

Rapport Technique V2

Méthodologie

Le travail étant conséquent, nous nous sommes fixés des objectifs de progression qu'il fallait respecter le plus possible pour éviter de prendre du retard. Et si c'était toutefois le cas, le fait d'avoir organiser notre travail en livrable nous permettra de quantifier le travail encore à faire pour le compléter au mieux.

Pour nous aider à atteindre cet objectif et garder cette méthodologie en place, nous nous sommes servis de plusieurs outils très efficace dans la gestion de projet et qui nous permettent de nous coordonner.

Ces outils sont les suivants :

- Trello : utilisé pour pouvoir planifier l'avancement du projet et mettre des deadlines pour ne pas dépasser le temps imparti.
- Github : utilisé afin de pouvoir partager les ressources et fichiers sur lesquels notre groupe travaille, et garder une trace écrite du projet.
- Overleaf(Latex) : utilisé afin de rédiger nos rapports réguliers et notre cahier des charges de manière structurée. ➔ Ensuite remplacé par Word pour la simplicité.

Au niveau des technologies fonctionnelles nous permettant de développer et de résoudre à proprement parler le problème :

- Docker avec Dockerhub : Docker est un incontournable pour mettre en place plusieurs services sur un seul et même VPS sans le surcharger. Dockerhub quant à lui nous permet de stocker à la manière de Github, nos dockers en ligne et de pouvoir les récupérer facilement et à tout moment depuis n'importe quel poste de travail.
- Nginx pour le service Web.
- Bind9 pour le service DNS.
- Postfix pour le service Mail.
- Et nous ne savons pas encore pour le service VOIP".

Etat d'avancement

Mission 0

- ✓ Nous avons réalisé le premier jet des différents schémas qui permettent d'avoir une visualisation de la structure réseau de l'entreprise.
- ✓ Nous avons commencé le premier jet de la rédaction des rapports (client et technique).

Toute la configuration des différents éléments de ces schémas restent cependant à faire.

Mission 1

- ✓ Connexion aux VPS et création des différents sudoers pour chaque membre du groupe.
- ✓ Sécurisation basique du VPS avec fail2ban et renseignements sur les autres mesures de sécurité (changements de ports, rkhunter, ...).
- ✓ Mis en place des dockers pour le service Web et le DNS sur le VPS.

Mission 2

- ✓ Configuration du service Web via NGINX (début).
- ✓ Configuration du service DNS via Bind9 (début).
- ✓ Création des dockers Users, simulant les différents départements de WoodyToys.
- ✓ Configuration du service Mail via Postfix (début).

Schémas réseaux et les justifications des choix architecturaux effectués

La structure des schémas réseaux est censé évoluée au fur et à mesure de l'avancée du projet étant donné que c'est une matière qui nous est nouvelle, des erreurs de conception peuvent intervenir.

Ces schémas ont été revu déjà 4 fois et sont sans doute une version finale.

