DDOS APPLICATIFS & WAAC

Retour d’expérience et WAAP as a Container · RESinfo 2026

UBIKA

SOMMAIRE

RESinfo 2026

01 UBIKA, la sécurité applicative souveraine

02 DDoS applicatifs : retour d'expérience

03 WAAC, le WAAP as a Container



UBIKA

La sécurité applicative souveraine

LEADER EUROPÉEN DE LA SÉCURITÉ APPLICATIVE

Éditeur français, pionnier du WAF en Europe depuis 2001

600

clients
protégés par nos solutions

25 ans

d'expertise
en protection des applications web et API

4

produits
sur une même technologie de protection

Héritière de **Bee Ware, DenyAll et Rohde & Schwarz Cybersecurity**, UBIKA fait partie du groupe TSS depuis 2022. Siège à Meudon.

UBIKA

SOLUTIONS SOUVERAINES, SEUL WAF CERTIFIÉ ANSSI

Une protection applicative conçue et éditée en France

Souveraineté

- Éditeur **français**, solutions conçues et développées en France
- Hors du champ des **lois extraterritoriales** américaines
- Conforme au **RGPD**, labellisé **France Cybersecurity**

Certification ANSSI

- UBIKA WAAP Gateway **certifié CSPN** par l'ANSSI
- Le **seul WAF** à détenir cette certification
- Un atout pour le **secteur public** et les **marchés régulés**

Source : ANSSI, certificat ANSSI-CSPN-2023/23 (UBIKA WAAP Gateway 6.11.1)

UNE SEULE TECHNOLOGIE, PLUSIEURS FORMATS



UBIKA WAAP GATEWAY
Self-hosted, dans votre datacenter

UBIKA WAAP GATEWAY
Chez votre cloud provider
AWS · Azure · Google Cloud · OpenStack · Outscale · OVHcloud

UBIKA CLOUD PROTECTOR
En SaaS, opéré par UBIKA

WAAC
Dans vos clusters Kubernetes

Facilité d'administration · mêmes moteurs, même politique, quel que soit le format

DDOS APPLICATIFS

Retour d’expérience



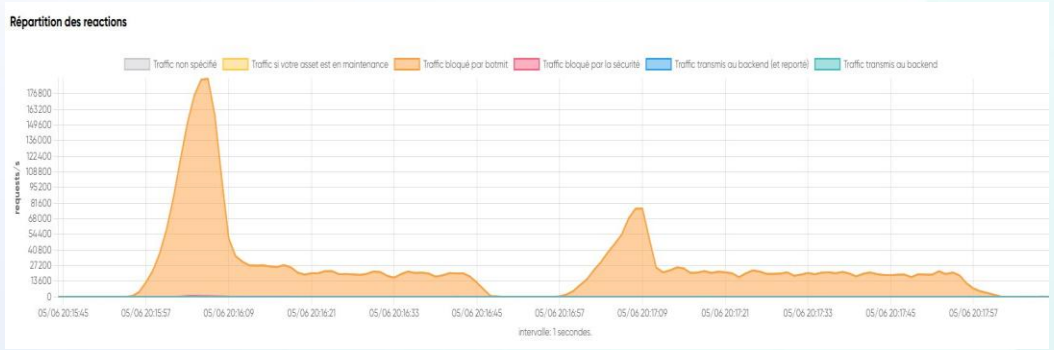
HTTP FLOOD, RETEX SUR CLOUD PROTECTOR

- Attaque de plus en plus fréquente : plusieurs fois par mois sur Cloud Protector. Plus fréquent que le DDoS réseau L3/L4 « classique ».

Attaque record sur notre plateforme :

- Près de 2,5 millions de requêtes seconde Anti-DDoS L3/L4 inefficient : trafic légitime d'un point de vue DDoS réseau, volumétrie par IP trop faible. Durée de l'attaque : du 5/06 au 10/06
- Blocage du trafic via la Bot Mitigation
- Scalabilité observée : le cluster est passé de 4 pods de filtrage à 120 pods (x30 - limite non atteinte)

=> Aucun impact opérationnel sur le trafic légitime !



ZOOM SUR NONAME057(16)

- Certaines attaques sont revendiquées : par ex. les activistes Russes NoName057(16) sur X.
- Volonté de déstabilisation d'institutions moyennes européennes et communication forte sur les dommages occasionnés.
- Utilisation d'un botnet géré comme un produit (DDoSia), qui fournit une interface de commande via un canal Telegram : DDoS as a Service.
- Les bots reçoivent des listes de cibles, et lancent des pot pourris d'attaques
- Quelques arrestations ont eu lieu en Europe en 2025, mais le groupe reste actif.



