

Pare-feu d'applications Web basé sur l'informatique en nuage

Promoteur :
Dr Bennouar Djamal

Par :
- Bourezane Nabil
- Tounani Abdellah

Blida, juin 2013



Plan

- Introduction
- Problématique
- Une solution
- Conception
- Mitigation des attaques
- Mise en production
- Conclusion

Introduction

Sécurité des applications Web



Introduction

- Les application web sont devenues omniprésentes.
- 50 millions de sites sont créés en 2012.
- Une grande partie des attaques destinées vers les entreprises représente les attaques sur les applications web.
- **55** % des vulnérabilités dévoilées concernaient des applications Web.
- **74** % des vulnérabilités affectant les WebApp restent sans patch de remédiation.



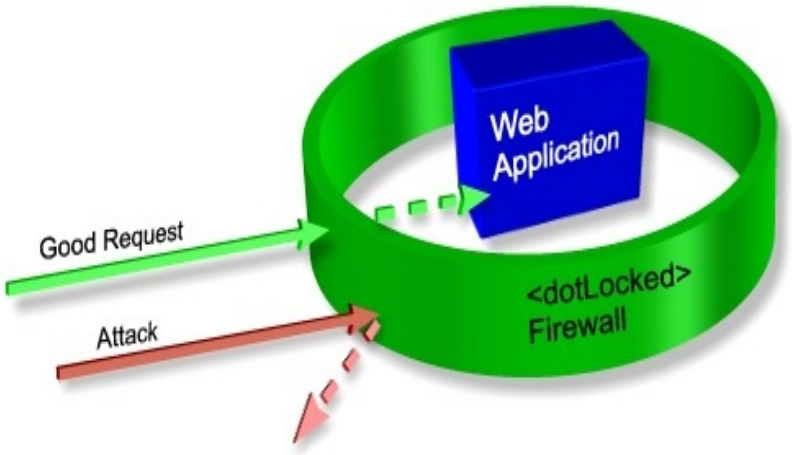
Concept de la sécurité Web

- Une gestion de risque :

$$Risque = \frac{Menace * Vulnérabilité}{Contre - mesure}$$

- Un investissement et une chaîne.
  - l'application a la sécurité de son maillon le plus faible.

- <u>Solutions pour la sécurité Web</u> :
  - ➔ Frameworks de sécurité Web
  - ➔ IDS/IPS
  - ➔ Pare-feux d'applications Web



