Haute Ecole Economique et Technique

Administration Système et Réseaux II

Rapport client

Groupe 2TL1-3

Romain Berger & Maxime De Cock

Cahier des charges

L'entreprise WoodyToys nous a demandé de mettre en place 3 sites web :

- Un site « principale » présentant l'entreprise aux internautes (Ce site sera statique)
- Un site web dynamique b2b se référant à une base de donnée contenant tous les produits de l'entreprise WoodyToys vendu en magasin. Il permettra au revendeur de passer des commandes.
- Enfin, nous devrons créer un intranet disponible uniquement aux employés du magasin.

Un service mail permettant à l'entreprise d'avoir un image plus professionnelle sera mis en marche :
Chaque employé disposera de son adresse e-mail personnelle sous la forme nom.prénom@<domaine>. Ils pourront dès alors communiquer entre eux ou avec des adresses mail extérieures. Les responsables des services (b2b, contact client, …) disposeront quant à eux d'adresses mail génériques.

Et pour finir, afin d'améliorer la communication au sein de l'entreprise, nous déploierons service téléphonique sur ip (VoIP) :
Les ouvriers travaillant à l'atelier, pourront joindre les autres département internes
Les commerciaux pourront appeler tout le monde aussi bien en interne qu'en externe (sauf le directeur).
La secrétaire et le directeur pourront joindre tous les postes de l'entreprise, et seule la secrétaire aura la capacité de joindre le directeur, elle se chargera donc de transférer les appels.
Chaque département aura une boîte vocale.

Contraintes techniques

Il faut prendre en compte le fait que l'entreprise puisse fusionner avec une autre branche

Solutions techniques

Serveur DNS

Nous avons choisis d'utiliser Bind pour la réalisation de ce projet, en premier lieu car c'est l'un des serveur les plus utilisé dans le monde, ayant une vaste communauté nous trouverons plus de forum et recevront facilement de l'aide en cas de besoin, il y a aussi un large panel de tuto permettant de bien commencer avec bind. En second lieu, le langage est openSource et possède des fonctionnalités qui nous seront utiles, tel que la récursivité (pour les requêtes vers internet) et l'autorité, permettant de mettre en place un système de serveur esclave (convient mieux aux utilisations sur un serveur interne).

Serveur WEB

Pour le serveur web nous avons utilisé apache, un logiciel libre connu pour sa popularité et sa flexibilité.
Ce dernier nous permet de créer 3 redirections :

- *www.wt1-3.ephec-ti.be -> Site grand public*
- *b2b.wt1-3.ephec-ti.be -> Site pour les professionels*
- *intranet.wt1-3.ephec-ti.be -> Intranet*

Une première version de test est en HTTP.
Une seconde version est prévue avec une redirection forcé avec l'utilisation de HTTPS afin de sécuriser un maximum les connexions et transactions du site.

Serveur Mail

Nous ne sommes pas encore complètement sûr, mais nous allons probablement utilisé le protocole IMAP pour la réception des messages, il sera mieux que POP3 car il permet de stocker les messages sur le serveur et il possède une méthode de synchronisation fixe qui permet d'avoir la même organisation sur un poste mobile qu'un poste fixe, cela sera utile pour les déplacements des différents cadres de l'entreprise. Pour l'envoi SMTP, car il n'en existe pas d'autre.

Ce qui est actuellement fonctionnel

- *Le DNS est fonctionnel et configurable*
- *Le serveur WEB et la redirection des pages avec accès interne/externe est fonctionnel*
- *Le serveur VOIP est configuré mais non-fonctionnel (les tests ne sont pas encore suffisant pour statuer la finalité de ce dernier)*
- *Le serveur MAIL est en cours de tests*

