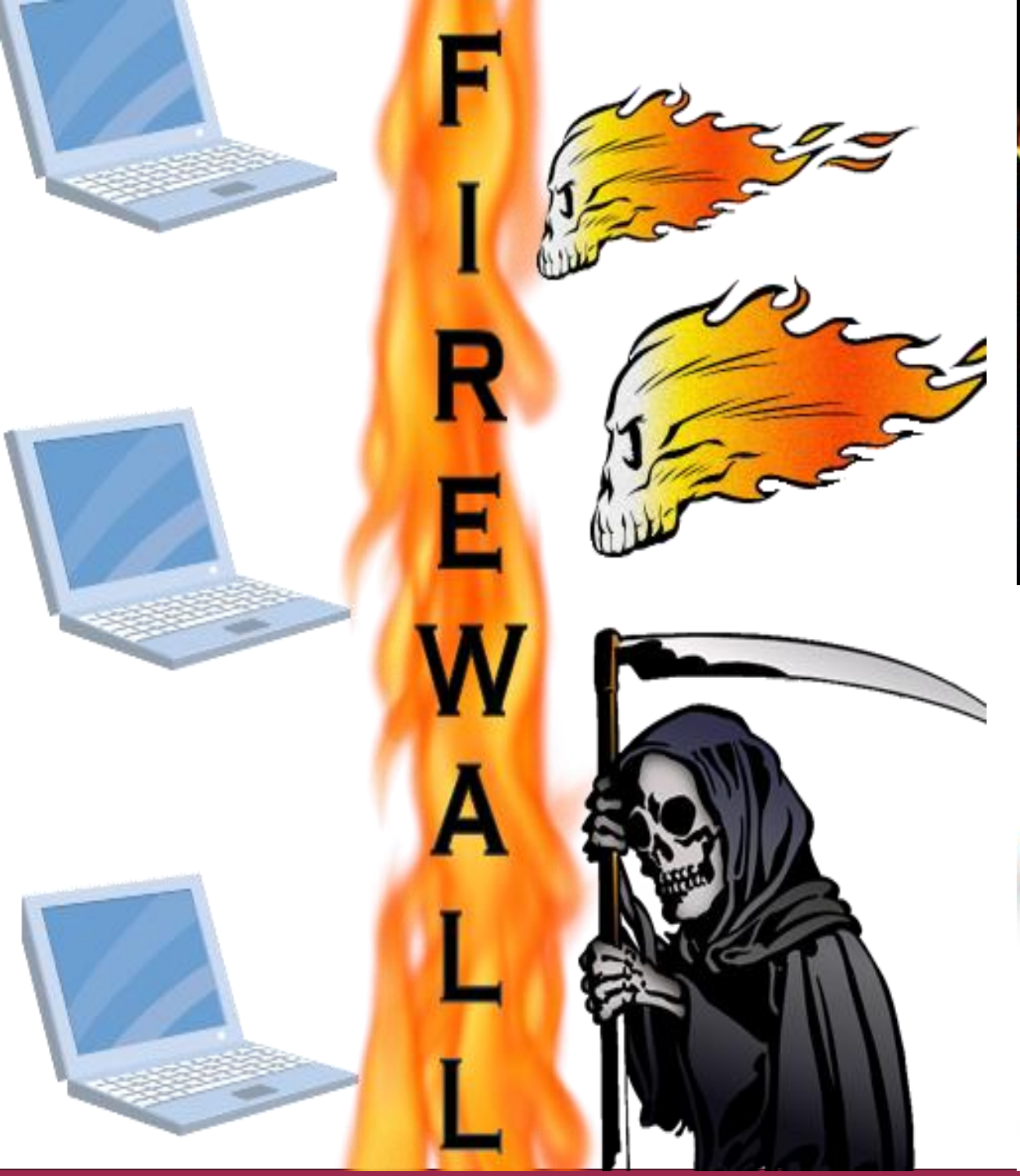


Vipin Gupta
BE,RHCSS,RHCE,CEH,CCNA,MCSE,MCSA
vipin2411@gmail.com
Mobile: 93563-10379
www.linuxexpert.in
https://www.youtube.com/techji

Available Firewalls

* Cisco ASA (adaptive security appliance)

* Checkpoint Firewall

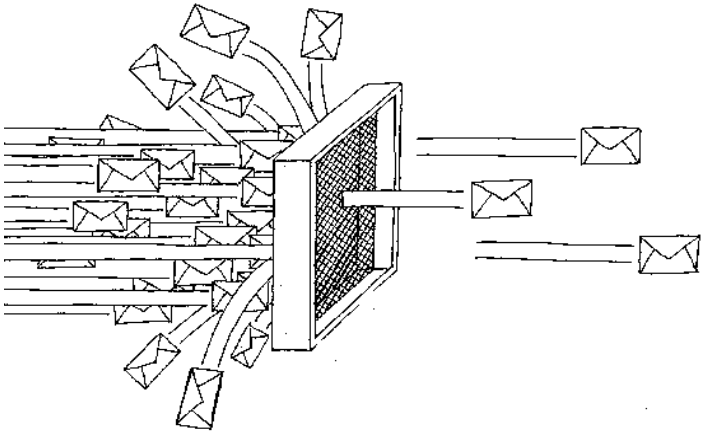
* Microsoft ISA

Microsoft®
Internet Security &
Acceleration Server

* Linux based Netfilter iptables Firewall

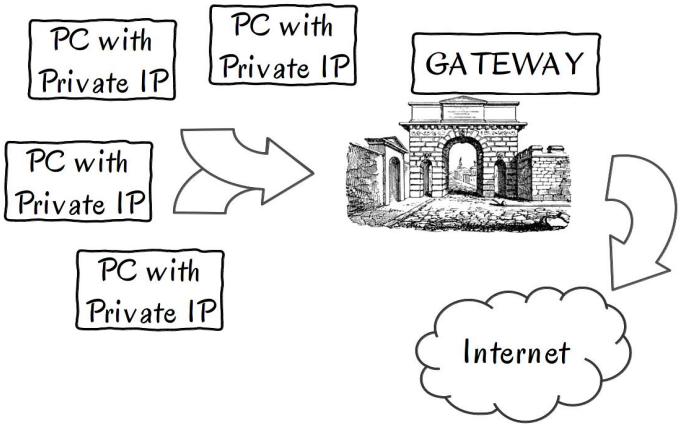
Types of Firewalls

* Filter



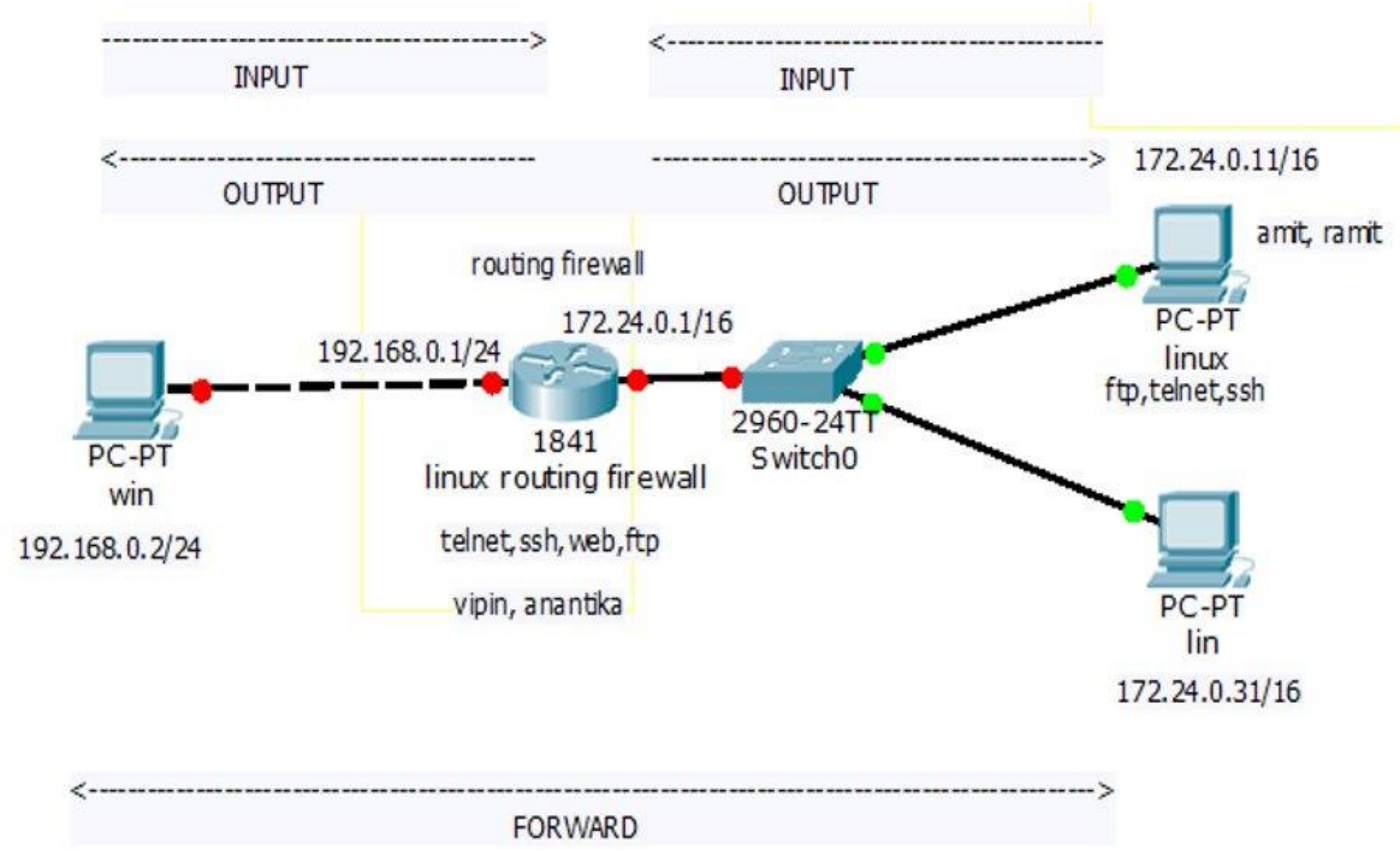
* NAT (Network Address Translation)

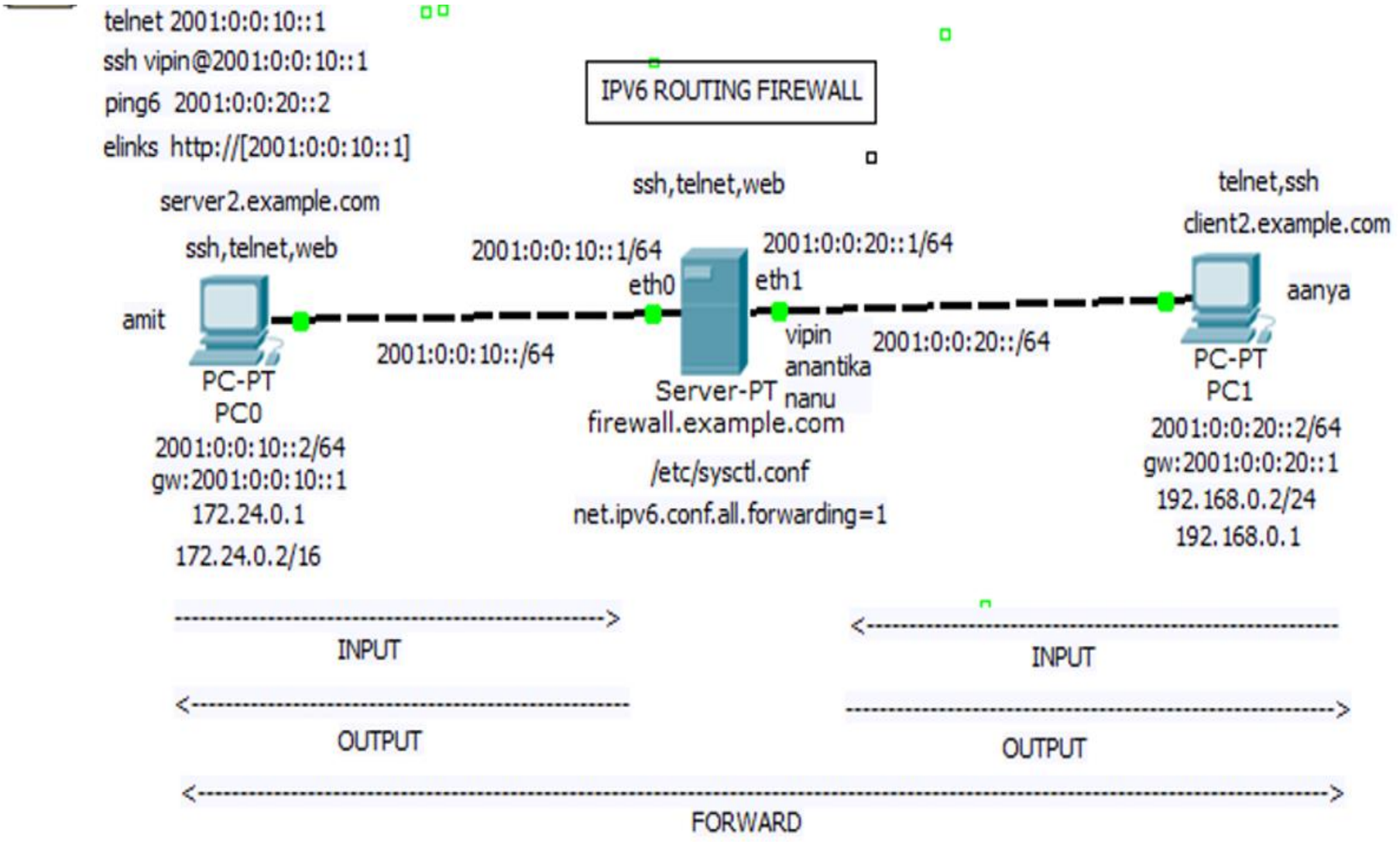
  - SNAT (Source NAT)
  - DNAT (Destination NAT)