Problématique

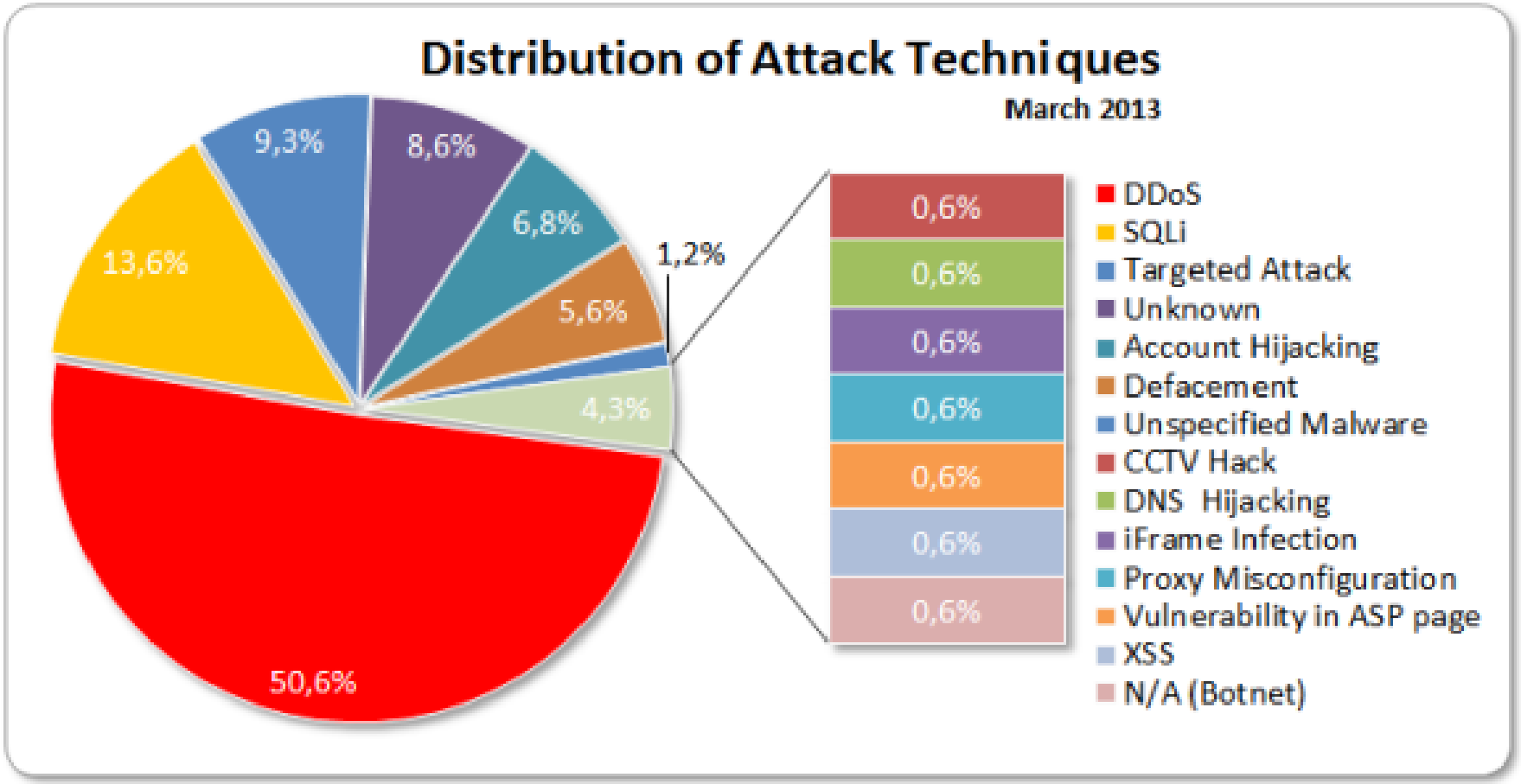
Défis de la sécurité des WebApp



La problématique

- Assurer la sécurité de son application Web et la maintenir est un défi auquel sont souvent confrontés les administrateurs des applications Web et les responsables informatiques des petites et moyennes entreprises.
- L'utilisation des pare-feux d'applications Web tente de limiter ces risques, par exemple : la norme de sécurité PCI DSS exige dans sa première condition de « construction et maintien d'un réseau sécurisé » : « l'installation et la gestion d'une configuration de pare-feu pour protéger les données des titulaires de cartes. »

Problématique - Hacktivisme





Problématique - Génération actuelle des par-feux

- Un nombre très limité de solutions open-sources dont une seule avec une communauté professionnelle (ModSecurity).
- Solutions mono-serveur destinées aux experts (regex)
- Inefficaces contre les attaques de masse ex. : DDoS.
- L'assistance, le soutien et l'évaluation continuelle sont une responsabilité de professionnels qui n'est pas donnée à tout le monde.

