Rapport technique final

# Schéma physique

De point de vue physique, nous avons structuré dans un premier temps les containers d’une façon simple. C’est-à-dire, un VPS héberge les parties DNS et VOIP, tandis que le second héberge les parties web, donc l’Intranet, le site vitrine et le site interactif. Cela est réalisé grâce au VirtualHosting. Il suffit donc de de rechercher "wt2.ephec-ti.be" pour trouver le site vitrine, "b2b.wt2.ephec-ti.be" pour avoir le site b2b et l'intranet (visible seulement depuis l’intérieur de l'entreprise) est accessible via "intranet.wt2.ephec-ti.be". C’est sur le second VPS que la communication avec la DB est également faite. Le troisième VPS héberge le serveur mail.

VPS517674

IP : 54.37.65.110 :80

Site interactif  
URL : b2b.wt2.ephec-ti.be  
IP : 172.17.0.6

Site vitrine  
URL : wt2.ephec-ti.be  
IP : 172.17.0.6

Intranet  
URL : intranet.wt2.ephec-ti.be  
IP : 172.17.0.6

Database  
IP : 172.17.0.3

IP : 54.37.65.110 :3306

VPS517640

DNS inverse

DNS  
IP : 172.17.0.2  
Port : 10000

IP : 54.37.65.43

VoIP  
IP : 172.17.0.3  
Port : 5060

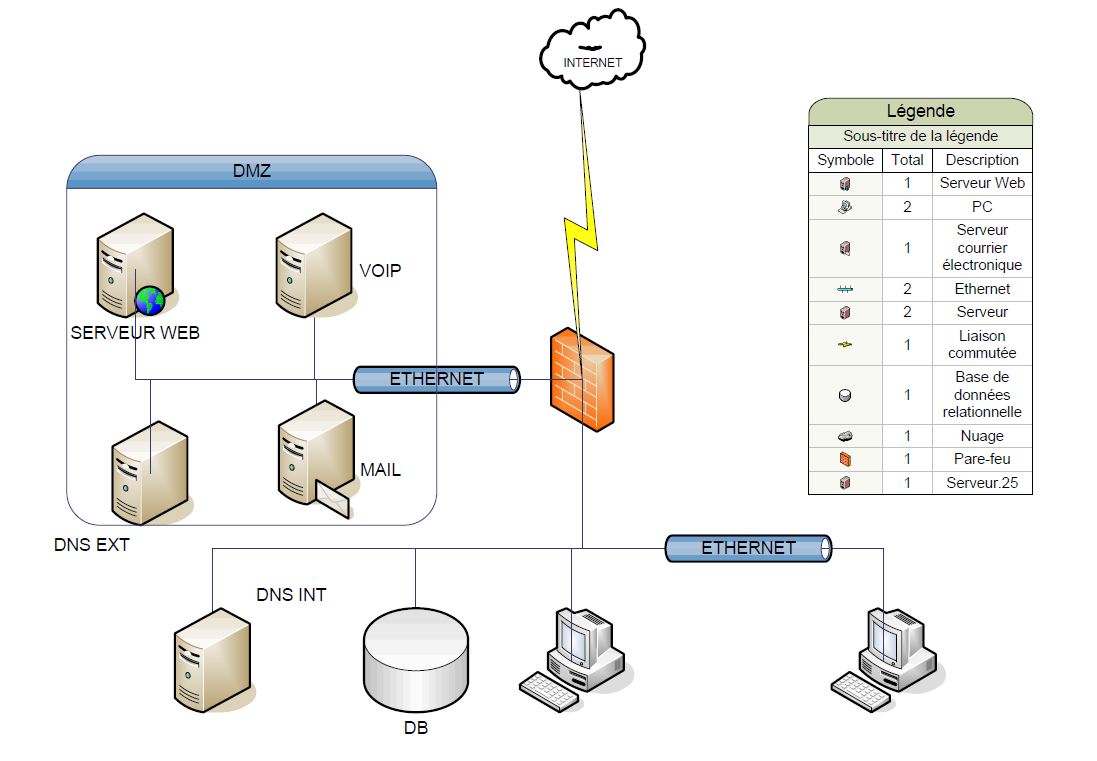
VPS517664

Mail  
IP : 172.17.0.1

IP : 54.37.65.92

# Schéma logique

Le schéma logique représente la manière dont on va déployer notre infrastructure sur le terrain. Le but étant de protéger le réseau de l’entreprise, le firewall est donc l’élément central. Ensuite, vient les différents subnets avec le réseau interne de l’entreprise qui comprend les PC et le serveur DNS interne. Les serveurs WEB, mail et DNS externe ont chacun un subnet séparé.



