# 8006 Assignment 2

Design & Documentation

Eric Wu, A00961904
Hong Kit, Wu A00968591

BTech 2020 Winter

## Table of contents

## Objectives

Design, implement and test a firewall for Linux that will implement the following rules:

- Set the initial default policies.
- Get user specified parameters and create a set of rules that will implement the firewall requirements. Specifically the firewall will control:
  - Inbound/Outbound TCP packets on allowed ports.
  - Inbound/Outbound UDP packets on allowed ports.
  - Inbound/Outbound ICMP packets based on type numbers.
  - All packets that fall through to the default rule will be dropped.
  - Drop all packets destined for the firewall host from the outside.
  - Drop any packets with a source address from the outside matching internal network.
  - Reject connections that are coming the “wrong” way (i.e., inbound SYN packets to high ports).
  - Accept fragments.
  - Accept all TCP packets that belong to an existing connection (on allowed ports).
  - Drop all TCP packets with the SYN and FIN bit set.
  - Drop all Telnet packets
  - Block all external traffic directed to ports 32768 – 32775, 137 – 139, TCP ports 111 and 515.
  - For FTP and SSH services, set control connections to "Minimum Delay" and FTP data to "Maximum Throughput".

## Approach

We will use **Netfilter** for the firewall implementation. The filter rules will be put together into a shell script files. The user specified parameters will be a set of defined macros in a config file. The script files will then configure firewall based on params specified in the config file.

As for the firewall testing, we will use **hping3** to probe the firewall host with both permitted and unpermitted packets, and log the response to text files. We will also be capturing traffic with **wireshark** during the probing. In the end, both wireshark captures and hping results will be compared against each other to see if the result matches with the requirement.

## Testing environment set up

The testing environment is set up with two machines. One machine operates as a firewall host, while the other one acts as an internal host. The firewall host will have one NIC configured to have public internet access (either through access point or ethernet cable), and another NIC configured as an internet gateway for the internal host. Below figure demonstrates the network architecture

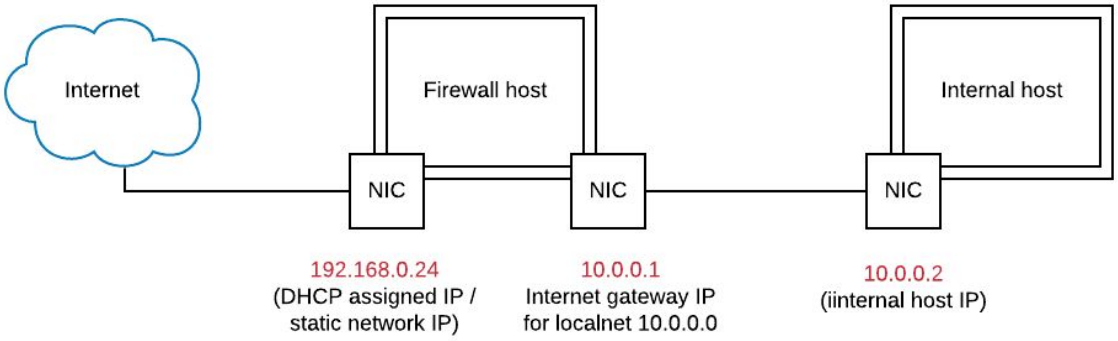
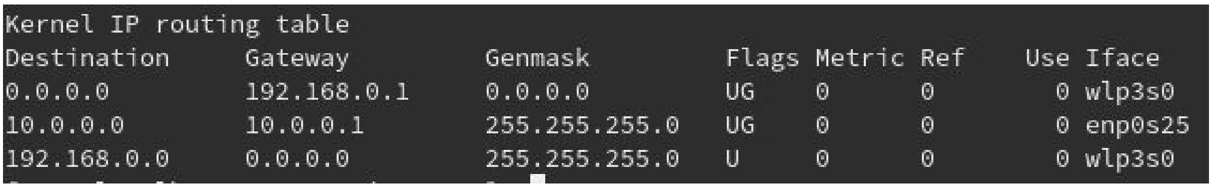


