THALES
Building a future we can all trust

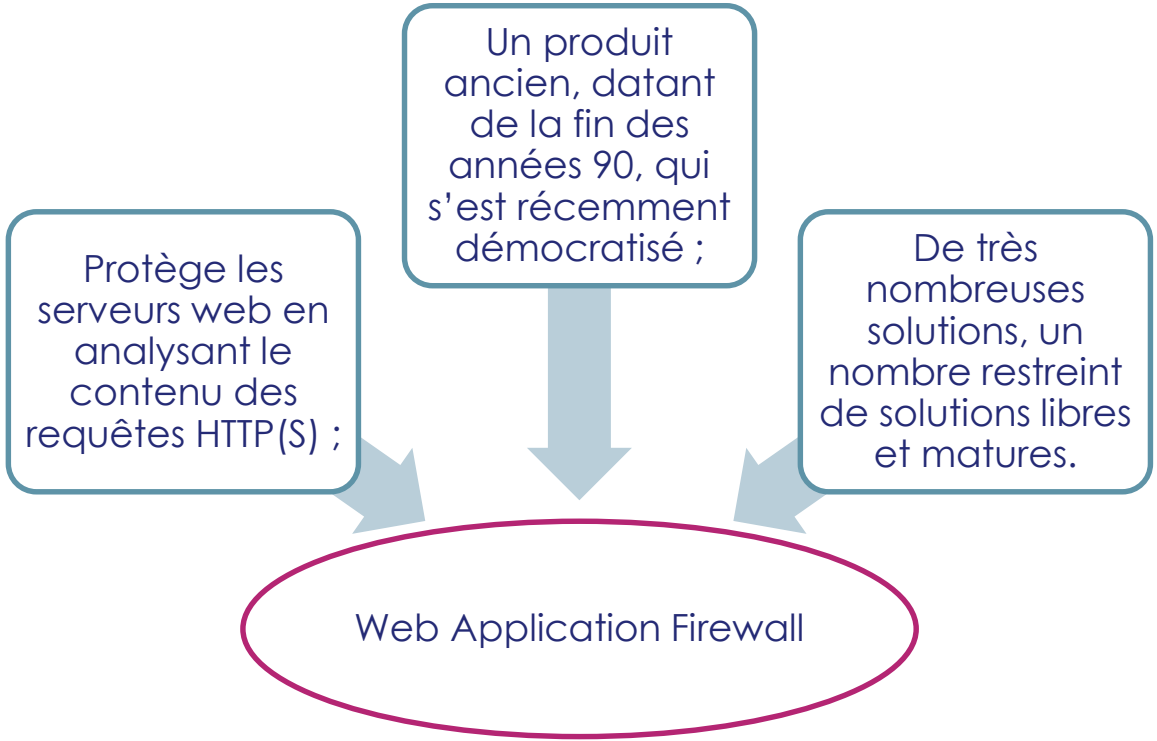
Web Application Firewall
Enjeux, fonctionnement et étude

Séminaire sur la confiance numérique
Télécom SudParis – Sécurité des Systèmes et des Réseaux
Thales SIX – Service Intégration & Validation de Sécurité
CHOU Constance – 11/10/2022

TELECOM SudParis

IP PARIS

Introduction | Pare-feu applicatif



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Sommaire

Le WAF et ses enjeux

- Problématique
- Fonctionnement
- Protection et fonctionnalités
- Ecosystème des technologies

Types de solution et critères d'évaluation

Implémentation, intérêts et limitations

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Problématique et besoin

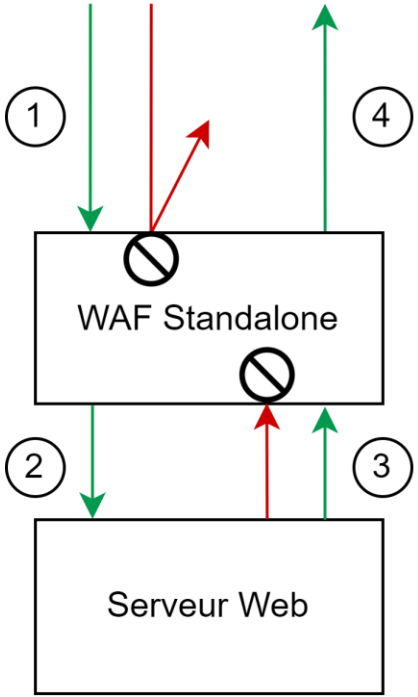
Constatation : il est parfois extrêmement difficile de sécuriser l'application web elle-même, ou d'appliquer des correctifs dans des délais convenables.

