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 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 <code shell> $ sudo ufw enable </code>
- Visualiser les paramètres actuels avec les numéros de règles <code shell> $ sudo ufw status numbered verbose </code>
  - autoriser une connexion entrante <code shell> $ sudo ufw allow 443/tcp </code>
  - supprimer une règle <code shell> $ sudo ufw delete allow 443/tcp </code>
  - supprimer une règle par son numéro <code shell> $ sudo ufw delete [numéro] </code>

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>).

IP Masquerading

L'IP Masquerading est une variante du NAT (network address translation) dans le noyau Linux pour translater le trafic réseau en réécrivant the network la source et la destination des adresse IP et des ports résedaux. Grâce à l'IP Masquerading, des ordinateurs du réseau local privé peuvent communiquer avec Internet en utilisant l'OS Linux comme une passerelle.

- activer le routage en modifiant /etc/ufw/sysctl.conf pour obtenir la ligne suivante :

```
net/ipv4/ip_forward=1
```

- activer le forwarding en modifiant le fichier /etc/default/ufw pour obtenir la ligne suivante :

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

- mofifier le fichier /etc/ufw/before.rules pour activer le forwarding en ajoutant les lignes suivantes

```
#NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]

# Forward traffic through eth0 - Change to public network interface
-A POSTROUTING -s 10.8.0.0/16 -o eth0 -j MASQUERADE

# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
```