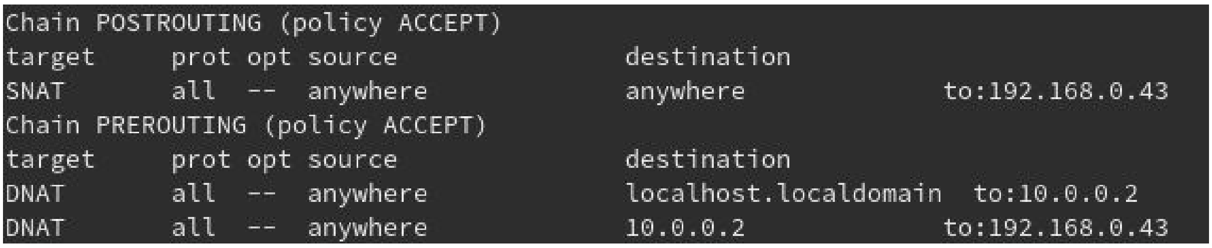
**Figure 1: Network architecture of the testing environment**

(Screen captures of routing rules on both machines)



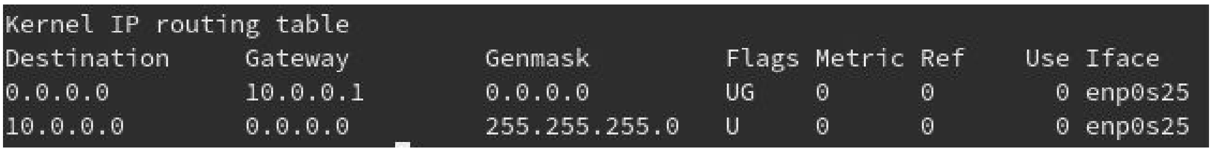
```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 wlp3s0
10.0.0.0        10.0.0.1        255.255.255.0   UG    0      0        0 enp0s25
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 wlp3s0
```

**Figure 2: Firewall host routing table**



```
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  anywhere             anywhere             to:192.168.0.43
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       all  --  anywhere             localhost.localdomain  to:10.0.0.2
DNAT       all  --  anywhere             10.0.0.2             to:192.168.0.43
```

**Figure 3: Firewall Nat table**



```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 enp0s25
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 enp0s25
```

**figure 4: Internal host**

## Firewall Design

Three user defined chains are created - **TCP_TRAFFIC, UDP_TRAFFIC** and **ICMP_TRAFFIC**. Below figure shows an overview of the design. The shaded circles are the user defined chains.

(*By default,  INPUT is set to DROP. If the firewall host is connected to the internet through access point (wireless), it will need to handle DHCP traffic in INPUT chain, which is why the traffic could be accepted. If no DHCP is needed for the internet access, traffic to INPUT chain will only go to DROP.)