Haute Ecole Economique et Technique

Administration Système et Réseaux II

Rapport technique

Informations du groupe

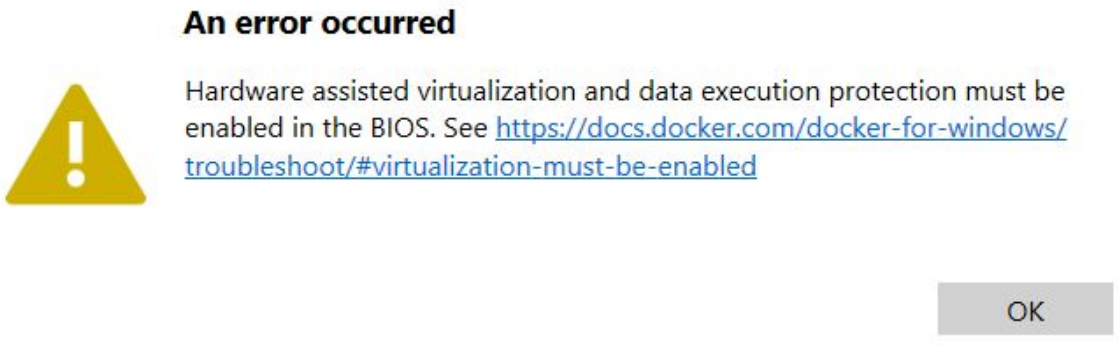
Numéro: 2TL1-3
Membres: Romain Berger & Maxime De Cock
Étudiant responsable de la mission 1 (DNS et Web) : *Romain Berger*
Étudiant responsable de la mission 2 (Mail) : *Maxime De Cock*
Étudiant responsable de la mission 3 (VoIP) : *Romain Berger & Maxime De Cock*

Bilan de la mission 1

Cette mission n'a malheureusement pas beaucoup avancée dû à la non disponibilité des VPS qui nous restreint énormément.
Nous avons cependant effectué certaines recherches au préalable afin de pouvoir, nous l'espérons, rattraper ce retard.
Nous avons dès le premier cours où les groupes ont été formés fait des recherches concernant DockerHub, son installation et son utilisation en pratique.
Nous sommes déjà prêt pour la mise en place des connexions SSH sécurisés et l'installation du serveur web.

Bilan de la mission 2

Durant cette mission, nous avons mis en place Docker et commencé la créations de nos Dockerfile DNS ainsi que Web.
Nous avons choisi d'utiliser Docker Desktop mais ce dernier nous à poser pas mal de soucis lors de son installation (De son coté, Maxime n'a pas réussi à l'installer sur son ordinateur personnel et à donc dû opter pour une installation sur son portable.



Message lors de l'installation nous signalant que la virtualisation n'était pas activé sur mon BIOS

Heureusement, en cherchant un peu il était possible d'activer manuellement la virtualisation du PCU en allant directement dans les options avancés du BIOS.

Suite à ça, nous nous sommes attelé à la création des dockerfile et autres fichiers de configurations du DNS et du WEB, ces derniers seront prêt pour la prochain mission.

Concernant le DNS, nous avons :

- Un fichier de zone local
- Un fichier de zone publique
- Une configuration forwarder
- Une configuration master
- Une ACL

```
$ORIGIN wt1-3.ephec-ti.be.
$TTL    3600
@                               IN      SOA   ns.wt1-3.ephec-ti.be. HE201639@students.ephec.be. (
          2001062501      ; Serial
                3600      ; Refresh après 1 heure
                 600      ; Retry après 10 minutes
               86400      ; Expire après 1 jour
               86400 )  ; TTL minimum de 1 jour

                           IN      NS    ns.wt1-3.ephec-ti.be.

                                 IN      A     51.178.40.161

wt1-3.ephec-ti.be.            IN      NS    ns.wt1-3.ephec-ti.be.

ns.wt1-3.ephec-ti.be.         IN      A     51.178.40.161
www.wt1-3.ephec-ti.be.        IN      A     51.178.40.161
b2b.wt1-3.ephec-ti.be.        IN      A     51.178.40.161
intranet.wt1-3.ephec-ti.be.   IN      A     51.178.40.161
```

Fichier de zone publique

Nous avons aussi modifié les délais de rafraîchissement ainsi que d'expiration afin de mieux correspondre à nos besoins.

