1. Le pare-feu UFW

1.1. Ressources

Lien :

- https://doc.ubuntu-fr.org/ufw
- https://www.digitalocean.com/community/tutorials/initial-server-setup-with-debian-10

1.2. Commandes de bases

- Lister les profils d'application dispobibles

```
$ sudo ufw list
```

- ATTENTION à faire en premier avant d'activer ufw : activer l'accès SSH

Autoriser l'accès SSH

```
$ sudo ufw allow OpenSSH
```

- Activer ufw

```
$ sudo ufw enable
```

* Visualiser les paramètres actuels avec les numéros de règles

```
$ sudo ufw status numbered verbose
```

- autoriser une connexion entrante

```
$ sudo ufw allow 443/tcp
```

- supprimer une règle

```
$ sudo ufw delete allow 443/tcp
```

- supprimer une règle par son numéro

```
$ sudo ufw delete [numéro]
```

1.3. Utiliser le fichier de règles

Le comportement par défaut de UFW est de bloquer tout le trafic, de bloquer tout le trafic forwarding et d'autoriser totu le traffic sortant (outbound). Le principe est de ne permettre à personne de pouvoir se connecter sauf en spécifiant l'ouverture d'un port. PAr contre les applications et services en cours d'exécution peuvent accéder à Internet.

Les stratégies par défaut sont définies dans le fichier **/etc/default/ufw** et peuvent être changées en modifiant manuellement le fichier ou en ligne de commandes (commande sudo ufw default <policy> <chain>).

Firewall policies are the foundation for building more complex and user-defined rules. Generally, the initial UFW Default Policies are a good starting point.

Application Profiles #

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/ufw/accueil?rev=1613242052

Last update: **2021/02/13 18:47**