

# Firewall Assignment

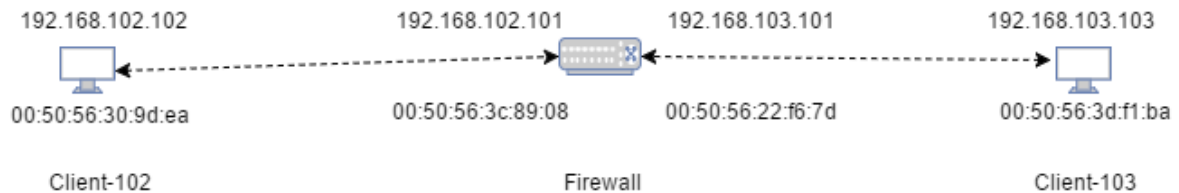
Group Members:

Mrinal Aich - cs16mtech11009

Tulja Vamshi Kiran – cs16mtech11020

## Network Architecture:

The network consists of two Clients in different subnets 192.168.102.0/24 and 192.168.103.0/24. They are connected to the Firewall with their default gateway.



## Task 1:

The forwarding logic is handled entirely by the Firewall program. Hence, IP Forwarding is not allowed at the Firewall's kernel.

## Case 1: Layer-3 forwarding using ICMP Protocol

```
root_michail102
root@ubuntu:/home/michail/work102# ifconfig ens33
ens33      Link encap:Ethernet  HWaddr 00:50:56:30:9d:ea
            inet addr:192.168.102.102  Bcast:192.168.102.255  Mask:255.255.255.0
            inet6 addr: fe80::250:56ff:fe30:9dea/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:48457 errors:0 dropped:0 overruns:0 frame:0
            TX packets:64733 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:12826001 (12.8 MB)  TX bytes:96822323 (96.8 MB)
            Interrupt:19 Base address:0x2000

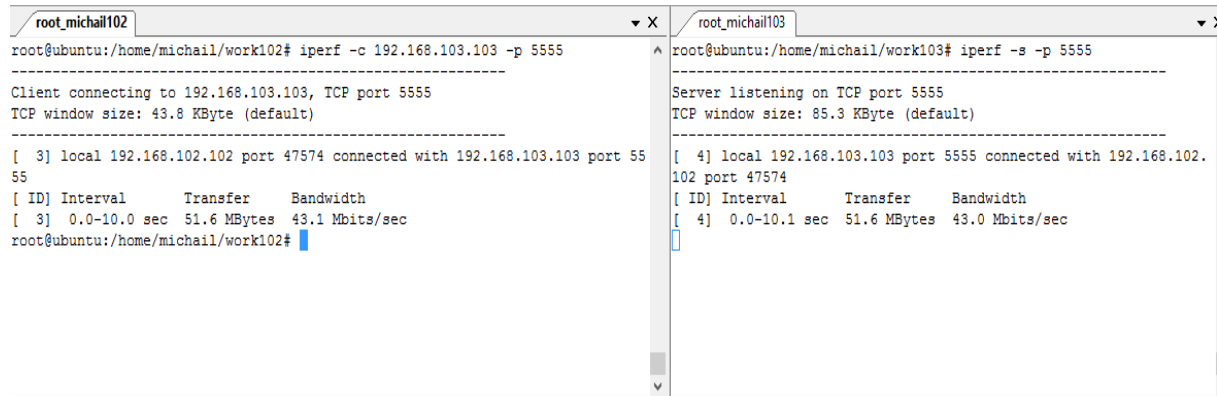
root@ubuntu:/home/michail/work102# ping 192.168.103.103 -c 2
PING 192.168.103.103 (192.168.103.103) 56(84) bytes of data.
64 bytes from 192.168.103.103: icmp_seq=1 ttl=64 time=1.39 ms
64 bytes from 192.168.103.103: icmp_seq=2 ttl=64 time=1.18 ms

--- 192.168.103.103 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.187/1.293/1.399/0.106 ms
root@ubuntu:/home/michail/work102#
```

### Case 2: Layer-4 forwarding using IPerf Application

'Host103' is running an IPerf server at port 5555, and 'Host102' acts as the IPerf client.

