Ubuntu Server - Paramétrer UFW

Difficulté : Novice

Notions : Sécurité, pare-feu, Ubuntu server

I. Introduction

Cette procédure vise à expliquer la mise en place et la configuration du pare-feu UFW (**U**ncomplicated **F**ire**W**all) sur les serveurs Ubuntu.

> **Info** : Les paquets sont normalement déjà pré-installés sur le serveur.

Voici la page d'aide de ufw :

```
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
```

II. Activation / Désactivation Firewall

Pour activer le firewall :

```
ufw enable
```

```
root@vulnerablelinux:/home/admin# ufw enable
Firewall is active and enabled on system startup
```

Désactiver le firewall :

```
ufw disable
```

```
root@vulnerablelinux:/home/admin# ufw disable
Firewall stopped and disabled on system startup
```

II. Gérer les règles

2.1 Créer les règles

Les règles se construisent selon le modèle suivant :

Commande	Action	(opt) source	(opt) destination	port	protocol
ufw	allow	ip unique	ip unique	numéro de port	tcp
	deny	cidr réseau	cidr réseau	alias (ex : http)	udp
	reject				...

Créer une règle courte pour du trafic entrant (ex: pour http et https):

```
ufw allow 80/tcp
ufw allow 443/tcp
```

```
root@vulnerablelinux:/home/admin# ufw allow 80/tcp
Rule added
Rule added (v6)
```

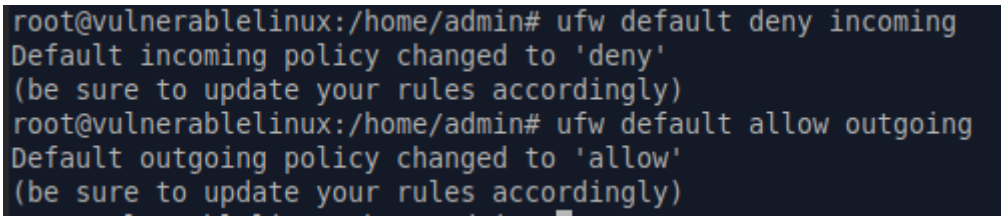
Pour ajouter des règles complexes (ex: limiter la connexion ssh) :

```
ufw allow from 172.16.11.1 to any port 22 proto tcp
```

```
root@vulnerablelinux:/home/admin# ufw allow from 172.16.11.1 to any port ssh proto tcp
Rule added
```

Créer une règle par défaut :

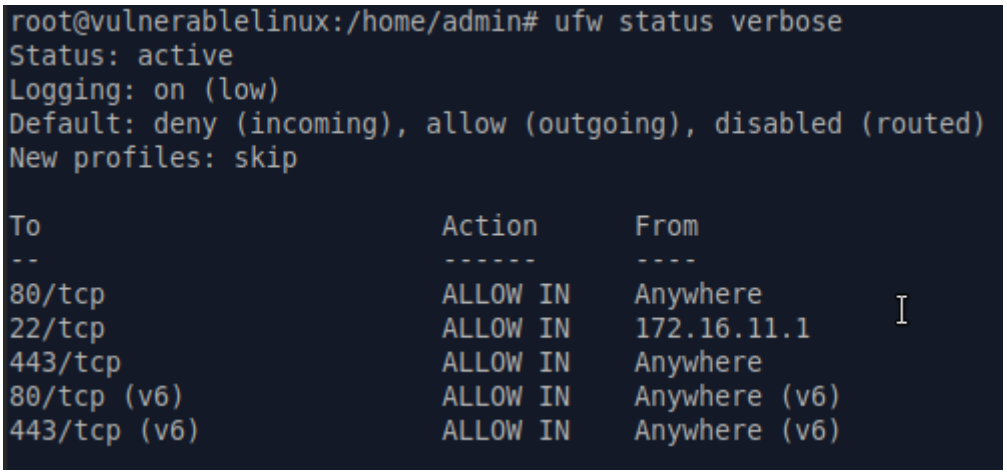
```
ufw default deny incoming
ufw default allow outgoing
```



2.2 Afficher les règles

Pour afficher le status avancé et les règles existantes :

```
ufw status verbose
```



Pour afficher les règles avec les numéros de règles :

```
ufw status numbered
```

```
root@vulnerablelinux:/home/admin# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    172.16.11.1
[ 3] 443/tcp                    ALLOW IN    Anywhere
[ 4] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 5] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
```

2.3 Supprimer les règles

Pour supprimer les règles, deux façon de faire :

- Supprimer la règle avec `ufw delete <réécrire la règle>`
- Supprimer par le numéro de règle `ufw delete <numéro de règle>`

```
root@vulnerablelinux:/home/admin# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    172.16.11.1
[ 3] 443/tcp                    ALLOW IN    Anywhere
[ 4] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 5] 443/tcp (v6)               ALLOW IN    Anywhere (v6)

root@vulnerablelinux:/home/admin# ufw delete 5
Deleting:
 allow 443/tcp
Proceed with operation (y|n)?
```

2.4 Appliquer les règles

> **Info** : après avoir changé les set de règles (ajout / supression, modification), il faut les appliquer.

Appliquer les règles :

```
ufw reload
```

```
root@vulnerablelinux:/home/admin# ufw reload
Firewall reloaded
```

III. Bloquer les réponses ICMP (ping)

Pour que le pare feu bloque par défaut les requêtes ICMP (echo-request), editer le fichier '**/etc/ufw/before.rules**'.

Modifier les deux lignes autorisant le ***echo-request*** en changeant le '***ACCEPT***' en '***DROP***'.

```
# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT
```

Sauvegarder et quitter. Puis appliquer la configuration avec :

```
ufw reload
```

```
root@vulnerablelinux:/home/admin# ufw reload
Firewall reloaded
```

Revision #2
Created 2026-07-29 12:10:21 UTC by Olivier
Updated 2026-07-29 13:02:42 UTC by Olivier