Network Port Testing

NMAP

> nmap -p <start_port>-<endport> <ip>

Example:

```
> nmap -p 30000-32000 127.0.0.1


Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-23 21:10 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00017s latency).
Not shown: 2000 closed ports
PORT      STATE    SERVICE
30500/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds




> nmap -p 30000-32000 10.250.220.238


Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-23 21:11 UTC
Nmap scan report for kubernetes-devtest-worker1 (10.250.220.238)
Host is up (0.00017s latency).
Not shown: 2000 closed ports
PORT      STATE SERVICE
30500/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

IPTables

iptables -[LS] [chain [rulenum]] [options]

```
Options:
    -4                          ipv4
    -6                         ipv6
        -j target           target for rule (may load target extension)
    -g chain            jump to chain with no return
    -m match            extended match (may load extension)
    -n numeric          output of addresses and ports
    -t table                table to manipulate (default: `filter')
    -v                         verbose mode
    --line-numbers             print line numbers when listing
    -x                         expand numbers (display exact values)
```

> iptables -L INPUT

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
cali-INPUT  all  --  anywhere             anywhere             /* cali:Cz_u1IQiXIMmKD4c */
KUBE-FIREWALL  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
           all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
```

> sudo iptables -S INPUT

```
-P INPUT ACCEPT
-A INPUT -m comment --comment "cali:Cz_u1IQiXIMmKD4c" -j cali-INPUT
-A INPUT -j KUBE-FIREWALL
-A INPUT -j ACCEPT
-A INPUT -i 127.0.0.1 -j ACCEPT
-A INPUT
-A INPUT -i lo -j ACCEPT
```

> sudo iptables -Ln

Modifying iptables to add logging

Save iptables to file

> sudo iptables-save > iptables.txt

Add to *filter target

-A INPUT -j LOG

Restore iptables after modifying

> sudo iptables-restore iptables.txt

View logs: (on ubuntu)

> tail -f /var/log/kern.log

References

Reference	URL
Enable Logging in iptables	https://tecadmin.net/enable-logging-in-iptables-on-linux/