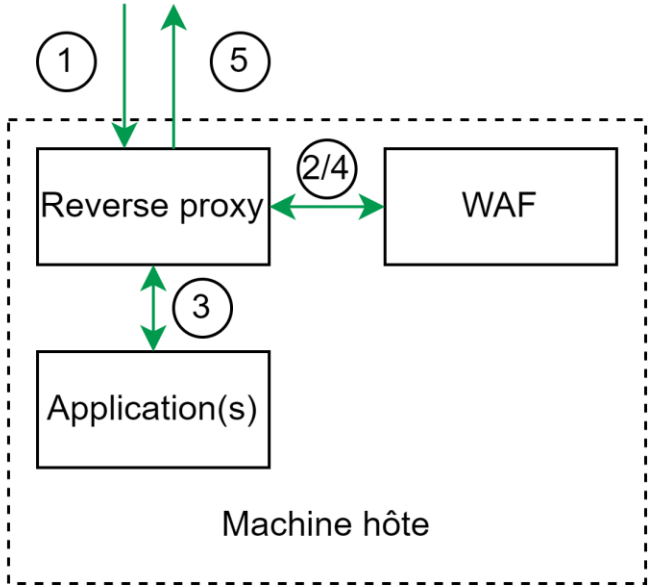
- Applications non modifiables fournies par des acteurs externes,
- Applications historiques à refondre entièrement,
- Applications critiques à long préavis de maintenance,
- Etc.

⇒ *Virtual patching*

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Fonctionnement d'un WAF





Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Protection offerte et autres fonctionnalités

Identification de motifs suspects

- Analyse des flux entrants :
  - Injections SQL,
  - Exploitations de *Cross Site Scripting* (XSS),
  - *Cross-Site Request Forgery* (CSRF),
  - *Local/Remote File Inclusion* (LFI/RFI),
  - Etc.
- Analyse des flux sortants : blocage des fuites de données

Apprentissage du trafic légitime, analyse comportementale

Filtrage des adresses IP, protection contre le DoS, le *brute force* d'identifiants, etc.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Ecosystème des technologies

Filtrage réseau :
ex. **Intrusion Detection/Prevention System**

Analyse applicative en amont de l'application web :
Web Application Firewall

Analyse applicative au sein de l'application web :
Runtime Application Self-Protection

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Sommaire

Le WAF et ses enjeux

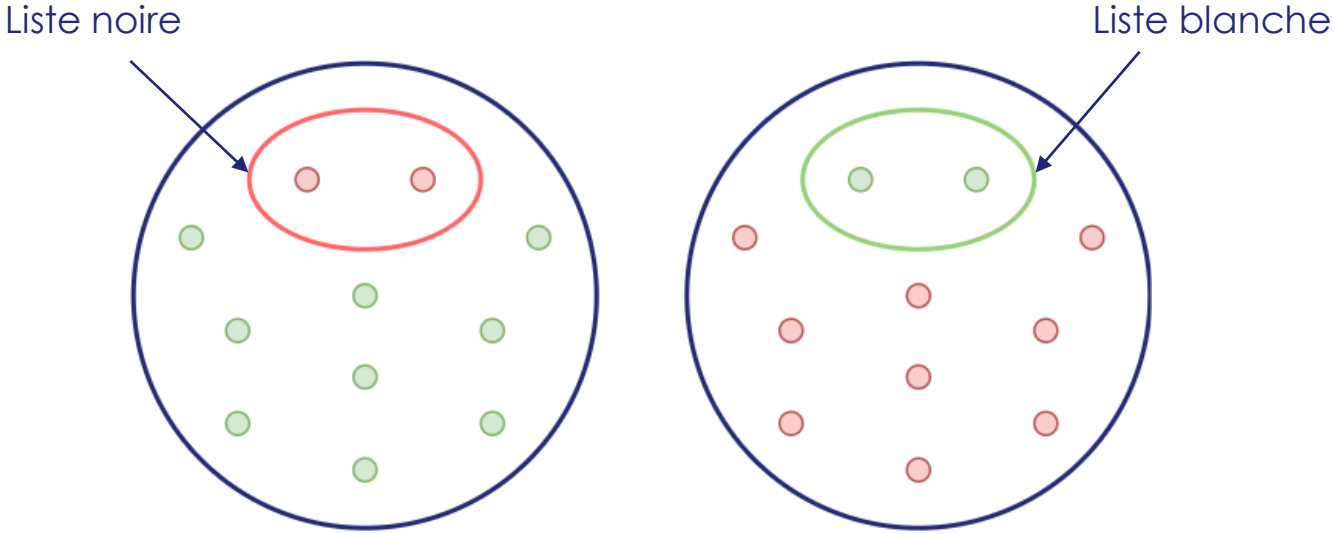
Types de solution et critères d'évaluation

