Better Performance Through Centralization of Security

Lori MacVittie, 2007-13-03

How a WAF increases the performance of your application by offloading security

One of the benefits of implementing a SOA is allegedly efficiency gains achieved through the reuse of common, shared code. If five applications implement the same logic, and that logic is moved to a single, shared service, then changes to that logic need only be applied, tested, and deployed once, rather than five times as is the case with "legacy" applications.

The concepts of SOA can also be applied to security logic as well, resulting in both efficiency and *performance* gains.

Data validation and scrubbing logic is not rocket science, even if it is encoded in an XML document. An SQL or command injection looks the same when embedded in an XML element as it does in a www-url-encoded name-value pair, which can be easily discovered by a Web Application Firewall (WAF) such as F5's Application Security Manager. WAF products specialize in scanning requests and responses for suspect data, so they're much better at it than developers and much faster, as that's all they do - security.

Developers can certainly code their own logic to look for SQL and command injection, as well as data validation and scrubbing functionality. But if you consider the number of functions and/or methods in any given application in which the developer must either add that logic or call another function to perform this task it quickly becomes an unwieldy, not to mention inefficient, method of protecting data. Just as important is that this is a resource intensive process that takes up CPU cycles and memory on the server that could better be spent responding to valid requests.

Analysts estimate that the processing of XML consumes about 30% of the server's resources, about the same as processing SSL. We've long along learned that offloading SSL and terminating it at the edge of the network decreases the burden on servers and increases their capacity, so it should come as no surprise that offloading security processing of XML and other web-applications at the edge of the network would similarly increase the overall capacity of servers.

It is a waste of resources to allow a malicious or invalid request to be parsed and examined on the server only to be rejected due to malformed data. By moving such processing to the edge of the network and into a WAF, the resources once used to process and reject malicious data can be used to process valid requests. The reduction in processing required to scan incoming requests translates directly to more resources for processing of valid data and therefore better overall performance of the application. The fewer requests a server needs to concurrently process, the faster the processing occurs.

Centralizing security services with a WAF leads to great efficiency of developers, better use of your network infrastructure, and better overall performance for you applications.

Imbibing: Mountain Dew

Technorati tags: F5, security, SOA, XML, application firewall, application delivery

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com