

Iptables Cheat Sheet

Iptables is a Linux kernel-level module allowing us to perform various networking manipulations (i.e. packet filtering) to achieve better network security.

View All Current Iptables Rules:

```
iptables -L -v
```

View All INPUT Rules:

```
iptables -L INPUT -nv
```

How To Block An IP Address Using Iptables:

```
iptables -I INPUT -s "201.128.33.200" -j DROP
```

To Block A Range Of IP Addresses:

```
iptables -I INPUT -s "201.128.33.0/24" -j DROP
```

How To Unblock An IP Address:

```
iptables -D INPUT -s "201.128.33.200" -j DROP
```

How To Block All Connections To A Port:

To block port 25:

```
iptables -A INPUT -p tcp --dport 25 -j DROP  
iptables -A INPUT -p udp --dport 25 -j DROP
```

How To Un-Block:

To enable port 25:

```
iptables -A INPUT -p tcp --dport 25 -j ACCEPT  
iptables -A INPUT -p udp --dport 25 -j ACCEPT
```

To Save All Rules So That They Are Not Lost In Case Of A Server Reboot:

```
/etc/init.d/iptables save
```

Or, alternatively:

```
service iptables save
```

Delete A Rule By Line Number

Output all the ip tables rules with line numbers:

```
iptables -L INPUT -n --line-numbers
```

You'll get the list of all blocked IP. Look at the number on the left, then :

```
iptables -D INPUT [LINE NUMBER]
```

Open Port 3306 (MySQL) To IP 1.2.3.4

```
iptables -I INPUT -i eth0 -s 1.2.3.4 -p tcp --destination-port 3306 -j ACCEPT -m comment --comment " MySQL Access By IP "
```

ADD RULE with PORT and IPADDRESS

```
sudo iptables -A INPUT -p tcp -m tcp --dport port_number -s ip_address -j ACCEPT
```

ADD RULE for PORT on all addresses

```
sudo iptables -A INPUT -p tcp -m tcp --dport port_number --sport 1024:65535 -j ACCEPT
```

DROP IPADDRESS

```
sudo iptables -I INPUT -s x.x.x.x -j DROP
```

VIEW IPTABLES with rule numbers

```
sudo iptables -L INPUT -n --line-numbers
```

REMOVE A RULE

#Use above command and note rule_number

```
sudo iptables -D INPUT rule_number
```

#DEFAULT POLICY

```
-P INPUT DROP
```

```
-P OUTPUT DROP
```

```
-P FORWARD DROP
```

```
-A INPUT -i lo -j ACCEPT #allow lo input
```

```
-A OUTPUT -o lo -j ACCEPT #allow lo output
```

```
-A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables-INPUT denied: " --log-level 7 #log INPUT Denied
```

```
-A OUTPUT -m limit --limit 5/min -j LOG --log-prefix "iptables-OUTPUT denied: " --log-level 7 #log OUTPUT Denied
```

```
#ALLOW OUTPUT PING/MTR (or traceroute -I, traceroute by default uses UDP - force with ICMP)
```

```
-A OUTPUT -p icmp --icmp-type 8 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
-A INPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
-A INPUT -p icmp --icmp-type 11 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
#ALLOW INPUT PING/MTR
```

```
-A INPUT -p icmp --icmp-type 8 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
-A OUTPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
#ALLOW OUTPUT
```

```
-A OUTPUT -p tcp -m multiport --dports 80,443 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
-A INPUT -p tcp -m multiport --sports 80,443 -m state --state ESTABLISHED -j ACCEPT
```

```
-A OUTPUT -p udp -m multiport --dports 53,123 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
-A INPUT -p udp -m multiport --sports 53,123 -m state --state ESTABLISHED -j ACCEPT
```