li> <li>• SIP—Session Initiation Protocol</li> </ul>
Port	<p>This field appears for any specified protocol.</p> <p>Enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as <b>10-20</b>. Enter <b>0</b> (zero) to indicate all ports.</p> <p>For a complete list of all protocols and ports, see the Internet Assigned Numbers Authority available at <a href="http://www.iana.org/numbers.html">www.iana.org/numbers.html</a>.</p>
All VLANs	<p>Select the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.</p>
VLAN	<p>This field appears if the All VLANs check box is cleared.</p> <p>In the Available Items list, select the VLANs to use for incoming traffic, then click <b>Add to Selection</b>. The items appear in the Selected Items list.</p> <p>To remove VLANs, select them in the Selected Items lists, then click <b>Remove from Selection</b>. The items appear in the Available Items list.</p> <p><b>Note</b> You cannot change the VLAN for a virtual server once it is specified. Instead, you need to delete the virtual server and create a new one with the desired VLAN.</p>

- Step 5** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy the configuration on the ACE appliance.

- **Cancel** to exit the procedure without saving your entries.

#### Related Topics

- [Configuring Virtual Servers, page 3-2](#)
- [Configuring Virtual Server SSL Termination, page 3-13](#)

## Configuring Virtual Server SSL Termination

SSL termination service allows the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients and then establishes a TCP connection to an HTTP server. When the ACE terminates the SSL connection, it decrypts the ciphertext from the client and transmits the data as clear text to an HTTP server.

Use this procedure to configure virtual server SSL termination service.

#### Assumption

A virtual server has been configured for HTTPS over TCP or Other over TCP in the Properties configuration subset. For more information, see [Configuring Virtual Server Properties, page 3-7](#).

#### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for SSL termination, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **SSL Termination**. The Proxy Service Name field appears.
- Step 4** In the Proxy Service Name field, select an existing SSL termination service, or select **\*New\*** to create a new SSL proxy service:
- If you select an existing SSL service, the screen refreshes and allows you to view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
  - If you select **\*New\***, the Proxy Service configuration subset appears.
- Step 5** Configure the SSL service using the in [Table 3-4](#).

**Table 3-4 Virtual Server SSL Termination Attributes**

Field	Description
Name	Enter a name for this SSL proxy service. Valid entries are alphanumeric strings with a maximum of 26 characters.
Key List	Select the SSL key pair to use during the SSL handshake for data encryption.
Certificate	Select the SSL certificate to use during the SSL handshake.
Chain Group	Select the chain group to use during the SSL handshake.
Auth Chain Group	Select the SSL authentication group to associate with this proxy server service.

**Table 3-4** Virtual Server SSL Termination Attributes (continued)

Field	Description
CRL Best-Effort	This option appears if you select an authentication group in the Auth Group Name field.  Select the check box to allow the ACE to search client certificates for the service to determine if it contains a CRL in the extension and retrieve the value, if it exists.  Clear the check box to disable this feature.
CRL Name	This option appears if the CRL Best-Effort check box is clear.  Select the Certificate Revocation List if the ACE is to use for this proxy service.
Parameter Map	Select the SSL parameter map to associate with this proxy server service.

For more information about SSL, see [Configuring SSL, page 7-1](#).

**Step 6** When you finish configuring virtual server properties, click:

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

#### Related Topics

- [Configuring Virtual Servers, page 3-2](#)
- [Configuring Virtual Server Properties, page 3-7](#)

## Configuring Virtual Server Protocol Inspection

Configuring protocol inspection allows the virtual server to verify protocol behavior and identify unwanted or malicious traffic passing through the ACE appliance.

In the Advanced View, protocol inspection configuration is available for the following virtual server protocol configurations:

- TCP with FTP, HTTP, HTTPS, RTSP, or SIP
- UDP with DNS or SIP

In the Basic View, protocol inspection configuration is available for TCP with FTP.

Use this procedure to configure protocol inspection on a virtual server.

#### Assumption

A virtual server has been configured to use one of the protocols that supports protocol inspection in the Properties configuration subset. See [Configuring Virtual Server Properties, page 3-7](#) for information on configuring these protocols.

### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to configure for protocol inspection, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Protocol Inspection**. The Enable Inspect check box appears.
- Step 4** Select the Enable Inspect check box to enable inspection on the specified traffic. Clear this check box to disable inspection on this traffic. By default, ACE appliances allow all request methods.
- Step 5** If you select the Enable Inspect check box, configure additional inspection options according to virtual server application protocol configuration:
- For DNS, in the Length field enter the maximum length of the DNS packet in bytes. Valid entries are from 512 to 65535 bytes. If you do not enter a value in this field, the DNS packet size is not checked.
  - For FTP, continue with [Step 6](#).
  - For HTTP and HTTPS, continue with [Step 7](#).
  - For SIP, continue with [Step 9](#).




---

**Note** There are no protocol-specific inspection options for RTSP.

---

- Step 6** For FTP protocol inspection:
- a. Select the Use Strict check box to indicate that the virtual server is to perform enhanced inspection of FTP traffic and enforce compliance with RFC standards. Clear this check box to indicate that the virtual server is not to perform enhanced FTP inspection.
  - b. If you select the Use Strict check box, in the Blocked FTP Commands field, identify the commands that are to be denied by the virtual server. See [Table 10-13](#) for more information about the FTP commands.
    - Select the commands that are to be blocked by the virtual server in the Available Items list, then click **Add**. The commands appear in the Selected Items list.
    - To remove commands that you do not want to be blocked, select them in the Selected Items list, then click **Remove**. The commands appear in the Available Items list.
- Step 7** For HTTP or HTTPS inspection:
- a. Select the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature 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. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic.
  - b. In the Policy subset, click **Add** to add a new match condition and action, or select an existing match condition and action, then click **Edit** to modify it. The Policy configuration pane appears.
  - c. In the Matches field, select an existing class map or **\*New\*** or **\*Inline Match\*** to configure new match criteria for protocol inspection.
 

If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
  - d. Configure match criteria and related actions by following the steps in [Table 3-5](#).

**Table 3-5 Protocol Inspection Match Criteria Configuration**

Selection	Action
Existing class map	<ol style="list-style-type: none"> <li>1. Click <b>View</b> to review the match condition information for the selected class map.</li> <li>2. Click: <ul style="list-style-type: none"> <li>– <b>Cancel</b> to continue without making changes and to return to the previous screen.</li> <li>– <b>Edit</b> to modify the existing configuration.</li> <li>– <b>Duplicate</b> to create a new class map with the same attributes without affecting other virtual servers using the same classmap.</li> </ul> <p>See <a href="#">Shared Objects and Virtual Servers, page 3-6</a> for more information about modifying shared objects.</p> </li> <li>3. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> <li>– <b>Permit</b>—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria.</li> <li>– <b>Reset</b>—Indicates that the specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.</li> </ul> </li> </ol>
*New*	<ol style="list-style-type: none"> <li>1. In the Name field, specify a unique name for this class map.</li> <li>2. In the Match field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> <li>– <b>Any</b>—Indicates that a match exists if at least one of the match conditions is satisfied.</li> <li>– <b>All</b>—Indicates that a match exists only if all match conditions are satisfied.</li> </ul> </li> <li>3. In the Conditions table, click <b>Add</b> to add a new set of conditions, or select an existing entry, then click <b>Edit</b> to modify it. The Type field appears.</li> <li>4. In the Type field, select the type of condition that is to be met for protocol inspection and configure protocol-specific criteria using the information in <a href="#">Table 3-6</a>.</li> <li>5. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> <li>– <b>Permit</b>—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria.</li> <li>– <b>Reset</b>—Indicates that the specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.</li> </ul> </li> </ol>
*Inline Match*	<ol style="list-style-type: none"> <li>1. In the Conditions Type field, select the type of inline match condition that is to be met for protocol inspection. <a href="#">Table 3-6</a> describes the types of conditions and their related configuration options.</li> <li>2. Provide condition-specific criteria using the information in <a href="#">Table 3-6</a>.</li> <li>3. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> <li>– <b>Permit</b>—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria.</li> <li>– <b>Reset</b>—Indicates that the specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.</li> </ul> </li> </ol>