- Modèles de sécurité
- Fonctionnement classique et configuration
- Critères d'évaluation
- Méthodologie d'évaluation

Implémentation, intérêts et limitations

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Modèles de sécurité et types de WAF associés



Modèle de sécurité négatif

Modèle de sécurité positif

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Exemples de signatures pour différents types de WAF

Protection contre la vulnérabilité Cross-Site Scripting : motif <script>

```
SecRule REQUEST_COOKIES | !REQUEST_COOKIES:/__utm/ | REQUEST_COOKIES_NAMES | REQUEST_FILENAME |
REQUEST_HEADERS:User-Agent | REQUEST_HEADERS:Referer | ARGS_NAMES | ARGS | XML:/* "@rx (?i)<script[^>]*>[\s\S]*?" \
    "id:941110,\
    phase:2,\
    block,\
    capture,\
    t:none,t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls,\
    msg:'XSS Filter - Category 1: Script Tag Vector',\
    logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\
    tag: [...]
    tag:'paranoia-level/1',\
    ctl:auditLogParts=+E,\
    ver:'OWASP_CRS/3.4.0-dev',\
    severity:'CRITICAL',\
    setvar:'tx.xss_score=+%{tx.critical_anomaly_score}',\
    setvar:'tx.anomaly_score_pl1=+%{tx.critical_anomaly_score}"'


MainRule "str:<" "msg:html open tag" "mz:ARGS | URL | BODY | $HEADERS_VAR:Cookie" "s:$XSS:8" id:1302;
```