La solution

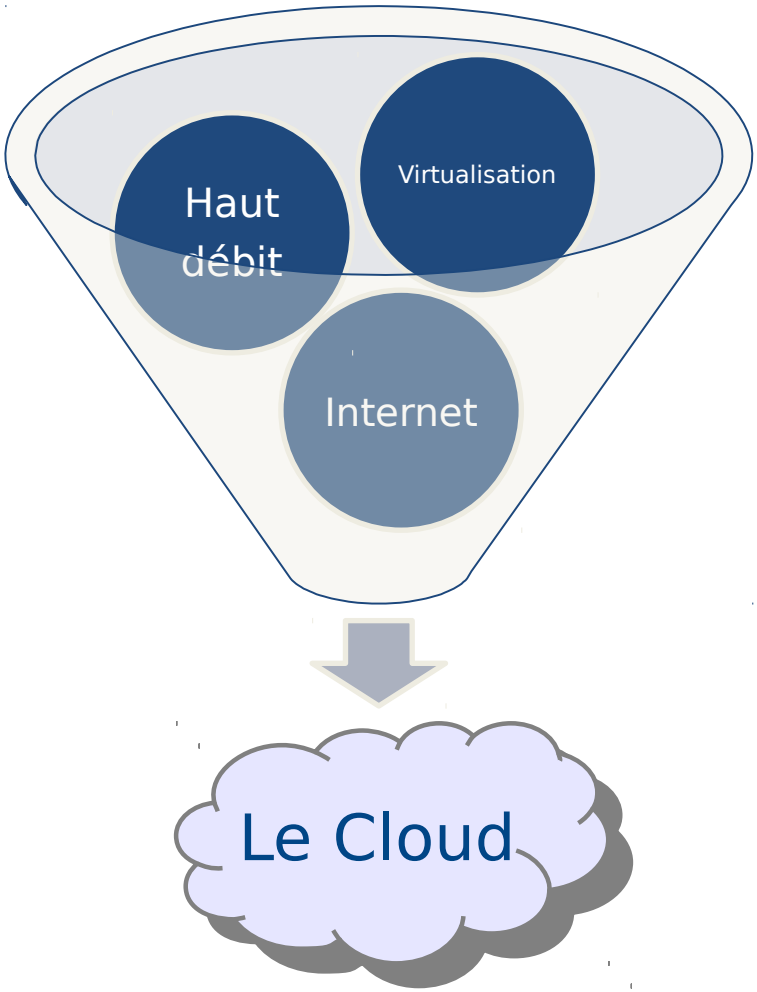
L'externalisation de la sécurité



L'idée

- Proposer un pare-feu distribué en nuage entant que service à la demande.
- Centralisé et étendu géographiquement, il participe d'une façon presque native au routage des requêtes sur Internet.
- Et donc, il pourra filtrer le trafic selon la politique posée pour l'abonné et le délivrer d'une façon optimisée à l'application.

Le Cloud Computing



1. Le libre-service à la demande
2. Un large accès au réseau
3. Des ressources mutualisé
4. Une élasticité vivace
5. Un service mesuré et facturé