**Table 3-6 HTTP and HTTPS Protocol Inspection Conditions and Options**

Condition	Description
None	No conditions are defined for application inspection decisions.
URL	<p>URL names are to be used for application inspection decisions.</p> <p>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 <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.</p>
URL Length	<p>URL length is to be used for application inspection decisions.</p> <p>In the URL Length field, enter the number of bytes to be used for application inspection decisions using one of the following formats:</p> <ul style="list-style-type: none"> <li>• <i>bytes</i>—Indicates that the URL length must equal the number of bytes specified. For example, <b>2048</b>.</li> <li>• <i>&gt;bytes</i>—Indicates that the URL length must be greater than the number of bytes specified. For example, <b>&gt;1026</b>.</li> <li>• <i>&lt;bytes</i>—Indicates that the URL length must be less than the number of bytes specified. For example, <b>&lt;512</b>.</li> <li>• <i>bytes1-bytes2</i>—Indicates that the URL length must fall within the range specified. For example, <b>1-300</b>.</li> </ul> <p>Valid entries are integers from 1 to 65535.</p>
Content	<p>Specific content contained within the HTTP entity-body is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Content field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255 bytes.</li> </ol>
Content Length	<p>The content parse length is used for application inspection decisions.</p> <p>In the Content Length field, enter the number of bytes to be used for application inspection decisions using one of the following formats:</p> <ul style="list-style-type: none"> <li>• <i>bytes</i>—Indicates that the content length must equal the number of bytes specified. For example, <b>2048</b>.</li> <li>• <i>&gt;bytes</i>—Indicates that the content length must be greater than the number of bytes specified. For example, <b>&gt;1026</b>.</li> <li>• <i>&lt;bytes</i>—Indicates that the content length must be less than the number of bytes specified. For example, <b>&lt;512</b>.</li> <li>• <i>bytes1-bytes2</i>—Indicates that the content length must fall within the range specified. For example, <b>1-300</b>.</li> </ul> <p>Valid entries are integers from 0 to 4294967295.</p>

Table 3-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Header	<p>The name and value in an HTTP header are used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. 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.</li> <li>2. 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. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. See <a href="#">Table 10-31</a> for a list of the supported characters that you can use in regular expressions.</li> </ol>
Header Length	<p>The length of the header in the HTTP message is used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Header Command field, specify whether HTTP header request or response messages are to be used for application inspection decisions: <ul style="list-style-type: none"> <li>– Request—Indicates that HTTP header request messages are to be checked for header length.</li> <li>– Response—Indicates that HTTP header response messages are to be checked for header length.</li> </ul> </li> <li>2. In the Header Length field, enter the number of bytes to be used for application inspection decisions using one of the following formats: <ul style="list-style-type: none"> <li>– <i>bytes</i>—Indicates that the header length must equal the number of bytes specified. For example, <b>248</b>.</li> <li>– <i>bytes</i>—Indicates that the header length must be greater than the number of bytes specified. For example, <b>&gt;126</b>.</li> <li>– <i>bytes</i>—Indicates that the header length must be less than the number of bytes specified. For example, <b>&lt;212</b>.</li> <li>– <i>bytes1-bytes2</i>—Indicates that the header length must fall within the range specified. For example, <b>1-30</b>.</li> </ul> <p>Valid entries are integers from 0 to 255.</p> </li> </ol>
Header MIME Type	<p>Multipurpose Internet Mail Extension (MIME) message types are used for application inspection decisions.</p> <p>In the MIME Type field, select the MIME message type to be used for this match condition.</p>
Port Misuse	<p>The misuse of port 80 (or any other port running HTTP) is to be used for application inspection decisions.</p> <p>Indicate the application category to be used for this match condition:</p> <ul style="list-style-type: none"> <li>• IM—Indicates that instant messaging applications are to be checked.</li> <li>• P2P—Indicates that peer-to-peer applications are to be checked.</li> <li>• Tunneling—Indicates that tunneling applications are to be checked.</li> </ul>
Request Method RFC	<p>A request method defined in RFC 2616 is to be used for application inspection decisions.</p> <p>In the RFC Request Method field, select the request method that is to be inspected.</p>

**Table 3-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)**

Condition	Description
Request Method EXT	An HTTP extension method is to be used for application inspection decisions. In the EXT Request Method field, select the HTTP extension request method that is to be inspected.
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: <ul style="list-style-type: none"> <li>• Chunked—The message body is transferred as a series of chunks.</li> <li>• Compress—The encoding format that is produced by the UNIX file compression program <i>compress</i>.</li> <li>• Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951.</li> <li>• Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952.</li> <li>• Identity—The default (identity) encoding which does not require the use of transformation.</li> </ul>
Strict HTTP	Compliance with HTTP RFC 2616 is to be used for application inspection decisions. <b>Note</b> Strict HTTP is only available as 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.
Content Type Verification	Verification of MIME-type messages with the header MIME-type is to be used for application inspection decisions. This option verifies that the header MIME-type value is in the internal list of supported MIME-types and that the header MIME-type matches the content in the data or body portion of the message. <b>Note</b> Content Type Verification is only available as 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.

- e. Click:
  - **OK** to save your entries. The Conditions table refreshes with the new entry.
  - **Cancel** to exit the Policy subset without saving your entries.
- f. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for protocol inspection are not met:
  - Permit—Indicates that the specified HTTP traffic is to be received by the virtual server.
  - Reset—Indicates that the specified HTTP traffic is to be denied by the virtual server
  - N/A—Indicates that this attribute is not set.

**Step 8** For SIP inspection:

- a. In the Actions subset, click **Add** to add a new match condition and action, or select an existing match condition and action, then click **Edit** to modify it. The Actions configuration pane appears.
- b. In the Matches field, select an existing class map or **\*New\*** or **\*Inline Match\*** to configure new match criteria for protocol inspection.

If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.

- c. Configure match criteria and related actions using the information in [Table 3-7](#).

**Table 3-7** *SIP Protocol Inspection Conditions and Options*

Condition	Description
None	No conditions are defined for application inspection decisions.
Message Path	<p>SIP inspection allows you to filter messages coming from or transiting through certain SIP proxy servers. The ACE maintains a list of the unauthorized SIP proxy IP addresses or URIs in the form of regular expressions and checks this list against the VIA header field in each SIP packet.</p> <p>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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p>
SIP Request Method	<p>A SIP request method is used for application inspection decisions.</p> <p>In the Request Method field, select the request method that is to be inspected.</p>
IM Subscriber	<p>An IM (instant messaging) subscriber is used for application inspection decisions.</p> <p>In the IP 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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p>
Third Party	<p>SIP allows users to register other users on their behalf by sending REGISTER messages with different values in the From and To header fields. This process can pose a security threat if the REGISTER message is actually a Deregister message. A malicious user could cause a DoS (denial-of-service) attack by deregistering all users on their behalf. To prevent this security threat, you can specify a list of privileged users who can register or unregister someone else on their behalf. The ACE maintains the list as a regex table. If you configure this policy, the ACE drops REGISTER messages with mismatched From and To headers and a From header value that does not match any of the privileged user IDs.</p> <p>In the Third Party Registration Entities field, enter a regular expression that identifies a privileged user who is authorized for third-party registrations. 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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p>

**Table 3-7 SIP Protocol Inspection Conditions and Options (continued)**

Condition	Description
URI Length	<p>The ACE can validate the length of SIP URIs or Tel URIs. A SIP URI is a user identifier that a calling party (source) uses to contact the called party (destination). A Tel URI is a telephone number that identifies the endpoint of a SIP connection. For more information about SIP URIs and Tel URIs, see RFC 2534 and RFC 3966, respectively.</p> <p>To filter SIP traffic based on URIs:</p> <ol style="list-style-type: none"> <li>In the URI Type field, indicate the type of URI to be used: <ul style="list-style-type: none"> <li>SIP URI—The calling party URI is to be used for this match condition.</li> <li>Tel URI—A telephone number is to be used for this match condition.</li> </ul> </li> <li>In the URI Operator field, confirm that Greater Than is selected.</li> <li>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.</li> </ol>
Called Party	<p>The destination or called party specified in the URI of the SIP To header is used for SIP protocol inspection decisions.</p> <p>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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p>
Calling Party	<p>The source or caller specified in the URI of the SIP From header is used for SIP protocol inspection decisions.</p> <p>In the Calling Party field, enter a regular expression that identifies the calling party in the URI of the SIP From 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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p>
SIP Content Type	<p>The content type in the SIP message body is used for SIP protocol inspection decisions.</p> <p>In the Content Type field, enter 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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p>
SIP Content Length	<p>The SIP message body content length is used for SIP protocol inspection decisions.</p> <p>To specify SIP traffic based on SIP message body length:</p> <ol style="list-style-type: none"> <li>In the Content Operator field, confirm that Greater Than is selected.</li> <li>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.</li> </ol>

- d. In the Action field, select the action that the virtual server is to take when the specified match conditions are met:
  - Permit—The specified SIP traffic is to be received by the virtual server.

