Using the Cisco ACE Application Control Engine Application Switches with the Cisco ACE XML Gateway

Applying Application Delivery Technology to Web Services

Overview

The Cisco® ACE XML Gateway is the newest technology in the Cisco application network services products. This document explains how to take advantage of the integrated functions of the Cisco ACE Application Switch and Cisco ACE XML Gateway to maximize availability, performance, and security of SOAP and XML (Extensible Markup Language) web services.

Challenge

As enterprises continue to migrate to service-oriented architectures based on web services, a major challenge is making sure that those services are highly available, meet performance requirements, and are secure from threats at the XML level. Because web services are deep in the network stack, addressing this challenge requires a solution that is fluent in XML and SOAP and that is also highly available and provides optimized HTTP-based application access. The wide variety of technologies used to implement web services compound this challenge, making coordination of security policies across the enterprise difficult. In addition, XML requires more processing power to implement security than other, lower-level protocols do. These challenges make an exclusively software solution impractical and mandate a network infrastructure solution.

Business Benefits

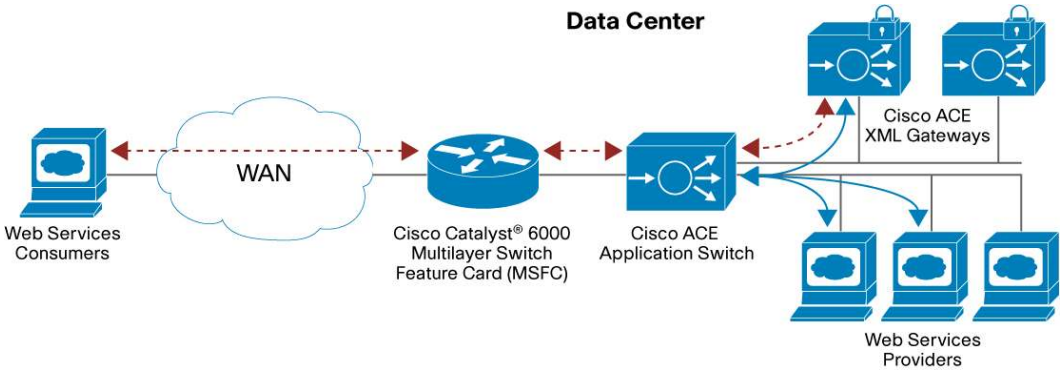
By using a Cisco ACE Application Switch, either the Cisco ACE Module or the Cisco ACE 4710 Appliance, for Layer 4 to 7 load balancing and optimization and a Cisco ACE XML Gateway for XML processing within the Layer 7 payload, you can achieve the following benefits:

- Accelerate and optimize access to web services applications: The Cisco ACE Application Switch plus Cisco ACE XML Gateway solution enables acceleration features such as Secure Sockets Layer (SSL) offload, HTTP 1.1 session reuse and multiplexing, and XML transformation and schema validation.
- Secure access to web services applications: The solution combines the TCP/IP normalization and HTTP RFC compliance functions of Cisco ACE with the industry-leading XML threat-defense capabilities of the Cisco ACE XML Gateway to provide protection from attacks at all levels of the network stack, Layers 4 to 7 and above.
- One-source solution for XML acceleration, availability, and security needs: Cisco is the only vendor that provides a complete solution.
- Use of your Cisco ACE investment to meet your web application, web services, and other network protocol needs: Virtualization in the Cisco ACE helps ensure that denial-of-service (DoS) attacks or traffic storms in browser-based applications do not affect your mission-critical web services, without requiring you to invest in separate infrastructure.

Combined Cisco ACE Application Switch and Cisco ACE XML Gateway Solution

Figure 1 shows a Cisco ACE Application Switch and Cisco ACE XML Gateway deployed in a combined configuration.

Figure 1. Cisco ACE Application Switch and Cisco ACE XML Gateway Deployment



In this example, a set of web services providers, using application server technologies such as Java 2 Platform Enterprise Edition (J2EE) or .NET, or packaged applications such as those from SAP or Oracle, are exposing web services to be used by a set of web services consumers connecting over a WAN. The consumers generate SOAP requests and send them using HTTP or HTTPS. The Cisco ACE Application Switch and Cisco ACE XML Gateway provide the acceleration, security, and availability functions to ensure that the consumers and providers can communicate.

