Delete (Flush) existing rules

iptables –F

## Set the default chain policies

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT DROP

## Show status of your firewall

## iptables -L -n -v --line-numbers

## Block an IP address

## iptables -A INPUT -s 1.2.3.4 -j DROP

## Block access to remote site

## iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP

## iptables -A OUTPUT -p tcp -d facebook.com -j DROP

## Allow ping from the outside

## iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

## iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

## Allow ping to the outside

## iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

## iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

## Allow all incoming SSH tunnels to eth0

## iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

## iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

## Allow incoming SSH tunnels only from a specific source

iptables -A INPUT -i eth0 -p tcp -s 192.168.0.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

## Allow HTTP web traffic

iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

## Load balance web traffic

iptables -A PREROUTING -p tcp --dport 80 -m state -m nth --every 3 --packet 0 -j DNAT --to-destination 10.0.0.4

iptables -A PREROUTING -p tcp --dport 80 -m state -m nth --every 3 --packet 1 -j DNAT --to-destination 10.0.0.5

iptables -A PREROUTING -p tcp --dport 80 -m state -m nth --every 3 --packet 2 -j DNAT --to-destination 10.0.0.6

## Allow outbound DNS

iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT

iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT

## Allow email traffic (inbound SMTP)

iptables -A INPUT -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT

## Allow inbound POP3

iptables -A INPUT -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT

## Port forwarding

## iptables -t nat -A PREROUTING -p tcp -d 1.2.3.4 --dport 422 -j DNAT --to 192.168.0.100:22