Conception

Une architecture évolutive et hautement disponible

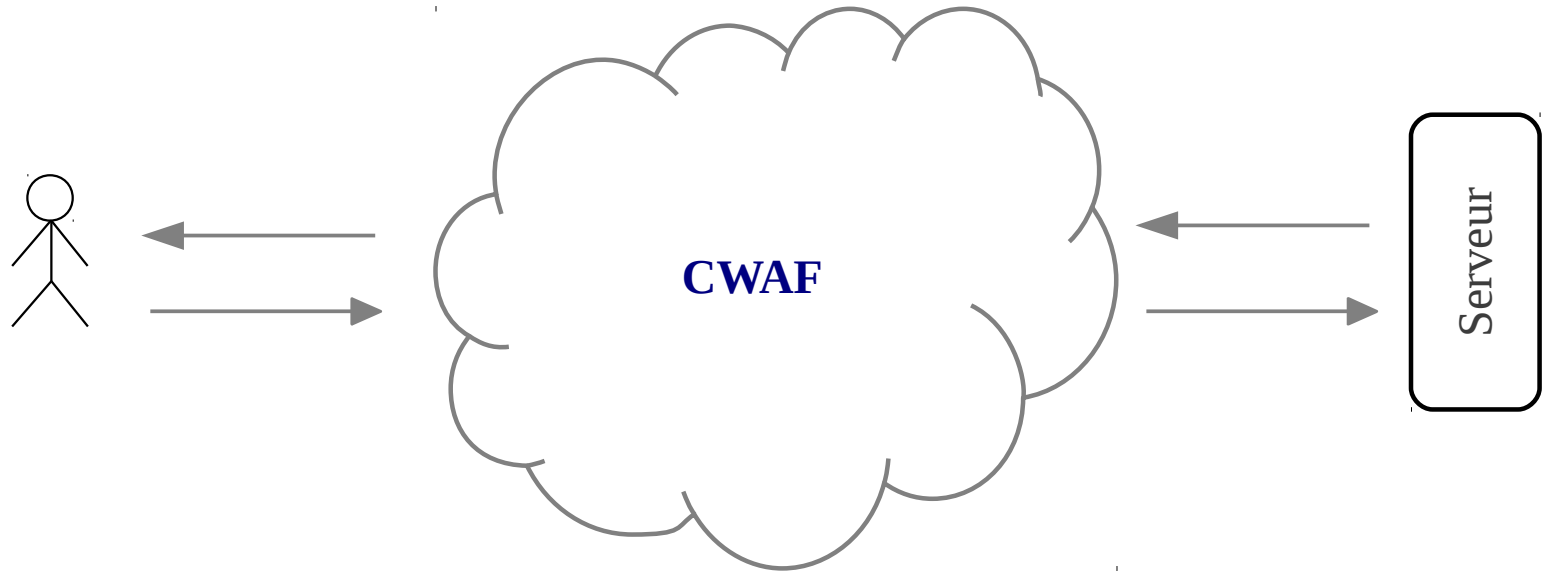


Architecture

- Caractéristiques doivent être présentes

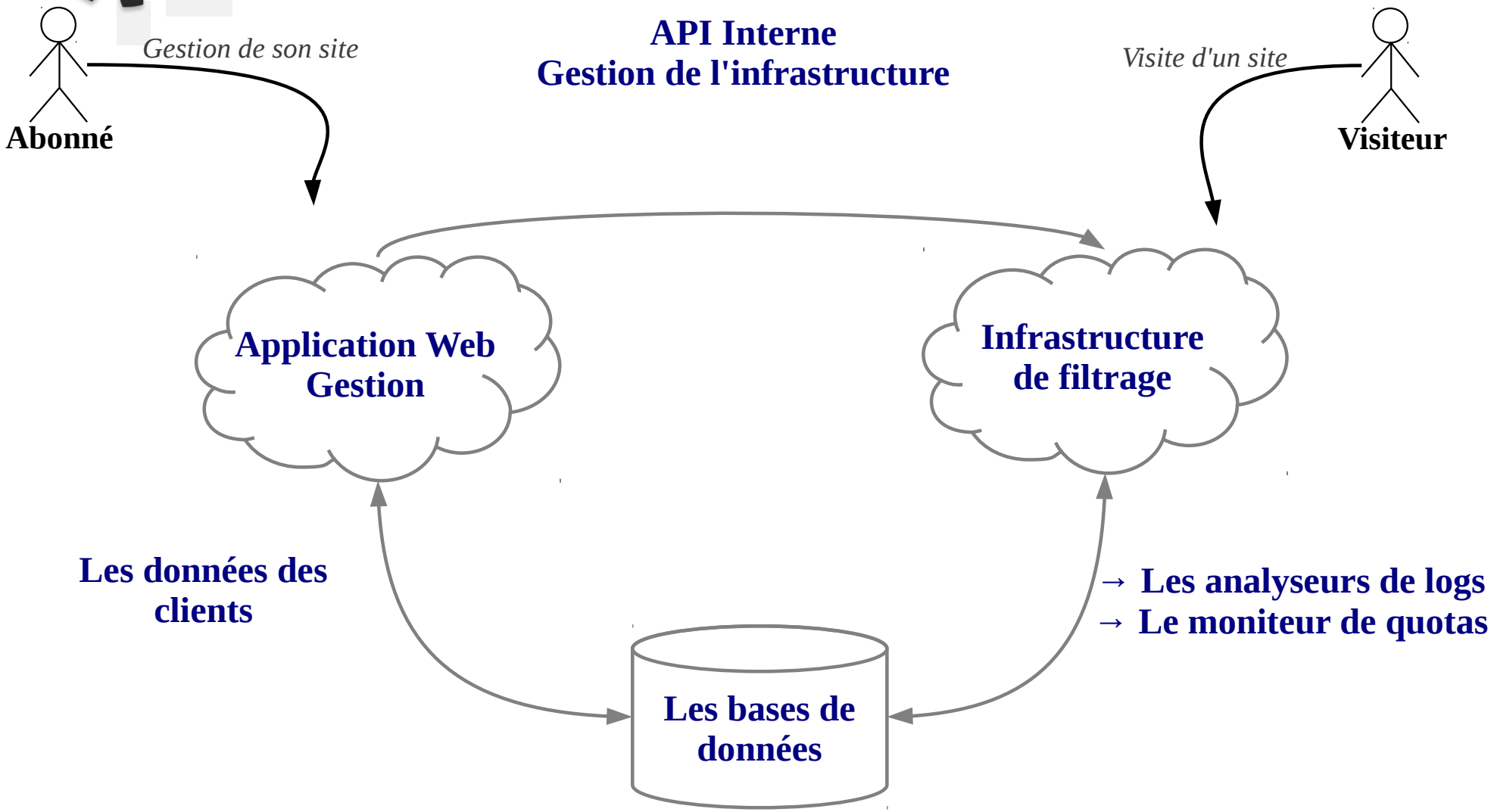
  - ➔ Infrastructure hautement disponible.
  - ➔ Infrastructure évolutive horizontalement.
  - ➔ Plateforme à multi-locataires.

