LE MACHINE LEARNING PLACE FORTIWEB À LA TÊTE DES SOLUTIONS WAF

RÉSUMÉ

Des entreprises comptant de plus en plus sur les applications Web et un paysage des menaces en constante évolution et de plus en plus redoutable, confèrent aux firewalls pour application Web (WAF) une place centrale dans l'architecture de sécurité de l'entreprise. Tous les WAF n'offrent toutefois pas des fonctionnalités de sécurité et un dimensionnement adaptés aux entreprises. C'est dans ce domaine que FortiWeb se démarque de la concurrence.

FortiWeb est une solution WAF hautement évolutive et robuste qui répond aux exigences des entreprises en matière de sécurité et d'opérations. FortiWeb excelle notamment dans l'utilisation du machine learning (apprentissage automatique) basé sur l'intelligence artificielle (IA) pour contrer les attaques « zero-day » et les vulnérabilités connues. Dans le même temps, cette technologie lui permet d'éliminer quasiment tous les faux positifs qui empoisonnent les autres solutions WAF. De plus, FortiWeb s'intègre en toute transparence à Fortinet Security Fabric, offrant un partage bidirectionnel des renseignements sur les menaces, notamment avec FortiSandbox, ainsi que l'automatisation des flux de travail et processus de sécurité.

FORTIWEB EXCELLE DANS LES FONDAMENTAUX DU WAF

Si l'on prend en compte les composants de base de la sécurité des applications Web, les WAF FortiWeb sortent indéniablement du lot. En 2017, Gartner considérait Fortinet comme un « challenger » dans le WAF Magic Quadrant[1], tandis que NSS Labs décrivait FortiWeb comme un « leader du marché » et lui attribuait l'évaluation « produit recommandé[2] ». Passons à nouveau en revue les principales raisons qui ont valu une telle reconnaissance à FortiWeb :

1. LE MOTEUR DE DÉTECTION DE SIGNATURES

Chaque produit autonome WAF comprend un moteur de détection de signatures, mais le flux de signatures utilisé par les WAF FortiWeb est unique. Il est mis à jour fréquemment et automatiquement à l'aide de données fournies par FortiGuard Labs, service Fortinet de premier ordre de renseignements sur les menaces. De plus, les WAF FortiWeb ont la possibilité d'intégrer des informations analytiques sur les menaces provenant d'autres périphériques connectés à la solution Fortinet Security Fabric, dont les pare-feux FortiGate et certains services tiers.

2. L'ANALYSE DE LA SOURCE

Les fonctionnalités de réputation IP de FortiWeb surveillent la source du trafic des applications Web. FortiWeb compare en particulier l'adresse IP d'origine d'un paquet à une liste noire et, à une liste blanche constamment mises à jour par FortiGuard Labs et d'autres périphériques Security Fabric. FortiWeb utilise également l'empreinte du périphérique pour identifier les sources du trafic et mettre à jour de manière dynamique le score du risque de l'émetteur en matière de réputation d'après le comportement du périphérique.

3. LA VALIDATION DE PROTOCOLE

La validation de protocole est un autre domaine dans lequel FortiWeb excelle. Grâce à la validation de protocole, FortiWeb vérifie que le trafic des applications Web est conforme en tout point aux normes HTTP RFC. Il peut ainsi mettre fin aux attaques visant à exploiter les faiblesses des protocoles Web.

