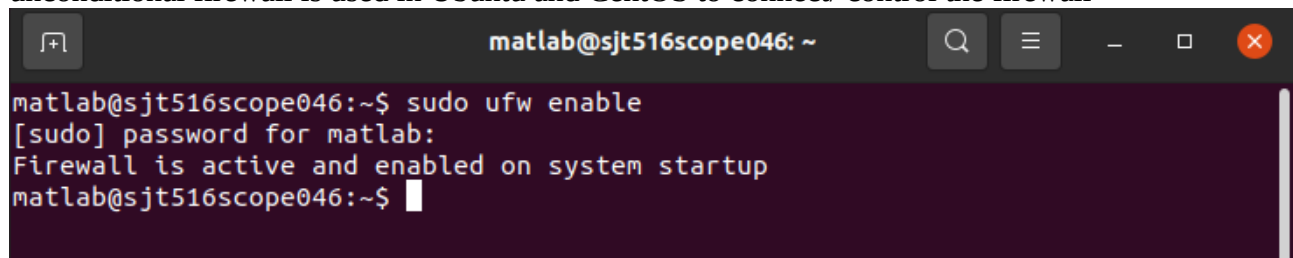


Harshit Srivastava
19BCE0382
Lab Assessment 5
Information Security Management
CSE3502 (Slot: L5+L6)
Winter Sem 2021-22
04/03/2022

\$ sudo ufw enable

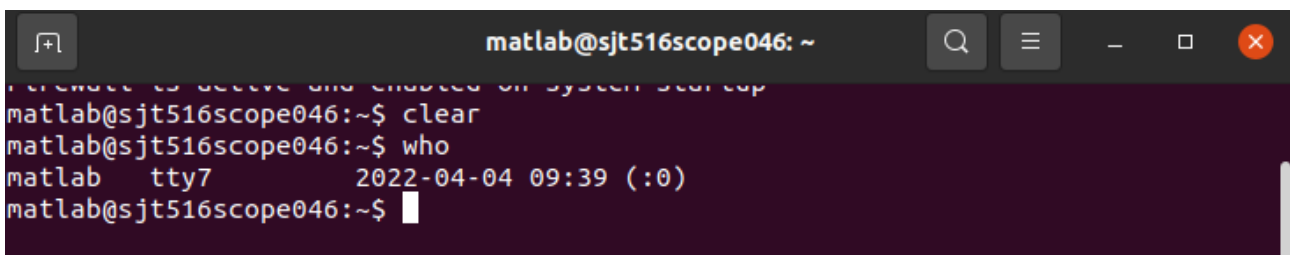
unconditional firewall is used in Ubuntu and CentOS to connect/ control the firewall



```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw enable  
[sudo] password for matlab:  
Firewall is active and enabled on system startup  
matlab@sjt516scope046:~$
```

\$ who

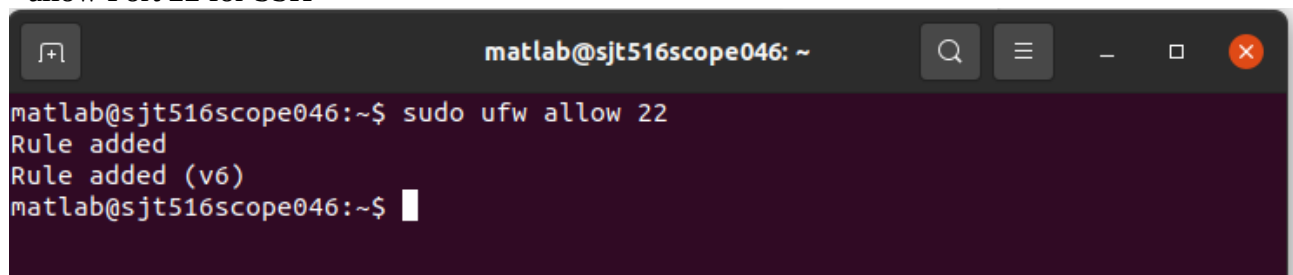
who command is used to print the information of all devices in this network



```
matlab@sjt516scope046:~$ clear  
matlab@sjt516scope046:~$ who  
matlab    tty7          2022-04-04 09:39 (:0)  
matlab@sjt516scope046:~$
```