The measured bandwidth is **45.1 Mbps**.



```
root_michail102 root_michail103
root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 -p 5555
Client connecting to 192.168.103.103, TCP port 5555
TCP window size: 43.8 KByte (default)

[ 3] local 192.168.102.102 port 47574 connected with 192.168.103.103 port 5555
[ ID] Interval      Transfer    Bandwidth
[ 3]  0.0-10.0 sec  51.6 MBytes 43.1 Mbits/sec
root@ubuntu:/home/michail/work102#

root@ubuntu:/home/michail/work103# iperf -s -p 5555
Server listening on TCP port 5555
TCP window size: 85.3 KByte (default)

[ 4] local 192.168.103.103 port 5555 connected with 192.168.102.102 port 47574
[ ID] Interval      Transfer    Bandwidth
[ 4]  0.0-10.1 sec  51.6 MBytes 43.0 Mbits/sec
```

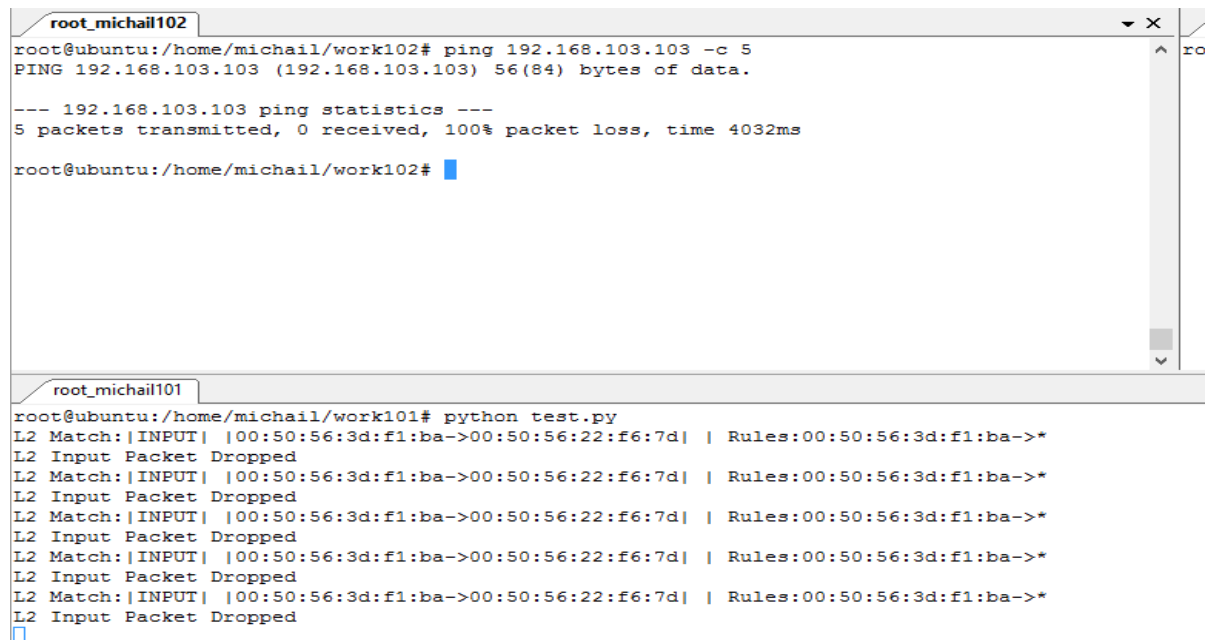
### Firewall Block Scenarios

Case 3: Layer-2 packets filtered by the Firewall.