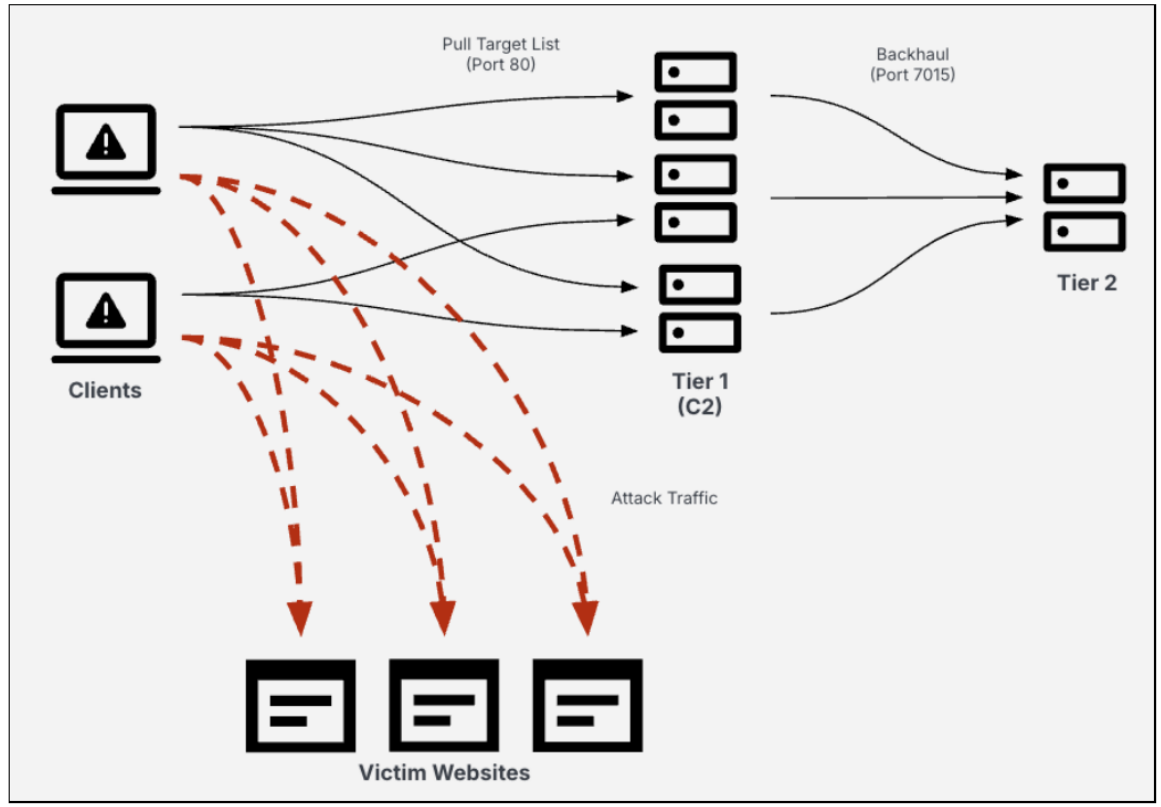
RETEX : ANALYSE D'UN BOTNET

Mise en place d'une task-force avec les équipes techniques OVH, entre 2 et 3h par jour pendant 1 mois:

- Reverse-engineering et falsification du serveur de contrôle « C2 », re-routage du trafic des bots.
- Déploiement d'un botnet NoName dans l'infrastructure OVH pour rejouer les attaques avec l'aide du CERT OVH.
- Implication de l'interCERT.

➔ Analyse du trafic et amélioration de la résilience du service de bout en bout.

➔ Détection et fix d'un bug Kernel chez OVH, ce qui a rendu les attaques NONAME complètement inopérantes pour nos clients.



AMÉLIORATIONS RÉALISÉES SUITE AUX ATTAQUES

Suite à incident fin 2024:

- Tuning des configurations pour améliorer la résilience aux différents types d'attaques lentes.
- Amélioration des performances des moteurs de sécurité pour protéger contre les attaques L7 très distribuées

Les moteurs traditionnels (IP Rep, IP Geoloc, Request Limiter, Black-List d'IP…) sont d'une efficacité limitée face à une attaque très distribuée => mise en place d'un nouveau moteur de « bot mitigation » qui permet de bloquer efficacement les botnets d'attaques tout en consommant très peu de ressources WAF.