Généralités

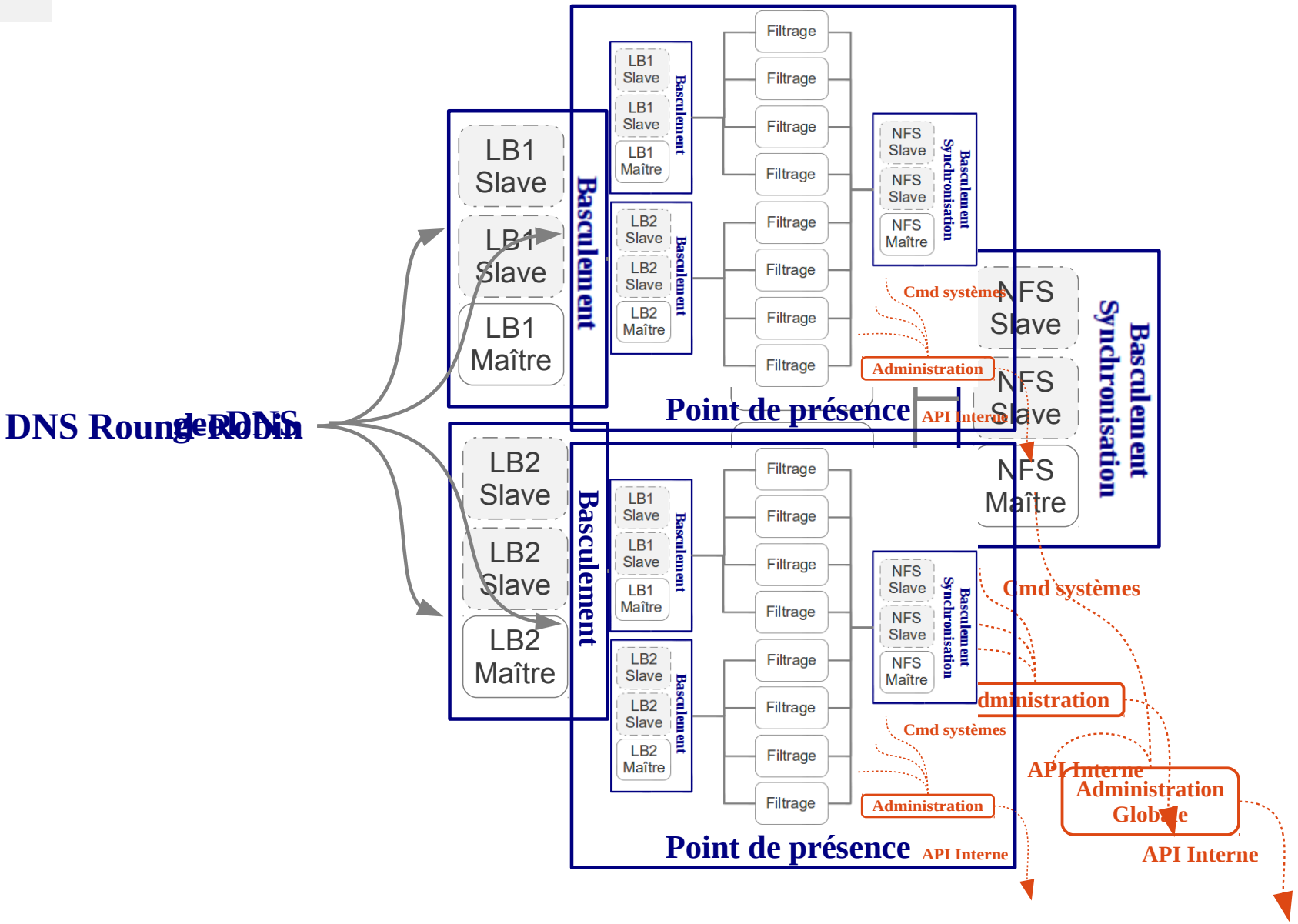


- **Infrastructure de filtrage.**
- **Application web de gestion.**
- **Bases de données communes.**

