CHAPTER 15

Working with Ports and Hostnames

This section describes how to open ports on the ACE XML Gateway to listen for client HTTP or HTTPS requests. It covers these topics:

About HTTP Ports

Clients access applications proxied by the ACE XML Gateway by addressing requests at the port number specified in its consumer interface. You can open an HTTP listening port on the ACE XML Gateway, and manage its configuration settings, using a port object. Port objects are created for you when you define new virtual web applications or virtual web services through the WSDL import process. However, you can also create them manually or modify existing definitions.

The ACE XML Gateway policy includes a built-in listening port for HTTP port 80. You can open additional listening ports using the HTTP Port policy object. You may need to open additional ports, for example, for SSL-secured connections (conventionally on port 443). After adding the listening port, you apply it to a virtual service or virtual web application to have requests for the service handled on the port.

Note The built-in default HTTP port (80) cannot be deleted, since it is used by certain internal system processes. However, you can edit the built-in port object by changing its name, port number, or other values from the Open HTTP(S) Ports page.

The port object contains settings that allow you to set up a name-based or IP-based virtual host for the ACE XML Gateway. The port can be configured to listen for traffic addressed to a particular hostname or IP address.

A port can be configured to respond to requests at a particular URL with a static response message. This capability is most often used to enable health monitoring of the ACE XML Gateway by upstream load balancers or other network hosts.

If response compression is enabled on a port definition, the ACE XML Gateway compresses responses that exceed the configured size threshold. The client must indicate by an Accept-Encoding header in the incoming request that it accepts compressed responses.

Note In the ACE XML Gateway chunked requests can be handled by the Reactor only. That is, the Flex Path does not support chunked requests (requests that indicate chunked transfer encoding). If it receives a chunked request, the ACE XML Gateway responds with a 411 error response code. Chunked responses from the backend server are supported, but for messages handled by the Flex Path, the Gateway assembles the chunked response prior to delivery to the client. Chunked responses handled by the Reactor are passed through chunked.

Opening a Port

To open a listening port on the ACE XML Gateway:

Step 1 While logged into the web console as an `Administrator` user or as a `Privileged` user with the `Routing` role, set the active subpolicy to the one in which you want to use the port.

Step 2 Click the **HTTP Ports & Hostnames** link in the navigation menu.

Step 3 In the **Open HTTP(S) Ports** page, click the **Add a New Port** button.

Step 4 In the **Edit Port** page, type a descriptive name for the new port definition in the **Name** field. This name identifies the port in the ACE XML Manager's console. It should be unique for port objects in the policy.

Step 5 Type the listening port number in the **Port Number** field.

Note To ensure proper operation of the system, be sure to avoid using port numbers reserved for administrative purposes by the ACE XML Gateway and Manager. These include ports in the range of 8200 through 8299 and 514. For a complete list of ports that may be used by the system, see *Cisco ACE XML Gateway Administration Guide*.

Step 6 To have the ACE XML Gateway apply transport layer security to traffic on the port, select the **SSL** checkbox.

The **Public/Private Keypairs** menu and **Upload** button are enabled.

Step 7 If SSL is enabled, choose an item from the **Public/Private Keypair** menu to specify the public/private keypair to be used for encrypting this connection.

If the correct keypair does not appear in the menu, it needs to be uploaded to the policy using the **Upload** button. For more information on SSL, see "Securing Traffic with SSL/TLS" section on page 19-195

Step 8 Optionally, specify the ciphers to be accepted in negotiating SSL connections with clients on this port in the SSL Cipher Suite menu. In the course of negotiating a secure connection, the ACE XML Gateway and client must be able to agree on the cipher suite to use for the connection. If the client does not support any cipher you specify here, the connection is not permitted.

By default, the connection will use the global SSL Cipher Suite settings for the HTTP server process of the ACE XML Gateway, as set in the **System Management > I/O Settings** page. This option lets you apply more specific settings for this port.

Specify a cipher suite by choosing custom from the SSL Cipher Suite menu and in the field that appears, enter the cipher suite to be accepted in OpenSSL Cipher string format, described here: http://www.openssl.org/docs/apps/ciphers.html

Note Use care when entering the cipher suite string. The ACE XML Manager web console interface does not verify the value you enter. If you mistype or enter a meaningless value, the ACE XML Gateway may not be able to open an SSL connection with the server.

Step 9 The port can listen for all traffic on this port or only for traffic on this port addressed to a particular host or IP address. This setting allows you to set up virtual hosts (vhosts) at the ACE XML Gateway, by either hostname and IP address.