The following sections describe two possible deployment scenarios in this environment: one in which the Cisco ACE Application Switch terminates SSL on behalf of the client, and one in which the Cisco ACE XML Gateway terminates SSL. Either scenario will provide an effective and secure solution, keeping the contents of messages between service consumers and providers private as they cross the WAN. The choice of which to use depends on your application's specific requirements.

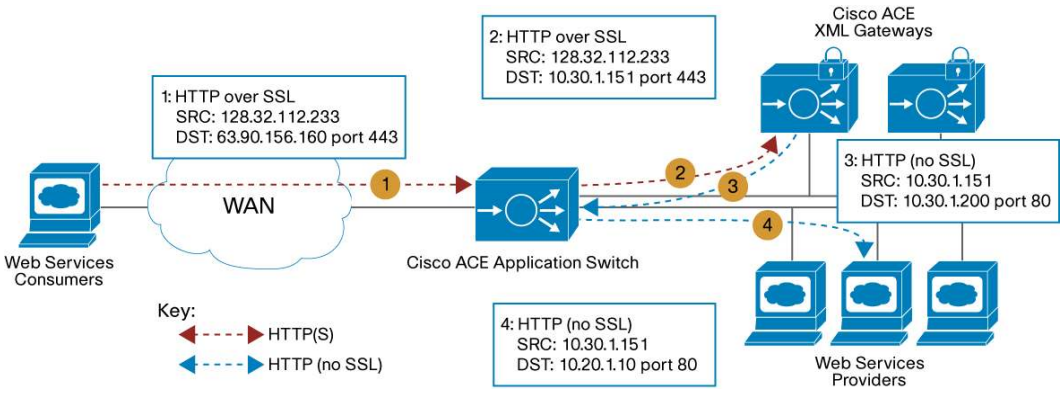
The configuration of both scenarios is simplified by the integration between the Cisco ACE Application Switch and Cisco ACE XML Gateway. The Web-based user interface for the Cisco ACE XML Gateway allows you to configure both the Layer 7 XML security policy and the Layers 4 through 7 load-balancing and application delivery features of the Cisco ACE Application Switch. Cisco is the only vendor providing a complete solution with integrated management. Other scenarios are possible as well; contact your Cisco representative for more information.

In both scenarios, the Cisco ACE Application Switch monitors the availability of both the Cisco ACE XML Gateways and the service providers. In the case of a device failure or overload, the Cisco ACE Application Switch can redirect requests to the remaining devices. Integration with Cisco Global Site Selector (GSS) Software also enables cross-site failover and load balancing for either the Cisco ACE XML Gateways or the web service providers in an integrated package.

Terminating SSL on the Cisco ACE XML Gateway

In this scenario, shown in Figure 2, the web services clients generate an SSL request to the virtual IP address (VIP) exposed on the Cisco ACE Application Switch (connection 1). After defending against attacks at the TCP/IP layer in the request, the Cisco ACE Application Switch makes a load-balancing decision about which Cisco ACE XML Gateway to forward the request to, on the basis of your configured policy and the state of the individual Cisco ACE XML Gateways (connection 2). Because this forwarding occurs at Layer 4, the Cisco ACE XML Gateway has full access to the SSL client certificate. This allows the XML Gateway to perform strong authentication of the client, first by validating the certificate was signed by a trusted certificate authority, and then by querying an identity store such as Lightweight Directory Access Protocol (LDAP) to authorize that client's access to the requested services.

Figure 2. Scenario 1: Terminating SSL on the Cisco ACE XML Gateway



Because web services applications often involve repeated messages between consumers and providers, SSL must be optimized to take advantage of session reuse, allowing the consumer to send a new request to the application without the need for a full SSL connection negotiation. The Cisco ACE Application Switch monitors the session identifiers negotiated between the service consumer and the Cisco ACE XML Gateway and ensures that repeated SSL connections with the same session identifier are always directed to the same Cisco ACE XML Gateway.

