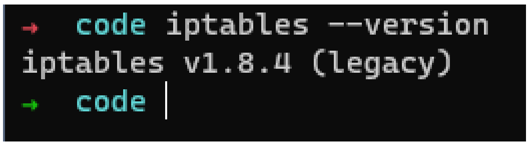
NSS Assignment

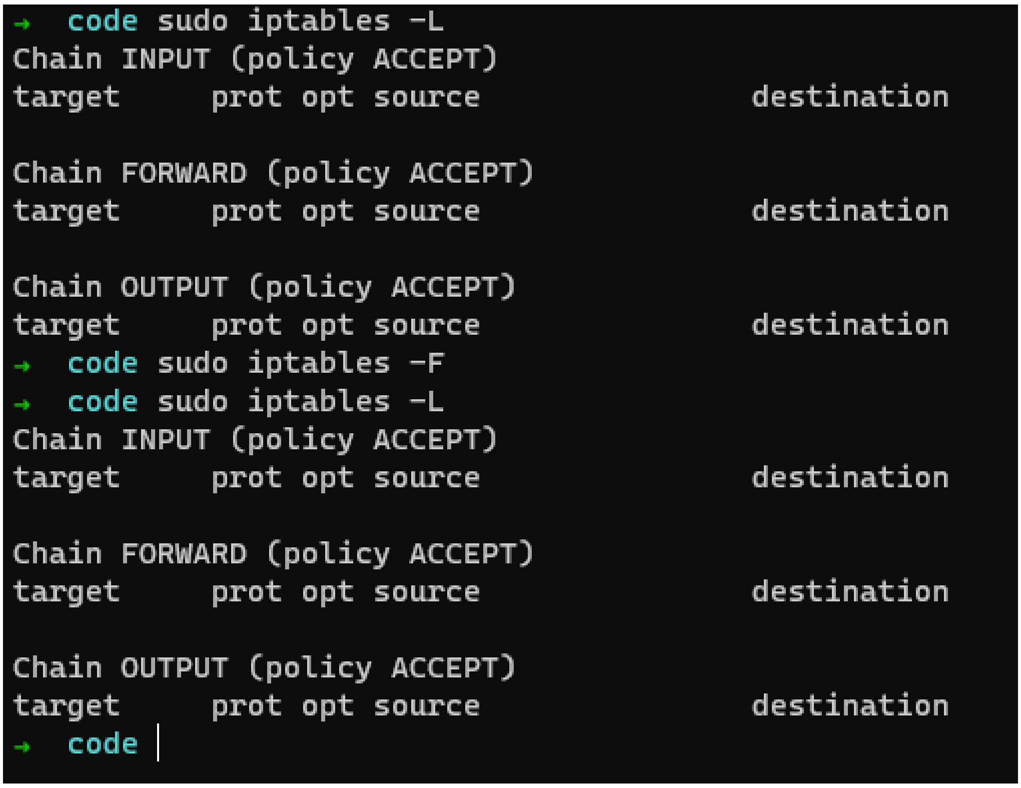
SAHIL BONDRE U18CO021

1. **Check if iptables are installed in your linux system or not. If not install it.**



```
→  code iptables --version
iptables v1.8.4 (legacy)
→  code 
```