PRINCIPALES CARACTÉRISTIQUES DE FORTIWEB

- Une approche double couche sophistiquée du « machine learning », basée sur une véritable intelligence artificielle, qui permet d'obtenir une précision de détection des menaces optimale tout en limitant les faux positifs
- Un moteur de détection de signatures qui s'appuie sur le service de renseignements sur les menaces de FortiGuard Labs et d'autres périphériques de la solution Fortinet Security Fabric
- Des vérifications dynamiques de la réputation IP à l'aide du service de renseignements sur les menaces et de l'empreinte des périphériques FortiWeb
- Un moteur antivirus primé
- L'intégration à Fortinet Security Fabric, qui facilite l'analyse sandbox approfondie des alertes de menace
- Une gestion intégrée rationalisée pour une administration réduite et une conformité accrue

4. LE MOTEUR ANTIVIRUS

Les fonctionnalités antivirus constituent un prérequis essentiel au fonctionnement d'un WAF. Dans le cas de FortiWeb, le moteur antivirus primé de FortiGuard Labs est utilisé pour analyser le trafic afin de détecter d'éventuelles menaces risquant d'infecter les serveurs ou les autres périphériques du réseau.[3]

5. ÉVOLUTIVITÉ ET PERFORMANCES

FortiWeb affiche le plus haut débit protégé WAF du marché.[4] En fait, le débit protégé de FortiWeb est capable d'atteindre 20 Gbit/s, soit le double du débit protégé officiel du deuxième WAF le plus rapide. Grâce à cette vitesse record, FortiWeb peut évoluer pour gérer les volumes toujours plus importants du trafic Web.

6. L'INTÉGRATION DE LA SÉCURITÉ

D'autres solutions WAF restent cloisonnées et ne s'intègrent pas à l'architecture de sécurité globale. Il en résulte un manque d'efficacité et de performance, car elles ne parviennent pas à suivre le rythme du paysage sophistiqué des menaces qui comprend des attaques polymorphes et multivectorielles.

En revanche, FortiWeb s'intègre de manière transparente à la solution Fortinet Security Fabric. De ce fait, les équipes de sécurité et réseau passent nettement moins de temps à compiler et à interpréter les journaux de sécurité manuels et autres informations. FortiWeb assure également la détection et la prévention des intrusions en temps réel. Par exemple, lorsqu'il identifie un fichier joint suspect, FortiWeb le transmet à FortiSandbox qui l'examine de plus près. L'intégration aux principaux scanners de vulnérabilités tiers permet à FortiWeb de fournir des correctifs virtuels dynamiques pour résoudre les problèmes de sécurité détectés dans les environnements applicatifs.

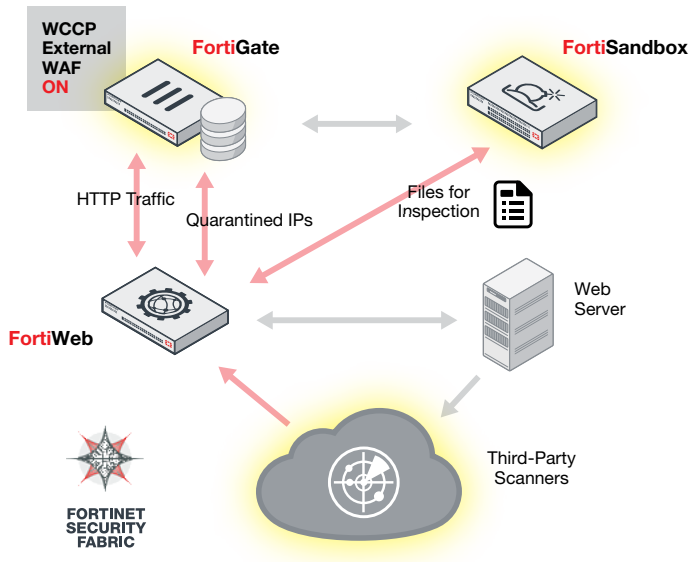

SCHÉMA 1 : L'INTÉGRATION À D'AUTRES ÉLÉMENTS DE FORTINET SECURITY FABRIC, NOTAMMENT FORTIGATE ET FORTISANDBOX, ASSURE LA PROTECTION DES APPLICATIONS ET ÉTEND L'ANALYSE DES VULNÉRABILITÉS AUX PRINCIPAUX FOURNISSEURS TIERS.