\$ sudo ufw allow 22

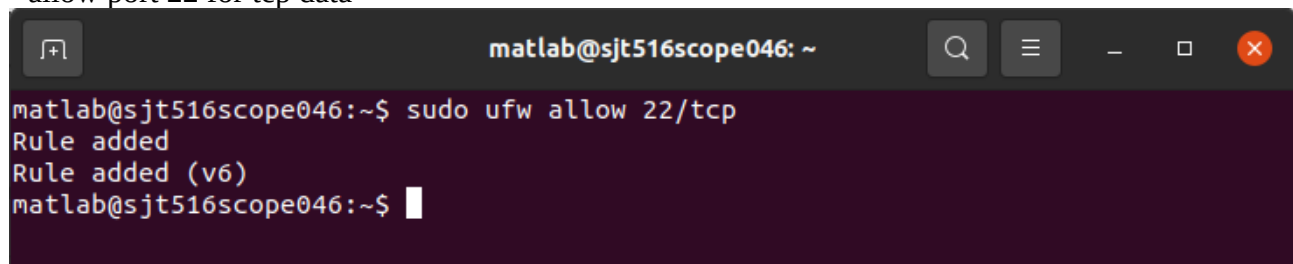
- allow Port 22 for SSH



```
matlab@sjt516scope046:~$ sudo ufw allow 22  
Rule added  
Rule added (v6)  
matlab@sjt516scope046:~$
```

\$ sudo ufw allow 22/tcp

- allow port 22 for tcp data



```
matlab@sjt516scope046:~$ sudo ufw allow 22/tcp  
Rule added  
Rule added (v6)  
matlab@sjt516scope046:~$
```

\$ sudo ufw allow ssh
– port 22 rule already exists

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw allow ssh  
Skipping adding existing rule  
Skipping adding existing rule (v6)  
matlab@sjt516scope046:~$
```

\$ sudo ufw reject out ssh
– Reject outgoing SSH traffic from our machine

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw reject out ssh  
Rule added  
Rule added (v6)  
matlab@sjt516scope046:~$
```

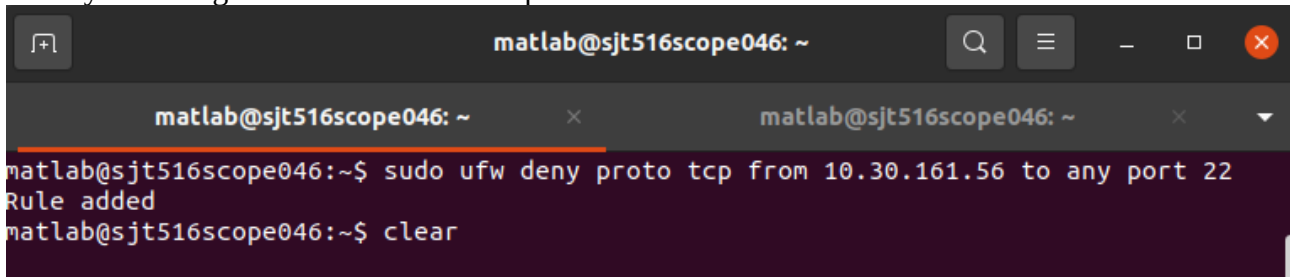
\$ sudo ufw status
– Shows current firewall rules

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw status  
Status: active  
  
To Action From  
--  
22 ALLOW Anywhere  
22/tcp ALLOW Anywhere  
22 (v6) ALLOW Anywhere (v6)  
22/tcp (v6) ALLOW Anywhere (v6)  
  