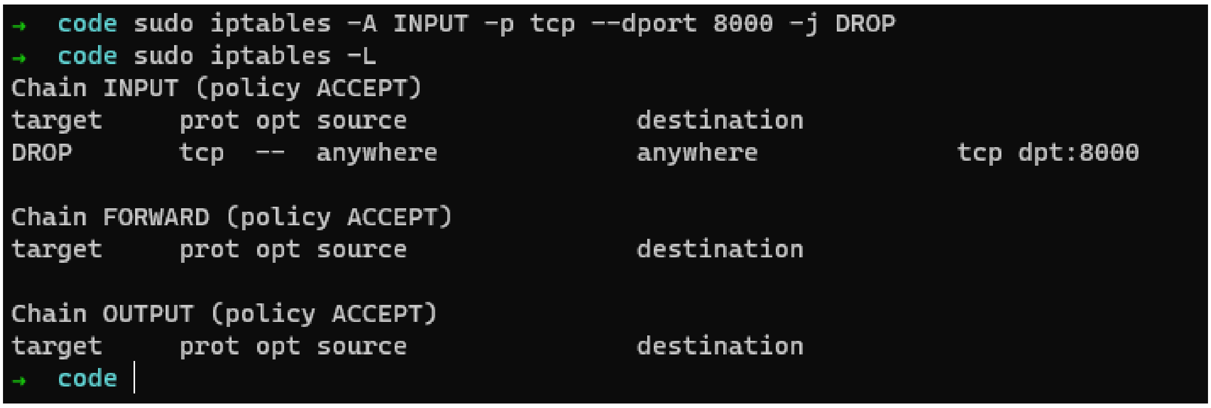
2. **Flush all existing IP tables rules if exists.**



```
→  code sudo 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
→  code sudo iptables -F
→  code sudo 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
→  code 
```

3. **Allow traffic on specific ports.**

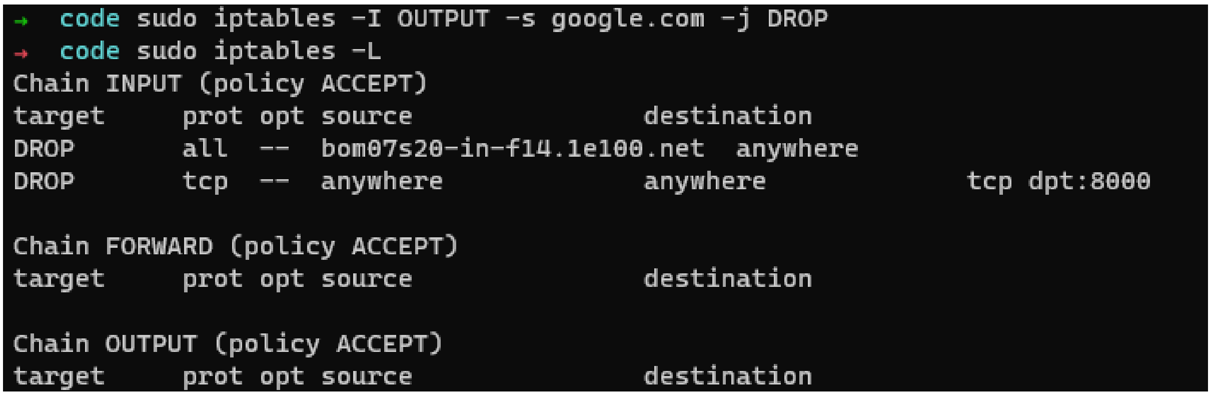
sudo iptables -A INPUT -p tcp --dport 8000 -j DROP



```
→  code sudo iptables -A INPUT -p tcp --dport 8000 -j DROP
→  code sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

4. **Block a particular website from accessing your machine**

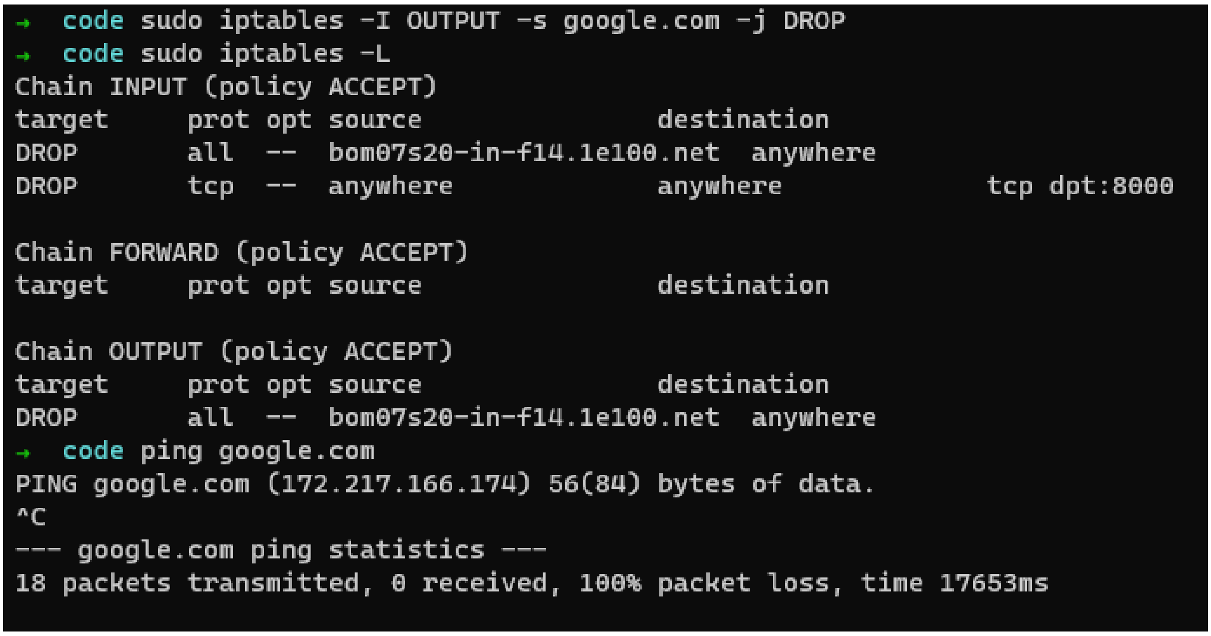
sudo iptables -I INPUT -s google.com -j DROP