The rule-set used:

On INPUT chain, L2 Packets with MAC Address: "00:50:56:3d:f1:ba" DROP

i.e. All L2 packets coming from 'Host103' gets dropped.



```
root_michail102 root_michail101
root@ubuntu:/home/michail/work102# ping 192.168.103.103 -c 5
PING 192.168.103.103 (192.168.103.103) 56(84) bytes of data.

--- 192.168.103.103 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4032ms

root@ubuntu:/home/michail/work102#

root@ubuntu:/home/michail/work101# python test.py
L2 Match:|INPUT| |00:50:56:3d:f1:ba->00:50:56:22:f6:7d| | Rules:00:50:56:3d:f1:ba->*
L2 Input Packet Dropped
L2 Match:|INPUT| |00:50:56:3d:f1:ba->00:50:56:22:f6:7d| | Rules:00:50:56:3d:f1:ba->*
L2 Input Packet Dropped
L2 Match:|INPUT| |00:50:56:3d:f1:ba->00:50:56:22:f6:7d| | Rules:00:50:56:3d:f1:ba->*
L2 Input Packet Dropped
L2 Match:|INPUT| |00:50:56:3d:f1:ba->00:50:56:22:f6:7d| | Rules:00:50:56:3d:f1:ba->*
L2 Input Packet Dropped
L2 Match:|INPUT| |00:50:56:3d:f1:ba->00:50:56:22:f6:7d| | Rules:00:50:56:3d:f1:ba->*
L2 Input Packet Dropped
```

All the ARP Reply packets sent by 'Host102' are dropped by the INPUT chain.

Case 4: Layer-3 packets filtered by the Firewall.

The rule-set used:

On OUTPUT chain, L3 Packets with IP Address: "192.168.102.102" DROP

i.e. All L3 packets going towards 'Host102' gets dropped.

```
root_michail102
root@ubuntu:/home/michail/work102# ping 192.168.103.103 -c 5
PING 192.168.103.103 (192.168.103.103) 56(84) bytes of data.

--- 192.168.103.103 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4032ms

root@ubuntu:/home/michail/work102#

root_michail101
root@ubuntu:/home/michail/work101# python test.py
L3 Match:|OUTPUT ICMP| |192.168.102.101->192.168.102.102| | Rules:*->192.168.102.102
L3 Output Packet Dropped
L3 Match:|OUTPUT ICMP| |192.168.102.101->192.168.102.102| | Rules:*->192.168.102.102
L3 Output Packet Dropped
L3 Match:|OUTPUT ICMP| |192.168.102.101->192.168.102.102| | Rules:*->192.168.102.102
L3 Output Packet Dropped
L3 Match:|OUTPUT ICMP| |192.168.102.101->192.168.102.102| | Rules:*->192.168.102.102
L3 Output Packet Dropped
L3 Match:|OUTPUT ICMP| |192.168.102.101->192.168.102.102| | Rules:*->192.168.102.102
L3 Output Packet Dropped
```

All ICMP Reply packets towards 'Host102' gets dropped by the OUTPUT chain.

## Case 5: Layer-4 packets filtered by the Firewall.

The rule-set used:

On INPUT chain, L4 TCP Packets with Source Port: "5555" DROP

i.e. All L4 TCP packets sent by Source Port 5555 gets dropped.

```
root_michail102
root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 -p 5555

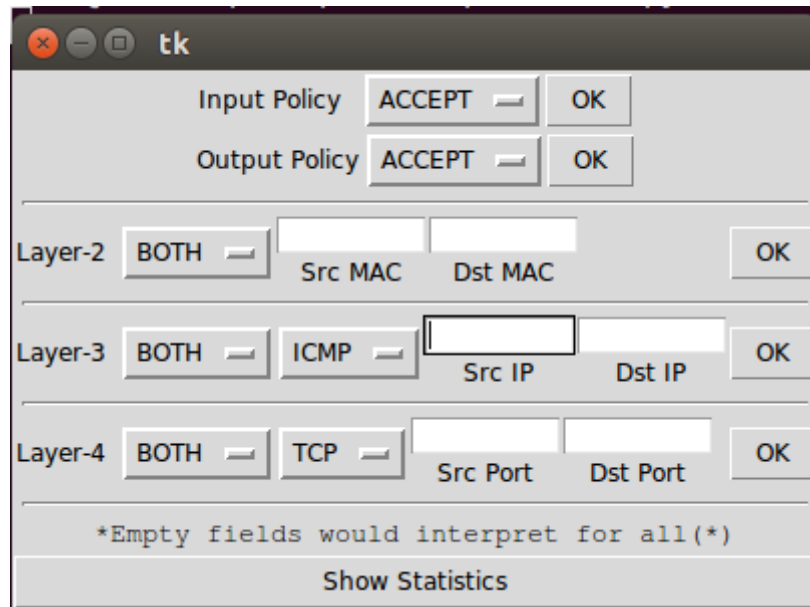
root_michail103
root@ubuntu:/home/michail/work103# iperf -s -p 5555
-----
Server listening on TCP port 5555
TCP window size: 85.3 KByte (default)
-----

root_michail101
root@ubuntu:/home/michail/work101# python test.py
L4 Input Packet Dropped
L4 Input Packet Dropped
L4 Input Packet Dropped
L4 Input Packet Dropped
L4 Input Packet Dropped
L4 Input Packet Dropped
L4 Input Packet Dropped
```