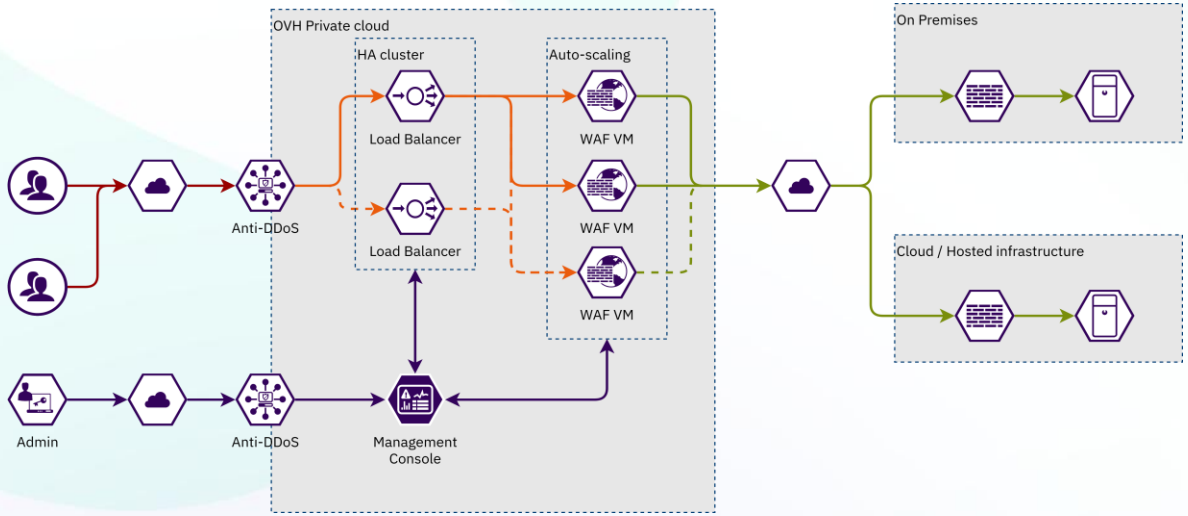
Nouvelle architecture « NG » en micro-services (kubernetes). Bénéfices versus notre infrastructure historique :

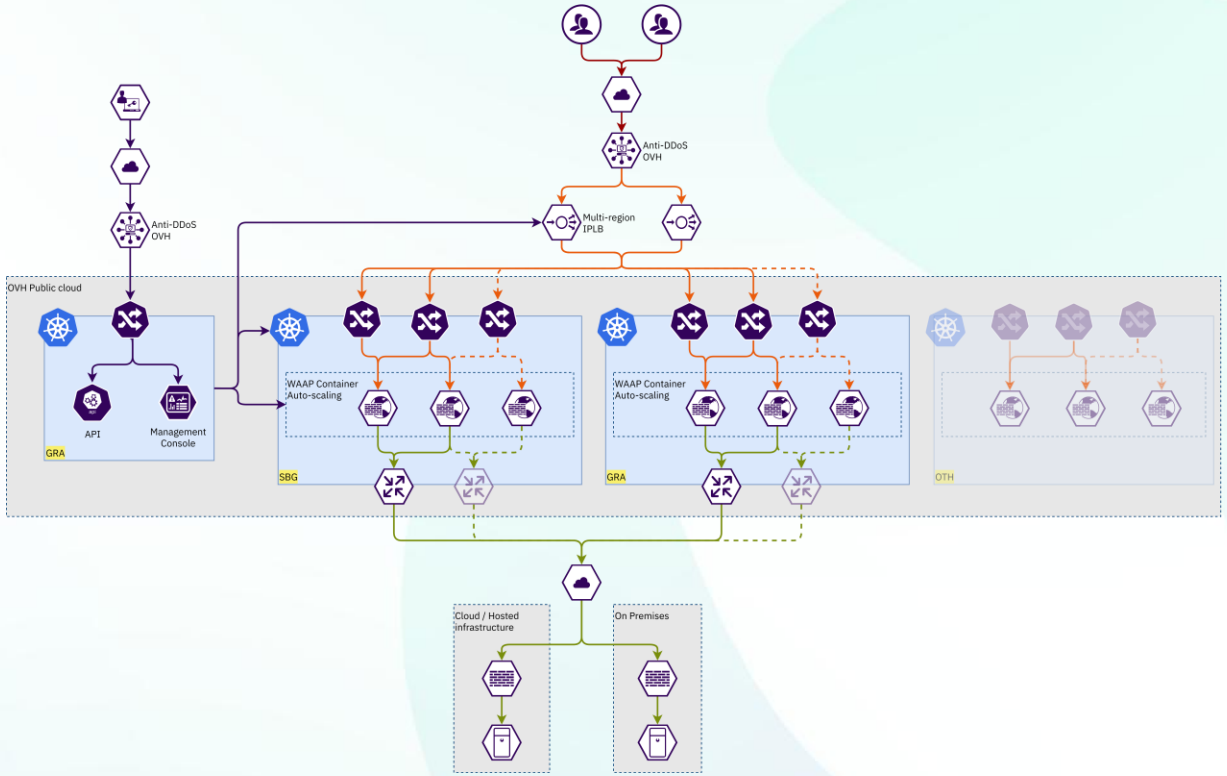
	Cloud Protector NG	Cloud Protector Legacy
Temps pour scaler une instance	30s	15 minutes
Overhead	Négligeable (container reverse-proxy)	1 VM complète (ressources système, OS, services OS)
Limitation scaling	Infini (limité par la totalité des ressources du cluster)	Limites système by design (load-balancer non-scalable)