- Drop—The specified SIP traffic is to be discarded by the virtual server.
  - Reset—The specified SIP traffic is to be denied by the virtual server.
- e. Click:
- **OK** to save your entries. The Conditions table refreshes with the new entry.
  - **Cancel** to exit the Conditions subset without saving your entries and to return to the Conditions table.
- f. In the SIP Parameter Map field, select an existing parameter map or select **\*New\*** to configure a new one.
- If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
- g. Configure SIP parameter map options using the information in [Table 6-9](#).
- h. In the Secondary Connection Parameter Map field, select an existing parameter map or select **\*New\*** to configure a new one.
- If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
- i. Configure secondary connection parameter map options using the information in [Table 6-2](#).
- j. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for SIP protocol inspection are not met:
- Permit—The specified SIP traffic is to be received by the virtual server.
  - Drop—The specified SIP traffic is to be discarded by the virtual server.
  - Reset—The specified SIP traffic is to be denied by the virtual server.
- k. Select the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature 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. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic.

**Step 9** When you finish configuring virtual server properties, click:

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

---

#### Related Topics

- [Configuring Virtual Server Properties, page 3-7](#)
- [Configuring Virtual Server SSL Termination, page 3-13](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 3-23](#)

## Configuring Virtual Server Layer 7 Load Balancing

Layer 7 load balancing is available for virtual servers configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

See [Configuring Virtual Server Properties, page 3-7](#) for information on configuring these protocols.

Use this procedure to configure Layer 7 load balancing on a virtual server.

### Assumption

A virtual server has been configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
  - Step 2** Select the virtual server you want to configure for Layer 7 load balancing, then click **Edit**. The Virtual Server configuration screen appears.
  - Step 3** Click **L7 Load-Balancing**. The Layer 7 Load-Balancing Rule Match table appears.
  - Step 4** In the Rule Match table, click **Add** to add a new match condition and action, or select an existing match condition and action, then click **Edit** to modify it. The Rule Match configuration pane appears.
  - Step 5** In the Rule Match field, select an existing class map or **\*New\*** or **\*Inline Match\*** to configure new match criteria for Layer 7 load balancing:
    - If you select an existing class map, click **View** to review, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
    - If you click **\*New\*** or **\*Inline Match\***, the Rule Match configuration subset appears.
  - Step 6** Configure match criteria by following the steps in [Table 3-8](#).

**Table 3-8 Layer 7 Load-Balancing Match Criteria Configuration**

Selection	Action
Existing class map	<ol style="list-style-type: none"> <li>1. Click <b>View</b> to review the match condition information for the selected class map.</li> <li>2. Click: <ul style="list-style-type: none"> <li>– <b>Cancel</b> to continue without making changes and to return to the previous screen.</li> <li>– <b>Edit</b> to modify the existing configuration.</li> <li>– <b>Duplicate</b> to create a new class map with the same attributes without affecting other virtual servers using the same classmap.</li> </ul> </li> </ol> <p>See <a href="#">Shared Objects and Virtual Servers, page 3-6</a> for more information about modifying shared objects.</p>
<b>*New*</b>	<ol style="list-style-type: none"> <li>1. In the Name field, enter a unique name for this class map.</li> <li>2. In the Match field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> <li>– Match Any—Indicates that a match exists if at least one of the match conditions is satisfied.</li> <li>– Match All—Indicates that a match exists only if all match conditions are satisfied.</li> </ul> </li> <li>3. In the Conditions table, click <b>Add</b> to add a new set of conditions or select an existing entry, then click <b>Edit</b> to modify it.</li> <li>4. In the Type field, select the match condition and configure any protocol-specific options: <ul style="list-style-type: none"> <li>– For Generic protocol options, see <a href="#">Table 10-8</a>.</li> <li>– For HTTP and HTTPS protocol options, see <a href="#">Table 3-9</a>.</li> <li>– For RADIUS protocol options, see <a href="#">Table 10-9</a>.</li> <li>– For RTSP protocol options, see <a href="#">Table 10-10</a>.</li> <li>– For SIP protocol options, see <a href="#">Table 10-11</a>.</li> </ul> </li> <li>5. Configure any condition-specific options using the information in <a href="#">Table 3-9</a>.</li> <li>6. Click: <ul style="list-style-type: none"> <li>– <b>OK</b> to accept your entries and to return to the Conditions table.</li> <li>– <b>Cancel</b> to exit this procedure without saving your entries and to return to the Conditions table.</li> </ul> </li> </ol>
<b>*Inline Match*</b>	<p>In the Conditions Type field, select the type of inline match condition and configure any protocol-specific options:</p> <ul style="list-style-type: none"> <li>• For Generic protocol options, see <a href="#">Table 10-8</a></li> <li>• For HTTP and HTTPS protocol options, see <a href="#">Table 3-9</a></li> <li>• For RADIUS protocol options, see <a href="#">Table 10-9</a></li> <li>• For RTSP protocol options, see <a href="#">Table 10-10</a></li> <li>• For SIP protocol options, see <a href="#">Table 10-11</a></li> </ul>

**Table 3-9 Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration**

Match Condition	Description
Http-cookie	<p>Indicates that HTTP cookies are to be used for this rule.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</li> <li>Select the Secondary Cookie Matching check box to indicate that the ACE appliance is to use both the cookie name and the cookie value to satisfy this match condition. Clear this check box to indicate that the ACE appliance is to use either the cookie name or the cookie value to satisfy this match condition.</li> </ol> <p>This field does not appear for inline match conditions.</p>
Http-header	<p>Indicates that the HTTP header and a corresponding value are to be used for this rule.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. <a href="#">Table 10-31</a> lists the supported characters that you can use in regular expressions.</li> </ol>
Http-url	<p>Indicates that this rule is to perform regular expression matching against the received packet data from a particular connections based on the HTTP URL string.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>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 <code>www.hostname.domain</code> in the match statement. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>. To match the <code>www.anydomain.com</code> portion, the URL string can take the form of a URL regular expression. The ACE appliance supports regular expressions for matching URL strings. <a href="#">Table 10-31</a> lists the supported characters that you can use in regular expressions.</li> <li>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).</li> </ol>

**Table 3-9** Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration (continued)

Match Condition	Description
Source-address	<p>Indicates that this rule is to use a client source IP address to establish match conditions.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the Source Address field, enter the source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).</li> <li>2. In the Netmask field, select the subnet mask to apply to the source IP address.</li> </ol>
Class-map	<p>Indicates that this rule is to use an existing class map to establish match conditions.</p> <p>If you select this method, in the Classmap field, select the class map to be used.</p> <p><b>Note</b> This option is not available for inline match conditions.</p>
Http-content	<p>Specific content contained within the HTTP entity-body is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset 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.</li> </ol>