Bilan de la mission 3

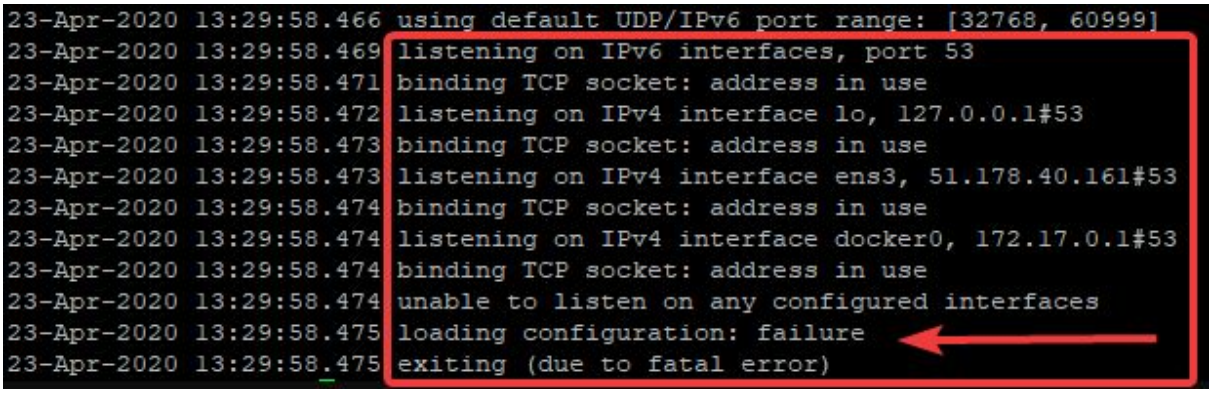
DNS

Cette mission fut assez lourde en recherches et en tests.
En effet, après avoir tenté de déployer notre DNS via docker, nous avons directement remarqué que ce dernier ne semblait pas fonctionner correctement.

Suite à plusieurs recherches et quelques discussions avec d'autres étudiants, nous nous sommes rendu comptes d'avoir oublié un détail important : Nous n'avions pas fournit le Glue Record au DNS de l'hébergeur.

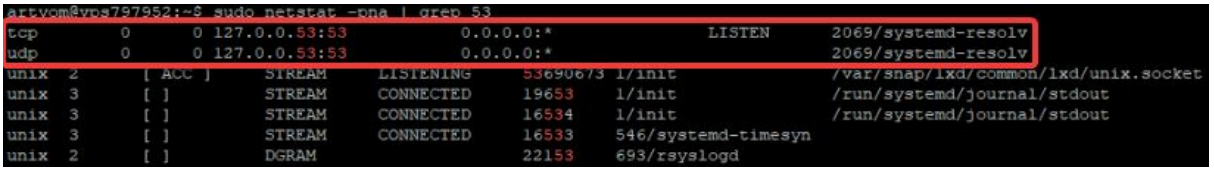
Une fois cela fait, nous pensions que cela allait résoudre notre problème mais hélas nous n'arrivions toujours pas à résoudre nos nom de domaines.
Nous avons donc essayé plusieurs configs différentes, changer nos fichiers DB, etc… mais nous ne faisions que rajouter des problèmes ou d'en résoudre à moitié.

Nous nous sommes donc penché sur une autre source potentiel du problème : Les ports. Suite à la lecture des logs dockers, nous avons constaté que notre DNS ne pouvait pas se lancer car impossible pour lui de se lier à une interface.