```
→  code sudo iptables -I OUTPUT -s google.com -j DROP
→  code sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

5. **Block your machine to access a particular website**

sudo iptables -I OUTPUT -s google.com -j DROP

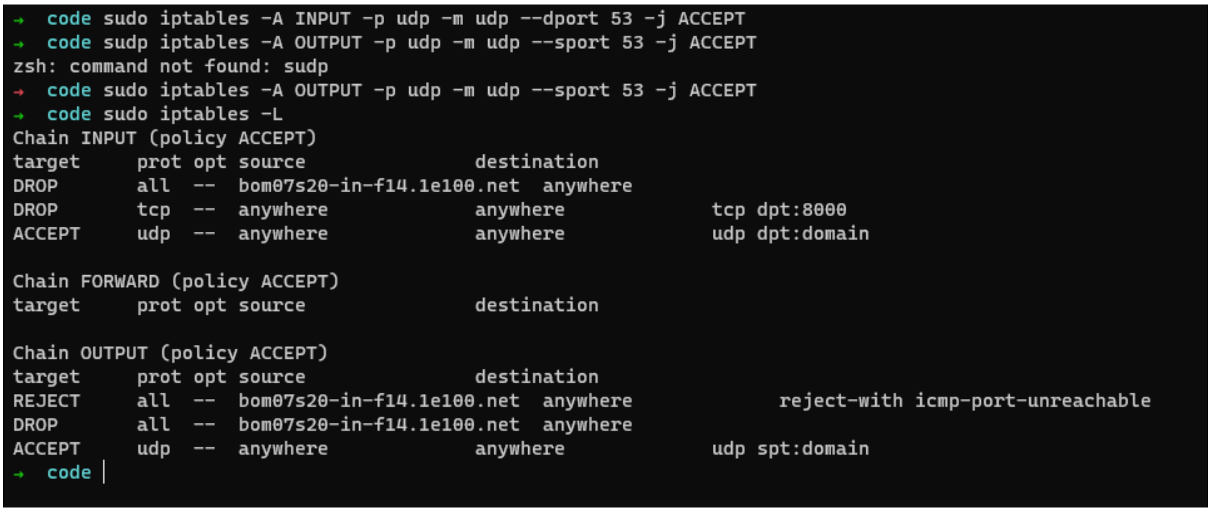


```
→  code sudo iptables -I OUTPUT -s google.com -j DROP
→  code sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
→  code ping google.com
PING google.com (172.217.166.174) 56(84) bytes of data.
^C
--- google.com ping statistics ---
18 packets transmitted, 0 received, 100% packet loss, time 17653ms
```

