




Étude technique préliminaire

WIZARDS & DICE

 Créateur : Hugo CLAMOND – Responsable infrastructure et système

 Date de Création : 28/12/2024

 Dernier modificateur : Axel MOURILLON – Chef de projet

 Date de modification : 11/01/2025

 Version : 2.1



Table des matières

Table des figures.....	2
I. Introduction.....	3
II. Infrastructure actuelle, estimation des coûts et interconnexion.....	4
A) Description de l'infrastructure actuelle.....	4
1/ Réseaux existants.....	4
2/ Site "Hugo".....	4
3/ Site "Loïs".....	4
B) Interconnexion via VPN.....	5
1/ Interconnexion entre les deux sites.....	5
2/ Spécificités de l'IPSec.....	5
3/ Spécificités du VPN SSL.....	5
C) Estimation des ressources nécessaires à l'infrastructure.....	5
1/ Machines virtuelles ou conteneurs LXC ?.....	5
2/ Ressources physiques prévus pour les hôtes.....	6
3/ Besoins en matériel.....	7
III. Les réseaux et leur découpage.....	8
A) Réseaux locaux virtuelles.....	8
B) DMZ.....	8
IV. Mesures de sécurité : de la redondance à la gestion des accès.....	9
A) Redondance.....	9
1/ Moyens pour mettre en place la redondance.....	9
2/ Les machines à redonder.....	9
3/ Accès à Internet.....	9
B) Sauvegarde et restauration.....	10
1/ Technologies mise en œuvre.....	10
2/ Plan de sauvegarde.....	10
C) Gestion des accès.....	10
1/ Bastion SSH.....	10
2/ Politique de mots de passe.....	11
3/ Gestion des incidents.....	11
V. Technologies Web, monitoring et règles de nommage.....	12
A) Technologies applicative du site.....	12
1/ Besoins d'un site de e-commerce.....	12
2/ Technologies adaptées.....	12
B) Suivi de l'état de l'infrastructure.....	12
1/ Technologies de supervision.....	12
2/ Points d'attention de l'infrastructure.....	13
3/ Gestion des alertes.....	13
C) Règles de nommage.....	13





Table des figures

Figure 1 : Schéma simplifié physique de l'infrastructure prévue.....	3
Figure 2 : Schéma logique de l'infrastructure d'un site.....	3





I. Introduction

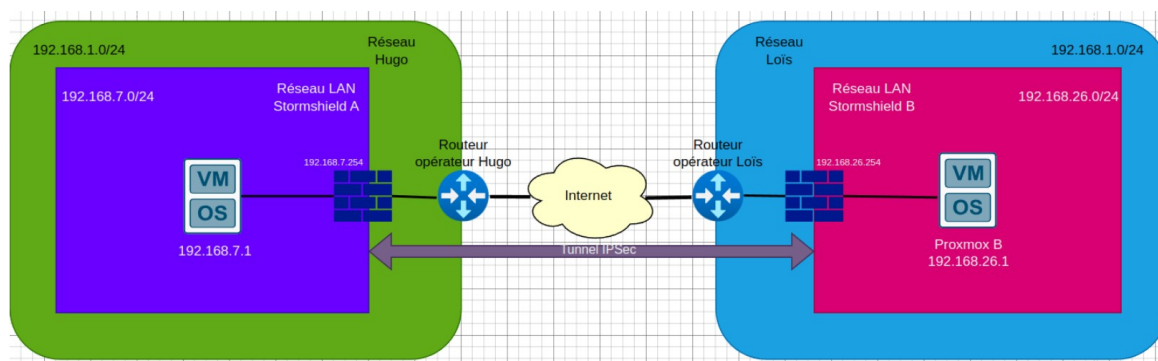


Figure 1 : Schéma simplifié physique de l'infrastructure prévue

Le projet Wizards & Dice a pour objectif de créer un site web de e-commerce. Notre équipe projet sera en charge d'assurer le fonctionnement de l'infrastructure hébergeant ce site. La plupart des logiciels et des services seront tirés du monde de l'open-source pour limiter au maximum les dépenses, matériel mis à part.