Architecture – Composition



Infrastructure de filtrage





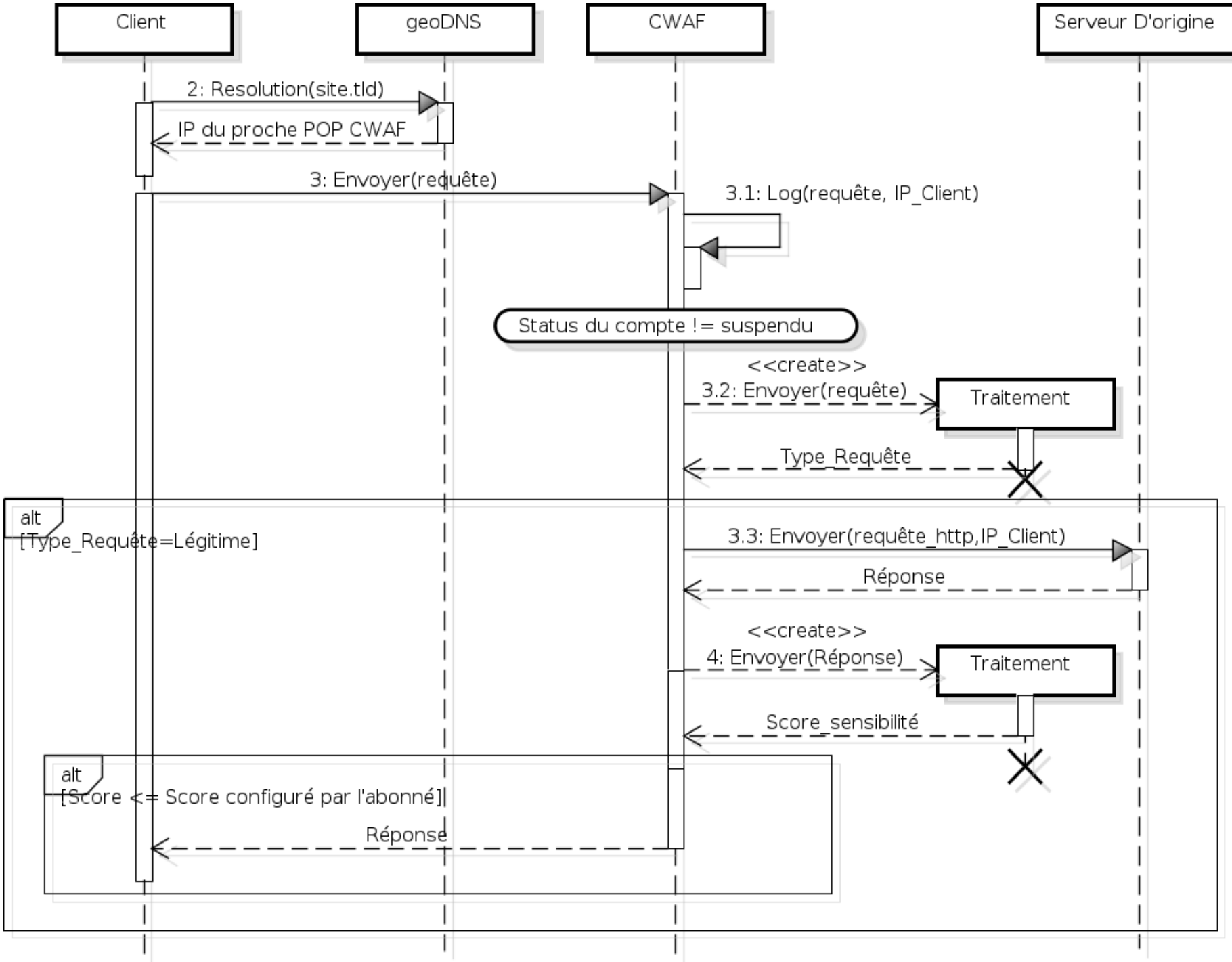
Quelques défis de l'architecture

- ✔ Synchronisation pseudo temps réels entre maître-esclaves.
  - ➔ Modèle « Event-Driven »
  - ➔ Basé sur « Inotify »
- ✔ Basculement entre maître-esclaves en cas de pannes.
  - ➔ Basé sur les adresses IP virtuelle
- ✔ Distribution de la couche virtuelle sur la couche physique
  - ➔ Garder un maximum de redondance réelle.

Mitigation d'attaques

Stratégies de défense

Le Fonctionnement



Contre-mesures

- ✔ Une protection contre les attaques connues, exemple :
  - ➔ Les injections
  - ➔ Les failles XSS (Cross-Site Scripting)
  - ➔ Cross-Site Request Forgery (CSRF)
  - ➔ Les techniques d'évasion et d'obfuscation
- ✔ Un suivi des fuites de données sensibles
- ✔ Une transmission chiffrée SSL et certificat électronique.

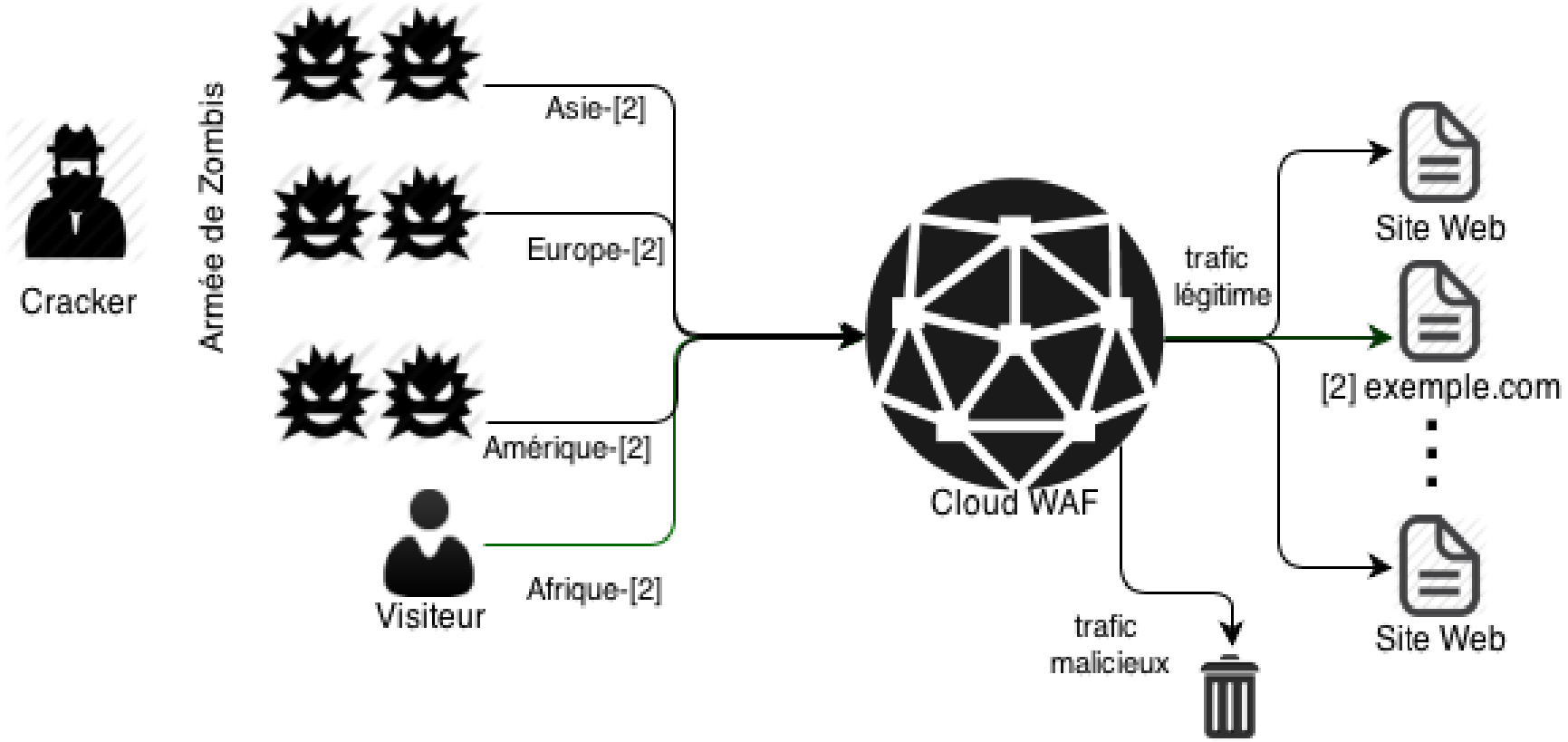




Contre-mesures

- L'authentification ;
- Protection de la politique HTTP ;
- Détection des malwares Web, bots, scanners et autres activités malicieuse ;
- Protection contre les chevaux de Troie par détection des accès ;
- Le WAF alertera l'utilisateur des problèmes de configuration signalés et améliorera l'opacité des applications ;
- Protection contre les attaques de masse (HTTP flooding, ralentissement des attaques HTTP DoS) ;

Mitigation géodistribuée



Suivi et maintenance de la sécurité

Journalisation avancée

Offrir une meilleure expérience à l'utilisateur le mettra plus à jour avec les besoins de son application (par exemple : pour prévoir des corrections).

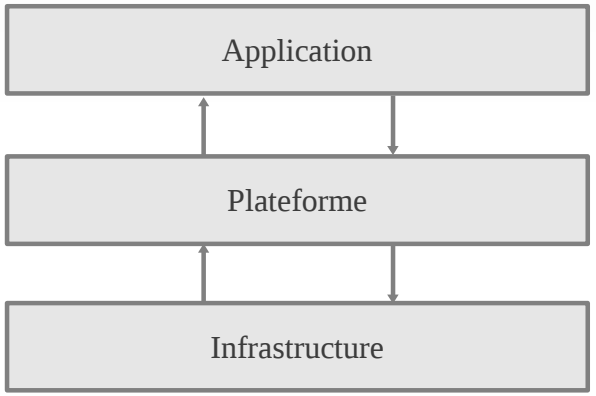
Les audits semi-automatiques

Une solution qui nous garantira un suivi de sécurité continuel.

Honeypot

Se prémunir contre de nouvelles attaques.

Mise en production



Modularité et performance



Implémentation - Infrastructure

- **Infrastructure - Redondance au niveau machine virtuelles:**
  - **Synchronisation :** Script basé sur « Inotify » et Rsync.
  - **Basculement :** Keepalived (VRRP) + configuration personnalisé pour :
    - Tolérance aux pannes au niveau application.
    - L'esclave qui prends la main ne la lâche qu'après son échoue.



