



Sécurité haute performance pour les applications et les APIs

Chaque application est différente. Au lieu d'une solution universelle, HAProxy Enterprise fournit des couches de sécurité personnalisables qui constituent les éléments constitutifs de la sécurité des applications et des API. Nous vous donnons le pouvoir de construire une sécurité approfondie, ciblée et évolutive, parfaitement adaptée à votre infrastructure.

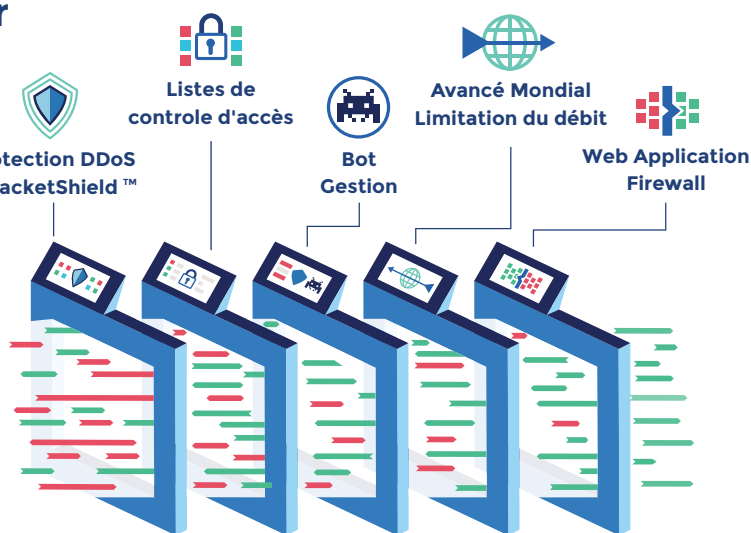
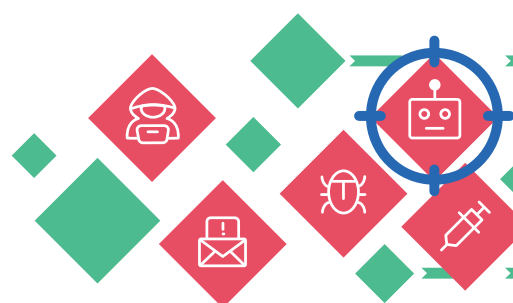
Maitrisez la protection en profondeur

Une ligne de défense unique est inévitablement vouée à l'échec. Combinez les couches de sécurité hautes performances de HAProxy Enterprise pour former une défense à toute épreuve contre un large éventail de menaces.

Le filtrage des paquets au débit linéaire, les listes de contrôle d'accès (ACL), les empreintes digitales des clients, le suivi en temps réel à l'échelle du cluster et notre WAF travaillent ensemble pour partager des informations et prendre des décisions rapides et précises.

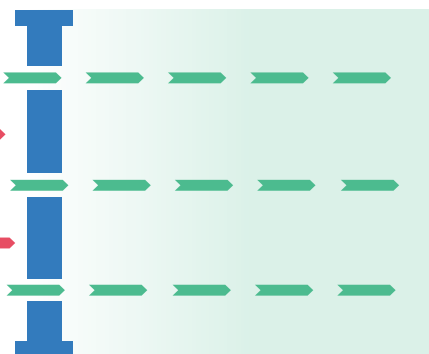
Déjouez les menaces évolutives

Depuis les DDoS jusqu'à la fraude, les robots automatisés menacent votre entreprise à grande échelle. Utilisez la puissance des couches de sécurité sophistiquées de HAProxy pour inspecter, filtrer et protéger le trafic réseau en temps réel. Détectez et bloquez efficacement vos plus grandes menaces, y compris le Top Ten OWASP.



Implémentez une sécurité flexible

Vos profils de trafic et de menaces sont uniques. Ce qui semble normal pour d'autres entreprises déclenche des signaux d'alarme pour la vôtre. HAProxy Enterprise vous permet de personnaliser les signaux de sécurité, les pondérations et les seuils qui déterminent les réponses à chaque couche. Prenez des décisions éclairées sur les attaques et les activités anormales affectant vos systèmes.



Les bases de la sécurité applicative

Les incidents de sécurité tels que les attaques DDoS, les menaces de robots et le vol de données coûtent aux entreprises des millions en perte de revenus. Les capacités de sécurité de HAProxy exploitent une base de code extrêmement efficace, flexible et dynamique, avec une pile SSL robuste, des systèmes de suivi ACL et Stick Table de pointe.

HAProxy Enterprise et **HAProxy Fusion** vous permettent de devancer les menaces actuelles en étendant les fonctionnalités de base de HAProxy. Ceux-ci incluent une analyse comportementale en temps réel à l'échelle du cluster ; inspection du contenu ; politiques de réponse adaptatives ; un WAF performant ; et gestion centralisée des politiques de sécurité, des certificats SSL et de l'observabilité.

ACL et suivi avancés

► Les listes de contrôle d'accès (ACL) flexibles fournissent une correspondance basée sur une myriade d'options :

- IP/CIDR
- Données SSL
- Support de cartographie des fichiers
- Gestion des opérateurs logiques
- Requêtes/entêtes de réponses et chemins

► Suivi temps réel de l'ensemble du cluster

- Stockage de valeurs de clé génériques
- Combinaison de n'importe quel nombre de métriques
- Suivi en temps réel sur n'importe quel nombre de métriques :
 - Compteur de taux de requêtes/erreurs
 - Vues uniques de pages par IP ou User-Agent
 - Taux et compteur de User-Agent uniques par IP
 - Nombre de violations du WAF par IP ou User-Agent
 - Et beaucoup plus...

Protection contre les DDoS et les robots

► Détecte et protège contre :

- Les submersions (flood) de GET/POST
- Le Web scraping
- Le brute force
- La vulnérabilité aux scanners
- Et beaucoup plus...
- Suivi d'empreintes avancée

► Politiques de réponses :

- Limitation du taux de requêtes, du Shadow banning, du tarpitting et du dropping
- Support du challenge/response et du reCAPTCHA



Empreinte client

- Identification immédiate des robots et scanners
- Triangulation de données pour créer un ID unique
- Découvre les clients qui falsifient des entêtes HTTP

Web Application Firewall

- Haute performance
- Support des signatures / listes noires
- Support des listes blanches
- Support des jeux de règles ModSecurity
- Journalisation détaillée
- Mode Liste blanche seul

SSL

- ECC/RSA
- OCSP Stapling
- Réduction de latence via le moteur OpenSSL Async
- Reprise de session TLS
- Protection 'Heartbleed' intégrée
- Reprise du temps d'aller-retour nul (0-RTT)

Fonctionnalités complémentaires

- Nettoyage des entêtes HTTP
- Injection de corps de réponse
- Support du masquage IP
- Support de programmation LUA
- API d'exécution
- Support de la mise à jour dynamique