6. **Allow DNS traffic on input and output chains**

sudo iptables -A OUTPUT -p udp -m udp --sport 53 -j ACCEPT

sudo iptables -A INPUT -p udp -m udp --dport 53 -j ACCEPT

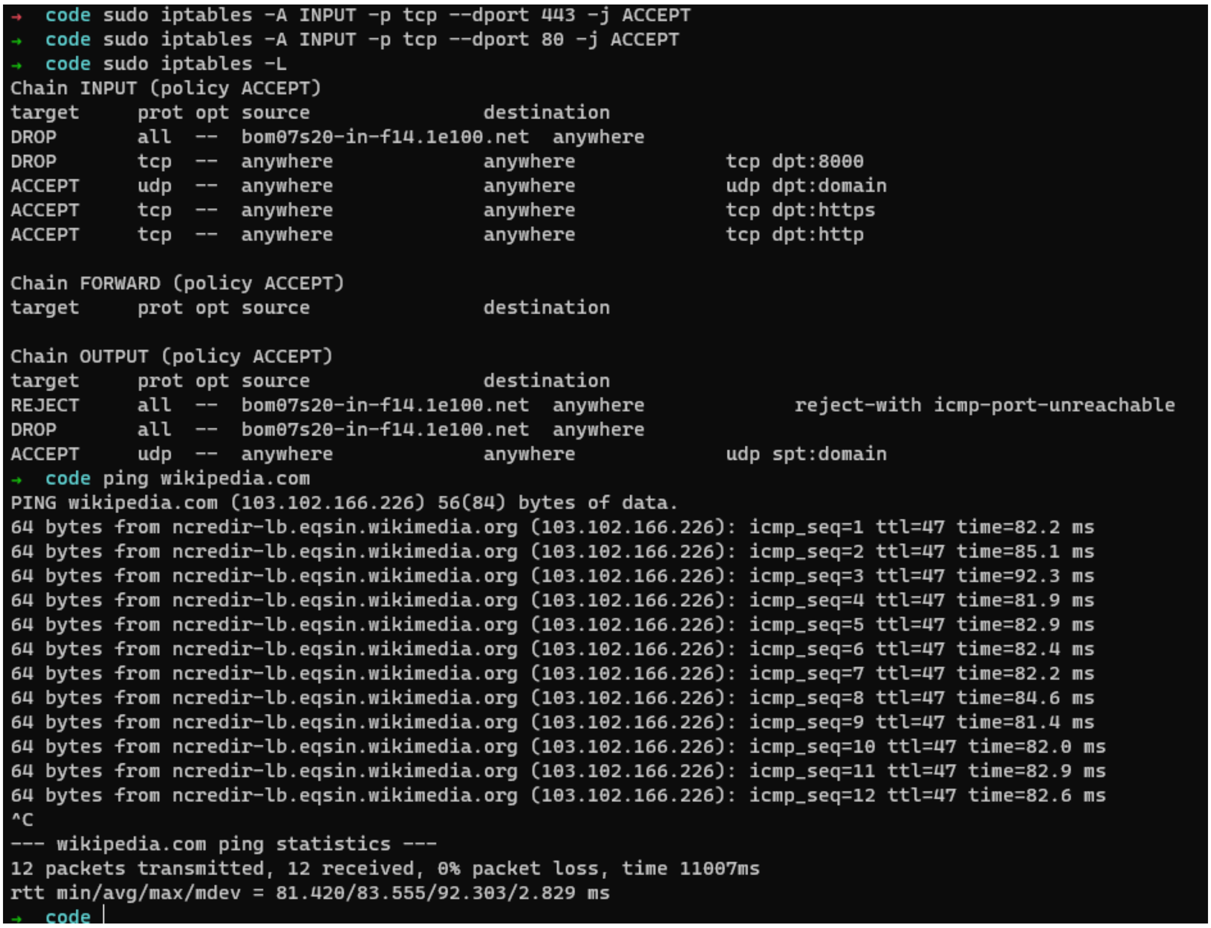


```
→  code sudo iptables -A INPUT -p udp -m udp --dport 53 -j ACCEPT
→  code sudp iptables -A OUTPUT -p udp -m udp --sport 53 -j ACCEPT
zsh: command not found: sudp
→  code sudo iptables -A OUTPUT -p udp -m udp --sport 53 -j ACCEPT
→  code sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  bom07s20-in-f14.1e100.net  anywhere             reject-with icmp-port-unreachable
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
ACCEPT     udp  --  anywhere             anywhere             udp spt:domain
→  code |
```

