Tom Ozoraï
Anh-Emile Pham
Allan Fontaine

Révision : 27/03/2020
Quadrimestre 2
Etudiant responsable : Allan Fontaine

Rapport Client v2 :

Ps : changements en italique et fluotés !

Contexte

Nous avons été contactés par l'entreprise WoodyToys qui souhaite remplacer ses serveurs qui se font vieillissants. Notre mission sera de conceptualiser une nouvelle infrastructure d'hébergement des services informatiques, *de la tester et de la valider par ensuite*.

Objectif

Cette infrastructure devra répondre aux besoins fictifs de l'entreprise et se présentera sous la forme de différents services qui seront implémentés dans des containers Docker respectifs, ces derniers étant implémentés sur des VPS.
L'infrastructure devra respecter un certain niveau de sécurité tant dans son schéma de fonctionnement (mise en place d'une DMZ,…) que dans l'implémentation des services et la sécurisation des VPS.

Descriptions

Structure de l'entreprise

L'usine comporte un atelier où sont fabriqués les jouets, un hangar de stockage d'où partent les produits vers les revendeurs, le bureau du directeur et les bureaux où travaillent les employés. Parmi ceux-ci, on trouve des comptables, des commerciaux et une secrétaire.
L'usine dispose d'une connexion à Internet. L'atelier, le hangar et le bureau comportent un certain nombre de postes de travail et de téléphones connectés via une infrastructure IP. Un réseau Wifi permet aux employés d'utiliser des appareils portables (laptops et smartphones).

Services informatiques

L'entreprise disposera de plusieurs services informatiques afin de disposer d'une communication interne entre les différents départements de l'entreprise et d'une distribution des ressources informatiques aux départements qui en ont besoin.
Les différents services souhaités sont :

- Un service mail *comprenant des adresses mails pour chacun de ses employés ainsi que des adresses mails génériques qui redirigeront vers des services spécifiques.*
- *Trois services web 1 interne et 2 externes.*
  - *En ce qui concerne le service web interne, il permettra la gestion des stocks, des contacts clients, des commandes et l'organisation de la production. Il s'agit d'un outil ERP uniquement accessible en interne.*

- ❖ *En ce qui concerne les services web externes, il y aura un site vitrine accessible à tous (www.woodytoys.be) qui présente les produits vendus par WoodyToys et un site réservé aux revendeurs (b2b.woodytoys.be) qui est un site de vente en ligne.*

- Deux services DNS *: un service interne permettant la gestion et la communication au sein même de l'entreprise et un service externe permettant l'accessibilité aux ressources demandées depuis l'extérieur.*
- Un service de VOIP *qui doit répondre à plusieurs contraintes expliquées plus bas (cf Contraintes) notamment : être accessible en VoIP depuis internet, avoir une communication interne et externe qui sous-tends les contraintes liées à la fonction des employés (secrétaire, directeur, commerciaux, …), les employés doivent disposer d'une boite vocale.*
- Une base de données interne qui contiendra les données de l'entreprise.
- Dans le cadre de ce projet, il ne nous est pas demandé de gérer la configuration IP mais que les postes puissent disposer d'un accès au réseau interne et externe (mise en place d'un schéma d'adressage). Il est aussi souhaitable d'avoir un contrôle du trafic Web des employés.

Contraintes

- Ventes des produits uniquement en B2B.
- Les postes doivent bénéficier d'un accès aux services internes et externes.
- Adresse mail unique pour chaque employé (nom.prenom@woodytoys.be) et adresses mails génériques permettant de contacter un département en particulier :
  - ❖ contact@woodytoys.be , redirigée vers la secrétaire.
  - ❖ b2b@woodytoys.be , redirigée vers les commerciaux.
- L'entreprise doit être accessible en VoIP depuis internet
- Les employés de l'entreprise doivent pouvoir communiquer entre eux, à l'intérieur de l'entreprise, mais également depuis l'extérieur dans le cas des commerciaux qui sont souvent en déplacement.
  Les communications identifiées sont les suivantes :
  - ❖ **Les ouvriers** : Ils disposent d'un poste de téléphonie IP dans leur atelier et dans le hangar pour joindre les autres départements internes.
  - ❖ **La secrétaire :** Elle dispose d'un PC sur lequel se trouve un softphone, lui permettant de contacter n'importe qui.
  - ❖ **Le service comptable** : Réparti dans deux bureaux, il dispose d'un numéro unique permettant de joindre le premier comptable disponible, ainsi que d'un numéro spécifique par bureau. Les comptables peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur.
  - ❖ **Les commerciaux :** Réunis dans un même bureau, ils peuvent joindre l'extérieur et tout le monde en interne à l'exception du directeur. Ils disposent de smartphones avec lesquels ils peuvent téléphoner en déplacement.

- ❖ **La direction :** Un numéro qui peut joindre tous les autres postes internes ainsi que l'extérieur. Ce numéro ne peut pas être joint directement, les appels devant transiter préalablement par la secrétaire.
- Les employés doivent pouvoir disposer d'une boîte vocale personnelles.

- Lors du rachat d'une entreprise (comme le suppose le cas présenté :
  - ❖ Les deux plans d'adressage doivent être fusionnés en minimisant les changements nécessaires.
  - ❖ Les deux serveurs de téléphonie doivent être configurés pour que les deux sites puissent se contacter en utilisant le nouveau plan d'adressage interne.

Propositions de solutions techniques

- Service de container : Docker, Azure
- Service web: Apache, Nginx
- Service DNS: Bind9, PowerDNS, Posadis, NSD

Choix et justification des solutions

- Pour le service de container, nous avons décidé de choisir Docker car cela faisait partie des contraintes imposées dans le projet et parce que nous l'avons abordé durant le cours d'administration réseau de ce quadrimestre. *Par ailleurs, Docker a prouvé par maintes reprises son efficacités et est un des pionniers dans le domaine de la containerisation. Cela implique d'avoir à disposition une quantité non négligeable de documentations accessible facilement.*
- Pour le service web, nous avons décidé d'utiliser Nginx car celui-ci possède une documentation un peu plus facile à appréhender pour des débutants. *Qui plus est, cela nous permet aussi de nous familiariser avec un nouvel environnement, ayant déjà travailler avec Apache dans le cours d'Admin du premier quadrimestre.*
- Pour les services DNS, nous avons décidé d'utiliser Bind9 parce que c'est un service qui dispose d'une très grande documentation et de tutoriels. *Mais aussi car c'est avec Bind9 que nous avons commencé à apprendre contrairement aux autres qui nous sont complétements inconnus.*

Etat d'avancement

Actuellement plusieurs implémentations ont déjà été faites :

- *Mise en place d'un service Web basique sur un des VPS.*
- *Configuration de tous les VPS.*
- *Mise en place d'un service DNS basique sur un des VPS.*

- *Mise en place de la sécurité de base (Fail2Ban, sudoers, …).*
- *Renseignement sur les différents dispositifs de sécurité mis à disposition.*

La finalisation des autres aspects du projet nous prendra encore certainement une trentaine d'heures.

Maintenance

Actuellement les besoins en maintenance n'ont pas été encore mis en place et ne le seront que plus tard dans le projet une fois l'implémentation de chaque service débuté.

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 délivrable 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 dépassser 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¨.*

Tom Ozoraï
Anh-Emile Pham
Allan Fontaine

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 pôrts, 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.

Schéma Woodytoys

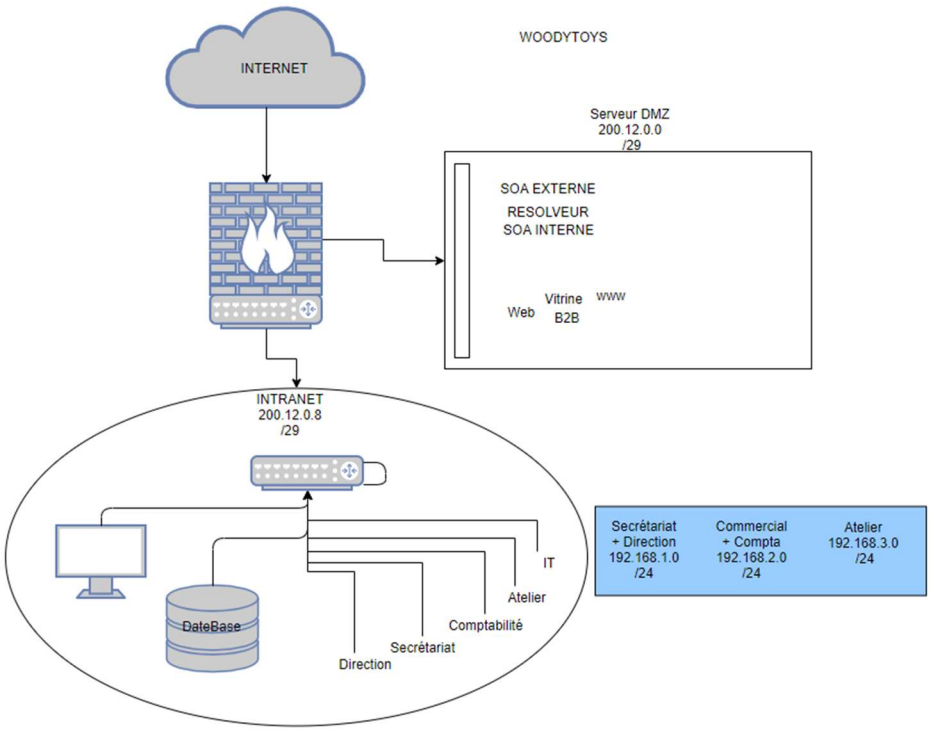


Figure 1 – schéma du réseau de l'entreprise Woodytoys

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 accessible 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.

Schéma Prototype

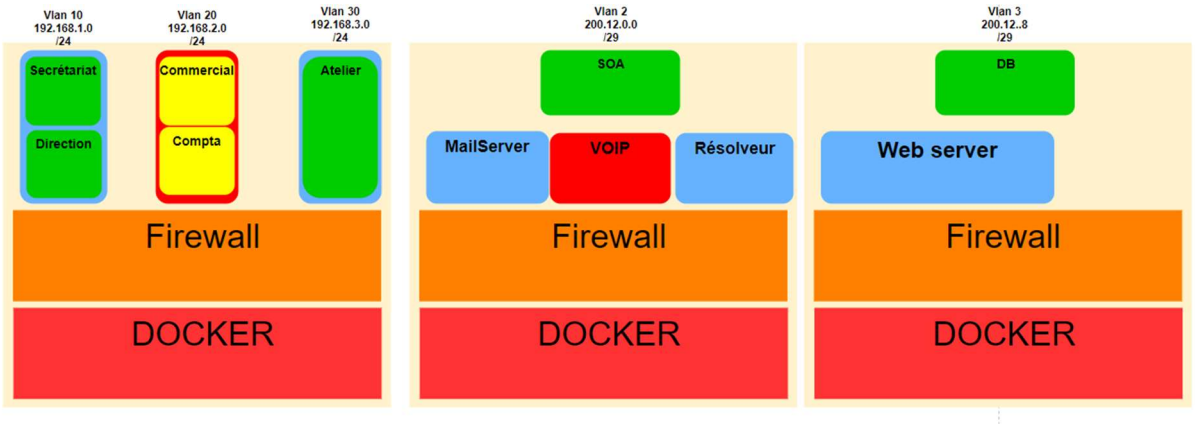


Figure 2 – schéma prototype de la structure réseau de l'entreprise Woodytoys

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.

- Le premier VPS contiendra toutes les VLANS
- Le deuxième VPS contiendra le service Mail, le service VoIP, le service DNS et SOA
- Le troisième VPS contiendra le service web et la base de données.

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/u demander de l'aide sur le Discord.

Monitoring

Nous n'avons pas encore recherché à ce sujet, ce point sera abordé plus tard.

Tom Ozoraï
Anh-Emile Pham
Allan Fontaine

Révision : 27/03/2020
Quadrimestre 2
Etudiant responsable : Allan Fontaine

Bilan

Pour l'instant le projet a pris beaucoup de retard et un investissement plus conséquent en temps devra lui être consacré. Malheureusement dans les circonstances actuelles et avec le second projet qu'est celui de développement Web, nous avons parfois du mal à tenir le cap. Ce qui est dérangeant aussi, c'est que pour vraiment arriver à faire tout le projet dans les temps, il est important de répartir énormément les tâches ce qui ne nous permet pas d'apprendre l'intégralité des services et de leurs mises en place.

Rapport de sécurité V2

Ps : Il n'y avait pas de V1 donc tout est nouveau !

Dans la mise en place de services réseaux, il faut prendre en considération les différents risques encourus par les infrastructures mises en contact avec Internet. Voici les problèmes courants et la résolution mise en place pour lutter contre ceux-ci.

Les VPS et l'infrastructure Docker

Risques

- Attaque en force (Bruteforce) de tout type (par dictionnaire, force pur, …) dans le but de trouver les identifiants de connexion.
- Interceptions des identifiants et des mots de passes si ceux-ci sont faibles ou peu protégés.
- Attaque par le conteneur (pour Docker). Il y a plusieurs failles dans certaines implémentations de conteneurs.

Résolutions

- Installation de Fail2Ban qui permet de limiter le nombre d'essai pour se connecter (avec bannissement temporaire de l'adresse qui essaye de se connecter en cas d'échec répétés.
- Changements des identifiants au départ puis configuration pour une communication en ssh + mise en place de groupe d'utilisateur et d'accès privilégiés, suppression du root user.
- Bonne implémentation des conteneurs et mise-à-jour permanente.

Configurations de base

*est-ce réellement très sécure d'exposer les configs ?

Les différents services déployés

*à diviser par services peut-être ?

Risques

- Attaque de la base de données pour modifier, supprimer, ajouter des données et ainsi corrompre son intégrité.
- Attaque par Phishing (mail frauduleux).
- Deny of Service sur les sites Webs.
- Attaque Man in the Middle : hacking du DNS et trafic passant du coup par un tiers frauduleux.

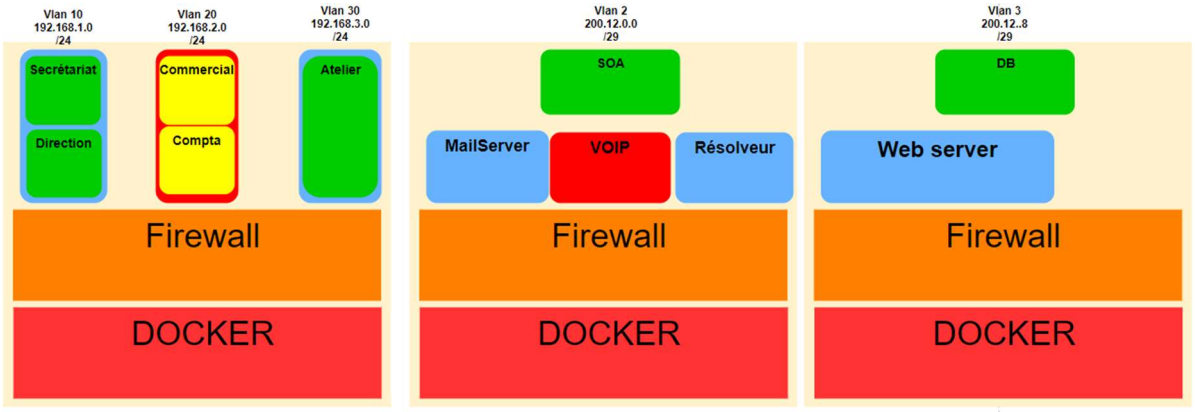
Résolutions

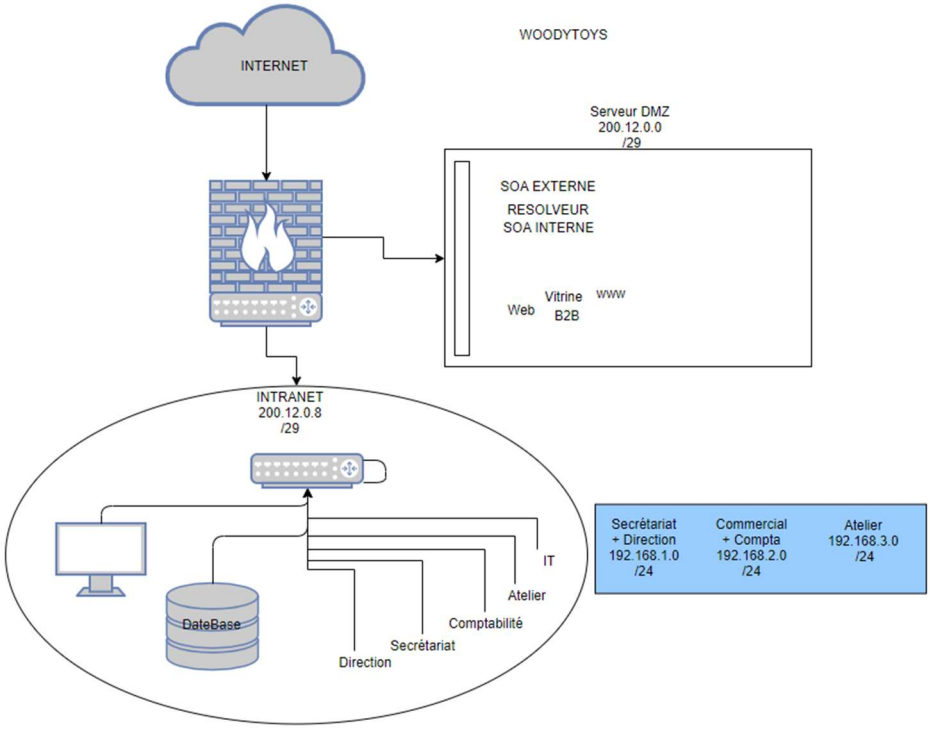
- Mise en place d'une DMZ protégé par un Dual Firewall (protégeant ainsi les services exposés en externe.
- Infrastructure réfléchie pour mettre en externes seulement les services qui ont besoin de l'être, privilégié l'interne.
- Configuration de la base de données pour n'accepter que certaines requêtes.

Configurations de base

A suivre.

SCHEMAS





Modifications apportées

Les modifications apportées sont mises en italique et fluotées en jaune pour bien être visible.
Dans cette deuxième version des rapports nous avons essayés de respecter au mieux les remarques effectués à notre égard sur notre travail. Nous avons aussi essayé de respecter au mieux la grille d'évaluation au possible. Notre but ici est de progressivement nous rapprocher de rapports complets pour ne pas non plus nous surcharger avec de l'administratif là où notre concentration devrait être mises à contribution pour la mise en place des services. Nous avons essayé de tenir compte de toute les remarques faites.