Implémentation - Plateforme

- **Plateforme :**
  - **Répartiteurs de charge :** Nginx – WRR + Retrait automatique des nœuds échoués
  - **Filtrage :** Nginx + ModSecurity, Analyseur de logs (NCSA CLF) → BDD
  - **Partage :** Implémentation NFS sous GNU/Linux
  - **DNS :** BIND + Patch geoDNS
  - **Bases de données :** MySQL
  - **Administration :** API Interne de gestion de l'infrastructure
  - **Application Web de gestion :** PHP (Yii Framework) ↔ API Interne

Exemple

http://vm-administration.vaccum.ghaim.net/api/api.php?
cmd=add&arg=eyJzaXRlIjoidW5pdi1ibGlkYS5kei1sICJhbGlhc2VzIjoid3d3LnVuaXYtYmxpZGEuZHoiLCAiYmFja2VuZElQIjoiMTkzLjE5NC44My4xNjMiLCAic3VzcGVuZGVkIjoibm8iLCAiaW5jU3RkTW9kU2VjIjoieWVzIn0K

{"site":"univ-blida.dz","aliases":"www.univ-blida.dz",
"backendIP":"193.194.83.163", "suspended":"no", "incStdModSec":"yes"}

```
server {
        error_log /var/log/nginx/univ-blida.dz-error_log warn;
        listen 80;
        server_name univ-blida.dz www.univ-blida.dz;
        access_log /home/weblogs/univ-blida.dz-bytes_log bytes_log;
        access_log /home/weblogs/univ-blida.dz combined;
```

```
root@vm1:/home/controle/conf/vhosts# locate univ-blida.dz
/home/controle/conf/vhosts/univ-blida.dz.conf
/home/controle/conf/vhosts/modsec/univ-blida.dz-std.conf
/home/controle/conf/vhosts/modsec/univ-blida.dz.conf
```

```
        location / {
          #TOADDAFTER
          root   html;
          index  index.html index.htm;
          ModSecurityEnabled on;
          ModSecurityConfig vhosts/modsec/univ-blida.dz*.conf;
          ModSecurityPass @backend;
        }

        location @backend {
              proxy_pass http://193.194.83.163:80;
              include proxy.inc;
        }

        location @backend_static {
              proxy_pass http://193.194.83.163:80;
              include proxy.inc;
              proxy_cache static;
```



Validation

[1] Test de pénétration

- Toutes les attaques menées par des outils de scan automatiques ont été détectées et prévenues.
- Parmi eux des failles de type SQL Injection qui nous donnaient la possibilité d'exposer l'intégralité de la BDD.

[2] Test de performance

- Gain: de -5% à +200 %
- Dépend de la nature du site web et de l'emplacement géographique du serveur d'origine et du client.



Conclusion

Conclusion et perspectives



Avantages du CWAF

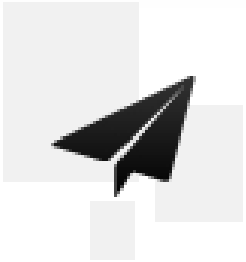
- Résoudre le maximum de problèmes d'attaques en masse (Flood, DoS, DdoS) avec la centralisation des ressources.
- Simplicité de déploiement du côté webmaster (DNS, ex. : pour se soumettre à la PCI Compliance).
- Configuration simple grâce à une plate-forme IHM ergonomique (journalisation, rapports...).
- Gestion centrale :
  - Application rapide des patchs de sécurité ;
  - Partage d'informations entre les sites sécurisés (une meilleure prévisibilité) ;
- Un « Business Model » pour les WAF.



Conclusion

Le but de cette étude était de présenter les aspects de cette technologie, mais également de développer et de proposer une solution open source et d'innover en matière d'architecture et de stratégies de défense pour assurer une haute disponibilité et de hautes performances dans la sécurité, la livraison et la mitigation des attaques DDoS.

Comme toutes les solutions, les pare-feux applicatifs web évoluent dans le même rythme que celui des besoins. Du fait que le courant de la sécurité est dirigé et dressé par celui de la malfaisance.



Perspectives

- Un apprentissage collectif et supervisé de l'environnement.
- Configurations spécifiques à certaines technologies et à certains produits.
- Générer des configurations personnalisées sur la base d'audits automatiques.
- Une API de framework-like.
- Un système de cache avancé pour un CDN plus performant.
- « Next Generation Firewall »

Fin

« there are only two types of companies: those that have been hacked and those that will be. »

Robert S. Mueller directeur du FBI