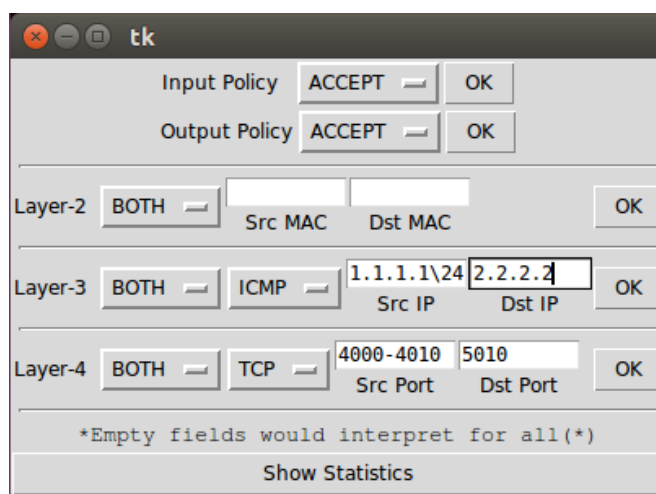
All TCP Syn packets sent by 'Host102' with Source Port =5555 gets dropped by the INPUT chain.

## Task 2: Graphical User Interface of the Firewall

The GUI was developed using Tkinter and it looks like



1. INPUT/OUTPUT Chain  
The user can select a default Input/Output Policy as 'Accept' or 'Drop'.  
On selecting a default policy, all the rules on that chain would be reset.
2. 'BOTH' in the Drop down menu signify the rule would be for both Input and Output Chain.
3. If a respective field is empty, the it is interpreted as '\*' ( for all).
4. Layer-3 supported protocols are 'IPv4' and 'IPv6'.
5. Layer-4 supported protocols are 'TCP' and 'UDP'.
6. Aggregation of IP prefix and Port-range are also handled.