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Configuration des WAFs

Configuration de seuils d'alerte

OWASP
ModSecurity
Core Rule Set
THE 1ST LINE OF DEFENSE

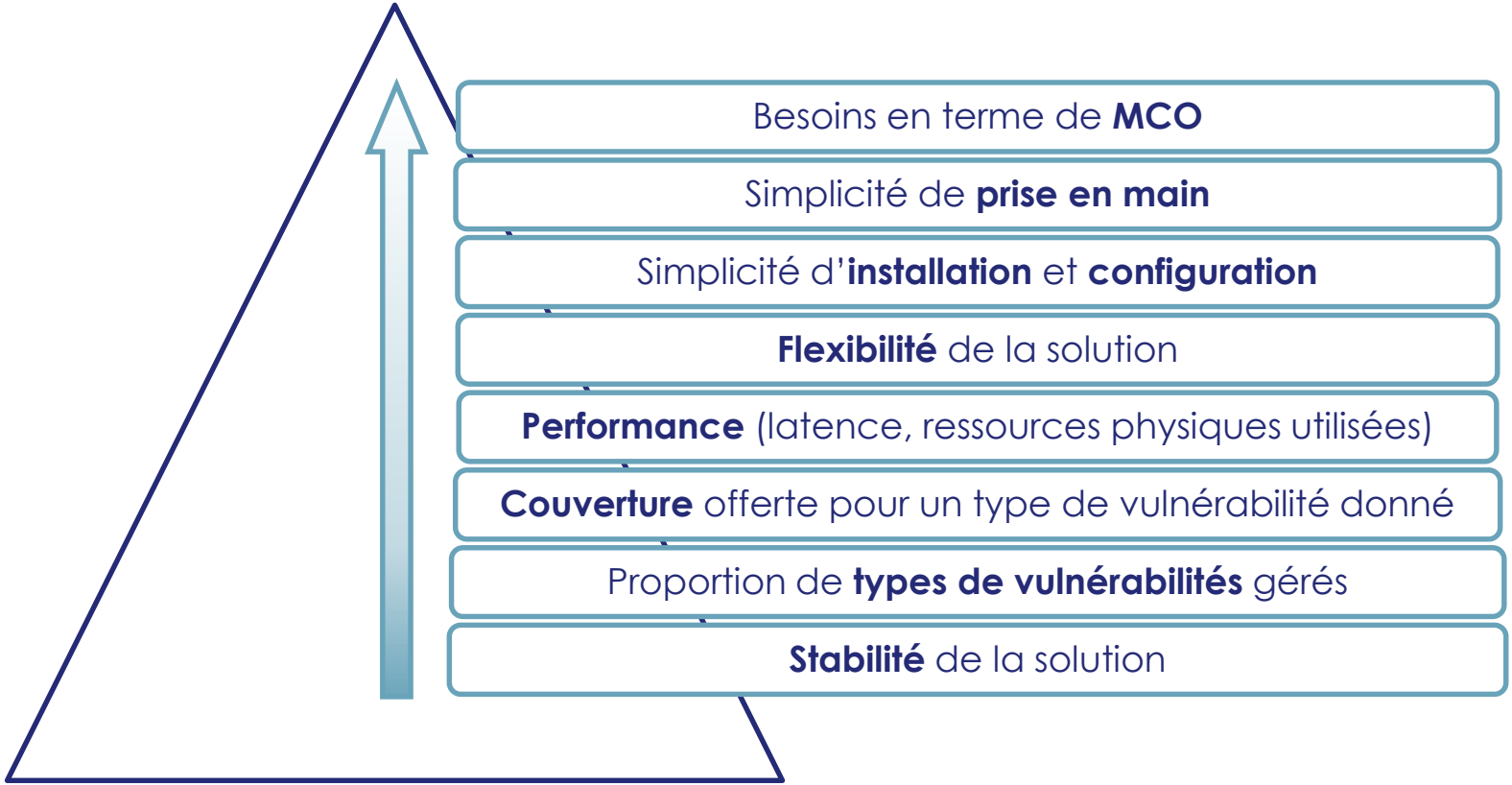
Niveau de paranoïa du CRS

Niveau de paranoïa	1	2	3	4
Nombre de signatures ajoutées	169	51	19	7

Mise en place d'exceptions et de règles personnalisées

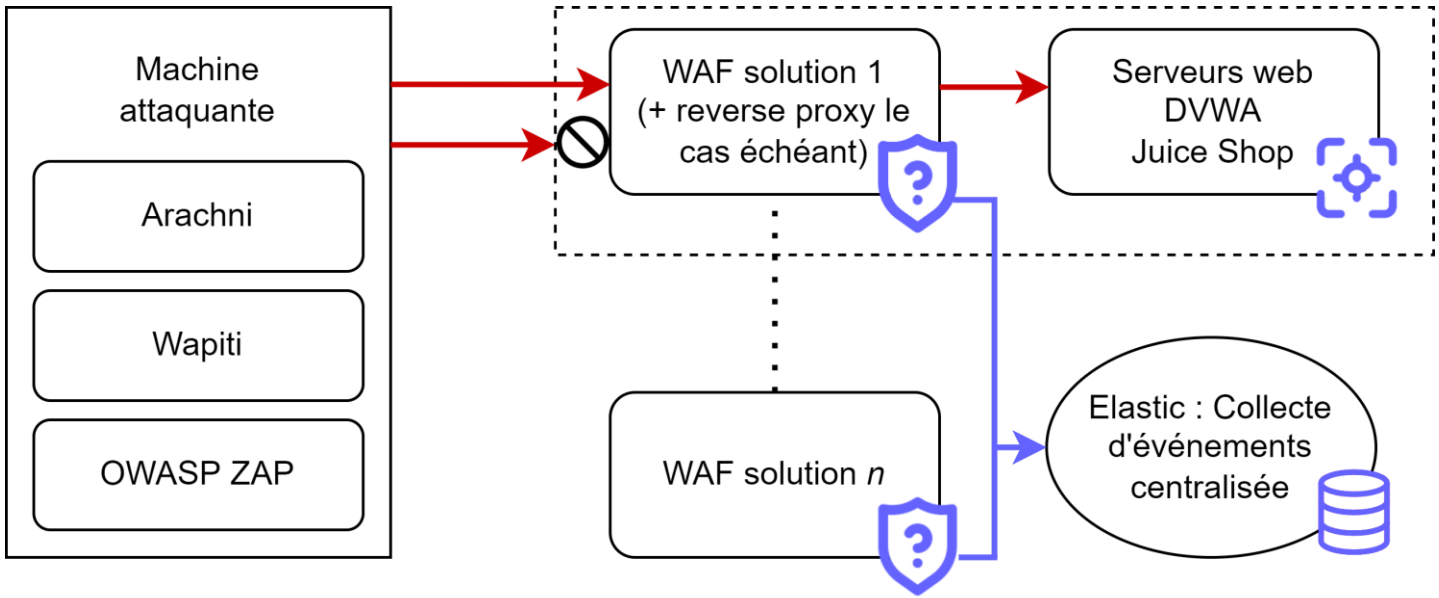
Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Critères génériques d'évaluation d'un WAF



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Proposition de méthodologie d'évaluation d'un WAF



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Sommaire

Le WAF et ses enjeux

Types de solution et critères d'évaluation

Implémentation, intérêts et limitations

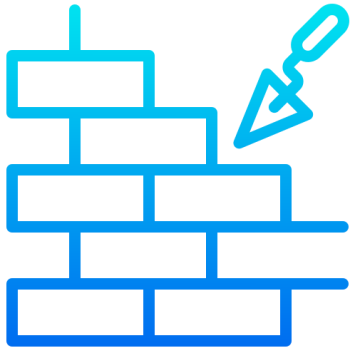
- Considérations de configuration
- Considérations de sécurisation
- Intérêts et limitations

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Implémentation | Configuration du *ruleset*

Méthodologie :

- Générer du trafic représentatif de l'utilisation en production ;
- Gérer les faux positifs en ajoutant des exceptions ;
- Minimiser la perte en sécurité en créant des exceptions suffisamment spécifiques …
- … Mais néanmoins suffisamment générales pour être pérennes.



