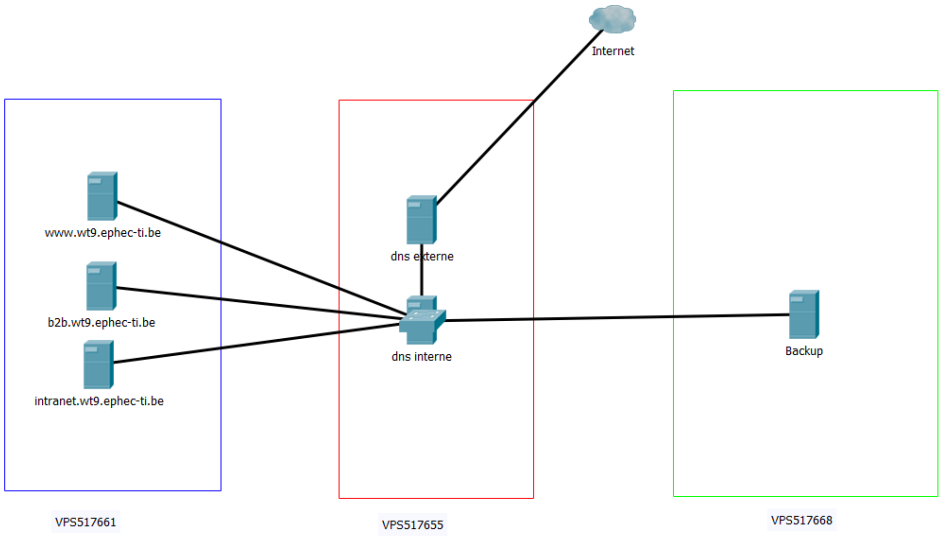
Gossens Jonathan
Blacks Sebastien
de Mahieu Benoit

jeudi 15 mars 2018

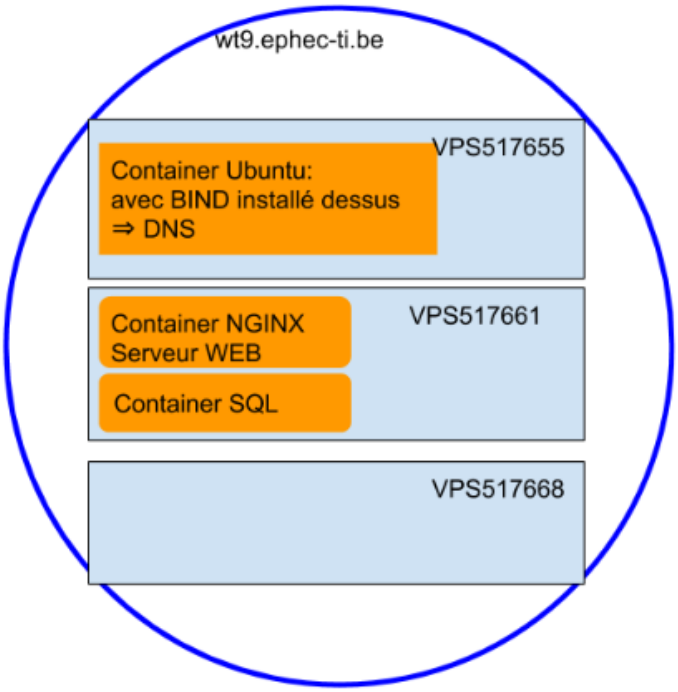
Rapport professeur

Schéma logique:



L'infrastructure choisie a été découpée en trois vps distincts. Le vps 517655 a été choisis pour abriter les deux containers nécessaires au fonctionnement d'un DNS. Le vps 517661 quand à lui héberge trois containers nginx dont un avec un serveur PHP/SQL pour les différents sites web demandés par le client. Le troisième vps 517668 est utilisé comme conteneur backup.

Schéma Physique:



Choix pour le DNS : Nous avons décidé de choisir un container ubuntu dans lequel on a installé Bind9 et tous les outils nécessaire à l'utilisation du DNS et à l'édition de fichiers de config. Une fois BIND installé, si l'on se souvient de comment faire un fichier de zone, c'est très simple d'utilisation.
Choix pour le WEB: Nous avons choisi d'utiliser un container nginx car nous avions déjà vu comment faire une configuration apache et que nous voulions essayer d'utiliser un autre service. Les informations trouvées
Choix pour SQL: MySQL est la base de données la plus répandue donc j'ai utilisé celle-là. Elle est accessible pour le moment sur internet mais il faudra empêcher cela à l'avenir.

Problèmes rencontrés et problèmes non résolus:

DNS → Quelques difficultés pour se rappeler du fonctionnement du DNS, des ressources records et des fichiers de zone…
Mécanismes d'exposition de ports ?
WEB → Problème au niveau des ports, pour accéder aux différents sites web, on utilise pour le moment des ports différents pour chaque site.
SQL → Connexion à travers le moteur de recherche et la sécurisation à ce niveau.

Techniques de sécurisation du VPS:

- Retirer la connexion au démarrage au compte root
- Remplacer l'authentification par mot de passe qui est par défaut par une authentification par clé asymétrique. Cette technique est plus sécurisée car les clés sont cryptées
- Installation de Fail2Ban qui ban des adresses IP lorsqu'un utilisateur se rate X fois lors de sa connexion. L'adresse est bannie durant 30 minutes.
- On aurait pu changer le port de connexion mais ce n'est pas pratique du point de vue du professeur de noter les ports de chaque groupe.
- Nous avons paramétré un firewall appelé *ufw* permettant de bloquer certain ports ou iptable.

Techniques de sécurisation des services:

- le fait que chaque service se trouve dans un container docker distincts permet d'isoler point de vue d'une attaque les différents services présents sur le vps attaqué