2TL1-10

# Projet admin
# Analyse de sécurité

## Vps et docker

Tous d'abord les risques encourus quand nous nous connectons par mot de passe à nos vps sont simples, si quelqu'un arrive à intercepter la communication, il pourra lire notre mot de passe et donc prendre possession de notre vps. De plus, il est important de ne pas mettre des containers docker accessibles depuis l'extérieur sur le même vps que des containeurs qui gérent l'interne. En effet, les serveurs en liens avec l'extérieur sont plus susceptibles de se faire pirater et donc pourrait donner des informations internes à l'entreprise.

## Solutions

Pour la connexion au vps nous allons nous connecter qu'une seule fois par mot de passe et ensuite utiliser la connexion par clé partagée. En effet, nous allons créer 4 utilisateurs sur chaque vps, et partager une clé pour chaque utilisateur. Grâce à cela seul les utilisateurs ayant la clé pourront se connecter au vps et le trafic sera chiffré.

Pour la répartition des containeurs, nous avons séparé les serveurs externes et les serveurs internes.

## Risques

### Web interne

D'autre utilisateurs externes puissent avoir accès.

### Dns interne :

D'autres utilisateurs externes puissent faire des requêtes dessus.

## Solutions

### Web interne

Lui donner grâce à la commande « Require » la liste des adresses ip qui sont autorisées.

### Dns interne

Modifier le fichier named.conf.options et ajouter allow-query{#ip} pour n'autoriser que les requêtes venant de ces adresses ip.