En roadmap : Black-List dynamique en masse d'IPs en périphérie de l'Infrastructure (sur les scrubbing center OVH)

UBIKA

UNE ARCHITECTURE ÉLASTIQUE



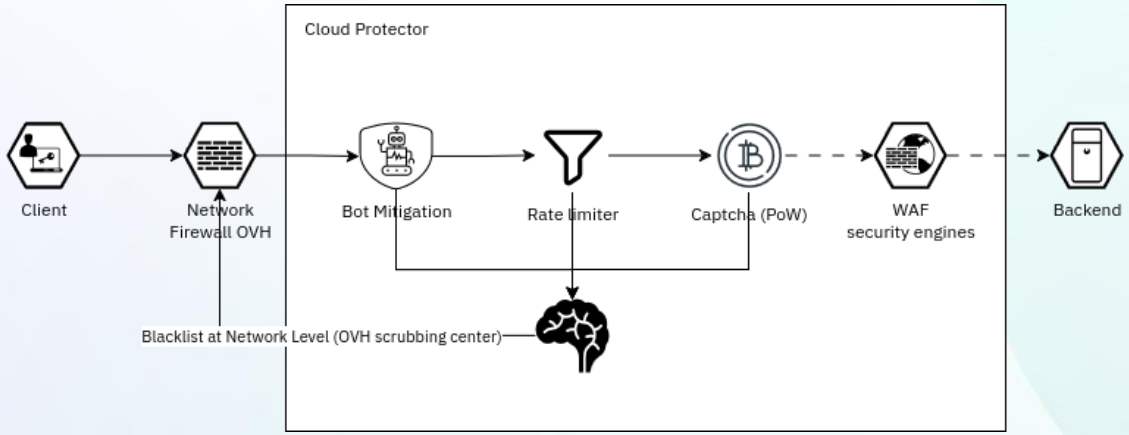


ANTIBOT AVANCÉ

Un premier mécanisme de blocage le plus léger possible pour plus d'efficacité

► Réponse HTTP en première barrière la plus petite possible : lors des attaques, le débit mesuré dépasse les 2 Gbps
► Les botnets rencontrés à l'heure actuelle ne sont pas capables de résoudre le challenge de Bot Mitigation. Étant prévu pour être exécutés sur une multitude de devices vulnérables (IOT, routeurs, …), ils n'embarquent pas de vrai navigateur.

► Contre les botnets « intelligents » émergents (jamais rencontrés en production à ce jour), plusieurs réponses sont complémentaires sont mises en place :
- Blacklist automatique des IP attaquantes au niveau firewall périmétrique (Scrubbing center OVH)
- Présentation en deuxième barrière d'un captcha de type « Proof of Work ». L'attaquant est bloqué face au coût CPU nécessaire pour résoudre le challenge (challenge type blockchain).





WAAC

Le WAAP as a Container

UBIKA

UNE SEULE TECHNOLOGIE, PLUSIEURS FORMATS



UBIKA WAAP GATEWAY
Self-hosted, dans votre datacenter

UBIKA CLOUD PROTECTOR
En SaaS, opéré par UBIKA

UBIKA WAAP GATEWAY
Chez votre cloud provider
AWS · Azure · Google Cloud · OpenStack · Outscale · OVHcloud

WAAC
Dans vos clusters Kubernetes

Facilité d'administration · mêmes moteurs, même politique, quel que soit le format

POURQUOI LE WAAP AS A CONTAINER ?