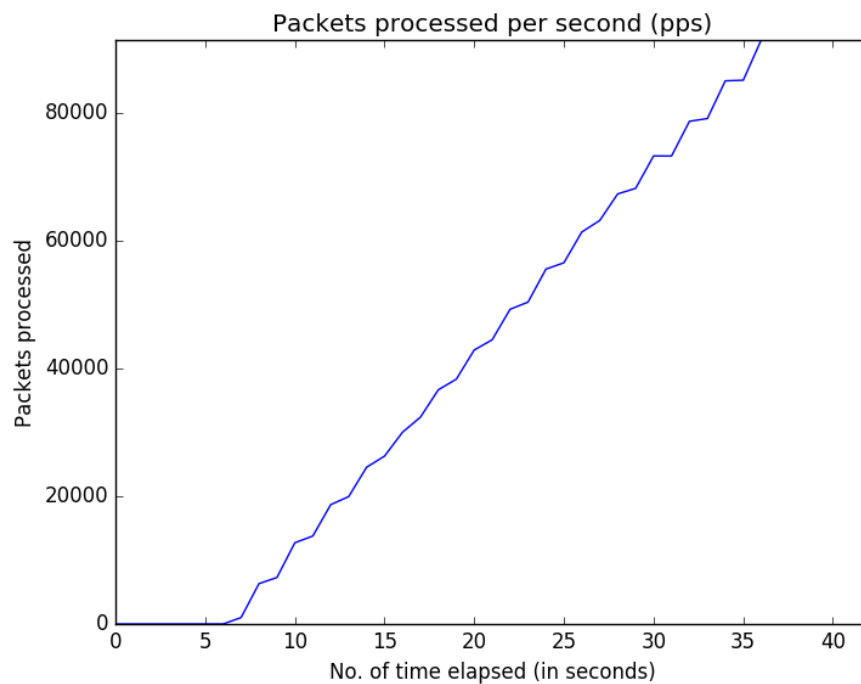


Eg. Layer-3: All source IP packets from 1.1.1.1\24 to 2.2.2.2 to be dropped.

Layer-4: All packets with source ports from 4000 to 4010 to destination port 5010 to be dropped.

7. 'Show Statistics' displays the total number of packets processed by the firewall .It also displays the Packet Counts in terms of Layer2,Layer3 andLayer4 along with the no. of packets that are being dropped by the firewall.

A graph is plotted with the time (in secs) in X-axis and Packets processed in the Y-axis.



Plot for an IPerf application starts at time (t=6) and finishes at time (t=36). The number of packets processed per second increases gradually with time. The bandwidth achieved was 46.8 Mbps.

### Task 3: Performance examination and improvement

#### (i). Measuring performance

Performance is measured by the *throughput* achieved via the firewall.

A single controlled traffic will be generated by 'Host102' to 'Host103'. The throughput achieved by the hosts will be considered as the throughput of the firewall.

(On an average the throughput for an IPerf application is close to 50 Mbps using our implementation.)

#### (ii). PPS handled by the firewall -

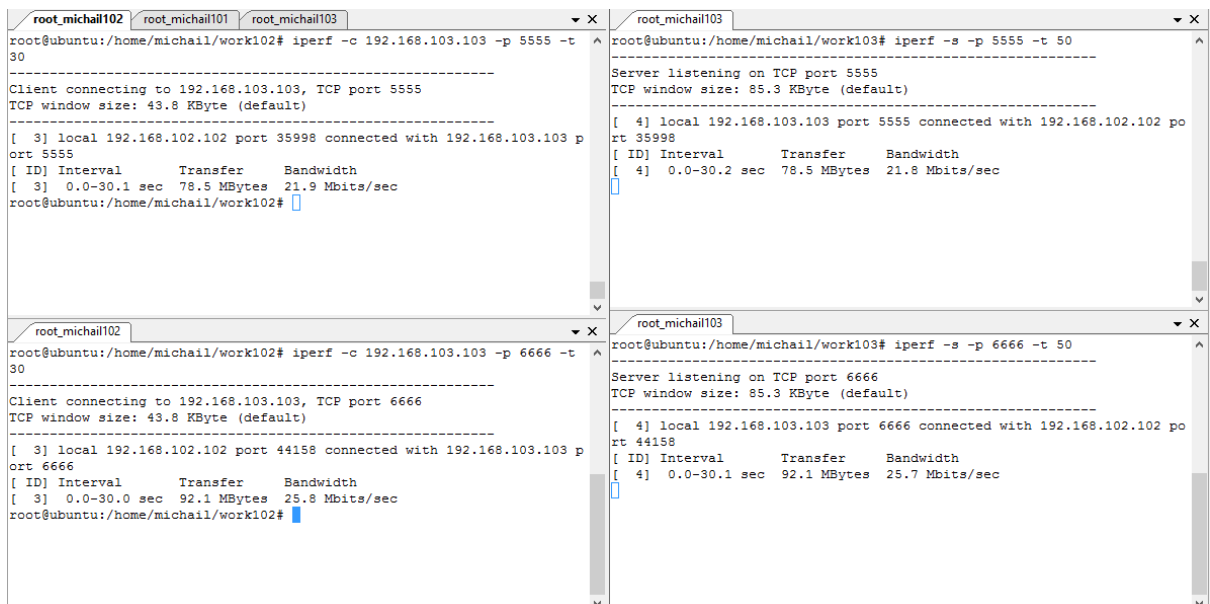
On average the packets processed per second by the firewall is close to 100000 IPerf packets.

