

## **ATELIER 3 :**

Dans un premier temps , je procède à l'installation d'un Serveur Ubuntu

### **Étape 1 — Utilisation d'IPv6 avec UFW (facultatif) :**

La valeur d'IPv6 et bien sur yes :

```
GNU nano 7.2 /etc/default/ufw
#
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPv6=yes
```

### **Étape 2 — Mise en place des politiques par défaut :**

ENSUITE, JE définis les valeurs par défaut pour refuser les connexions entrantes et autoriser les connexions sortantes.

```
idriiss@idriiss:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
idriiss@idriiss:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
idriiss@idriiss:~$ _
```

### **Étape 3 — Autoriser les connexions SSH**

Je configure le serveur de sorte à autoriser les connexions SSH entrantes,

```
idriiss@idriiss:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

On peut également remplacer le nom du service par le numéro de port :

```
idriiss@idriiss:~$ sudo ufw allow 22
Rules updated
Rules updated (v6)
idriiss@idriiss:~$
```

### **Étape 4 — Activation d'UFW**

Ensuite , j'active UFW et j'affiche les règles fixées :

```

idriss@idriss:~$ sudo ufw eneable
ERROR: Invalid syntax

Usage: ufw COMMAND

Commands:
enable          enables the firewall
disable         disables the firewall
default ARG     set default policy
logging LEVEL   set logging to LEVEL
allow ARGS      add allow rule
deny ARGS       add deny rule
reject ARGS     add reject rule
limit ARGS      add limit rule
delete RULE|NUM delete RULE
insert NUM RULE insert RULE at NUM
prepend RULE    prepend RULE
route RULE      add route RULE
route delete RULE|NUM delete route RULE
route insert NUM RULE insert route RULE at NUM
reload          reload firewall
reset           reset firewall
status          show firewall status
status numbered show firewall status as numbered list of RULES
status verbose  show verbose firewall status
show ARG        show firewall report
version         display version information

Application profile commands:
app list        list application profiles
app info PROFILE show information on PROFILE
app update PROFILE update PROFILE
app default ARG set default application policy

idriss@idriss:~$ sudo ufw status verbose
Status: inactive
idriss@idriss:~$ _

```

## Étape 5 — Autoriser d'autres connexions

Je peux désormais autoriser les connexions de mon choix :

```

idriss@idriss:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)
idriss@idriss:~$ sudo ufw allow 443
Rules updated
Rules updated (v6)
idriss@idriss:~$

```

Je peu également accepter les connexions à des adresse ip spécifiques et également des sous-réseaux :

```

idriss@idriss:~$ sudo ufw allow from 192.168.17.79
Rules updated

```

## Étape 6 — Refuser les connexions

Je peux également refuser les connexion que ce soit à des adresse ip , des serveur ect ...

```
idriss@idriss:~$ sudo ufw deny http
Rules updated
Rules updated (v6)
```

## Étape 7 — Suppression de règles

Il y'a plusieurs manières de supprimer les regles :

Premierement , par numéro de règle :

```
idriss@idriss:~$ sudo ufw delete 2
Deleting:
allow 22
```

ET en citant directement la règle :

```
idriss@idriss:~$ sudo ufw delete deny http
Rules updated
Rules updated (v6)
```

## Étape 9 - Désactivation ou réinitialisation d'UFW (facultatif) :

```
idriss@idriss:~$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20250123_085701'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250123_085701'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250123_085701'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250123_085701'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250123_085701'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250123_085701'
```