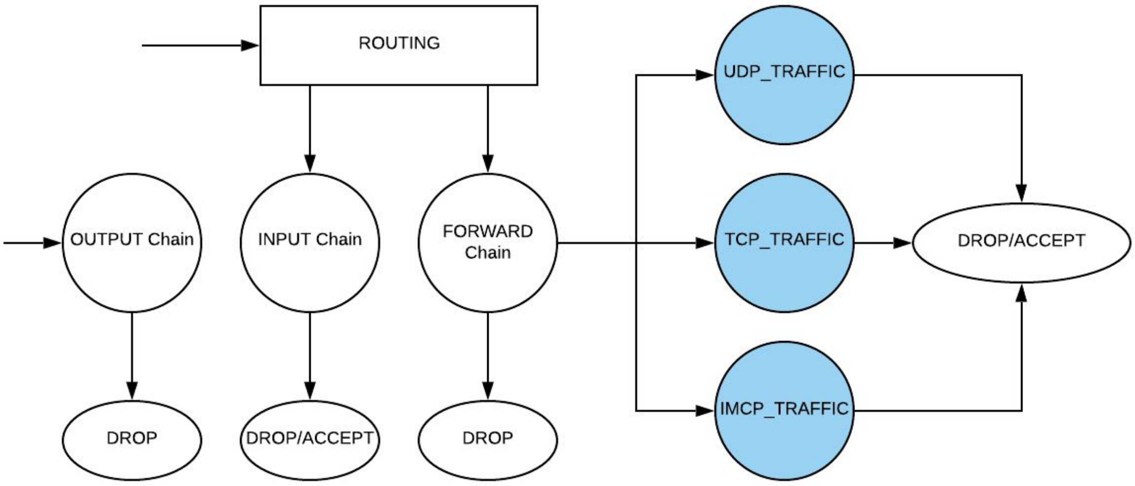


**Figure 3: IP tables (assuming DHCP involved)**

(Rules implementation in detail, order matters, for the **highlight** params, refer to the **How to** section, or read the macros in the config.sh)

**INPUT**

- Accept udp traffic to port 67:68 traffic from port 67:68 (DHCP)
- Drop on default

**OUTPUT**

- Drop on default

**FORWARD**

- Drop any incoming traffic with a source address from outside matching the internal network **LOCAL_NET**
- Drop any traffic direct to port/port range specified in **BLOCK_ALL**
- If incoming traffic is tcp, direct to **TCP_TRAFFIC**
- If incoming traffic is udp, direct to **UDP_TRAFFIC**
- If incoming traffic is icmp, direct to **ICMP_TRAFFIC**
- Drop all inbound SYN packets with destination port **HIGHPORT_RANGE**
- Drop on default

**TCP_TRAFFIC**

- Drop any traffic that has destination port matches with any port specified in **TCP_BLOCK**
- Accept traffic that is
    - Destined to internal host IP **AND**
    - Has destination port that matches with any port specified in **TCP_INBOUND_ALLOWED** **AND**
    - with NEW,ESTABLISHED state
- Accept traffic that is
    - Destined to internal host IP **AND**
    - Has source port that matches with any port specified in **TCP_INBOUND_ALLOWED** **AND**
    - with ESTABLISHED state
- Accept traffic that is
    - Originate from internal host IP **AND**
    - Has destination port that matches with any port specified in **TCP_OUTBOUND_ALLOWED** **AND**
    - with NEW, ESTABLISHED state
- Accept traffic that is
    - Originate from internal host IP **AND**
    - Has source port that matches with any port specified in **TCP_OUTBOUND_ALLOWED** **AND**
    - with ESTABLISHED state
- Drop the rest of the traffic

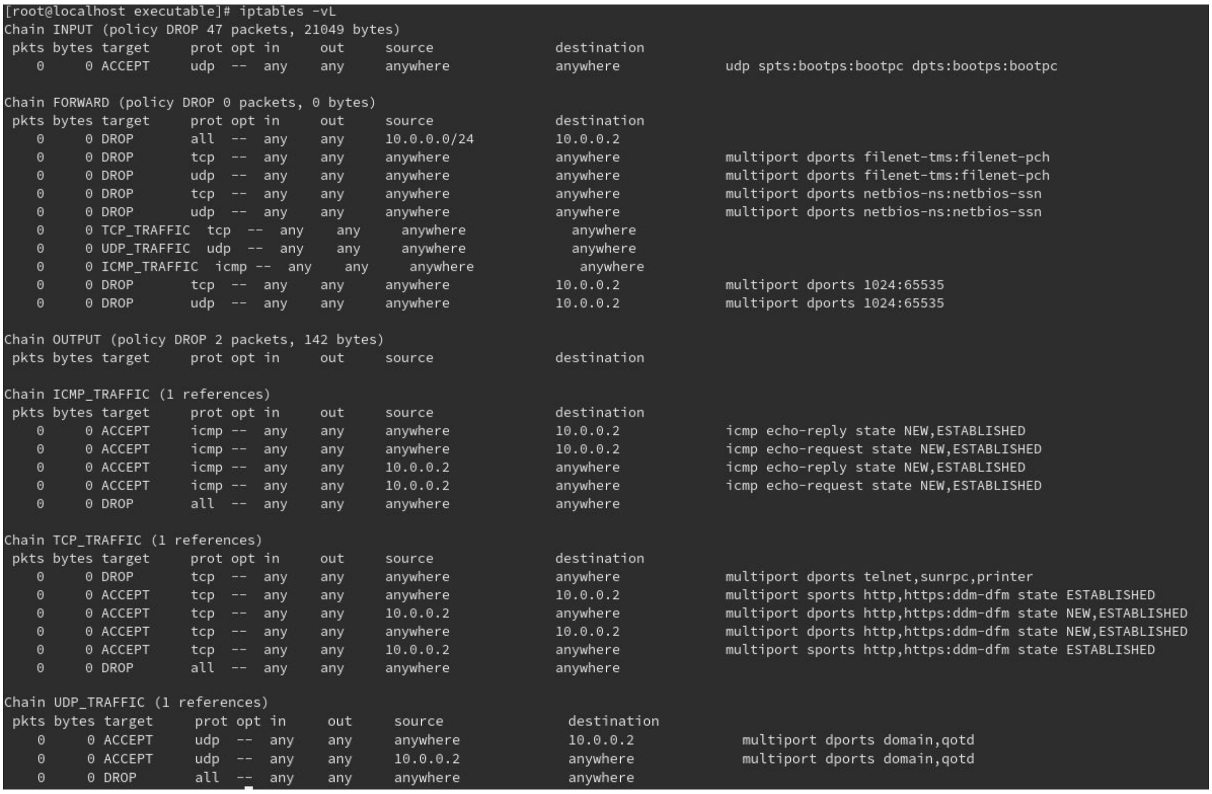
**UDP_TRAFFIC**

- Drop any traffic that has destination port matches with any port specified in **UDP_BLOCK**
- Accept traffic that is
  - Destined to internal host IP **AND**
  - Has destination port that matches with any port specified in **UDP_INBOUND_ALLOWED**
- Accept traffic that is
  - Originate from internal host IP **AND**
  - Has destination port that matches with any port specified in **UDP_OUTBOUND_ALLOWED**
- Drop the rest of the traffic

**ICMP_TRAFFIC**

- Accept traffic that is
  - Destined to internal host IP **AND**
  - Has icmp type matches with any type specified in **ICMP_INBOUND_ALLOWED** **AND**
  - with NEW,ESTABLISHED state
- Accept traffic that is
  - Originate from internal host IP **AND**
  - Has icmp type matches with any type specified in **ICMP_OUTBOUND_ALLOWED** **AND**
  - with NEW,ESTABLISHED state
- Drop the rest of the traffic

# Sample iptable listing on firewall host



```
[root@localhost executable]# iptables -vL
Chain INPUT (policy DROP 47 packets, 21049 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spts:bootps:bootpc dpts:bootps:bootpc

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  any    any     10.0.0.0/24          10.0.0.2
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             multiport dports filenet-tms:filenet-pch
    0     0 DROP       udp  --  any    any     anywhere             anywhere             multiport dports filenet-tms:filenet-pch
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             multiport dports netbios-ns:netbios-ssn
    0     0 DROP       udp  --  any    any     anywhere             anywhere             multiport dports netbios-ns:netbios-ssn
    0     0 TCP_TRAFFIC  tcp  --  any    any     anywhere             anywhere
    0     0 UDP_TRAFFIC  udp  --  any    any     anywhere             anywhere
    0     0 ICMP_TRAFFIC  icmp --  any    any     anywhere             anywhere
    0     0 DROP       tcp  --  any    any     anywhere             10.0.0.2             multiport dports 1024:65535
    0     0 DROP       udp  --  any    any     anywhere             10.0.0.2             multiport dports 1024:65535

Chain OUTPUT (policy DROP 2 packets, 142 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain ICMP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere

Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             multiport dports telnet,sunrpc,printer
    0     0 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2             multiport sports http,https:ddm-dfm state ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere             multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2             multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere             multiport sports http,https:ddm-dfm state ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere

Chain UDP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  any    any     anywhere             10.0.0.2             multiport dports domain,qotd
    0     0 ACCEPT     udp  --  any    any     10.0.0.2             anywhere             multiport dports domain,qotd
    0     0 DROP       all  --  any    any     anywhere             anywhere
```

## How to

The programs are separated to four .sh file

- setup.sh (serve as program entry point for setting up environment, put up firewall and update firewall)
- firewall.sh (firewall rules implementation)
- config.sh (user defined parames for environment setup and firewall rules tweaking)
- firewall-test.sh (automatic test scripts for both internal and external testing)

**Environment setup**

Before setting up, make sure to change params in the "**firewall host and internal host setup"** section in config.sh to match your system params. And then run

```
$ ./setup.sh
```

An option menu will show up, enter

"0" for firewall host setup (includes running ./firewall.sh)
"1" for internal host setup
"2" firewall update
"3" iptables listing
"4" firewall internal test
"5" firewall external test
"q" quit

**Firewall setup**

Choosing option "0" when running setup.sh will automatically put up a firewall. To tweak the firewall setting, modify the params in the "**Firewall params**" section in config.sh. And then run setup.sh again, and enter "2" for firewall update. A list of firewall params will show up in the console to indicate the update completion.

**Firewall test**

Choosing either option "4" or "5" will automatically run through predefined test cases in firewall-test.sh. The result will be logged to a text file, the filename will be whatever assigned for the macro $OUTPUT in config.sh

**Firewall params example**

```
TCP_INBOUND_ALLOWED="80,443:447"
TCP_OUTBOUND_ALLOWED="80,443:447"
```

This example shows that the firewall allows inbound and outbound http and https tcp traffic

```
UDP_INBOUND_ALLOWED="53,17"
UDP_OUTBOUND_ALLOWED="53,17"
```

This example shows that the firewall allows inbound and outbound DNS udp traffic

```
ICMP_INBOUND_ALLOWED=( ”0” , ”8” )
ICMP_OUTBOUND_ALLOWED=( ”0” , ”8” )
```

This example shows that the firewall allows inbound icmp echo reply and outbound icmp echo request.

```
TCP_BLOCK=”23,111,515”
UDP_BLOCK=””
BLOCK_ALL=”32768:32775 137:139”
```

This example shows that the firewall block tcp traffic direct to port 23 (telnet), and all traffic direct to port range 0~1023 and 137~139

```
HIGHPORT_RANGE=”1024:65535”
```

This example shows that the firewall block all incoming SYN packets to high ports

```
OUTPUT_FILE=”result.txt”
```

Result of firewall-test will be direct to the file name result.txt

## Test cases & Results

(*support data for each of the test can be found at **Support evidence** section)

| | |
|---|---|
| Internet gateway IP | : 192.168.0.1 |
| Firewall host internet IP | : 192.168.0.43 |
| Firewall host private network IP | : 10.0.0.1 |
| Internal host private network IP | : 10.0.0.2 |

