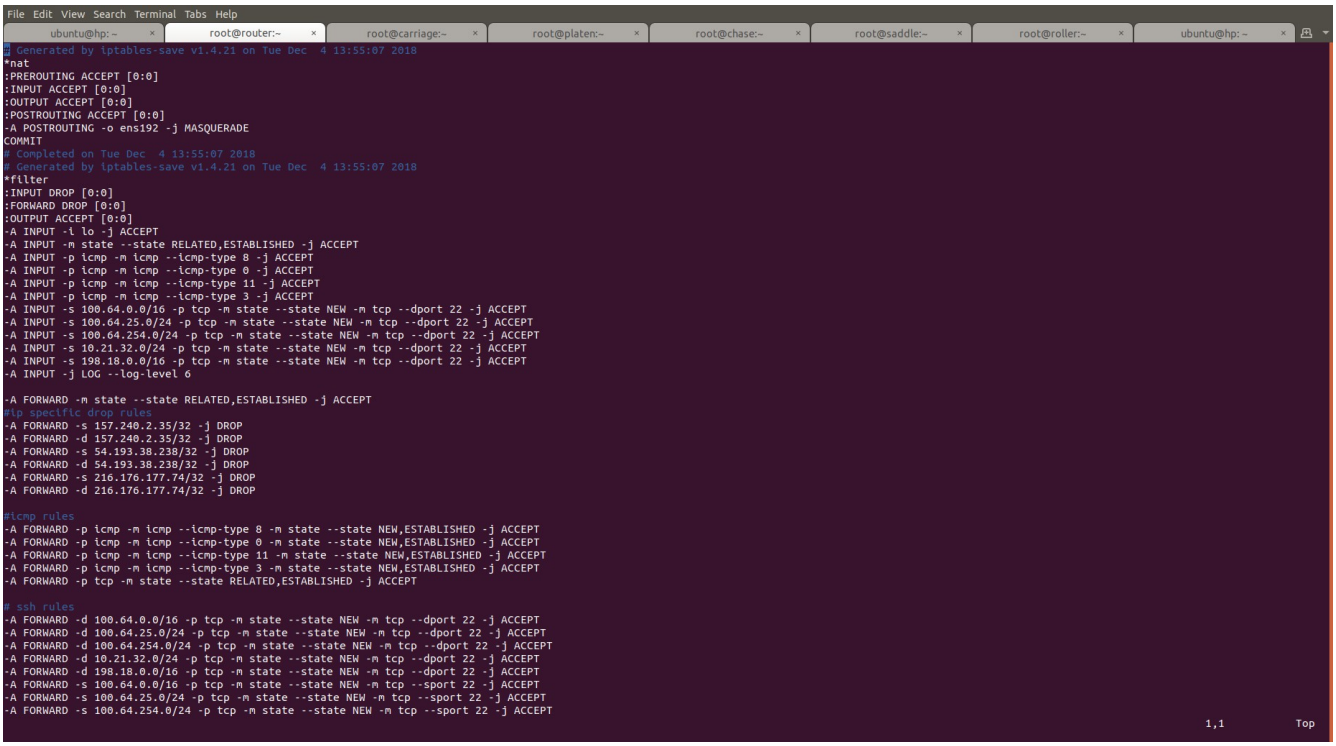
Lab 6 Notes

Ehsan Karimi

Following are the screenshots of /etc/sysconf/iptables for all the machines:

Machine A:

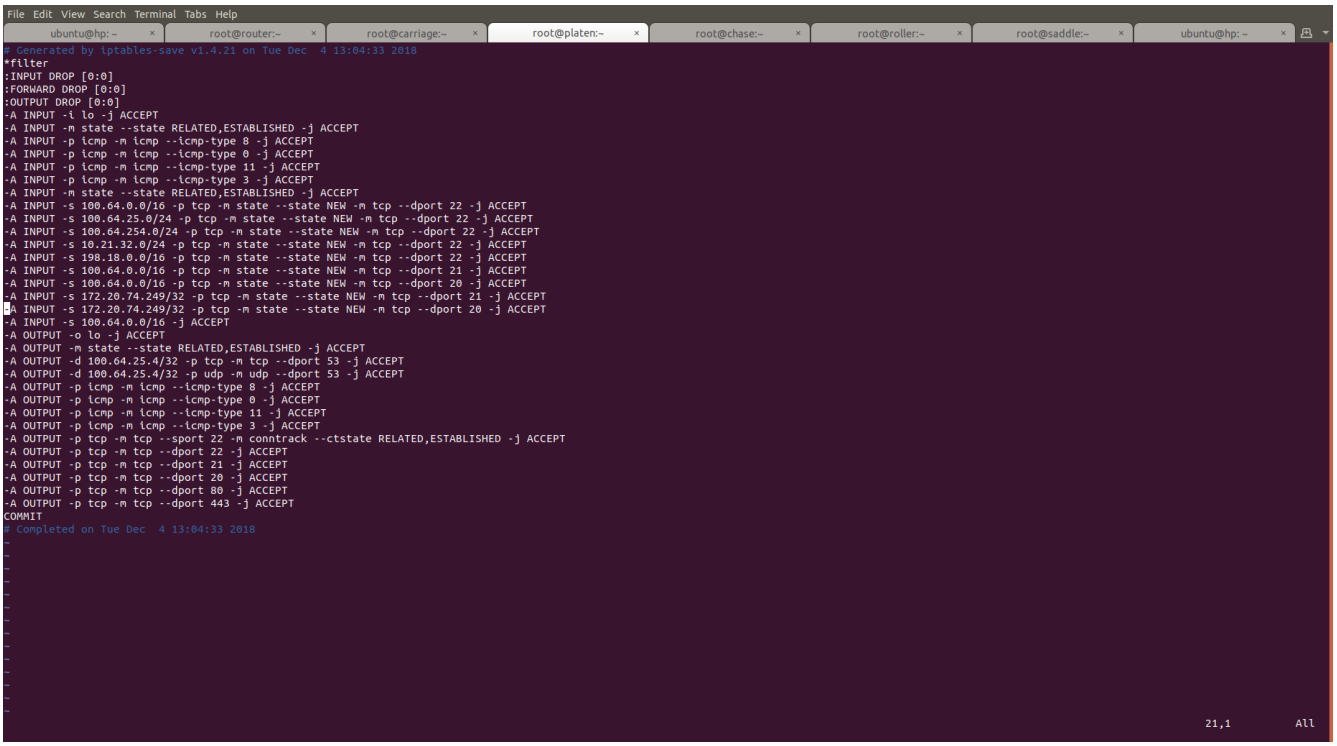


```
-A FORWARD -d 216.176.177.74/32 -j DROP

#icmp rules
-A FORWARD -p icmp -m icmp --icmp-type 8 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 0 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 11 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 3 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT

# ssh rules
-A FORWARD -d 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT

# Machine B and F
-A FORWARD -d 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A FORWARD -d 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A FORWARD -s 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --sport 80 -j ACCEPT
-A FORWARD -s 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --sport 443 -j ACCEPT
-A FORWARD -d 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A FORWARD -d 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A FORWARD -s 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --sport 80 -j ACCEPT
-A FORWARD -s 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --sport 443 -j ACCEPT

# Machine C
-A FORWARD -s 100.64.0.0/16 -d 100.64.25.3/32 -j ACCEPT
-A FORWARD -s 100.64.0.0/16 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 20 -j ACCEPT
-A FORWARD -s 100.64.0.0/16 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A FORWARD -s 172.20.74.249 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 20 -j ACCEPT
-A FORWARD -s 172.20.74.249 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 20 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 21 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 80 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 443 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 22 -j ACCEPT

# Machine D
-A FORWARD -d 100.64.25.4/32 -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -d 100.64.25.4/32 -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -s 100.64.25.4/32 -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -s 100.64.25.4/32 -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT

-A OUTPUT -o lo -j ACCEPT
COMMIT
# Completed on Tue Dec  4 13:55:07 2018
                                                                        86,1          Bot
```

