



# Web Application Firewall

As enterprises rely more and more on the Internet for business-critical transactions, they are exposing their corporate data and business operations to increasing risks of disruption and compromise from a wide range of network threats. At the same time, these threats are becoming more sophisticated, with the majority of attacks now evading traditional firewalls and exploiting higher-level Web application vulnerabilities instead.

The pressures of today's competitive marketplace have created a highly susceptible Web infrastructure environment. Applications are written with an emphasis on time-to-market over security. Deployment architectures are complex, requiring the integration of many heterogeneous technologies and creating the potential for numerous vulnerabilities. Rapid development cycles and continual application updates further compound the problem.

The business risk is far too great to ignore, as these vulnerabilities put critical business operations and sensitive data in jeopardy. Significant losses can result from business disruption, theft of intellectual property, and damage to customer trust and brand reputation, which directly impacts revenue. In many cases, application security is also a legal requirement — such as complying with the PCI Data Security Standards, for example.

## Web Application Firewall

The Web Application Firewall (WAF) module provides customers with a highly scalable layer of protection against application-level attacks. Running on Akamai's globally distributed network of more than 90,000 servers, WAF helps detect and deflect threats in HTTP and HTTPS traffic, issuing alerts or blocking attack traffic near its source, before it reaches origin servers. Customers can deploy Akamai WAF either as their primary application firewall or to augment an existing security ecosystem.

## How Web Application Firewall Works

WAF detects attacks by filtering all incoming HTTP and HTTPS traffic through configurable network and application layer controls. WAF's core security parameters are based on ModSecurity, an industry standard and trusted rule set that detects and prevent common exploitation techniques such as SQL Injection and Cross Site Scripting (XSS). WAF runs across Akamai's distributed EdgePlatform, performing its inspections before Akamai serves each request.

Customers can easily configure WAF rules, alerts and actions, as well as IP blacklists and whitelists, through the EdgeControl portal. Configurations and updates are deployed through Akamai metadata and distributed across the network over a Fast Channel enabling expedited global deployment.

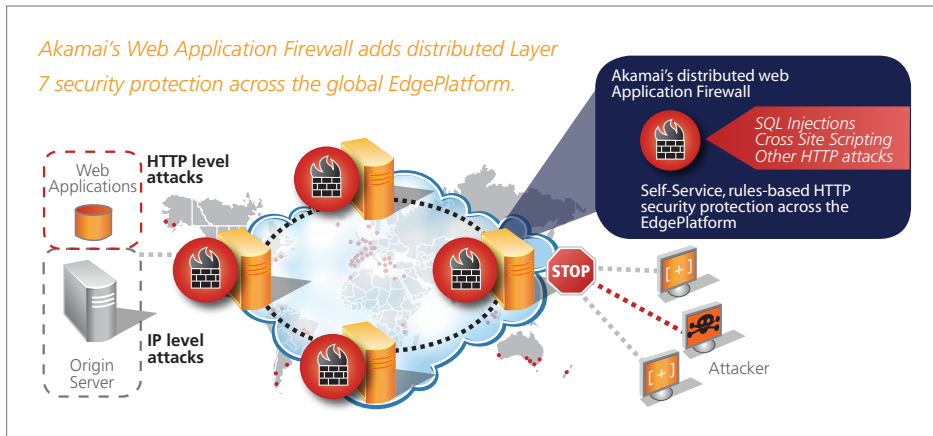
Customers who accelerate their secure applications using Akamai Secure Delivery or Web Application Accelerator can enable WAF to seamlessly protect these applications as well. Moreover, because Akamai holds a private key used for encrypting SSL between the client and the Edge platform, these applications are secured without the overhead of SSL key exchange.

