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.

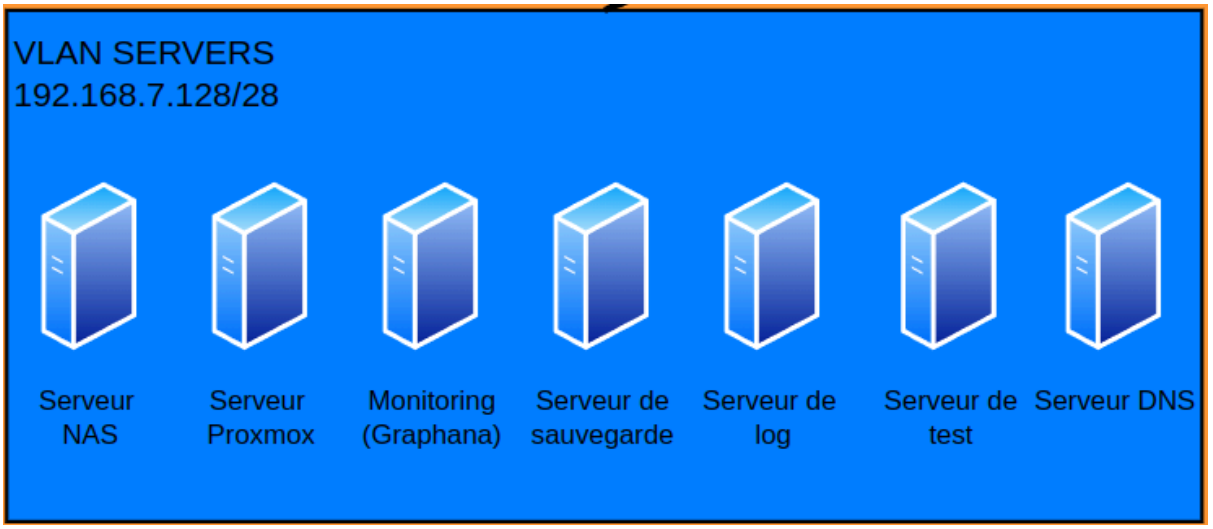
Recommandations :

- 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.

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 (port 14714) 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.
- Ajout de Prometheus sur le serveur de monitoring en écoute sur le port 49080
    - Changement du port par défaut de SNMP EXPORTER de Prometheus => 58419
    - Changement du port par défaut de ALERT MANAGER de Prometheus => 47171
    - Changement du port par défaut de NODE EXPORTER de Prometheus => 59051

B) Recommandations

- 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.

I. Introduction générale au PCA

Cette section présente les mesures préventives mises en œuvre pour maintenir l'activité critique de Wizards & Dice en cas de dégradation partielle ou totale de l'environnement technique. Contrairement au PRA, le PCA s'inscrit dans une logique d'anticipation et de maintien temporaire de l'activité, même dans un contexte fortement perturbé. Ce document s'appuie sur l'infrastructure en place (deux sites avec redondance, Proxmox, NAS, PBS) et les scénarios d'indisponibilité identifiés.

A) Objectifs du PCA

Le PCA a pour objectif de :

- **Assurer un service minimal** (site e-commerce, accès clients, consultation catalogue) même en cas d'indisponibilité partielle.
- **Garantir un accès sécurisé à distance** pour l'administration technique.
- **Prévoir des solutions de contournement temporaires** avant un retour à la normale via le PRA.

B) Périmètre du PCA

Le PCA couvre les activités essentielles suivantes :

- Affichage et consultation du catalogue produits via WordPress/WooCommerce
- Accès aux bases de données utilisateurs et commandes
- Administration distante via Bastion SSH
- Synchronisation minimale des sauvegardes entre les deux sites
- Et d'autres plus tard...

Ces éléments sont considérés comme prioritaires pour maintenir une présence commerciale et la continuité des commandes en cas d'incident.

II. Plan de continuité d'activité

Cette section présente les actions prévues pour garantir la continuité de service de l'infrastructure Wizards & Dice en cas d'incident majeur. Les scénarios traités ici correspondent aux risques identifiés comme prioritaires : perte d'un serveur, panne du site e-commerce, corruption de sauvegardes ou indisponibilité du stockage principal. L'objectif est de permettre une reprise rapide de l'activité sans perte critique de données.