22/tcp REJECT OUT Anywhere  
22/tcp (v6) REJECT OUT Anywhere (v6)  
  
matlab@sjt516scope046:~$
```

\$ sudo ufw delete reject out ssh
– Delete a rule from firewall

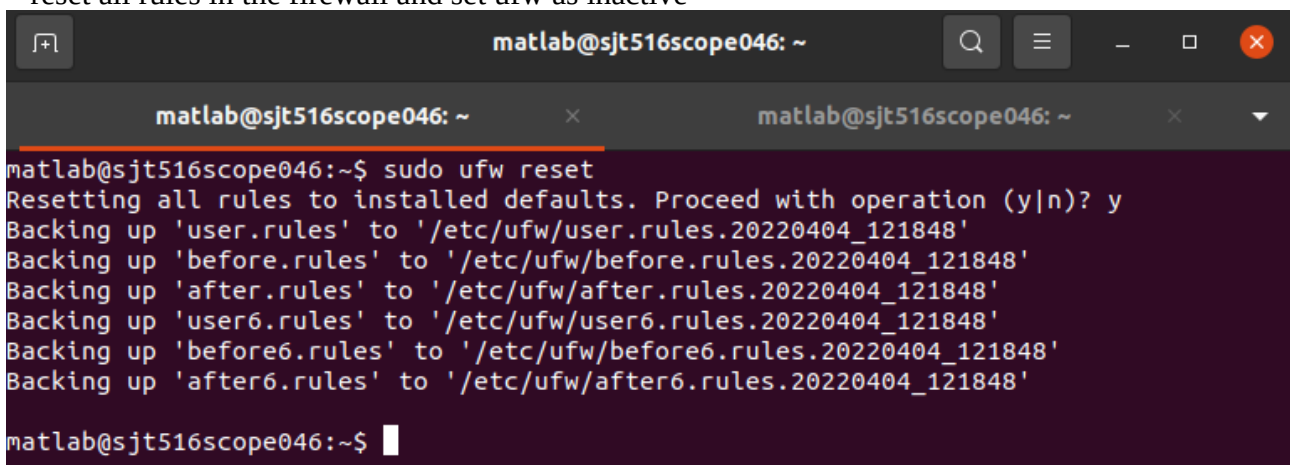
```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw delete reject out ssh  
Rule deleted  
Rule deleted (v6)  
matlab@sjt516scope046:~$
```

\$ sudo ufw deny proto tcp from 10.30.161.56 to any port 22
– Deny incoming traffic form IP to 22/tcp



```
matlab@sjt516scope046: ~  
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw deny proto tcp from 10.30.161.56 to any port 22  
Rule added  
matlab@sjt516scope046:~$ clear
```

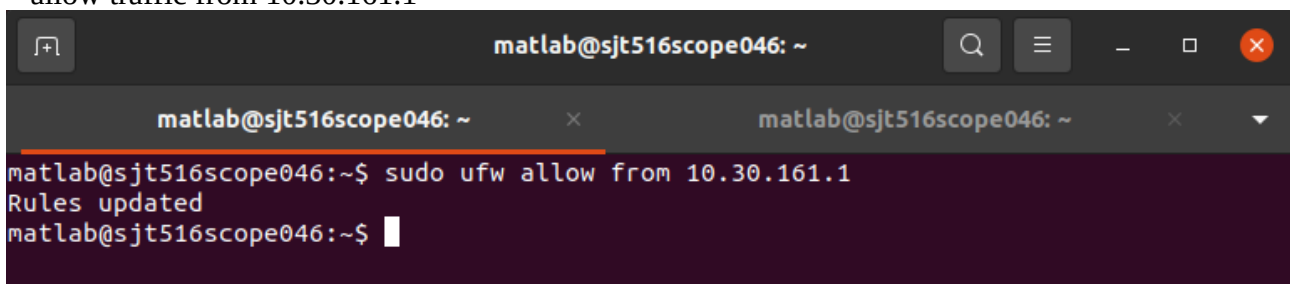
\$ sudo ufw reset
– reset all rules in the firewall and set ufw as inactive



```
matlab@sjt516scope046: ~  
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw reset  
Resetting all rules to installed defaults. Proceed with operation (y|n)? y  
Backing up 'user.rules' to '/etc/ufw/user.rules.20220404_121848'  
Backing up 'before.rules' to '/etc/ufw/before.rules.20220404_121848'  
Backing up 'after.rules' to '/etc/ufw/after.rules.20220404_121848'  
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20220404_121848'  
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20220404_121848'  
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20220404_121848'  
matlab@sjt516scope046:~$
```

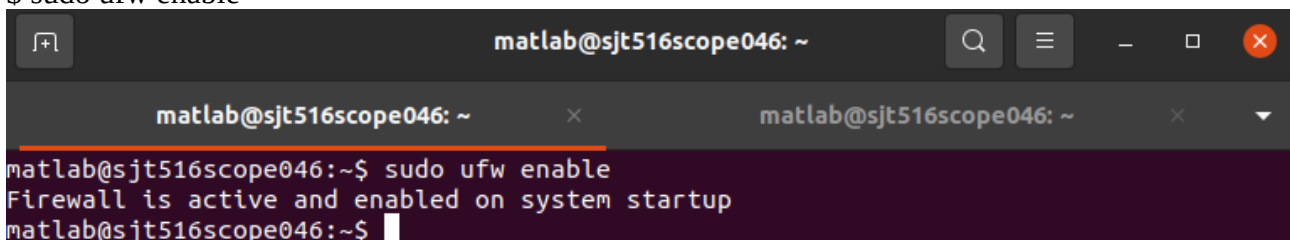
PART 2

\$ sudo ufw allow from 10.30.161.1
– allow traffic from 10.30.161.1



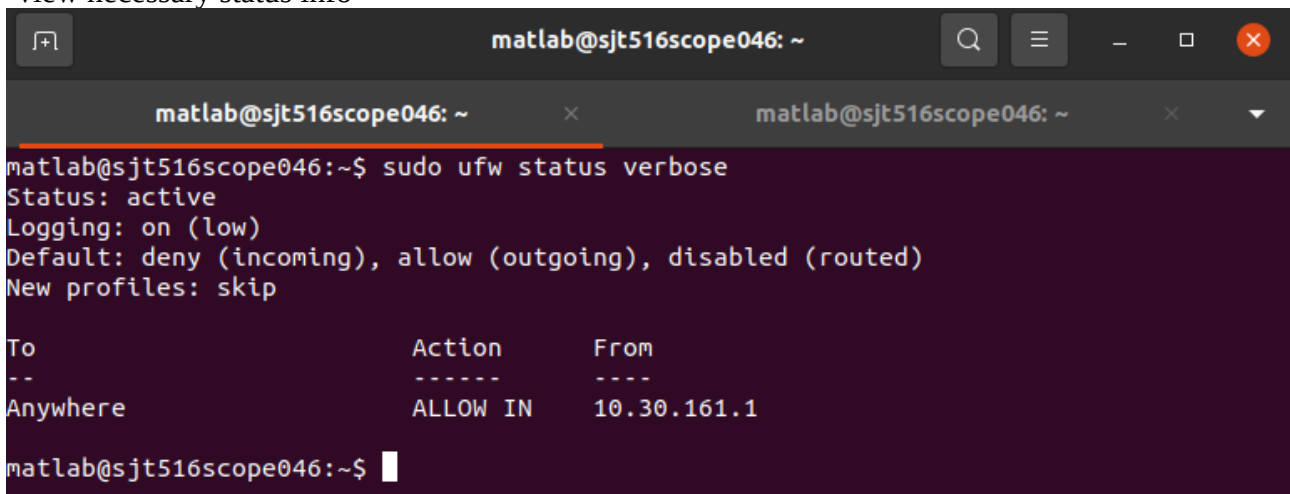
```
matlab@sjt516scope046: ~  
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw allow from 10.30.161.1  
Rules updated  
matlab@sjt516scope046:~$
```

\$ sudo ufw enable



