Web Application Firewall

Web applications grease the wheels of the internet. They offer richer user experiences, greater interactivity, and more flexibility than the static technologies of yesteryear. Yet with sophistication comes risk. The vast majority of web applications built today do not incorporate adequate security. Until web developers, IT teams, and security managers get in better sync, a Web Application Firewall (WAF) is necessary – not only to be in compliance with regulations, but more importantly to maintain a truly protected Web site.

Akamai's Kona WAF detects potential web application attacks in HTTP traffic before the traffic reaches the customer's data center. It gives customers the ability to detect anomalous and potentially malicious patterns in HTTP request headers and body contents, and either issue an alert or block the traffic altogether. Should traffic be blocked, the service provides customers with several options for responding to blocked HTTP requests. It provides customers with summary and trend reporting on attacks through the Akamai LUNA Control Center. Customers that need more detailed visibility into, and information about, the attack traffic can use the Akamai Security Monitor or configure the firewall to send logs to their log management system directly for analysis.

Customers can deploy Kona WAF independently or as part of an existing security ecosystem. The WAF provides a distributed approach to web application security by leveraging the Akamai Intelligent Platform and its distributed network architecture. The service scales automatically, on-demand, offering the capability to defend against massive-scale attacks. Because the Kona WAF runs across more than 100,000 servers in Akamai's Intelligent Platform, it frees companies from the need for constant upgrades of hardware, reducing CAPEX and operational expenditure. It also helps enterprises comply with PCI requirements.

How the Kona WAF Works

The Kona WAF is an embedded process within the Akamai Intelligent Platform. As such, it is capable of inspecting both HTTP and HTTPS requests before either serve the request. Because Akamai holds a private key used for encrypting SSL between the client and the Edge platform, customers who accelerate their secure application using the Secure Delivery service can easily enable WAF to protect these applications as well – all without the need to share a private key with Akamai.

The module allows changes to firewall rules to customize the defense perimeter for each specific environment being protected. Kona WAF works through the implementation of Network and Application layer controls.

Application Layer Controls: WAF includes a rich collection of pre-defined but configurable application-layer firewall rules, which Akamai maintains with regular updates, for different categories such as: Protocol Violations, Request Limit Violations, HTTP Policy Violations, Malicious Robots, Generic and Command Injection Attacks, Trojan Backdoors and Outbound Content Leakage. Kona WAF Rules can be broken down into 3 categories: Open Web Application Security Project (OWASP) ModSecurity™ Core Rule Set (CRS) 2.2.6,, Akamai Common Rules, and Akamai Custom Rules.

OWASP Core Rule Set implementation includes:

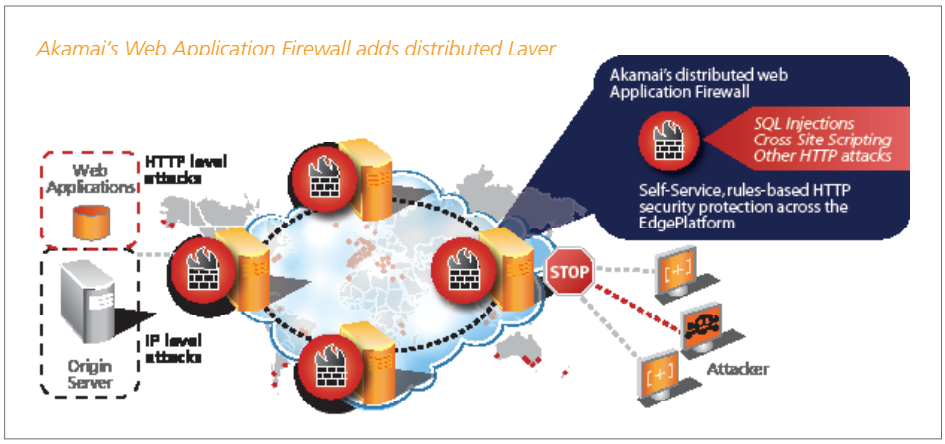
- Anomaly scoring whereby each rule contributes to an overall risk score. Alert/Deny decisions are based on the total score.
- Legacy support for Core Rule Set 1.6.1
- An upgrade wizard for existing customers to upgrade WAF policies from 1.6.1 to 2.2.6
- Inspection of HTTP Request/Response Headers and HTTP POST Request/Response Bodies.

