CHAPTER 7

XML Threat Defense

This chapter describes the XML validation and threat defense features of the Cisco ACE Web Application Firewall. It covers these topics:

About XML Threat Defense

While the ACE Web Application Firewall does not provide the advanced XML and Web Service security and integration capabilities of the Cisco ACE XML Gateway product, it does include features for defending against XML threats. The XML threat defense features can identify and defend against XML-based attacks, such as XML denial-of-service (XDoS) attacks.

Threat defense settings allow you to apply limits based on various properties of XML messages, including their size, number of elements, size of attributes, and so on. When the ACE Web Application Firewall encounters a message that violates a rule, it logs the event and drops the message.

In addition to XML-specific threat inspection, an XML message is subject to message inspection rules and other processing measures configured for the profile applied by the virtual web application.

Tuning Threat Defense Settings

The settings for XML threat defense are preconfigured with values that are appropriate for most purposes. You can view and modify the values as follows:

Step 1 In the web console, click the **System Management** link on the navigation menu.

Step 2 Under the ACE Web Application Firewall header, click the **I/O process settings** link.

Step 3 The settings appear under the **Reactor** heading. Configure the settings as desired. Examples of settings available include maximum document size, element levels, attributes per element, and so on.

For details on the settings, see the online help page accessible from the **I/O process settings** page.

Step 4 Click **Save Changes** to have your changes saved to the working policy.

Once the policy is deployed, incoming requests that do not meet the requirements you have configured are blocked by the ACE Web Application Firewall.