#### (iii). Change of performance if drop or pass the packet -

Considerable change is observed if particular packets are dropped by the firewall.

Scenario: Two IPerf servers are running on 'Host103' at ports 5555 and 6666.

'Host103' runs two IPerf clients and connects to 'Host103'.



The screenshot displays four terminal windows arranged in a 2x2 grid, showing IPerf performance tests. The top-left window (root\_michail102) shows a client connecting to 192.168.103.103 on port 5555, achieving a bandwidth of 21.9 Mbps. The top-right window (root\_michail103) shows a server listening on port 5555, receiving a bandwidth of 21.8 Mbps. The bottom-left window (root\_michail102) shows a client connecting to 192.168.103.103 on port 6666, achieving a bandwidth of 25.8 Mbps. The bottom-right window (root\_michail103) shows a server listening on port 6666, receiving a bandwidth of 25.7 Mbps. All tests were run for 30 seconds.

```
root_michail102 root_michail101 root_michail103 root_michail103
root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 -p 5555 -t 30
-----
Client connecting to 192.168.103.103, TCP port 5555
TCP window size: 43.8 KByte (default)
-----
[ 3] local 192.168.102.102 port 35998 connected with 192.168.103.103 port 5555
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-30.1 sec  78.5 MBytes  21.9 Mbits/sec
root@ubuntu:/home/michail/work102#

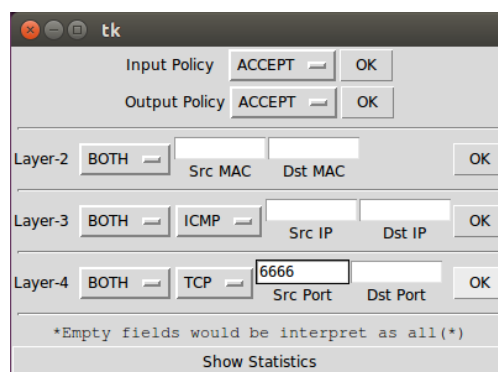
root@ubuntu:/home/michail/work103# iperf -s -p 5555 -t 50
-----
Server listening on TCP port 5555
TCP window size: 85.3 KByte (default)
-----
[ 4] local 192.168.103.103 port 5555 connected with 192.168.102.102 port 35998
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.0-30.2 sec  78.5 MBytes  21.8 Mbits/sec

root_michail102 root_michail103
root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 -p 6666 -t 30
-----
Client connecting to 192.168.103.103, TCP port 6666
TCP window size: 43.8 KByte (default)
-----
[ 3] local 192.168.102.102 port 44158 connected with 192.168.103.103 port 6666
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-30.0 sec  92.1 MBytes  25.8 Mbits/sec
root@ubuntu:/home/michail/work102#

root@ubuntu:/home/michail/work103# iperf -s -p 6666 -t 50
-----
Server listening on TCP port 6666
TCP window size: 85.3 KByte (default)
-----
[ 4] local 192.168.103.103 port 6666 connected with 192.168.102.102 port 44158
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.0-30.1 sec  92.1 MBytes  25.7 Mbits/sec
```

Analysis: The two IPerf Clients are getting shared throughput of 21.9 Mbps and 25.0 Mbps.

Scenario: One IPerf flow is blocked by the firewall, say all TCP traffic to port 6666 gets dropped.



