



# HAProxy Enterprise Pare-feu d'applications web

## La livraison sécurisée des applications simplifiée

Le pare-feu d'applications web (WAF) HAProxy Enterprise stoppe les attaques qui ciblent la couche application. Celles-ci peuvent entraîner des fuites de données, la dégradation de sites web, des pannes système, voire la perte de confiance du public. Le WAF protège l'ensemble de votre organisation, y compris si elle s'appuie sur des microservices et des piles technologiques hétérogènes.

**Le WAF est compris dans votre instance de HAProxy Enterprise !**



## Menaces actuelles pour les applications web

- ▶ L'hameçonnage par courrier électronique (phishing) et l'ingénierie sociale sont la cause principale des fuites de données. Mais les attaques contre les applications web restent une menace constante.
- ▶ L'injection SQL, l'inclusion de fichiers locaux et les scripts intersites sont des vecteurs d'attaque courants contre les applications web.
- ▶ Les bots sont une source majeure d'intrusion. Ils recherchent systématiquement les failles et exploitent les vulnérabilités connues des serveurs.
- ▶ 43 % des attaques ciblent les petites entreprises. Il n'y a pas que les grandes sociétés qui sont menacées.

## Une contre-mesure puissante

Le WAF HAProxy Enterprise inspecte les requêtes à la recherche de données malveillantes. Vous contrez ainsi les menaces avant qu'elles n'atteignent vos applications web. Ses trois modes d'utilisation s'adaptent parfaitement à vos besoins.



### Protection nouvelle génération

- Propulsé par notre moteur WAF intelligent avec détection non basée sur la signature
- Haute performance et faible latence
- Sécurité renforcée avec un taux de précision incomparable de 98,526%
- Configuration simple, protection efficace prête à l'emploi sans des règles complexes, avec OWASP transparent et personnalisable Compatibilité CRS si nécessaire
- Détecter et bloquer de manière fiable l'injection SQL (SQLi), intersite scripts (XSS), falsification de requêtes intersites (CSRF) et d'autres menaces courantes



### Compatibilité avec les Core Rule Set (CRS) OWASP

- Une protection robuste contre les menaces Web les plus courantes menaces liées aux applications et aux API
- Amélioré par notre moteur WAF intelligent pour Performances OWASP CRS massivement améliorées et faibles taux de faux positifs par rapport aux autres implémentations OWASP WAF
- Directement intégré à HAProxy Enterprise et au Kubernetes Ingress Controller, pas de serveurs Web supplémentaires ou procurations nécessaires
- Qualité renforcée au niveau entreprise mondiale
- Démontre un net gain de performances par rapport aux autres OWASP Implémentations CRS

### Faites confiance aux experts de HAProxy Technologies

HAProxy apporte à nos clients des performances, une observabilité et une sécurité optimales.

Notre pare-feu pour applications web protège certains des sites web les plus visités au monde.

- Nous l'utilisons nous-mêmes pour protéger HAProxy Edge, qui traite 100 milliards de requêtes par jour.
- Soutenu par une équipe d'ingénieurs et de professionnels réseaux reconnus internationalement.
- Utilisé par des acteurs soumis à une réglementation stricte, dans le domaine financier, commercial et de la santé.