Parmi les objectifs principaux se trouve la réalisation d'une redondance des machines virtuelles par liaison IPSec. Cette liaison, et l'infrastructure en général, représentent un défi technique de taille. En effet, la partie sécurité étant également virtualisée, nous devons articuler la sécurité avec le niveau de fonctionnalité et de facilité de gestion que nous voulons mettre en œuvre.

Le schéma d'infrastructure ci-dessous résume ce qui doit être soutenu par l'hyperviseur Proxmox. L'exemple d'adressage concerne le site Hugo.

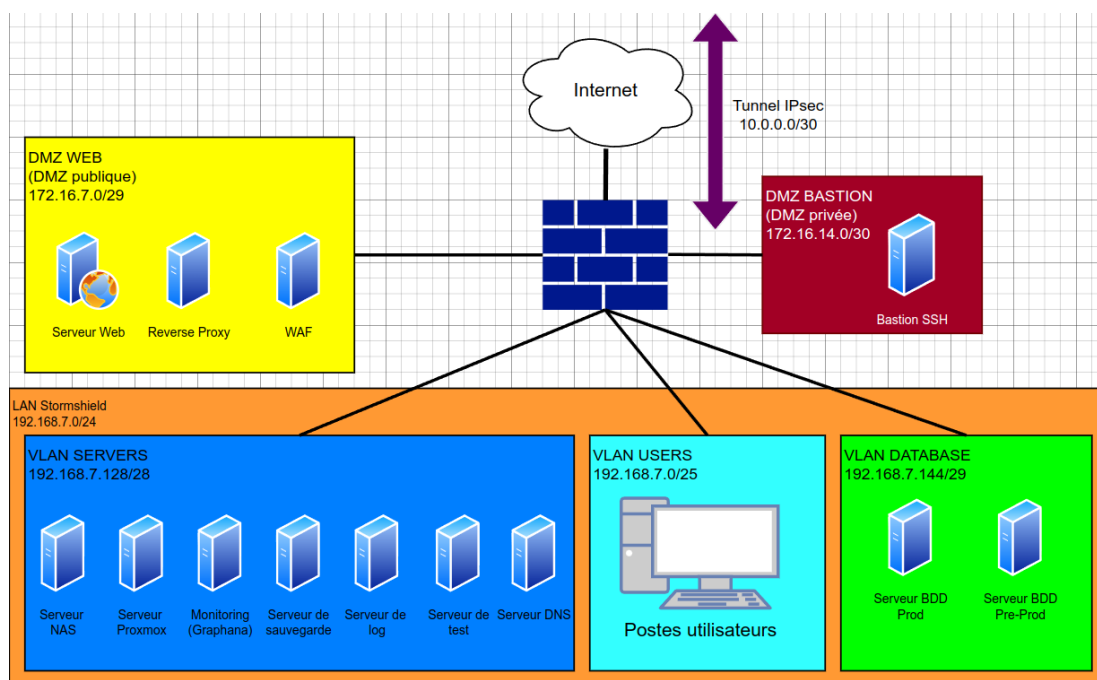


Figure 2 : Schéma logique de l'infrastructure d'un site





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 importants 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)





B) Interconnexion via VPN

1/ Interconnexion entre les deux sites

L'ensemble de la connexion inter-sites n'existe pas encore car elle doit être déployée à l'aide des pare-feux Stormshield qui seront virtualisés dans les serveurs Proxmox. Lorsque les pare-feux seront en place, un tunnel IPSec par VTI (Virtual Tunnel Interface) sera mis en place.