A) Perte ou panne d'un hyperviseur Proxmox

1/ Arrêt brutal d'un hôte Proxmox (site AARD ou DRYN)

En cas de panne matérielle ou logicielle de l'hyperviseur (alimentation, carte mère, système Proxmox inaccessible), les VMs hébergées sur cette machine deviennent inaccessibles.

Deux cas sont possibles :

Si les disques sont intacts (ZFS ou LVM non corrompus), il est recommandé de transférer les disques physiques dans un second hôte ou de booter Proxmox depuis un live ISO pour accéder manuellement aux VMs.

Si la panne est critique ou les données inaccessibles, on bascule sur les sauvegardes journalières disponibles sur le NAS local ou le disque de secours.

👉 En cas de panne prolongée, les VMs critiques (site web, bases de données, bastion SSH) seront restaurées sur l'autre hôte depuis PBS.

📁 Procédure technique sur le GIT :
wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Procédure_restauration_VM.pdf

2/ Cluster Proxmox non joignable

Si le cluster PVE devient indisponible (panne réseau ou split-brain), il est possible de basculer les VMs manuellement sur un hôte secondaire configuré.

Voir procédure dans :

📁 wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Failover_cluster_hosts.pdf

B) Indisponibilité du site e-commerce en production

Le site web WordPress/WooCommerce est hébergé sur le site AARD. En cas de défaillance de ce site (coupure réseau, perte de Proxmox, problème logiciel sur la VM web, problème sur le serveur web), une intervention manuelle est requise pour relancer le service depuis le site DRYN.

Voici les étapes à suivre :

1. Vérifier si la VM web du site DRYN est prête à être lancée

   VM clonée ou restaurée en avance via rsync + PBS, avec le même contenu et base de données.

2. Accéder au tableau de bord OVH → OVH MANAGER

3. Aller dans "Domaines" > clamond.fr > Zone DNS

   ➤ Modifier les enregistrements A :

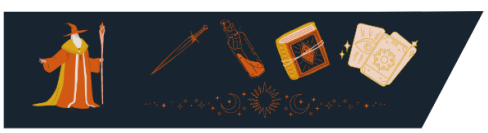
Nom	Ancienne IP (AARD)	Nouvelle IP (DRYN)
@ (racine)	xxx.xxx.xxx.1	xxx.xxx.xxx.2
www	xxx.xxx.xxx.1	xxx.xxx.xxx.2

4. Vérifier que le reverse proxy et le serveur web répondent bien sur DRYN avant de basculer.

5. Attendre la propagation DNS (de quelques secondes à 10–15 min selon TTL).

6. Une fois le site visible sur la nouvelle IP, faire des tests rapides : affichage page produit, commande, connexion admin.

📁 Pour plus de détails sur la procédure DNS OVH et test de basculement sur le GIT : wizards-n-dices\Infrastructure\SitesWeb\Failover_OVH.txt



III. Suivi et test du PCA

Cette section précise le cadre de vérification du PCA et la responsabilité du maintien en condition opérationnelle.

A) Fréquence des tests

1/ Tests semestriels

Un test de restauration des VMs critiques est effectué tous les 6 mois pour vérifier la validité des sauvegardes.

2/ Vérification des sauvegardes NAS

Le NAS effectue un rapport hebdomadaire de l'espace disque et de l'état des datastores, envoyé automatiquement par mail via SMTP.

II. Infrastructure actuelle, estimation des coûts et interconnexion

Introduction de la section :
Cette section traite du matériel dont nous disposons et de l'estimation de ce que nous aurons besoin, ainsi que de deux sites de notre infrastructure.