```
matlab@sjt516scope046: ~  
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
matlab@sjt516scope046:~$
```

\$ sudo ufw status verbose
-view necessary status info



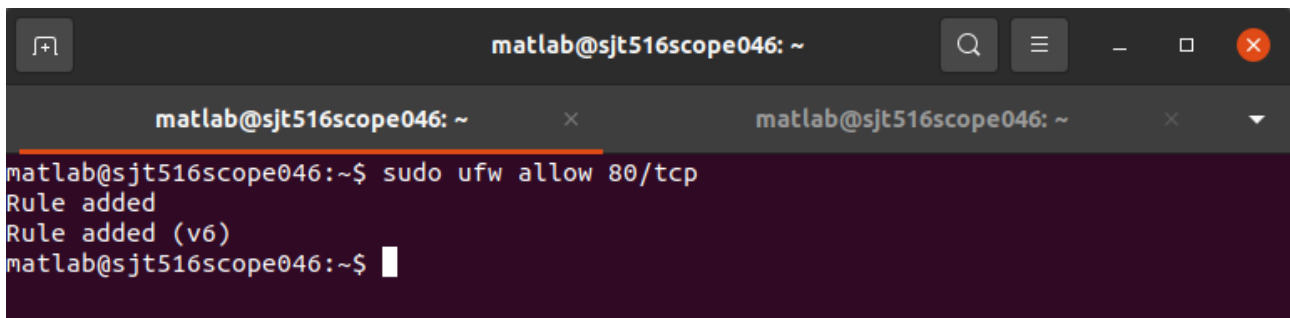
A terminal window titled 'matlab@sjt516scope046: ~' with two tabs. The active tab shows the output of 'sudo ufw status verbose'. The output indicates that UFW is active, logging is on (low), and the default policy is deny for incoming traffic. A single rule is shown: allowing incoming traffic from 10.30.161.1 anywhere.

```
matlab@sjt516scope046:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
Anywhere ALLOW IN 10.30.161.1

matlab@sjt516scope046:~$
```

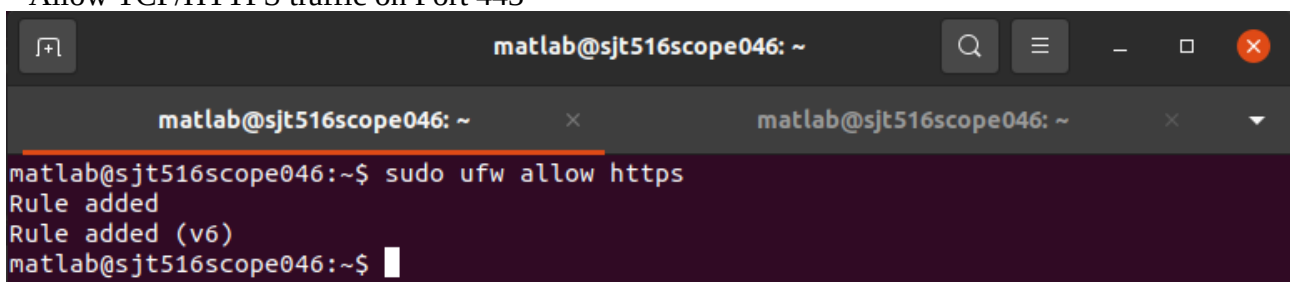
\$ sudo ufw allow 80/tcp
– Allow TCP traffic on port 80



A terminal window titled 'matlab@sjt516scope046: ~' with two tabs. The active tab shows the output of 'sudo ufw allow 80/tcp'. The output indicates that the rule was successfully added for both IPv4 and IPv6.