2/ Spécificités de l'IPSec

Les paramètres IPSec seront les suivants :

- Algorithme de chiffrement : AES256
- Utilisation de PSK pour négocier le tunnel
- Utilisation d'IKEv2
- Extrémités de trafic utilisent des VTI, réseau 10.0.0.0/31

Les deux extrémités de trafic sont des pare-feux Stormshield EVA1

3/ Spécificités du VPN SSL

Les éléments importants de la configuration d'un tunnel VPN SSL seront les suivants :

- Ouverture d'un portail captif en interne et externe sur un port spécifique (à définir)
- Service de VPN SSL ouvert sur le port « sslvpn » de Stormshield
- Attribution d'une IP sur un réseau « VPNSSL » qui a les mêmes accès qu'un utilisateur interne

Note : tous les accès par VPN, que ce soit IPSec ou SSL, seront tracés dans les logs avec la fonction « avancé » dans les traces de la page d'admin du firewall, ce qui active la journalisation pour la règle de filtrage cible.

C) Estimation des ressources nécessaires à l'infrastructure

1/ Machines virtuelles ou conteneurs LXC ?

Voici la liste des hôtes virtualisés au sein de l'infrastructure prévue :

- Serveur web Apache → Debian (LXC)
- Serveur BDD Articles → Debian (VM)
- 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	Réplication 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.





III. Les réseaux et leur découpage

Introduction de la section :

Cette section traite du découpage en multiples réseaux internes et des surfaces de contacts externe de celle-ci.

- Réseaux locaux virtuelles : établies les réseaux virtuels régissant notre réseau interne
- DMZ : caractérise nos surfaces de contacts externe

A) Réseaux locaux virtuelles

Ci-dessous se trouve un tableau des VLANs de la patte LAN de chaque site ainsi que leur adressage réseau. Dans l'adressage, le X représente « 7 » dans le site d'Hugo, et « 26 » dans le site de Loïs.

ID	Nom	Adressage
10	USERS	192.168.X.0/25
20	SERVERS	192.168.X.128/28
30	DATABASE	192.168.X.144/29

B) DMZ

Voici l'adressage régissant les DMZ de l'infrastructure

Nom	Emplacement	Adressage
dmz_priv	Site Hugo	172.16.14.0/30
dmz_pub	Site Hugo	172.16.7.0/29
dmz_priv	Site Loïs	172.16.52.0/30
dmz_pub	Site Loïs	172.16.26.0/29





IV. Mesures de sécurité : de la redondance à la gestion des accès

Introduction de la section :

Cette section traite de la sécurisation de nos données par la sauvegarde, mais parle aussi de la redondance qui nous aidera à attendre la haute disponibilité pour notre site de e-commerce.

- Redondance : aborde les aspects importants de l'application des principes de redondance dans notre infrastructure
- Sauvegarde et restauration : parle de nos méthodes de sauvegarde
- Gestion des accès : détaille les mesures de sécurité appliquées à notre infrastructure

A) Redondance

1/ Moyens pour mettre en place la redondance

L'hyperviseur Proxmox mettant en grappe les deux hôtes physiques, les VM et les conteneurs d'un site seront sauvegardés sur l'autre. On met alors en place un système de site « principal » et l'autre « secondaire », pour les hôtes virtuels du site web et des BDD. Ces dernières peuvent être mises en « master-slave » pour assurer un fail-over. Des outils comme Master High Availability ou Orchestrator permettent de gérer le fail-over des BDD. Pour le contenu des sites, étant donné que les hôtes virtuels se trouvent dans une DMZ publique, nous effectuerons la synchro par rsync à travers un tunnel SSH.

2/ Les machines à redonder

Le site web et le serveur de BDD de production doivent être redondés avec les méthodes citées ci-dessus. Les autres hôtes virtuels seront simplement sauvegardés.

3/ Accès à Internet

La connexion d'utilisateurs au site repose sur un enregistrement DNS au sein d'un fournisseur dédié. Ce fournisseur doit pouvoir assurer le basculement automatique sur une autre IP publique en cas de défaillance de la connexion internet du premier site. Même si c'est moins important, il doit également être en mesure de nous créer des adresses e-mail liées à notre domaine. Si nous avons besoin d'un cloud pour y stocker quelques fichiers, nous créerons un compte de stockage cloud à l'aide de nos adresses déjà établies.

Quelques fournisseurs et une estimation des coûts mensuels (failover DNS + boîtes mail) :

- Google Cloud DNS + Google Workspace - ~34€/mois
- Amazon Route 53 + Amazon WorkMail : ~22€/mois
- Cloudflare + Zoho Mail : ~25€/mois
- OVH : ~13€/mois





B) Sauvegarde et restauration

1/ Technologies mise en œuvre

Un serveur de sauvegarde Proxmox Backup Server sera mis en place sur chaque site. Son but est de sauvegarder les hôtes virtuels mais aussi l'hôte physique.

PBS permet de piloter les différents supports de sauvegarde : disques branchés en interne, disques externes, NAS... Les jobs de sauvegarde en eux-même sont pilotés par PVE, d'où l'intérêt de mettre en grappe les serveurs PVE – on pilote les jobs de tous les nœuds de manière centralisée.

Sauvegarder vers un emplacement réseau, tel qu'un partage de fichiers vers un disque dur interne de sauvegarde, demande de monter un chemin réseau sur PBS. Pour cela on peut s'appuyer sur NFS, facile à monter, ou bien son alternative plus sécurisée, SSHFS (authentification par clé pour monter le partage).

2/ Plan de sauvegarde

Les sauvegardes de l'intégralité des hôtes seront effectuées de quotidiennement et pointeront vers un NAS situé sur le site d'Hugo. Les backups tourneront le soir à 22h et devront s'arrêter à 6h, quoi qu'il arrive.

Des sauvegardes hebdomadaires seront effectuées sur un HDD interne ou externe branché sur l'hôte physique. Même plage horaire que les backups quotidiennes.

En dehors de la fenêtre de sauvegarde définie, si le disque de sauvegarde est externe, doit être débranché et emmené avec Hugo ou Loïs en cas de déplacement.

C) Gestion des accès

1/ Bastion SSH

L'idée de base est d'utiliser un bastion qui va avoir pour objectif de centraliser les connexions SSH vers les autres hôtes à partir de cet hôte en particulier. Cela offre plusieurs avantages :

- Point d'entrée unique dans l'infra d'un site,
- Monitoring des actions et des connexions.

Si l'on devait assurer un niveau minimal d'accessibilité, nous ferions uniquement un bastion SSH. Pour prendre en charge d'autres protocoles comme VNC ou RDP, nous allons mettre en place un bastion Guacamole, potentiellement avec des plugins supplémentaires pour compléter les fonctionnalités de cette solution assez sommaire (mais qui fera déjà bien le travail).





De par le fait que le bastion peut logger les connexions, on crée un identifiant unique « adm_wnd », possédant les droits sudo, et on désactive root sur les services que l'on installe par-dessus les hôtes virtuels. Par mesure de précaution, on ne le désactive pas du système lui-même, ça peut toujours être utile pour dépanner...

Chaque connexion SSH gérée par le bastion aura un jeu de clés SSH. Les connexions SSH seront communes à tous les utilisateurs habilités à réaliser des opérations d'administrateur. Pour le RDP, chacun aura son utilisateur pour éviter les erreurs de connexion ou les déconnexions intempestives.

2/ Politique de mots de passe

Il sera obligatoire, pour chaque membre du projet, d'utiliser un mot de passe robuste, d'entropie minimale à 90 bits. Pour calculer l'entropie d'un mot de passe, il est possible de passer par un [calculateur d'entropie](#).

Note : cela vaut aussi pour les comptes utilisateurs des machines. Nous stockerons les mots de passe communs dans une base de données KeePass, elle-même stockée dans un Drive commun.

3/ Gestion des incidents

La gestion des incidents repose sur 3 points :

1. Sources de détection :
 - Alertes via Grafana
 - Remontées utilisateurs (tickets dans le cadre du projet)
 - Journaux (centralisés par le serveur de log)
2. Types d'incident :
 - Performance : ralentissements des applications, surcharge serveur/VM...
 - Sécurité : tentatives de connexions non autorisées, logiciels malveillants
 - Matériel : panne de disque dur, défaillance matérielle sur les hôtes physiques
 - Réseau : tunnel IPSec en panne, problème de connexion internet...
 - Applicatif : erreurs de site web, logiciels/services déployés
3. Classification des priorités/gravités
 - Critique : impacte directement le service client/interne
 - Haute : Affecte les opérations mais avec une solution temporaire
 - Moyenne : Nécessite une action corrective, mais sans impact direct sur les opérations.
 - Basse : Impact faible à négligeable sur les opérations.

