**Livrable : Partie 5 Sécurisation des serveurs / Firewall**

Pour commencer la mise en place du FireWall UFW on a vérifié qu’on l’avait bien sur notre VM ubuntu :

Une image contenant texte

Description générée automatiquement

Comme On peut le voir grâce a « sudo ufw status » on a rentré notre mot de passe et on a vu le status de ufw, ici inactive.

Ensuite nous avons fait « sudo ufw enable » afin d’activer le FireWall UFW.

Nous avons vérifié son status avec « sudo ufw status verbose », on voit bien que le firewall est lancé et aussi on peut voir les règles par défaut d’UFW.

Nous devions maintenant mettre en place des règles bien précises :

Une image contenant texte

Description générée automatiquement

1.1)Autoriser que les connexion entrantes sur ssh / Port 22

Une image contenant texte

Description générée automatiquement

1.2)Autoriser que les connexion entrantes sur https / Port 443

Une image contenant texte

Description générée automatiquement

1.3) Autoriser que les connexions entrantes sur http / Port 80

Une image contenant texte

Description générée automatiquement

On peut vérifier le statu des règles mis en place avec encore la commande « sudo ufw status verbose »

Une image contenant texte

Description générée automatiquement

2) Limiter le nombre de connexions à la seconde au port http

Nous avons fait « cd /etc/ufw/ » afin de nous déplacer dans le dossier de  « ufw », pour s’occuper du dossier « before.rules », ce dossier qui contient toute les règles qui s’effectue avant les règles personnalisées.



On c’est mis dans le dossier « before.rules » avec la commande « sudo nano before.rules » pour le modifier.

On a ajouté quelques lignes au début du fichier :

Une image contenant texte

Description générée automatiquement

Ce qui veux dire que nous allons appeler une règle que nous allons définir juste après.

Une image contenant texte

Description générée automatiquement

Sur ce screen on voit donc la règles custom ayant pour objectif de bloquer le nombre de connexion X en un nombre de secondes Y.

Limite de connexion par IP, on est à 45 toute les 10 secondes

Limite de paquets par IP, on est à 45 par secondes

Et donc si une adresse ip respecte cette règle, elle est « ACCEPT » et donc peut entrer sur le site.