Specify the requests this port is to monitor from the **Listen For** menu, from these options:

- All traffic on this port—The port listens for any traffic addressed to the Gateway on this port.
- Requests to a hostname—The port listens for any traffic addressed to the Gateway on this port and to this hostname. Specify one or more hostnames by typing the literal hostname or a POSIX 1003.2 regular expression in the **Hostname** field. To use a regular expression, click the **Allow regular expression matching in the hostname** checkbox.
- Requests to specific IP addresses—The port listens for any traffic addressed to this IP address. Enter one or more IP addresses in the **IP Addresses** field. Use paragraph returns to separate multiple IP addresses, so that each address is on its own line.

  Any IP address you enter must also be configured at the network interface for each Gateway appliance. For more information, see the *Cisco ACE XML Gateway Administration Guide*.

Step 10 You can serve a static response message at a particular URL on this port by choosing the **serve the following static page on this port** option from the **Static Content** menu.

For more information, see "Configuring a Static Content Response" section on page 15-162.

Step 11 If desired, enable response compression on this port by enabling the Compression option. Also, indicate the minimum size of messages to be compressed, 2KB by default. For more information, see "Compressing Responses" section on page 15-164.

Step 12 Choose the **Flex Path** option if you want message handling at this port to bypass the Reactor process. If a task defined for a Gateway service is not supported by the Reactor (such as protocol mediation), the Reactor automatically hands off the request message for flex path processing. After the response has complete processing, including a possible round trip to the service, it is handed back to Reactor for delivery back to the client.

To ensure compatibility with external clients, you may wish to disable Reactor on the port by choosing this option. In general, it is recommended that you use Reactor in production systems only after careful testing for interoperability with the client. Also, for performance reasons, the Reactor performs less logging than the flex path. For this reason, you may wish to disable Reactor during initial policy development.

Note For systems upgraded to release 5.0, this option is enabled by default for port objects that existed in the policy prior to the upgrade.

Step 13 Click **Save Changes**.

The port now appears in the **HTTP Port** menu in virtual service configuration pages.

Listening on a Virtual Hostname

The ACE XML Gateway supports IP-based and name-based virtual hosting. This support allows the Gateway to serve as a reverse proxy for multiple addressable hosts. The virtual hostname settings for the ACE XML Gateway appear in the port object configuration in the policy.

A virtual hostname on a port directs the ACE XML Gateway to service requests addressed to the specified hostname. You can configure multiple ports in the policy to listen on a single port number, but each on a different hostname or IP address.

To set a virtual hostname for the ACE XML Gateway, follow these steps:

Step 1 Create or modify the port object on which you would like the ACE XML Gateway to listen to requests for the host. For more information on creating port objects, see "Opening a Port" section on page 15-160.

Step 2 In the Listen For menu, choose **requests to a hostname**, for name-based virtual hosting, or **requests to specific IP addresses**, for IP-based virtual hosting.

Step 3 If you configured the port to listen for requests to an IP address, specify the IP addresses in the text field. The IP addresses you enter must also be configured on the network interface of the ACE XML Gateway appliance. For more information, see the *Cisco ACE XML Gateway Administration Guide*.

Step 4 If you configured the port to listen for requests to a hostname, enter the hostname in the text field. You can use regular expression matching for the hostname by checking the Allow regular expression matching in the hostname box and entering the hostname as a regular expression, such as:

^example$ | example:80 | example.cisco.com |

In this case, the port accepts requests in which the host is addressed as example (as a whole word), example.cisco.com, or example:80. Note that with regular expression matching enabled, a value in host of simply "example" would match any request URL in which "example" appears as a substring, which may or may not be as intended.

Step 5 Click **Save Changes** when finished and deploy the policy to have the changes take effect at the ACE XML Gateway.

Configuring a Static Content Response

The ACE XML Gateway can be configured to serve a static response message at a particular URL on a port. Other network elements (such as load balancers) can use this mechanism to perform health checks against the ACE XML Gateway. You can set up a static response in the form of an HTML page, SOAP response, text only response, and more.

There are a few points to note regarding static response pages:

- A virtual host configuration for a port (that is, a particular configuration in the **Listen For** option) does not affect the static page response. That is, if you configure port 8080, for instance, to listen only for requests to the hostname "mygateway," the static content page will be served for a request to the configured URL path at port 8080, regardless of the hostname requested.
- Load balancers sometimes send HEAD method requests for health checks on balanced devices. The response page on the port automatically responds to HEAD method requests as well as GET requests.
- If you enable compression on the port, compression does not apply to the static response.

To set up a static response:

Step 1 Create or edit a port object, as described in "Opening a Port" section on page 15-160

Step 2 From the **Static Content** menu, choose the option **serve the following static page on this port**.