7. **Accept all HTTP and HTTPS connections**

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

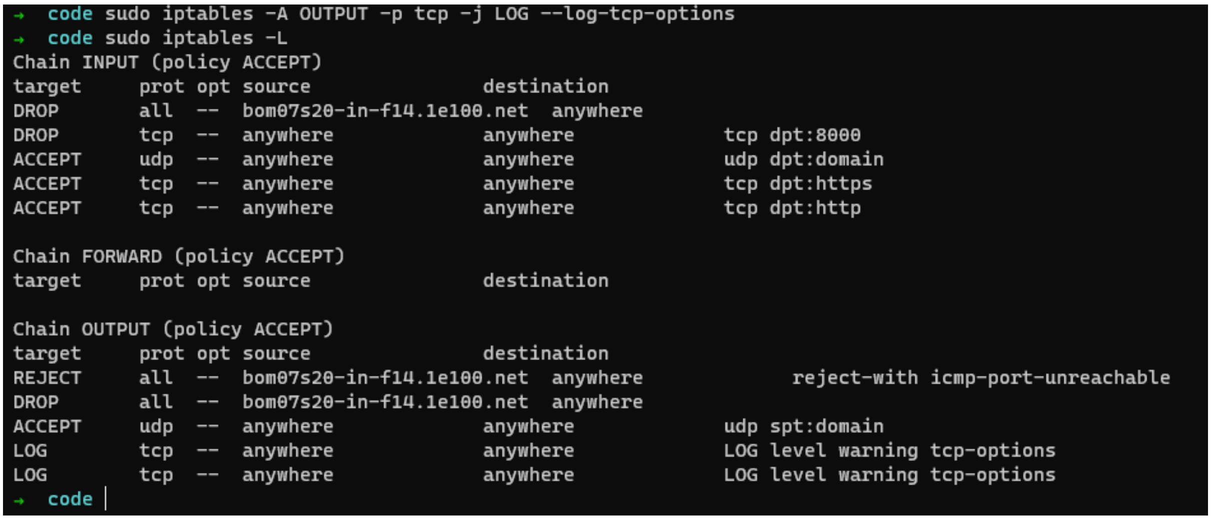
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT



```
→  code sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
→  code sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
→  code sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  bom07s20-in-f14.1e100.net  anywhere             reject-with icmp-port-unreachable
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
ACCEPT     udp  --  anywhere             anywhere             udp spt:domain
→  code ping wikipedia.com
PING wikipedia.com (103.102.166.226) 56(84) bytes of data.
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=1 ttl=47 time=82.2 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=2 ttl=47 time=85.1 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=3 ttl=47 time=92.3 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=4 ttl=47 time=81.9 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=5 ttl=47 time=82.9 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=6 ttl=47 time=82.4 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=7 ttl=47 time=82.2 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=8 ttl=47 time=84.6 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=9 ttl=47 time=81.4 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=10 ttl=47 time=82.0 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=11 ttl=47 time=82.9 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=12 ttl=47 time=82.6 ms
^C
--- wikipedia.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11007ms
rtt min/avg/max/mdev = 81.420/83.555/92.303/2.829 ms
→  code
```

