

Groupe 2 :

Crenier Amaury

Castermane Robin

Cotton Victor

Référent :

Van Den Schrieck V.

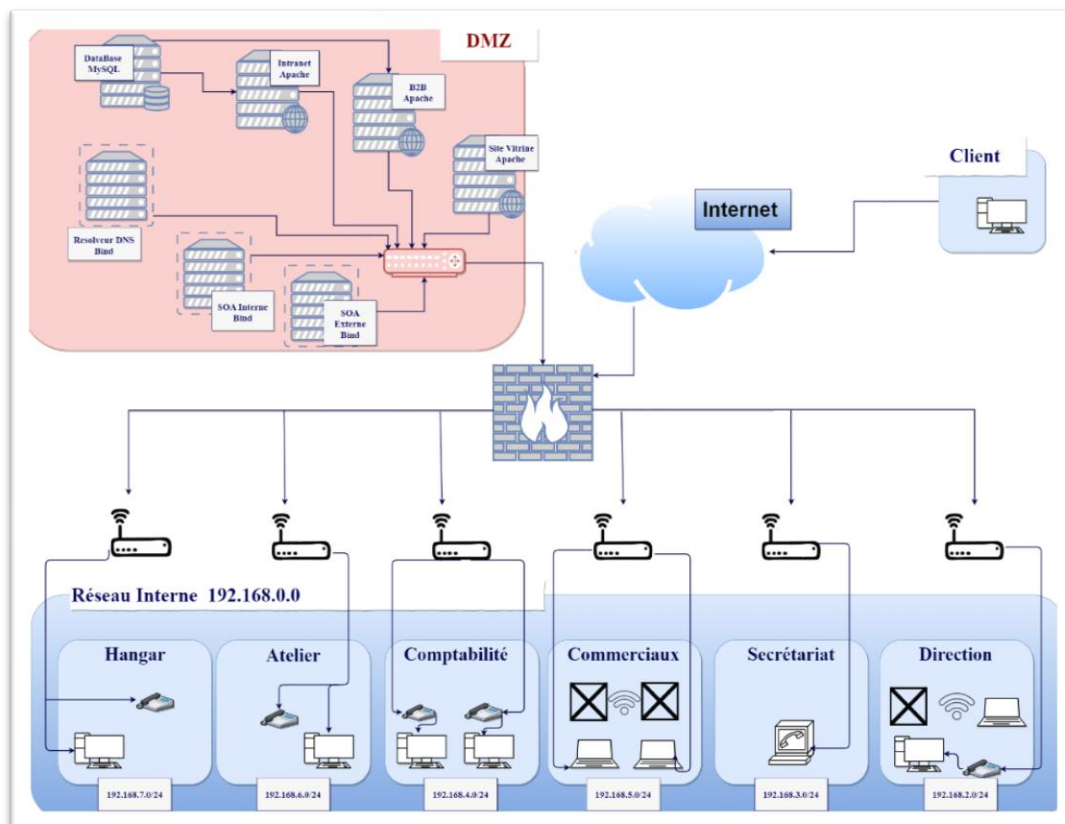
Systeme et réseau

WoodyToys

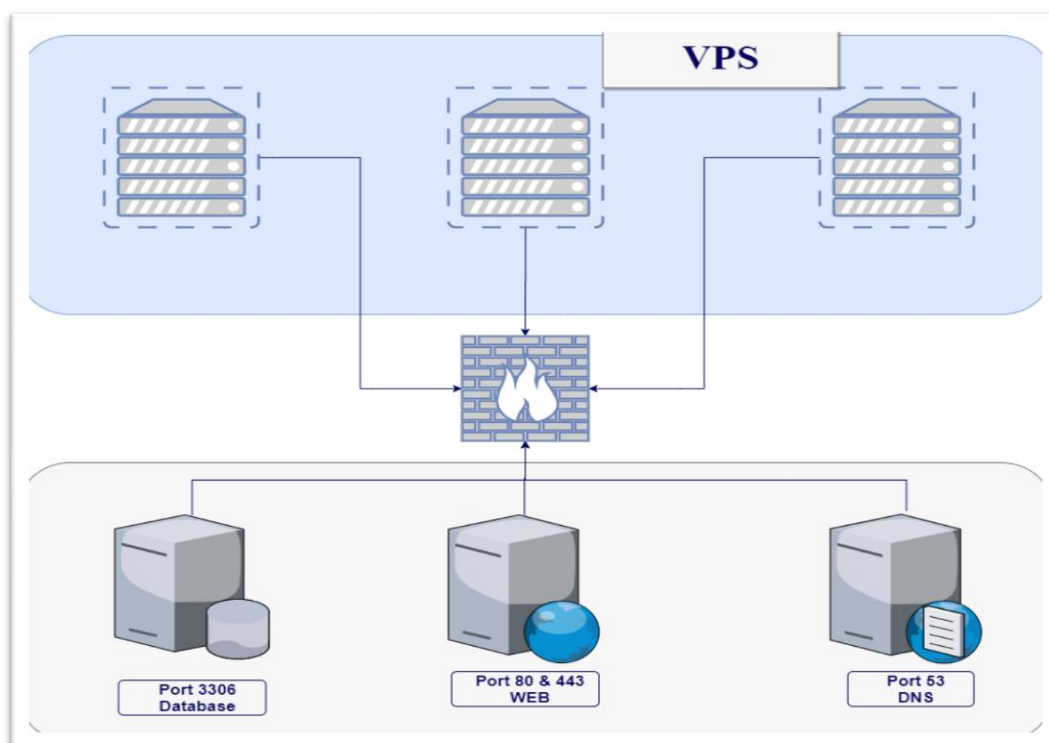
Rapport Mission 2

1. Schéma

1.1 Schéma WoodyToys (update 1)



1.2 Schéma Prototype



1.3 Plan d'adressage

VLAN 1	NATIF	/
VLAN 10	IT	192.168.1.0 /24
VLAN 20	Direction	192.168.2.0 /24
VLAN 30	Secrétariat	192.168.3.0 /24
VLAN 40	Compta	192.168.4.0 /24
VLAN 50	Commerciaux	192.168.5.0 /24
VLAN 60	Atelier	192.168.6.0 /24
VLAN 70	Hangar	192.168.7.0 /24

Nous avons décidé de se baser sur une table d'adressage simple et peu optimisée pour le réseau interne. Ce choix a été fait par question de facilités pour nous et pour l'entreprise. Les différents sous-réseaux laissent la possibilité à l'entreprise de pouvoir s'étendre, vu le nombre d'adresses réservées.

2. Difficulté

2.1 Serveur Web

Nous avons d'abord testé les différentes configurations dans un centenaire Docker pour après les mettre dans un Dockerfile.

Nous avons décidé d'utiliser la mise en place d'un serveur Apache.

2.2 Serveur Base de Donnée

Etant déjà familiariser avec SQL et l'ayant déjà utilisé sur nos différents pcs, cela ne nous a pas posé de problèmes.

2.3 Serveur DNS

Cette partie-là nous a été la plus compliqué. Nous avons créé un Dockerfile ainsi qu'un fichier de configuration. Nous avons créé un Dockerfile pour bind9 ainsi qu'un fichier de configuration. *Pour faire face à ces petits soucis rencontrés, nous nous sommes documentés au mieux sur internet (formation, site d'entraides, ...).*