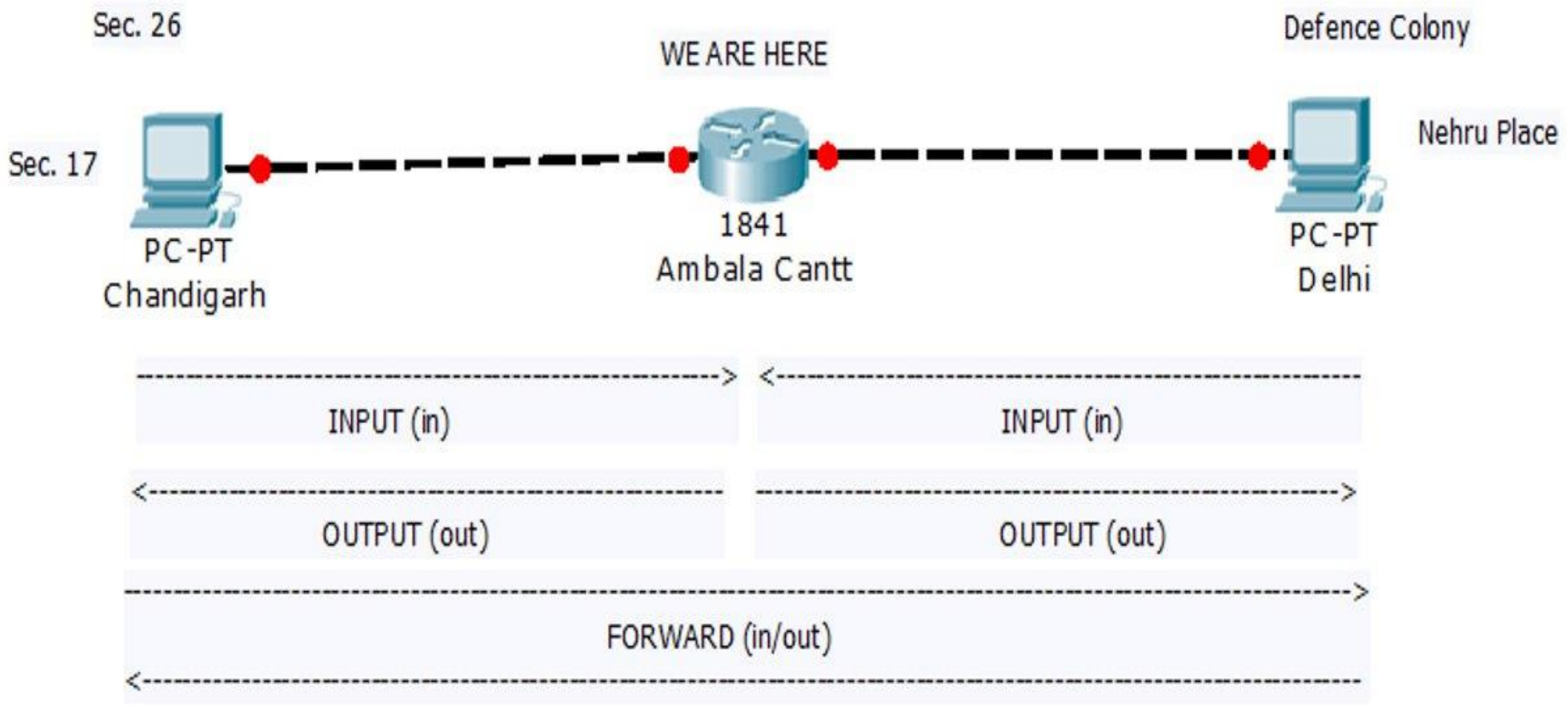
* Mangle

Direction of Firewall



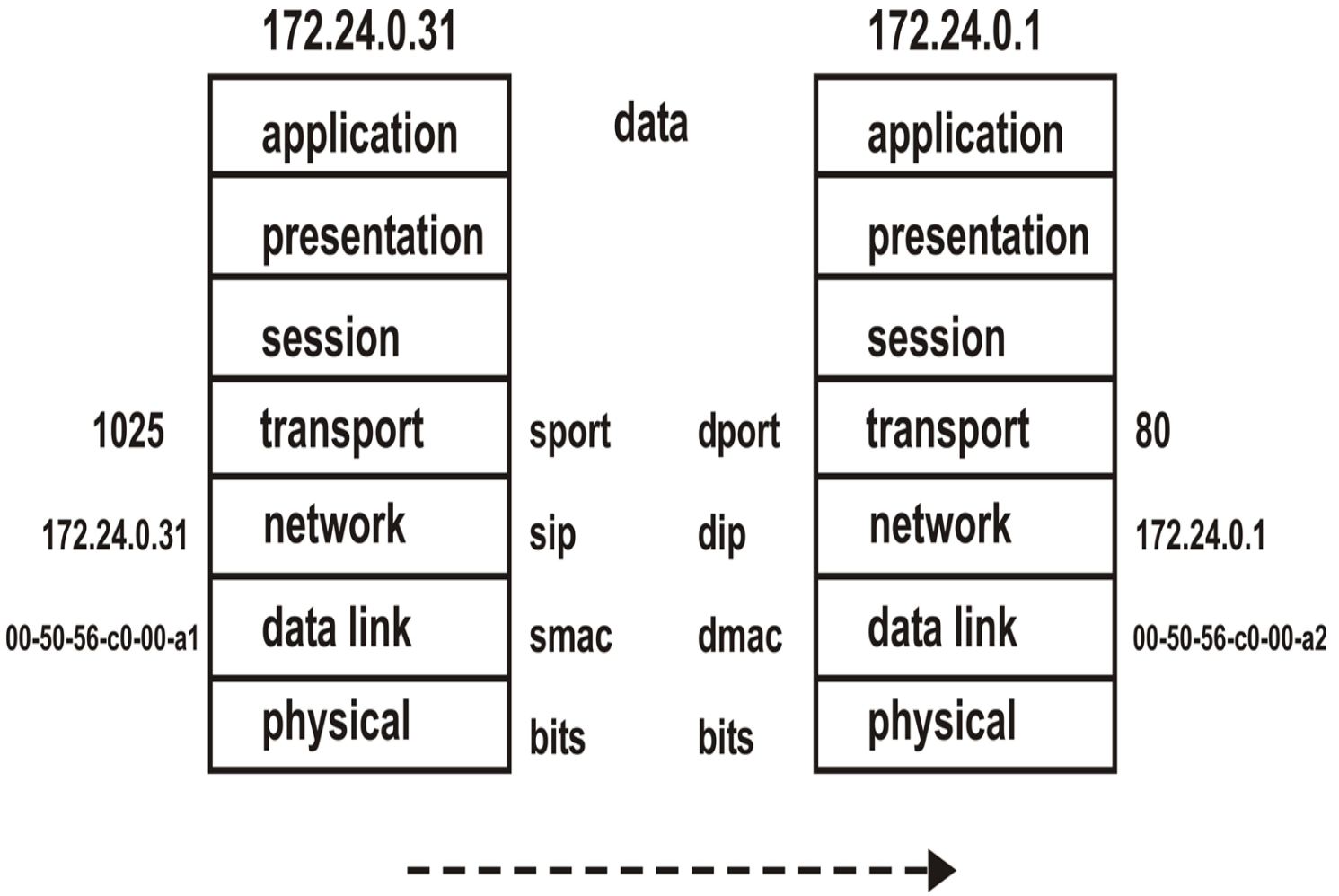


Meaning of Direction in Real Life

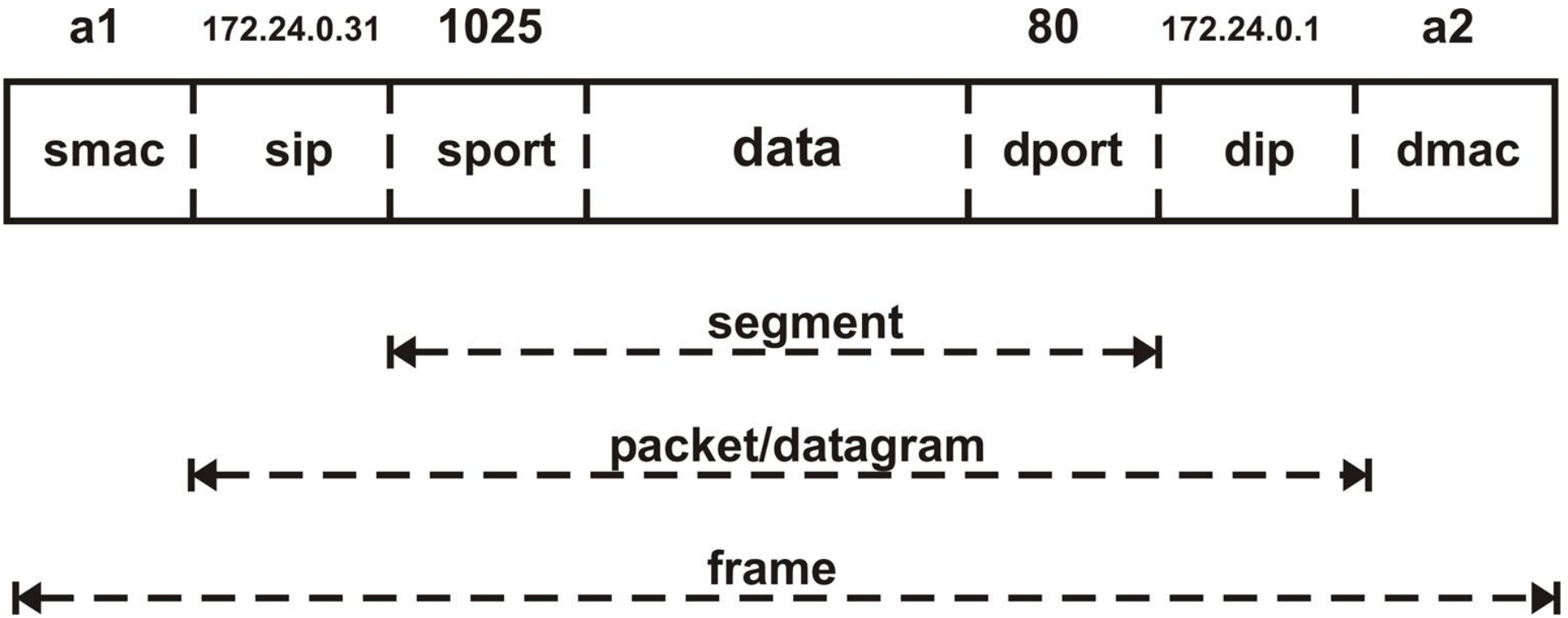


INPUT means traffic coming towards/terminating at Ambala
OUTPUT means traffic originating from Ambala & going towards Chandigarh or Delhi
FORWARD means traffic going through Ambala (from sec. 26, Chandigarh to Nehru Place, Delhi or vice versa)