**Table 3-9 Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration (continued)**

Match Condition	Description
SSL	<p>Defines load balancing decisions based on the specific SSL cipher or cipher strength. 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.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the SSL Cipher Match Type field, select the match type. Options include: <ul style="list-style-type: none"> <li>- Equal-to—Specifies an SSL cipher for the load balancing decision.</li> <li>- Less-than—Specifies SSL cipher strength for the load balancing decision.</li> </ul> </li> <li>2. If you selected Equal-to, in the Cipher Name field specify an SSL cipher for the load balancing decision. The possible values include: <ul style="list-style-type: none"> <li>- RSA_EXPORT1024_WITH_DES_CBC_SHA</li> <li>- RSA_EXPORT1024_WITH_RC4_56_MD5</li> <li>- RSA_EXPORT1024_WITH_RC4_56_SHA</li> <li>- RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>- RSA_EXPORT_WITH_RC4_40_MD5</li> <li>- RSA_WITH_3DES_EDE_CBC_SHA</li> <li>- RSA_WITH_AES_128_CBC_SHA</li> <li>- RSA_WITH_AES_256_CBC_SHA</li> <li>- RSA_WITH_DES_CBC_SHA</li> <li>- RSA_WITH_RC4_128_MD5</li> <li>- RSA_WITH_RC4_128_SHA</li> </ul> </li> <li>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.</li> </ol> <p>The possible values include:</p> <ul style="list-style-type: none"> <li>- 128—128-bit strength</li> <li>- 168—168-bit strength</li> <li>- 256—256-bit strength</li> <li>- 56—56-bit strength</li> </ul>
Layer4-payload	The virtual server is to stick client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet.
Calling-station-id	The virtual server is to stick client connections based on the RADIUS framed IP attribute and the calling station ID attribute.
Username	The virtual server is to stick client connections based on the RADIUS framed IP attribute and the username attribute.

**Table 3-9** Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration (continued)

Match Condition	Description
RTSP-header	The virtual server is to stick client connections to the same real server based on the RTSP Session header field.
SIP-header	The virtual server is to stick client connections to the same real server based on the SIP Call-ID header field

- Step 7** In the Primary Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria:
- Drop—Indicates that client requests for content are to be discarded when match conditions are met. Continue with [Step 10](#).
  - Forward—Indicates that client requests for content are to be forwarded without performing load balancing on the requests when match conditions are met. Continue with [Step 10](#).
  - Load Balance—Indicates that client requests for content are to be directed to a server farm when match conditions are met. Continue with [Step 8](#).
  - Sticky—Client requests for content are handled by a sticky group when match conditions are met. Continue with [Step 8](#).
- Step 8** If you select Load Balance as the primary action, you can configure load balancing using a server farm, a server farm/backup server farm pair, an existing sticky group, or a new sticky group.



**Note** If you select an existing object in any of these scenarios, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects in virtual servers.

Configure load balancing using the information in [Table 3-10](#).

**Table 3-10** Virtual Server Load-Balancing Options

To configure...	Do this...
Load balancing using a server farm	In the Server Farm field, select the server farm to be used for load balancing for this virtual server, or select <b>*New*</b> to configure a new server farm (see <a href="#">Table 3-11</a> ).
Load balancing using a server farm/backup server farm pair	<ol style="list-style-type: none"> <li>1. In the Server Farm field, select the primary server farm to use for load balancing, or select <b>*New*</b> to configure a new server farm (see <a href="#">Table 3-11</a>).</li> <li>2. In the Backup Server Farm field, select the server farm to act as the backup server farm for load balancing if the primary server farm is unavailable, or select <b>*New*</b> to configure a new backup server farm (see <a href="#">Table 3-11</a>).</li> </ol>

Table 3-10 Virtual Server Load-Balancing Options (continued)

To configure...	Do this...
Load balancing using an existing sticky group	<ol style="list-style-type: none"> <li>1. In the Server Farm field, select the primary server farm to use for load balancing. This must be the primary server farm specified in the existing sticky group.</li> <li>2. In the Backup Server Farm field, select the backup server farm to use for load balancing. This must be the backup server farm specified in the existing sticky group.</li> <li>3. In the Sticky Group field, select the sticky group to use.</li> </ol> <p><b>Note</b> Sticky groups appear in the Sticky Group field <b>only</b> when their configured primary and backup server farms are selected, respectively. If you select a sticky group and then select a different primary or backup server farm, the sticky group that you selected in the Sticky Group field no longer appears. To change an existing sticky group configuration, modify it in the Stickiness configuration screen (<b>Config &gt; Virtual Contexts &gt; context &gt; Load Balancing &gt; Stickiness</b>).</p>
Load balancing using a new sticky group	<ol style="list-style-type: none"> <li>1. In the Server Farm field, select the primary server farm to use for load balancing, or select <b>*New*</b> to configure a new server farm (see <a href="#">Table 3-11</a>).</li> <li>2. In the Backup Server Farm field, select the server farm to act as the backup server farm for load balancing if the primary server farm is unavailable, or select <b>*New*</b> to configure a new backup server farm (see <a href="#">Table 3-11</a>).</li> <li>3. In the Sticky Group field, select <b>*New*</b>, then configure a new sticky group using the information in <a href="#">Table 3-13</a>.</li> </ol> <p><b>Note</b> The context in which you configure a sticky group must be associated with a resource class that allocates a portion of ACE appliance resources to stickiness. See <a href="#">Managing Resource Classes, page 2-28</a> for more information on resource classes.</p>

**Table 3-11**      **New Server Farm Attributes**

Field	Description
Name	Enter a unique name for this server farm. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Type	<p>Select the type of server farm:</p> <ul style="list-style-type: none"> <li>• <b>Host</b>—A typical server farm that consists of real servers that provide content and services to clients.</li> </ul> <p>By default, if you configure a backup server farm and all real servers in the primary server farm go down, the primary server farm fails over to the backup server farm. Use the following options to specify thresholds for failover and returning to service.</p> <ol style="list-style-type: none"> <li>a. In the Partial Threshold Percentage field, enter the minimum percentage of real servers in the primary server farm that must remain active for the server farm to stay up. If the percentage of active real servers falls below this threshold, the ACE takes the server farm out of service. Valid entries are integers from 0 to 99.</li> <li>b. In the Back Inservice field, enter the percentage of real servers in the primary server farm that must be active again for the ACE to place the server farm back into service. Valid entries are integers from 0 to 99. The value in this field should be larger than the value in the Partial Threshold Percentage field.</li> </ol> <ul style="list-style-type: none"> <li>• <b>Redirect</b>—A server farm that consists only of real servers that redirect client requests to alternate locations specified in the real server configuration.</li> </ul>
Fail Action	<p>Select the action the ACE appliance is to take with respect to connections if any real server in the server farm fails:</p> <ul style="list-style-type: none"> <li>• <b>N/A</b>—Indicates that the ACE appliance is to take no action if any server in the server farm fails.</li> <li>• <b>Purge</b>—Indicates that the ACE appliance is to remove connections to a real server if that real server in the server farm fails. The ACE appliance sends a reset command to both the client and the server that failed.</li> </ul>
Transparent	<p>This field appears only for real servers identified as host servers.</p> <p>Specify whether network address translation from VIP address to server IP is to occur:</p> <ul style="list-style-type: none"> <li>• <b>N/A</b>—Indicates that the default value is to be used; the default value is False.</li> <li>• <b>False</b>—Indicates that network address translation from VIP address to server IP address is not to occur.</li> <li>• <b>True</b>—Indicates that network address translation from VIP address to server IP address is to occur.</li> </ul>
Predictor	<p>Specify the method for selecting the next server in the server farm to respond to client requests. Roundrobin is the default predictor method for a server farm.</p> <p>See <a href="#">Table 3-12</a> for the supported predictor methods and configurable attributes for each predictor method.</p>

Table 3-11 New Server Farm Attributes (continued)

Field	Description
Probe	<p>Specify the health monitoring probes to use:</p> <ul style="list-style-type: none"> <li>• To include a probe that you want to use for health monitoring, select it in the Available Items list, then click <b>Add</b>. The probe appears in the Selected Items list.</li> <li>• To remove a probe that you do not want to use for health monitoring, select it in the Selected Items list, then click <b>Remove</b>. The probe appears in the Available Items list.</li> <li>• To specify a sequence for probe use, select probes in the Selected Items list, then click <b>Up</b> or <b>Down</b> until you have the desired sequence.</li> <li>• Click <b>Create</b> to add a new probe. See <a href="#">Configuring Health Monitoring for Real Servers, page 4-23</a>.</li> <li>• Select a probe in the list on the right, then click <b>View</b> to review its configuration.</li> </ul> <p>After you add a probe, you can modify the attributes for a health probe from the Health Monitoring table (<b>Config &gt; Virtual Contexts &gt; context &gt; Load Balancing &gt; Health Monitoring</b>) as described in <a href="#">Configuring Health Monitoring for Real Servers, page 4-23</a>. You can also delete an existing health probe from the Health Monitoring table.</p>
Real Servers	<p>The Real Servers table allows you to add, modify, remove, or change the order of real servers.</p> <ol style="list-style-type: none"> <li>1. Select an existing server, or click <b>Add</b> to add a server to the server farm: <ul style="list-style-type: none"> <li>– If you select an existing server, you can view, modify, or duplicate the server’s existing configuration. See <a href="#">Shared Objects and Virtual Servers, page 3-6</a> for more information about modifying shared objects.</li> <li>– If you click <b>Add</b>, the table refreshes and allows you to enter server information.</li> </ul> </li> <li>2. In the IP Address field, enter the IP address of the real server in dotted-decimal format.</li> <li>3. In the Name field, enter the name of the real server.</li> <li>4. In the Port field, enter the port number to be used for server port address translation (PAT). Valid entries are integers from 1 to 65535.</li> <li>5. In the Weight field, enter the weight to assign to this server in the server farm. Valid entries are integers from 1 to 100, and the default is 8.</li> <li>6. In the Rate Bandwidth, field, specify the real server bandwidth limit in bytes per second. Valid entries are integers from 1 to 300000000.</li> <li>7. In the Rate Connection field, specify the limit for connections per second. Valid entries are integers from 1 to 350000.</li> <li>8. In the State field, select the administrative state of this server: <ul style="list-style-type: none"> <li>– Inservice—The server is to be placed in use as a destination for server load balancing</li> <li>– Out of Service—The server is not to be placed in use by a server load balancer as a destination for client connections.</li> <li>– Inservice Standby—The server is a backup server and is to remain inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.</li> </ul> </li> <li>9. Click: <ul style="list-style-type: none"> <li>– <b>OK</b> to accept your entries and add this real server to the server farm. The table refreshes with updated information.</li> <li>– <b>Cancel</b> to exit this procedure without saving your entries and to return to the Real Servers table.</li> </ul> </li> </ol>

Table 3-12 Predictor Methods and Attributes

Predictor Method	Description / Action
hash_address	<p>Indicates that the ACE appliance is to select the server using a hash value based on the source or destination IP address.</p> <p>To configure the hash address predictor method:</p> <ol style="list-style-type: none"> <li>In the Mask Type field, indicate whether server selection is based on source IP address or the destination IP address: <ul style="list-style-type: none"> <li>N/A—Indicates that this option is not defined.</li> <li>Source—Indicates that the server is selected based on the source IP address.</li> <li>Destination—Indicates that the server is selected based on the destination IP address.</li> </ul> </li> <li>In the IP Netmask field, select the subnet mask to apply to the address. If none is specified, the default is 255.255.255.255.</li> </ol>
hash_content	<p>The ACE selects the server by using a hash value based on the specified content string of the HTTP packet body.</p> <ol style="list-style-type: none"> <li>In the Begin Pattern field, enter the beginning pattern of the content string and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the Length field, enter the length in bytes of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. <p>The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.</p> <p><b>Note</b> You cannot specify both the length and the end-pattern options for a Hash Content predictor.</p> </li> <li>In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.</li> </ol>

Table 3-12 Predictor Methods and Attributes (continued)

Predictor Method	Description / Action
hash_cookie	<p>Indicates that the ACE appliance is to select the server by using a hash value based on the cookie name.</p> <p>In the Cookie Name field, enter a cookie name in the form of an unquoted text string with no spaces and a maximum of 64 characters.</p>
hash_header	<p>Indicates that the ACE appliance is to select the server by using a hash value based on the header name.</p> <p>In the Header Name field, select the HTTP header to be used for server selection:</p> <ul style="list-style-type: none"> <li>To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button and enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</li> <li>To specify one of the standard HTTP headers, select the second radio button, then select one of the HTTP headers from the list.</li> </ul>
hash_layer 4	<p>The ACE selects the server by using a Layer 4 generic protocol load-balancing method. Use this predictor to load balance packets from protocols that are not explicitly supported by the ACE.</p> <ol style="list-style-type: none"> <li>In the Begin Pattern field, enter the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>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. <a href="#">Table 10-31</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the Length field, enter the length in bytes of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. <p>The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.</p> <p><b>Note</b> You cannot specify both the length and end-pattern options for a Hash Layer 4 predictor.</p> </li> <li>In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.</li> </ol>

Table 3-12 Predictor Methods and Attributes (continued)

Predictor Method	Description / Action
hash_url	<p>Indicates that the ACE appliance is to select the server using a hash value based on the URL. Use this method to load balance firewalls.</p> <p>Enter values in one or both of the pattern fields:</p> <ul style="list-style-type: none"> <li>In the URL Begin Pattern field, enter the beginning pattern of the URL and the pattern string to parse.</li> <li>In the URL End Pattern field, enter the ending pattern of the URL and the pattern string to parse.</li> </ul> <p>Valid entries for these fields are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters for each pattern you configure.</p>
leastbandwidth	<p>The ACE selects the server with the least amount of network traffic over a specified sampling period.</p> <ol style="list-style-type: none"> <li>In the Assess Time field, enter the number of seconds for which the ACE is to collect traffic information. Valid entries are integers from 1 to 10 seconds.</li> <li>In the Least Bandwidth Samples field, enter the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).</li> </ol>
leastconnections	<p>Indicates that the ACE appliance is to select the server with the fewest number of connections.</p> <p>In the Slowstart Duration field, enter the slow-start value to be applied to this predictor method. Valid entries are integers from 1 to 65535, where 1 is the slowest ramp-up value.</p> <p>The slow-start mechanism is used to avoid sending a high rate of new connections to servers that you have just put into service.</p>
leastloaded	<p>The ACE selects the server with the lowest load based on information from SNMP probes.</p> <ol style="list-style-type: none"> <li>In the SNMP Probe Name field, select the name of the SNMP probe to use.</li> <li>In the Auto Adjust field, configure the autoadjust feature to assign a maximum load value of 16000 to that server to prevent it from being flooded with new incoming connections. The ACE periodically adjusts this load value based on feedback from the server's SNMP probe and other configured options. Options include: <ul style="list-style-type: none"> <li>N/A—Indicates that this option is not defined.</li> <li>Average—Instructs the ACE to apply the average load of the server farm to a real server whose load reaches zero. The average load is the running average of the load values across all real servers in the server farm.</li> <li>Off—Overrides the default behavior of the ACE of setting the load value for a server with a load of zero to 16000. When you configure this parameter, the ACE sends all new connections to the server that has a load of zero until the next load update arrives from the SNMP probe for this server. There may be times when you want the ACE to send all new connections to a real server whose load is zero.</li> </ul> </li> <li>In the Weight Connection field, select the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.</li> </ol>

**Table 3-12** *Predictor Methods and Attributes (continued)*

<b>Predictor Method</b>	<b>Description / Action</b>
response	<p>The ACE selects the server with the lowest response time for a requested response-time measurement.</p> <ol style="list-style-type: none"> <li>1. In the Response Type field, select the type of measurement to use: <ul style="list-style-type: none"> <li>– App-req-to-req—The response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.</li> <li>– Syn-to-close—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server.</li> <li>– Syn-to-synack—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a SYN-ACK from the server.</li> </ul> </li> <li>2. In the Response Samples field, enter the number of samples over which you want to average the results of the response-time measurement. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).</li> </ol>
roundrobin	Indicates that the ACE appliance is to select the next server in the list of servers based on server weight. This is the default predictor method.