La suite reste à développer.

3. Bilan

Au terme de cet 2^e mission, nous avons commencé à configurer les dockerfile et mit en place le serveur Apache pour le site vitrine. Cette 1^{ère} partie fût réalisée sans réels soucis mais il reste encore pas mal de travaux.

Groupe 2 :

Crenier Amaury

Castermane Robin

Cotton Victor

Référent :

Van Den Schrieck V.

Systeme et réseau

WoodyToys

Rapport sécurité

1. Sécuriser un VPS

Lorsque vous commandez votre VPS, aucun protocole de sécurité n'est implémenté nativement. Voici donc quelque commande/pratique à effectuer avant de mettre nos services respectifs en place sur ceux-ci.

Premièrement accédez à votre VPS en tant que root (connexion SSH nécessaire). Celle-ci permettant de sécuriser l'accès au VPS.

Pour des raisons de sécurité vous allez ensuite mettre à jour le système en 2 étapes :

- apt-get update
- apt-get upgrade

Après cela la modification du numéro de port peut être changé, étant donné que les tentatives de piratages cible par défaut le port 22, il pourrait être plus judicieux de le changer.

Une autre étape importante est de créer un utilisateur avec des droits restreints. L'accès direct au root lors de la connexion au VPS n'est pas recommandé en cas de mauvaise manipulation, certaines pourraient être irréversibles.

- adduser nomUtilisateur

Par la suite vous pouvez donc désactiver l'accès au VPS pour l'utilisateur « root ».

En dernier lieu, afin de prévenir contre certaines instructions comme bloquer les adresses IP inconnues tentant de rentrer dans le système, l'installation/configuration de Fail2Ban est nécessaire.