BUSINESS BENEFITS

- Improve brand and customer confidence
- Increase confidentiality, integrity, and availability
- Reduce bandwidth costs and resource usage
- Reduce operational costs associated with constant security infrastructure maintenance and upgrades
- Reduce capital expenditures on security hardware and software
- Reduce expenses from over-provisioning Web Application Firewalls
- Reduce business risk from under-provisioning Web application firewalls

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 traffic from existing security architecture



Akamai Common Rules: Akamai professional services have developed rules over the course of the past two years that address some of the most recent threats and attacks against our hundreds of customers. Those rules are updated regularly by Akamai's Threat Intelligence team and are available to all Kona WAF customers. The rules protect against attacks such as: Low Orbit Ion Cannon, High Orbit Ion Cannon, HULK, Dirt Jumper, Havij SQL Injection Tool, Netsparker, ApacheBench, and Webhive.

Custom Rules: This feature enables customers to create Akamai metadata-based rules that are enforced after the execution of the Application Layer rules. Custom rules can serve as "Virtual Patches" in which new website vulnerabilities may be mitigated quickly before standard rules are defined in the WAF. Custom rule configurations are done via the WAF Fast Channel.

Network Layer Controls: The Kona WAF also provides network layer controls to allow or restrict requests from certain IP addresses to protect the origin server from application layer attacks.

IP Black List: Kona WAF supports the ability to define a list of IP addresses/CIDR blocks to be blocked along with the subnet masks to be used in the matching process; the list can be up to 10K entries. IP address updates can be propagated within 30 minutes. This supports a negative security model of "accept all except that which is explicitly denied."

IP White List: Kona WAF supports the ability to define a list of IP addresses, or IP address ranges to be allowed; the individual IP address list can be up to 10K entries. IP address updates can be propagated within 30 minutes. The IP White List is used in conjunction with the Strict Whitelist feature, which allows traffic only from the defined addresses, while denying all other traffic.

Strict IP White List: Allows only those IPs in the allowed IPs list, all other IPs are denied. This supports a positive security model of "deny all except that which is explicitly trusted."

Logging: The Kona WAF supports event logging. Customers can elect to log firewall events using Akamai's log delivery service (LDS), which now supports the addition of WAF events in W3C and combined formats. Alternatively, customers can employ the new Real Time Reporting functionality that enables customers to incorporate WAF firewall events in near real time into their log management or security information and event management (SIEM) infrastructures. This new feature enables customers to increase their threat posture awareness.

Reporting: Additionally the WAF firewall provides service reports such as the Firewall Rule Activities as well as Blocked IP report. Reports are constantly updated and delivered via the LUNA Control Center.

Security Monitor: The Security Monitor is a security data visualization solution that incorporates WAF and rate control data in real-time. This significantly improves the customer's ability to investigate WAF activities by supporting advanced filtering, search and eventually notification functions.

The Security Monitor also provides the capability to drill down into attack alerts to retrieve detailed information on who are attacking, what they are attacking, what defense capabilities triggered the attack declaration and what specifically was seen in the requests that triggered site defenses.

Quick Configuration: Allows a customer with limited security resources to quickly implement a firewall policy. The customer simply answers a number of yes/no questions and then stipulates some match target information. The portal then selects the proper rules based on the answers and generates a basic firewall policy.

Rate Controls: WAF enables customers to protect their applications against DDoS attacks by monitoring and controlling the rate of requests against the Akamai Intelligent Platform and customer origin. Rate categories can be incorporated as WAF rules thus enabling the customer to dynamically alert and/or block clients exhibiting excessive request rate behaviors. Requests are controlled based on behavior pattern – not request structure.

Customers can implement rate policies using client identifiers such as IP address, user agent, cookie, and session ID within the rate control. These rate policies can then be applied to edge request traffic, forward requests to origin, and even the response traffic from origin. The Rate Control feature allows the Akamai edge server to identify attackers hiding behind proxies. Kona WAF can respond to bursts of requests within seconds.

Rate Controls further protect customers by mitigating Slow POST DDoS attacks. POST requests are not sent to the origin until the POST body completes at the edge. POST bodies that take too long to complete are terminated.

Akamai FASTER FORWARD

Akamai® is the leading cloud platform for helping enterprises provide secure, high-performing user experiences on any device, anywhere. At the core of the company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com and follow @Akamai on Twitter.