Assignment 2

Tao Yuan & Wei XingHua

A00952007 & A00978597

COMP 8006 February 12,2020

Test Cases:

Rule #	Test Description	Tool Used	Expected Results	Pass/Fail
1	Allow user defined inbound TCP packets on allowed ports(22,80,443)	Test script using hping3	All results to defined ports will be ACCEPT. Otherwise will be drop	Pass. Detailed results are attached.
2	Allow user defined outbound TCP packets on allowed ports(22,80,443)	Test script using hping3	All results to defined ports will be ACCEPT. Otherwise will be drop	Pass. Detailed results are attached.
3	Allow user defined inbound UDP packets on allowed ports(53)	Test script using hping3	All results to defined ports will be ACCEPT. Otherwise will be drop	Pass. Detailed results are attached.
4	Allow user defined outbound UDP packets on allowed ports(53)	Test script using hping3	All results to defined ports will be ACCEPT. Otherwise will be drop	Pass. Detailed results are attached.
5	Allow user defined inbound ICMP packets on allowed type(0,8)	Test script using hping3	All results to defined ports will be ACCEPT. Otherwise will be drop	Pass. Detailed results are attached.
6	Allow user defined outbound ICMP packets on allowed type(0,8)	Test script using hping3	All results to defined ports will be ACCEPT. Otherwise will be drop	Pass. Detailed results are attached.
7	All packets fall through default rule will be DROPPED(port 50 not defined)	Test script using hping3	Packets will be DROPPED	Pass. Detailed results are attached.

8	Drop any packets with a source address from the outside matching my internal network	Test script using hping3	Packets will be DROPPED	Pass. Detailed results are attached.
9	SYN packets to high ports are blocked.	Test script using hping3	Packets will be DROPPED	Pass. Detailed results are attached.
10	Accept Fragmented packets	Test script using hping3	Fragment packets will be Accept	Pass. Detailed results are attached.
11	Accept all TCP packets that belong to an existing connection	Test script using ncat	Packets will be accepted	Pass. Detailed results are attached.
12	SYN, FIN packets are blocked.	Test script using hping3	all SYN FIN will be DROPPED	Pass. Detailed results are attached.
13	Telnet is always blocked.	Test script using hping3	All results to port 23 should be dropped.	Pass. Detailed results are attached.
14	Ports 32768-32775, 137-139, 111 & 515 blocked.	Test script using hping3	All results that target these ports should be DROPPED.	Pass. Detailed results are attached.
15	FTP & SSH ser-vices set for Min-imum Delay & Maximum Throughput	Open an SSH connection and inspect packets with tcpdump.	The TOS bit should be set on TCP packets for these con-nections.	Pass. Detailed results are attached.

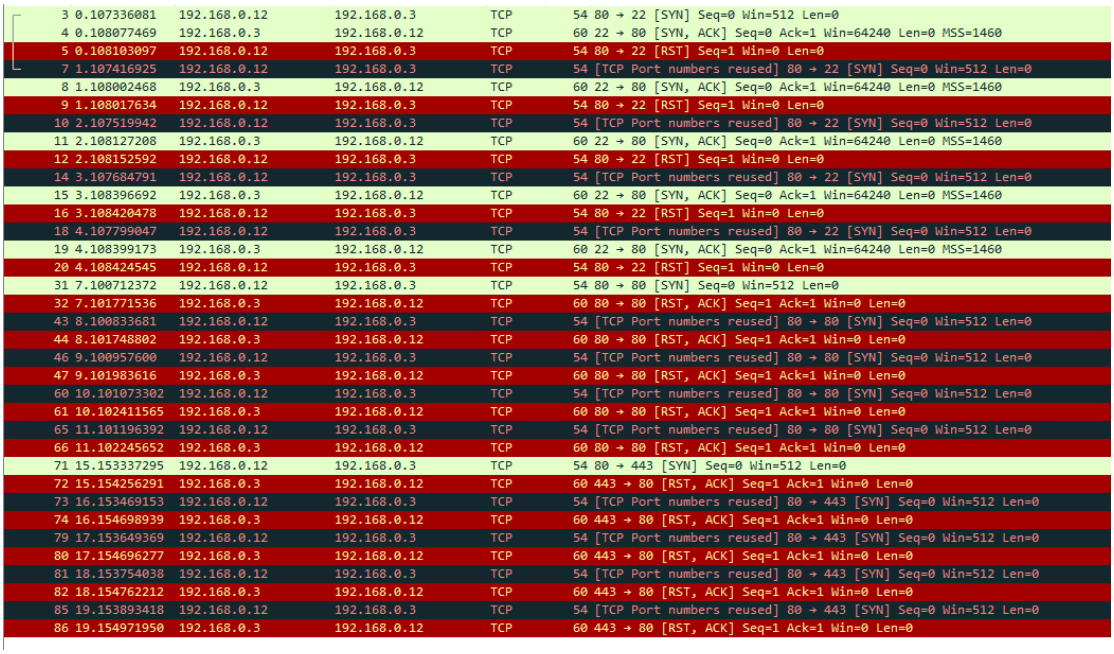
Test1 - Allow user defined inbound TCP packets on allowed ports(22,80,443)

Before we test TCP inbound, by using iptables -vL, it shows no packets.

```
18:58:08(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

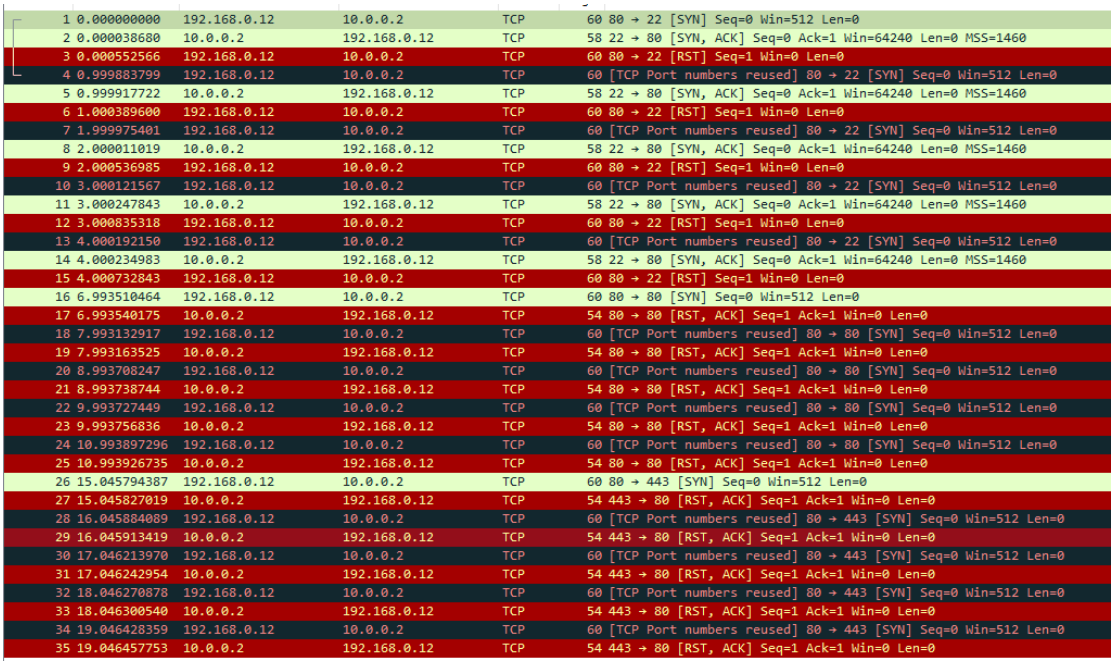
```
19:02:22(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 80 -p 22 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=1.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=1001.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=2001.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=3001.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=4001.7 ms

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.7/2001.7/4001.7 ms
19:03:39(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 80 -p 80 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=1.3 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=1001.3 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=2003.3 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=3003.3 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=4003.3 ms

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.3/2002.5/4003.3 ms
19:03:46(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 80 -p 443 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=2.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=1002.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=2002.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=3002.7 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=4002.7 ms

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.7/2002.7/4002.7 ms
19:03:54(-)root@datacomm-192-168-0-12:Downloads$
```

From 192.168.0.12 to 192.168.0.3 (showed in 192.168.0.12)



3	0.107336081	192.168.0.12	192.168.0.3	TCP	54 80 → 22 [SYN] Seq=0 Win=512 Len=0
4	0.108077469	192.168.0.3	192.168.0.12	TCP	60 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.108103097	192.168.0.12	192.168.0.3	TCP	54 80 → 22 [RST] Seq=1 Win=0 Len=0
7	1.107416925	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
8	1.108002468	192.168.0.3	192.168.0.12	TCP	60 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	1.108017634	192.168.0.12	192.168.0.3	TCP	54 80 → 22 [RST] Seq=1 Win=0 Len=0
10	2.107519942	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
11	2.108127208	192.168.0.3	192.168.0.12	TCP	60 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
12	2.108152592	192.168.0.12	192.168.0.3	TCP	54 80 → 22 [RST] Seq=1 Win=0 Len=0
14	3.107684791	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
15	3.108396692	192.168.0.3	192.168.0.12	TCP	60 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16	3.108420478	192.168.0.12	192.168.0.3	TCP	54 80 → 22 [RST] Seq=1 Win=0 Len=0
18	4.107799047	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
19	4.108399173	192.168.0.3	192.168.0.12	TCP	60 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
20	4.108424545	192.168.0.12	192.168.0.3	TCP	54 80 → 22 [RST] Seq=1 Win=0 Len=0
31	7.100712372	192.168.0.12	192.168.0.3	TCP	54 80 → 80 [SYN] Seq=0 Win=512 Len=0
32	7.101771536	192.168.0.3	192.168.0.12	TCP	60 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	8.100833681	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
44	8.101748802	192.168.0.3	192.168.0.12	TCP	60 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46	9.100957600	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
47	9.101983616	192.168.0.3	192.168.0.12	TCP	60 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	10.101073302	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
61	10.102411565	192.168.0.3	192.168.0.12	TCP	60 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	11.101196392	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
66	11.102245652	192.168.0.3	192.168.0.12	TCP	60 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
71	15.153337295	192.168.0.12	192.168.0.3	TCP	54 80 → 443 [SYN] Seq=0 Win=512 Len=0
72	15.154256291	192.168.0.3	192.168.0.12	TCP	60 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
73	16.153469153	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
74	16.154698939	192.168.0.3	192.168.0.12	TCP	60 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	17.153649369	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
80	17.154696277	192.168.0.3	192.168.0.12	TCP	60 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
81	18.153754038	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
82	18.154762212	192.168.0.3	192.168.0.12	TCP	60 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	19.153893418	192.168.0.12	192.168.0.3	TCP	54 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
86	19.154971950	192.168.0.3	192.168.0.12	TCP	60 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

From 192.168.0.12 to 192.168.0.3 (showed in 192.168.0.3)



1	0.000000000	192.168.0.12	10.0.0.2	TCP	60 80 → 22 [SYN] Seq=0 Win=512 Len=0
2	0.000038680	10.0.0.2	192.168.0.12	TCP	58 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000552566	192.168.0.12	10.0.0.2	TCP	60 80 → 22 [RST] Seq=1 Win=0 Len=0
4	0.999883799	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
5	0.999917722	10.0.0.2	192.168.0.12	TCP	58 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6	1.000389600	192.168.0.12	10.0.0.2	TCP	60 80 → 22 [RST] Seq=1 Win=0 Len=0
7	1.999975401	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
8	2.000011019	10.0.0.2	192.168.0.12	TCP	58 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	2.000536985	192.168.0.12	10.0.0.2	TCP	60 80 → 22 [RST] Seq=1 Win=0 Len=0
10	3.000121567	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
11	3.000247843	10.0.0.2	192.168.0.12	TCP	58 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
12	3.000835318	192.168.0.12	10.0.0.2	TCP	60 80 → 22 [RST] Seq=1 Win=0 Len=0
13	4.000192150	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=512 Len=0
14	4.000234983	10.0.0.2	192.168.0.12	TCP	58 22 → 80 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	4.000732843	192.168.0.12	10.0.0.2	TCP	60 80 → 22 [RST] Seq=1 Win=0 Len=0
16	6.993510464	192.168.0.12	10.0.0.2	TCP	60 80 → 80 [SYN] Seq=0 Win=512 Len=0
17	6.993540175	10.0.0.2	192.168.0.12	TCP	54 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	7.993132917	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
19	7.993163525	10.0.0.2	192.168.0.12	TCP	54 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	8.993708247	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
21	8.993738744	10.0.0.2	192.168.0.12	TCP	54 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	9.993727449	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
23	9.993756836	10.0.0.2	192.168.0.12	TCP	54 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	10.993897296	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0
25	10.993926735	10.0.0.2	192.168.0.12	TCP	54 80 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	15.045794387	192.168.0.12	10.0.0.2	TCP	60 80 → 443 [SYN] Seq=0 Win=512 Len=0
27	15.045827019	10.0.0.2	192.168.0.12	TCP	54 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	16.045884089	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
29	16.045913419	10.0.0.2	192.168.0.12	TCP	54 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	17.046213970	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
31	17.046242954	10.0.0.2	192.168.0.12	TCP	54 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	18.046270878	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
33	18.046300540	10.0.0.2	192.168.0.12	TCP	54 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	19.046428359	192.168.0.12	10.0.0.2	TCP	60 [TCP Port numbers reused] 80 → 443 [SYN] Seq=0 Win=512 Len=0
35	19.046457753	10.0.0.2	192.168.0.12	TCP	54 443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Firewall after

After testing, as we notice that all the packets through the traffic have been showed below.

```
19:12:03(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 15 packets, 1028 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   17   680 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
   12  1060 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   32  2136 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
   29  2941 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    5   200 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    5   600 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
 1752  182K ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
 1004 3759K ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    5   200 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    5   600 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
   72  4732 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
   72 10700 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 56 packets, 12172 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Test 2 - Allow user defined outbound TCP packets on allowed ports(22,80,443)

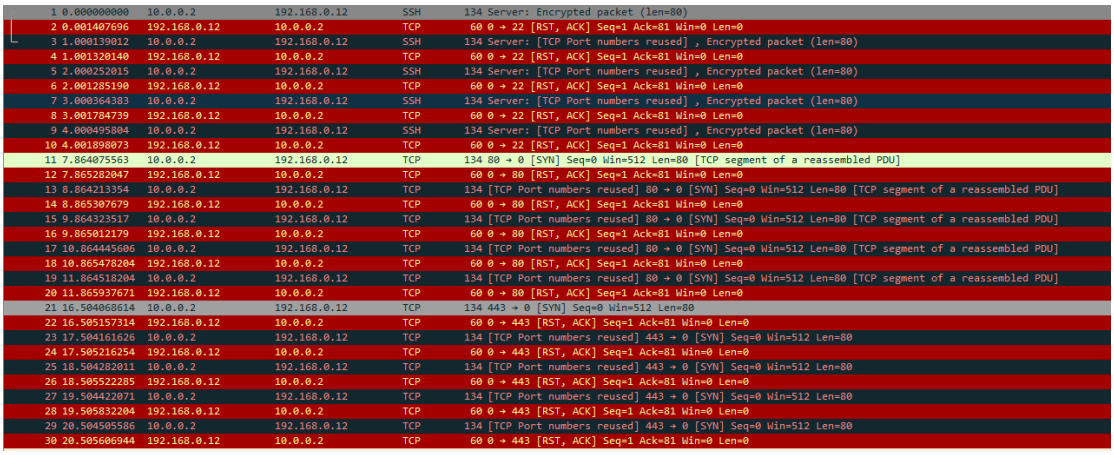
Before we test TCP inbound and outbound, by using iptables -vL, it shows no packets.

```
18:58:08(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

The first is to test tcp ports from the external, the graph will show what is the command.

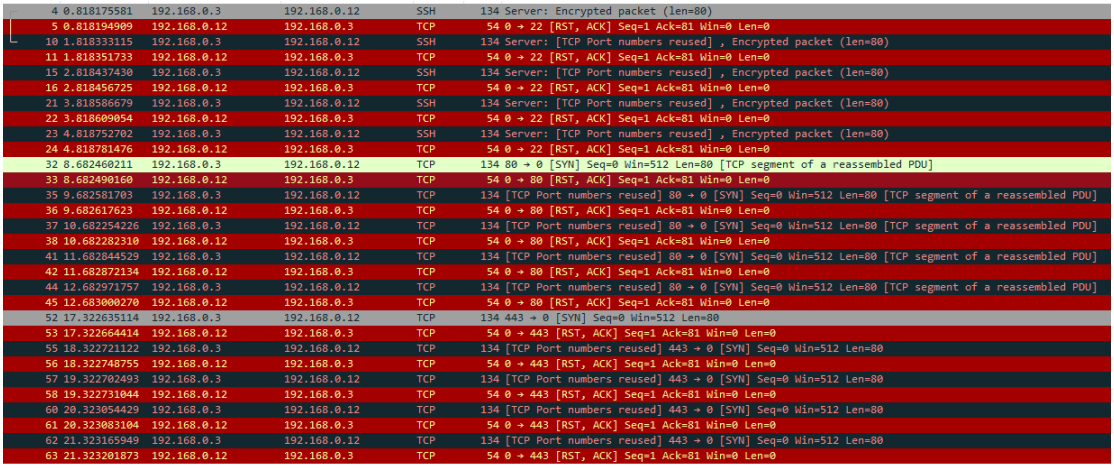
```
19:09:11(-)root@localhost:Desktop$ hping3 192.168.0.12 -S -s 22 -d 80 -c 5 --keep
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 80 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=1.6 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=1001.6 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=2001.6 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=3003.6 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=4003.6 ms

--- 192.168.0.12 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.6/2002.4/4003.6 ms
19:09:30(-)root@localhost:Desktop$ hping3 192.168.0.12 -S -s 80 -d 80 -c 5 --keep
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 80 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=1.5 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=1001.4 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=2001.5 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=3003.5 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=4003.5 ms

--- 192.168.0.12 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.5/2002.3/4003.5 ms
19:09:38(-)root@localhost:Desktop$ hping3 192.168.0.12 -S -s 443 -d 80 -c 5 --keep
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 80 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=2.5 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=1002.4 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=2002.5 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=3002.5 ms
DUP! len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=4002.5 ms

--- 192.168.0.12 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.5/2002.5/4002.5 ms
```

From 192.168.0.3 to 192.168.0.12 (showed in 192.168.0.3)



1	0.000000000	10.0.0.2	192.168.0.12	SSH	134 Server: Encrypted packet (len=80)
2	0.001407696	192.168.0.12	10.0.0.2	TCP	60 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
3	1.000139012	10.0.0.2	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
4	1.001320140	192.168.0.12	10.0.0.2	TCP	60 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
5	2.000252015	10.0.0.2	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
6	2.001285190	192.168.0.12	10.0.0.2	TCP	60 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
7	3.000364383	10.0.0.2	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
8	3.001784739	192.168.0.12	10.0.0.2	TCP	60 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
9	4.000495804	10.0.0.2	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
10	4.001898073	192.168.0.12	10.0.0.2	TCP	60 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
11	7.864075563	10.0.0.2	192.168.0.12	TCP	134 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
12	7.865282047	192.168.0.12	10.0.0.2	TCP	60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
13	8.864213354	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
14	8.865307679	192.168.0.12	10.0.0.2	TCP	60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
15	9.864323517	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
16	9.865012179	192.168.0.12	10.0.0.2	TCP	60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
17	10.864445606	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
18	10.865478204	192.168.0.12	10.0.0.2	TCP	60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
19	11.864518204	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
20	11.865937671	192.168.0.12	10.0.0.2	TCP	60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
21	16.504068614	10.0.0.2	192.168.0.12	TCP	134 443 → 0 [SYN] Seq=0 Win=512 Len=80
22	16.505157314	192.168.0.12	10.0.0.2	TCP	60 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
23	17.504161626	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
24	17.505216254	192.168.0.12	10.0.0.2	TCP	60 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
25	18.504282011	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
26	18.505522285	192.168.0.12	10.0.0.2	TCP	60 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
27	19.504422071	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
28	19.505832204	192.168.0.12	10.0.0.2	TCP	60 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
29	20.504505586	10.0.0.2	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
30	20.505606944	192.168.0.12	10.0.0.2	TCP	60 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0

From 192.168.0.3 to 192.168.0.12 (showed in 192.168.0.12)



4	0.818175581	192.168.0.3	192.168.0.12	SSH	134 Server: Encrypted packet (len=80)
5	0.818194909	192.168.0.12	192.168.0.3	TCP	54 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
10	1.818333115	192.168.0.3	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
11	1.818351733	192.168.0.12	192.168.0.3	TCP	54 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
15	2.818437430	192.168.0.3	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
16	2.818456725	192.168.0.12	192.168.0.3	TCP	54 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
21	3.818586679	192.168.0.3	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
22	3.818609054	192.168.0.12	192.168.0.3	TCP	54 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
23	4.818752702	192.168.0.3	192.168.0.12	SSH	134 Server: [TCP Port numbers reused] , Encrypted packet (len=80)
24	4.818781476	192.168.0.12	192.168.0.3	TCP	54 0 → 22 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
32	8.682460211	192.168.0.3	192.168.0.12	TCP	134 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
33	8.682490160	192.168.0.12	192.168.0.3	TCP	54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
35	9.682581703	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
36	9.682617623	192.168.0.12	192.168.0.3	TCP	54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
37	10.682254226	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
38	10.682282310	192.168.0.12	192.168.0.3	TCP	54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
41	11.682844529	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
42	11.682872134	192.168.0.12	192.168.0.3	TCP	54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
44	12.682971757	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
45	12.683000270	192.168.0.12	192.168.0.3	TCP	54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
52	17.322635114	192.168.0.3	192.168.0.12	TCP	134 443 → 0 [SYN] Seq=0 Win=512 Len=80
53	17.322664414	192.168.0.12	192.168.0.3	TCP	54 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
55	18.322721122	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
56	18.322748755	192.168.0.12	192.168.0.3	TCP	54 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
57	19.322702493	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
58	19.322731044	192.168.0.12	192.168.0.3	TCP	54 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
60	20.323054429	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
61	20.323083104	192.168.0.12	192.168.0.3	TCP	54 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
62	21.323165949	192.168.0.3	192.168.0.12	TCP	134 [TCP Port numbers reused] 443 → 0 [SYN] Seq=0 Win=512 Len=80
63	21.323201873	192.168.0.12	192.168.0.3	TCP	54 0 → 443 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0

After

```
19:12:03(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 15 packets, 1028 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   17   680 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
   12  1060 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   32  2136 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
   29  2941 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    5   200 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    5   600 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
 1752  182K ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
 1004 3759K ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    5   200 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    5   600 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
   72  4732 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
   72 10700 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spts:bootps:bootpc state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 56 packets, 12172 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Test 3 - Allow user defined inbound UDP packets on allowed ports(53)

Before

```
19:14:12(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 3 packets, 454 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

The step is to test udp ports from the 192.168.0.12, the graph will show what is the command.

```
19:16:06(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 --udp -s 80 -p 53 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

From 192.168.0.12 to 192.168.0.03 (showed in 192.168.0.12)

4	2.224666604	192.168.0.12	192.168.0.3	UDP	42 80 → 53 Len=0
5	3.224804950	192.168.0.12	192.168.0.3	UDP	42 80 → 53 Len=0
7	4.224907902	192.168.0.12	192.168.0.3	UDP	42 80 → 53 Len=0
8	5.225047829	192.168.0.12	192.168.0.3	UDP	42 80 → 53 Len=0
11	6.225126018	192.168.0.12	192.168.0.3	UDP	42 80 → 53 Len=0

From 192.168.0.3 to 192.168.0.12 (showed in 192.168.0.3)

1	0.000000000	192.168.0.12	10.0.0.2	UDP	60 80 → 53 Len=0
2	0.000045367	10.0.0.2	192.168.0.12	ICMP	70 Destination unreachable (Port unreachable)
3	1.000132722	192.168.0.12	10.0.0.2	UDP	60 80 → 53 Len=0
4	1.000179307	10.0.0.2	192.168.0.12	ICMP	70 Destination unreachable (Port unreachable)
5	2.000164490	192.168.0.12	10.0.0.2	UDP	60 80 → 53 Len=0
6	2.000202575	10.0.0.2	192.168.0.12	ICMP	70 Destination unreachable (Port unreachable)
7	3.000301815	192.168.0.12	10.0.0.2	UDP	60 80 → 53 Len=0
8	3.000347831	10.0.0.2	192.168.0.12	ICMP	70 Destination unreachable (Port unreachable)
9	4.000348931	192.168.0.12	10.0.0.2	UDP	60 80 → 53 Len=0
10	4.000387526	10.0.0.2	192.168.0.12	ICMP	70 Destination unreachable (Port unreachable)

After the test:

```
19:14:17(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 20 packets, 1920 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   10   561 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
   10   882 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    1    63 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    1   239 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
   10   280 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
   10  1080 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 42 packets, 9370 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Test 4 - Allow user defined outbound UDP packets on allowed ports(53)

Before the test:

```
19:14:12(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 3 packets, 454 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

The step is to test udp ports from the 192.168.0.3, the graph will show what is the command.

```
19:18:22(-)root@localhost:Desktop$ hping3 192.168.0.12 --udp -s 53 -d 80 -c 5 --keep
HPING 192.168.0.12 (enp2s0 192.168.0.12): udp mode set, 28 headers + 80 data bytes

--- 192.168.0.12 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

From 192.168.0.3 to 192.168.0.12 (showed in 192.168.0.3)

1	0.000000000	10.0.0.2	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
2	1.000131573	10.0.0.2	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
3	2.000239522	10.0.0.2	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
4	3.000350843	10.0.0.2	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
5	4.000483372	10.0.0.2	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]

From 192.168.0.3 to 192.168.0.12 (showed in 192.168.0.12)

3	1.654475320	192.168.0.3	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
4	1.654509565	192.168.0.12	192.168.0.3	ICMP	150	Destination unreachable (Port unreachable)
5	2.654630660	192.168.0.3	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
6	2.654673678	192.168.0.12	192.168.0.3	ICMP	150	Destination unreachable (Port unreachable)
8	3.654644299	192.168.0.3	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
9	3.654686396	192.168.0.12	192.168.0.3	ICMP	150	Destination unreachable (Port unreachable)
15	4.654885563	192.168.0.3	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
16	4.654919640	192.168.0.12	192.168.0.3	ICMP	150	Destination unreachable (Port unreachable)
21	5.655061523	192.168.0.3	192.168.0.12	DNS	122	Unknown operation (11) 0x5858[Malformed Packet]
22	5.655097203	192.168.0.12	192.168.0.3	ICMP	150	Destination unreachable (Port unreachable)

After the test:

```
19:14:17(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 20 packets, 1920 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   10   561 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
   10   882 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    1    63 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    1   239 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
   10   280 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
   10  1080 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 42 packets, 9370 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Test 5 - Allow user defined inbound ICMP packets on allowed type(0,8)

Before the test:

```
19:23:35(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

The step is to test ICMP from the 192.168.0.12, the graph will show what is the command.

```
19:22:59(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -C 8 -c 5
HPING 192.168.0.3 (eno1 192.168.0.3): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 id=60238 icmp_seq=0 rtt=0.8 ms
len=46 ip=192.168.0.3 ttl=63 id=60775 icmp_seq=1 rtt=2.6 ms
len=46 ip=192.168.0.3 ttl=63 id=61145 icmp_seq=2 rtt=2.5 ms
len=46 ip=192.168.0.3 ttl=63 id=61238 icmp_seq=3 rtt=2.3 ms
len=46 ip=192.168.0.3 ttl=63 id=61726 icmp_seq=4 rtt=2.2 ms

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/2.1/2.6 ms
```

From 192.168.0.12 to 192.168.0.03 (showed in 192.168.0.12)

From 192.168.0.12 to 192.168.0.03 (showed in 192.168.0.3)

After the test:

```
19:23:37(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 11 packets, 2052 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Test 6 - Allow users defined outbound ICMP packets on allowed type(0,8)

Before the test:

```
19:23:35(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

The step is to test ICMP from the 192.168.0.3, the graph will show what is the command.

```
19:18:35(-)root@localhost:Desktop$ hping3 192.168.0.12 -C 8 -c 5
HPING 192.168.0.12 (enp2s0 192.168.0.12): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.12 ttl=63 id=47351 icmp_seq=0 rtt=2.7 ms
len=46 ip=192.168.0.12 ttl=63 id=47537 icmp_seq=1 rtt=1.4 ms
len=46 ip=192.168.0.12 ttl=63 id=48470 icmp_seq=2 rtt=1.3 ms
len=46 ip=192.168.0.12 ttl=63 id=48904 icmp_seq=3 rtt=3.2 ms
len=46 ip=192.168.0.12 ttl=63 id=48927 icmp_seq=4 rtt=1.1 ms

--- 192.168.0.12 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.9/3.2 ms
```

From 192.168.0.3 to 192.168.0.12 (showed in 192.168.0.3)

1	0.000000000	10.0.0.2	192.168.0.12	ICMP	42	Echo (ping) request id=0x941b, seq=0/0, ttl=64 (reply in 2)
2	0.001206100	192.168.0.12	10.0.0.2	ICMP	60	Echo (ping) reply id=0x941b, seq=0/0, ttl=63 (request in 1)
3	1.000136975	10.0.0.2	192.168.0.12	ICMP	42	Echo (ping) request id=0x941b, seq=256/1, ttl=64 (reply in 4)
4	1.001295608	192.168.0.12	10.0.0.2	ICMP	60	Echo (ping) reply id=0x941b, seq=256/1, ttl=63 (request in 3)
5	2.000252650	10.0.0.2	192.168.0.12	ICMP	42	Echo (ping) request id=0x941b, seq=512/2, ttl=64 (reply in 6)
6	2.001479253	192.168.0.12	10.0.0.2	ICMP	60	Echo (ping) reply id=0x941b, seq=512/2, ttl=63 (request in 5)
7	3.000358078	10.0.0.2	192.168.0.12	ICMP	42	Echo (ping) request id=0x941b, seq=768/3, ttl=64 (reply in 8)
8	3.001572536	192.168.0.12	10.0.0.2	ICMP	60	Echo (ping) reply id=0x941b, seq=768/3, ttl=63 (request in 7)
9	4.000440351	10.0.0.2	192.168.0.12	ICMP	42	Echo (ping) request id=0x941b, seq=1024/4, ttl=64 (reply in 10)
10	4.001345090	192.168.0.12	10.0.0.2	ICMP	60	Echo (ping) reply id=0x941b, seq=1024/4, ttl=63 (request in 9)

From 192.168.0.3 to 192.168.0.12 (showed in 192.168.12)

1	0.000000000	192.168.0.3	192.168.0.12	ICMP	60	Echo (ping) request id=0x941b, seq=256/1, ttl=63 (reply in 2)
2	0.000066866	192.168.0.12	192.168.0.3	ICMP	42	Echo (ping) reply id=0x941b, seq=256/1, ttl=64 (request in 1)
3	1.000174762	192.168.0.3	192.168.0.12	ICMP	60	Echo (ping) request id=0x941b, seq=512/2, ttl=63 (reply in 4)
4	1.000205211	192.168.0.12	192.168.0.3	ICMP	42	Echo (ping) reply id=0x941b, seq=512/2, ttl=64 (request in 3)
6	2.000305301	192.168.0.3	192.168.0.12	ICMP	60	Echo (ping) request id=0x941b, seq=768/3, ttl=63 (reply in 7)
7	2.000335308	192.168.0.12	192.168.0.3	ICMP	42	Echo (ping) reply id=0x941b, seq=768/3, ttl=64 (request in 6)
8	3.000113161	192.168.0.3	192.168.0.12	ICMP	60	Echo (ping) request id=0x941b, seq=1024/4, ttl=63 (reply in 9)
9	3.000144586	192.168.0.12	192.168.0.3	ICMP	42	Echo (ping) reply id=0x941b, seq=1024/4, ttl=64 (request in 8)

After the test:

```
19:24:51(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 1 packets, 76 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    5   361 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    5   681 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    1    63 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    1   239 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 30 packets, 6476 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Test 7 - All packets fall through default rule will be DROPPED(port 50 not defined)

If the port is not defined, it should not goes through the firewall. In this case, port 50 is not defined

Hping3 through port 50

```
19:44:36(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 50 -d 50 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 50 data bytes

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Before the test:

We can see there is no DROP packets

```
19:45:14(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

After the test:

```
19:45:33(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 5 packets, 450 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    5   361 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    5   681 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    1    63 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    1   239 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 16 packets, 1120 bytes)
```

We can see that in the Forward Chain above, there are 5 packets Dropped

```
      6 2.750075346   192.168.0.12          192.168.0.3           TCP       104 50 → 0 [SYN] Seq=0 Win=512 Len=50
└     9 3.750137775   192.168.0.12          192.168.0.3           TCP       104 [TCP Port numbers reused] 50 → 0 [SYN] Seq=0 Win=512 Len=50
     10 4.750255736   192.168.0.12          192.168.0.3           TCP       104 [TCP Port numbers reused] 50 → 0 [SYN] Seq=0 Win=512 Len=50
     16 5.750385885   192.168.0.12          192.168.0.3           TCP       104 [TCP Port numbers reused] 50 → 0 [SYN] Seq=0 Win=512 Len=50
     17 6.750495372   192.168.0.12          192.168.0.3           TCP       104 [TCP Port numbers reused] 50 → 0 [SYN] Seq=0 Win=512 Len=50
```

Therefore, firewall successfully filter the traffic.

Test 8 - Drop any packets with a source address from the outside matching my internal network

If the outside network is the same as internal network, e.g, 10.0.0.2, it should be dropped

```
19:55:29(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -a 10.0.0.2 -S -s 80 -d 80 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Before the test:

We can see there is no packet dropped

```
19:23:35(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

After the test:

```
19:53:56(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 5 packets, 450 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    5   600 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   11   774 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
   10  1362 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    2   126 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    2   478 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 32 packets, 2222 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

We can see there are 5 packets dropped

```
     2 0.561406331   10.0.0.2          192.168.0.3       TCP      134 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
     3 1.561537498   10.0.0.2          192.168.0.3       TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
     8 2.561664018   10.0.0.2          192.168.0.3       TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
     9 3.561799000   10.0.0.2          192.168.0.3       TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    12 4.561923524   10.0.0.2          192.168.0.3       TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
```

Therefore, firewall successfully filter the traffic.

Test 9 - SYN packets to high ports are blocked.

Packets with SYN flag and port larger than 1023 should be dropped

```
20:10:01(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 10080 -d 80 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
20:11:01(-)root@datacomm-192-168-0-12:Downloads$
```

Before the test:

```
19:23:35(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

We can see there are traffic

After the test:

```
20:10:27(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    5   600 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 76 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
      5 1.546605650   192.168.0.12    192.168.0.3     TCP      134 10080 → 0 [SYN] Seq=0 Win=512 Len=80
└    10 2.546690024   192.168.0.12    192.168.0.3     TCP      134 [TCP Port numbers reused] 10080 → 0 [SYN] Seq=0 Win=512 Len=80
     13 3.546798496   192.168.0.12    192.168.0.3     TCP      134 [TCP Port numbers reused] 10080 → 0 [SYN] Seq=0 Win=512 Len=80
     15 4.546930640   192.168.0.12    192.168.0.3     TCP      134 [TCP Port numbers reused] 10080 → 0 [SYN] Seq=0 Win=512 Len=80
     17 5.547039393   192.168.0.12    192.168.0.3     TCP      134 [TCP Port numbers reused] 10080 → 0 [SYN] Seq=0 Win=512 Len=80
```

We can see that there are 5 packets dropped

Therefore, firewall successfully filter the packets.

Test 10 - Accept Fragmented packets

By default, Hping3 allow fragments, in this case, we also define –f when using Hping3

In this case, we are sending from port 80 to port 80, which should be accepted

```
20:15:23(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 80 -d 80 -f -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=3.4 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=1003.3 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=2003.4 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=3003.3 ms
DUP! len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=4003.3 ms

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.4/2003.4/4003.3 ms
```

Before the test:

```
19:23:35(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

We can see there is no packets accepted

After the test:

```
    1 0.000000000   192.168.0.12        10.0.0.2            TCP      134 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
    2 0.000039255   10.0.0.2            192.168.0.12        TCP       54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    3 1.000213926   192.168.0.12        10.0.0.2            TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    4 1.000251148   10.0.0.2            192.168.0.12        TCP       54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    5 2.000291492   192.168.0.12        10.0.0.2            TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    6 2.000328841   10.0.0.2            192.168.0.12        TCP       54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    7 3.000383217   192.168.0.12        10.0.0.2            TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    8 3.000420836   10.0.0.2            192.168.0.12        TCP       54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    9 4.000552785   192.168.0.12        10.0.0.2            TCP      134 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
   10 4.000592531   10.0.0.2            192.168.0.12        TCP       54 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
```

```
20:15:57(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    5   200 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    5   600 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 2 packets, 152 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

We can see that there are 10 packets accepted, each direction 5 packets.

```
    10 2.020473315   192.168.0.12    192.168.0.3     TCP      38 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassembled PDU]
    11 2.021886489   192.168.0.3     192.168.0.12    TCP      60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    18 3.020654398   192.168.0.12    192.168.0.3     TCP      38 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    19 3.021795268   192.168.0.3     192.168.0.12    TCP      60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    30 4.020782002   192.168.0.12    192.168.0.3     TCP      38 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    31 4.022246592   192.168.0.3     192.168.0.12    TCP      60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    38 5.020905787   192.168.0.12    192.168.0.3     TCP      38 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    39 5.021987537   192.168.0.3     192.168.0.12    TCP      60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
    48 6.021088185   192.168.0.12    192.168.0.3     TCP      38 [TCP Port numbers reused] 80 → 0 [SYN] Seq=0 Win=512 Len=80 [TCP segment of a reassemble…
    49 6.022296650   192.168.0.3     192.168.0.12    TCP      60 0 → 80 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
```

Therefore, firewall successfully filtered the packets.

Test 11 - Accept all TCP packets that belong to an existing connection

In this case, we use ncat to transfer a file between two machines where it will need to keep connected to transfer

```
20:20:54(-)root@datacomm-192-168-0-12:Downloads$ nc -l -p 80 > hello.txt
20:22:25(-)root@datacomm-192-168-0-12:Downloads$ nc -l -p 80 > hello.txt
```

```
20:22:25(-)root@localhost:Desktop$ nc 192.168.0.12 80 < hello.txt
```

Wireshark capture

```
     9 4.959029991   192.168.0.3     192.168.0.12    TCP      74 33030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3478486109 TSecr=0 WS=…
    10 4.959066548   192.168.0.12    192.168.0.3     TCP      74 80 → 33030 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4236036523 …
    11 4.960004087   192.168.0.3     192.168.0.12    TCP      66 33030 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3478486110 TSecr=4236036523
    12 4.960040596   192.168.0.3     192.168.0.12    TCP      75 33030 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=9 TSval=3478486110 TSecr=4236036523
    13 4.960051837   192.168.0.12    192.168.0.3     TCP      66 80 → 33030 [ACK] Seq=1 Ack=10 Win=65152 Len=0 TSval=4236036524 TSecr=3478486110
    14 4.960055881   192.168.0.3     192.168.0.12    TCP      66 33030 → 80 [FIN, ACK] Seq=10 Ack=1 Win=64256 Len=0 TSval=3478486110 TSecr=4236036523
    15 4.960259370   192.168.0.12    192.168.0.3     TCP      66 80 → 33030 [FIN, ACK] Seq=1 Ack=11 Win=65152 Len=0 TSval=4236036524 TSecr=3478486110
    16 4.961068322   192.168.0.3     192.168.0.12    TCP      66 33030 → 80 [ACK] Seq=11 Ack=2 Win=64256 Len=0 TSval=3478486112 TSecr=4236036524
```

We can see that files are successfully transferred, therefore, firewalls succesfully fitered the packets.

Test 12 - SYN, FIN packets are blocked.

In this case, we use the following command to test TCP packets with SYN and FIN bit set will be dropped , its obvious that 5 packets transmitted, but 0 packets received.

```
20:30:58(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -SF -s 80 -d 80 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): SF set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

In addition, we can also use wireshark to see the result.

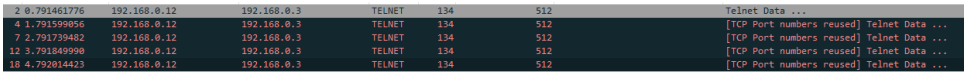
Therefore, SYN, FIN packets are blocked.

Test 13 - Telnet is always blocked

By inputing the following command, we can see that telnet(port 23) is blocked,

```
20:34:12(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -H tcp -S -s 23 -d 80 -c 5 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

As we can see , it is obvious that telnet is blocked



By inputing iptables –vL, the telnet packets have been dropped

```
20:34:17(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 7 packets, 726 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
   13  1446 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
   21  1174 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
   20  1992 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    2   126 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    2   478 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
```

Test 14 - Ports 32768-32775, 137-139, 111 & 515 blocked.

Port 111, 515, 137-139, 32768-32775 should be dropped

Port 111

```
20:45:12(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 111 -d 80 -c 3 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Port 515

```
20:47:10(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 515 -d 80 -c 3 --keep
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Port 137-139

```
20:50:48(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 137 -d 80 -c 3
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
20:51:02(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 137 -d 80 -c 3
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
20:51:16(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 137 -d 80 -c 3
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Port 32768-32775:

```
20:51:22(-)root@datacomm-192-168-0-12:Downloads$ hping3 192.168.0.3 -S -s 32768 -d 80 -c 8
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 80 data bytes

--- 192.168.0.3 hping statistic ---
8 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Before the test:

There are no packets

```
19:23:35(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

After the test:

```
20:45:22(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    3   360 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
    11 6.146585305   54.149.52.86     192.168.0.12     TLSv1.2    97 Application Data
    12 6.146792362   192.168.0.12     54.149.52.86     TLSv1.2   101 Application Data
    13 6.159767189   54.149.52.86     192.168.0.12     TCP        66 443 → 45206 [ACK] Seq=32 Ack=36 Win=118 Len=0 TSval=3780077086 TSecr=2858526225
    17 10.434200140  192.168.0.12     192.168.0.3      RPC       134 Continuation
    23 11.434318652  192.168.0.12     192.168.0.3      RPC       134 [TCP Port numbers reused] Continuation
    25 12.434451485  192.168.0.12     192.168.0.3      RPC       134 [TCP Port numbers reused] Continuation
```

Port 111 have dropped 3 packets

```
20:47:55(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 2 packets, 152 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    3   360 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    3   360 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 63 packets, 4240 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
     5 1.176108784   192.168.0.12          192.168.0.3           LPD      134 LPD continuation
    11 2.176187069   192.168.0.12          192.168.0.3           LPD      134 [TCP Port numbers reused] LPD continuation
    14 3.176311777   192.168.0.12          192.168.0.3           LPD      134 [TCP Port numbers reused] LPD continuation
```

Port 515 have dropped 3 packets

```
20:50:55(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    9  1080 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    6   413 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    5   681 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    1    63 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    1   239 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 3 packets, 202 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
     2 0.241283763   192.168.0.12          192.168.0.3           TCP      134 137 → 0 [SYN] Seq=0 Win=512 Len=80
     6 1.241355052   192.168.0.12          192.168.0.3           TCP      134 138 → 0 [SYN] Seq=0 Win=512 Len=80
     8 2.241486209   192.168.0.12          192.168.0.3           NBSS     134 NBSS Continuation Message
    25 13.605134308  192.168.0.12          192.168.0.3           TCP      134 [TCP Port numbers reused] 137 → 0 [SYN] Seq=0 Win=512 Len=80
    28 14.605265731  192.168.0.12          192.168.0.3           TCP      134 [TCP Port numbers reused] 138 → 0 [SYN] Seq=0 Win=512 Len=80
    30 15.605393930  192.168.0.12          192.168.0.3           NBSS     134 [TCP Port numbers reused] NBSS Continuation Message
    37 19.555170985  192.168.0.12          192.168.0.3           TCP      134 [TCP Port numbers reused] 137 → 0 [SYN] Seq=0 Win=512 Len=80
    41 20.555290911  192.168.0.12          192.168.0.3           TCP      134 [TCP Port numbers reused] 138 → 0 [SYN] Seq=0 Win=512 Len=80
    43 21.555399849  192.168.0.12          192.168.0.3           NBSS     134 [TCP Port numbers reused] NBSS Continuation Message
```

Port 137-139 have dropped 9 packets

```
20:51:58(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    8   960 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    9  1080 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    6   413 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    5   681 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    1    63 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    1   239 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 9 packets, 614 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
        3 0.717972499   192.168.0.12          192.168.0.3           TCP       134 32768 → 0 [SYN] Seq=0 Win=512 Len=80
        4 1.718128447   192.168.0.12          192.168.0.3           TCP       134 32769 → 0 [SYN] Seq=0 Win=512 Len=80
        8 2.718221880   192.168.0.12          192.168.0.3           TCP       134 32770 → 0 [SYN] Seq=0 Win=512 Len=80
       10 3.718294596   192.168.0.12          192.168.0.3           TCP       134 32771 → 0 [SYN] Seq=0 Win=512 Len=80
       12 4.718377413   192.168.0.12          192.168.0.3           TCP       134 32772 → 0 [SYN] Seq=0 Win=512 Len=80
       13 5.718515039   192.168.0.12          192.168.0.3           TCP       134 32773 → 0 [SYN] Seq=0 Win=512 Len=80
       17 6.718646508   192.168.0.12          192.168.0.3           TCP       134 32774 → 0 [SYN] Seq=0 Win=512 Len=80
       18 7.718784363   192.168.0.12          192.168.0.3           TCP       134 32775 → 0 [SYN] Seq=0 Win=512 Len=80
```

Port 32768-32775 has dropped 8 packets

Therefore, firewall successfully filtered the traffic.

Test 15 - FTP & SSH ser-vices set for Min-imum Delay & Maximum Throughput

For SSH, just SSH into another machine

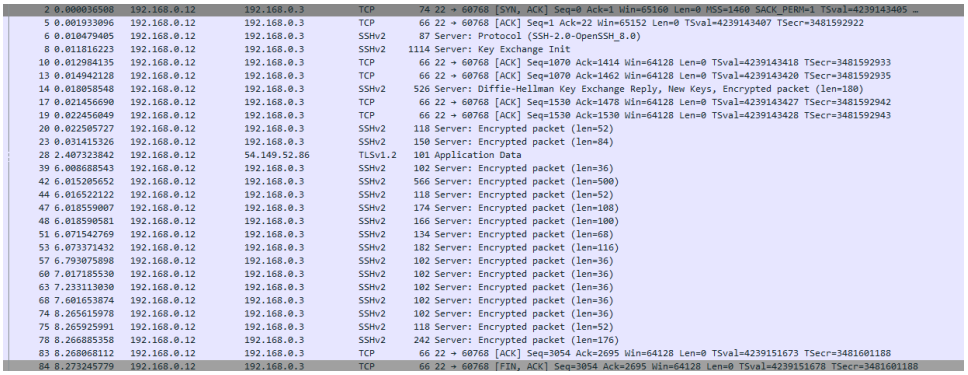
```
21:15:00(-)root@localhost:Desktop$ ssh 192.168.0.12
root@192.168.0.12's password:
Last login: Wed Feb 12 21:01:12 2020 from 192.168.0.3
21:15:23(-)root@datacomm-192-168-0-12:~$ exit
logout
```

Before the test:

```
19:23:35(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

After the test:

```
21:14:59(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 1 packets, 40 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/FIN,SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:1023:65535 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:filenet-tms:filenet-pch
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spts:netbios-ns:netbios-ssn
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:sunrpc
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp dpt:printer
    0     0 DROP       tcp  --  eno1   any     anywhere             anywhere             tcp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp dpt:printer
    0     0 DROP       udp  --  eno1   any     anywhere             anywhere             udp spt:printer
    0     0 DROP       all  --  eno1   any     10.0.0.0/24          anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere
   39  4729 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
   27  4465 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:ssh state ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:ssh state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:ssh state ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:http state ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:http state ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp spt:https state ESTABLISHED
    0     0 ACCEPT     tcp  --  eno1   enp2s0  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp2s0 eno1    anywhere             anywhere             tcp spt:https state ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp spt:domain state ESTABLISHED
    0     0 ACCEPT     udp  --  eno1   enp2s0  anywhere             anywhere             udp dpt:domain state NEW,ESTABLISHED
    0     0 ACCEPT     udp  --  enp2s0 eno1    anywhere             anywhere             udp spt:domain state ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  eno1   enp2s0  anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  enp2s0 eno1    anywhere             anywhere             icmp echo-request state NEW,ESTABLISHED

Chain OUTPUT (policy DROP 1 packets, 76 bytes)
 pkts bytes target     prot opt in     out     source               destination
```



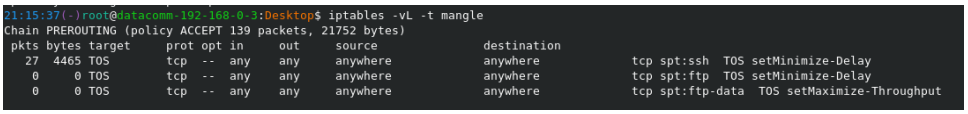
```
     2 0.000036508   192.168.0.12    192.168.0.3     TCP       74 22 → 60768 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4239143405 …
     5 0.001933096   192.168.0.12    192.168.0.3     TCP       66 22 → 60768 [ACK] Seq=1 Ack=22 Win=65152 Len=0 TSval=4239143407 TSecr=3481592922
     6 0.010479405   192.168.0.12    192.168.0.3     SSHv2     87 Server: Protocol (SSH-2.0-OpenSSH_8.0)
     8 0.011816223   192.168.0.12    192.168.0.3     SSHv2   1114 Server: Key Exchange Init
    10 0.012984135   192.168.0.12    192.168.0.3     TCP       66 22 → 60768 [ACK] Seq=1070 Ack=1414 Win=64128 Len=0 TSval=4239143418 TSecr=3481592933
    13 0.014942128   192.168.0.12    192.168.0.3     TCP       66 22 → 60768 [ACK] Seq=1070 Ack=1462 Win=64128 Len=0 TSval=4239143420 TSecr=3481592935
    14 0.018058548   192.168.0.12    192.168.0.3     SSHv2    526 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=180)
    17 0.021456690   192.168.0.12    192.168.0.3     TCP       66 22 → 60768 [ACK] Seq=1530 Ack=1478 Win=64128 Len=0 TSval=4239143427 TSecr=3481592942
    19 0.022456049   192.168.0.12    192.168.0.3     TCP       66 22 → 60768 [ACK] Seq=1530 Ack=1530 Win=64128 Len=0 TSval=4239143428 TSecr=3481592943
    20 0.022505727   192.168.0.12    192.168.0.3     SSHv2    118 Server: Encrypted packet (len=52)
    23 0.031415326   192.168.0.12    192.168.0.3     SSHv2    150 Server: Encrypted packet (len=84)
    28 2.407323842   192.168.0.12    54.149.52.86    TLSv1.2  101 Application Data
    39 6.008688543   192.168.0.12    192.168.0.3     SSHv2    102 Server: Encrypted packet (len=36)
    42 6.015205652   192.168.0.12    192.168.0.3     SSHv2    566 Server: Encrypted packet (len=500)
    44 6.016522122   192.168.0.12    192.168.0.3     SSHv2    118 Server: Encrypted packet (len=52)
    47 6.018559007   192.168.0.12    192.168.0.3     SSHv2    174 Server: Encrypted packet (len=108)
    48 6.018590581   192.168.0.12    192.168.0.3     SSHv2    166 Server: Encrypted packet (len=100)
    51 6.071542769   192.168.0.12    192.168.0.3     SSHv2    134 Server: Encrypted packet (len=68)
    53 6.073371432   192.168.0.12    192.168.0.3     SSHv2    182 Server: Encrypted packet (len=116)
    57 6.793075898   192.168.0.12    192.168.0.3     SSHv2    102 Server: Encrypted packet (len=36)
    60 7.017185530   192.168.0.12    192.168.0.3     SSHv2    102 Server: Encrypted packet (len=36)
    63 7.233113030   192.168.0.12    192.168.0.3     SSHv2    102 Server: Encrypted packet (len=36)
    68 7.601653874   192.168.0.12    192.168.0.3     SSHv2    102 Server: Encrypted packet (len=36)
    74 8.265615978   192.168.0.12    192.168.0.3     SSHv2    102 Server: Encrypted packet (len=36)
    75 8.265925991   192.168.0.12    192.168.0.3     SSHv2    118 Server: Encrypted packet (len=52)
    78 8.266885358   192.168.0.12    192.168.0.3     SSHv2    242 Server: Encrypted packet (len=176)
    83 8.268068112   192.168.0.12    192.168.0.3     TCP       66 22 → 60768 [ACK] Seq=3054 Ack=2695 Win=64128 Len=0 TSval=4239151673 TSecr=3481601188
    84 8.273245779   192.168.0.12    192.168.0.3     TCP       66 22 → 60768 [FIN, ACK] Seq=3054 Ack=2695 Win=64128 Len=0 TSval=4239151678 TSecr=3481601188
```

We can see there are SSH packets being accepted

Therefore, SSH firewall success.

We can see SSH success

For FTP, we just check mangle table



```
21:15:37(-)root@datacomm-192-168-0-3:Desktop$ iptables -vL -t mangle
Chain PREROUTING (policy ACCEPT 139 packets, 21752 bytes)
 pkts bytes target     prot opt in     out     source               destination
   27  4465 TOS        tcp  --  any    any     anywhere             anywhere             tcp spt:ssh  TOS setMinimize-Delay
    0     0 TOS        tcp  --  any    any     anywhere             anywhere             tcp spt:ftp  TOS setMinimize-Delay
    0     0 TOS        tcp  --  any    any     anywhere             anywhere             tcp spt:ftp-data  TOS setMaximize-Throughput
```

Testing Scripts:

Inbound test:

 # Testing allowed TCP ports 22 80 443 on 192.168.0.3

--- 192.168.0.3 hping statistic ---

1 packets transmitted, 1 packets received, 0% packet loss

round-trip min/avg/max = 1.7/1.7/1.7 ms

HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=1.7 ms

**** Port 22 is open and service is running on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---

1 packets transmitted, 1 packets received, 0% packet loss

round-trip min/avg/max = 1.5/1.5/1.5 ms

HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=1.5 ms

**** Port 80 is open, but no service is responding on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---

1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=0.8 ms

**** Port 443 is open, but no service is responding on 192.168.0.3.**

 # Testing blocked TCP ports 32768 32769 32770 32771 32772 32773 32774 32775 137 138 139 111 515 on 192.168.0.3

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32768 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32769 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32770 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32771 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32772 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32773 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32774 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 32775 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 137 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

**port 138 are DROPPED on 192.168.0.3.

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

**port 139 are DROPPED on 192.168.0.3.

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

**port 111 are DROPPED on 192.168.0.3.

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

**port 515 are DROPPED on 192.168.0.3.

 # Testing inbound SYN to port 1025 on 192.168.0.3

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

**port 1025 are DROPPED on 192.168.0.3.

 # Testing if fragments are received from 192.168.0.3

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss

round-trip min/avg/max = 1.8/1.8/1.8 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=1.8 ms

**** Port 22 is open and service is running on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.8/2.8/2.8 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=2.8 ms

**** Port 80 is open, but no service is responding on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=0.8 ms

**** Port 443 is open, but no service is responding on 192.168.0.3.**

 # Testing 192.168.0.3 responds to SYN,FIN packets

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): SF set, 40 headers + 0 data bytes

****port 22 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): SF set, 40 headers + 0 data bytes

****port 80 are DROPPED on 192.168.0.3.**

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): SF set, 40 headers + 0 data bytes

****port 443 are DROPPED on 192.168.0.3.**

 # Testing if 192.168.0.3 responds to TELNET packets

--- 192.168.0.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.3 (eno1 192.168.0.3): S set, 40 headers + 0 data bytes

****port 23 are DROPPED on 192.168.0.3.**

Outbound Testing:

 # Testing allowed TCP ports 22 80 443 on 192.168.0.12

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.8/2.8/2.8 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=2.8 ms

**** Port 22 is open and service is running on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.8/1.8/1.8 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=1.8 ms

**** Port 80 is open, but no service is responding on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---

1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.8/2.8/2.8 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=2.8 ms

**** Port 443 is open, but no service is responding on 192.168.0.12.**

 # Testing blocked TCP ports 32768 32769 32770 32771 32772 32773 32774 32775 137 138 139 111 515 on 192.168.0.12

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32768 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32769 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32770 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32771 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32772 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32773 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32774 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 32775 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 137 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

**port 138 are DROPPED on 192.168.0.12.

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

**port 139 are DROPPED on 192.168.0.12.

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

**port 111 are DROPPED on 192.168.0.12.

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

**port 515 are DROPPED on 192.168.0.12.

 # Testing inbound SYN to port 1025 on 192.168.0.12

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

**port 1025 are DROPPED on 192.168.0.12.

 # Testing if fragments are received from 192.168.0.12

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss

round-trip min/avg/max = 0.8/0.8/0.8 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.8 ms

**** Port 22 is open and service is running on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.8/1.8/1.8 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=1.8 ms

**** Port 80 is open, but no service is responding on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.8/1.8/1.8 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.12 ttl=63 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=1.8 ms

**** Port 443 is open, but no service is responding on 192.168.0.12.**

 # Testing 192.168.0.12 responds to SYN,FIN packets

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): SF set, 40 headers + 0 data bytes

****port 22 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): SF set, 40 headers + 0 data bytes

****port 80 are DROPPED on 192.168.0.12.**

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): SF set, 40 headers + 0 data bytes

****port 443 are DROPPED on 192.168.0.12.**

 # Testing if 192.168.0.12 responds to TELNET packets

--- 192.168.0.12 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.12 (enp2s0 192.168.0.12): S set, 40 headers + 0 data bytes

****port 23 are DROPPED on 192.168.0.12.**