The screenshot shows a window titled 'tk' with a grey background. It contains several sections for configuring firewall rules. The 'Input Policy' and 'Output Policy' are both set to 'ACCEPT'. Below these, there are sections for 'Layer-2', 'Layer-3', and 'Layer-4'. 'Layer-2' has 'BOTH' selected for the policy, with empty fields for 'Src MAC' and 'Dst MAC'. 'Layer-3' has 'BOTH' selected for the policy, 'ICMP' selected for the protocol, and empty fields for 'Src IP' and 'Dst IP'. 'Layer-4' has 'BOTH' selected for the policy, 'TCP' selected for the protocol, and '6666' entered in the 'Src Port' field, with an empty field for 'Dst Port'. At the bottom, there is a note: '\*Empty fields would be interpret as all(\*)' and a 'Show Statistics' button.

```

root_michail102 root_michail101 root_michail103 root_michail103
root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 -p 5555 -t 30
-----
Client connecting to 192.168.103.103, TCP port 5555
TCP window size: 43.8 KByte (default)
-----
[ 3] local 192.168.102.102 port 36722 connected with 192.168.103.103 port 5555
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-30.2 sec  167 MBytes  46.4 Mbits/sec
root@ubuntu:/home/michail/work102#

root@ubuntu:/home/michail/work103# iperf -s -p 5555 -t 50
-----
Server listening on TCP port 5555
TCP window size: 85.3 KByte (default)
-----
[ 4] local 192.168.103.103 port 5555 connected with 192.168.102.102 port 36722
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.0-30.4 sec  167 MBytes  46.1 Mbits/sec

root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 -p 6666 -t 30
-----
Client connecting to 192.168.103.103, TCP port 6666
TCP window size: 43.8 KByte (default)
-----
[ 3] local 192.168.102.102 port 36722 connected with 192.168.103.103 port 6666
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-30.2 sec  167 MBytes  46.4 Mbits/sec
root@ubuntu:/home/michail/work102#

root@ubuntu:/home/michail/work103# iperf -s -p 6666 -t 50
-----
Server listening on TCP port 6666
TCP window size: 85.3 KByte (default)
-----
[ 4] local 192.168.103.103 port 6666 connected with 192.168.102.102 port 36722
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.0-30.4 sec  167 MBytes  46.1 Mbits/sec

```

Analysis: On blocking one IPerf flow by the firewall, the throughput of the other flow increases. IPerf packets for port 5555 are successful and for port 6666 are dropped by the firewall. Due to this, the throughput of the valid flow increases to 46.4 Mbps.

(v). Increase the number of matching fields in a filtering rule (MAC address only or Prefix/Port/Protocol combination).

Scenario: Added 200 Rules to drop TCP packets in range Source Ports 4000-4100 and Destination Port:1111. On running the IPerf client-server as before over port 5555.

tk

Input Policy: ACCEPT OK

Output Policy: ACCEPT OK

Layer-2: BOTH Src MAC Dst MAC OK

Layer-3: BOTH ICMP Src IP Dst IP OK

Layer-4: BOTH TCP 4000-4100 1111 OK

\*Empty fields would be interpret as all(\*)

Show Statistics

```

root_michail102 root_michail101 root_michail103
root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 -p 5555 -t 30
-----
Client connecting to 192.168.103.103, TCP port 5555
TCP window size: 43.8 KByte (default)
-----
[ 3] local 192.168.102.102 port 41574 connected with 192.168.103.103 port 5555
[ ID] Interval      Transfer    Bandwidth
[ 3]  0.0-30.2 sec  79.2 MBytes  22.0 Mbits/sec
root@ubuntu:/home/michail/work102#

root@ubuntu:/home/michail/work103# iperf -s -p 5555 -t 50
-----
Server listening on TCP port 5555
TCP window size: 85.3 KByte (default)
-----
[ 4] local 192.168.103.103 port 5555 connected with 192.168.102.102 port 41574
[ ID] Interval      Transfer    Bandwidth
[ 4]  0.0-30.4 sec  79.2 MBytes  21.9 Mbits/sec

```

Analysis: The rule matching would be done by the firewall, thus increasing the delay in forwarding the traffic which decreases the throughput from 50 Mbps(avg.) to 22 Mbps.

(vi). Controlled or random traffic, to benchmark the system.