What Firewall Can block/permit



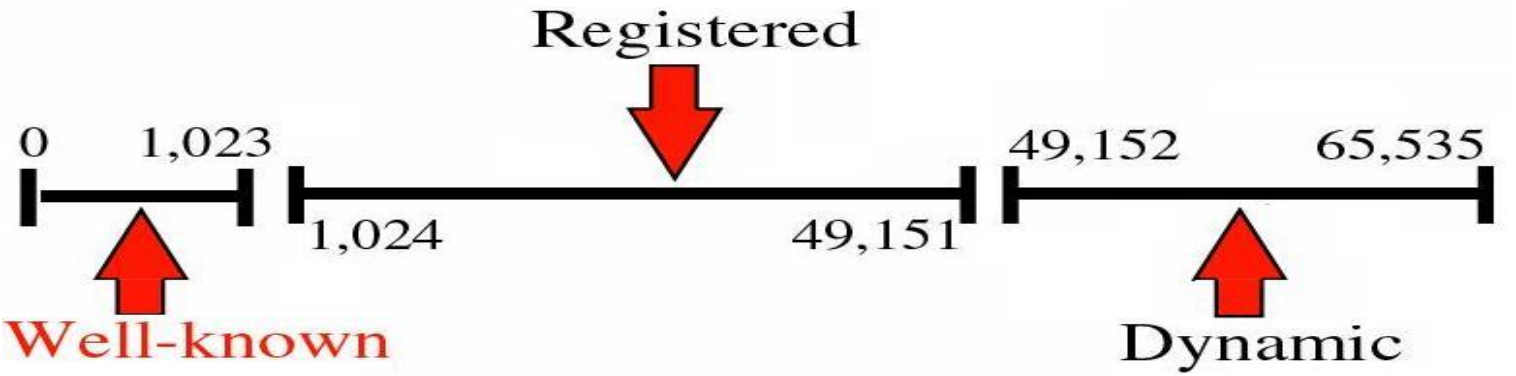
What Firewall Can block/permit



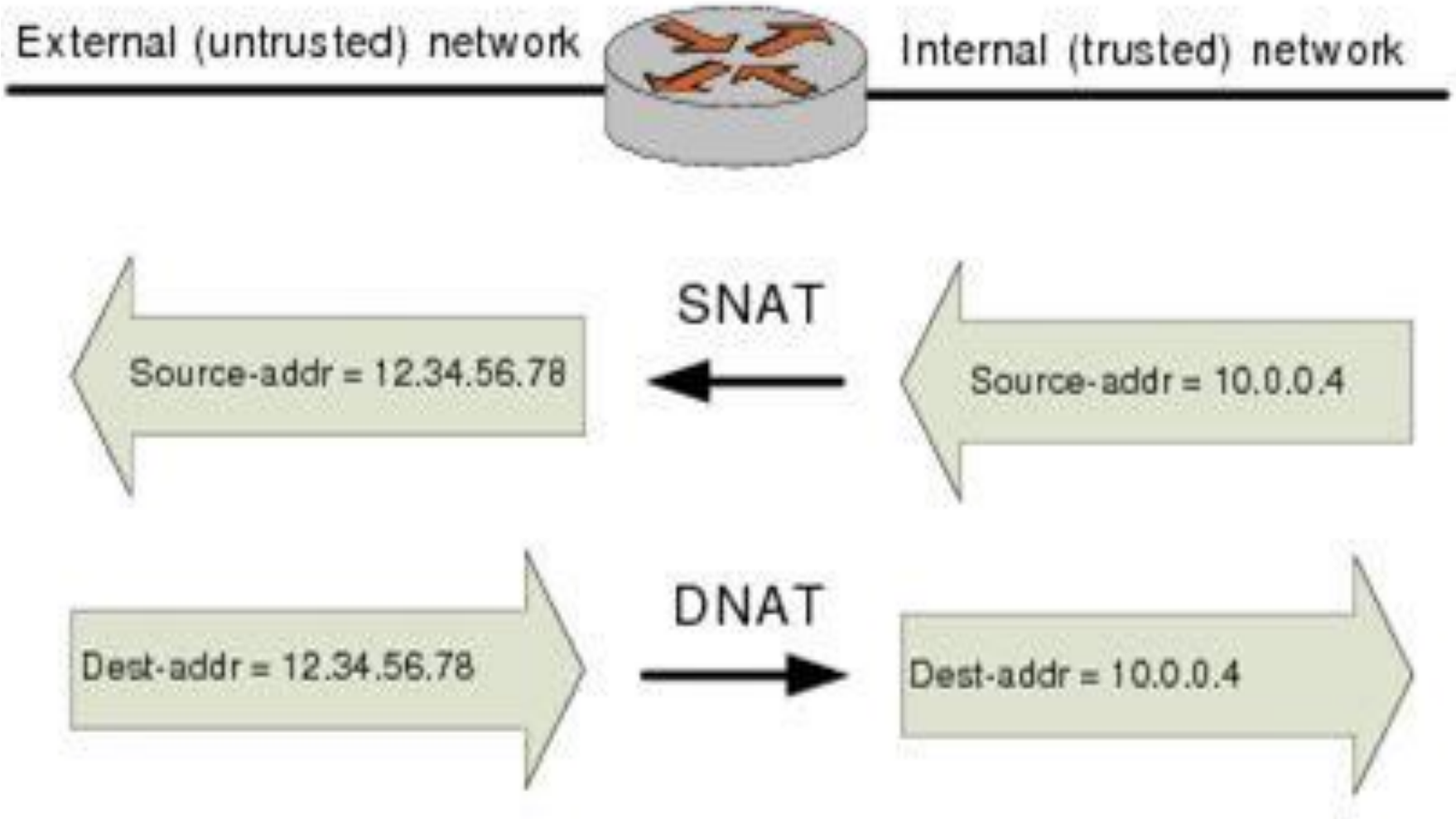
Ports

Port #	Protocol
21	FTP Control
20	FTP Data
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
443	HTTPS

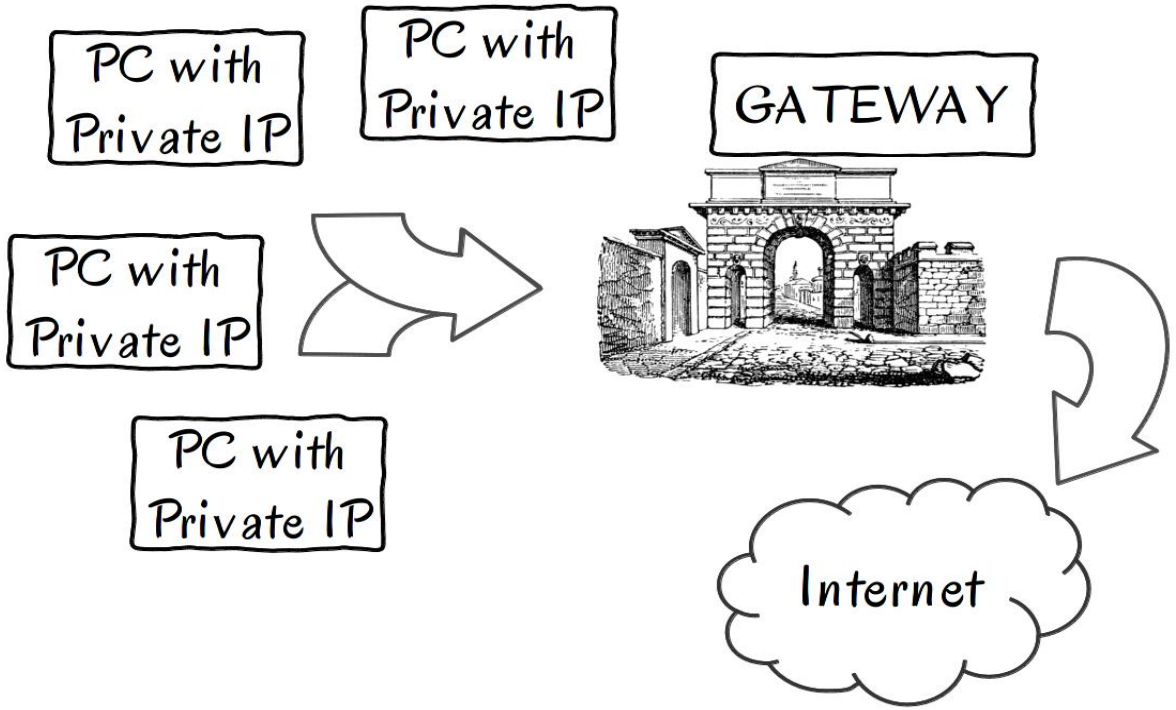
```
telnet      172.24.0.1
ssh         vipin@172.24.0.1
ftp         172.24.0.1
elinks      http://172.24.0.1
ping        172.24.0.1
```



SNAT/DNAT



SNAT/DNAT



Check telnet connectivity

```
[root@client11 ~]# telnet 172.24.0.1
Trying 172.24.0.1...
Connected to server1.example.com (172.24.0.1).
Escape character is '^]'.
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686
login: vipin
Password:
Last login: Tue Nov 19 02:59:10 from 172.24.0.11
[vipin@server1 ~]$
```

Check ssh connectivity

```
[root@client11 ~]# ssh vipin@172.24.0.1
vipin@172.24.0.1's password:
Last login: Tue Nov 19 02:59:29 2013 from 172.24.0.11
[vipin@server1 ~]$ _
```

Check ftp connectivity

```
[root@client11 ~]# ftp 172.24.0.1
Connected to 172.24.0.1.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (172.24.0.1:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
227 Entering Passive Mode (172,24,0,1,183,234)
150 Here comes the directory listing.
dr-xr-xr-x    9 0        0            4096 Nov 18 18:11 pub
```

Check web connectivity + ping

```
[root@client11 ~]# elinks --dump http://172.24.0.1
   wel to routing firewall
```

```
[root@client11 ~]# ping 172.24.0.1
PING 172.24.0.1 (172.24.0.1) 56(84) bytes of data.
64 bytes from 172.24.0.1: icmp_seq=1 ttl=64 time=0.813 ms
64 bytes from 172.24.0.1: icmp_seq=2 ttl=64 time=0.578 ms
64 bytes from 172.24.0.1: icmp_seq=3 ttl=64 time=0.461 ms
64 bytes from 172.24.0.1: icmp_seq=4 ttl=64 time=0.572 ms
```

Routing Firewall Configuration

```
[root@server1 ~]# ifconfig |grep "inet addr"
          inet addr:172.24.0.1  Bcast:172.24.255.255  Mask:255.255.0.0
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet addr:127.0.0.1  Mask:255.0.0.0
[root@server1 ~]#
```

Block everything from particular ip “172.24.0.11”

```
[root@server1 ~]# iptables -t filter -A INPUT -s 172.24.0.11 -j DROP
```

Switches	Examples & Meanings
-A	“append” rule at end of chain
-D	“delete” rule from the chain
-F	“flush” all the rules from the chain, but does not flush the policy
-I	“insert” rule at specified line number. if no number specified, at the beginning.
-L	“list” all the rules in specified chain. if no chain is specified, then all rules in all chains will be listed
-P	set the default policy to “ACCEPT/DROP”. default is “ACCEPT”
-t <table>	<table> could be “filter”, “nat” or “mangle”. if not specified, the “filter” is default. “mangle” is used rarely.
-j <target>	<target> could be “ACCEPT”, “DROP”, “REJECT”, “DNAT”, “SNAT”, “MASQUERADE”

Verify connectivity from “172.24.0.11”

```
[root@client11 ~]# ifconfig |grep "inet addr"
          inet addr:172.24.0.11  Bcast:172.24.255.255  Mask:255.255.0.0


[root@client11 ~]# ping 172.24.0.1
PING 172.24.0.1 (172.24.0.1) 56(84) bytes of data.

--- 172.24.0.1 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4002ms

[root@client11 ~]# elinks --dump http://172.24.0.1

[root@client11 ~]# ssh vipin@172.24.0.1

[root@client11 ~]# ftp 172.24.0.1
[root@client11 ~]#
[root@client11 ~]# telnet 172.24.0.1
Trying 172.24.0.1...
```

Verify connectivity from “172.24.0.31”

```
[root@client31 ~]# ifconfig |grep "inet addr"
          inet addr:172.24.0.31  Bcast:172.24.255.255  Mask:255.255.0.0
          inet addr:127.0.0.1  Mask:255.0.0.0
```

```
[root@client31 ~]# ping 172.24.0.1
PING 172.24.0.1 (172.24.0.1) 56(84) bytes of data.
64 bytes from 172.24.0.1: icmp_seq=1 ttl=64 time=2.62 ms
64 bytes from 172.24.0.1: icmp_seq=2 ttl=64 time=0.537 ms
```

Delete the rule

```
[root@server1 ~]# iptables -t filter -D INPUT -s 172.24.0.11 -j DROP
```

Block everything from network “172.24.0.0/16”

```
[root@server1 ~]# iptables -t filter -A INPUT -s 172.24.0.0/16 -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -D INPUT -s 172.24.0.0/16 -j DROP
```

Block everything from all

```
[root@server1 ~]# iptables -t filter -A INPUT -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -D INPUT -j DROP
```

Block telnet, web access from “172.24.0.11”

```
[root@server1 ~]# iptables -t filter -A INPUT -m tcp -p tcp --dport 23 -s 172.24.0.11
 -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -A INPUT -m tcp -p tcp --dport 80 -s 172.24.0.11
 -j DROP
[root@server1 ~]#
```

Verify telnet, web, ssh connectivity from “172.24.0.11”

```
[root@client11 ~]# telnet 172.24.0.1
Trying 172.24.0.1...

[root@client11 ~]# elinks --dump http://172.24.0.1


[root@client11 ~]# ssh vipin@172.24.0.1
vipin@172.24.0.1's password:
```

