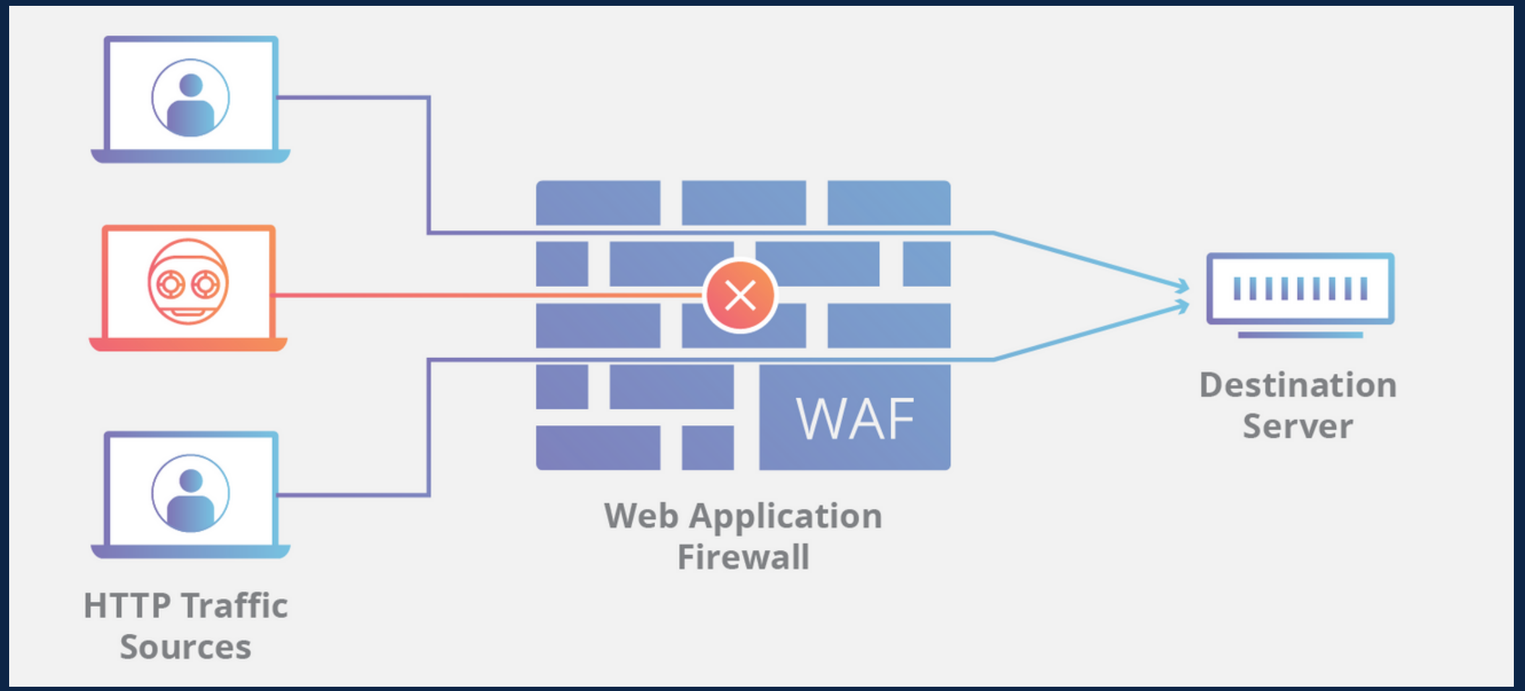
WAF

Web Application Firewall

Anthony Semal

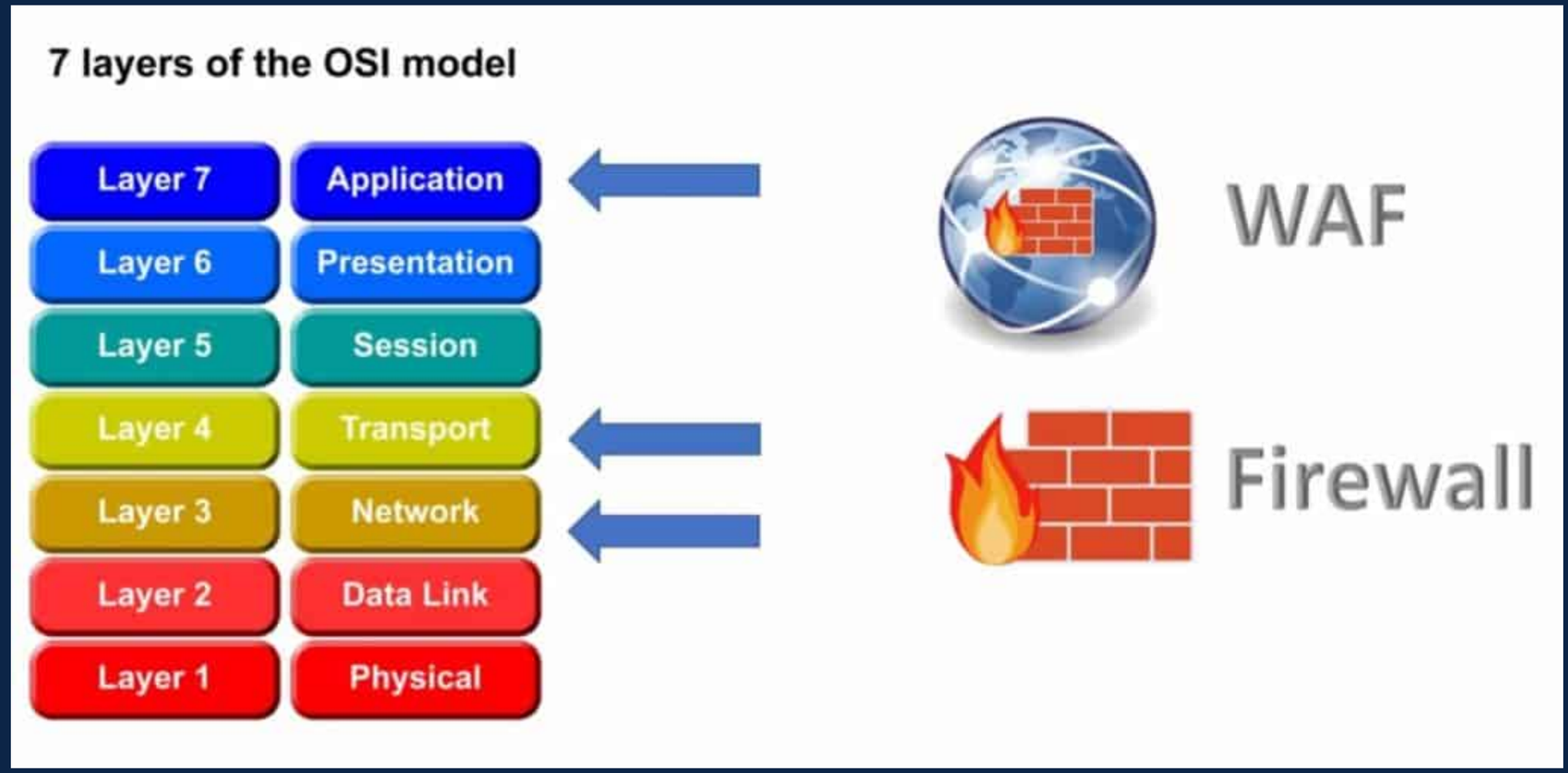
Qu'est ce que c'est

Un WAF crée un bouclier entre une application Web et Internet ; ce bouclier peut aider à atténuer de nombreuses attaques courantes.



