Rapport d'analyse détaillé

Site: https://env-9206928-wp02-nosecure.hidora.com/

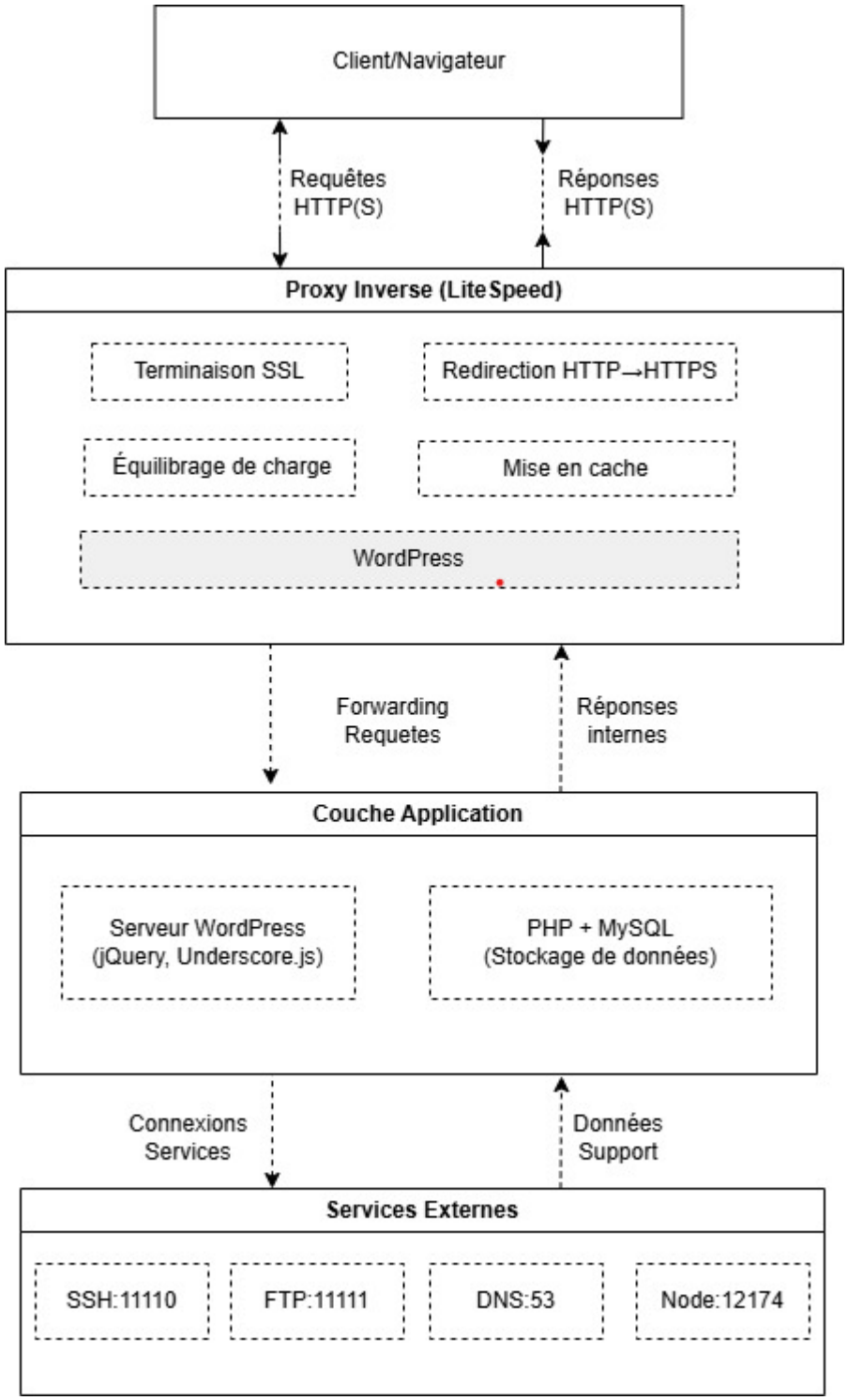
Introduction

Dans le cadre de l'audit du Système d'Information (SI), ce rapport vise à fournir une analyse détaillée de l'architecture technique et des flux d'informations du système, ainsi qu'à identifier les points forts et les points faibles de l'infrastructure. Le Système d'Information en question repose principalement sur des technologies web modernes, notamment WordPress, des mécanismes de sécurité avancés, et des outils d'optimisation des performances. Ce rapport prend en compte des éléments cruciaux comme l'hébergement, les protocoles de sécurité, la gestion des données, et les configurations spécifiques des composants techniques afin de fournir une vue d'ensemble sur l'état actuel du système et des recommandations pour son amélioration.

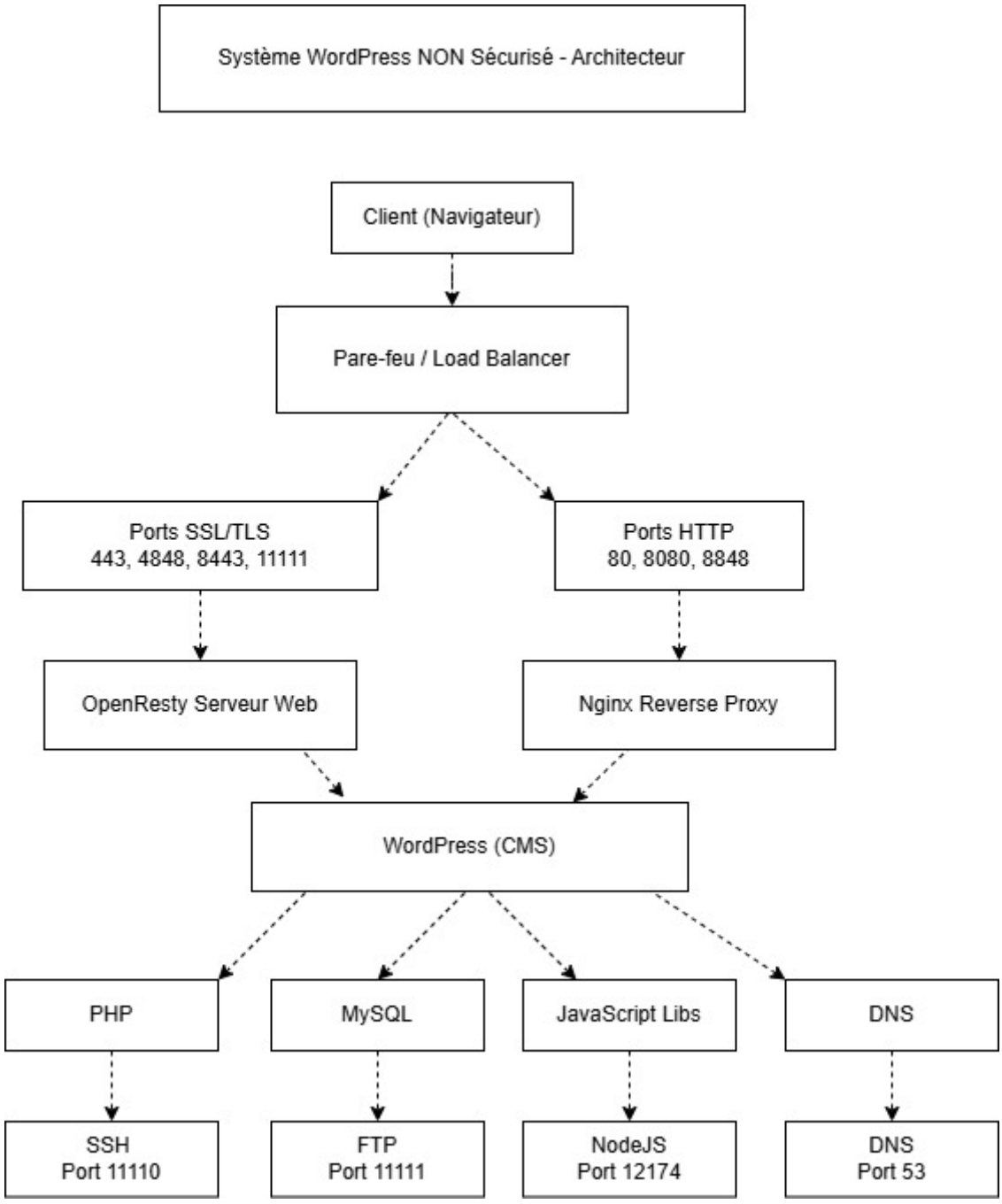
L'objectif principal de cette analyse est de renforcer la sécurité, d'améliorer les performances et d'assurer la conformité aux bonnes pratiques et aux normes de sécurité actuelles. L'approche repose sur l'évaluation de chaque composant majeur du SI, tout en examinant les flux d'informations critiques pour garantir une gestion optimale des données.

Description de l'Architecture du Système d'Information (SI)

Architecture du Système



Flux d'Informations



Résultats de l'Audit de Sécurité

L'audit de sécurité a été effectué sur plusieurs niveaux de l'architecture du système d'information. Voici les points principaux identifiés lors de l'audit:

Points Forts:

- Performance de l'Hébergement et Sécurisation du Serveur:

- LiteSpeed comme serveur web est un choix optimal pour une gestion performante des connexions simultanées et pour les sites utilisant WordPress. Le cache LiteSpeed activé permet d'améliorer les temps de chargement.
- HTTPS et SSL/TLS assurent une communication sécurisée avec les utilisateurs, protégeant les données échangées.

- Le serveur dispose d’un accès SSH sécurisé avec des clés, augmentant la sécurité des connexions distantes.
- L'activation de HTTP/3 améliore la vitesse des connexions, en particulier pour les utilisateurs mobiles ou ayant des connexions instables.

Sécurité Renforcée:

- Le protocole HTTPS et le mécanisme HSTS assurent une communication sécurisée, en forçant l’utilisation de HTTPS et en empêchant les connexions non sécurisées.
- Port FTP fermé : Cette mesure réduit la surface d'attaque en désactivant un protocole potentiellement vulnérable.

Gestion de Contenu avec WordPress:

WordPress est un CMS flexible et performant avec une large communauté, permettant une gestion facile du contenu et une personnalisation via des plugins comme W3 Total Cache et des thèmes comme Twenty Twenty-Four.

L’utilisation de plugins de sécurité comme WPScan permet une gestion proactive des failles de sécurité.

Chiffrement des Données:

Les données échangées sont chiffrées via SSL/TLS, garantissant la sécurité des informations sensibles.

Points Faibles:

Version de WordPress Obsolète (6.6.2):

La version de WordPress utilisée est obsolète, ce qui expose le site à des vulnérabilités connues. Il est impératif de mettre à jour vers la dernière version stable.

XML-RPC Activé:

Le protocole XML-RPC est activé, ce qui expose le site à des attaques par DDoS et force brute. Si cette fonctionnalité n'est pas utilisée, elle doit être désactivée pour limiter les risques.

Plugins et Thèmes Obsolètes:

Le plugin W3 Total Cache (version 2.7.6) et le thème Twenty Twenty-Four (version 1.2) sont obsolètes et présentent des vulnérabilités. Il est essentiel de mettre à jour ces composants pour corriger les failles de sécurité.

Gestion des Cookies Non Avancée:

Bien que la gestion des cookies soit conforme au RGPD, l'absence de personnalisation avancée et d'outils de reciblage publicitaire limite l'interaction des utilisateurs avec le site et pourrait affecter les conversions.

Absence de Sauvegardes de Configuration:

L'absence de sauvegardes régulières de la configuration du site rend la récupération difficile en cas de panne ou d'attaque.

Manque d'Outils de Statistiques Avancées:

L'absence d'outils comme Real User Monitoring (RUM) empêche de suivre l'expérience utilisateur en temps réel et de détecter rapidement des problèmes de performance.

Conclusion

L'architecture du Système d'Information (SI) présente de nombreux points forts, notamment en termes de sécurité et de performance, grâce à des technologies comme LiteSpeed, SSL/TLS, et WordPress. Cependant, certains points faibles existent, principalement autour de la mise à jour des composants critiques (version de WordPress, plugins obsolètes) et de la gestion de certains paramètres de sécurité (XML-RPC activé, gestion des cookies, etc.).

Il est essentiel de mettre à jour régulièrement les composants du site, de désactiver les fonctionnalités inutilisées (comme XML-RPC), et d'implémenter des outils de monitoring avancés pour garantir une performance optimale et une sécurité renforcée.

En résumé, le SI est bien conçu avec des mécanismes de sécurité robustes, mais des améliorations sont nécessaires pour minimiser les risques potentiels et maximiser les performances et l'engagement des utilisateurs.