Rapport technique : mission 1

# Schéma physique

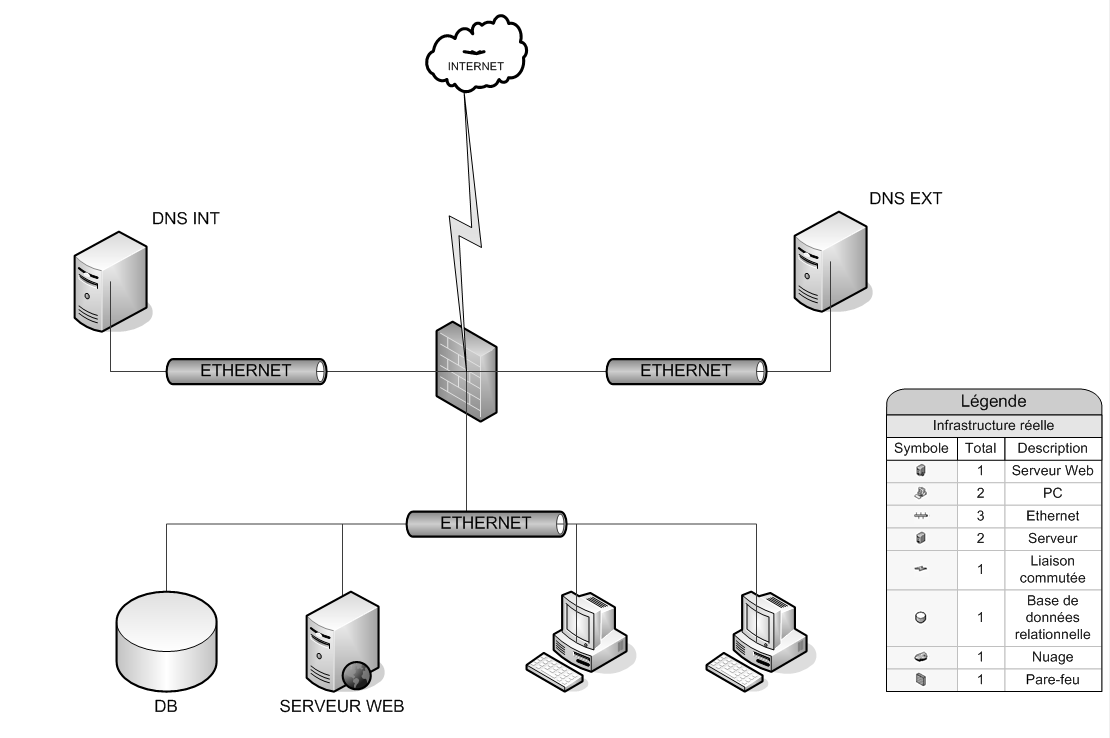
De point de vue physique, nous avons structuré dans un premier temps les containers d’une façon simple. C’est-à-dire, un VPS héberge les parties DNS, tandis que le second héberge les parties web, donc l’Intranet, le site vitrine et le site interactif. C’est sur ce second VPS que la communication avec la DB est également faite.

|  |
| --- |
| VPS517640  DNS inverse  DNS IP : 54.37.65.43  IP : 54.37.65.43  VPS517674  Intranet IP : 54.37.65.110:44000  Site vitrine IP : 54.37.65.110:8081  Site interactif IP : 54.37.65.110:8080  IP : 54.37.65.110 |

Ce schéma n’est pas forcément le plus idéal, mais était plus une question de facilité pour le début du projet.

# 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 web. Les serveurs DNS interne et externe ont chacun un subnet séparé.



# Problèmes techniques rencontrés

Nous avons rencontré quelques problèmes durant la mise en place de cette première phase :

* Au départ l’échange des clés pour la communication ssh entre PC/VPS a posé quelques soucis. Notamment, 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 trouvé le bon fichier, car il y avait 3 named.conf.xxxx
  + Compréhension ce qui se trouve dans les différents fichiers
* La communication entre le service web et la DB a également pris du temps. L’accès à la DB par le site était refusé.
  + Solution : A REMPLIR JUSTIN ☺

# Sécurité mise en place

Nous n’avons pas encore regardé particulièrement à la mise en place de sécurité, mais nous avons remarqué que DNSSEC est activé de base dans le container BIND9.

Pour éviter que quelqu’un ne fasse trop de demande de connexion avec la même adresse IP, nous mettrons en place Fail2Ban pour exclure l’IP en conséquence.