Les outils que nous envisageons de déployer pour gérer les incidents

- Outils de monitoring : Grafana
- Suivi de tickets d'incident : Taiga
- Centralisation des journaux : Techno à définir (ElasticSearch, Logstash, Kibana...)





V. Technologies Web, monitoring et règles de nommage

Introduction de la section :

Cette section aborde le sujet des technologies applicatives que nous utiliserons pour suivre l'état de notre infrastructure mais aussi du site Web en lui-même.

- Technologies applicative du site : parle des applications qui nous permettrons de mettre un place le site de e-commerce
- Suivi de l'état de l'infrastructure : parle des applications qui aiderons à superviser notre infrastructure
- Règles de nommage : détaille les règles de nommages régissant les hôtes de notre infrastructure

A) Technologies applicative du site

1/ Besoins d'un site de e-commerce

Défilement d'articles sur une page d'accueil, des pages « statiques » pour les articles. Pages de profil utilisateur.

Dans un second temps : possibilité de monter des forums.

2/ Technologies adaptées

CMS spécialisés E-commerce ou avec plugins :

- PrestaShop,
- Wordpress + WooCommerce

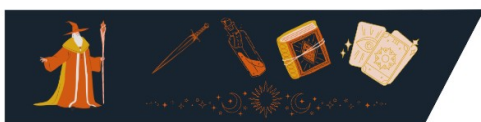
Après tests, deux CMS très prometteurs et très personnalisables. Possibilité de mettre en place des paiements par CB, PayPal ou virement bancaire sous Prestashop avec un module supplémentaire (gratuit). Pareil sous WooCommerce (WooPayments).

Forums : Prestashop : modules existants ; Wordpress : pléthore de plugins existants.

B) Suivi de l'état de l'infrastructure

1/ Technologies de supervision

Grafana a été recommandé par Ulysse : à priori simple, peu gourmand et flexible.





2/ Points d'attention de l'infrastructure

Un site surveille ses propres VMs ainsi que la connectivité au sein du tunnel IPSec.

3/ Gestion des alertes

Les alertes seront envoyées par e-mail à une adresse créée spécialement pour cela à l'aide du fournisseur d'adresses mail choisi.

C) Règles de nommage

Ci-dessous sont détaillé les règles de nommage utilisé dans l'infrastructure :

- Pour les hôtes
 - Serveurs virtuels : SRV-NomService
Potentielles VMs clients : PC-Date-de-creation-numero (si plusieurs déployé)
 - Hôtes physiques :
 - Drôme : SRV-WND-DRYN (sonorité « Drôme » et peut être associé à « dryade »)
 - Ardèche : SRV-WND-AARD (sonorité « Ardèche » et rappelle le signe d'Aard du Sorcelleur)
- Réseaux
 - VLAN : suivre le tableau sur les VLAN.
- Interfaces
 - Interfaces des conteneurs : toujours eth0.
 - Interfaces rattachées aux PVE :
Nommé en fonction du type de réseau auquel se rattache l'interface.
Exemple :
« in » à rattacher à la patte LAN du Stormshield ⇒ *in.ID_VLAN_SERVERS*
pour la patte du PVE se trouvant dans le VLAN SERVERS.
- Bastion
 - Création d'une connexion : le nom de la connexion doit correspondre au nom d'hôte du serveur cible.
 - Création d'un utilisateur : le nom de l'utilisateur doit correspondre à « nomdefamille » suivi de la première lettre du prénom : Hugo CLAMOND → clamondh
- DNS
 - Local : wizardsndice.local
 - Global : wizardsndice.fr