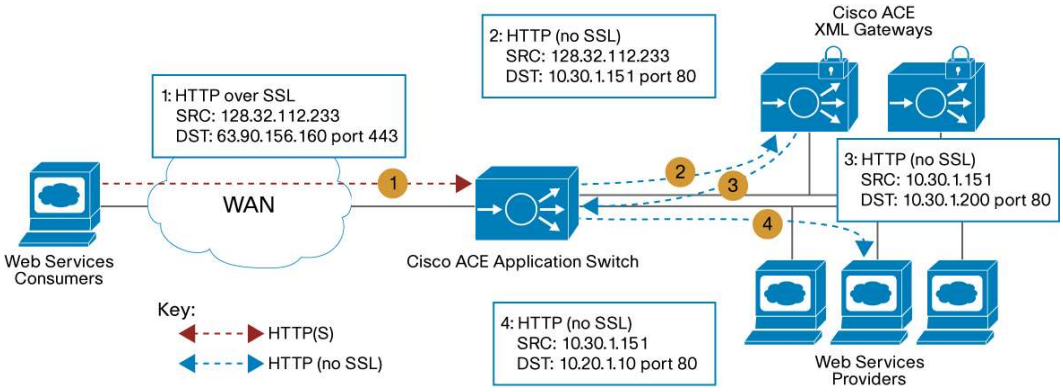
The Cisco ACE XML Gateway also performs threat defense on the incoming request, looking for attacks at the SOAP layer that are opaque to most network devices. These attacks include general application attacks such as Structured Query Language (SQL) injection and buffer overflow as well as XML-based attacks such as entity expansion and overly recursive documents. Because the Cisco ACE XML Gateway understands XML natively, it can thwart attempts to use entity encoding or packet fragmentation to bypass threat defense.

After authenticating the client and determining that the message is not malicious, the Cisco ACE XML Gateway initiates a new connection to a second VIP exposed on the Cisco ACE Application Switch that faces the web service providers (connection 3). Because the Cisco ACE XML Gateway acts as a full proxy, it can perform HTTP multiplexing, handling simultaneous requests from hundreds or thousands of web services consumers and limiting the connection load on individual web service providers. It can also throttle the number of messages sent to each provider, protecting them from out-of-memory and overload conditions.

Terminating SSL on the Cisco ACE Application Switch

In an alternative implementation, shown in Figure 3, the architecture can be set up so that SSL is terminated at the Cisco ACE Application Switch instead of at the Cisco ACE XML Gateway. In this case, the Cisco ACE Application Switch makes a Layer 7 load-balancing decision, negotiating the SSL session with the client directly (connection 1) and then forwarding the HTTP request to the Cisco ACE XML Gateway unencrypted (connection 2). The Cisco ACE XML Gateway continues to perform its threat defense and HTTP 1.1 multiplexing of the request back to the web service providers (connection 3). This approach allows you to consolidate all SSL server certificates for both XML- and browser-based applications in a single device, especially useful in situations where the web service is public or authenticated using a password instead of an SSL client certificate. The approach can also be useful in situations where Web Services Security (WS-Security) signatures and encryption are in use, reserving the cryptographic capacity of the Cisco ACE XML Gateway for message-level security.

Figure 3. Scenario 2: Terminating SSL on the Cisco ACE Application Switch



Because the Cisco ACE Application Switch can examine the HTTP headers to make its routing decision, it can also handle applications that combine XML and browser-based access. Such a combination is an increasingly important part of Web 2.0 Asynchronous JavaScript and XML (AJAX)–based applications, where HTML, XML, and JavaScript are used together to provide a rich, interactive application experience to users. The Cisco ACE Application Switch can forward XML-formatted requests, based on the requested URL or the content type of the request, to the Cisco ACE XML Gateway for XML-specific processing. This processing may include message transformation, allowing browsers to access rich, SOAP-based web services from the service providers.

Intelligent Networking

The combination of the Cisco ACE Application Switch and the Cisco ACE XML Gateway is a critical infrastructure component of a service-oriented networking architecture (SONA), combining high availability and HTTP acceleration with XML-specific security and optimization. As XML becomes the default encoding for all business data, the capability to handle it natively within the network will become a distinct competitive advantage for those enterprises that want to increase the agility of their IT infrastructure.

Why Cisco?

Cisco is the only vendor that offers a combined solution for web application and web services security and optimization. The Cisco ACE Application Switch and the Cisco ACE XML Gateway have been proven in the marketplace by Fortune 100 enterprises wanting to secure web services handling billions of dollars in transactions, from financial services, to consumer media, to manufacturing. The integration of the Cisco ACE XML Gateway with the Cisco ACE product line makes Cisco the leading vendor of application delivery solutions at Layers 4 to 7 of the network stack and above.

For More Information

To learn more about the Cisco ACE Application Switch and the Cisco ACE XML Gateway, visit: http://www.cisco.com/go/ace.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-416510-01 01/08

