Gateway

Catégorie pare-feu

On installe Debian (ou n'importe quel autre système d'exploitation sans son interface graphique). Je choisis debian, après avoir hésité entre windows et ubuntu, car il m'est plus familier au niveau du système et des commandes.

Je m'occupe du pare-feu avec iptables, je l'installe : apt install ufw
Problème :

- accès refusé pour installer quoi que ce soit
- bash sudo : commande introuvable

On tape alors la commande **su -** qui nous met directement en root, avec ça nous pouvons donc installer et faire ce qu'il faut.

1. apt install ufw
2. apt install sudo

Modification du pare-feu

Avant de commencer, on regarde bien que ufw status soit désactivé pour éviter de mauvaises surprises, comme une mauvaise manip qui nous retire la connexion internet, par exemple.

Toujours en sudo, on refuse les connexions entrantes (c'est toujours mieux de désactiver surtout avec un pare-feu qui va servir l'entreprise) et on autorise les connexions sortantes via le port 30 et la commande :

- ufw default deny incoming
- ufw default allow outgoing

On autorise toutes les communications http et https, sorties et entrantes avec le port 80. On autorise ici l'accès à "internet" avec la commande.

- ufw allow http
  ou
- ufw allow port 80
- ufw allow port 443

Pour pouvoir accéder à cette machine à distance on utilisera le ssh, donc le port 22. Il est donc impératif que le pare-feu autorise cette connexion via ce port.

- ufw allow ssh

Pour le serveur FTP, on fera la commande :

- ufw allow ftp
  ou
- ufw allow port 21

Pour être sûre qu'il soit bien activé et fonctionnel, il suffit ensuite de taper cette commande telnet **lenomdevotredomaine**.com 21

On va autoriser le protocole LDAP. Il permet aux entreprises de stocker, gérer et sécuriser leurs informations et celles de leurs utilisateurs ainsi que d'autres ressources telles que les noms d'utilisateurs et mots de passe.

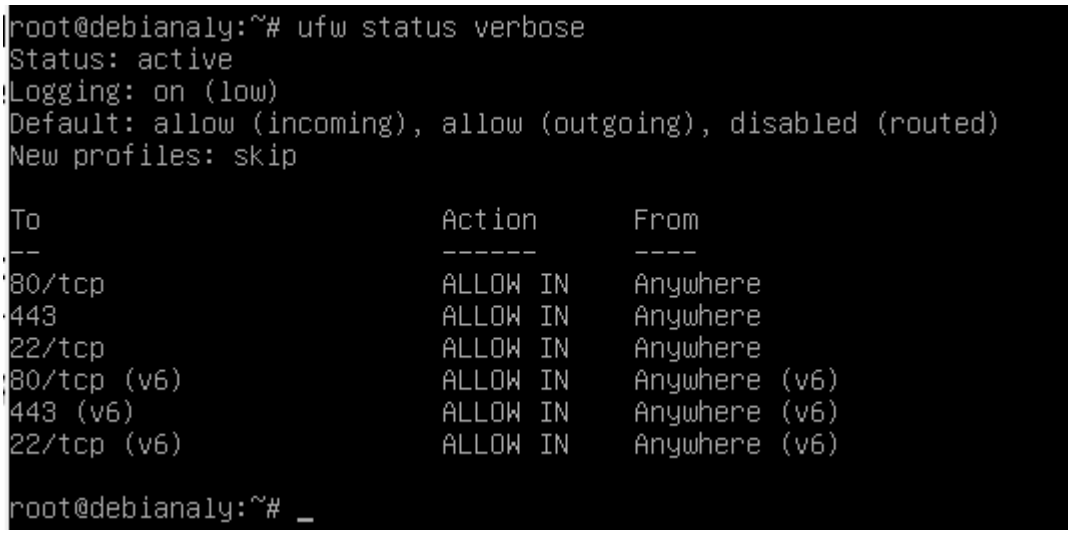
- ufw allow port 389

On a refusé et autorisé tout ce qui est entrant et sortant, on a aussi autorisé l'accès à internet. On a autorisé pleins d'autres choses, bref on peut donc activer notre pare-feu avec

- ufw enable

Pour bien vérifier nôtre statut et voir l'historique de ce qu'on a activé, on fait la commande :

- ufw status verbose



script setup gateway :

```
#!/bin/bash
echo "Please enter the username :\n"
read user
echo "Now enter the user password :\n"
read pass
su -
apt install ufw
apt install sudo
echo -ne ‘$user\n$pass\n’
apt install ufw
apt install sudo
ufw default deny incoming
ufw default allow outgoing
ufw allow port 80
ufw allow port 443
```

ufw allow ssh

ufw allow port 389

ufw allow ftp

ufw enable

ufw status verbose

Script pour git pull :

- installer cron
- copier le repo git

crontab -e

5 * * * * * cd /chemin-vers-le-git/… git pull

—----------

Auto sauvegarde de FTP :

Date=`date "+%d-%m-%y_%H:%M"`

echo "Please enter the username :\n"

read user

echo "Now enter the user password :\n"

read pass

echo "And now the IP of the FTP server :\n"

```
read IP

tar -zcvf Backup_$Date.tar.gz /etc/proftpd/

echo "Please enter the username :\n"

read user

echo "lcd /home/$user\nmirror -R ../../FTP/Pour_aller_plus_loin/B*\nexit\n" | lftp -u $usern,$pass $IP
```