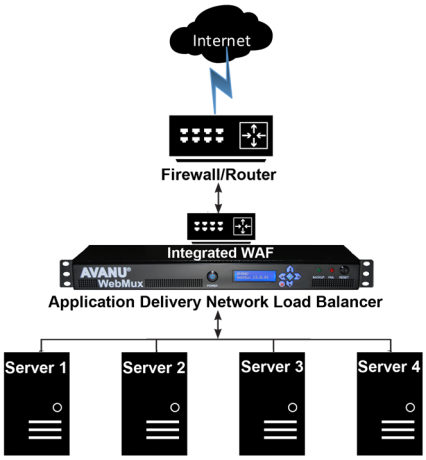
# The Web Application Firewall (WAF) An Added Safety Net

Web sites have moved beyond a mere collection of static HTML pages since the emergence of Web 2.0. Now Web applications allow for dynamic sites to respond to the open public inputs on a web browser just like an individual using their personal desktop applications software. The Web servers servicing dynamic sites now become a central hub of users' application data. If the Web servers are compromised causing service interruptions, it will affect all users. Such servers become a high target for malicious attackers exploiting their public accessibility. A traditional firewall that merely blocks ports and IPs cannot provide adequate application protection, because the service ports must remain open and attackers' IP addresses are unpredictable. Furthermore, since Web applications respond to user input, bugs or unsecure configurations can cause them to respond in ways that cause service interruptions or security breaches.

The Web Application Firewall (WAF) is your indispensable line of defense in these situations. It does not replace your traditional firewall but rather augments it. The best location for a WAF is behind the traditional firewall but in front of the Web server. The traditional firewall will then block unnecessary ports and blacklisted IPs wholesale, while the WAF will detect additional malicious attacks. The WAF does its job by examining the web client requests and Web server responses. Thus, not only does the WAF protect against incoming malicious activities, but it also prevents your Web application from revealing information useful to attackers.




Sometimes if a Web server or application is not configured or coded properly, the server or application error response can reveal weaknesses or other exploitable information. Error responses may be helpful for developers and systems administrators, but such information should remain confidential. The WAF will keep those error responses private to prevent further probing by an attacker.

Sometimes security holes arise from unintended, overlooked, or forgotten default settings. Often server software defaults to using extremely insecure settings for debugging purposes during setup. These settings may escape revision, and it only takes one successful attack because of them to wreak havoc on a system. The WAF is a safety net that can plug some of these more commonly overlooked security holes and keep your service up and running smoothly.

AVANU, Inc. is the developer of the WebMux Network Traffic Manager, an enterprise-class application delivery network load balancing solution. AVANU offers Virtual WebMux appliances for cloud environments as well as a network hardware appliance for plug-and-run ease of use and management along with reliable high performance. Both platforms are scalable to meet your local traffic management requirements as well as affordable for all business sizes.

For information on AVANU WebMux Networks Traffic Manager, visit their web site at 'www[dot] avanu[dot]com; email 'info[at]avanu[dot]com; or call 1.888.248.4900 U.S. Toll Free Number; 1.408.248.8960 International.