Les fonctionnalités de machine learning basé sur l'intelligence artificielle de FortiGuard Labs s'appuient sur **des dizaines de milliers d'attaques connues** pour définir une analyse comportementale.

FortiWeb est capable d'atteindre **un débit protégé de 20 Gbit/s.** Il s'agit du double du débit protégé officiel du deuxième WAF le plus rapide.

FORTIWEB EN TÊTE DU MARCHÉ WAF GRÂCE À SES CAPACITÉS DE DÉTECTION DE COMPORTEMENT

Nombreux sont les fournisseurs de solutions WAF qui proposent la détection de menaces comportementales basée sur l'apprentissage des applications, ce qui est extrêmement basique.[5] Ces solutions comparent le trafic des applications Web aux modèles observés et signalent tous les écarts par rapport à ces normes. Dans cette approche, il est donc nécessaire d'enquêter sur chaque comportement d'utilisateur ou de périphérique que le WAF n'a pas observé auparavant. Cette tâche mobilise un nombre démesuré de ressources humaines. Cela pose véritablement problème dans un environnement où les responsables sécurité doivent déjà faire face à un manque de personnel qualifié en sécurité et à des budgets plus restreints.[6] Au final, le personnel déjà surchargé se retrouve encore plus démuni et les risques augmentent.

Dans ce cas de figure, identifier les véritables menaces affectant les applications Web protégées, tout en limitant le nombre de faux positifs, nécessite un véritable apprentissage automatique basé sur l'intelligence artificielle (« AI-based machine learning »). FortiWeb est le seul à proposer cette fonctionnalité.

FortiWeb adopte une approche multicouche de la technologie de détection du comportement. La première couche de « machine learning » construit un profil et un modèle mathématique pour chaque paramètre de l'application Web protégée. Elle surveille les variations des différents paramètres, en utilisant des données à dimensions multiples pour évaluer la probabilité qu'une variation représente une anomalie.

Chaque fois qu'une variation atteint un seuil prédéfini sur cette échelle de probabilité, FortiWeb l'envoie à une deuxième couche de machine learning afin de déterminer s'il s'agit d'une menace. L'anomalie est comparée à des modèles de menaces continuellement mis à jour, développés et gérés par FortiGuard Labs. Ces modèles s'appuient sur des analyses de dizaines de milliers d'attaques connues. Ils comprennent une fonction de détection basée sur la syntaxe afin d'identifier les attaques par injection SQL, ainsi qu'un code de machine learning spécialement conçu pour reconnaître les exploitations dans les scripts site à site, l'injection dans le système d'exploitation et autres attaques. Enfin, lorsque l'équipe FortiGuard Labs identifie de nouvelles attaques, elle envoie automatiquement à FortiWeb les modifications de modèle de menace en temps réel.

Cette approche à double couche limite les faux positifs en s'assurant que seules les attaques avérées sont bloquées plutôt que n'importe quelle anomalie mineure, comme cela se produit avec les WAF basés sur l'apprentissage applicatif.

UNE GESTION ET UN REPORTING RATIONALISÉS

FortiWeb limite également les exigences en matière de gestion. Alors que les utilisateurs d'Akamai se plaignent d'une « courbe d'apprentissage plus longue que prévu » et que ceux de Barracuda Networks s'inquiètent du manque d'agrégation d'alertes du produit[7], FortiWeb ne requiert quasiment pas de ressources pour déployer et configurer. L'approche de la gestion des WAF choisie par Fortinet tient en trois mots : « programmez et oubliez ».

Cette facilité d'utilisation est optimisée par les fonctions d'analyse graphique et de reporting de pointe de FortiWeb. Les responsables sécurité peuvent facilement visualiser et explorer en détail les éléments clés de FortiWeb, tels que les configurations IP ou serveur, les journaux des attaques et du trafic, les cartes d'attaques et les activités des utilisateurs. Autrement dit, le personnel peut comprendre en un coup d'œil et de manière approfondie les menaces qui pèsent sur les applications Web de l'entreprise et allouer bien moins de ressources à l'obtention de ces informations analytiques.

