Table of Contents

Flush changes.....2
Drop all traffic.....2
Allow incoming ssh.....2
Allow outgoing ssh.....2
Allow ssh from specific network...2
Allow ssh Outgoing specific network 2
Allow web traffic.....3
Allow web ssl traffic.....3
Allow ping response.....3
Allow ping request.....3
Using multiport.....3
New Chain with limitation.....3
Nating.....4
Routing.....4

Flush changes

```
# iptables -F
```

Drop all traffic

```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
# iptables -P OUTPUT DROP
```

Allow incoming ssh

```
# 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 outgoing ssh

```
# iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state
--state ESTABLISHED -j ACCEPT
# iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

Allow ssh from specific network

```
# iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --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 ssh Outgoing specific network

```
# iptables -A OUTPUT -o eth0 -p tcp -d 192.168.100.0/24
--dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state
ESTABLISHED -j ACCEPT
```

Allow web traffic

```
# iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state
--state ESTABLISHED -j ACCEPT
```

Allow web ssl traffic

```
# iptables -A INPUT -i eth0 -p tcp --dport 443 -m state
--state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state
--state ESTABLISHED -j ACCEPT
```

Allow ping response

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

Allow ping request

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

Using multiport

```
# iptables -A INPUT -i eth0 -p tcp -m multiport --dports
22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports
22,80,443 -m state --state ESTABLISHED -j ACCEPT
```

New Chain with limitation

```
# iptables -N SSH
# iptables -A INPUT -p tcp --dport 22 ! --syn -j ACCEPT
# iptables -A INPUT -p tcp --dport 22 --syn -j SSH
# iptables -A SSH -s 192.168.0.0/27 -j ACCEPT
# iptables -A SSH -m limit --limit 5/s -j LOG
# iptables -A SSH -j DROP
```

Nating

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
route add  -net  192.56.76.0  netmask  255.255.255.0 metric
1024 dev eth0
```

Routing

```
//router
# echo “1” > /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# iptables -A FORWARD -i eth1 -j ACCEPT
//client
# route add default gw 192.168.1.200
```