

Permit multicasts

```
iptables -A FORWARD -m pkttype --pkt-type multicast -j ACCEPT
```

Log Dropped Packets

```
iptables -N LOGGING
```

```
iptables -A INPUT -j LOGGING
```

```
iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables Packet Dropped: " --log-level 7
```

```
iptables -A LOGGING -j DROP
```

Port Forwarding

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.102.37 --dport 422 -j DNAT --to 192.168.102.37:22
```

```
iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
ACCEPT iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state ESTABLISHED -j ACCEPT
```

Prevent DoS Attack

```
iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

Combine Multiple Rules Together using MultiPorts

```
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
```

Enable access to internet to other LAN hosts

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
iptables -A FORWARD -i eth1 -j ACCEPT
```

Allow Incoming SSH only from a 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 Incoming HTTP and HTTPS

```
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
```

```
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 Outgoing SSH

```
iptables -A OUTPUT -o eth0 -p tcp --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 Ping from Inside to Outside

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

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

Allow Ping from Outside to Inside

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

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

Load Balance Incoming Web Traffic

```
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every 3 --packet 0 -j DNAT --to-destination 192.168.1.101:443
```

```
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every 3 --packet 1 -j DNAT --to-destination 192.168.1.102:443
```

```
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every 3 --packet 2 -j DNAT --to-destination 192.168.1.103:443
```

Allow Outgoing HTTPS

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

```
iptables -A INPUT -i eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

Allow Outgoing SSH only to a 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 Loopback Access

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A OUTPUT -o lo -j ACCEPT
```

Allow Internal Network to External network.

```
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

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
```



By **Arest (arest)**
cheatography.com/arest/

Not published yet.
Last updated 21st May, 2023.
Page 1 of 2.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>

Allow Rsync From a Specific Network

```
iptables -A INPUT -i eth0 -p tcp -s 192.16-  
8.101.0/24 --dport 873 -m state --state  
NEW,ESTABLISHED -j ACCEPT  
  
iptables -A OUTPUT -o eth0 -p tcp --sport  
873 -m state --state ESTABLISHED -j  
ACCEPT
```

MySQL connection only from a specific network

```
iptables -A INPUT -i eth0 -p tcp -s 192.16-  
8.100.0/24 --dport 3306 -m state --state  
NEW,ESTABLISHED -j ACCEPT  
  
iptables -A OUTPUT -o eth0 -p tcp --sport  
3306 -m state --state ESTABLISHED -j  
ACCEPT
```

Allow IMAPS traffic

```
iptables -A INPUT -i eth0 -p tcp --dport 993  
-m state --state NEW,ESTABLISHED -j  
ACCEPT  
  
iptables -A OUTPUT -o eth0 -p tcp --sport  
993 -m state --state ESTABLISHED -j  
ACCEPT
```

Allow POP3 and POP3S

```
iptables -A INPUT -i eth0 -p tcp --dport 110  
-m state --state NEW,ESTABLISHED -j  
ACCEPT  
  
iptables -A OUTPUT -o eth0 -p tcp --sport  
110 -m state --state ESTABLISHED -j  
ACCEPT
```

Allow POP3S access

```
iptables -A INPUT -i eth0 -p tcp --dport 995  
-m state --state NEW,ESTABLISHED -j  
ACCEPT  
  
iptables -A OUTPUT -o eth0 -p tcp --sport  
995 -m state --state ESTABLISHED -j  
ACCEPT
```



By **Arest** (arest)
cheatography.com/arest/

Not published yet.
Last updated 21st May, 2023.
Page 2 of 2.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>