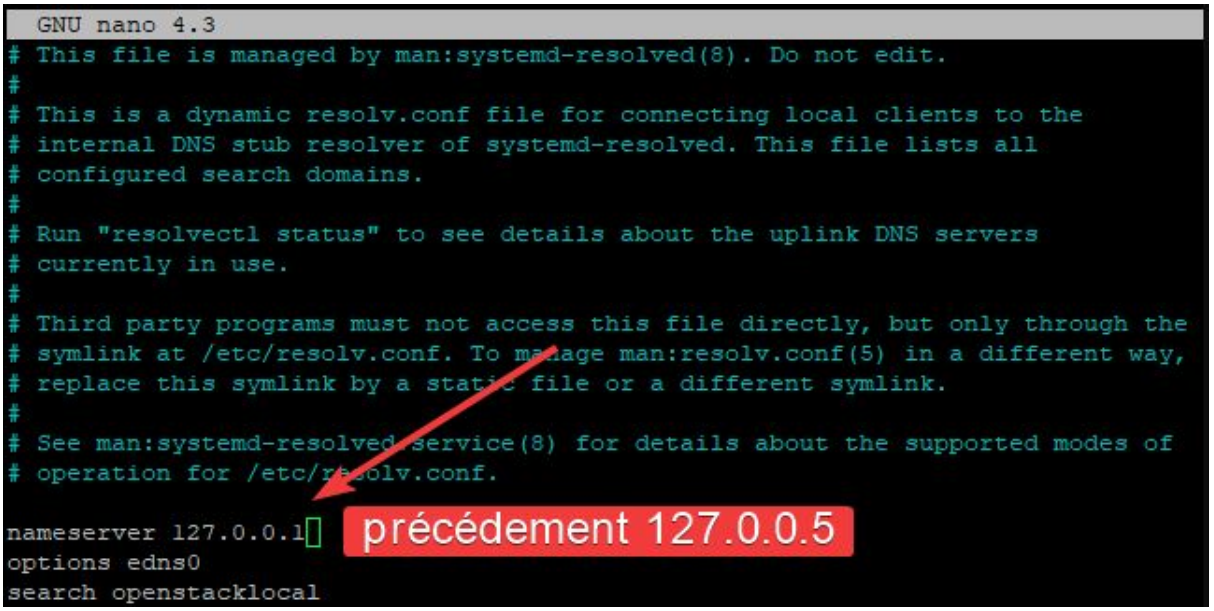
Les logs du container nous ont bien fait comprendre que les ports étaient une source du problème

Suite à ça, nous avons découvert que notre container DNS était configuré pour se lié au port 53 du VPS. Cependant, le port 53 fut déjà utilisé par le résolveur par défaut de ce dernier.



Le container tentait de se lier à un port déjà utiliser par défaut par systemd-resolv

Après plusieurs modification dans la configuration du vps, nous sommes arrivé à résoudre le problème et notre container DNS fut enfin fonctionnel.
Il suffisait de modifier le nameserver afin de permettre à notre DNS de prendre le pas sur le resolver par défaut



Il nous a suffit de changer 127.0.0.53 en 127.0.0.1 pour “promouvoir” notre DNS

Web

Suite à cela, nous avons testé notre container WEB et ce dernier, contre toute attente suite au retard pris avec le DNS, a fonctionné du premier coup !
Ce qui permet à n'importe qui à l'heure actuelle d'accéder à

- *www.wt1-3.ephec-ti.be -> Site grand public*
- *b2b.wt1-3.ephec-ti.be -> Site pour les professionels*
- *intranet.wt1-3.ephec-ti.be -> Intranet (uniquement accessible via whitelist)*

Mail

La configuration est quasiment terminée et les tests devraient suivre dans les jours qui viennent.

VoIP

Pour le VoIP, nous avons réussi à lancer le container non sans plusieurs tentatives et plusieurs modifications (notamment la version qui semblait poser problème).
Cependant un problème persiste au niveau des users qui ne se "chargent" pas et la connectivité bancale mais nous travaillons dessus.

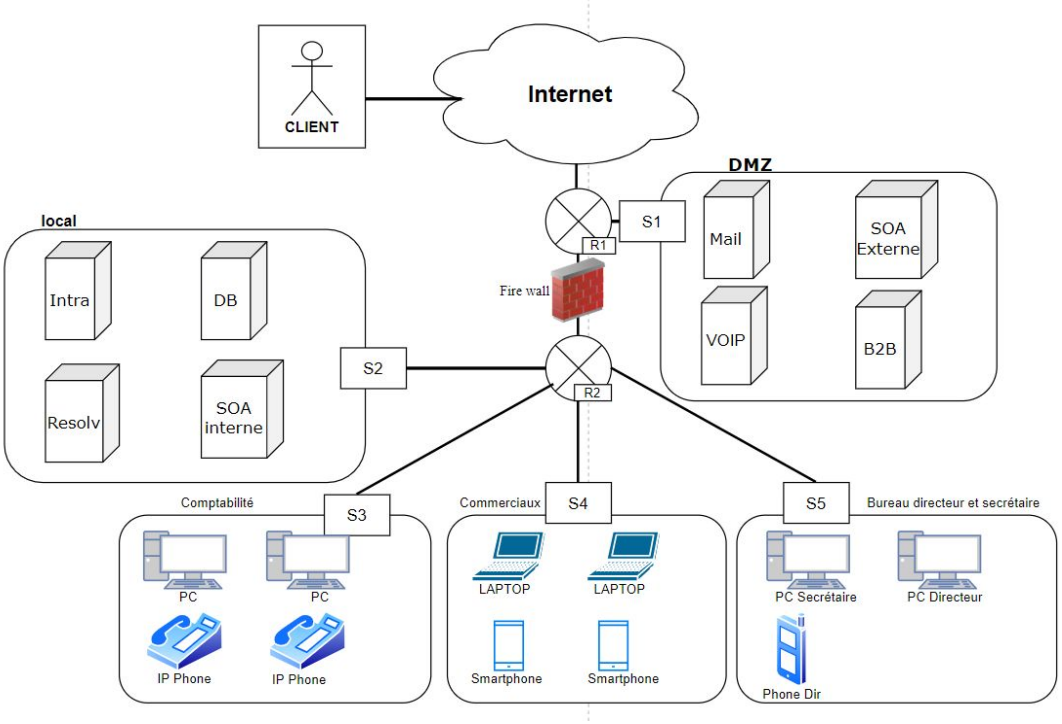
Plan d'adressage et ports

Nous avons déjà déterminé les différents ports qui seront utilisés :

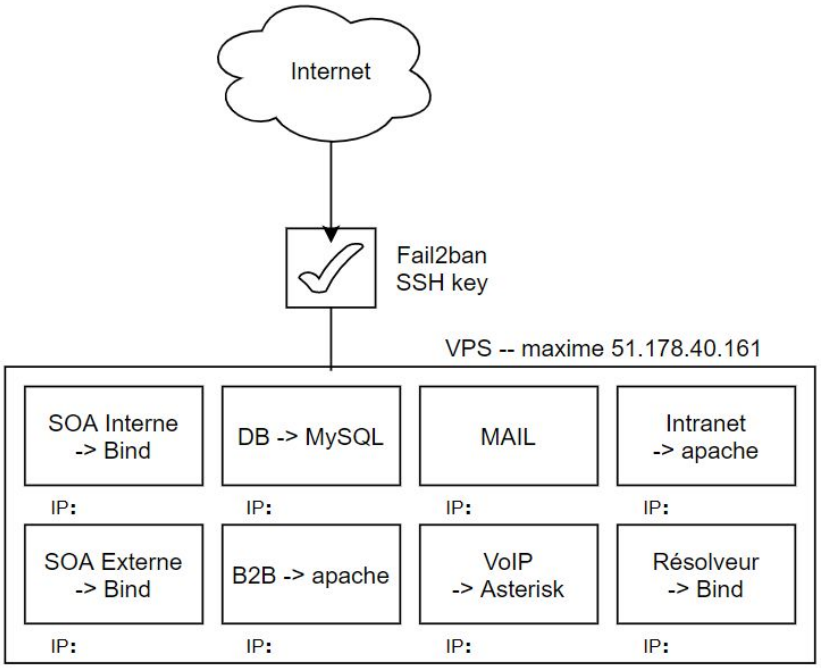
- SSH : Port 22 (par défaut, pourra changer selon les mesures de sécurités)
- DNS : Port 53
- http : 80
- https : 443
- VoIP : 5060

Schémas réseaux

Logique



Prototype



Haute Ecole Economique et Technique

Administration Système et Réseaux II

Rapport de sécurité

Risque(s) encouru(s) par le VPS

Les VPS d'OVH à notre (future) disposition ne seront protégés que par un simple mot de passe facilement crackable.
Il nous revient la responsabilité de les sécuriser rapidement afin de ne pas en perdre le contrôle, ce qui serait vraiment fâcheux.