# Problèmes techniques rencontrés

* Au départ l’échange des clés pour la communication SSH entre PC et VPS a posé quelques soucis. Le fait de bien générer les clés sur le PC, et non sur le serveur pour garder la clé privée sur le PC.
  + Solution : Effacer les clés générées sur le VPS et les générer sur le PC directement à la place.
* A la commande *docker restart*, notre container ne redémarrait plus. Il faisait le *stop*, mais une erreur se produisait au niveau du *start*. Et cela plusieurs fois dans des cas différents. C’est arrivé pour le container Apache et pour le container Bind. (Ce problème est également arrivé à d’autres personnes dans d’autres groupes)
  + Solution : Ne plus faire *docker restart* mais décomposer : *docker stop* puis *docker start*.
* Pour le DNS, une difficulté était de trouver le bon fichier, car il y avait 3 named.conf.xxxx
  + Compréhension de ce qui se trouve dans les différents fichiers
* La communication entre le service web et la DB a également pris du temps. Au début nous avons testé Nginx avec lequel nous ne sommes pas arrivé à mettre en place PHP, nous nous sommes donc tournés vers Apache dont nous avons créé une image qui installait PHP directement lors de sa création
  + Grâce à PHP nous avons pu utiliser PDO en récupérant les informations des hostname avec « docker network inspect bridge », créé un utilisateur grâce à l’IP du container Web et lui autoriser la connexion à la base de données
* Un nouveau problème a été rencontré avec le DNS.
  + Le container ne reconnaissait plus les fichiers de zones. On a donc récréé une nouvelle image et donc construit à nouveau le container sur une base saine.
* Pour les VirtualHost nous étions d’abord parti sur trois containers tournant sur différents ports à mapper dans le DNS. Cependant il s’est révélé plus simple de faire des VirtualHost sur le nom de domaine.
* Une des difficultés rencontrées lors de la mise en place du serveur mail était de trouver une image qui correspondait au cahier des charges. Nous avons finalement choisi tvial/docker-mailserver car c’est une image assez complète et simple à mettre en place.
* *[NEW !]* Nous avons quelques difficultés à mettre l'intranet seulement visible pour les employés de l'intérieur du réseau dans le DNS.
  + Pour résoudre ce problème nous avons décidé de filtrer au niveau du serveur web et non plus au niveau DNS.
* Pour la VOIP, nous avons eu notre première difficulté lors de l'installation d'Asterisk, car depuis la rédaction dans la documentation Ubuntu, certaines versions du service ont changé !
  + Nous avons pour cela été voir un cran en arrière dans la hiérarchie de l'URL pour pouvoir ensuite choisir la nouvelle version.
  + Ensuite, certains packages "–dev" étaient manquant, on les a donc installés lorsque l'erreur correspondante survenait.
* *[NEW !]* Lors de l’activation du firewall sur le vps contenant le serveur mail, la connexion ssh a été coupée. En effet, suit à un oubli de notre part, le vps n’acceptait pas les connexions entrantes sur le port 22. Cela a été corrigé en faisant « ufw allow 22 » et « ufw allow ssh ». Les commandes sont redondantes mais nous avons préféré mettre les 2 pour plus de sûreté.

# Etat d'avancement

* Service Web :
  + La page vitrine est opérationnelle
  + La page dynamique d’e-commerce est opérationnelle
  + La page d’intranet est opérationnelle, requiert une identification et un mot de passe et n’est pas accessible en dehors du réseau interne de l’entreprise
* Base de données :
  + Table des produits créée
  + Table des employés créée
* Service DNS :
  + Fichiers de zone rédigés
  + DNSSEC mis en place
  + Accès aux sites par les URL demandés
  + Intranet seulement accessible de l'intérieur
  + DNS inverse opérationnel
  + La configuration du service DNS est organisée comme suit :
    - named.conf.local est le fichier comprenant les "view" interne et externe ainsi que l'access list (acl).
    - db.internal.wt2.ephec-ti.be est le fichier de zone interne.
    - db.wt2.ephec-ti.be est le fichier de zone externe.
* Service mail :
* Fichiers de configuration modifiés pour correspondre au cahier des charges
* Container docker “up and running”
* Adresses mails et alias créées
* Certificat ssl créé
* *[NEW !]* Les boîtes mails sont consultables de partout.
* *[NEW !]* Les employés peuvent recevoir et envoyer des mails de et à tout le monde (autres employés ou personnes extérieures).
* *[NEW !]* Des filtres anti-spam sont déployés avec SpamAssassin
* *[NEW !]* Le serveur ne permet pas d’envoyer des mails qui ne viennent pas de l’entreprise
* *[NEW !]* VOIP :
* Fichiers de configuration édités pour implémenter une "entreprise" composée d'un directorat (directeur + secrétaire), d'un service de comptabilité (2 comptable), un département commercial et l'atelier avec le reste des employés. Voici un plan de l'adressage des numéros d'appel :

|  |  |  |
| --- | --- | --- |
| Contexte | Personne | Code d'appel |
| directorat | Directeur | 1001 |
| directorat | Secrétaire | 1002 |
| directorat | voicemail | 1999 |
| comptabilite | groupeComptable | 2000 |
| comptabilite | Comptable 1 | 2001 |
| comptabilite | Comptable 2 | 2002 |
| comptabilite | voicemail | 2999 |
| commercial | Commercial 1 | 3001 |
| commercial | Commercial 2 | 3002 |
| commercial | voicemail | 3999 |
| atelier | atelier | 4000 |
| atelier | Louis | 4001 |
| atelier | Justine | 4002 |
| atelier | Justin | 4003 |
| atelier | voicemail | 4999 |

* Communications inter et intra services opérationnels.
* Voice-mail est configuré.
* Joignable depuis l'extérieur.
* Redirection vers le/la secrétaire lorsque quelqu'un tente de joindre le directeur. Et la secrétaire peut rediriger les appels vers n'importe quel autre numéro.
* La VOIP est organisée comme suit :
  + Le fichier sip.conf comprend l'organisation des canaux SIP.
  + Le fichier users.conf comprend la configuration des utilisateurs.
  + Le fichier extensions.conf est la configuration du DialPlan.
  + Le fichier voicemail.conf est le fichier de configuration pour les messageries des utilisateurs.
  + Le fichier iax.conf est le fichier de configuration pour les appels entre domaines.

# Sécurité mise en place

* DNSSEC est activé de base dans le container BIND9.
* Pour éviter que quelqu’un ne fasse trop de demandes de connexion avec la même adresse IP, nous avons mis en place Fail2Ban sur tous les VPS pour exclure l’IP qui ferait des demandes de connexion à répétition.
* Firewall en cours de configuration.