



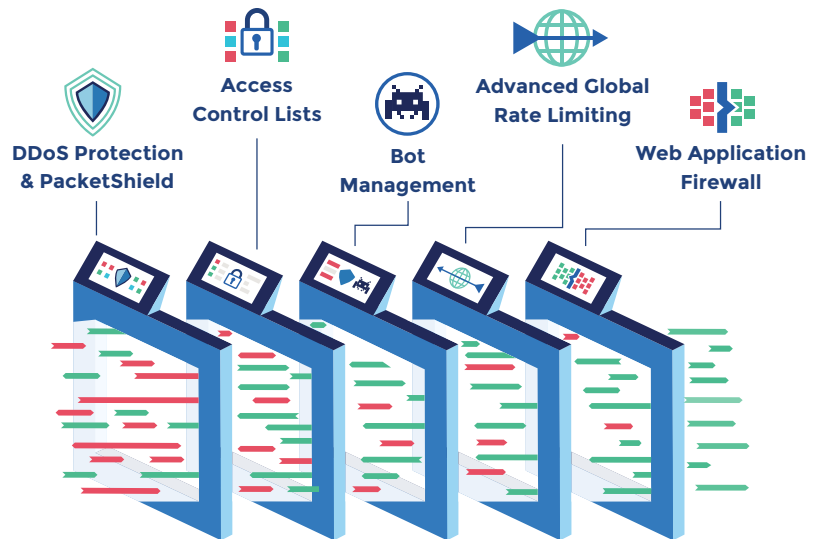
High-Performance Security for Apps and APIs

Every application is different. Instead of a one-size-fits-all solution, HAProxy Enterprise provides customizable security layers that form the building blocks of application and API security. We give you the power to build deep, targeted, and scalable security adapted perfectly to your infrastructure.

Harness Defense in Depth

A single line of defense will inevitably fail. Combine HAProxy Enterprise's high-performance security layers to form an ironclad defense against a broad spectrum of threats.

Line-rate packet filtering, Access Control Lists (ACLs), HAProxy Enterprise Bot Management Module, Global Rate Limiting, and HAProxy Enterprise WAF collaboratively share intelligence to make fast, accurate decisions.



Defeat Evolving Threats

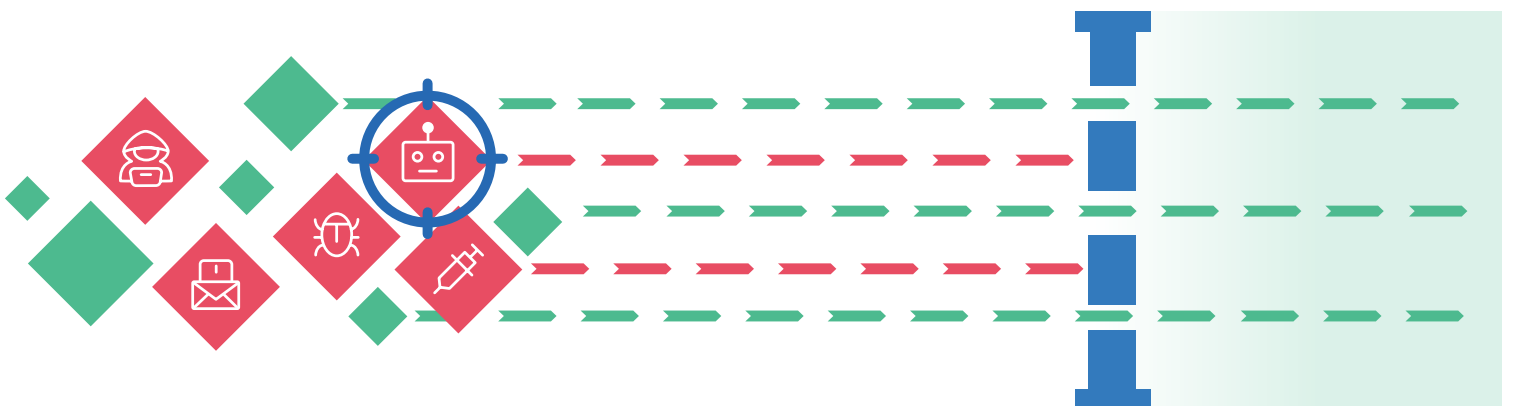
From DDoS to fraud, automated bots threaten your business at massive scale.

Wield the power of HAProxy's sophisticated security layers to inspect, filter, and protect real-time network traffic. Efficiently detect and block your biggest threats.

Implement Adaptable Security

Your traffic and threat profiles are unique. What looks normal for other businesses raises red flags for yours.

HAProxy Enterprise lets you customize the security signals, weightings, and thresholds that determine responses at each layer. Make informed decisions about the attacks and anomalous activity affecting your systems.



The Building Blocks of Application Security

Security incidents such as DDoS attacks, bot threats, and data theft cost companies millions in lost revenue. HAProxy's security capabilities leverage an extremely efficient, flexible, and dynamic code base—with a robust SSL stack, industry-leading ACL, and Stick Table tracking systems.

HAProxy Enterprise and **HAProxy Fusion** keep you ahead of threats by extending the core capabilities of HAProxy. Security enhancements include the HAProxy Enterprise Bot Management Module, the HAProxy Enterprise WAF, Global Rate Limiting (powered by the Global Profiling Engine), content inspection, adaptive response policies, plus centralized management of security policy, SSL certificates, and observability.



Advanced ACLs and Tracking

► Flexible Access Control Lists (ACLs) provide matching based on multiple options:

- IP / CIDR
- SSL Data
- Map File Support
- Logical Operator Support
- Request/Response Headers and Paths

► Global Profiling Engine:

- Generic Key-Value Storage
- Combine any Number of Metrics
- Real time cluster-wide tracking for the following:
 - Request/Error Rate and Counts
 - Unique Page Views per IP or User-Agent
 - Rate and Counts of Unique User-Agents per IP
 - Number of WAF Violations from an IP or User-Agent
 - And Much More

DDoS and Bot Management

► Detect and Protect against:

- GET/POST Floods
- Web Scraping
- Brute Forcing
- Vulnerability Scanning

► Response Policies:

- Request Rate Limiting, Shadow Banning, Tarpitting, and Dropping
- Challenge/Response and reCAPTCHA Support

► Client Fingerprinting

- Identify bots and scanners immediately

- Triangulate data to form a unique ID
- Uncover clients that spoof HTTP headers

HAProxy Enterprise WAF

- High throughput and low latency
- OWASP Core Rule Set (CRS) compatibility with massively boosted performance and low false positives
- Unmatched balanced accuracy (low false positives and low false negatives)
- Deny-list / Signature Support
- Allow-list Support
- Detailed Logging

SSL

- ECC/RSA
- OCSP Stapling
- Reduce Latency by Using OpenSSL Async Engine
- TLS Session Resumption
- Built-in Heartbleed Protection
- Zero Round Trip Time Resumption (0-RTT)

Extra Capabilities

- HTTP Header Sanitization
- Response Body Injection
- IP Masking Support
- Lua Scripting Support
- Runtime API
- Dynamic Update Support