CHAPTER 2

Planning the Installation

This chapter describes planning considerations for installing Cisco ACE XML Gateway and Manager appliances. It covers these topics:

Considerations for the Installation Target Network

To perform its daily operations, the ACE XML Gateway relies on a variety of agreements, protocols, and physical connections. Implementing the ACE XML Gateway involves not only configuring settings on the appliance itself, but configuring settings to accommodate the appliance in the target network (for example, by configuring adjacent firewalls or remote network management devices).

The appliances can be deployed to several types of target environments:

- In a production environment, one or more ACE XML Gateways are typically deployed to the network DMZ, often behind a load balancer. In this setting, the Gateway receives client requests from outside the network and passes them back through the load balancer to destination servers within the organization.
- During policy development or testing, the ACE XML Gateway usually resides within a protected network.
- The ACE XML Manager normally resides in the internal, protected network, where it is not exposed to external traffic. However, it needs to be able to connect to each ACE XML Gateway, and be available to policy developers.

In production deployments, the ACE XML Gateway and Manager usually require access to external networks. Depending on your network topology, you may need to configure an outgoing HTTP proxy for the appliances. The ACE XML Gateway and Manager use the proxy for all outbound HTTP connections. The HTTP Proxy settings are individually configurable for Gateway and Manager appliances, as set in the System Management page of the web console. For more information, see the Manager online help available from the web console.

Ports Used by the ACE XML Gateway and Manager

For appliances to function properly in your network, you need to ensure that existing network devices (such as internal firewalls) permit the types of traffic used by the appliances.

In particular, the firewalls affected by an ACE XML Gateway and Manager installation may include:

- Firewalls between each ACE XML Gateway and the Manager that controls it.
- Firewalls between the Manager and the computer used to access the web console.
- Firewalls between the Gateway and the external network.

The following sections list the ports that may need to be opened.

System Traffic Ports

The following ports are used by the system for operation purposes (that is, for traffic other than service traffic). This information should be used to configure internal firewalls. The use of a port is implementation-specific. For example, if you do not use NTP, you do not have to configure firewall to permit TCP/UDP traffic on port 123.

The ACE XML Manager uses the following ports and protocols:

- ICMP from anywhere
- TCP on port 22 from anywhere. This port exposes SSH, for administrators who want to start terminal sessions on the Manager.
- TCP on port 8243 from anywhere. This port exposes the Manager web console for browser access.

  Optionally, you can configure the Manager to present its web console on another port.
- UDP on port 53 from anywhere. The Manager uses this port to perform DNS lookups.
- UDP on port 161 from anywhere. This port enables the Manager to receive SNMP queries.
- UDP on port 514 from ACE XML Gateways. The Manager listens on this port to receive syslog information from the Gateways. This information is aggregated to make up the event logs.

On the Gateway, traffic is passed on the following ports and protocols:

- ICMP from anywhere
- TCP on port 22 from anywhere. This port exposes SSH, for the sake of administrators who want to start terminal sessions on the Gateway.
- TCP on port 8200 only from the Manager. The Gateway requires this port to be open so that it can receive control messages from its Manager.
- UDP on port 53 from anywhere. This port enables the Gateway to perform DNS lookups.
- UDP on port 161 from anywhere. This port enables the Gateway to receive SNMP queries.

Each Gateway sends traffic to its Manager on the ports opened on the Manager for that purpose. Additionally, the Manager and Gateway appliances may generate network traffic on the following ports:

- TCP/UDP on port 123, for Network Time Protocol (NTP).
- TCP on port 25, to send email alerts via SMTP.
- UDP on port 162, for SNMP traps.

Service Traffic Ports

In addition to allowing traffic for ports required for system traffic mentioned in "System Traffic Ports" section on page 2-6, firewalls need to allow traffic on service ports configured in the ACE XML Gateway policy.

The ports used for service traffic vary by policy, but generally include ports 80 and 443, for standard HTTP and HTTPS traffic, respectively.

Considerations for Load Balancers

Best performance can usually be achieved by placing multiple ACE XML Gateways behind one or more load-balancing devices. In general, you do not need to place a load balancer ahead of a dedicated Manager, since it is not usually subject to high volumes of traffic.

Load balancers are used to ensure high availability of the Gateway or to balance the workload. The number of load balancers to use depends on the amount of traffic you expect each Gateway to handle, as well as the specifications of the load balancers. For assistance in determining the number of load balancers you'll need, contact the manufacturer of the load balancer.

In general, configuring a load balancer for the ACE XML Gateway is similar to setting up load balancing for any web server; you configure a virtual IP (VIP) for the Gateway cluster in the load balancer with an message allocation scheme of your choice for routing messages to individual Gateways in the cluster.

Load balancers need to be able to monitor the health of the Gateways. The ACE XML Gateway supports application-level monitoring—the load balancer can send an HTTP request (HEAD or GET) to the Gateway and get back an HTML page or other type of response to indicate the health of the appliance. Using a HEAD method request may be preferable in most cases, since it can check the system health with minimal use of bandwidth.

