Parc d'Activités Schweitzer
26 rue du bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

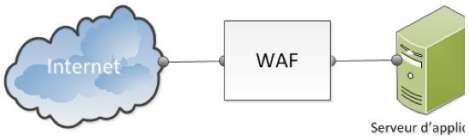
espace technologie

FICHE CONSEIL

WAF
Web Application Firewall

Protection des Sites Web et des Logiciels exposés sur le Web

Notre solution « WAF » est un pare feu applicatif, développée par un éditeur français de logiciels de cyber sécurité. C'est une solution de sécurisation des sites web et logiciels exposés sur Internet grâce à son Intelligence Artificielle et à ses algorithmes d'analyse comportementale.



Nous utilisons aussi l'application WAF pour sécuriser les logiciels métiers nécessitant un navigateur internet afin d'éviter les intrusions et compromissions liées aux failles de sécurité générées par l'applicatif.

Il est courant que des éditeurs de logiciels métiers ouvrent un port du réseau pour communiquer vers l'extérieur. Notre solution WAF permet d'analyser les flux et bloquer les requêtes malveillantes, réduisant ainsi la surface d'attaque.

❖ L'Intelligence artificielle au service de la sécurité des applications Web

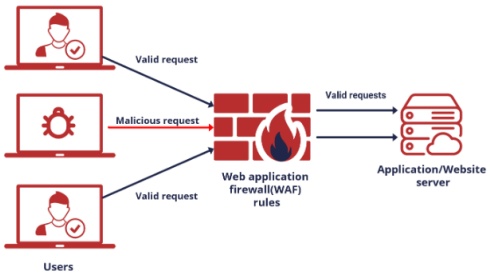
- I.A. : Nous utilisons une technologie d'Intelligence Artificielle pour effectuer une analyse complète et très performante de toutes les requêtes en transit vers votre site, application web ou logiciel nécessitant une ouverture de ports.

- **Analyse des menaces connues :** La première, validée par nos analystes sécurité, intègre les règles de sécurité de l'IA permettant la protection contre les attaques connues. Elle est capable de détecter toutes les failles de sécurité référencées dans les rapports OWASP, et vous protègent ainsi dès la mise en place de la solution.

- **Apprentissage des modèles de comportement :** L'intelligence artificielle prend le relais. Ce système apprend les comportements de navigation des utilisateurs et détecte les comportements suspects. Ainsi, lors d'une session de navigation, le « WAF » évalue la confiance des requêtes en fonction de nombreux critères (réputation de l'IP, analyse du comportement de navigation, contenu de la requête, etc.) et est capable de distinguer parfaitement les attaques des comportements normaux.

- **Au final :** L'IA définit un comportement type, face à chaque site web protégé. Les utilisateurs qui s'éloignent trop de ce comportement type, sont automatiquement rejetés. De plus, notre intelligence artificielle possède une forte capacitée d'adaptation. En effet, lors de changement sur un site web (ajout ou modification de pages, complète refonte du site, etc.), l'intelligence s'adapte à ces nouvelles évolutions jusqu'à réinitialiser son profil type pour en recréer un nouveau.

❖ Protection en temps réel et sur mesure de vos applications web



· **Protection sur mesure :** Notre moteur d'intelligence artificielle compare chaque requête reçue aux comportements typiques de vos utilisateurs et décidera si elle doit être acceptée ou bloquée.

· **Zéro Day :** La politique de sécurité du WAF de Nouvelle Génération est basée sur le comportement des utilisateurs et sur le chemin possible de navigation de chaque site protégé. Une nouvelle attaque, l'exploitation d'une nouvelle vulnérabilité seront alors bloquées car sortant du champ normal d'utilisation de votre application web. Aucune attaque et même les 0-Day ne peuvent traverser le WAF que nous proposons.

· **Customisation fine de la configuration :** La plateforme d'administration en ligne permet de garder un œil sur toutes les requêtes entrantes sur le site (ainsi que les bots). La configuration, facilement compréhensible, peut être modifiée à tout moment pour accepter ou rejeter une requête spéciale, créer des exceptions sur les URL, whitelister des IP unitairement ou bloquer des pays.

· **Certificat SSL :** Notre protection WAF fournit automatiquement et gratuitement un certificat SSL. Ce certificat est mis à jour automatiquement. Il est aussi possible d'ajouter son propre certificat via le dashboard.

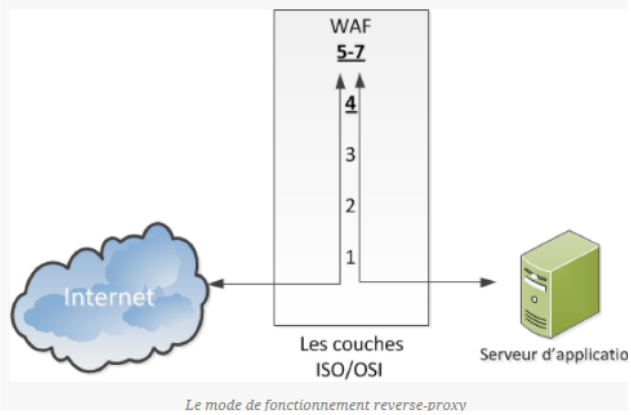
Fonctionnalités		Nous contacter
Protection contre les attaques connues (Owasp10)	√	√
Protection par IA & analyses comportementales	√	√
Protection contre malware/ ransomware	√	√
Protection contre le vol de données	√	√
Protection contre le brute force	√	√
Protection contre les malicious Bots	√	√
Protection contre le DDOS	√	√
Visualisation des attaques en temps réels	√	√
Partage de tableau de bord (multi user)	√	√
Gestion URL + IP Exception	√	√
Blocage par pays	√	√
Certificat ssl inclus	√	√
Jusque 10 Millions de requêtes / mois	√	> 10 Millions
Cluster OGO dédié		√
Conservation des logs		√
API de Log		√
API Provisionning + Dashboard		√

❖ Un Dashboard pour visualiser les informations essentielles

Pour les GEEKS

❖ Un peu de technique – Firewall Vs Firewall Applicatif (WAF)

OSI est un mode permettant de normaliser l'interconnexion de systèmes informatiques.



Le mode de fonctionnement reverse-proxy

<u>Il est composé de 7 couches :</u>

Couche 7 – La couche d'**application**. ...
Couche 6 – La couche de **présentation**. ...
Couche 5 – La couche **session**. ...
Couche 4 – La couche de **transport**. ...
Couche 3 – La couche **réseau**. ...
Couche 2 – La couche de **liaison de données**.
Couche 1 – La couche **physique**.

Le Firewall classique, équipement indispensable pour la sécurité de votre système d'information, protège les couches 1 à 4.

Afin de protéger les couches dites applicatives (5 à 7) le WAF doit être mis en place afin de compléter la sécurité du Firewall.

S'agissant de couches applicatives la protection n'est utile que pour les sites Web et les logiciels exposés sur Internet.

La solution WAF est devenu indispensable pour éviter le piratage de vos sites Web ainsi que pour les logiciels nécessitant un navigateur et ceux échangeant des données vers l'extérieur.

78% des sites WEB présentent des Vulnérabilités

Pôle Activ'Océan
9 Rue de Bois Fossé - BP 147
85301 CHALLANS Cedex

Tél. : 02 51 49 31 31
Email : contact@espace-technologie.com
Web : www.espace-technologie.com

Organisme de formation n° 52850059385 - SAS au capital de 38 500 € - Siret : 38979357100024 - APE : 4741Z - RCS La Roche sur Yon B389793571