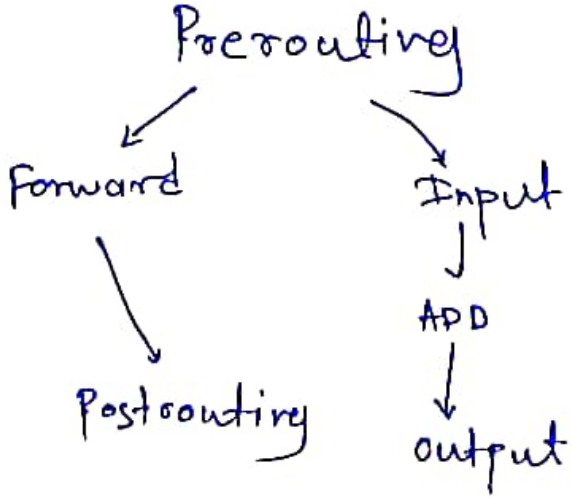
IP tables:- Installation

```
# systemctl stop firewalld.service
# systemctl disable firewalld.service
# yum install iptables-services iptables-utils
# systemctl start iptables
# systemctl enable iptables
```

```
# iptables -L → List
# iptables -t filter -L → 3 stages
# iptables -t nat -L → 4 stages
# iptables -t mangle -L → All 5 chains
# iptables -t raw -L → 2 chains
# iptables --flush → Flush the data from filter
# iptables -P FORWARD DROP → chain forward=DROP
# iptables -D INPUT 2 → It will delete line 2 from INPUT RULE
```



IP forwarding:-

cat /proc/sys/net/ipv4/ip_forward

↳ ~~total~~ 0 (if it is 0 add 1 in it)

echo 1 > /proc/sys/net/ipv4/ip_forward

vi /etc/sysctl.conf

↳ net.ipv4.ip_forward = 1

iptable -F

iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -o ens33 -j MASQUERADE

Assignment :- Allow these sites only

Client 1	client 2	For all
youtube	Azure	google.
microsoft	Heroku ~~sit~~	wikipedia
cisco	redhat	centos.
Aws cloud		

all other site block.

iptables -A FORWARD -s 10.10.10.130 -d www.youtube.com -p tcp --dport=443 -j ACCEPT

iptables -A FORWARD -d 10.10.10.130 -s www.youtube.com -p tcp --sport=443 -j ACCEPT

iptables -L

Now client 1 is able to access youtube.com

DNS Rule

```
# iptables -A ~~forw~~ FORWARD -s 10.10.10.0/24 -s
  192.168.44.2 -p Udp --dport 53 -j ACCEPT
# iptables -A FORWARD -d 10.10.10.0/24 -d
  192.168.44.2 -p Udp --sport 53 -j ACCEPT
```

network ip

dns

Stateful Packet inspection firewall :-

```
# iptables -A FORWARD -s 10.10.10.130 -d www.youtube
  .com -p tcp --dport=443 -m state --state
  NEW,ESTABLISHED -j ACCEPT

# iptables -A FORWARD -d 10.10.10.130 -s www.youtube
  .com -p tcp --sport=443 -m state --state
  NEW,ESTABLISHED -j ACCEPT
```

Block pinging from another ip

```
# iptables -A INPUT -d 192.168.44.138 -p ICMP
  --icmp-type echo-request -j DROP
```

~~Port~~ Packate limit

```
# iptables -A INPUT -d 192.168.44.138 -p ICMP
  -m limit --limit 5/s -j ACCEPT
```

Ping maximum limit upto 256 bytes packets

ping -l 256 nat ip

Block internet of client machine

iptables -A INPUT -i eny33 -p

client ip ftpserver

iptables -A FORWARD -s 192.168.72.10 -d 172.16.0.1 -p tcp --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

-m limit — allow you to specify no. of packets to be accepted per second

-m length — allow you to specify length of the packet to be accepted