01 · CONTINUITÉ DE SERVICE

Disponible et élastique

- Recrudescence des attaques DDoS
- Coût des composants en hausse : il faut de l'élasticité
- Adoption massive de Kubernetes comme orchestrateur

02 · DEVSECOPS

Gouvernée comme du code

- Limiter les erreurs humaines
- Versioning, visibilité, revue, gouvernance de la politique
- « No drift » : la production reste l'état déclaré

LA RÉPONSE UBIKA

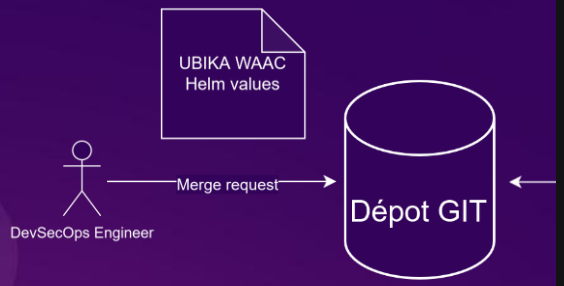
WAAP as a Container

Intégration totale
à Kubernetes et à ses design patterns

Security-as-code
par conception, pour un flux GitOps

En production
chez France Identité depuis juillet 2026, certification ANSSI en cours

DU COMMIT AU POD, AVEC WAAC



assets-1-values-harbor.yaml

```yaml
assets:
  - name: my-asset-1
    hostnames:
      - app1.cp-demo.denyall.com
      - my-asset-1.test
      - my-asset-1.other.test
    backend:
      certificateCheck: DISABLED # FULL

      stickiness: true
      members:
        - url: https://a.cp-demo.denyall.com/member1/
        - url: https://a.cp-demo.denyall.com/member2/

    apiModule:
      paths:
        - path: /v1
          openapi: "my-api-v1"
        - path: /v2
          openapi: "my-api-v2"

    applicationModule:
      securityMode: BLOCK

    advanced:
      logHeaders:
        - my-header-1
        - toto
        - my-hdr

    deploymentConfigurations:
      resources:
        requests:
          cpu: 1m
          memory: 11Mi
        limits:
          cpu: 123m
          memory: 123Mi
      imagePullSecrets:
```

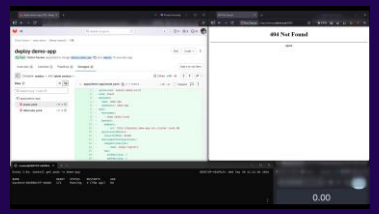


- La politique de sécurité est versionnée, lisible, protégée pa
- Tout changement de la politique peut être soumis à review
- Respect des design patterns de Kubernetes = meilleure sca observabilité
- En cas de panique : un revert de commit remet dans l'état

LA DÉMO, EN TROIS VIDÉOS

01

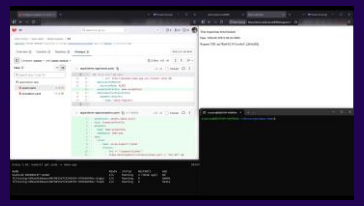
Déploiement de la protection



Réactivité · Simplicité · Preuves

02

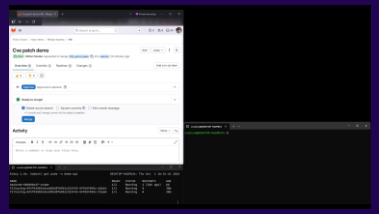
Le faux positif



Supervision · Résilience · MCO/MCS

03

Le patch de la CVE



Réactivité · Adaptabilité

VOS ENJEUX, DÉMONTRÉS

VOTRE ENJEU	LA PREUVE DANS LA DÉMO	
01 Industrialiser la sécurité comme les services	Une application protégée en une douzaine de lignes de YAML, livrées par Git comme le code	Vidéo 1
02 Faire du MCS une boucle continue	Le faux positif lu dans le journal, corrigé par une exception versionnée et relue	Vidéo 2
03 Monter en puissance sans sacrifier la stabilité	La politique change, les pods se renouvellent, le trafic ne s'interrompt pas	Vidéo 2
04 Réduire le temps entre menace et protection	De la CVE au blocage en une minute environ, sans toucher à l'application	Vidéo 3
05 Démontrer la maîtrise sécuritaire en continu	La configuration invalide rejetée avant la production, la merge request fait foi	Vidéo 3

CONTACTS

Vos interlocuteurs UBIKA

Antoine Jacquart

Ingénieur avant-vente

antoine.jacquart@ubikasec.com
06 07 64 93 16

Hélène Selosse

Responsable Commerciale Secteur public

helene.selosse@ubikasec.com
+33 6 65 12 96 07

UBIKA · 9 - 11 rue Jeanne Braconnier, 92360 Meudon, France
www.ubikasec.com

MERCI

www.ubikasec.com | info@ubikasec.com

UBIKA