Annexe 1 – Découverte du firewall UFW (Uncomplicated Firewall)

I - Introduction

UFW (**Uncomplicated Firewall**) est le pare-feu installé par défaut sous **Ubuntu**. C'est un nouvel outil de configuration simplifié en ligne de commande de **Netfilter**, qui donne une alternative à l'outil **iptables**.

Remarque : L'**ordre** de déclaration des **règles** est très important, le système utilisant une politique « **premier arrivé, premier servi** ». Prenez donc soin d'ajouter vos règles spécifiques avant les règles générales lorsqu'elles concernent des éléments communs.

II - Installation et utilisation

Pour installer **UFW**, il faut installer le paquet **ufw** : **apt-get install ufw**.

L'outil **UFW** n'est pas activé par défaut. Pour l'activer, il faut taper : **ufw enable** et pour le désactiver : **ufw disable**.

L'**autorisation** d'un **flux entrant** de manière simple, se fait comme ceci : **ufw <allow|reject|deny> <port>**.

Par exemple, pour autoriser les connexions **ssh** : **ufw allow 22**.

Par exemple, pour ouvrir le port **53** en **TCP** et **UDP** : **ufw allow 53**.

Par exemple, pour ouvrir le port **25** en **TCP** uniquement : **ufw allow 25/tcp**.

UFW possède un ensemble de **règles prédéfinies** permettant d'autoriser certaines **applications** sans avoir à connaître les numéros de port. On peut obtenir la liste des **applications** connues avec la commande : **ufw app list**.

Pour **autoriser** une application, comme précedemment : **ufw <allow|reject|deny> <application>**. Par exemple, pour autoriser les connexions **ssh** : **ufw allow SSH**.

Il est possible de créer des **règles** plus **complexes**, permettant par exemple de filtrer par adresses IP. La syntaxe est alors la suivante : **ufw <allow|reject|deny> [proto <protocole>] [from <IP_Source> [port <port_source>]] [to <IP_dst> [port <port_dst>]]**.

Par exemple, pour bloquer les requêtes **ssh provenant** de l'**IP 192.168.10.1** : **ufw deny from 192.168.10.1 to any port 22**.

On pourra afficher les règles en place : **ufw status** ou **ufw status verbose**.

On pourra supprimer une règle avec le mot clé **delete** devant les arguments qui ont servis à la créer. Par exemple : **ufw delete allow 22**.

On pourra supprimer une règle selon son **rang**. Il faut d'abord afficher les règles avec leur numéro : **ufw status numbered** puis effacer la règle correspondant au numéro saisie : **ufw delete 2**.