- Description de l'infrastructure actuelle : aborde la situation en date du 28/12/2024
- Interconnexion via VPN : établit des points important pour l'établissement d'une interconnexion
- Estimation des ressources nécessaires à l'infrastructure : contient l'estimation préliminaire des ressources nécessaires pour mettre en place notre infrastructure

A) Description de l'infrastructure actuelle

1/ Réseaux existants

À l'heure actuelle, deux réseaux existent, chacun sur un site d'hébergement. Il s'agit des réseaux privés du routeur opérateur d'Hugo, ainsi que celui de Loïs. Il a été convenu d'héberger l'infrastructure chez ces deux membres, leurs liens fibre étant les plus fiables et les plus performants des membres du projet.

2/ Site "Hugo"

Voici les adresses majeures du site situé chez Hugo CLAMOND :

- Adressage : 192.168.1.0/24
- Passerelle : 192.168.1.254
- IP publique : 82.64.57.23

3/ Site "Loïs"

Voici les adresses majeures du site situé chez Loïs ALLAIRE :

- Adressage : 192.168.1.0/24
- Passerelle : 192.168.1.1
- IP publique : NON-ATTRIBUÉ (changement de FAI)

- Serveur BDD Utilisateurs → Debian (VM)
- Serveur de cache → Debian (LXC)
- Serveur mail → Debian (LXC)
- Serveur de log → Debian (LXC)
- Serveur de monitoring → Grafana (LXC)
- Serveur de test (environnement de staging)→ Debian + XRDP (VM)
- Serveur WAF (Web Application Filtering) → Debian (LXC)
- Bastion SSH → Debian (LXC)
- Reverse Proxy → Debian (LXC)
- Serveur de sauvegarde (Proxmox Backup Server) (VM)
- Stormshield EVA1 (VM)

2/ Ressources physiques prévus pour les hôtes

L'avantage des conteneurs LXC est qu'ils partagent les ressources de l'hôte physique et, par leur nature de conteneur, consomment moins de ressources qu'une VM. Voici ce que ça donnerait au niveau de la répartition de la charge :

Service	Type d'hôte	Nombre vCPUs	Quantité RAM	Espace disque	Commentaires
Serveur web	LXC	1	512 Mo	8 Go	Apache/Nginx - Hébergement de pages plutôt légères.
Serveur DNS interne	LXC	1	512 Mo	2 Go	Webmin ou PiHole - très peu de ressources
Serveur de log	LXC	1	512 Mo	16 Go	Graylog/ELK – prévision d'une faible charge de journaux
Serveur de monitoring	LXC	1	512 Mo	16 Go	Grafana, peu de ressources demandées
Serveur WAF	LXC	1	512 Mo	8 Go	ModSecurity ou équivalent basé sur Nginx
Bastion SSH	LXC	1	256 Mo	2 Go	Faible charge pour la gestion des connexions SSH
Reverse Proxy	LXC	2	512 Mo	4 Go	Nginx ou HAProxy
Serveur BDD Production	VM	2	2 Go	32 Go	Contient les articles, les utilisateurs, les commandes
Serveur BDD Pre-prod	VM	1	1 Go	32 Go ou moins	
Serveur de test	VM ou LXC	2	4 Go	32 Go	Réplique de la prod, y fait tourner des services RDS
Serveur de sauvegarde	VM	2	4 Go	64 Go	Serveur Proxmox Backup Server (PBS)
Stormshield EVA 1	VM	2	2 Go	8 Go	Firewall virtualisé avec charge réseau modérée

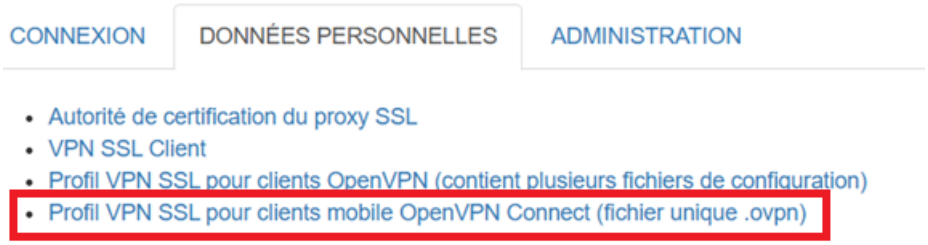
3/ Besoins en matériel

À partir du tableau ci-dessus, nous pouvons établir une liste des besoins matériels pour les deux hôtes Proxmox :