**Table 3-13 Sticky Type Attributes**

Field	Description
Group Name	Enter a unique identifier for the sticky type. You can either accept the automatically incremented entry given or you can enter your own. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Sticky Type	<p>Select the method to be used when establishing sticky connections:</p> <ul style="list-style-type: none"> <li>• HTTP Cookie—Indicates that the virtual server is either to learn a cookie from the HTTP header of a client request or to insert a cookie in the Set-Cookie header of the response from the server to the client, and then use the learned cookie to provide stickiness between the client and server for the duration of the transaction.</li> <li>• HTTP Header—Indicates that the virtual server is to stick client connections to the same real server based on HTTP headers.</li> <li>• IP Netmask—Indicates that the virtual server is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both.</li> </ul> <p><b>Note</b> If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence.</p> <ul style="list-style-type: none"> <li>• HTTP Content—The virtual server is to stick client connections to the same real server based on a string in the data portion of the HTTP packet. See <a href="#">Table 5-2</a> for additional configuration options.</li> <li>• Layer 4 Payload—The virtual server is to stick client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. See <a href="#">Table 5-6</a> for additional configuration options.</li> <li>• RADIUS—The virtual server is to stick client connections to the same real server based on a RADIUS attribute. See <a href="#">Table 5-7</a> for additional configuration options.</li> <li>• RTSP Header—The virtual server is to stick client connections to the same real server based on the RTSP Session header field. <a href="#">Table 5-8</a> for additional configuration options.</li> <li>• SIP Header—The virtual server is to stick client connections to the same real server based on the SIP Call-ID header field.</li> </ul>
Cookie Name	<p>This option appears for sticky type HTTP Cookie.</p> <p>Enter a unique identifier for the cookie. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</p>
Enable Insert	<p>This option appears for sticky type HTTP Cookie.</p> <p>Select this check box if the virtual server is to insert a cookie in the Set-Cookie header of the response from the server to the client. This option is useful when you want to use a session cookie for persistence but the server is not currently setting the appropriate cookie. When selected, the virtual server selects a cookie value that identifies the original server from which the client received a response. For subsequent connections of the same transaction, the client uses the cookie to stick to the same server.</p> <p>Clear this check box to disable cookie insertion.</p>

**Table 3-13** *Sticky Type Attributes (continued)*

Field	Description
Browser Expire	This option appears for sticky type HTTP Cookie and you select Enable Insert. Select this check box to allow the client's browser to expire a cookie when the session ends. Clear this check box to disable browser expire.
Offset	This option appears for sticky types HTTP Cookie and HTTP Header. Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.
Length	This option appears for sticky types HTTP Cookie and HTTP Header. Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE appliance is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.
Secondary Name	This option appears for sticky type HTTP Cookie. Enter an alternate cookie name that is to appear in the URL string of the Web page on the server. The virtual server uses this cookie to maintain a sticky connection between a client and a server and adds a secondary entry in the sticky table. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Header Name	This option appears for sticky type HTTP Header. Select the HTTP header to use for sticking client connections.
Netmask	This field appears for sticky type IP Netmask. Select the netmask to apply to the source IP address, destination IP address, or both.
Address Type	This field appears for sticky type IP Netmask. Indicate whether this sticky type is to be applied to the client source IP address, the destination IP address, or both: <ul style="list-style-type: none"> <li>• Both—Indicates that this sticky type is to be applied to both the source IP address and the destination IP address.</li> <li>• Source—Indicates that this sticky type is to be applied to the source IP address only.</li> <li>• Destination—Indicates that this sticky type is to be applied to the destination IP address only.</li> </ul>
Aggregate State	Select this check box to indicate that the state of the primary server farm is to be tied to the state of all real servers in the server farm and in the backup server farm, if configured. The ACE appliance declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down. Clear this check box if the state of the primary server farm is not to be tied to all real servers in the server farm and in the backup server farm.
Sticky Enabled	Select this check box to indicate that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky.
Replicate	Select this check box to indicate that the virtual server is to replicate sticky table entries on the backup server farm. If a failover occurs and this option is selected, the new active server farm can maintain the existing sticky connections. Clear this check box to indicate that the virtual server is not to replicate sticky table entries on the backup server farm.

Table 3-13 Sticky Type Attributes (continued)

Field	Description
Timeout	Enter the number of minutes that the virtual server keeps the sticky information for a client connection in the sticky table after the latest client connection terminates. Valid entries are integers from 1 to 65535; the default is 1440 minutes (24 hours).
Timeout Active Connections	Select this check box to specify that the virtual server is to time out sticky table entries even if active connections exist after the sticky timer expires.  Clear this check box to specify that the virtual is not to time out sticky table entries even if active connections exist after the sticky timer expires. This is the default behavior.

- Step 9** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the appliance compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.



**Note** By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

Options include:

- deflate—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. deflate, the data format for compression described in RFC1951
- gzip—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.
- N/A—HTTP compression is disabled.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/\*).
- Minimum size—512 bytes.
- User agent—None.

- Step 10** In the SSL Initiation field, select an existing service, or select **\*New\*** to create a new service. SSL initiation allows the virtual server to act as an SSL proxy client to initiate and maintain an SSL connection between itself and an SSL server. In this particular application, the ACE receives clear text from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the ACE decrypts the ciphertext that it receives from the SSL server and sends the data to the client as clear text.



**Note** The SSL Initiation field appears only in the Advanced View, and when TCP is the selected protocol and Other, HTTP, or HTTPS is the application protocol.

- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
- If you select **\*New\***, configure the service using the information in [Table 3-14](#).

**Table 3-14 Virtual Server SSL Initiation Attributes**

Field	Description
Name	Enter a name for this SSL proxy service. Valid entries are alphanumeric strings with a maximum of 26 characters.
Key List	Select the SSL key pair to use during the SSL handshake for data encryption.
Certificate	Select the SSL certificate to use during the SSL handshake.
Chain Group	Select the chain group to use during the SSL handshake.
Auth Chain Group	Select the SSL authentication group to associate with this proxy server service.
CRL Best-Effort	This option appears if you select an authentication group in the Auth Group Name field.  Select the check box to allow the ACE to search client certificates for the service to determine if it contains a CRL in the extension and retrieve the value, if it exists.  Clear the check box to disable this feature.
CRL Name	This option appears if the CRL Best-Effort check box is clear.  Select the Certificate Revocation List if the ACE is to use for this proxy service.
Parameter Map	Select the SSL parameter map to associate with this proxy server service.

For more information about SSL, see [Configuring SSL, page 7-1](#).

**Step 11** In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format ***header\_name=header\_value*** where:

- ***header\_name*** represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
- ***header\_value*** represents the 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. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 10-31](#) lists the supported characters that you can use in regular expressions.

For example, you might enter **Host=www.cisco.com**.

**Step 12** Click:

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

**Step 13** When you finish configuring virtual server properties, click:

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

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

**Related Topics**

- [Configuring Virtual Servers, page 3-2](#)
- [Configuring Virtual Server Properties, page 3-7](#)
- [Configuring Virtual Server SSL Termination, page 3-13](#)
- [Configuring Virtual Server Protocol Inspection, page 3-14](#)

## Configuring Virtual Server Default Layer 7 Load Balancing

Use this procedure to configure default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions.

**Assumption**

A virtual server has been configured. See [Configuring Virtual Servers, page 3-2](#) for information on configuring a virtual server.

**Procedure**

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for default Layer 7 load balancing, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Default L7 Load-Balancing Action**. The Default L7 Load-Balancing Action configuration pane appears.
- Step 4** In the Primary Action field, indicate the default action the virtual server is to take in response to client requests for content when specified match conditions are not met:
- **Drop**—Indicates that client requests that do not meet specified match conditions are to be discarded. Continue with [Step 6](#).
  - **Forward**—Indicates that client requests that do not meet specified match conditions are to be forwarded without performing load balancing on the requests. Continue with [Step 6](#).
  - **Load Balance**—Indicates that client requests for content are to be directed to a server farm. If you select Load Balance, server farm, backup server farm, and sticky configuration options appear. Continue with [Step 5](#).
  - **Sticky**—Client requests for content are handled by a sticky group when match conditions are met. Continue with [Step 5](#).
- Step 5** If you select Load Balance as the primary action, you can configure load balancing using a server farm, a server farm/backup server farm pair, an existing sticky group, or a new sticky group.



**Note** If you select an existing object in any of these scenarios, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects in virtual servers.

---

Configure load-balancing using the information in [Table 3-10](#).

- Step 6** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the appliance compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.



**Note** By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

Options include:

- deflate—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. deflate, the data format for compression described in RFC1951
- gzip—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.
- N/A—HTTP compression is disabled.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/\*).
- Minimum size—512 bytes.
- User agent—None.