Step 3 For the **Path**, specify the URL path for addressing the response.

Step 4 Choose the type of response from the **Content-Type** menu:

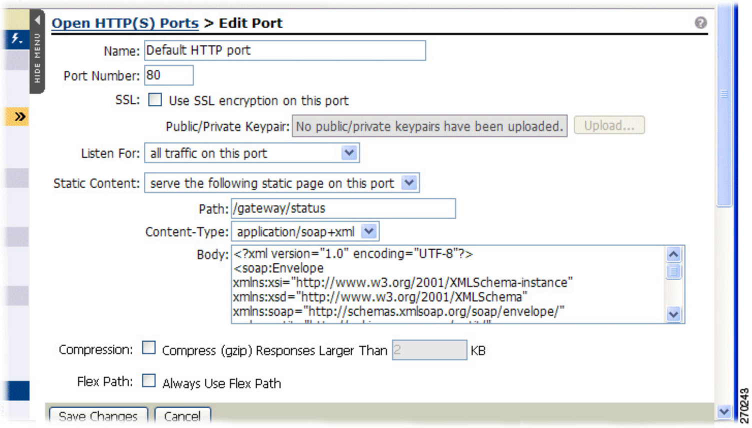
- HTML
- XML
- SOAP
- Text
- or a custom response

Notice that you need to enter the appropriate body content given the response content type. For HTML, for instance, this means that appropriate markup tags are included in the response.

Step 5 In the **Body** field, enter the body of the response message.

The body needs to include markup tags appropriate for the content type you chose, if appropriate. For example, for a SOAP message, the body must include the XML element and envelope markup, as in the following figure.

Figure 15-1 Static Content Message Configuration



Open HTTP(S) Ports > Edit Port

Name: Default HTTP port

Port Number: 80

SSL: □ Use SSL encryption on this port

Public/Private Keypair: No public/private keypairs have been uploaded.

Listen For: all traffic on this port

Static Content: serve the following static page on this port

Path: /gateway/status

Content-Type: application/soap+xml

Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
```

Compression: □ Compress (gzip) Responses Larger Than 2 KB

Flex Path: □ Always Use Flex Path

Step 6 Click **Save Changes** to commit changes to the working policy.

When the policy is deployed, the page is available at the ACE XML Gateway address, such as:

```
http://xmlgate.example.com:80/gateway/status
```

Compressing Responses

The ACE XML Gateway can optimize traffic by compressing outgoing responses that exceed a configurable size. When response compression is enabled on a port, the Gateway compresses responses for clients who indicate acceptance of compressed responses in the HTTP `Accept-Encoding` header of the request, as in the following sample header:

```
Accept-Encoding: compress, gzip
```

The ACE XML Gateway compresses qualifying responses using the GZIP compression format.

Only responses on virtual services that use Flex Path processing can be compressed. That is, the Reactor does not support response compression. If you are enabling response compression on a port that otherwise permits Reactor processing (that is, it does not have the **Flex Path** option enabled), you should check whether the virtual service for which you want compression uses Reactor processing. If it does and response compression is important for your application, you may wish to force Flex Path processing for the service by choosing the "Always use Flex Path" setting for the service.

Note For more information on Reactor and Flex Path processing, see Chapter 20, "Configuring Reactor Processing."

The ACE XML Gateway will not attempt to apply additional compression to a response that has already been returned from the backend system in compressed form. This option should be enabled in the policy only if you want compression to be initiated at the ACE XML Gateway.

Note To have backend systems perform response compression instead of the Gateway, you will need to configure passthrough for the Accept-Encoding HTTP header in the request. Unless specifically configured for propagation to the outgoing request, this header is removed from requests at the ACE XML Gateway.

To configure response compression:

Step 1 In the Open HTTP(S) Ports page, click the **edit** link for the port for which you would like to configure compression.

Step 2 Check the **Compression** checkbox.

Step 3 If desired, change the default message size that triggers response compression. Responses smaller than this size are not compressed. The default is 2 kilobytes.

Step 4 Click **Save Changes** and deploy the policy to have your changes take effect at the Gateway.

When a response message is compressed, the event is indicated in the event log at the notice level. Information level event log items indicate whether a message is smaller or larger than the compression threshold. For a compressed response, the event log indicates the size of the message before and after compression as follows:

```
Returning response 200 for request message to client; 379 bytes
Compressed Response From 1802 bytes to 379 bytes
This message will be compressed on its way out
Message size is larger than or equal to compression threshold (1KB)
```

If message logging is enabled for the service for which a response has been compressed, the message is logged in its form prior to compression; that is, the message log doesn't show the message in compressed format.