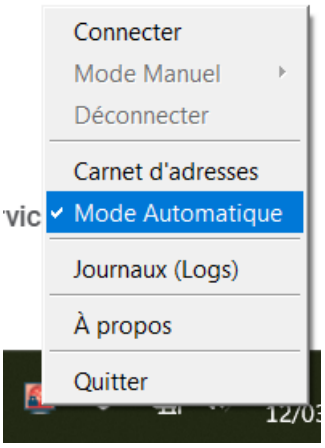
- CPU : Processeur à 4 ou 8 cœurs (8 étant plus recommandé pour être tranquille)
- RAM : 16 Go DDR3/4, cadence et génération de RAM à voir en fonction de la machine choisie
- Stockage : 512 Go en SSD minimum, plus 1 To de stockage HDD pour sauvegardes locales (optionnel), interne ou externe.

En plus des hôtes physiques, un NAS 4 baies (potentiellement Terramaster) monté en RAID 5 est à prévoir.

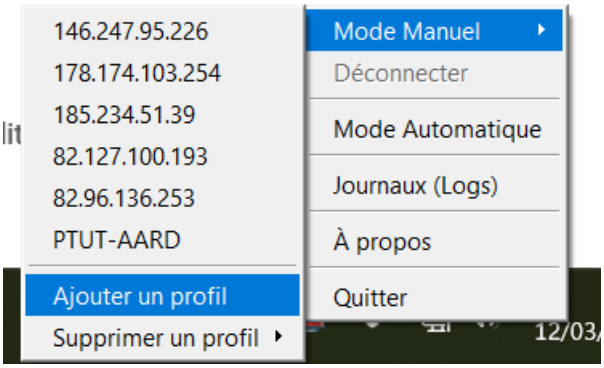
1. Ouvrir : https://82.64.57.23:43538/auth/
2. Se connecter avec les identifiants AD
3. Télécharger le profil .ovpn



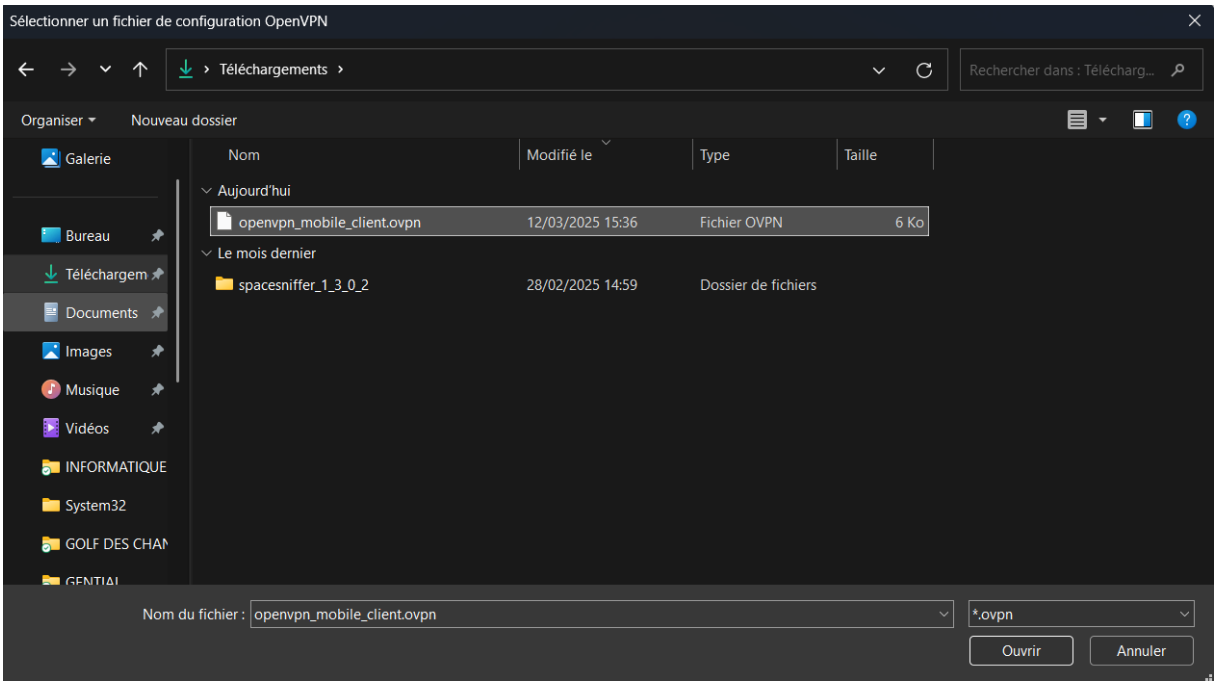
4. Ouvrir le fichier .ovpn avec le bloc-notes et modifier la ligne “remote 192.168.1.219 43537 udp” pour la remplacer par “remote 82.64.57.23 43537 udp” si vous vous connectez au VPN du site AARD, “remote 88.160.94.24 43537 udp” si vous vous connectez au VPN du site DRYN.
5. Télécharger et installer le client VPN SSL Stormshield : https://vpn.stormshield.eu/
6. Lancer le client VPN.
7. Clic droit sur l’icône rouge du VPN -> Cliquer sur "Mode automatique" pour basculer sur le mode manuel.