```
matlab@sjt516scope046:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
matlab@sjt516scope046:~$
```

\$ sudo ufw allow https
– Allow TCP/HTTPS traffic on Port 443



A terminal window titled 'matlab@sjt516scope046: ~' with two tabs. The active tab shows the output of 'sudo ufw allow https'. The output indicates that the rule was successfully added for both IPv4 and IPv6.

```
matlab@sjt516scope046:~$ sudo ufw allow https
Rule added
Rule added (v6)
matlab@sjt516scope046:~$
```

\$ sudo ufw status numbered

– Display status in Numbered form

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw status numbered  
Status: active  
  
      To      Action      From  
      --      -  
[ 1] Anywhere  ALLOW IN    10.30.161.1  
[ 2] 80/tcp    ALLOW IN    Anywhere  
[ 3] 443/tcp    ALLOW IN    Anywhere  
[ 4] 80/tcp (v6) ALLOW IN    Anywhere (v6)  
[ 5] 443/tcp (v6) ALLOW IN    Anywhere (v6)  
matlab@sjt516scope046:~$
```

\$ sudo ufw delete 4

– Delete an entry according to number in table

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw delete 4  
Deleting:  
  allow 80/tcp  
Proceed with operation (y|n)? y  
Rule deleted (v6)  
matlab@sjt516scope046:~$
```

\$ sudo ufw status numbered

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw status numbered  
Status: active  
  
      To      Action      From  
      --      -  
[ 1] Anywhere  ALLOW IN    10.30.161.1  
[ 2] 80/tcp    ALLOW IN    Anywhere  
[ 3] 443/tcp    ALLOW IN    Anywhere  
[ 4] 443/tcp (v6) ALLOW IN    Anywhere (v6)  
matlab@sjt516scope046:~$
```

CHECK WITH NMAP

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw allow ssh  
Rule added  
Rule added (v6)  
matlab@sjt516scope046:~$ sudo ufw status numbered  
Status: active  


|      | To           | Action   | From          |
|------|--------------|----------|---------------|
|      | --           | -----    | ----          |
| [ 1] | Anywhere     | ALLOW IN | 10.30.161.1   |
| [ 2] | 80/tcp       | ALLOW IN | Anywhere      |
| [ 3] | 443/tcp      | ALLOW IN | Anywhere      |
| [ 4] | 22/tcp       | ALLOW IN | Anywhere      |
| [ 5] | 443/tcp (v6) | ALLOW IN | Anywhere (v6) |
| [ 6] | 22/tcp (v6)  | ALLOW IN | Anywhere (v6) |

  
matlab@sjt516scope046:~$
```

NMAP WORKS AS ALL PORTS ARE ALLOWED

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ nmap 10.30.161.56  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-04 12:41 IST  
Nmap scan report for sjt516scope046 (10.30.161.56)  
Host is up (0.00016s latency).  
Not shown: 994 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
53/tcp    open  domain  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
7070/tcp  open  realserver  
  
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds  
matlab@sjt516scope046:~$
```

DENYING IN FOR ALL PORTS AND ADDRESSES

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo ufw deny ssh  
Rule updated  
Rule updated (v6)  
matlab@sjt516scope046:~$ sudo ufw status numbered  
Status: active  


|      | To           | Action   | From          |
|------|--------------|----------|---------------|
|      | --           | -----    | ----          |
| [ 1] | Anywhere     | ALLOW IN | 10.30.161.1   |
| [ 2] | 80/tcp       | ALLOW IN | Anywhere      |
| [ 3] | 443/tcp      | ALLOW IN | Anywhere      |
| [ 4] | 22/tcp       | DENY IN  | Anywhere      |
| [ 5] | 443/tcp (v6) | ALLOW IN | Anywhere (v6) |
| [ 6] | 22/tcp (v6)  | DENY IN  | Anywhere (v6) |

  
matlab@sjt516scope046:~$ sudo ufw deny tcp  
ERROR: Could not find a profile matching 'tcp'  
matlab@sjt516scope046:~$ sudo ufw deny 80/tcp  
Rule updated  
Rule added (v6)  
matlab@sjt516scope046:~$ sudo ufw status numbered  
Status: active  


