IPTables

Quelque règles utiles

```
# Uptime Robot
-A INPUT -m iprange --src-range 74.86.158.106-110.0.0.0 -j ACCEPT
-A INPUT -s 46.137.190.132/32 -i eth0 -j ACCEPT
-A INPUT -s 122.248.234.23/32 -i eth0 -j ACCEPT
-A INPUT -s 188.226.183.141/32 -i eth0 -j ACCEPT
-A INPUT -s 178.62.52.237/32 -i eth0 -j ACCEPT
-A INPUT -s 54.79.28.129/32 -i eth0 -j ACCEPT
-A INPUT -s 54.94.142.218/32 -i eth0 -j ACCEPT
-A INPUT -s 104.131.107.63/32 -i eth0 -j ACCEPT
-A INPUT -s 54.67.10.127/32 -i eth0 -j ACCEPT
-A INPUT -s 54.64.67.106/32 -i eth0 -j ACCEPT
# Spoofing
-A INPUT -s 10.0.0.0/8 -j DROP
-A INPUT -s 169.254.0.0/16 -j DROP
-A INPUT -s 172.16.0.0/12 -j DROP
-A INPUT -s 127.0.0.0/8 -j DROP
-A INPUT -s 192.168.0.0/24 -j DROP
-A INPUT -s 224.0.0.0/4 -j DROP
-A INPUT -d 224.0.0.0/4 -j DROP
-A INPUT -s 240.0.0.0/5 -j DROP
-A INPUT -d 240.0.0.0/5 -j DROP
-A INPUT -s 0.0.0.0/8 -j DROP
-A INPUT -d 0.0.0.0/8 -j DROP
-A INPUT -d 255.255.255.255 -j DROP
# DNS
-A INPUT -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
# Ping
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
# SMURF
-A INPUT -p icmp -m icmp --icmp-type address-mask-request -j DROP
-A INPUT -p icmp -m icmp --icmp-type timestamp-request -j DROP
# flooding of RST packets, smurf attack Rejection
-A INPUT -p tcp -m tcp --tcp-flags RST RST -m limit --limit 2/second --
limit-burst 2 -j ACCEPT
# Invalid
-A INPUT -m state --state INVALID -j DROP
# Portscan
-N PORT_SCANNING
-A PORT_SCANNING -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s
-j RETURN
-A PORT_SCANNING -j DROP
# Bad
-A INPUT -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
```

```
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
-A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
-A INPUT -p tcp -m tcp --tcp-flags FIN,RST FIN,RST -j DROP
-A INPUT -p tcp -m tcp --tcp-flags FIN,ACK FIN -j DROP
-A INPUT -p tcp -m tcp --tcp-flags ACK,URG URG -j DROP
# XMAS
-A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
-A INPUT -p tcp --tcp-flags ALL ALL -j DROP
# NULL
-A INPUT -p tcp --tcp-flags ALL NONE -j DROP
# Drop
-A INPUT  -j DROP
-A FORWARD -j DROP
-A OUTPUT -p icmp --icmp-type 8 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state INVALID -j DROP
```

Nettoyer tout

Méthode 1

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
```

Méthode 2

```
iptables --flush
```