## BUSINESS BENEFITS

- Mitigate business risks and improve brand and customer confidence by bolstering site's security triad – Confidentiality, Integrity, and Availability
- Reduce attack traffic bandwidth costs and resource usage
- Reduce operational costs associated with constant security infrastructure maintenance and upgrades
- Reduce capital expenditures on security hardware and software
- Eliminate expenses from overprovisioning and business risk from underprovisioning Web application firewalls
- Promote compliance with mandatory PCI requirements

## OPERATIONAL AND TECHNICAL BENEFITS

- Enable automatic, on-demand scaling to handle massive attacks
- Mitigate attacks at the source, away from the origin datacenter
- Eliminate need to provision and architect for Web application firewall failover
- Offload and augment existing security architecture



### Custom Rules

This feature enables a user to create Akamai metadata-based rules that are enforced after the execution of the Application Layer rules. Custom rules serve as “Virtual Patches” wherein new website vulnerabilities may be mitigated quickly before standard rules are defined in the WAF. Like all WAF features the propagation of Custom Rules configurations is done via the WAF Fast Channel. Additionally, the actions of each custom rule will be reported alongside that of standard rules. Each custom rule will support the following:

- ID
- Title
- Description
- Metadata Body (that defines the rule)
- Default Action

### Policy Management and Reporting

**Rule Management and Deployment:** Customers select, configure, enable and disable WAF policy rules using the EdgeControl portal. For rules that are enabled, multiple actions are available, such as alert only, drop, and notify. Changes to firewall policies can be expedited using a dedicated FastChannel to quickly deploy rule updates in response to an attack.

### Reporting and Logging

Akamai WAF makes event logging, reporting and auditing available through the EdgeControl portal. These include:

**Frequently updated service reports**, such as the Firewall Rule Activities report and the Blocked IP report

**Logging of firewall events** in the W3C or the NCSA Combined Log format using Akamai's Log Delivery Service (LDS)

**Real-Time Reporting** feature that streams WAF events in an open format to the customer's log server. This is used for integration with other security controls such as Log Management and Security Information and Event Management (SIEM) solutions.

### Application Layer Controls

WAF includes a rich collection of pre-defined but configurable application-layer firewall rules, which Akamai maintains with regular updates. They are categorized as follows:

- Protocol Violations
- Request Limit Violations
- HTTP Policy Violations
- Malicious Robots
- Generic and Command Injection Attacks
- Trojan Backdoors
- Outbound Content Leakage (Server Banners)

### Network Layer Controls

WAF provides the ability to enforce customer-defined IP whitelists and blacklists. List updates are propagated across Akamai's global network within 30 minutes, enabling real time response to attacks.

**IP White List:** Customers can define up to 512 IP addresses or CIDR entries of trusted hosts/networks to be granted access per the Strict Whitelist feature, which allows traffic only from the defined addresses, while denying all other traffic. This supports a positive security model of “deny all except that which is explicitly trusted.”

**IP Black List:** Customers can define up to 512 IP addresses or CIDR entries to block from access. This supports a negative security model of “accept all except that which is explicitly denied.”

### Rate Control

This WAF feature enables a customer to protect both their websites and applications against Distributed Denial of Service (DDoS) attacks by monitoring and controlling the rate of requests against the Akamai EdgePlatform. Rate Categories can be incorporated as WAF rules thus enabling the customer to dynamically alert and/or block clients exhibiting excessive request rate behaviors. If a client IP exhibits a request rate that exceeds either the Burst Threshold or the Average Threshold, their requests can be blocked until their associated request rate decreases to acceptable values. The Rate Control feature includes the following category definition parameters:

- Client Identification: client-ip
- HOIT
- URI
- HTTP Method
- Edge Hit
- Origin Hit
- Burst Threshold
- Average Threshold
- Penalty Box for Excessive Rates

## Akamai Technologies, Inc.

### U.S. Headquarters

8 Cambridge Center  
Cambridge, MA 02142  
Tel 617.444.3000  
Fax 617.444.3001  
U.S. toll-free 877.4AKAMAI  
(877.425.2624)

[www.akamai.com](http://www.akamai.com)

### International Offices

Unterfoehring, Germany  
Paris, France  
Milan, Italy  
London, England  
Madrid, Spain  
Stockholm, Sweden  
Bangalore, India  
Sydney, Australia  
Beijing, China  
Tokyo, Japan  
Seoul, Korea  
Singapore



©2012 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice.