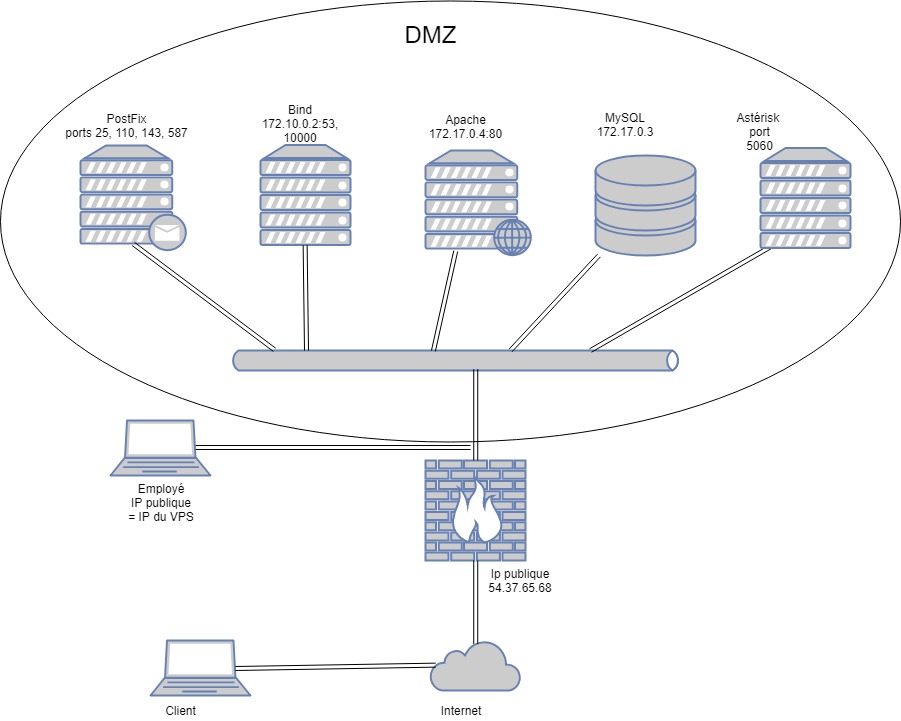
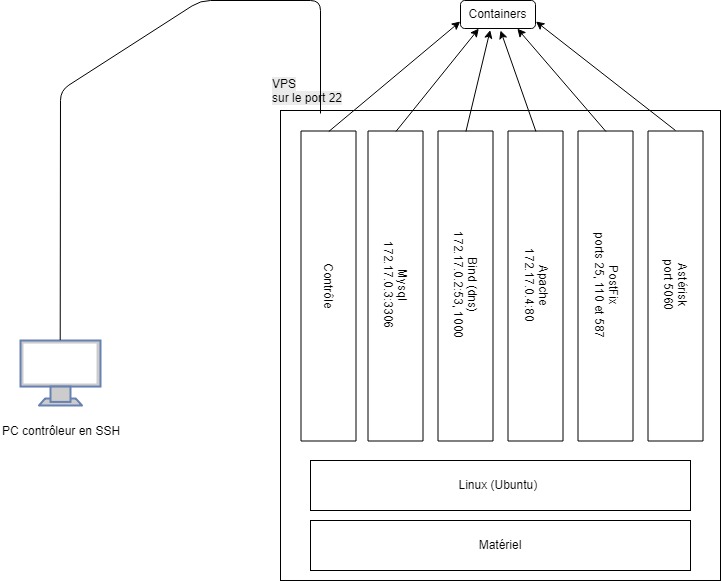
Groupe 12 (Cornil Jean, Feyereisen Thomas, Lapière Nicolas) 30 mai 2018

# Rapport technique final du projet d’administration systèmes et réseau

## Schéma réseau logique



## Schéma réseau physique



## Difficultés rencontrées

### DNS

Nous avons eu quelques difficultés quant à la mise en place du DNS. En effet, notre fichier de zone a dû être modifiée à de multiples reprises, jusqu’à avoir un fichier de zone qui fonctionne. Nous accédons sans difficultés à nos pages web et les requêtes sur la base de données se font de manière fonctionnelle. A l’heure actuelle, notre container servant au DNS de nos sites web est parfaitement fonctionnel, la translation de nom de domaine se fait sans problèmes.

### Mail

Ensuite, au niveau du début de la partie mail du projet, nous avons eu un souci lors du lancement du container mail avec Postfix. En effet, nous avons un problème qui est toujours d’actualité avec Docker, certaines commandes que nous avions toujours utilisées jusqu’à présent ne fonctionnent plus dû certainement à la mise en place du container mail, qui a aussi provoqué un crash de tous les autres containers de manière inexpliquée. Après avoir fouillé un peu dans le VPS afin de trouver une solution, nous avons réussi à récupérer les commandes que nous voulions et nous avons repris notre travail et nous avons installé le container Postfix. Notre configuration des utilisateurs nous a aussi posé quelque « bêtes » soucis, lors de l’identification de l’utilisateur sur le serveur SMTP. Nous avions mis le mot de passe entre crochet, car nous pensions que la syntaxe l’obligeait, mais du coup l’authentification ne fonctionnait pas. Après avoir trouvé cette erreur, nous avons pu finaliser notre installation d’une infrastructure mail.