En outre, comme FortiWeb est un élément principal de la solution Fortinet Security Fabric, il peut s'intégrer dans un tableau de bord de gestion unifiée de la sécurité à l'échelle de l'entreprise via FortiSIEM ou FortiAnalyzer. Ce modèle consolidé de suivi et de reporting en temps réel, qui s'étend à tous les domaines de la sécurité, permet aux responsables sécurité de démontrer la conformité de l'entreprise aux normes de sécurité et spécifications du secteur, allant des normes 800 NIST (National Institute of Standards and Technology) aux normes ISO 27001 en passant par les normes de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS).

FortiWeb permet de réduire **jusqu'à 30%** le coût total de possession par connexion protégée.[8]

L'identification de toutes les menaces réelles affectant les applications Web protégées, tout en limitant le nombre de faux positifs, **nécessite un véritable apprentissage automatique basé sur l'intelligence artificielle (« AI-based machine learning »).**

FortiWeb utilise la détection comportementale des menaces basée sur l'apprentissage applicatif, ce qui lui permet de limiter les faux positifs **en s'assurant que seules les attaques avérées sont bloquées** plutôt que n'importe quelle anomalie mineure.

SYNTHÈSE

En adoptant une approche multicouche complète et corrélée de la sécurité des applications Web, FortiWeb protège les applications Web contre les 10 principaux risques en matière de sécurité, tels qu'identifiés par l'Open Web Application Security Project (OWASP).[9] Comparé aux autres WAF, FortiWeb élimine quasiment tous les faux positifs et détecte avec précision les exploitations connues et inconnues qui ciblent les applications Web.

En outre, avec l'explosion du trafic et l'évolution et l'intensification du volume, de la rapidité et de la sophistication des menaces, FortiWeb, qui affiche le débit protégé WAF le plus rapide du marché, offre une solution WAF qui peut facilement évoluer et s'étendre pour répondre à ces nouveaux défis.

Son utilisation du machine learning basé sur l'intelligence artificielle pour la détection des menaces comportementales, parallèlement à son intégration à Security Fabric, démarque FortiWeb de toutes les solutions WAF concurrentes disponibles sur le marché. De ce fait, les responsables sécurité sont en mesure d'améliorer la sécurité sur deux plans à la fois : l'efficacité et l'efficience.

Références :

[1,5,7] Jeremy D'Hoinne, Adam Hils et Claudio Neiva, « Magic Quadrant for Web Application Firewalls », Gartner, 7 août 2017.

[2] « Web Application Firewall Group Test », NSS Labs, 11 avril 2017.

[3] « AV-Comparatives Awards », consulté le 25 mai 2018.

[4] D'après des données publiées dans Fortinet et des fiches techniques de produits concurrents.

[6] Jon Oltsik, « Research suggests cybersecurity skills shortage is getting worse », CSO Online, 11 janvier 2018.

[8] D'après des recherches internes réalisées par Fortinet.

[9] « OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks », The OWASP Foundation, consulté le 25 mai 2018.

SIÈGE SOCIAL INTERNATIONAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1 408 235 7700
www.fortinet.com/sales

France
TOUR ATLANTIQUE
24ème étage,
1 place de la Pyramide
92911 Paris
La Défense Cedex
France
Ventes: +33 (0) 1 80 42 05 40

SUCCURSALE EMEA
905 rue Albert Einstein
06560 Valbonne
France
Tél. : +33 4 8987 0500

SUCCURSALE APAC
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapour 038988
Tél. : +65 6395 7899
Fax : +65 6295 0015

AMÉRIQUE LATINE — SIÈGE SOCIAL
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Tél. : +1 954 368 9990

222603-0-1-FR