List Firewall rules

```
[root@server1 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  172.24.0.11          anywhere            tcp dpt:telnet
DROP       tcp  --  172.24.0.11          anywhere            tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

List firewall rules without resolving DNS

```
[root@server1 ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  172.24.0.11          0.0.0.0/0           tcp dpt:23
DROP       tcp  --  172.24.0.11          0.0.0.0/0           tcp dpt:80
```

List firewall rules along with rule numbers

```
[root@server1 ~]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  172.24.0.11          0.0.0.0/0           tcp dpt:23
2    DROP       tcp  --  172.24.0.11          0.0.0.0/0           tcp dpt:80
```

Delete rule 2

```
[root@server1 ~]# iptables -D INPUT 2
[root@server1 ~]#
[root@server1 ~]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  172.24.0.11          0.0.0.0/0           tcp dpt:23

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

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

Delete (Flush) all rules & Save

```
[root@server1 ~]# iptables -F
[root@server1 ~]#
[root@server1 ~]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@server1 ~]#
[root@server1 ~]# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:                [  OK  ]
```

Block telnet, ssh using multiport module

```
[root@server1 ~]# iptables -t filter -A INPUT -m tcp -m multiport -p tcp --dports 22,23
-s 172.24.0.11 -j DROP
```

Verify ssh, telnet, web connectivity “172.24.0.11”

```
[root@client11 ~]# ssh vipin@172.24.0.1

[root@client11 ~]# telnet 172.24.0.1
Trying 172.24.0.1...

[root@client11 ~]# elinks --dump http://172.24.0.1
   wel to routing firewall
```

Delete multiport rule

```
[root@server1 ~]# iptables -t filter -D INPUT -m tcp -m multiport -p tcp --dports 22,23
-s 172.24.0.11 -j DROP
```

Block ping

```
[root@server1 ~]# iptables -t filter -A INPUT -m icmp -p icmp -j DROP
```

Verify ping connectivity from “172.24.0.11”

```
[root@client11 ~]# ping 172.24.0.1
PING 172.24.0.1 (172.24.0.1) 56(84) bytes of data.

--- 172.24.0.1 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5004ms

[root@client11 ~]# elinks --dump http://172.24.0.1
   wel to routing firewall
```

Block only “echo-request”

```
[root@server1 ~]# ping -c 2  172.24.0.11
PING 172.24.0.11 (172.24.0.11) 56(84) bytes of data.

--- 172.24.0.11 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1002ms

You have mail in /var/spool/mail/root
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -D INPUT -m icmp -p icmp -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -A INPUT -p icmp --icmp-type echo-request -j DROP
[root@server1 ~]#
[root@server1 ~]# ping -c 2  172.24.0.11
PING 172.24.0.11 (172.24.0.11) 56(84) bytes of data.
64 bytes from 172.24.0.11: icmp_seq=1 ttl=64 time=2.98 ms
64 bytes from 172.24.0.11: icmp_seq=2 ttl=64 time=0.388 ms
```

Tables & Meaning

table	meaning
filter	for packet filtering. default table if not specified
nat	network address translation. for changing source or destination ip addresses in packets
mangle	used for setting packet options & marking packets for further filtering/routing purposes. rarely used.

Actions & Meaning

Action	Description
ACCEPT	allow the packet
DROP	drop the packet without generating any "ICMP" message
REJECT	drop the packet & generate "ICMP" message
DNAT	performs destination address translation
SNAT	performs source address translation
MASQUERADE	special case of "SNAT", used when ip address is assigned dynamically

Options & Meaning

-p <protocol>	specifies protocol. could be "tcp", "udp", "icmp". different scenarios can be *-p tcp --sport 2001* *(single value)* *-p tcp --sport 2001:2010* *(range of values)* *-p tcp --dport 80* *(destination port 80)* *-p tcp --dport 4002:4005* *-p tcp --syn* *("syn" packet used for new connection request)* *-p udp --sport 2001* *(single value)* *-p udp --sport 2001:2010* *(range of values)* *-p udp --dport 80* *(destination port 80)* *-p udp --dport 4002:4005* *-p icmp --icmp-type echo-request* *(ping)* *-p icmp --icmp-type echo-reply* *(pong)*

Options & Meaning

-s <ip address> or --src <ip address> --source <ip address>	specifies "source ip address". the different scenarios can be -s 192.168.0.2 (match specified single ip address) -s !192.168.0.2 (do not match specified address) ! -s 192.168.0.2 (do not match specified address) -s 192.168.0.0/255.255.255.0 (match specified network) -s 192.168.0.0/24 (match specified network)
-d <ip address> or --dst <ip address> --destination <ip address>	specifies "destination ip address". the different scenarios can be -d 172.24.0.11 (match specified single ip address) -d !172.24.0.11 (do not match specified address) ! -d 172.24.0.11 (do not match specified address) -d 172.24.0.0/255.255.0.0 (match specified network) -d 172.24.0.0/24 (match specified network)

Block access from firewall

```
[root@server1 ~]# iptables -t filter -A OUTPUT -m owner --uid-owner 500 -j DROP
[root@server1 ~]#
```

Verify outbound connectivity from firewall

```
[vipin@server1 ~]$ id
uid=500(vipin) gid=500(vipin) groups=500(vipin)
[vipin@server1 ~]$
[vipin@server1 ~]$ ssh amit@172.24.0.11

[vipin@server1 ~]$
```

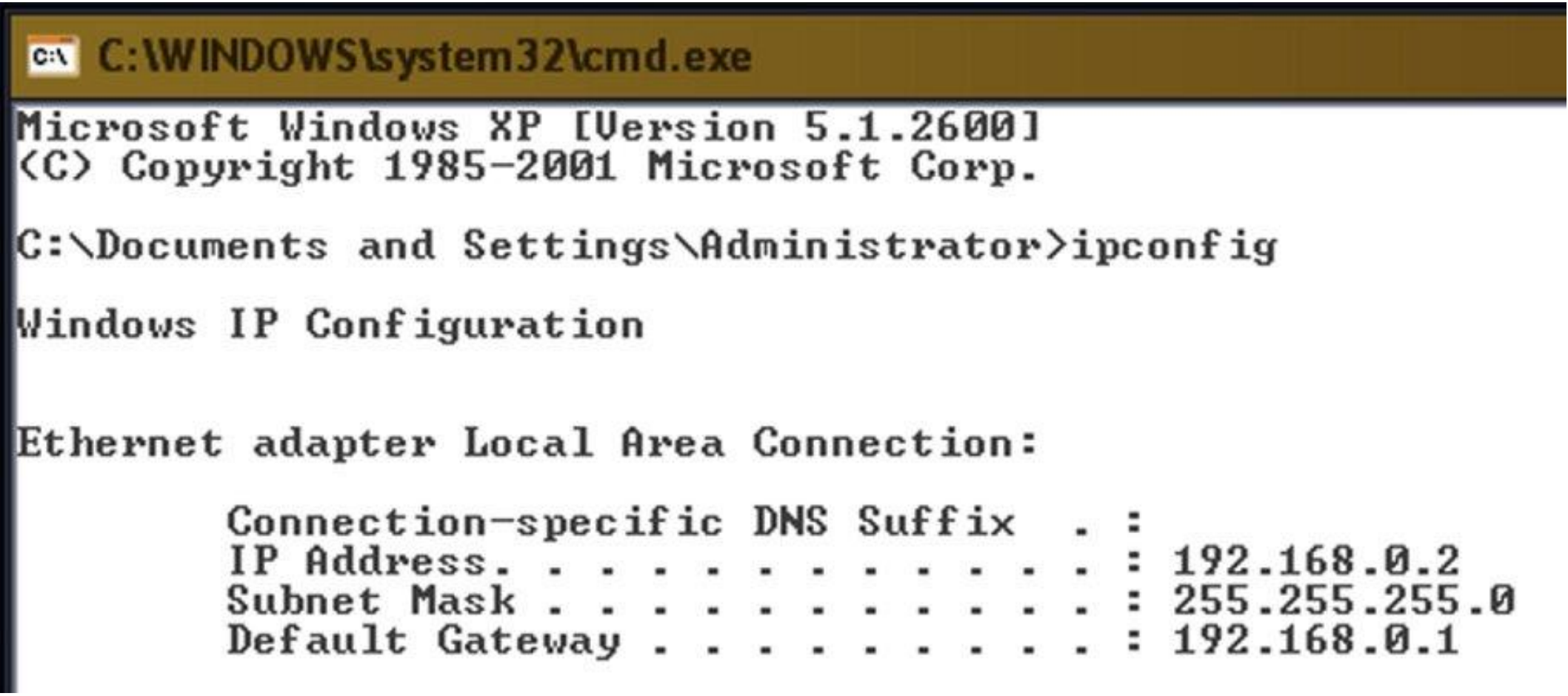
Verify outbound connectivity from firewall

```
[anantika@server1 ~]$ id
uid=501(anantika) gid=501(anantika) groups=501(anantika)
[anantika@server1 ~]$
[anantika@server1 ~]$ ssh amit@172.24.0.11
amit@172.24.0.11's password:
Last login: Tue Nov 19 13:07:26 2013 from server1.example.com
[amit@client11 ~]$
```

List/Delete Output rules

```
[root@server1 ~]# iptables -L OUTPUT -n
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0           OWNER UID match 500
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -D OUTPUT -m owner --uid-owner 500 -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -L OUTPUT -n
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@server1 ~]#
```

IP Address of Windows machine



Check forward connectivity

```
C:\Documents and Settings\Administrator>ping 172.24.0.11

Pinging 172.24.0.11 with 32 bytes of data:

Reply from 172.24.0.11: bytes=32 time<1ms TTL=63
Reply from 172.24.0.11: bytes=32 time=1ms TTL=63
Reply from 172.24.0.11: bytes=32 time=1ms TTL=63
Reply from 172.24.0.11: bytes=32 time=1ms TTL=63

Ping statistics for 172.24.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Administrator>telnet 172.24.0.11
```

Block telnet, ping in Forward direction

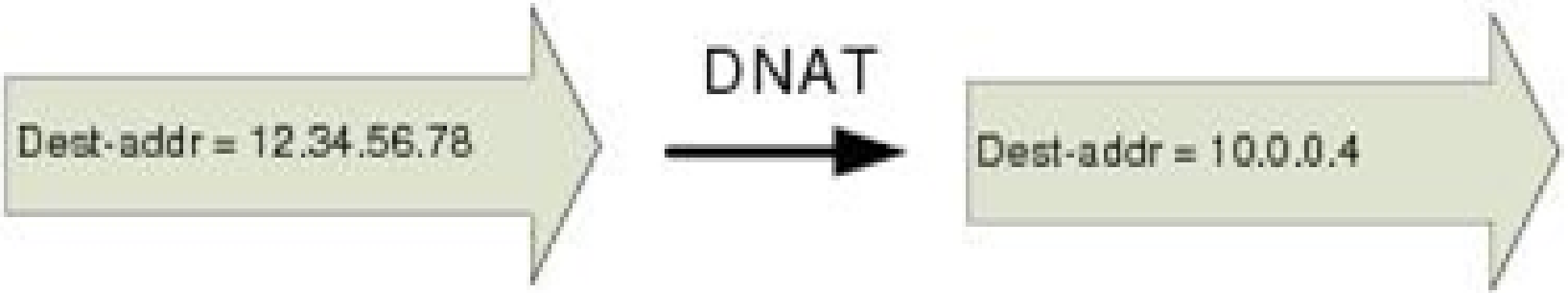
```
[root@server1 ~]# iptables -t filter -A FORWARD -m tcp -p tcp -s 192.168.0.2 -d 172.24.0.11
--dport 23 -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -A FORWARD -p icmp -s 192.168.0.2 -d 172.24.0.11 -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -L FORWARD -n
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.0.2          172.24.0.11         tcp dpt:23
DROP       icmp --  192.168.0.2          172.24.0.11
```

Verify ping connectivity to “172.24.0.11” & “172.24.0.31”

```
C:\Documents and Settings\Administrator>ping 172.24.0.11

Pinging 172.24.0.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.24.0.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

C:\Documents and Settings\Administrator>ping 172.24.0.31

Pinging 172.24.0.31 with 32 bytes of data:

Reply from 172.24.0.31: bytes=32 time=3ms TTL=63
Reply from 172.24.0.31: bytes=32 time=1ms TTL=63
```

Verify telnet connectivity to “172.24.0.11”

```
C:\Documents and Settings\Administrator>telnet 172.24.0.11
Connecting To 172.24.0.11...Could not open connection to the host, on port 23:
onnect failed
```



