





Revue de Sécurité

WIZARDS & DICE

 Créateur : Hugo CLAMOND - Responsable technique

 Date de Création : 06/01/2025

 Version : 1.4

 Modificateur : Arthur YANG – Responsable Documentation & Administratif


 Date de modification : 07/03/2025



Table des matières

Table des matières.....	2
Table des figures.....	2
I. Introduction.....	3
II. Ouverture sur l'extérieur.....	3
A) DMZ publique.....	3
Services hébergés :	4
Ports ouverts :	4
Évaluation :	4
Recommandations :	4
B) VPN.....	5
Ports ouverts :	5
Évaluation :	5
Recommandations :	5
III. DMZ privée.....	6
A) Services hébergés.....	6
B) Recommandations :	6
IV. VLAN DATABASE.....	7
A) Services hébergés.....	7
B) Recommandations.....	7
V. VLAN SERVERS.....	8
A) Services hébergés.....	8
B) Recommandations.....	9
VI. Résumé des recommandations.....	9

Table des figures

Nom de la figure	Description de la figure	Page de la figure
Figure 1	Visualisation logique de la DMZ publique à l'heure de l'écriture du document	2/9
Figure 2	Visualisation logique de la DMZ privée à l'heure de l'écriture du document	5/9
Figure 3	Visualisation logique du VLAN DATABASE à l'heure de l'écriture du document	6/9





Figure 4	Visualisation logique du VLAN SERVERS à l'heure de l'écriture du document	7/9
----------	---	-----





I. Introduction

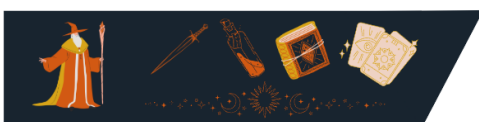
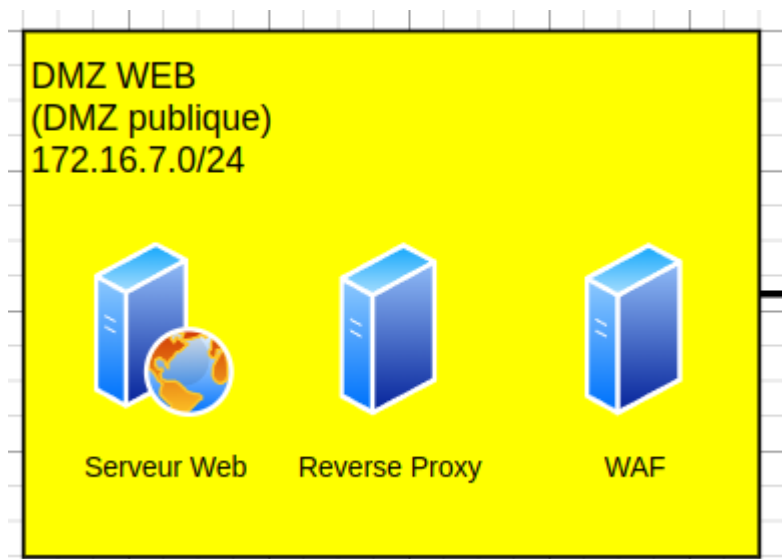
Cette revue vise à évaluer la sécurité des services et ports ouverts sur les différentes zones du réseau, en mettant l'accent sur la segmentation, les flux entrants/sortants, et les bonnes pratiques de protection.

II. Ouverture sur l'extérieur

Cette section vise à lister les surfaces d'attaque et les recommandations à suivre concernant les services ouverts sur l'extérieur.

A) DMZ publique

Figure 1 : Visualisation logique de la DMZ publique à l'heure de l'écriture du document





Services hébergés :

- Web Application Firewall (WAF) : Apache + ModSecurity
- Reverse Proxy : gestion des flux HTTP/HTTPS vers le/les serveurs en backend
- Wordpress : Hébergement du site web public.
- SSH : prise en main depuis le bastion et tunnel entre serveur de test et serveur de backend en DMZ.

Ports ouverts :

- HTTP (TCP 80) : trafic web, à migrer dès que possible vers HTTPS.
- HTTPS (TCP 443) : une fois le certificat émis par une autorité de certification.

Évaluation :

Scan initial depuis la patte WAN de la Freebox : les ports ne sont pas visibles mais un nouveau test sera requis une fois la DMZ Freebox activée et le Stormshield monté en frontal.