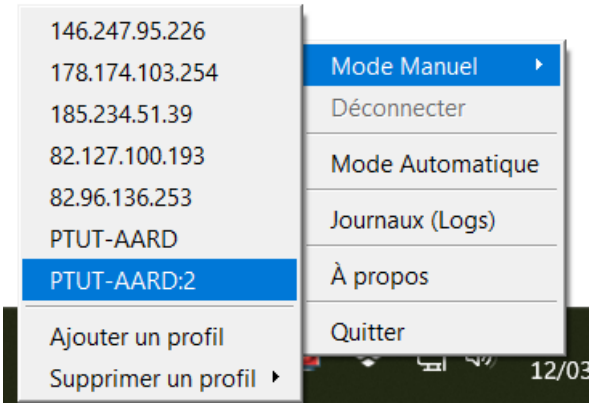
8. Clic droit sur l’icône du VPN et passer la souris sur "Mode manuel >" puis cliquer sur "Ajouter un profil".



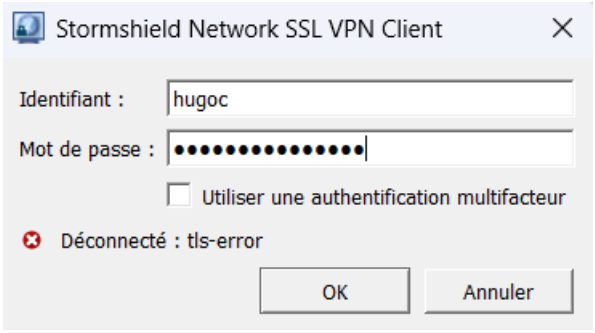
9. Rechercher le .ovpn téléchargé précédemment et le sélectionner, puis l’ouvrir.



10. Donner un nom au profil et cliquer sur OK.
11. Clic droit sur l'icône de VPN -> "Mode Manuel >" -> Cliquer sur le profil nouvellement créé.



12. Entrer les identifiants AD et cliquer sur OK.



A noter que le VPN peut avoir du mal à se connecter et bloquer sur « WAIT », auquel cas se déconnecter et relancer la connexion au VPN.

WIZARDS & DICE

E-commerce & forum dédié au jeu de rôle

www.wizardsndice.fr

contact.wizardsndice@gmail.com

CARTE - PALADIN
WIZARDS & DICE

ARTHUR YANG

Responsable Documentation & Administratif

Maître des Rituels Légaux & Protecteur des Jalons

+3 Dextérité : Navigue avec précision dans les contrats

+1 Force : défend le dialecte obscur du code civil

-2 Charisme : Prend tout au premier degré

CARTE - BARDE
WIZARDS & DICE

LOÏS ALLAIRE

Responsable
Design & Marketing

Négociateur de Génie & Alchimiste de l'Attrait

+2 **Charisme : Charme son prochain pour gagner son pain**

+2 **Dextérité : manipule les lignes pour attirer l'œil**

-3 **Chance : Se retrouve toujours dans le pétrin**