Note A load balancer can also use a *ping* message to check the responsiveness of the ACE XML Gateway. However, using an HTTP request ensures that advanced processes in the Gateway are active.

In the Gateway policy, you set up a HTTP health check page (as a static response message) on the port object. For more information on configuring a health check response on a port object in the policy, see the chapter "Working with Ports and Hostnames" in the *Cisco ACE XML Gateway User Guide*.

Note that the port object in the policy is typically configured to listen on a port number and for one or more virtual IP addresses or hostnames. The hostname in the port configuration is the one by which the client or upstream load balancer should address service traffic to the Gateway. The physical interfaces on each Gateway need to be configured for a particular IP address as well.

While a port object may define multiple IP addresses on which to listen for requests for an application, the Gateway will ignore IP addresses in the port object for which its physical interface has not been set. The following configuration scenario helps to illustrate how such IP addresses on the port object are used to disambiguate requests when there are multiple applications exposed at a given port number at the Gateway.

Consider a cluster of two Gateways that need to expose three web applications on the default HTTPS port, 443. Since the certificate (and key) associated with a given virtual hostname must be chosen at SSL handshake time (before the Host header from the client is seen), the application targeted by a request must be disambiguated by IP address. To implement this scenario, you could give the physical interface at each Gateway three IP addresses, one for each application. Gateway A, for instance, could have 10.0.2.5–7 and Gateway B could have 10.0.3.5–7. The web site https://example.com could be at 10.0.2.5

on Gateway A and 10.0.3.5 on Gateway B. So the HTTP Port used for site https://example.com would need to specify both 10.0.2.5 and 10.0.3.5 as IP addresses on which to listen for requests. (The ports for the other two applications would listen on the other two addresses on each Gateway.)

Enabling Web Console Access through a Proxy Server

The primary development environment for the system is the Manager web console, a browser-based interface for developing the policy. Policy developers in your organization will need to be able to access the web console from their work environments. If forward proxy servers are used for client web access, you may need to modify the configuration to accommodate the proxy server.

By default, the Manager web console runs on port 8243 (leaving port 443 available for web service traffic). After installation, policy developers who attempt to connect to the Manager with a browser configured to use a proxy server that doesn't allow access to 8243 will get a “permission denied” error.

To correct this issue, you can configure the proxy server to allow access to the Manager appliance on port 8243. Alternatively, the Manager can be configured to present the web console on a port other than 8243. As an additional alternative, the browsers that need to access the web console can be configured to bypass the proxy server when connecting to the web console.

Appliance Network Interface Considerations

Cisco ACE XML Gateway appliances use Ethernet for networking communications. They do not support other kinds of networks, such as token ring or PS/2 networks. For full Gigabit Ethernet performance, the cabling that composes your network must be rated at CAT 5e or better. The appliances accept standard RJ-45 Ethernet connectors.

The 1U platform is equipped with four network interfaces on which it can accept service traffic (an additional RJ-45 interface is dedicated to connectivity for the Integrated Lights-Out module). The interfaces can be configured to run at full-duplex 10baseT, 100baseT or gigabit Ethernet speeds.

Although the interfaces can be configured to negotiate this setting automatically, you'll obtain best performance by avoiding the use of auto-negotiation and setting each interface to a specific speed. The reason for this recommendation is that the time required to auto-negotiate bandwidth settings inflicts a small amount of performance overhead. Changing network conditions may cause unnecessary re-negotiation of bandwidth settings, again reducing performance. Problems with other network devices, such as firewalls and routers, may propagate unnecessarily slow performance when using auto-negotiate bandwidth. Theoretically, one malfunctioning router could cause all of the auto-negotiating ACE XML Gateways that work with it to bottleneck all the traffic they handle, potentially reducing bandwidth in zones that have nothing to do with the failed router.

Auto-negotiation often makes performance issues difficult to track down, while preset bandwidth settings can help to identify a malfunctioning router, firewall or ACE XML Gateway quickly.

IP Address Requirements

Depending on the model, the appliance chassis can have up to five Ethernet ports. The Integrated Lights-Out (iLO) port is for management purposes only, and not intended for service traffic.

Typically, the use of a single interface and IP address is sufficient for handling traffic for the ACE XML Gateway. In some cases, administrators may choose to separate service traffic from Manager traffic addressed to the Gateway onto two different Ethernet ports. This is an optional configuration, however, meant to enhance security.

Another configuration option involves having multiple IP addresses associated with a given Gateway interface, and accepting traffic for various services on different virtual hosts. To do so, you will need to specify the addresses in the network configuration of the Gateway appliance, as described in this guide. In the policy, you then associate ports definitions with the additional IP address. For more information on configuring ports, see the *Cisco ACE XML Gateway User Guide*.

IP Addresses for the Manager

Each Manager uses only one Ethernet port and one static IP address. On appliance chassis that have multiple physical Ethernet ports, you can use any Ethernet port to connect the Manager to the network.

For extra security, some network administrators place the Manager appliance behind their own firewall. Typically, this firewall resides within the corporate intranet, behind the DMZ. The resulting configuration places a minimum of three firewall barriers and at least one Gateway between production Manager appliances and packets arriving from the extranet.