### Web

Au niveau web nous avons amélioré notre infrastructure par la mise en place d’un seul container Apache au lieu de trois à la base. Nous avons implémenté le Virtual Hosting de nos sites web sur ce container afin de simplifier la réalisation du DNS. Nous avons donc trois sites web hébergés sur notre container Apache. Nous avons donc supprimé les anciens containers qu’on utilisait via le numéro de port. Au début de l’installation de phase d’installation d’un service Web, nous voulions utiliser Ngnix comme serveur web. Cependant, nous devions communiquer entre une base de données installée préalablement et notre page Web b2b à l’aide d’un code en PHP qui s’y connectait. Ngnix ne pouvait pas interpréter nativement le PHP et nous devions donc l’implémenter dans notre configuration. Après de multiples tentatives non fructueuses nous avons trouvé un Dockerfile sur internet qui utilisait l’image Apache où PHP était intégré dedans. Nous avons donc utilisé ce DockerFile qui a bien marché du premier coup pour la connexion à la base de données.

### VOIP

Nous avons à l’heure actuelle réussi à implémenter une solution de VOIP sur notre VPS commun. En effet, nous avons installé un container Astérisk à côté de nos précédents containers. Nous avons choisi la solution Astérisk car c’est celle que nous avons le plus développé en cours et aussi car il s’agit d’un des services des plus répandus. Nous avons trouvé pas mal de tutoriaux sur Internet sur son utilisation et son installation sur une machine Linux. Au départ nous voulions installer un container Ubuntu pour ensuite y insérer Astérisk dessus, mais à notre grande surprise nous n’y sommes pas parvenus. En effet, nous avons tenté d’installer de multiples images Ubuntu (de la version 14.04 à 18.04 ou Debian), mais jamais avec succès. Le problème ne vient certainement pas de la machine sur laquelle nous travaillons car l’installation d’autre containers de test tels que Bind ou Apache a fonctionné. Nous avons donc décidé de nous tourner vers une utilisation d’un Dockerfile, ce qui a marché du premier coup sans erreurs ni obstacles. Notre système de VOIP fonctionne sans problèmes en interne, nous recevons les appels des personnes se trouvant sur le même domaine (sur la même adresse IP que le VPS) que nous et nous pouvons émettre des appels. Nous n’avons pas implémenté une solution de communication sur IP vers l’extérieur, nous manquions de temps et ne voulions pas nous précipiter pour régler ce point et risquer que la configuration ne fonctionne plus.

## Technique de sécurisation

La sécurisation du VPS hébergeant notre infrastructure est terminée. Nous n’avons pas spécialement travaillé pour l’instant la sécurité de l’intranet, ou la restriction d’accès à la base de données car nous préférons nous concentrer sur la mise en place de l’infrastructure pour l’instant. La base de données que nous utilisons est protégée car une seul adresse IP peut y avoir accès. Nous avons configuré ça directement à l’intérieur de la base de données en créant un nouvel utilisateur sur base de l’adresse IP. Nous n’avons pas installé Fail2Ban pour protéger notre VOIP, ce qui pourrait poser un problème au niveau de la sécurité.

## Validation de la solution

Nous pouvons valider notre solution d’infrastructure réseau pour l’instant. Nous avons effectué des tests des pages web localement à la base avant de les publier sur le serveur et la résolution des noms vers les IP fonctionne (test via les noms de domaines wt12.ephec-ti.be). L’intranet demandé par le client n’est pas totalement fini. En effet, l’accès peut toujours de faire depuis n’importe quel pc, et ce de manière non sécurisée. Nous comptons utiliser un container simulant un système d’exploitation linux qui aurait une adresse IP privée interne au VPS, et que nous utiliserions pour construire une liste d’accès dans le DNS. Ceci permettra de limiter l’accès à la page Intranet aux IP internes au VPS. Au niveau du serveur mail nous pouvons valider notre solution en utilisant les adresses mails qui s’y retrouve afin de se connecter et d’avoir la possibilité de communiquer par mail depuis l’une de ces adresses, mais également vers l’une de ces adresses. Nous pensons que la solution que nous proposons et que nous développons est conforme aux exigences du client. Les tests sur les éléments demandés se font sans problèmes.

Voici la liste des tests à effectuer pour valider notre solution :

* Accéder aux pages web b2b et page statique depuis n’importe où ;
* Accéder à la page Intranet depuis l’intérieur du VPS ;
* Accéder à la base de données uniquement depuis la page b2b (si nous programmons une page PHP avec un PDO depuis un autre site que le b2b, cela ne doit pas fonctionner) ;
* Tester la translation de nos noms de domaines et rediriger les noms vers les pages web correspondantes ;
* Envoyer et recevoir des mails simples depuis les adresses créées sur le container MAIL en envoyant des messages entre personne de l’entreprise mais aussi depuis l’extérieur, et en testant en ajoutant des fichiers à transmettre ;
* Tester la VOIP et la boite vocale de celle-ci ;
* Tester la VOIP entre les différents groupes pour tester la communication extérieure ;