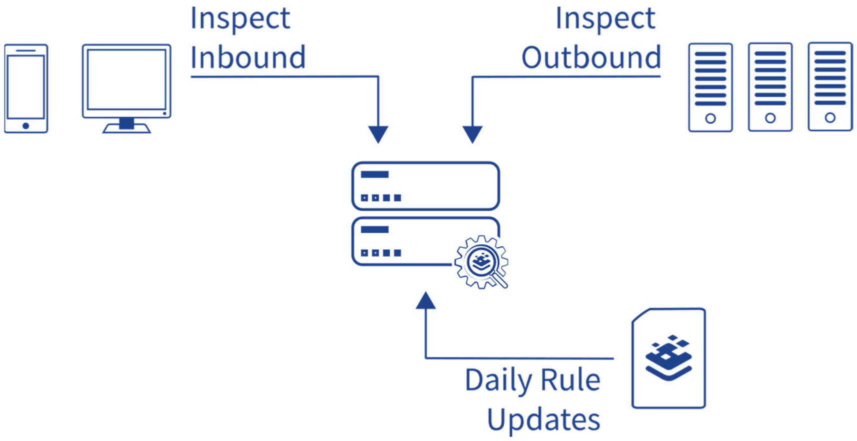
kemp

Web Application Firewall (WAF)

.

Securing Application Deployment

Kemp's Web Application Firewall (WAF) combines Layer 7 Web Application Firewall protection with other application delivery services including intelligent load balancing, intrusion detection, intrusion prevention as well as edge security and authentication. By integrating the world's most deployed web application firewall engine, ModSecurity, augmented by threat intelligence and research from information security provider, Trustwave, Kemp provides ongoing protection against known and evolving vulnerabilities.



With a targeted focus on application-specific exploits missed by traditional firewalling techniques, Kemp WAF plays a key part in a defense-in-depth strategy that mitigates risk and optimizes application security. With Kemp's focus on simplicity and shortening time to production for application deployment, LoadMaster with Web Application Firewall enables secure, scalable, and always-on workload delivery in one fully integrated, easy to use and deploy load balancing solution.

Feature	Benefit
Integrated with ADC Platform	Simplified deployment and management of application protection services
Operate as Active or Passive	Allows flexible deployment in either a block and log (Active) mode or in a log only (passive) mode
Daily Rule Updates	Maximizes protection against evolving threats and latest application vulnerabilities
SQL Injection protection	Protect against exploits that leverage weaknesses in Web application SQL implementations
Cross-site scripting mitigation	Prevent injection of untrusted content into user content
Cookie tampering protection	Disallow the modification of cookies to facilitate attacks
Data leakage protection	Prevent sensitive corporate and personal data such as credit card numbers from being accessed
Custom rule support	Easily build deeper levels of protection for applications.
Regulatory compliance simplification	Enables compliance with PCI-DSS (Payment Card Industry) security standards

Copyright 2002-2019 Kemp Technologies
All Rights Reserved.

Specifications

Standard Features

- Protection against the Open Web Application Security Project's (OWASP) top ten vulnerabilities
- Support for standard and custom applications
- Active (block and log) mode operation support
- Passive (log only) mode operation support
- Distributed Denial of Service (DDOS) mitigation
- Trojan protection
- IP reputation checking
- Daily rules updates
- Data leakage protection
- Built in logging including log field masking (i.e. credit card numbers)

Security Functionality

- Layer 7 Intrusion Prevention System
- SNORT-Rule Compatible
- Global & per VS Black list and White list (Access Control List)
- IP address filtering

PCI Compliance Support

- Section 1.2: Deny traffic from untrusted networks and hosts
- Section 3.3: Mask account numbers when displayed
- Section 3.5: Protect encryption keys against disclosure and misuse
- Section 4.1: Use strong cryptography and security protocols
- Section 6.6: Audit and correct application code vulnerabilities or institute an application firewall

Threats Mitigated

- Cookie Tampering
- Cross Site Request Forgery
- Cross-Site Scripting
- Data Loss Prevention (DLP)
- Injection Attacks

Administration

- Fully configurable using Web User Interface (WUI)
- SSH and HTTPS (WUI) remote access for administration
- Easy start and maintenance wizards
- WUI-based Help Assistant
- Automation/Orchestration via REST API
- Real time performance and availability displays
- Preconfigured Application templates
- Remote syslogd support
- WUI Log Reporting
- SNMP support for event traps & performance metrics

* Specifications are subject to change without prior notice.

The Kemp Web Application Firewall is included in the Enterprise Plus subscription package and includes daily rule updates.

Copyright 2002-2019 Kemp Technologies
All Rights Reserved.