|      | To           | Action   | From          |
|------|--------------|----------|---------------|
|      | --           | -----    | ----          |
| [ 1] | Anywhere     | ALLOW IN | 10.30.161.1   |
| [ 2] | 80/tcp       | DENY IN  | Anywhere      |
| [ 3] | 443/tcp      | ALLOW IN | Anywhere      |
| [ 4] | 22/tcp       | DENY IN  | Anywhere      |
| [ 5] | 443/tcp (v6) | ALLOW IN | Anywhere (v6) |
| [ 6] | 22/tcp (v6)  | DENY IN  | Anywhere (v6) |
| [ 7] | 80/tcp (v6)  | DENY IN  | Anywhere (v6) |


```

```
matlab@sjt516scope046:~$ sudo ufw deny from 10.30.161.1  
Rule updated  
matlab@sjt516scope046:~$ sudo ufw deny 443/tcp  
Rule updated  
Rule updated (v6)
```

```
matlab@sjt516scope046:~$ sudo ufw deny from 10.30.161.56  
Rule added  
matlab@sjt516scope046:~$ sudo ufw status numbered  
Status: active  


|      | To           | Action  | From          |
|------|--------------|---------|---------------|
|      | --           | -----   | ----          |
| [ 1] | Anywhere     | DENY IN | 10.30.161.1   |
| [ 2] | 80/tcp       | DENY IN | Anywhere      |
| [ 3] | 443/tcp      | DENY IN | Anywhere      |
| [ 4] | 22/tcp       | DENY IN | Anywhere      |
| [ 5] | Anywhere     | DENY IN | 10.30.161.56  |
| [ 6] | 443/tcp (v6) | DENY IN | Anywhere (v6) |
| [ 7] | 22/tcp (v6)  | DENY IN | Anywhere (v6) |
| [ 8] | 80/tcp (v6)  | DENY IN | Anywhere (v6) |


```


NMAP WORKS EVEN AFTER ALL PORTS AND CONNECTIONS ARE DENIED

```
matlab@sjt516scope046: ~
matlab@sjt516scope046:~$ nmap 10.30.161.56
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-04 12:47 IST
Nmap scan report for sjt516scope046 (10.30.161.56)
Host is up (0.00012s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
```

INSTALLING SQUID

[illegible]

```
matlab@sjt516scope046: ~  
matlab@sjt516scope046: ~  
matlab@sjt516scope046: ~  
matlab@sjt516scope046: ~  
matlab@sjt516scope046:~$ sudo -H  
Usage: squid [-cdzCFNRVX] [-n name] [-s | -l facility] [-f config-file] [--au port] [-k signal]  
-h | --help          Print help message.  
-v | --version       Print version details.  
  
-a port             Specify HTTP port number (default: 3128).  
-d level            Write debugging to stderr also.  
-f file             Use given config-file instead of /etc/squid/squid.conf  
-k reconfigure|rotate|shutdown|restart|interrupt|kill|debug|check|parse  
                   Parse configuration file, then send signal to running copy (except -k parse) and exit.  
-n name             Specify service name to use for service operations default is: squid.  
-s | -l facility    Enable logging to syslog.  
-u port             Specify ICP port number (default: 3130), disable with 0.  
-Z                 Create missing swap directories and then exit.  
-C                 Do not catch fatal signals.  
-D                 OBSOLETE. Scheduled for removal.  
-F                 Don't serve any requests until store is rebuilt.  
-N                 Master process runs in foreground and is a worker. No kids.  
--foreground        Master process runs in foreground and creates worker kids.  
--kid role-ID       Play a given SMP kid process role, with a given ID. Do not use this option. It is meant for the master process use only.  
-R                 Do not set REUSEADDR on port.  
-S                 Double-check swap during rebuild.  
-X                 Force full debugging.  
-Y                 Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.  
matlab@sjt516scope046:~$
```