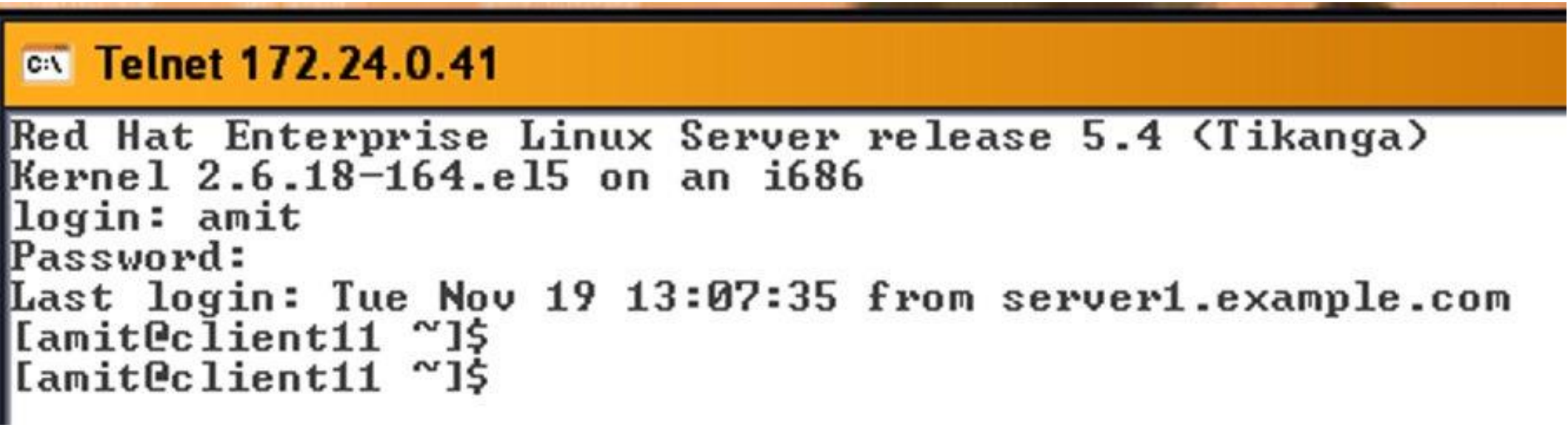
Try to telnet to non-existant ip “172.24.0.41”

```
C:\Documents and Settings\Administrator>telnet 172.24.0.41
Connecting To 172.24.0.41...Could not open connection to the host, on port 23:
onnect failed
```

Change Destination from “172.24.0.41” to “172.24.0.11”

```
[root@server1 ~]# iptables -t nat -A PREROUTING -m tcp -p tcp -d 172.24.0.41 --dport 23 -j DNAT
 --to-dest 172.24.0.11
[root@server1 ~]#
[root@server1 ~]# iptables -L -t nat -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  0.0.0.0/0            172.24.0.41         tcp dpt:23 to:172.24.0.11
```

Try to telnet to non-existant ip “172.24.0.41”



Delete/List nat rules

```
[root@server1 ~]# iptables -F -t nat
[root@server1 ~]#
[root@server1 ~]# iptables -L -t nat -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

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

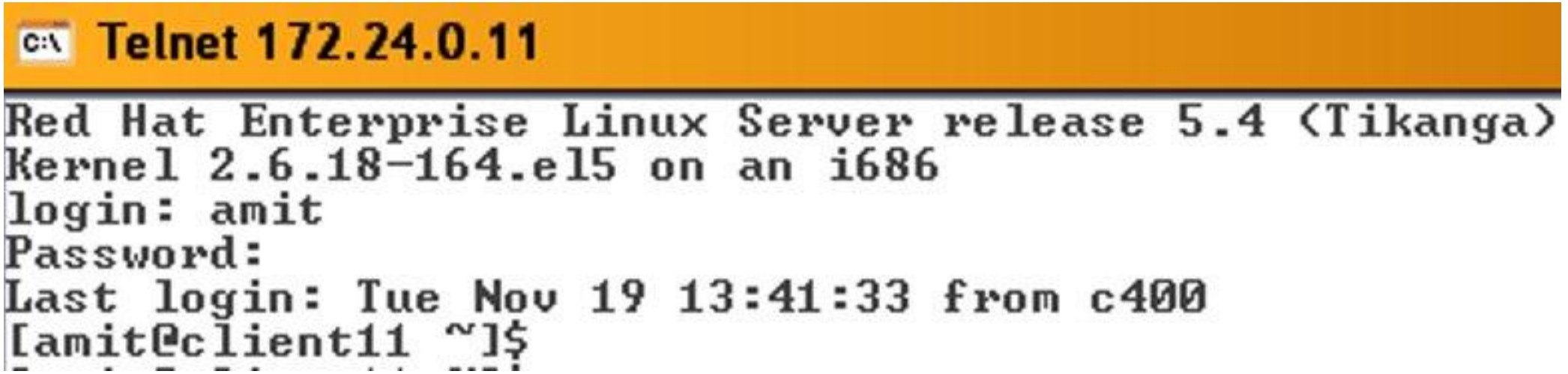
Block telnet access on client11 from “192.168.0.2”

```
[root@client11 ~]# cat /etc/hosts.deny
in.telnetd:192.168.0.2
[root@client11 ~]#
```

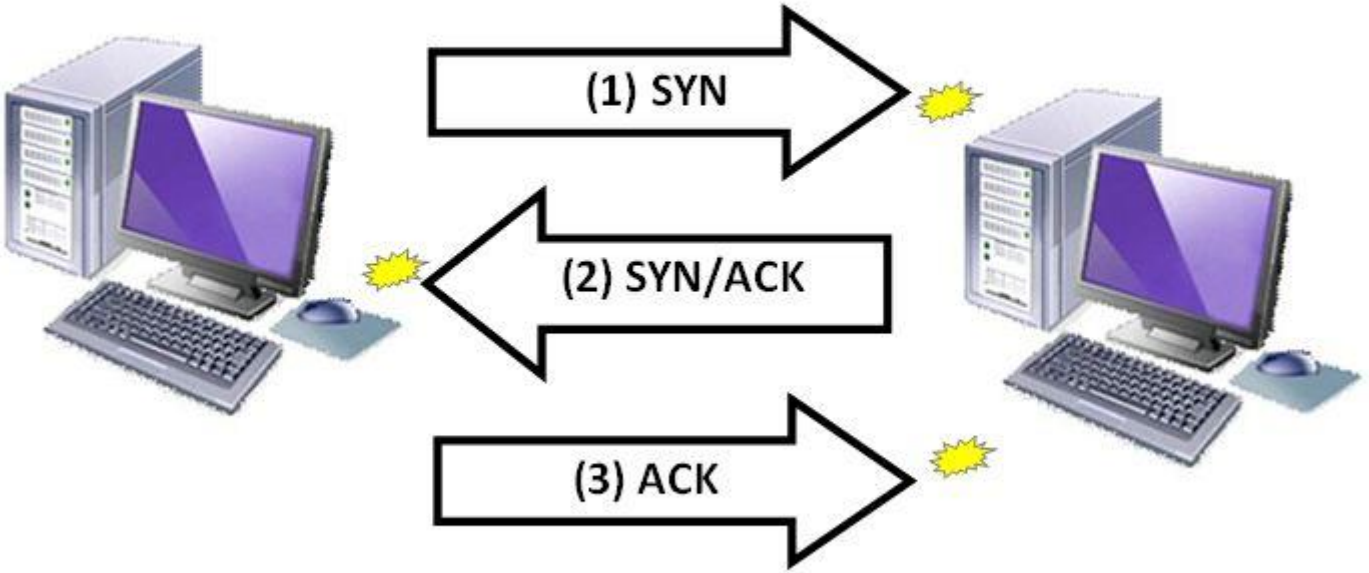
Change Source from restricted “192.168.0.2” to unrestricted “192.168.0.12”

```
[root@server1 ~]# iptables -t nat -A POSTROUTING -m tcp -p tcp -s 192.168.0.2 --dport 23
-j SNAT --to-source 192.168.0.12
[root@server1 ~]#
```

Verify telnet connectivity

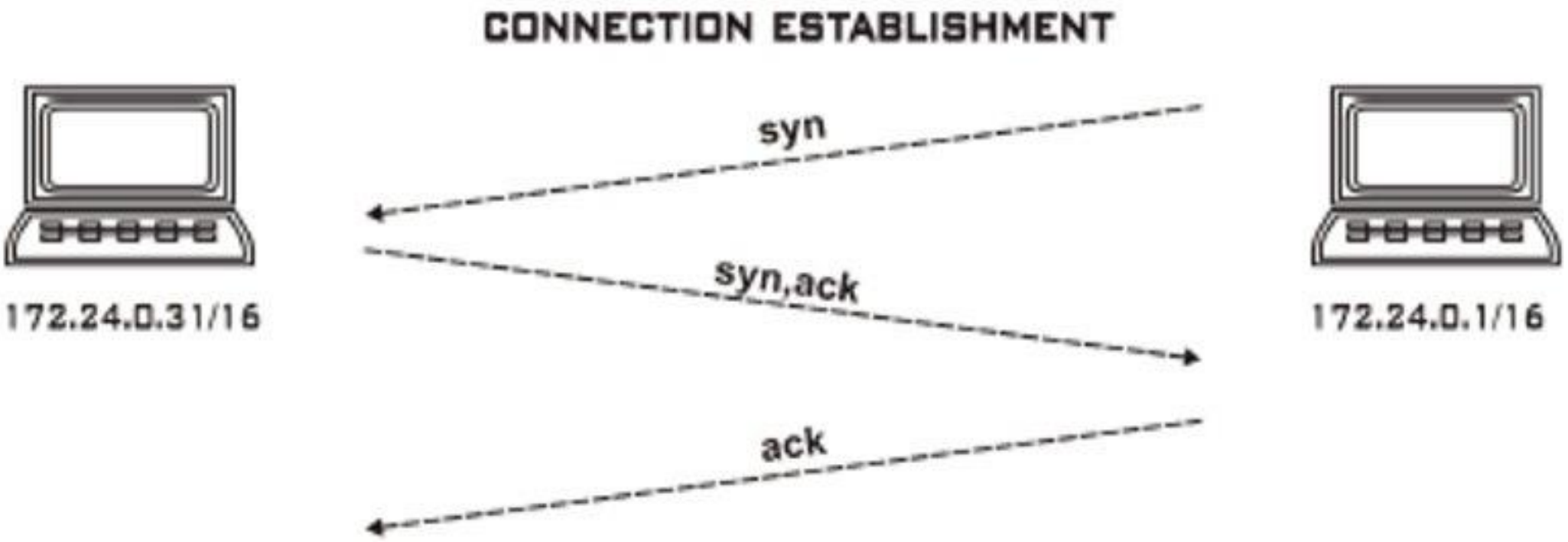


THREE-WAY HANDSHAKE (TCP)



SYN = SYNCHRONIZATION

ACK = ACKNOWLEDGEMENT



Block Everying in INPUT direction
But we are not able to telnet in outbound direction. Why ?

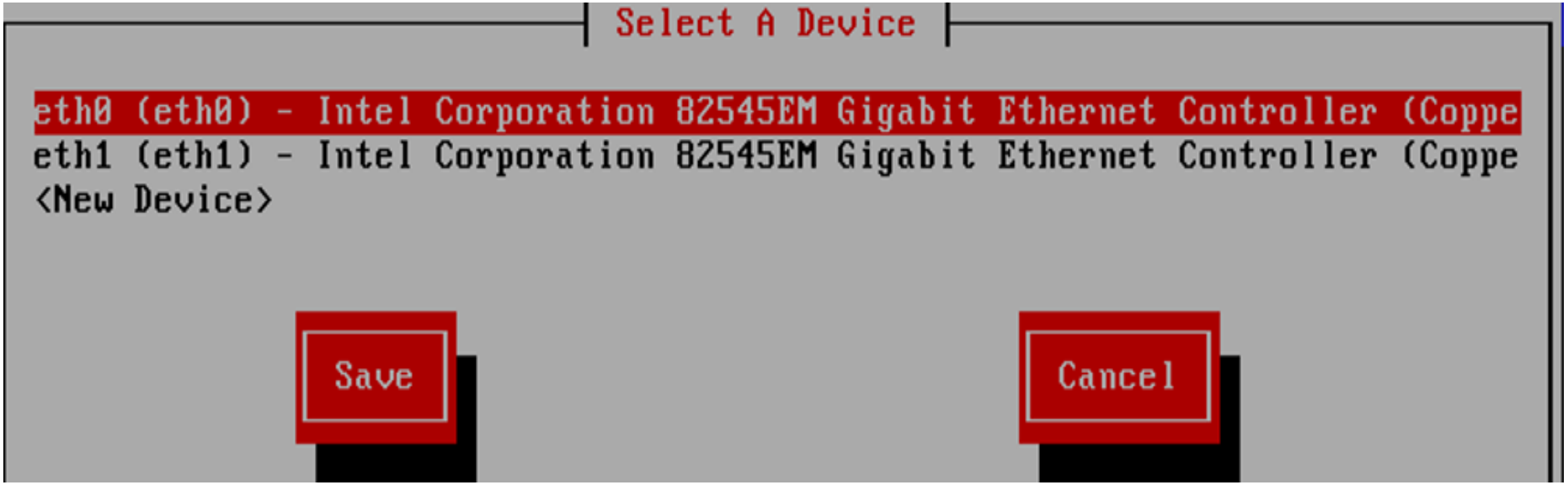
```
[root@server1 ~]# iptables -t filter -A INPUT -j DROP
[root@server1 ~]#
[root@server1 ~]# telnet 172.24.0.11

