3. Configuration du Firewall

- Mise en place & configuration du Firewall
- Liste de commandes UFW

Mise en place & configuration du Firewall

Installation

```
sudo apt install ufw
```

Une fois installé, il est conseillé de mettre en place une configuration par défaut des connexions entrantes et sortantes.

Connexion entrantes

Par défaut refuser toutes les entrées.

```
sudo ufw default deny incoming
```

Connexion sortantes

Par défaut autoriser toutes les sorties.

```
sudo ufw default allow outgoing
```

Configuration

> ATTENTION, UNE MAUVAISE CONFIGURATION PEUT VOUS ÉJECTER DE VOTRE PROPRE SERVEUR.

Tout d'abord il convient de définir les ports autorisant les connexions entrantes.

Par exemple si l'on n'autorise pas le port SSH (soit le port 22) alors plus aucun utilisateur ne pourra se connecter a distance sur le serveur. Le seul moyen de rattraper ce cas c'est d'avoir un accès physique au serveur.

>

> Par conséquent, il convient d'autoriser certains ports par défaut pour éviter de se fairebannir de son propre serveur.

Ouverture du port SSH

```
sudo ufw allow ssh
```

Ce qui équivaut a faire :

```
sudo ufw allow 22
```

Ouverture des ports pour le Web

Si vous serveur héberge un ou plusieurs site(s) web alors vous allez devoir ouvrir le port 80 (pour les requêtes HTTP) et le port 443 (pour les requêtes HTTPS)

```
sudo ufw allow 80
```

```
sudo ufw allow 443
```

Ouverture des ports par service

Si votre serveur héberge d'autres services utilisant des ports différents que ceux ouvert précédemment alors vous devrez ouvrir les ports utilisés. Dans le cas contraire vos services ne seront pas accessibles depuis l'extérieure.

Par exemple votre serveur héberge une base de données PostgreSQL et vous souhaitez y accéder depuis l'extérieur pour la manager. Dans ce cas vous devrez ouvrir le port 5432 (port utilisé par défaut par PostgreSQL).

```
sudo ufw allow $PORT
```

Ouverture d'un port par adresse IP

Vous pouvez également spécifier un port spécifique auquel l'adresse IP est autorisée à se connecter en ajoutant à tout port suivi le numéro du port. Par exemple, si vous voulez autoriser 203.0.113.4 à se connecter au port 22 (SSH), utilisez cette commande :

```
sudo ufw allow from 203.0.113.4 to any port 22
```

Vérification de la configuration

Si vous n'êtes pas sur de votre configuration et que vous voulez la vérifier avant de l'activer, il possible de le faire avec la commande suivante :

```
sudo ufw status verbose
```

Ce qui devrez vous affichez les informations suivantes :

```
# Afficher toutes les règles définit sur le firewall
Status: inactive
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80                         ALLOW IN    Anywhere
22                         ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
80 (v6)                    ALLOW IN    Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
```

Activation du Firewall

Une fois la configuration terminé vous allez devoir activer le service pour que celui-ci fonctionne.

> Lors de l'activation du pare-feu votre connexion au serveur sera interrompu vous allez devoir vous reconnecter.

```
sudo ufw enable
```

```
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Liste de commandes UFW

Commandes UFW

D'autres commandes ufw qui peuvent être utiles.

- Recharger les règles du pare-feu

```
sudo ufw reload
```

- Activer / Désactiver le service

```
# Activer
sudo ufw enable

# Désactiver
sudo ufw disable
```

- Statut du service

```
sudo service ufw status
```

- Liste des règles du firewall

```
# lister les règles
sudo ufw status
# OU lister les règles en les numérotants
sudo ufw status numbered
# OU lister les règles avec le détail
sudo ufw status verbose
```

- Supprimer une règle du firewall en fonction de son numéro

```
sudo ufw delete 5
```

- Supprimer une règle du firewall en fonction de son activation

```
sudo ufw delete allow 80
```

- Autoriser toutes les connexions en réseau local

```
# Pour autoriser toutes les connexions sur une seule ip local:
sudo ufw allow from 192.170.0.0

# Pour autoriser toutes les connexions sur plusieurs ip local: ip.adress.local =
192.170.0.0/24
# pour les ip de 192.170.0.1 à 192.170.0.255
sudo ufw allow from 192.170.0.0/24
```

Résultat :

```
To                         Action      From
--                         ------      ----
Anywhere                   ALLOW       192.170.0.0/24
Anywhere                   ALLOW       192.170.255.0/24
```