

HAProxy Enterprise Web Application Firewall

Secure Application Delivery Simplified

The **HAProxy Enterprise Web Application Firewall (WAF)** stops threats that target the web application tier. These threats can cause data breaches, system crashes, website defacement, and loss of public trust. The WAF provides protection across an organization, even when using a mix of technology stacks and microservices. Simplify your security posture by employing a proxy-level WAF.

The WAF is included with your instance of HAProxy Enterprise!



Modern Threats to Web Applications

- Web application attacks remain an enduring threat, despite email phishing and social engineering taking the top spot for data breaches.
- SQL Injection, Local File Inclusion, and Cross-Site Scripting are common attack vectors against web applications.
- Bots are a prevalent source of intrusions, utilizing automated scans and exploiting well-known vulnerabilities against servers.
- 43% of breaches occur in small businesses, showing that attacks are not limited to large companies.

A Powerful Countermeasure

The HAProxy Enterprise WAF inspects requests for malicious payloads allowing you to stop threats in their tracks before they reach your web application. It supports three modes of operation to fit your use case.

Simple SQLi / XSS

Set up SQL Injection and Cross-Site Scripting protection in minutes.

- Extremely fast detection of SQL injection (SQLi) and Cross-Site Scripting (XSS)
- Simple configuration in minutes
- Tight integration with HAProxy ACLs and logging
- Supports various responses including deny, silent drop and tarpit
- SQLi fingerprint list can be updated dynamically across a cluster of HAProxy instances

Advanced Whitelist-Only

When you require the strictest level of access, use the Advanced Whitelist-Only Mode.

- Highly restrictive ruleset for zero-trust security
- Fine-grained whitelisting allows expected client behavior only
- Blocks SQLi, XSS, Remote File Inclusion, Directory Traversal, Evasion Tricks and more
- Tight integration with HAProxy ACLs and logging
- Supports various responses including deny, silent drop and tarpit
- Whitelist rules can be based on request path, variable, or combination of both

ModSecurity

Defend against attacks with the industry-leading software, ModSecurity.

- Blocks SQL Injection, Cross-Site Scripting, Remote Code Execution and more...
- Utilize the OWASP ModSecurity Core Rule Set or define custom rules
- Directly integrated with HAProxy Enterprise and the Kubernetes Ingress Controller, no additional web servers or proxies needed
- Hardened version of ModSecurity
- Demonstrates a clear performance gain over other ModSecurity implementations

Trust the Experts at HAProxy Technologies

Our customers use HAProxy to achieve the utmost performance, observability and security. The Web Application Firewall is deployed to protect some of the most highly visited websites in the world.

- We use it ourselves to safeguard HAProxy Edge, which serves 70 billion requests per day
- Supported by a world-class team of engineers and network professionals
- Used by finance, retail and healthcare organizations that must comply with strict regulations