Exemple règles Iptables

sécurité, firewall, iptables

Méthode iptables

Un exemple de règles iptables. La logique est que par défaut tout est ouvert, et il faut commencer par vider toutes les tables pour réinitialiser les règles, puis tout bloquer, puis définir nos règles.

```
#Réinitialiser toutes les règles :
iptables -t filter -F
iptables -t filter -X

#Tout bloquer :
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT DROP

#Autoriser localhost:
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

#Autoriser les connexions déjà établies :
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#Ouverture port HTTP 80 et HTTPS 443 pour serveur web :
iptables -t filter -A OUTPUT -p tcp --dport 80 -j DROP
iptables -t filter -A INPUT -p tcp --dport 80 -j DROP
iptables -t filter -A OUTPUT -p tcp --dport 443 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT

#Autoriser ping :
iptables -t filter -A INPUT -p icmp -j ACCEPT
iptables -t filter -A OUTPUT -p icmp -j ACCEPT

#Ouverture port SSH 22 :
iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT

#Ouverture port DNS 53:
iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

# Mail SMTP :
iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 25 -j ACCEPT

# Mail POP3 :
```

```
iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 110 -j ACCEPT

# Mail IMAP :
iptables -t filter -A INPUT -p tcp --dport 143 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 143 -j ACCEPT

# NTP (serveur de temps) :
iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT

#Ouverture port DHCP 68 :
iptables -t filter -A OUTPUT -p udp --dport 68 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 68 -j ACCEPT

#Supprimer les règles "ACCEPT all" :
iptables -t filter -D INPUT 1
iptables -t filter -D OUTPUT 1
```

Pour lister les règles :

```
iptables -nvL
```