[root@server1 ~]#
```

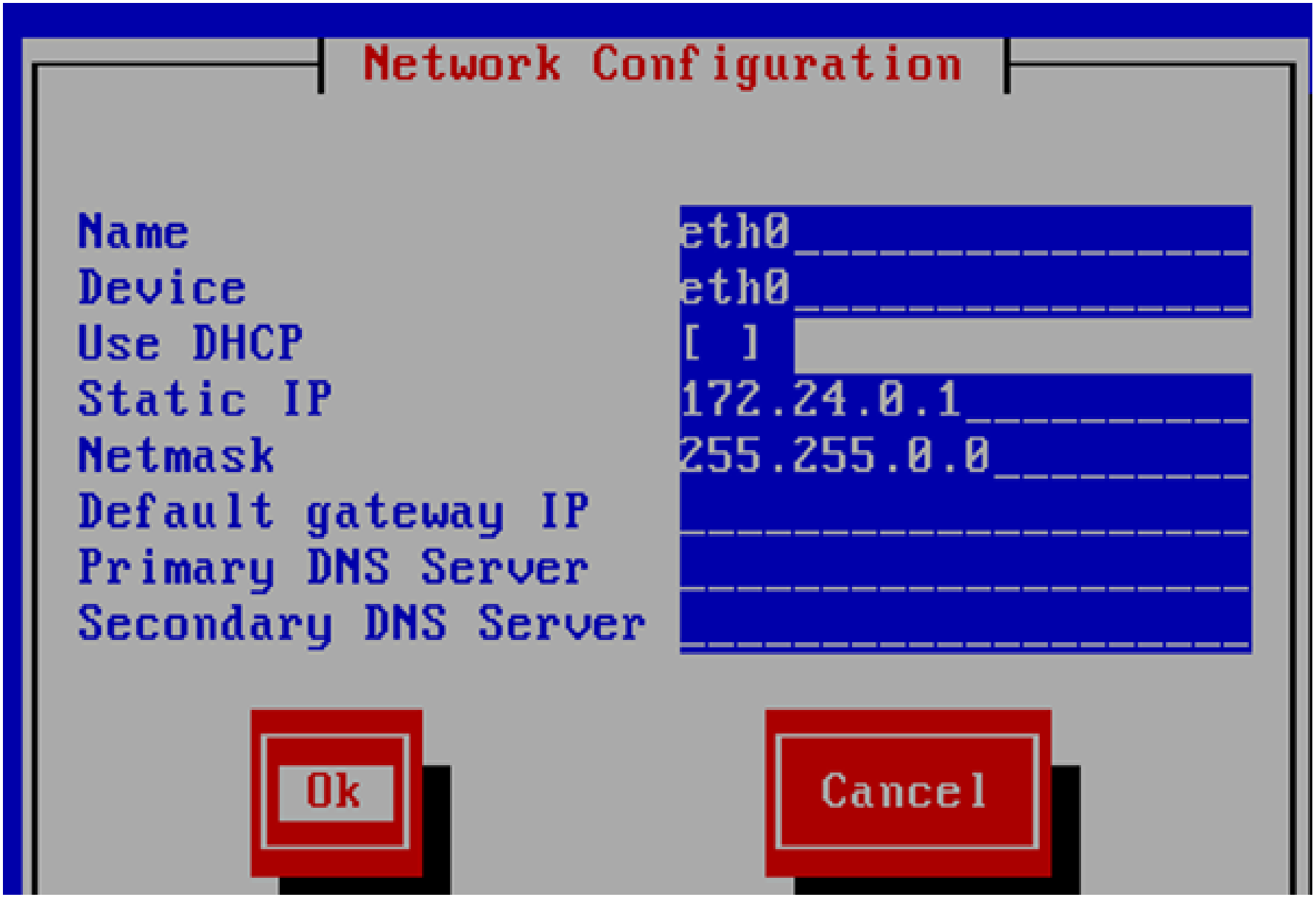
Modify rule to block only “syn”

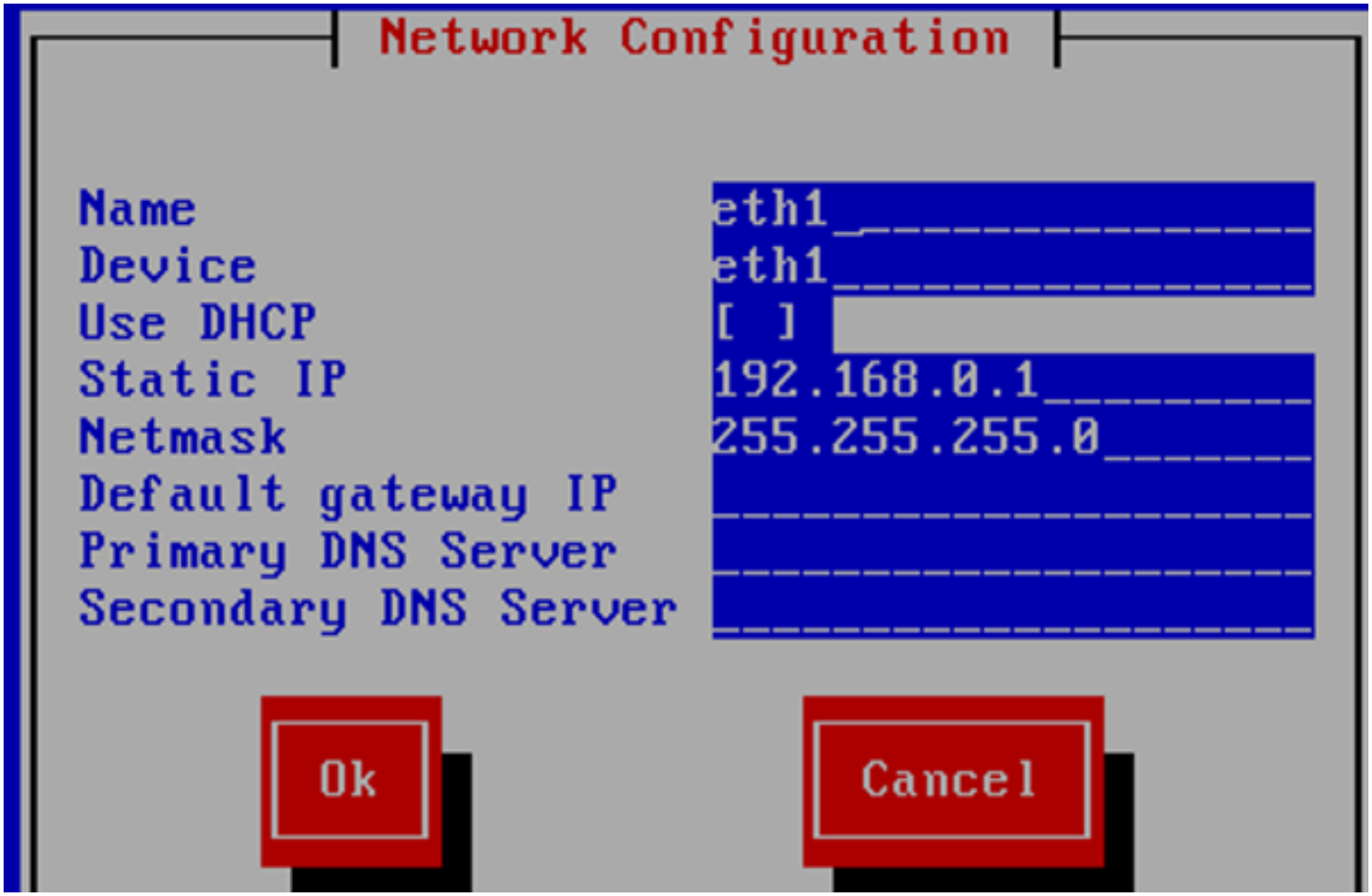
```
[root@server1 ~]# iptables -t filter -D INPUT -j DROP
[root@server1 ~]#
[root@server1 ~]# iptables -t filter -A INPUT -m tcp -p tcp --syn -j DROP
[root@server1 ~]#
[root@server1 ~]# telnet 172.24.0.11
Trying 172.24.0.11...
Connected to 172.24.0.11 (172.24.0.11).
Escape character is '^]'.
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686
login: amit
Password:
```

