

Iptables Lab

Installation:

Install iptables rpm package from the Redhat distribution CD.
It may also be installed by default during Redhat installation.

```
# rpm -ivh iptables-1.2.5-3.rpm
```

Using Iptables:

1. To view all iptables command line options:

```
# iptables -h
```

2. To list all current default rules/chains:

```
# iptables -L
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

3. To set the default policies for all chains:

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

# iptables -L

Chain INPUT (policy DROP)
target     prot opt source                destination

Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
```

Now, all packets will be dropped – no network traffic to/from the host
The default policy should be to DROP all packets not matched by any rules/chains.

4. To allow ping to work to/from your host to anywhere

```
# iptables -A INPUT -p ICMP -j ACCEPT
# iptables -A OUTPUT -p ICMP -j ACCEPT
```

List the iptables rules now:

```
# iptables -L
```

```
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     icmp -- anywhere             anywhere
```

```
Chain FORWARD (policy DROP)
target     prot opt source                destination
```

```
Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     icmp -- anywhere             anywhere
```

5. To allow ping to work only across the firewall but not to/from it:

Flush the previous FORWARD chain rules:

```
# iptables -F FORWARD
```

Apply the new rule:

```
# iptables -A FORWARD -p ICMP -j ACCEPT
```

List the rules now:

```
# iptables -L --line-numbers
```

```
Chain INPUT (policy DROP)
num target     prot opt source                destination
```

```
Chain FORWARD (policy ACCEPT)
num target     prot opt source                destination
1  ACCEPT      icmp -- anywhere             anywhere
```

```
Chain OUTPUT (policy DROP)
num target     prot opt source                destination
```

6. To allow all internal users to access websites on the Internet:

```
# iptables -A FORWARD -i eth1 -o eth0 -p tcp --dport 80 -j ACCEPT
# iptables -A FORWARD -i eth0 -o eth1 -p tcp -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Note: eth0 = outside interface, eth1 = inside interface

7. To allow some external users access to SSH, SMTP, POP, HTTP, DNS servers in your internal network:

Inbound FORWARD rules:

```
# iptables -A FORWARD -s 202.52.250.0/24 -d 202.52.255.1 -i eth0 -o eth1 -p tcp --dport 22 -j ACCEPT

# iptables -A FORWARD -s 202.52.250.0/24 -d 202.52.255.3 -i eth0 -o eth1 -p tcp --dport 25 -j ACCEPT

# iptables -A FORWARD -s 202.52.250.0/24 -d 202.52.255.6 -i eth0 -o eth1 -p tcp --dport 110 -j ACCEPT

# iptables -A FORWARD -s 202.52.250.0/24 -d 202.52.255.35 -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT

# iptables -A FORWARD -s 202.52.250.0/24 -d 202.52.255.47 -i eth0 -o eth1 -p udp -dport 53 -j ACCEPT
```

Outbound FORWARD rules:

```
# iptables -A FORWARD -s 202.52.255.0/24 -i eth1 -o eth0 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

# iptables -A FORWARD -s 202.52.255.0/24 -i eth1 -o eth0 -p udp -m state --state ESTABLISHED -j ACCEPT
```

8. To view all current rules with numeric addresses:ports and rule line numbers:

```
# iptables -L -n --line-numbers
```

9. To save all rules/chains to /etc/sysconfig/iptables to make permanent:

```
# service iptables save
```

10. To stop iptables and flush all rules:

```
# service iptables stop
```

11. To start and all saved rules:

```
# service iptables start
```

12. To load iptables at every system startup:

```
# chkconfig iptables on
```

NAT exercises:

1. Fixed IP address mapping (inbound) - maps the public IP of a server to the private IP of the internal server

```
# iptables -t -nat -A PREROUTING -i eth1 -d 202.52.255.5 -j DNAT -to-destination 192.168.0.1
```

2. Port mapping (inbound) - maps port 80 of host with IP 202.52.255.5 to port 8080 of the internal host having IP 192.168.14.2

```
# iptables -t -nat -A PREROUTING -i eth0 -d 202.52.255.5 -p tcp -m tcp -dport 80 -j DNAT -to-destination 192.168.0.1:8080
```

3. IP Masquerading (outbound) - translates the source IP of all outbound packets to 202.52.255.5, the IP of eth0

```
# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

4. SNAT (outbound) - The source IP of all outbound packets will be converted to 202.52.255.5

```
# iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24 -j SNAT -to-source 202.52.255.5
```

5. Fixed IP mapping (outbound) - The source IP of 192.168.10.11 will be converted to 202.52.255.5 while exiting from eth0

```
# iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.11 -j SNAT -to-source 202.52.255.5
```