Recommandations :

- Activer et sécuriser la DMZ en filtrant très strictement les flux entrants.
- Effectuer des tests réguliers de scan de ports pour identifier les services ouverts de manière non intentionnelle.
- Filtrer le trafic pour éviter tout débordement depuis la DMZ public Stormshield vers le réseau local de la Freebox.
- Séparer les machines de la DMZ publique avec des VLAN pour éviter les débordements et les rebonds.





B) VPN

Ports ouverts :

- VPN SSL (UDP 43537) : créer un objet Port dans le firewall lors de la configuration du VPN SSL.
- VPN SSL Freebox (UDP, site Hugo : XXXXX ; site Loïs : YYYYY)
- VPN IPsec (TCP/UDP 4500 ISAKMP et Protocole 50 ESP) : connexion site-à-site. Ports non maîtrisables.

Évaluation :

Attention à l'ouverture du portail de connexion au VPN SSL Stormshield (<https://<IP>/auth>), et utiliser un mot de passe robuste. Pas de portail de connexion pour le VPN monté sur les Freebox, mais demander à l'administrateur de chacune des Freebox de créer les utilisateurs et d'envoyer les certificats OpenVPN.

Les deux sites doivent pouvoir être joignables sur Internet pour permettre la montée d'IPsec.

Recommandations :

- Ne pas ouvrir le portail de connexion au VPN SSL Stormshield à Internet mais seulement au réseau interne et externe (Network_out).
- VPN SSL Freebox : générer un mot de passe, ne pas mettre un mot de passe habituellement utilisé ailleurs car il doit être envoyé à l'administrateur de chaque Freebox.





III. DMZ privée

Cette section concerne uniquement la DMZ privée, et les quelques services s'y trouvant.

Figure 2 : Visualisation logique de la DMZ privée à l'heure de l'écriture du document

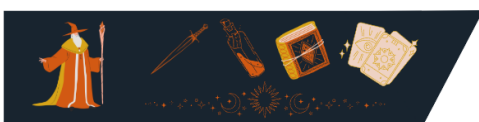


A) Services hébergés

- Bastion par page web : accessible en HTTP, à sécuriser le plus tôt possible avec HTTPS. Utiliser un certificat auto-signé, il n'est pas obligatoire de faire signer ce certificat par une autorité de certification. (inaccessible depuis internet)
- SSH : prise en main du bastion par SSH dans le cas où la page web devient inaccessible.

B) Recommandations :

- Limiter l'accès au bastion au VPN SSL Stormshield.
- Chiffrer HTTP avec TLS dès que possible.
- Utiliser l'authentification par clés pour obtenir un accès SSH au bastion. (Envoyer sa clé publique au responsable technique.)

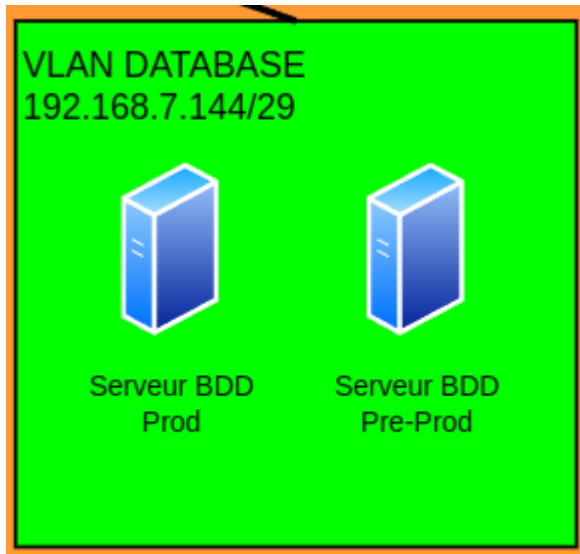




IV. VLAN DATABASE

Cette section concerne uniquement le VLAN DATABASE, et les quelques services s'y trouvant.

Figure 3 : Visualisation logique du VLAN DATABASE à l'heure de l'écriture du document



A) Services hébergés

- Base de données SQL : pour la production et la pré-production.
- SSH : prise en main depuis le bastion.

B) Recommandations

- Restreindre l'accès aux bases de données aux seuls serveurs applicatifs.
- Activer la journalisation des requêtes SQL pour détecter les abus. (possibilité de récupérer via le collecteur de logs)
- Restreindre l'accès du VLAN DATABASE aux autres ressources : ce VLAN communique avec la DMZ publique pour le serveur web public, et avec le VLAN SERVERS pour le serveur web de test.
- Changement de ports d'écoute sur les serveurs pour éviter d'utiliser ceux par défaut.
 - Exemples : le port 29590 pour le serveur BDD de prod et le port 29591 pour celui de pré-prod.

