




# Jalon 4 : part d'Axel pour les répétitions


## WIZARDS & DICE

 Créateur : Axel MOURILLON – Chef de projet

 Date de Création : 12/02/2025

 Dernier modificateur : <Prénom NOM> – <Rôle>

 Date de modification : JJ/MM/2025

 Version : 1.0



# Table des matières

<b>I. Rationalisation et synthèse.....</b>	<b>2</b>
<b>II. Suggestions pour le support de diapositive.....</b>	<b>4</b>





# I. Rationalisation et synthèse

## II. Présentation globale de l'infrastructure

### **Réseaux existants**

- Chaque site : un plan d'adressage IP et VLANs segmentés par usage
- VLAN : servers, users, BDD et DMZ
- Segmentation : services isolés / performances optimisées / trafic sécurisés

### **Interconnexion des sites via VPN**

- VPN IPSec : communication sécurisée entre sites
- Tunnel VPN : gestion centralisée et accès aux ressources distantes le tout en sécurité

### **Connexion aux sites via VPN**

- VPN SSL : complément du VPN IPSec ; accès distant sécurisé  
⇒ Pour les connexion des admins et des users hors site

## III. Sécurisation et supervision (R5.Cyber.11)

### **Recommandations de sécurité**

- Revue de sécurité réalisée  
⇒ Analyser les risques potentiels, appliquer les bonnes pratiques de cybersécurité
- Plusieurs aspects critiques revus :
  - Surface exposé à Internet
  - Protection des accès distants
  - Gestion des flux internes (entre site / VLAN)
- Analyse de la surface exposé
  - DMZ publique : serveur web / reverse proxy / WAF  
⇒ Objectifs : Réduire au maximum la surface d'attaque ; restreindre et filtrer les flux trafic nécessaire
- Éléments mis en place suite à la revue de sécurité
  - Interdiction d'HTTP ⇒ utilisation d'HTTPS forcé
  - Revue régulières des ports ouverts (scan) : détection d'expositions involontaires
  - Filtrage strict des flux au niveau du pare-feu [de chaque site]
- But : limiter les risques d'intrusion depuis l'extérieur / conserver de la flexibilité pour l'administration de l'infra

## IV. Point techniques et d'avancement

### **Choix des solutions et justification des technologies**

#### → **Hyperviseur et virtualisation**

- Virtualisation de l'infrastructure par Proxmox VE (PVE)
  - Solution open-source, robuste, et gratuite
  - Supporte les VM et les conteneurs ⇒ optimisation des ressources
  - Intégration native de gestion des sauvegardes avec Proxmox Backup Server (PBS)



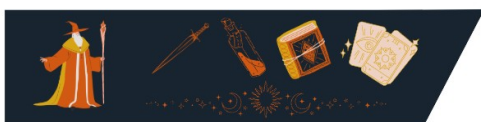


- Architecture mixte de VM et de conteneurs LXC
  - VMs pour les services critiques / un isolement complet : BDD, sauvegardes, AD
  - Conteneurs pour des services légers partageant le noyau d'un hôte : serveurs web / WAF / monitoring et reverse proxy
  - ⇒ Améliorer les perf et optimiser et réduire la consommation des ressources
- **Applicatif et serveur web (Apache/WordPress)**
- Côté applicatif : plateforme e-commerce donc WordPress + WooCommerce.
  - PrestaShop envisagé : performant mais moins flexible pour certaines de nos fonctionnalités (ex : blog)
  - Magento envisagé : trop complexe à administrer trop gourmand en ressources
- Le cas WordPress + WooCommerce : compromis idéal
  - Facilité de déploiement / administration (même pour des non-techniques)
  - Écosystème riche en extensions : ajout rapide de nouvelles fonctionnalités (paiements, gestion des stocks, avis clients, ...)
  - Optimisé pour le SEO [Search Engine Optimization] : référencement du site
  - Flexibilité pour intégration d'éléments communautaires (blog, forums, système de membres)
- Serveur web Apache plutôt que Nginx
  - Compatibilité avec .htaccess : gestion des redirections et des règles de sécurité.
  - Meilleure compatibilité avec les modules PHP
  - Configuration plus intuitive : facilite son administration

## V. Planning et organisation

### **Prochaines étapes**

- En cours : déploiement basique des services et serveurs ⇒ Socle de notre architecture
  - Bastion SSH
  - Serveur de logs
  - Bases de données
  - Serveur web
  - Services transverses (lien avec Active Directory notamment – LDAP)
- Défis techniques : choses retors mais qui avancent
  - Configuration avancée du pare-feu nécessite des ajustements
  - Ajustement de la récente mise en cluster des hyperviseurs Proxmox
- Les étapes suivantes (techniques only) :
  - Mise en place du reverse proxy, du WAF et de la supervision / monitoring infra
  - Finalisation des configurations le nécessitant : système, réseau et applicatif
    - ⇒ Chaque service doit fonctionner correctement
  - Sécurisation de l'infrastructure
    - Réseau : pare-feu Stormshield, segmentation VLAN, restrictions d'accès
    - Système : pare-feu sur les VM, restrictions des logiciels
    - Applicative : durcissement des services, protection contre les vulnérabilités, monitoring des activités suspectes
  - Implémentation et la mise en production du site e-commerce
    - Paramétrage de WordPress et WooCommerce
    - Optimisation des performances
    - Tests fonctionnels avant la validation du Proof of Concept (POC).





## II. Suggestions pour le support de diapositive

### II. Présentation globale de l'infrastructure

Pour représenter et/ou illustrer les parties suivantes :

- Réseaux existants  
Plan d'adressage des IP (utilisées) et des réseaux
- Réseaux existants ; Interconnexion des sites via VPN ; Connexion aux sites via VPN  
Schéma d'interconnexion des sites, avec les IP importantes du VPN (voir sur l'étude technique ou avec le responsable technique)
- Connexion aux sites via VPN  
Logo OpenVPN (pas sur, pas primordial)

### III. Sécurisation et supervision (R5.Cyber.11)

Pour représenter et/ou illustrer les parties suivantes :

- Recommandations de sécurité  
Pictogrammes pour les aspects critiques de la revue de sécurité (Surface exposé à Internet / Protection des accès distants / Gestion des flux internes)  
⇒ Idée de réduire la surface d'attaque et de filtrer les flux (tout en gardant de la flexibilité pour l'administration)

### IV. Point techniques et d'avancement

Pour représenter et/ou illustrer les parties suivantes :

- Choix des solutions et justification des technologies → Hyperviseur et virtualisation  
Logo Proxmox Virtual Environnement et Proxmox Backup Server  
Schéma de comparaison VM – conteneur
- Choix des solutions et justification des technologies → Applicatif et serveur web  
Logo Apache, Wordpress et WooCommerce  
Pictogramme pour l'aspect SEO [Search Engine Optimization] de Wordpress

### V. Planning et organisation

Pour représenter et/ou illustrer les parties suivantes :

- Prochaines étapes  
[Aux choix ou plusieurs] Illustration de planning / screenshot du GANTT W&D / GANTT simplifié et schématisé  
Cheminement de pictogrammes : Fin déploiement basique > Fin configuration des fonctionnalités > Sécurisation > Mise en prod du site

### **OVERALL (pour toutes les parties)**

Pictogramme / logo de solutions à la convenance