Injection SQL, XSS, attaques zero-days, DDOS

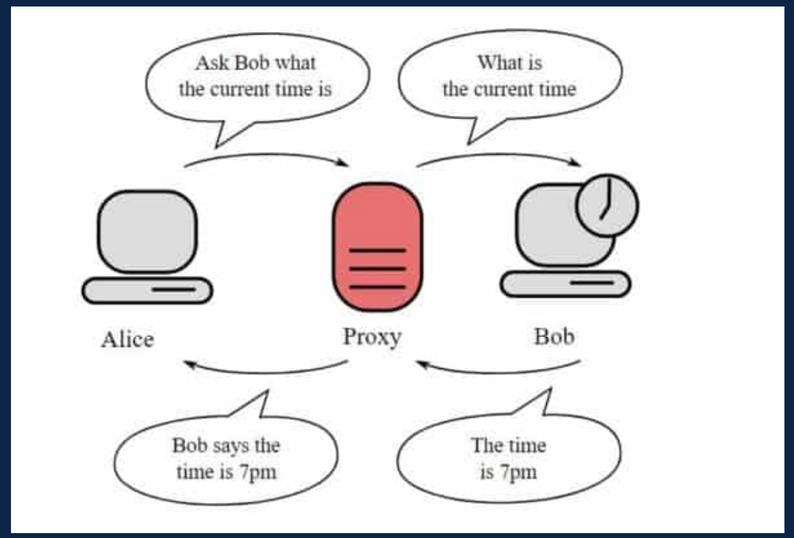
La couche application



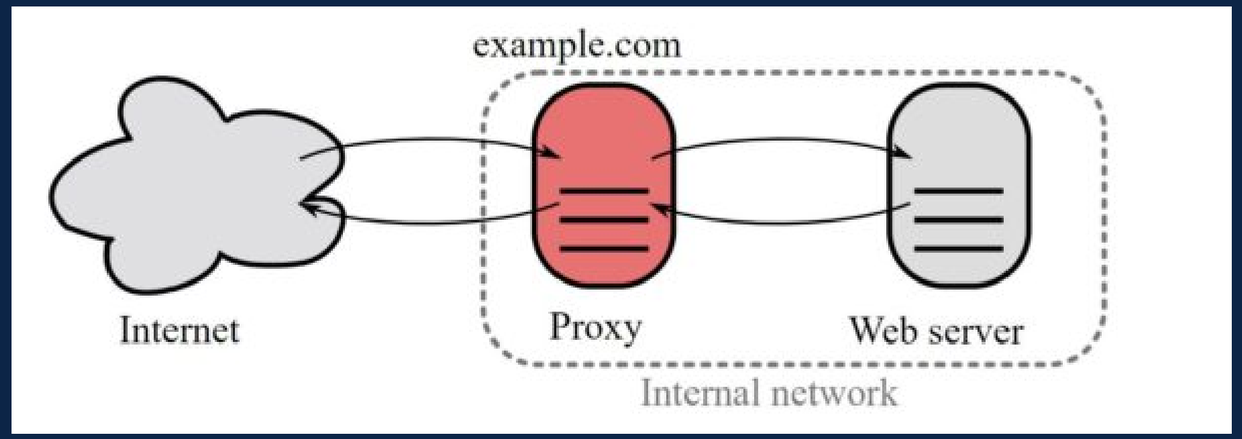
Proxy inverse

Un utilisateur qui veut accéder à un serveur de l'entreprise

Simple intermédiaire entre deux entités



Le proxy (servant aussi de cache) gère les demandes des deux entités
Les internautes ne verront que le proxy



Fonctionnement

Ensemble de règles (ou politiques)

Liste Blanche

- Refuse par défaut toutes les demandes
- Moins gourmande en ressources que la liste noir
- Peut refuser le trafic légitime

Liste Noire

- Laisse passer les paquets
- Utilise des signatures prédéfinies pour bloquer
- Gourmande en ressources
- Nécessite plus d'informations pour filtrer les paquets

Sécurité Hybride

Un peu de blanche, un peu de noir

Mode Logging ou blocking

Logging: requêtes suspectes sont enregistrée mais pas bloquées pour éviter les faux positifs

Blocking: Les attaques détectées sont bloquées

Type de WAF

WAF en réseau

- Installés au niveau local
- Latence réduite
- Option coûteuse
- Espace/maintenance

WAF basé sur l'hôte

- Intégré dans le logiciel
- Plus personnalisable
- Consommation

Hébergé sur le cloud

- Facile à mettre en œuvre
- Coût minimal
- Gestion minimale
- Devoir faire confiance au gestionnaire du service

Avantages

Niveau de sécurité supplémentaire:

Associé à d’autres mesures de sécurité, un WAF offre un niveau de protection supplémentaire contre les accès non autorisés.

Protection des anciens systèmes et des anciennes applications:

Les failles de sécurité peuvent persister longtemps, en particulier avec les logiciels utilisés depuis longtemps et qui n’ont pas été programmés en interne. Un WAF offre ici une sécurité supplémentaire.

Inconvénients

ou plutot ses limites

- Un WAF n’offre pas une protection complète
  il doit toujours faire partie d’une stratégie de sécurité globale.
- WAF ne protège pas contre les logiciels malveillants déjà présents sur le réseau.
- Un WAF reste un logiciel et peut aussi comporter des vulnérabilités.
- JavaScript et d’autres contenus web actifs ne sont actuellement pas pris en charge par de nombreux pare-feu d’applications web.

Quelques outils

ModSecurity

https://github.com/SpiderLabs/ModSecurity

https://www.linuxcapable.com/how-to-install-nginx-with-modsecurity-3-on-ubuntu-22-04-lts/

https://www.it-connect.fr/installation-de-mod_security-devant-un-serveur-web-apache/

Naxsi

https://www.proteansec.com/application-security/naxsi/

AQTRONiX WebKnight

https://www.iis.net/downloads/community/2016/04/aqtronix-webknight

Cloudflare, Amazon, Microsoft, etc...

https://geekflare.com/fr/web-application-firewall/

Sources

https://actualiteinformatique.fr/cybersecurite/quest-ce-que-le-waf-web-application-firewall

https://www.cloudflare.com/fr-fr/learning/ddos/glossary/web-application-firewall-waf/

https://desgeeksetdeslettres.com/cybersecurite/waf-pare-feu-application-web

https://cyberguide.ccb.belgium.be/fr/utilisez-pare-feux

https://www.crowdstrike.com/cybersecurity-101/web-application-firewall/

https://www.oracle.com/fr/security/waf-definition-pare-feu.html

https://aws.amazon.com/fr/waf/

https://fr.wikipedia.org/wiki/Web_application_firewall

https://www.malekal.com/waf-web-application-firewall-proteger-son-serveur-web-attaques-dos-piratages/#Les_limites_des_WAF

https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quun-reverse-proxy-le-serveur-reverse-proxy/

Quand Chat Chafouin dit wouaf trop souvent, c'est que le monde va de mal en pis