8. **Log all traffic. (use LOG target with –j option)**

sudo iptables -A OUTPUT -p tcp -j LOG --log-tcp-options



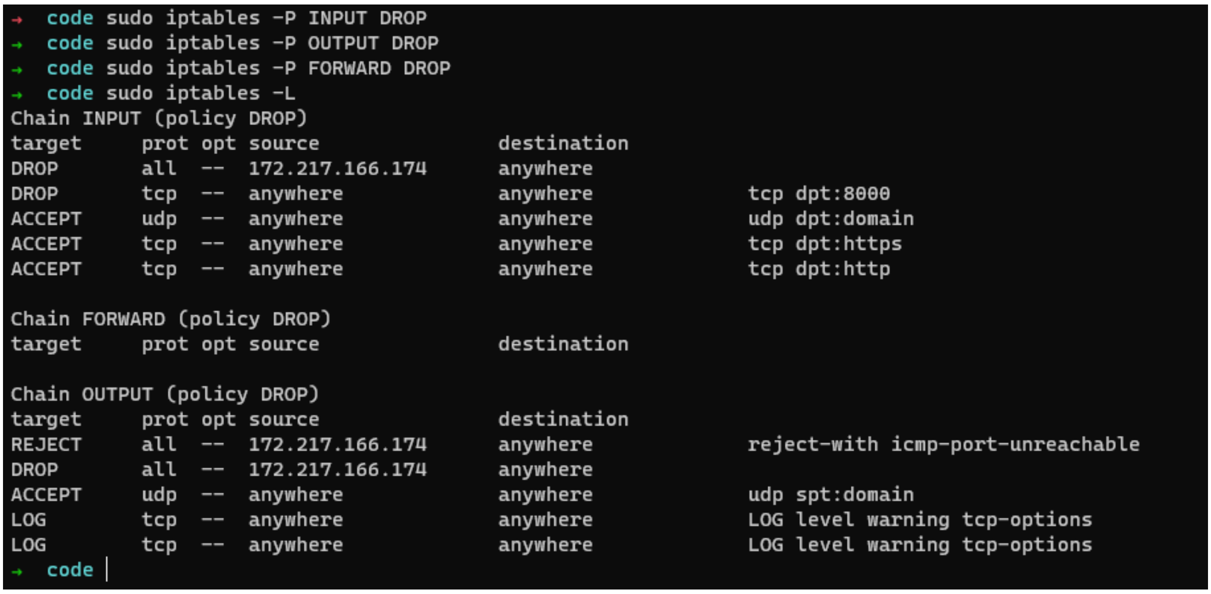
```
→  code sudo iptables -A OUTPUT -p tcp -j LOG --log-tcp-options
→  code sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  bom07s20-in-f14.1e100.net  anywhere             reject-with icmp-port-unreachable
DROP       all  --  bom07s20-in-f14.1e100.net  anywhere
ACCEPT     udp  --  anywhere             anywhere             udp spt:domain
LOG        tcp  --  anywhere             anywhere             LOG level warning tcp-options
LOG        tcp  --  anywhere             anywhere             LOG level warning tcp-options
→  code
```

9. **Change default policy of all iptable chains to DROP policy.**

sudo iptables -P INPUT DROP

sudo iptables -P OUTPUT DROP

sudo iptables -P FORWARD DROP



```
→  code sudo iptables -P INPUT DROP
→  code sudo iptables -P OUTPUT DROP
→  code sudo iptables -P FORWARD DROP
→  code sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       all  --  172.217.166.174      anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:8000
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
REJECT     all  --  172.217.166.174      anywhere             reject-with icmp-port-unreachable
DROP       all  --  172.217.166.174      anywhere
ACCEPT     udp  --  anywhere             anywhere             udp spt:domain
LOG        tcp  --  anywhere             anywhere             LOG level warning tcp-options
LOG        tcp  --  anywhere             anywhere             LOG level warning tcp-options
→  code
```