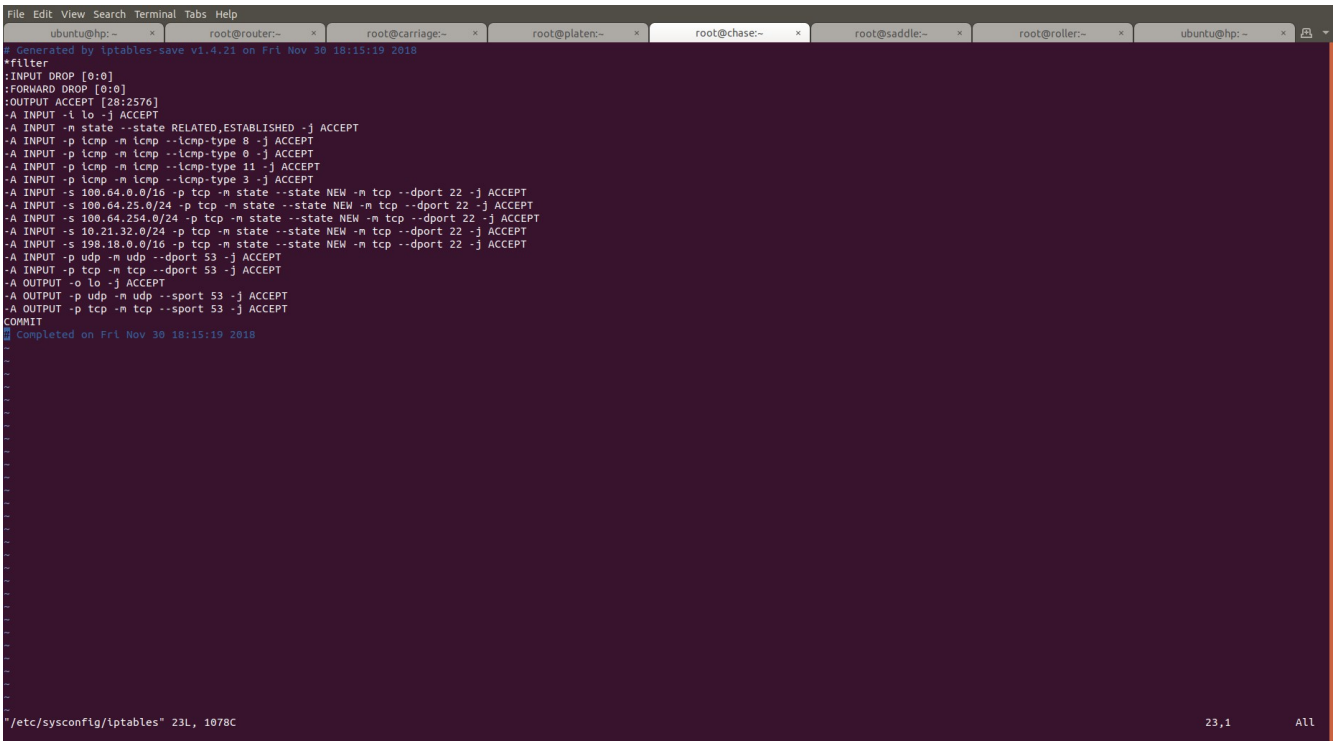
Machine B:

```
# Generated by iptables-save v1.4.21 on Thu Nov 29 15:01:48 2018
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [21:11176]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
COMMIT
# Completed on Thu Nov 29 15:01:48 2018
"/etc/sysconfig/iptables" 21L, 1032C                                    21,1          All
```