```
[root@firewall ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D3:CE:D5
          inet6 addr: fe80::20c:29ff:fed3:ced5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:255 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43090 (42.0 KiB)  TX bytes:632 (632.0 b)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:D3:CE:DF
          inet6 addr: fe80::20c:29ff:fed3:cedf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:255 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

```
[root@firewall ~]# system-config-network
```







```
[root@firewall ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:0c:29:d3:ce:d5
NM_CONTROLLED=yes
ONBOOT=no
TYPE=Ethernet
UUID="dec50645-ec94-47d0-a13b-eddec3e9f7b9"
IPADDR=172.24.0.1
NETMASK=255.255.0.0
IPV6INIT=no
USERCTL=no
[root@firewall ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
BOOTPROTO=none
HWADDR=00:0c:29:d3:ce:df
NM_CONTROLLED=yes
ONBOOT=no
TYPE=Ethernet
UUID="cb06b1ba-c732-481d-8be6-eee879b5c25d"
IPADDR=192.168.0.1
NETMASK=255.255.255.0
IPV6INIT=no
USERCTL=no
[root@firewall ~]# _
```

```
[root@firewall ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:0c:29:d3:ce:d5
NM_CONTROLLED=yes
ONBOOT=yes
TYPE=Ethernet
UUID="dec50645-ec94-47d0-a13b-eddec3e9f7b9"
IPADDR=172.24.0.1
NETMASK=255.255.0.0
IPV6INIT=yes
USERCTL=no
IPV6ADDR="2001:0:0:10::1/64"
[root@firewall ~]#
```

```
[root@firewall ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
BOOTPROTO=none
HWADDR=00:0c:29:d3:ce:df
NM_CONTROLLED=yes
ONBOOT=yes
TYPE=Ethernet
UUID="cb06b1ba-c732-481d-8be6-eee879b5c25d"
IPADDR=192.168.0.1
NETMASK=255.255.255.0
IPV6INIT=yes
USERCTL=no
IPV6ADDR="2001:0:0:20::1/64"
[root@firewall ~]#
```

```
[root@firewall ~]# service NetworkManager stop
Stopping NetworkManager daemon:                            [  OK  ]
[root@firewall ~]#
[root@firewall ~]# chkconfig NetworkManager off
[root@firewall ~]#
[root@firewall ~]# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Bringing up interface eth1:                                [  OK  ]
[root@firewall ~]#
[root@firewall ~]# _
```

```
[root@firewall ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D3:CE:D5
          inet addr:172.24.0.1  Bcast:172.24.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:fed3:ced5/64 Scope:Link
          inet6 addr: 2001:0:0:10::1/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9660 errors:0 dropped:0 overruns:0 frame:0
          TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1621683 (1.5 MiB)  TX bytes:17702 (17.2 KiB)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:D3:CE:DF
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2001:0:0:20::1/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fed3:cedf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
[root@firewall ~]# cat /etc/sysctl.conf |head -10
# Kernel sysctl configuration file for Red Hat Lin
#
# For binary values, 0 is disabled, 1 is enabled.
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
#net.ipv4.ip_forward = 0
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1

[root@firewall ~]#
[root@firewall ~]# sysctl -p |grep forward
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
```

```
[root@firewall ~]# hostname
firewall.example.com
[root@firewall ~]# dnsdomainname
example.com
[root@firewall ~]#
[root@firewall ~]# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
172.24.0.1  firewall.example.com firewall
192.168.0.1 firewall.example.com firewall
[root@firewall ~]#
```

```
[root@firewall ~]# mount /dev/dvd /media/
mount: block device /dev/sr0 is write-protected, mounting read-only
[root@firewall ~]# cp -a /media/. /var/ftp/pub/
[root@firewall ~]#
[root@firewall ~]# cd /var/ftp/pub/
[root@firewall pub]#
[root@firewall pub]# cd Packages/
[root@firewall Packages]#
[root@firewall Packages]# rpm -ivh deltarpm-3.5-0.5.20090913git.el6.x86_64.rpm p
ython-deltarpm-3.5-0.5.20090913git.el6.x86_64.rpm createrepo-0.9.8-5.el6.noarch.
rpm
warning: deltarpm-3.5-0.5.20090913git.el6.x86_64.rpm: Header V3 RSA/SHA256 Signa
ture, key ID fd431d51: NOKEY
Preparing...                ########################################### [100%]
   1:deltarpm               ########################################### [ 33%]
   2:python-deltarpm        ########################################### [ 67%]
   3:createrepo             ########################################### [100%]
[root@firewall Packages]#
[root@firewall Packages]# cd ..
[root@firewall pub]#
[root@firewall pub]# cp Server/repodata/c27858b7430afeb372d0dd50d8a56fd46b47bc81
bb9580c2bb91ab697e40592e-comps-rhel6-Server.xml s.xml
[root@firewall pub]#
[root@firewall pub]# createrepo -g s.xml .
```

```
[root@firewall pub]# createrepo -g s.xml .
3299/3653 - Packages/cyrus-imapd-2.3.16-6.el6_2.5.x86_64.rpm
iso-8859-1 encoding on Ville Skytt▪ <ville.skytta@iki.fi> - 2.8.2-2

3653/3653 - Packages/dovecot-pgsql-2.0.9-2.el6_1.1.x86_64.rpm
Saving Primary metadata
Saving file lists metadata
Saving other metadata
[root@firewall pub]#
[root@firewall pub]# service vsftpd start
Starting vsftpd for vsftpd:                                [  OK  ]
[root@firewall pub]# chkconfig vsftpd on
[root@firewall pub]#
[root@firewall pub]# tail -6 /etc/yum.conf
[yummy]
name=yum server
baseurl=ftp://172.24.0.1/pub
enabled=1
gpgcheck=0
```

```
 telnet-server         x86_64         1:0.17-47.el6          yummy           37 k

Transaction Summary
================================================================================
Install       1 Package(s)

Total download size: 37 k
Installed size: 53 k
Downloading Packages:
telnet-server-0.17-47.el6.x86_64.rpm                     |  37 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Warning: RPMDB altered outside of yum.
  Installing : 1:telnet-server-0.17-47.el6.x86_64                          1/1
Installed products updated.
  Verifying  : 1:telnet-server-0.17-47.el6.x86_64                          1/1

Installed:
  telnet-server.x86_64 1:0.17-47.el6

Complete!
[root@firewall publ# yum -y install telnet-server
```

```
[root@firewall pub]# chkconfig telnet on
[root@firewall pub]#
[root@firewall pub]# useradd vipin
[root@firewall pub]# useradd anantika
[root@firewall pub]# useradd nanu
[root@firewall pub]# passwd vipin
Changing password for user vipin.
New password:
BAD PASSWORD: it is WAY too short
BAD PASSWORD: is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully
[root@firewall pub]# _
```

```
[root@server2 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:0c:29:3d:e2:b7
NM_CONTROLLED=yes
ONBOOT=yes
TYPE=Ethernet
UUID="e1a4bc53-77da-4329-b714-8b9d289c975c"
IPADDR=172.24.0.2
NETMASK=255.255.0.0
GATEWAY=172.24.0.1
IPV6INIT=yes
IPV6ADDR="2001:0:0:10::2/64"
USERCTL=no
[root@server2 ~]#
[root@server2 ~]# ifconfig eth0 |head -6
eth0      Link encap:Ethernet  HWaddr 00:0C:29:3D:E2:B7
          inet addr:172.24.0.2  Bcast:172.24.255.255  Mask:255.255.0.0
          inet6 addr: 2001:0:0:10::2/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe3d:e2b7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1229 errors:0 dropped:0 overruns:0 frame:0
[root@server2 ~]#
```

```
[root@client2 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:0c:29:d2:5e:34
NM_CONTROLLED=yes
ONBOOT=yes
TYPE=Ethernet
UUID="bfd1226f-5785-4c2f-933a-488e4d644b82"
IPADDR=192.168.0.2
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
IPV6INIT=yes
IPV6ADDR="2001:0:0:20::2/64"
USERCTL=no
[root@client2 ~]#
[root@client2 ~]# ifconfig eth0 |head -6
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D2:5E:34
          inet addr:192.168.0.2  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2001:0:0:20::2/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fed2:5e34/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2768 errors:0 dropped:0 overruns:0 frame:0
[root@client2 ~]#
```

```
[root@server2 ~]# ip -6 route add 2001:0:0:20::/64 via 2001:0:0:10::1
[root@server2 ~]#
[root@server2 ~]# route -n -A inet6
Kernel IPv6 routing table
Destination                                 Next Hop
    Flags Metric Ref    Use Iface
2001:0:0:10::/64                            ::
    U     256    1        0 eth0
2001:0:0:20::/64                            2001:0:0:10::1
    UG    1024   0        0 eth0
fe80::/64                                   ::
    U     256    0        0 eth0
::1/128                                     ::
    U     0      3        1 lo
2001:0:0:10::2/128                          ::
    U     0      0        1 lo
fe80::20c:29ff:fe3d:e2b7/128                ::
    U     0      0        1 lo
ff00::/8                                    ::
    U     256    0        0 eth0
[root@server2 ~]# _
```

```
[root@client2 ~]# ip -6 route add 2001:0:0:10::/64 via 2001:0:0:20::1
[root@client2 ~]#
[root@client2 ~]# route -n -A inet6
Kernel IPv6 routing table
Destination                                 Next Hop
    Flags Metric Ref    Use Iface
2001:0:0:10::/64                            2001:0:0:20::1
    UG    1024   0        0 eth0
2001:0:0:20::/64                            ::
    U     256    1        0 eth0
fe80::/64                                   ::
    U     256    0        0 eth0
::1/128                                     ::
    U     0      0        1 lo
2001:0:0:20::2/128                          ::
    U     0      0        1 lo
fe80::20c:29ff:fed2:5e34/128                ::
    U     0      0        1 lo
ff00::/8                                    ::
    U     256    0        0 eth0
[root@client2 ~]# _
```

```
[root@server2 ~]# ping6 2001:0:0:20::2
PING 2001:0:0:20::2(2001:0:0:20::2) 56 data bytes
From 2001:0:0:10::1 icmp_seq=1 Destination unreachable: Administratively prohibi
ted
From 2001:0:0:10::1 icmp_seq=2 Destination unreachable: Administratively prohibi
ted
From 2001:0:0:10::1 icmp_seq=3 Destination unreachable: Administratively prohibi
ted
From 2001:0:0:10::1 icmp_seq=4 Destination unreachable: Administratively prohibi
ted
^C
--- 2001:0:0:20::2 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3758ms

[root@server2 ~]# _
```

```
[root@firewall ~]# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all      anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     ipv6-icmp    anywhere             anywhere
ACCEPT     all      anywhere             anywhere
ACCEPT     tcp      anywhere             anywhere            state NEW tcp dpt:s
sh
REJECT     all      anywhere             anywhere            reject-with icmp6-a
dm-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all      anywhere             anywhere            reject-with icmp6-a
dm-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@firewall ~]#
[root@firewall ~]# ip6tables -F
[root@firewall ~]# service ip6tables save
```

```
[root@server2 ~]# ping6 2001:0:0:20::2
PING 2001:0:0:20::2(2001:0:0:20::2) 56 data bytes
64 bytes from 2001:0:0:20::2: icmp_seq=1 ttl=63 time=6.19 ms
64 bytes from 2001:0:0:20::2: icmp_seq=2 ttl=63 time=1.08 ms
64 bytes from 2001:0:0:20::2: icmp_seq=3 ttl=63 time=1.08 ms
64 bytes from 2001:0:0:20::2: icmp_seq=4 ttl=63 time=1.02 ms
^C
--- 2001:0:0:20::2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3486ms
rtt min/avg/max/mdev = 1.028/2.347/6.191/2.219 ms
[root@server2 ~]#
```

```
[root@server2 ~]# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all      anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     ipv6-icmp    anywhere             anywhere
ACCEPT     all      anywhere             anywhere
ACCEPT     tcp      anywhere             anywhere            state NEW tcp dpt:s
sh
REJECT     all      anywhere             anywhere            reject-with icmp6-a
dm-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all      anywhere             anywhere            reject-with icmp6-a
dm-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@server2 ~]#
[root@server2 ~]# ip6tables -F
```

```
[root@client2 ~]# ip6tables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all      ::/0                 ::/0                state RELATED,ESTAB
LISHED
ACCEPT     icmpv6    ::/0                 ::/0
ACCEPT     all      ::/0                 ::/0
ACCEPT     tcp      ::/0                 ::/0                state NEW tcp dpt:2
2
REJECT     all      ::/0                 ::/0                reject-with icmp6-a
dm-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all      ::/0                 ::/0                reject-with icmp6-a
dm-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@client2 ~]# ip6tables -F
[root@client2 ~]# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[  OK  ]
```

```
[root@client2 ~]# ip6tables -L -n
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
[root@client2 ~]#
```

```
[root@firewall ~]# ip6tables -t filter -A INPUT -p icmpv6 -s 2001:0:0:10::2 -j D
ROP
[root@firewall ~]#
[root@firewall ~]# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       ipv6-icmp    2001:0:0:10::2/128   anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@firewall ~]#
```

```
[root@server2 ~]#
[root@server2 ~]# ping6 2001:0:0:10::1
PING 2001:0:0:10::1(2001:0:0:10::1) 56 data bytes
^C
--- 2001:0:0:10::1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2875ms

[root@server2 ~]# _
```

```
[root@client2 ~]# ping6 2001:0:0:20::1
PING 2001:0:0:20::1(2001:0:0:20::1) 56 data bytes
64 bytes from 2001:0:0:20::1: icmp_seq=1 ttl=64 time=1.57 ms
64 bytes from 2001:0:0:20::1: icmp_seq=2 ttl=64 time=0.562 ms
^C
--- 2001:0:0:20::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1773ms
rtt min/avg/max/mdev = 0.562/1.066/1.571/0.505 ms
[root@client2 ~]# _
```

```
[root@firewall ~]# ping6 2001:0:0:10::2
PING 2001:0:0:10::2(2001:0:0:10::2) 56 data bytes
From 2001:0:0:10::1 icmp_seq=2 Destination unreachable: Address unreachable
From 2001:0:0:10::1 icmp_seq=3 Destination unreachable: Address unreachable
From 2001:0:0:10::1 icmp_seq=4 Destination unreachable: Address unreachable
^C
--- 2001:0:0:10::2 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3353ms

[root@firewall ~]# ping6 2001:0:0:20::2
PING 2001:0:0:20::2(2001:0:0:20::2) 56 data bytes
64 bytes from 2001:0:0:20::2: icmp_seq=1 ttl=64 time=2.61 ms
64 bytes from 2001:0:0:20::2: icmp_seq=2 ttl=64 time=0.595 ms
^C
--- 2001:0:0:20::2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1670ms
rtt min/avg/max/mdev = 0.595/1.605/2.616/1.011 ms
[root@firewall ~]#
```

```
[root@firewall ~]# ping6 2001:0:0:10::2
PING 2001:0:0:10::2(2001:0:0:10::2) 56 data bytes
From 2001:0:0:10::1 icmp_seq=2 Destination unreachable: Address unreachable
From 2001:0:0:10::1 icmp_seq=3 Destination unreachable: Address unreachable
From 2001:0:0:10::1 icmp_seq=4 Destination unreachable: Address unreachable
^C
--- 2001:0:0:10::2 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3353ms

[root@firewall ~]# ping6 2001:0:0:20::2
PING 2001:0:0:20::2(2001:0:0:20::2) 56 data bytes
64 bytes from 2001:0:0:20::2: icmp_seq=1 ttl=64 time=2.61 ms
64 bytes from 2001:0:0:20::2: icmp_seq=2 ttl=64 time=0.595 ms
^-
```

```
[root@firewall ~]# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       ipv6-icmp    anywhere            anywhere            ipv6-icmp echo-
request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

```
[root@server2 ~]# ping6 2001:0:0:10::1
PING 2001:0:0:10::1(2001:0:0:10::1) 56 data bytes
^C
--- 2001:0:0:10::1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3105ms
```

```
[root@client2 ~]# ping6 2001:0:0:20::1
PING 2001:0:0:20::1(2001:0:0:20::1) 56 data bytes
^C
--- 2001:0:0:20::1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3165ms
```

```
[root@firewall ~]# ip6tables -t filter -D INPUT -p icmpv6 --icmpv6-type echo-req
uest -j DROP
```

```
[root@server2 ~]# telnet 2001:0:0:10::1
Trying 2001:0:0:10::1...
Connected to 2001:0:0:10::1.
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.3 (Santiago)
Kernel 2.6.32-279.el6.x86_64 on an x86_64
login: vipin
Password:
Last login: Fri Nov  4 15:19:13 from firewall
[vipin@firewall ~]$
```

```
[root@server2 ~]# ssh vipin@2001:0:0:10::1
vipin@2001:0:0:10::1's password:
Last login: Sat Nov  5 00:11:35 2016 from 2001:0:0:10::2
[vipin@firewall ~]$
```

