HAPROXY

ESSAI GRATUIT www. haproxy.com | contact@haproxy.com

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. Simplifiez votre défense à l'aide d'un WAF situé au niveau de vos serveurs mandataires (proxys).

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 SQLi / XSS simplifiée

Configurez en quelques minutes la protection contre les injections SQL et les scripts intersites.

- Détection immédiate des injections SQL (SQLi) et des scripts intersites (XSS).
- Configuration simple en quelques minutes.
- Intégration étroite avec les ACL et la journalisation HAProxy.
- Prend en charge diverses réponses, notamment *deny*, *silent drop* et *tarpit*.
- La liste des signatures SQLi peut être mise à jour dynamiquement sur un cluster d'instances HAProxy.

Liste blanche avancée

Pour contrôler strictement les accès, utilisez le mode liste blanche avancé.

- Ensemble strict de règles pour une sécurité Zero Trust.
- Une liste blanche détaillée n'autorise que les comportements attendus.
- Bloque les attaques SQLi et XSS, l'inclusion de fichiers à distance, les failles de traversement de répertoires (TRV), les attaques par évasion et bien plus encore.
- Intégration étroite avec les ACL et la journalisation HAProxy.
- Prend en charge diverses réponses, notamment *deny, silent drop* et *tarpit*.
- Les règles de liste blanche se basent sur le chemin de la requête, une variable, ou une combinaison des deux.

ModSecurity

Protège contre les attaques à l'aide du leader du marché, ModSecurity.

- Bloque l'injection SQL, les scripts intersites, l'exécution de code à distance et plus encore...
- Utilisez l'ensemble de règles de base ModSecurity de l'OWASP ou définissez vos propres règles.
- Directement intégré à HAProxy Enterprise et au contrôleur Ingress Kubernetes ; aucun serveur web ou proxy supplémentaire n'est nécessaire.
- Version renforcée de ModSecurity.
- Apporte un net gain de performance par rapport aux autres mises en œuvre de ModSecurity.

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 70 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.