Schéma Woodytoys

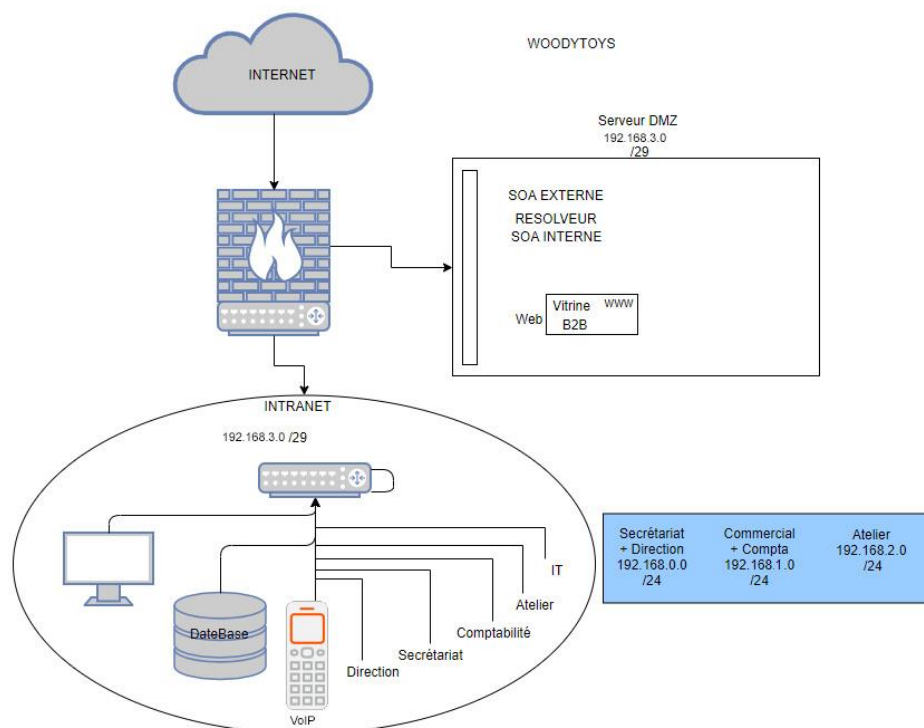


Figure 1 – schéma du réseau de l'entreprise Woodytoys

Nous avons divisé le réseau en 3 parties :

1. Une partie Internet
2. Une partie DMZ
3. Une partie intranet

Le réseau DMZ sert pour les fonctionnalités qui doivent être accessibles en externe mais de manière sécurisée. Le résolveur en fait donc partie ainsi que le serveur mail, le VoIP, le SOA et la partie web divisé en vitrine (www) et B2B. La partie intranet sert uniquement pour des besoins internes à la société comme tous les secteurs de la compagnie ainsi que la base de données.

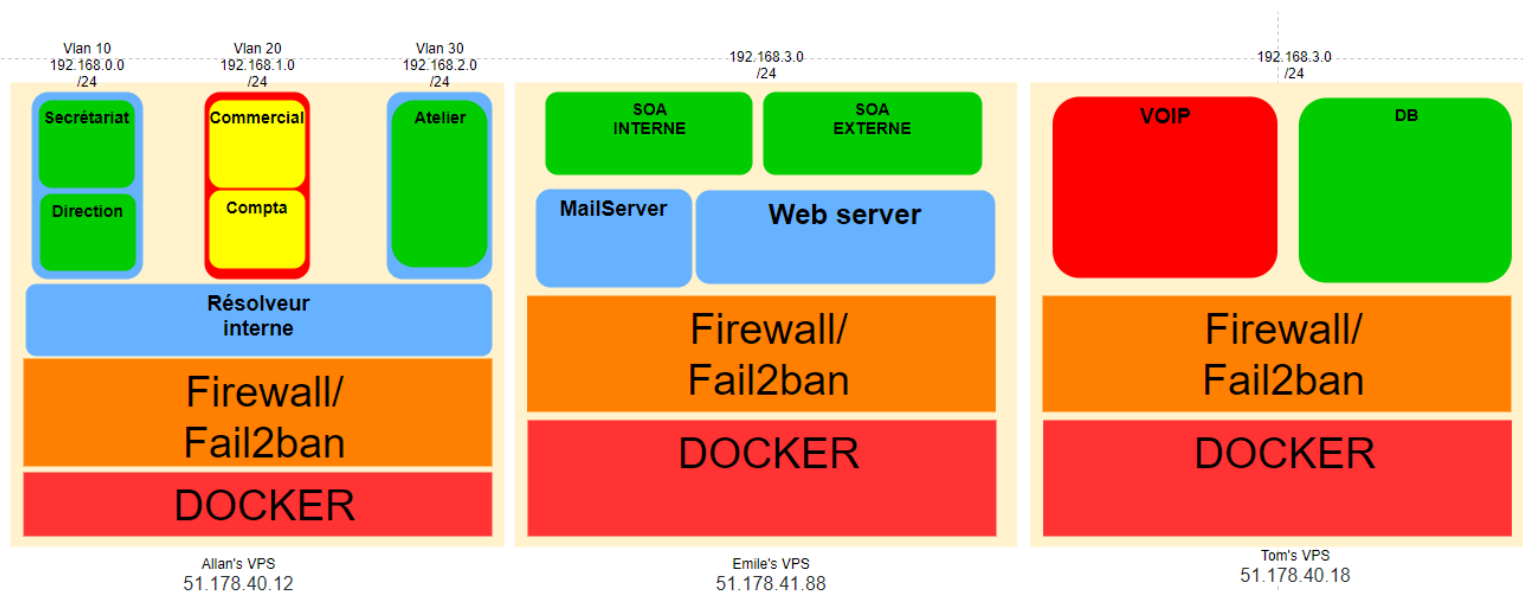


Figure 2 – schéma prototype de la structure réseau de l'entreprise Woodytoys

Pour chaque VPS, nous avons placé un docker afin d'avoir un container dans lequel nous allons placer nos différents services qui seront protégé par un firewall individuel ainsi que Fail2ban.

- Le premier VPS (celui d'Allan) contiendra toutes les VLANS des différents secteurs et également le résolveur interne.
- Le deuxième VPS (celui d'Emile) contiendra le service Mail, serveur web, le service DNS et SOA.
- Le troisième VPS (celui de Tom) contiendra la base de données et la VoIp.

Le choix de cette implémentation s'explique par notre volonté de déployer une solution efficace et sécurisée pour la société. Chaque VPS étant censé représenter un aspect du réseau, notre schéma a donc été rempli dans ce but-là.

Difficultés rencontrées

Tout au long du projet, de nombreuses difficultés ont été rencontrées, notamment dans l'implémentation des différents dockers et services. Certaines installations se sont révélées bien plus difficiles que prévu. Comme par exemple l'installation de Bind9 qui nous a demandé plusieurs jours, ce qui aurait pu être réduits à quelques heures si nous avions utilisé l'outil d'échange qu'est Discord plus tôt.

Ensuite pour ce qui est du service mail, le problème ici vient du Docker dont le remplissage n'est pas toujours évident, tant il n'est pas facile de savoir quoi mettre dedans. Pour résoudre ce problème, il n'y a pas de miracle, il faudra faire des recherches plus conséquentes et/ou demander de l'aide sur le Discord.

Le plus gros problème que nous ayons rencontré est au niveau du SOA. On a longtemps été bloqué pour une simple erreur qui était d'ouvrir le port UDP. Cela nous a beaucoup retardé sur les autres éléments du serveur.

Nous avons rencontré un problème au niveau de la base de données en réseau interne. Il fallait refaire un serveur web sur le même VPS que la celui de la base de données afin d'éviter une connexion tierce et avoir un risque de sécurité. Il fallait également ouvrir une connexion dans les SOA interne pour prévenir d'un autre serveur Web.

Nous n'avons pas réussi à obtenir un VoIP fonctionnel bien que les configurations et l'installation soient bonnes. Nous avons eu des soucis pour démarrer le service VoIP et avons réussi à les régler mais trop tard.

Monitoring

Pour gérer notre serveur, nous pouvons utiliser les fichiers de configuration comme « named.conf » pour le DNS. Nous pouvons également utiliser Nagios qui permet de faire du monitoring sur notre VoIP et notre serveur mail.

Bilan

Notre projet lors de sa finalité comporte plusieurs des éléments essentiels. Nous avons un SOA interne et externe fonctionnelles. Nous avons un serveur web interne sans base de données et un serveur externe fonctionnelles. Notre serveur mail fonctionne et possède des certificats. Notre VoIP cependant n'est pas fonctionnelle, ses configurations et son installation sont faites mais nous avons manqué de temps pour le rendre vraiment fonctionnel.