- Step 7** In the SSL Initiation field, select an existing service, or select **\*New\*** to create a new service. SSL initiation allows the virtual server to act as an SSL proxy client to initiate and maintain an SSL connection between itself and an SSL server. In this particular application, the ACE receives clear text from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the ACE decrypts the ciphertext that it receives from the SSL server and sends the data to the client as clear text.



**Note** The SSL Initiation field appears only in the Advanced View, and when TCP is the selected protocol and Other, HTTP, or HTTPS is the application protocol.

- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
- If you select **\*New\***, configure the service using the information in [Table 3-14](#).

For more information about SSL, see [Configuring SSL, page 7-1](#).

- Step 8** In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format *header\_name=header\_value* where:

- **header\_name** represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
- **header\_value** represents the 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. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 10-31](#) lists the supported characters that you can use in regular expressions.

For example, you might enter `Host=www.cisco.com`.

**Step 9** When you finish configuring virtual server properties, click:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

---

#### Related Topics

- [Configuring Virtual Server Properties, page 3-7](#)
- [Configuring Virtual Server SSL Termination, page 3-13](#)
- [Configuring Virtual Server Protocol Inspection, page 3-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 3-23](#)

## Configuring Application Acceleration and Optimization

The ACE appliance includes configuration options that allow you to accelerate enterprise applications, resulting in increased employee productivity, enhanced customer retention, and increased online revenues. The application acceleration functions of the ACE appliance apply several optimization technologies to accelerate Web application performance. The application acceleration functionality in the ACE appliance enables enterprises to optimize network performance and improve access to critical business information. This capability accelerates the performance of Web applications, including customer relationship management (CRM), portals, and online collaboration by up to 10 times.

Refer to [Configuring Application Acceleration and Optimization, page 11-1](#) or the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for more information about application acceleration and optimization.

Use this procedure to configure acceleration and optimization on virtual servers.

#### Assumption

A virtual server has been configured. See [Configuring Virtual Servers, page 3-2](#) for information on configuring a virtual server.

#### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for optimization, then click **Edit**. The Virtual Server configuration screen appears.

- Step 3** Click **Application Acceleration and Optimization**. The Application Acceleration and Optimization configuration pane appears.
- Step 4** In the Configuration field, indicate the method you want to use to configure application acceleration and optimization:
- EZ—Indicates that you want to use standard acceleration and optimization options. Continue with [Step 5](#).
  - Custom—Indicates that you want to associate specific match criteria, actions, and parameter maps for application acceleration and optimization for this virtual server. If you choose this option, continue with [Step 6](#).
- Step 5** If you select EZ, the Latency Optimization (FlashForward) and Bandwidth Optimization (Delta) fields appear.
- a. Select the Latency Optimization (FlashForward) check box to indicate that the ACE appliance is to use bandwidth reduction and download acceleration techniques to objects embedded within HTML pages. Clear this check box to indicate that the ACE appliance is not to employ these techniques to objects embedded within HTML pages. Latency optimization corresponds to FlashForward functionality. For more information about FlashForward functionality, see [Optimization Overview, page 11-1](#).
  - b. Select the Bandwidth Optimization (Delta) check box to indicate that the ACE appliance is to dynamically update client browser caches with content differences, or deltas. Clear this check box to indicate that the ACE appliance is not to dynamically update client browser caches. Bandwidth optimization corresponds to action list Delta optimization. For more information about Delta optimization, see [Optimization Overview, page 11-1](#) and [Configuring an HTTP Optimization Action List, page 11-3](#).
  - c. Continue with [Step 11](#).
- Step 6** If you select Custom, the Actions configuration pane appears with a table listing match criteria and actions. Click **Add** to add an entry to this table, or select an existing entry, then click **Edit** to modify it. The configuration subset refreshes with the available configuration options.
- Step 7** In the Apply Template field, select one of the configuration templates for the type of optimization you want to configure, or leave blank to configure optimization without a template:
- Bandwidth Optimization—Maximizes bandwidth for Web-based traffic.
  - Latency Optimization for Embedded Objects—Reduces the latency associated with embedded objects in Web-based traffic.
  - Latency Optimization for Embedded Images—Reduces the latency associated with embedded images in Web-based traffic.
  - Latency Optimization for Containers—Reduces the latency associated with Web containers.
- If you do not select a template and select **\*New\*** in the Rule Match and Actions fields, you are creating your own optimization rules and actions.
- Step 8** In the Rule Match field, select an existing class map or click **\*New\*** to specify new match criteria:
- If you select an existing class map, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
  - If you click **\*New\***, the screen refreshes with the default configuration settings for the template you selected. You can accept the default settings or modify them using the information in [Table 3-15](#).

**Table 3-15 Optimization Rule Match Configuration Options**

Field	Description
Name	Enter a unique name for this match criteria rule.
Match	Select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> <li>Match Any—A match exists if at least one of the match conditions is satisfied.</li> <li>Match All—A match exists only if all match conditions are satisfied.</li> </ul>
Conditions	Click <b>Add</b> to add a new set of conditions or select an existing entry, then click <b>Edit</b> to modify it: <ol style="list-style-type: none"> <li>In the Type field, select the match condition to be used, then configure any condition-specific options using the information in <a href="#">Table 3-16</a>.</li> <li>Click <b>OK</b> to save your entries, or <b>Cancel</b> to exit this procedure without saving your entries.</li> </ol>

**Step 9** In the Actions field, select an existing action list to use for optimization or click **\*New\*** to create a new action list.

- If you select an existing optimization action list, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 3-6](#) for more information about modifying shared objects.
- If you click **\*New\***, the screen refreshes with the default configuration settings for the template you selected. You can accept the default settings or modify them using the information in [Table 3-16](#).

**Table 3-16 Optimization Action List Configuration Options**

Field	Description
Action List Name	Enter a unique name for the optimization action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Enable Delta	Delta optimization dynamically updates client browser caches directly with content differences, or deltas, resulting in faster page downloads. Select this check box to enable delta optimization for the specified URLs. Clear this check box to disable delta optimization for the specified URLs. <b>Note</b> The ACE restricts you from enabling delta optimization if you have previously specified either Cache Dynamic or Dynamic Etag.
Enable AppScope	AppScope runs on the Management Console of the optional Cisco AVS 3180A Management Station and measures end-to-end application performance. Select this check box to enable AppScope performance monitoring for use with the ACE appliance. Clear this check box to disable AppScope performance monitoring for use with the ACE appliance.

**Table 3-16 Optimization Action List Configuration Options (continued)**

Field	Description
FlashForward	<p>The FlashForward feature reduces bandwidth usage and accelerates embedded object downloading by combining local object storage with dynamic renaming of embedded objects, thereby enforcing object freshness within the parent HTML page.</p> <p>Specify how the ACE appliance is to implement FlashForward:</p> <ul style="list-style-type: none"> <li>• N/A—Indicates that this feature is not enabled.</li> <li>• FlashForward—Indicates that FlashForward is to be enabled for the specified URLs and that embedded objects are to be transformed.</li> <li>• FlashForward Object—Indicates that FlashForward static caching is to be enabled for the objects that the corresponding URLs refer to, such as Cascading Style Sheets (CSS), JPEG, and GIF files.</li> </ul>
Cache Dynamic	<p>Select this check box to enable Adaptive Dynamic Caching for the specified URLs even if the expiration settings in the response indicate that the content is dynamic. The expiration of cache objects is controlled by the cache expiration settings based on time or server load.</p> <p>Clear this check box to disable this feature.</p> <p><b>Note</b> The ACE restricts you from enabling Cache Dynamic if you have previously specified either Enable Delta or Dynamic Etag.</p>
Cache Forward	<p>Select this check box to enables the cache forward feature for the corresponding URLs. Cache forward allows the ACE to serve the object from its cache (static or dynamic) even when the object has expired if the maximum cache TTL time period has not yet expired (set by specifying the Cache Time-to-Live Duration (%): field in an Optimization parameter map). At the same time, the ACE sends an asynchronous request to the origin server to refresh its cache of the object.</p> <p>Clear this check box to disable this feature.</p>
Dynamic Etag	<p>This feature enables the acceleration of noncacheable embedded objects, which results in improved application response time. When enabled, this feature eliminates the need for users to download noncacheable objects on each request.</p> <p>Select this check box to indicate that the ACE appliance is to implement just-in-time object acceleration for noncacheable embedded objects.</p> <p>Clear this check box to disable this feature.</p> <p><b>Note</b> The ACE restricts you from enabling Dynamic Etag if you have previously specified either Enable Delta or Cache Dynamic.</p>
Fine Tune Optimization Parameters	<p>Click this header to configure additional optimization attributes. When expanded, the configuration pane displays options specific to the type of optimization you are configuring and features that you enable.</p> <p>Refer to <a href="#">Table 6-6</a> for information about specific options that appear.</p>

- Step 10** When you finish configuring match criteria and actions, click:
- **OK** to save your entries and to return to the Rule Match and Actions table.
  - **Cancel** to exit this procedure without saving your entries and to return to the Rule Match and Actions table.