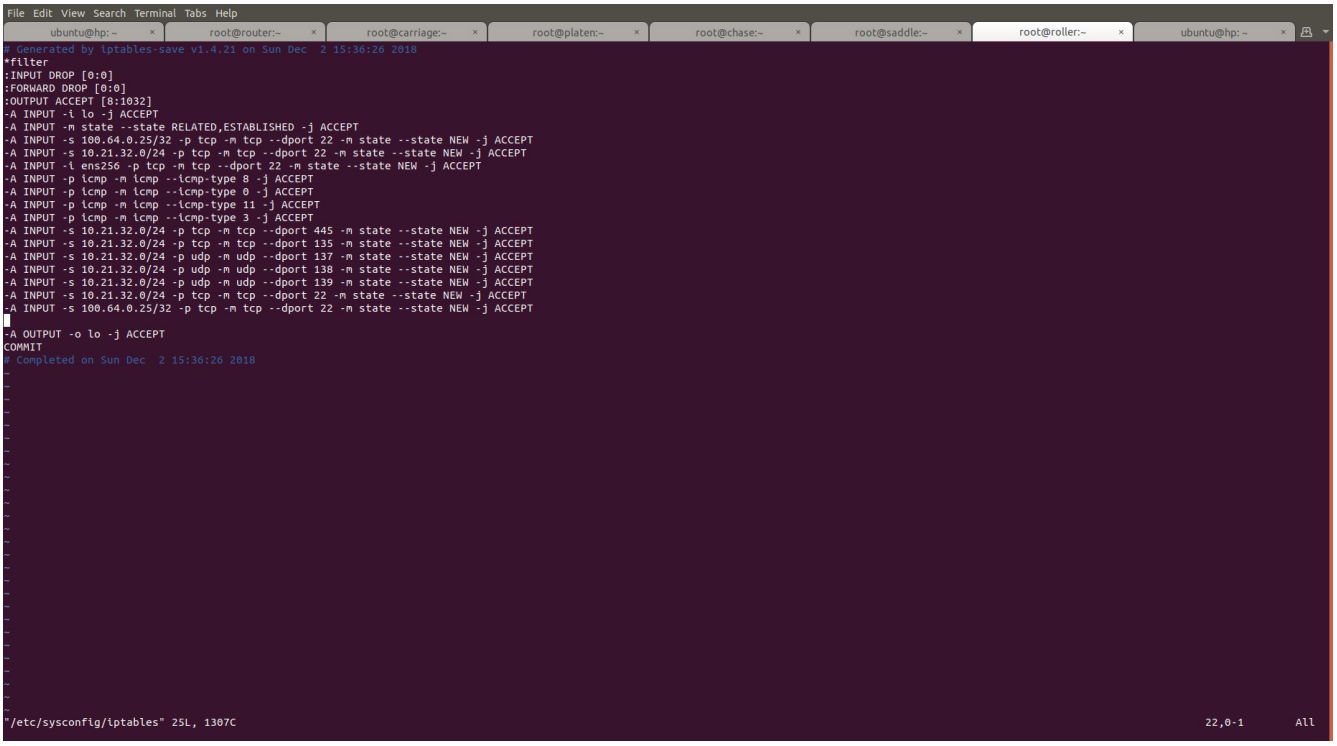
Machine C:



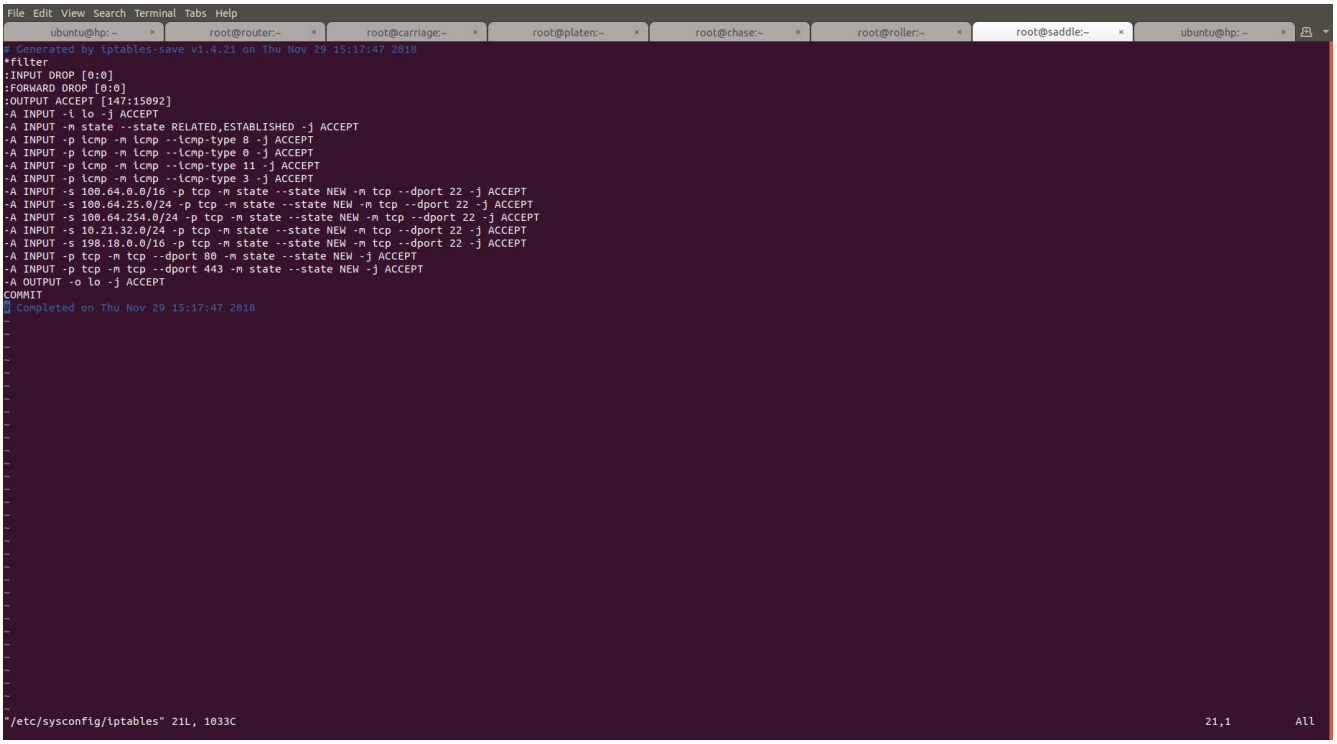
Machine D:



Machine E:



Machine F:



Following are screenshots demonstrating samples of the key functioning requirements:

Blocking Facebook :

```
[root@carriage ~]# ping 157.240.2.35
PING 157.240.2.35 (157.240.2.35) 56(84) bytes of data.
```

```
 26  2184 DROP       all  --  *      *       0.0.0.0/0            157.240.2.35
```

allow Inbound Ssh connections:

```
[root@carriage ~]# ssh root@100.64.25.3
root@100.64.25.3's password:
```

```
 0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
tcp spt:22 ctstate RELATED,ESTABLISHED
 6   360 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

Sending Http request from external network to machine B:

```
ubuntu@hp:~$ wget http://100.64.25.2:80/index.html
--2018-12-05 15:57:41--  http://100.64.25.2/index.html
Connecting to 100.64.25.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13888 (14K)
Saving to: ‘index.html.6’

index.html.6          100%[======================>]  13.56K  5.40KB/s    in 2.5s

2018-12-05 15:57:44 (5.40 KB/s) - ‘index.html.6’ saved [13888/13888]
```

router:

```
   state NEW tcp spt:22
    1    60 ACCEPT     tcp  --  *      *       0.0.0.0/0            100.64.25.2
   state NEW tcp dpt:80
```

MachineB:

```
 state NEW tcp dpt:22
  3   180 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
 tcp dpt:80 state NEW
```

Allow NEW inbound ftp traffic only from 100.64.0.0/16 and 172.20.74.249:

MachineB:

```
[root@carriage ~]# wget ftp://100.64.25.3/
--2018-12-05 16:01:42--  ftp://100.64.25.3/
           => '.listing'
Connecting to 100.64.25.3:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> PASV ... done.    ==> LIST ... done.

    [ <=>                                                ] 0

2018-12-05 16:01:42 (0.00 B/s) - '.listing' saved [0]

Removed '.listing'.
Wrote HTML-ized index to 'index.html.11' [196].
```

MachineC:

```
state NEW tcp dpt:22
 1    60 ACCEPT     tcp  --  *      *       100.64.0.0/16        0.0.0.0/0
state NEW tcp dpt:21
```

DNS query from machine E:

MachineE:

```
[root@roller ~]# nslookup www.google.com
Server:         100.64.25.4
Address:        100.64.25.4#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.3.4
```

MachineA:

```
tcp dpt:22
 1    60 ACCEPT     udp  --  *      *       0.0.0.0/0            100.64.25.4
udp dpt:53 state NEW,ESTABLISHED
 0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            100.64.25.4
tcp dpt:53 state NEW,ESTABLISHED
```

MachineD: