Iptables configuration minimale

1) Configuration minimaliste

1.1) Que veut-on faire ?

- ➫ tout bloquer en entrée
- ➫ bloquer le forwarding
- ➫ dropper les requête echo (le TTL indique l'OS)
- ➫ préserver la boucle locale (lo)
- ➫ autoriser les ports 22,80,443 en entrée
- ➫ autoriser les ports 22,80,443,53 en sortie
- ➫ protéger le serveur web de trop nombreuses requêtes
- ➫ maintenir les connexions établies
- ➫ loger les requêtes bloquées (dropped)
- ➫ loger les tentatives de connexions
- ➫ dropper les paquet invalide
- ➫ dropper une plage d'adresse (à titre d'exemple , indiquer une plage que vous avez ciblé.)

REJECT et **DROP** ont un comportement différent, **REJECT** renvoie un message d'interdiction donc ça répond, alors que **DROP** jette les packets sans envoyer de réponse.

1.2) Lister les règles

```
$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 2 packets, 152 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 2 packets, 152 bytes)
 pkts bytes target     prot opt in     out     source
destination
```

1.2.1) Commande

```
sudo iptables -A INPUT -j REJECT
sudo iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j DROP
sudo iptables -A FORWARD -j REJECT
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT
sudo iptables -A INPUT  -p tcp -m multiport --dports 22,80,443 -j ACCEPT
sudo iptables -A OUTPUT -p tcp -m multiport --sports 22,80,443,53 -j ACCEPT
sudo iptables -A INPUT -p tcp -m multiport --dport 80,443 -m limit --limit
100/minute --limit-burst 200 -j ACCEPT
sudo iptables -A INPUT -i eth0 -j LOG --log-prefix "IPtables dropped packets:"
sudo iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables
denied: " --log-level 7
sudo iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
sudo iptables -A INPUT -s xxx.xxx.xxx.xxx/xx -j DROP
```

1.2.2) Rechercher dans les logs

➪

Rechercher les packets droppés `sudo grep "IPtables dropped packets:" /var/log/messages`

➪

Rechercher les tentatives de logs `sudo grep "iptables denied: " /var/log/auth.log` ## save and restore

Précédement nous avons entré nos commandes *iptables* une à une, il nous faut les sauver , puis indiquer que l'on souhaite restaurer la configuration lors d'un redémarrage (nuance: en réalité les règles sont restauré aprés le boot, qui lui contient dèjà une configuration au niveau du noyaux, avec *iptables*, nous utilisons donc un "logiciel").
Les commandes indiquent de : * sauver les règles * créer notre script *iptables* * le rendre executable * y ecrire l'entête du script (interpréteur) * y ecrire la commande de restauration (/sbin/iptables-restore) en lui passant les règles.

```
# iptables-save > /etc/iptables.up.rules
# touch /etc/network/if-pre-up.d/iptables
# chmod +x /etc/network/if-pre-up.d/iptables
# echo "#! /bin/bash" >> /etc/network/if-pre-up.d/iptables
# echo "/sbin/iptables-restore < /etc/iptables.up.rules" >> /etc/network/if-pre-up.d/iptables
```