Controlled traffic is generated by a single IPerf application to get achieve the maximum throughput of the firewall. On avg. the value is 50 Mbps.

```

root_michail102 root_michail103
root@ubuntu:/home/michail/work102# ifconfig ens33
ens33      Link encap:Ethernet  HWaddr 00:50:56:30:9d:ea
          inet addr:192.168.102.102  Bcast:192.168.102.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe30:9dea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48471 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64735 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12827818 (12.8 MB)  TX bytes:96822519 (96.8 MB)
          Interrupt:19 Base address:0x2000

root@ubuntu:/home/michail/work102# iperf -c 192.168.103.103 5555
iperf: ignoring extra argument -- 5555
-----
Client connecting to 192.168.103.103, TCP port 5001
TCP window size: 43.8 KByte (default)
-----
[ 3] local 192.168.102.102 port 58982 connected with 192.168.103.103 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3]  0.0-10.3 sec  10.2 MBytes  8.38 Mbits/sec
root@ubuntu:/home/michail/work102#

root@ubuntu:/home/michail/work103# ifconfig ens33
ens33      Link encap:Ethernet  HWaddr 00:50:56:3d:f1:ba
          inet addr:192.168.103.103  Bcast:192.168.103.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe3d:f1ba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:729035 errors:1 dropped:13 overruns:0 frame:0
          TX packets:1414441 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:215769562 (215.7 MB)  TX bytes:2047253811 (2.0 GB)
          Interrupt:19 Base address:0x2000

root@ubuntu:/home/michail/work103# iperf -s 5555
iperf: ignoring extra argument -- 5555
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
[ 4] local 192.168.103.103 port 5001 connected with 192.168.102.102 port 58982
[ ID] Interval      Transfer    Bandwidth
[ 4]  0.0-10.4 sec  10.2 MBytes  8.29 Mbits/sec

```



Random Traffic is generated by running 4 IPerf servers at Host103 and being accessed by Host102. The throughput of all the applications is reduced considerably.

<div>root_michail102</div> <div>root_michail101</div> <div>[ 3] local 192.168.102.102 port 45784 connected with 192.168.103.103 port 5555</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 3] 0.0-30.3 sec 44.1 MBytes 12.2 Mbits/sec</div> <div>root@ubuntu:/home/michail/work102#</div>	<div>root_michail103</div> <div>[ 4] local 192.168.103.103 port 5555 connected with 192.168.102.102 port 45784</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 4] 0.0-30.6 sec 44.1 MBytes 12.1 Mbits/sec</div>
<div>root_michail102</div> <div>[ 3] local 192.168.102.102 port 51600 connected with 192.168.103.103 port 5556</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 3] 0.0-30.0 sec 21.5 MBytes 6.00 Mbits/sec</div> <div>root@ubuntu:/home/michail/work102#</div>	<div>root_michail103</div> <div>[ 4] local 192.168.103.103 port 5556 connected with 192.168.102.102 port 51600</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 4] 0.0-30.4 sec 21.5 MBytes 5.94 Mbits/sec</div>
<div>root_michail102</div> <div>Client connecting to 192.168.103.103, TCP port 5557</div> <div>TCP window size: 43.8 KByte (default)</div> <div>[ 3] local 192.168.102.102 port 52612 connected with 192.168.103.103 port 5557</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 3] 0.0-30.0 sec 49.5 MBytes 13.8 Mbits/sec</div> <div>root@ubuntu:/home/michail/work102#</div>	<div>root_michail103</div> <div>Server listening on TCP port 5557</div> <div>TCP window size: 85.3 KByte (default)</div> <div>[ 4] local 192.168.103.103 port 5557 connected with 192.168.102.102 port 52612</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 4] 0.0-30.2 sec 49.5 MBytes 13.7 Mbits/sec</div>
<div>root_michail102</div> <div>Client connecting to 192.168.103.103, TCP port 5558</div> <div>TCP window size: 43.8 KByte (default)</div> <div>[ 3] local 192.168.102.102 port 37186 connected with 192.168.103.103 port 5558</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 3] 0.0-30.0 sec 36.0 MBytes 10.1 Mbits/sec</div> <div>root@ubuntu:/home/michail/work102#</div>	<div>root_michail103</div> <div>Server listening on TCP port 5558</div> <div>TCP window size: 85.3 KByte (default)</div> <div>[ 4] local 192.168.103.103 port 5558 connected with 192.168.102.102 port 37186</div> <div>[ ID] Interval Transfer Bandwidth</div> <div>[ 4] 0.0-30.2 sec 36.0 MBytes 10.0 Mbits/sec</div>

[illegible]