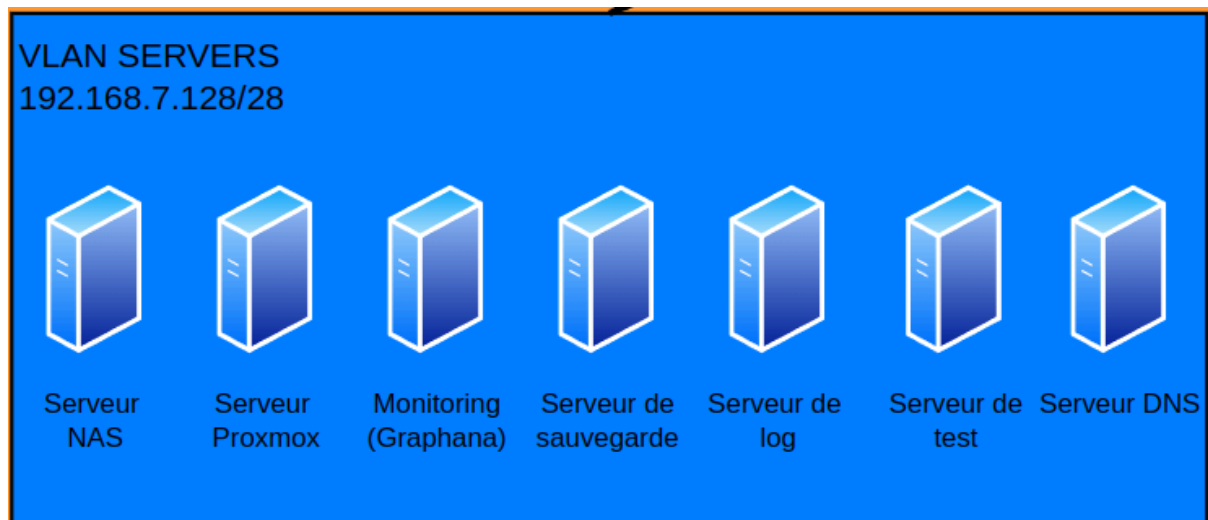




V. VLAN SERVERS

Cette section concerne uniquement le VLAN SERVERS, et les quelques services s'y trouvant.

Figure 4 : Visualisation logique du VLAN SERVERS à l'heure de l'écriture du document



A) Services hébergés

- NAS : partage NFS sécurisé via SSH et interface web d'administration (8181 par défaut) => 42621 dans notre infrastructure.
- Proxmox Virtual Environment : interface web d'administration (8006, mieux vaut ne pas changer le port)
- Grafana : interface web de supervision (58272)
- Collecteur de logs : Déploiement de Loki, qui centralise les logs et qui écoute sur le port HTTP (3100 par défaut) ou HTTPS.
- Agent Promtail : Déploiement sur les différents serveurs et accessible via http sur le port personnalisé 9080 pour apercevoir les résumés de prises d'informations via une page web.
- Serveur de test : sert de pré-production au site web et de workstation graphique avec RDP (port personnalisé).
- Serveur DNS : Directement installé avec le serveur Active Directory.
- SSH pour la prise en main des hôtes virtuels par le bastion.





B) Recommendations

- Limiter strictement les accès aux pages d'administration des services via le RDP.
- Réaliser des audits réguliers des accès au NAS et aux systèmes critiques.
- Réaliser un contrôle fréquent du bon fonctionnement des sauvegardes.

VI. Résumé des recommandations

- Chiffrement : il est impératif de passer les services écoutant sur un port HTTP vers HTTPS pour chiffrer les communications.
- Segmentation : renforcer l'isolation entre les VLAN, isoler les machines de la DMZ publique dans des VLAN attitrés.
- Contrôles d'accès : réaliser des règles de filtrage limitant strictement les débordements sur d'autres réseaux, le passage non maîtrisé d'un VLAN à un autre, l'accès aux pages d'administration des services.
- Mettre en place un système de surveillance centralisé ainsi que l'audit des connexions.
- Réaliser régulièrement des tests d'intrusion sur les différentes zones.
- Contrôler régulièrement le bon état et le bon fonctionnement des sauvegardes NAS ET disque externe.
- Changer les ports par défaut pour ajouter une barrière supplémentaire aux attaquants si des attaques venaient à arriver. Ils seront obligés de trouver, dans un premier temps, le bon port d'écoute pour parvenir à quelque chose.

