

Le pare-feu UFW

Ressources

Lien :

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

Commandes de bases

- Lister les profils d'application disponibles

```
$ 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]`

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 tout le trafic 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>`).

IP Masquerading

L'IP Masquerading est une variante du NAT (network address translation) dans le noyau Linux pour traduire le trafic réseau en réécrivant le trafic en réécrivant les adresses IP de source et de destination et les ports. Avec IP Masquerading, vous pouvez permettre à une ou plusieurs machines dans un réseau privé de communiquer avec Internet en utilisant une machine Linux qui agit comme un gateway.

Configurer IP Masquerading avec UFW implique plusieurs étapes.

First, you need to enable IP forwarding. To do that, open the `/etc/ufw/sysctl.conf` file:

```
sudo nano /etc/ufw/sysctl.conf
```

 Find and uncomment the line which reads `net.ipv4.ip_forward = 1`:

```
/etc/ufw/sysctl.conf net/ipv4/ip_forward=1
```

 Copy Next, you need to configure UFW to allow forwarded packets. Open the UFW configuration file:

From:
/ - Les cours du BTS SIO

Permanent link:
[/doku.php/reseau/ufw/accueil?rev=1613242192](https://doku.php/reseau/ufw/accueil?rev=1613242192)

Last update: 2021/02/13 19:49