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Implémentation | Considérations de sécurisation

Redondance matérielle

Durcissement de l'OS

Durcissement de l'exécutable

- PIE (Position-Independent Executable)
- Canaris
- RELRO (RELocation Read Only)
- Pile non exécutable, etc.

Configuration du *reverse proxy*

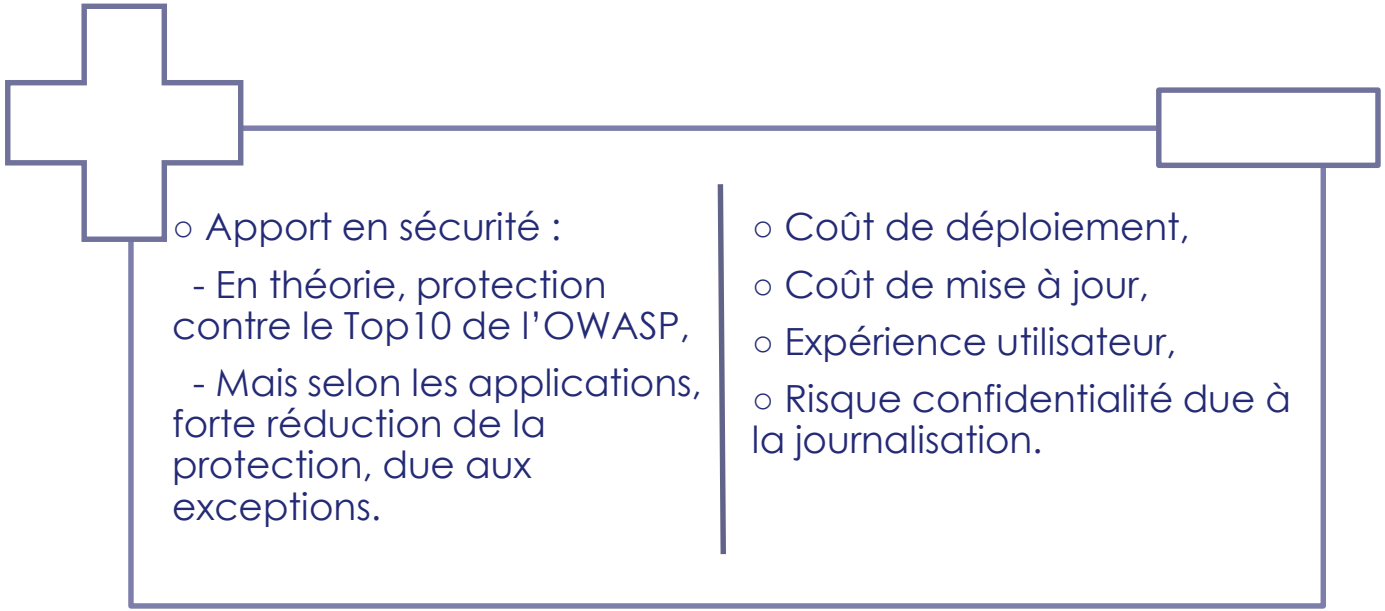
- Application du référentiel CIS (guide NGINX de février 2019)
- Suites cryptographiques conformes au guide ANSSI 2017 relatif à TLS 1.2

Gestion de l'espace de stockage des journaux

Minimisation des permissions de fichiers, etc.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Intérêts et limitations de l'utilisation d'un WAF



- Apport en sécurité :
  - En théorie, protection contre le Top10 de l'OWASP,
  - Mais selon les applications, forte réduction de la protection, due aux exceptions.

- Coût de déploiement,
- Coût de mise à jour,
- Expérience utilisateur,
- Risque confidentialité due à la journalisation.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Conclusion

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.

Sources

- Les logos sont la propriété de leur entreprise, organisation ou projet respectif
- Les icônes sont issus de https://www.flaticon.com/ par smalllikeart, toempong, Ajmal Naha, Eucalyp et srip.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de THALES - © 2021 THALES. Tous Droits réservés.