- Step 11** When you finish configuring virtual server properties, click:
- **Deploy Now** to save your entries. The ACE appliance validates the optimization action list configuration and deploys it on the ACE appliance.
  - **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

#### Related Topics

- [Configuring Virtual Server Properties, page 3-7](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 11-2](#)
- [Configuring Traffic Policies for HTTP Optimization, page 11-6](#)
- [Configuring Virtual Server Protocol Inspection, page 3-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 3-23](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 3-40](#)

## Configuring Virtual Server NAT

Use this procedure to configure Name Address Translation (NAT) for virtual servers.

#### Assumptions

- A virtual server has been configured. See [Configuring Virtual Servers, page 3-2](#) for information on configuring a virtual server.
- A VLAN has been configured. See [Configuring Virtual Context VLAN Interfaces, page 8-6](#) for information on configuring a VLAN interface.
- At least one NAT pool has been configured on a VLAN interface. See [Configuring VLAN Interface NAT Pools, page 8-13](#) for information on configuring a NAT pool.

#### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for NAT, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **NAT**. The NAT table appears.
- Step 4** Click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it.
- Step 5** In the VLAN field, select the VLAN you want to use NAT. For more information about NAT, see [Configuring VLAN Interface NAT Pools, page 8-13](#).
- Step 6** In the NAT Pool ID field, select the NAT pool that you want to associate with the selected VLAN.
- Step 7** Click:
- **OK** to save your entries and to return to the NAT table. The NAT table refreshes with the new entry.
  - **Cancel** to exit the procedure without saving your entries and to return to the NAT table.

- Step 8** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE appliance.
  - **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

#### Related Topics

- [Configuring Virtual Servers, page 3-2](#)
- [Configuring Virtual Server Properties, page 3-7](#)
- [Configuring Virtual Server SSL Termination, page 3-13](#)
- [Configuring Virtual Server Protocol Inspection, page 3-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 3-23](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 3-40](#)

## Managing Virtual Servers

After you have created a virtual server the following options are available:

Task	Related Topics
Modify a virtual server configuration	<a href="#">Configuring Virtual Servers, page 3-2</a>
List virtual servers by virtual context	<a href="#">Viewing Virtual Servers by Context, page 3-48</a>
Activate a virtual server	<a href="#">Activating Virtual Servers, page 3-48</a>
Suspend a virtual server	<a href="#">Suspending Virtual Servers, page 3-49</a>
View detailed information about a virtual server and its configured state	<a href="#">Viewing Detailed Virtual Server Information, page 3-49</a>

## Viewing Virtual Servers by Context

Use this procedure to view all virtual servers associated with a virtual context.

### Procedure

---

- Step 1** Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.
- Step 2** Select the context associated with the virtual servers you want to view, then select **Load Balancing > Virtual Servers**. The Virtual Servers table appears with the following information:
- Virtual server name
  - Configured state, such as Inservice
  - IP address
  - Port
  - Associated VLANs
  - Associated server farms
- 

### Related Topics

- [Configuring Virtual Servers, page 3-2](#)
- [Managing Virtual Servers, page 3-47](#)

## Activating Virtual Servers

Use this procedure to activate a virtual server.

### Procedure

---

- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the server that you want to activate, then click **Activate**. The server is activated and the screen refreshes with updated information in the Configured State column.
- 

### Related Topics

- [Managing Virtual Servers, page 3-47](#)
- [Viewing All Virtual Servers, page 3-50](#)
- [Suspending Virtual Servers, page 3-49](#)

## Suspending Virtual Servers

Use this procedure to suspend a virtual server.

### Procedure

- 
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the server that you want to suspend, then click **Suspend**. The server is taken out of service and the screen refreshes with updated information in the Configured State column.
- 

### Related Topics

- [Managing Virtual Servers, page 3-47](#)
- [Viewing All Virtual Servers, page 3-50](#)
- [Activating Virtual Servers, page 3-48](#)

## Viewing Detailed Virtual Server Information

Use this procedure to view detailed information about the state of a virtual server.

### Procedure

- 
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server whose configuration details you want to view, then click **Details**. The Details window appears with the following information:
- Current operational status
  - Description, if one was entered
  - Configured interfaces, such as VLANs
  - Configured service policies including:
    - Configured class maps, detailed by type (such as load balancing or inspection)
    - States of configured options, indicated by word (**ACTIVE**, **DISABLED**, **OUTOFSERVICE**) and color (green, orange/yellow, and red)
    - Associated policy maps with details on their type and action (L7 loadbalance, serverfarm)
    - Statistics regarding connections and counts

### Related Topics

- [Configuring Virtual Servers, page 3-2](#)
- [Managing Virtual Servers, page 3-47](#)

## Viewing All Virtual Servers

To view all virtual servers, select **Config > Operations > Virtual Servers**. The Virtual Servers table appears with the following information for each server:

- Server name, grouped by virtual context
- Configured state
- IP address
- Port
- VLANs
- Server farms
- Virtual context

You can activate or suspend virtual servers from this table and obtain additional information about the state of the virtual server.

### Related Topics

- [Activating Virtual Servers, page 3-48](#)
- [Suspending Virtual Servers, page 3-49](#)
- [Viewing Detailed Virtual Server Information, page 3-49](#)

## Configuring Secure KAL-AP

A keepalive-appliance protocol (KAL-AP) on the ACE allows communication between the ACE and the Global Site Selector (GSS), which send KAL-AP requests, to report the server states and loads for global-server load-balancing (GSLB) decisions. The ACE uses KAL-AP through a UDP connection to calculate weights and provide information for server availability to the KAL-AP device. The ACE acts as a server and listens for KAL-AP requests. When KAL-AP is initialized on the ACE, the ACE listens on the standard 5002 port for any KAL-AP requests. You cannot configure any other port.

The ACE supports secure KAL-AP for MD5 encryption of data between it and the GSS. For encryption, you must configure a shared secret as a key for authentication between the GSS and the ACE context.

Use this procedure to configure secure KAL-AP associated with a virtual context.

### Assumptions

- You have created a virtual context that specifies the Keepalive Appliance Protocol over UDP.
- You have enabled KAL-AP on the ACE by configuring a management class map and policy map, and apply it to the appropriate interface.

### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Secure KAL-AP**. The Secure KAL-AP table appears.
- Step 2** Click **Add** to configure secure KAL-AP for MD5 encryption of data . The Secure KAL-AP configuration screen appears.

**Step 3** In the IP Address field, enable secure KAL-AP by configuring the VIP address for the GSS. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

In the Hash Key field, enter the MD5 encryption method shared secret between the KAL-AP device and the ACE. Enter the shared secret as a case-sensitive string with no spaces and a maximum of 31 alphanumeric characters. The ACE supports the following special characters in a shared secret:

, . / = + - ^ @ ! % ~ # \$ \* ( )

**Step 4** Click:

- **Deploy Now** to save your entries. The ACE appliance validates the secure KAL-AP configuration and deploys it.
  - **Cancel** to exit this procedure without accepting your entries and to return to the Secure KAL-AP table.
  - **Next** to accept your entries.
- 

#### Related Topics

- [Creating Virtual Contexts, page 2-2](#)
- [Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 10-13](#)