```
[root@server2 ~]# elinks --dump http://[2001:0:0:10::1]
   wel to ipv6
[root@server2 ~]#
```

```
[root@firewall ~]# ip6tables -t filter -A INPUT -p tcp -s 2001:0:0:10::2 --dport
 22 -j DROP
[root@firewall ~]# ip6tables -t filter -A INPUT -m multiport -p tcp -s 2001:0:0:
10::2 --dports 23,80 -j DROP
[root@firewall ~]#
[root@firewall ~]# ip6tables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp      2001:0:0:10::2/128   ::/0                tcp dpt:22
DROP       tcp      2001:0:0:10::2/128   ::/0                multiport dports 23
,80

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@firewall ~]# _
```

```
[root@server2 ~]# telnet 2001:0:0:10::1
Trying 2001:0:0:10::1...
^C
[root@server2 ~]# ssh vipin@2001:0:0:10::1
ssh: connect to host 2001:0:0:10::1 port 22: Connection timed out
[root@server2 ~]#
[root@server2 ~]# elinks --dump http://[2001:0:0:10::1]
ELinks: Connection timed out
[root@server2 ~]#
[root@server2 ~]# ping6 -c2 2001:0:0:10::1
PING 2001:0:0:10::1(2001:0:0:10::1) 56 data bytes
64 bytes from 2001:0:0:10::1: icmp_seq=1 ttl=64 time=13.0 ms
64 bytes from 2001:0:0:10::1: icmp_seq=2 ttl=64 time=0.474 ms
```

```
[root@firewall ~]# ip6tables -t filter -A INPUT -p icmpv6 -j LOG --log-prefix "p
ing6 denied"
[root@firewall ~]#
[root@firewall ~]# ip6tables -t filter -A INPUT -p icmpv6 -j REJECT --reject-wit
h icmp6-adm-prohibited
[root@firewall ~]#
[root@firewall ~]# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp      2001:0:0:10::2/128   anywhere            tcp dpt:ssh
DROP       tcp      2001:0:0:10::2/128   anywhere            multiport dports te
lnet,http
LOG        ipv6-icmp    anywhere             anywhere            LOG level warni
ng prefix `ping6 denied'
REJECT     ipv6-icmp    anywhere             anywhere            reject-with icm
p6-adm-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@firewall ~]# _
```

```
[root@server2 ~]# ping6 2001:0:0:10::1
PING 2001:0:0:10::1(2001:0:0:10::1) 56 data bytes
From 2001:0:0:10::2 icmp_seq=1 Destination unreachable: Address unreachable
From 2001:0:0:10::2 icmp_seq=2 Destination unreachable: Address unreachable
From 2001:0:0:10::2 icmp_seq=3 Destination unreachable: Address unreachable
From 2001:0:0:10::2 icmp_seq=4 Destination unreachable: Address unreachable
From 2001:0:0:10::2 icmp_seq=5 Destination unreachable: Address unreachable
From 2001:0:0:10::2 icmp_seq=6 Destination unreachable: Address unreachable
^C
--- 2001:0:0:10::1 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6384ms
```

```
[root@firewall ~]# tail -2 /var/log/messages
Nov  5 13:06:46 firewall kernel: ping6 deniedIN=eth0 OUT= MAC=33:33:ff:00:00:01:
00:0c:29:3d:e2:b7:86:dd SRC=2001:0000:0000:0010:0000:0000:0000:0002 DST=ff02:000
0:0000:0000:0000:0001:ff00:0001 LEN=72 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=ICMPv6
TYPE=135 CODE=0
Nov  5 13:06:46 firewall kernel: ping6 deniedIN=eth1 OUT= MAC=33:33:ff:00:00:01:
00:0c:29:3d:e2:b7:86:dd SRC=2001:0000:0000:0010:0000:0000:0000:0002 DST=ff02:000
0:0000:0000:0000:0001:ff00:0001 LEN=72 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=ICMPv6
TYPE=135 CODE=0
[root@firewall ~]#
```

```
[root@server2 ~]# ping6 -c1 2001:0:0:20::2 |head -2
PING 2001:0:0:20::2(2001:0:0:20::2) 56 data bytes
64 bytes from 2001:0:0:20::2: icmp_seq=1 ttl=127 time=0.840 ms
[root@server2 ~]#
[root@server2 ~]# ssh aanya@2001:0:0:20::2
aanya@2001:0:0:20::2's password:
Last login: Sat Nov  5 13:35:16 2016 from 2001:0:0:10::2
[aanya@client2 ~]$ logout
Connection to 2001:0:0:20::2 closed.
[root@server2 ~]#
[root@server2 ~]# telnet 2001:0:0:20::2
Trying 2001:0:0:20::2...
Connected to 2001:0:0:20::2.
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.3 (Santiago)
Kernel 2.6.32-279.el6.x86_64 on an x86_64
login: aanya
Password:
Last login: Sat Nov  5 13:35:50 from 2001:0:0:10::2
[aanya@client2 ~]$ Connection closed by foreign host.
[root@server2 ~]#
```

```
[root@firewall ~]# ip6tables -t filter -A FORWARD -p tcp -s 2001:0:0:10::/64 -d
2001:0:0:20::2 --dport 23 -j DROP
[root@firewall ~]#
[root@firewall ~]# ip6tables -t filter -A FORWARD -p tcp -s 2001:0:0:10::/64 -d
2001:0:0:20::2 --dport 22 -j DROP
[root@firewall ~]#
[root@firewall ~]# ip6tables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp      2001:0:0:10::/64     2001:0:0:20::2/128  tcp dpt:23
2    DROP       tcp      2001:0:0:10::/64     2001:0:0:20::2/128  tcp dpt:22

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

```
[root@server2 ~]#
[root@server2 ~]# ssh aanya@2001:0:0:20::2
^C
[root@server2 ~]# telnet 2001:0:0:20::2
Trying 2001:0:0:20::2...
^C
[root@server2 ~]# ping6 -c1 2001:0:0:20::2 |head -2
PING 2001:0:0:20::2(2001:0:0:20::2) 56 data bytes
64 bytes from 2001:0:0:20::2: icmp_seq=1 ttl=127 time=2.55 ms
```

```
[root@firewall ~]# ip6tables -t filter -A FORWARD -p icmpv6 -s 2001:0:0:10::/64
-d 2001:0:0:20::2  -j DROP
[root@firewall ~]#
[root@firewall ~]# ip6tables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       icmpv6    2001:0:0:10::/64     2001:0:0:20::2/128

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@firewall ~]# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       ipv6-icmp    2001:0:0:10::/64     2001:0:0:20::2/128

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@firewall ~]# _
```

```
[root@server2 ~]# ping6 2001:0:0:20::2
PING 2001:0:0:20::2(2001:0:0:20::2) 56 data bytes
^C
--- 2001:0:0:20::2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time

[root@server2 ~]# telnet 2001:0:0:20::2
Trying 2001:0:0:20::2...
Connected to 2001:0:0:20::2.
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.3 (Santiago)
Kernel 2.6.32-279.el6.x86_64 on an x86_64
login: aanya
Password:
Last login: Sat Nov  5 13:36:03 from 2001:0:0:10::2
[aanya@client2 ~]$ ogout
Connection closed by foreign host.
[root@server2 ~]# ssh aanya@2001:0:0:20::2
aanya@2001:0:0:20::2's password:
Last login: Sat Nov  5 14:26:45 2016 from 2001:0:0:10::2
[aanya@client2 ~]$
```

```
[root@firewall ~]# ip6tables -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
[root@firewall ~]#
[root@firewall ~]# ip6tables -P INPUT DROP
[root@firewall ~]# ip6tables -P OUTPUT DROP
[root@firewall ~]# ip6tables -P FORWARD DROP
[root@firewall ~]#
[root@firewall ~]# ip6tables -L
Chain INPUT (policy DROP)
target     prot opt source                destination

Chain FORWARD (policy DROP)
target     prot opt source                destination

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

```
[root@server2 ~]# telnet 2001:0:0:10::1
Trying 2001:0:0:10::1...
^C
[root@server2 ~]# ssh vipin@2001:0:0:10::1
ssh: connect to host 2001:0:0:10::1 port 22: No route to host
[root@server2 ~]# ^C
[root@server2 ~]# ping6 2001:0:0:10::1
PING 2001:0:0:10::1(2001:0:0:10::1) 56 data bytes
^C
--- 2001:0:0:10::1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1479ms

[root@server2 ~]# elinks --dump http://[2001:0:0:10::1]
ELinks: No route to host
[root@server2 ~]#
```

```
[root@firewall ~]# ip6tables -A INPUT -p tcp -m state --state NEW --dport 23 -j
ACCEPT
[root@firewall ~]#
[root@firewall ~]# ip6tables -A OUTPUT -p tcp -m state --state ESTABLISHED,RELAT
ED -j ACCEPT
[root@firewall ~]#
[root@firewall ~]# ip6tables -A INPUT -p tcp -m state --state ESTABLISHED,RELATE
D -j ACCEPT
[root@firewall ~]#
[root@firewall ~]# ip6tables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp      anywhere             anywhere            state NEW tcp dpt:t
elnet
ACCEPT     tcp      anywhere             anywhere            state RELATED,ESTAB
LISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp      anywhere             anywhere            state RELATED,ESTAB
LISHED
```

```
[root@server2 ~]# telnet 2001:0:0:10::1
Trying 2001:0:0:10::1...
telnet: connect to address 2001:0:0:10::1: No route to host
[root@server2 ~]# _
```

```
[root@firewall ~]# ip6tables -A INPUT -p icmpv6 -j ACCEPT
[root@firewall ~]# ip6tables -A OUTPUT -p icmpv6 -j ACCEPT
[root@firewall ~]#
[root@firewall ~]# ip6tables -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp      ::/0                 ::/0                 state NEW tcp
dpt:23
2    ACCEPT     tcp      ::/0                 ::/0                 state RELATED,
ESTABLISHED
3    ACCEPT     icmpv6    ::/0                  ::/0

Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp      ::/0                 ::/0                 state RELATED,
ESTABLISHED
2    ACCEPT     icmpv6    ::/0                  ::/0
[root@firewall ~]# _
```

```
[root@server2 ~]# telnet 2001:0:0:10::1
Trying 2001:0:0:10::1...
Connected to 2001:0:0:10::1.
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.3 (Santiago)
Kernel 2.6.32-279.el6.x86_64 on an x86_64
login: vipin
Password:
Last login: Sat Nov  5 00:11:44 from 2001:0:0:10::2
[vipin@firewall ~]$ logout
Connection closed by foreign host.
[root@server2 ~]#
[root@server2 ~]# ssh vipin@2001:0:0:10::1
ssh: connect to host 2001:0:0:10::1 port 22: Connection timed out
[root@server2 ~]# _
```

```
[root@firewall ~]# ip6tables -A INPUT -p tcp -m state --state NEW --dport 22 -j
ACCEPT
[root@firewall ~]# ip6tables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp      anywhere             anywhere            state NEW tcp dpt:t
elnet
ACCEPT     tcp      anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     ipv6-icmp    anywhere             anywhere
ACCEPT     tcp      anywhere             anywhere            state NEW tcp dpt:s
sh

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp      anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     ipv6-icmp    anywhere             anywhere
[root@firewall ~]#
```

```
[root@server2 ~]# ssh vipin@2001:0:0:10::1
vipin@2001:0:0:10::1's password:
Last login: Sat Nov  5 15:06:28 2016 from 2001:0:0:10::2
[vipin@firewall ~]$ logout
Connection to 2001:0:0:10::1 closed.
[root@server2 ~]# telnet 2001:0:0:10::1
Trying 2001:0:0:10::1...
Connected to 2001:0:0:10::1.
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.3 (Santiago)
Kernel 2.6.32-279.el6.x86_64 on an x86_64
login: vipin
Password:
Last login: Sat Nov  5 15:15:58 from 2001:0:0:10::2
[vipin@firewall ~]$ Connection closed by foreign host.
[root@server2 ~]#
```

```
[root@firewall ~]# ip6tables -F
[root@firewall ~]# ip6tables -L
Chain INPUT (policy DROP)
target     prot opt source                                destination

Chain FORWARD (policy DROP)
target     prot opt source                                destination

Chain OUTPUT (policy DROP)
target     prot opt source                                destination
[root@firewall ~]#
[root@firewall ~]# ip6tables -P INPUT ACCEPT
[root@firewall ~]# ip6tables -P OUTPUT ACCEPT
[root@firewall ~]# ip6tables -P FORWARD ACCEPT
[root@firewall ~]#
[root@firewall ~]# ip6tables -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
[root@firewall ~]# _
```

Reference: “Linux Essentials, Services & Security” by Vipin Gupta

https://www.youtube.com/techji

https://www.udemy.com/course/mastering-iptables-firewall