2. Serveur DNS

Utilisation de DNSsec ainsi que l'utilisation d'un serveur proxy. Celui-ci vérifiera la validité des échanges. Il aura donc un rôle de filtre et de serveur cash.

3. Serveur Web

Utilisation du protocole HTTPS port 443 (prochainement).

4. Serveur Base de Donnée

La création d'un login et d'un mot de passe prochainement pour limiter l'accès.

5. Infrastructure du client

Nous utilisons un Firewall qui se trouvera au cœur du schéma réseau, celui-ci filtrera les échanges avec le monde extérieur et pourra donc filtrer les menaces.

Exemple de différentes utilisations qui seront protégés :

- Infiltration à la boîte mail
- Accès à la base de données
- Sécuriser les serveurs

Source :

<https://docs.ovh.com/fr/vps/conseils-securisation-vps/>

Groupe 2 :

Crenier Amaury

Castermane Robin

Cotton Victor

Référent :

Van Den Schrieck V.

Systeme et réseau

WoodyToys

Rapport client

1. Cahier des charges :

WoodyToys, fabricant de jouets en bois de manière artisanale souhaite remplacer ses vieux serveurs pour mettre en place une nouvelle infrastructure d'hébergement de ses services informatiques.

L'infrastructure déployée doit permettre la mise en place de 3 sites web :

- Un site web vitrine (www.woodytoys.be).
- Un site web b2b permettant un système de commandes (b2b.woodytoys.be).
- Un site intranet (intranet.woodytoys.be).

Un service mail doit être mis en place afin de communiquer au sein de l'entreprise et avec l'extérieur. Il y a d'une part les adresses mail des employés (nom.prenom@woodytoys.be) et d'autre part des adresses génériques pour différents services (contact@woodytoys.be, b2b@woodytoys.be, ...).

Il faut mettre en place un service de téléphonie IP pour que :

- L'entreprise soit accessible depuis internet par appel via l'adresse contact@woodytoys.be qui est dirigée vers le poste de la secrétaire.
- Les employés communiquent entre eux à l'intérieur et à l'extérieur de l'entreprise.
- Les employés puissent disposer d'une boîte vocale.
- La fusion avec le réseau téléphonique d'une entreprise en cours de rachat soit possible.

2. Besoins techniques :

Mise en place de serveurs permettant le déploiement des différents services :

- Un serveur Web contenant les fichiers relatifs aux différents sites web (html, css, ...).
- Un serveur pour la base de données permettant les commandes (php, mysql).
- Un serveur DNS pour accéder aux noms de domaine.
- Utilisation de serveur SMTP, POP ou IMAP pour le service mail.

3. Solutions techniques :

3.1. Serveur Web :

Mise en place d'un serveur Apache qui est gratuit, fiable et facile à configurer. Les fichiers de configuration utilisent ASCII ce qui les rend plus simple à administrer car n'importe quel éditeur de texte permet d'éditer les fichiers. Il est extensible et stable. De plus, il est OS indépendant et peut donc aussi bien fonctionner sur Unix que sur Windows.

Une autre solution est Nginx qui est plus performant pour les sites statiques mais qui est égal lorsque l'on se dirige vers du dynamique (benchmark de 2015 <http://www.speedemy.com/apache-vs-nginx-2015/>). Une grosse différence est la gestion des modules qui est dynamique pour Apache alors que pour Nginx, ils doivent être sélectionnés et compilés dans le logiciel de base.

3.2. Serveur DNS :

Utilisation de Bind9 qui est très utilisé et facilement configurable.

3.3. Serveur de base de données :

MySQL est très répandu et nous connaissons déjà ce type de base de données.

Sources :

<https://www.supinfo.com/articles/single/5509-apache-vs-nginx>

GROUPE 2 – 2TL2

Résumé des changements effectués suite au feedback

Rapport Sécurité :

- Ajout des sources à la fin du document
- Reformulation/structuration des phrases sur la partie « sécurité VPS »
- Ajout d'une information pour la base de données (qui sera appliqué prochainement)

Rapport technique :

- Ajout du responsable de la mission ainsi que son bilan
- Modification du schéma WoodyToys (ajout des différents sous-réseaux, modification entre la zone DMZ et Pare-Feu)
- Ajout de l'explication du plan d'adressage
- Ajout résolution face aux problèmes rencontrés

Rapport client :

- Modifications des fautes de frappes
- Ajout de sources pour les solutions