Une fois la connexion sécurisée établie, nous n'aurons plus qu'à filtrer les tentatives d'accès avec Fail2Ban et notre VPS sera isolé de toute menace primaires.

Contres-Mesures mises en places

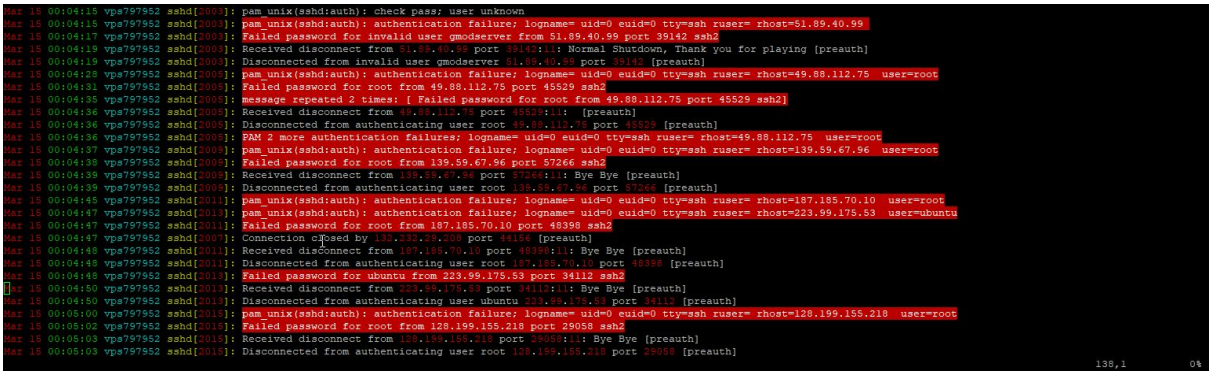
Utilisateurs et SSH

Avant tout chose, nous avons créé les différents users à savoir :

- artyom (Romain Berger)
- maxime (Maxime De Cock)
- vvandens

Ensuite nous avons généré les différentes clés publiques et privées et nous avons assigné la clé publique de chaque utilisateur dans son fichier **authorized_keys**.
Nous avons utilisé la norme de cryptage SSH-2 RSA avec une longueur de 2048 bits pour la génération des clés.

Une fois cela fait et la connection via tunnel sécurisé fonctionnel, nous avons désactivé l'authentification au root ainsi qu'aux utilisateurs via mot de passe.
Nous avons également changé le port SSH.
Malgré que certains articles et témoignages mentionnent l'inutilité de le changer* nous l'avons tout de même fait car c'est toujours mieux d'avoir des logs de connexion "propres" de toutes tentatives futiles.



*https://www.adayinthelifeof.nl/2012/03/12/why-putting-ssh-on-another-port-than-22-is-bad-idea/

Fail2Ban

Nous avons mis en place Fail2Ban avec une configuration assez simpliste :

```
[DEFAULT]
ignoreip = 127.0.0.1
findtime = 3600
bantime = 86400
maxretry = 3

[sshd]
enabled = true
port = 457
```

```
artyom@vps797952:/etc/fail2ban/jail.d$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

Vérification de la configuration de fail2ban

LogRotate

Nous avons également mis en place logrotate qui permet l'archivage automatique des logs afin de limiter l'espace mémoire utilisé par les logs.
Voici un exemple avec fail2ban :

```
/var/log/fail2ban.log {
    weekly
    size 100M
    rotate 2
    compress
    delaycompress
    missingok
    postrotate
        fail2ban-client flushlogs 1>/dev/null
    endscript
}
```

Modification du port d'écoute SSH

Suite à plusieurs recherches sur le sujet, nous avions pris l'initiative de changer le port d'écoute par défaut du service SSH afin de bloquer une grosse partie des tentatives d'intrusions via ce dernier.

Cependant, après discussion avec le professeur, nous avons conclu que l'intérêt de ce changement n'était pas nécessaire et pourrait entrer en conflit avec les méthodes d'évaluation du projet.

Contre-mesure(s) prévue(s)

- *Utilisation d'un Certificat SSL en tant que protocoles de sécurisation des échanges sur Internet. (principalement pour les transactions et les connexions)*