**Internal test (running from internal host)**

| **Rule #** | **Test Description & precondition** | **Tool Used** | **Expected Result** | **Pass/ Failed** |
|---|---|---|---|---|
| 1 | Verify that TCP traffic generated from the internal host can get through the firewall host and reach outside network. The destination port should match with any of the port specified in TCP_OUTBOUND_ALLOW | hping3, wireshark | ● The internal host should receive reply from the external computer<br>● iptable listing should show total of 10 packets that hit the **TCP_TRAFFIC** chain<br>● Wireshark captures on external computer should show received packets sent from internal host | **Pass** |
| 2 | Verify that UDP traffic generated from the internal host can get through the firewall host and reach outside network. The destination port should match with any of the port specified in UDP_OUTBOUND_ALLOW | hping3, wireshark | ● iptable listing on firewall host should show total of 5 packets that hit the **UDP_TRAFFIC** chain<br>● Wireshark captures on external computer should show received packets sent from internal host | **Pass** |
| 3 | Verify that ICMP traffic generated from the internal host can get through the firewall host and reach outside network. The icmp type should match with any of the types specified in ICMP_OUTBOUND_ALL | hping3, wireshark | ● Internal host should receive reply from the external computer<br>● iptable listing on firewall host should show packets send from internal host hit the | **Pass** |

|  |  |  |  |  |
|---|---|---|---|---|
|  | OW. |  | **ICMP_TRAFFIC** chain<br>● Wireshark captures on the external computer should show received echo request sent from internal host |  |
| 4 | Verify that All TCP, UDP or ICMP packets that fall through default gateway are dropped | hping3, wireshark | ● Internal host should **not** receive any reply from the external computer<br>● iptable listing on firewall host should show packets sent from internal host hit the **TCP_TRAFFIC, UDP_TRAFFIC and ICMP_TRAFFIC** chains and go to **DROP**<br>● Wireshark captures on firewall host should show up packets sent from internal host | **Pass** |
| 5 | Verify that all outgoing telnet packets are dropped | hping3, wireshark | ● Internal host should **not** receive any reply from the external computer<br>● iptables listing on firewall host should show that packets sent from external computer hit the **TCP_TRAFFIC** chain and get **DROP**<br>● Wireshark capture on firewall host should show telnet packets sent from internal host | **Pass** |

**External test (running from machines outside of internal network)**

| Rule # | Test Description & precondition | Tool Used | Expected Result | Pass/ Failed |
|---|---|---|---|---|
| 1 | Verify that TCP traffic generated from the external computer can get through the firewall host and reach the internal host. The destination port should match with any of the port specified in TCP_INBOUND_ALLOW | hping3, wireshark | ● External computer should receive reply from the internal host<br>● iptable listing on firewall host should show total of 10 packets that hit the **TCP_TRAFFIC** chain<br>● Wireshark captures on internal host should show received packets sent from external computer | **Pass** |
| 2 | Verify that UDP traffic generated from the external computer can get through the firewall host and reach the internal host. The destination port should match with any of the port specified in UDP_INBOUND_ALLOW | hping3, wireshark | ● iptable listing on firewall host should show total of 5 packets that hit the **UDP_TRAFFIC** chain<br>● Wireshark captures on internal host should show received packets sent from external computer | **Pass** |
| 3 | Verify that ICMP traffic generated from the external computer can get through the firewall host and reach the internal host. The icmp type should match with any of the types specified in ICMP_INBOUND_ALLOW | hping3, wireshark | ● External computer should receive reply from the internal host<br>● iptable listing on firewall host should show packets send from external computer hit the **ICMP_TRAFFIC** chain<br>● Wireshark captures on internal host should show received packets sent from external computer | **Pass** |
| 4 | Verify that all TCP, UDP or | hping3, | ● External computer | **Pass** |

| | | | | |
|---|---|---|---|---|
| | ICMP packets that fall through default gateway are dropped | wireshark | should **not** receive any reply from the internal host<br>● iptable listing should show packets sent from external computer hit the **TCP_TRAFFIC, UDP_TRAFFIC and ICMP_TRAFFIC** chains<br>● Wireshark captures on firewall host should show up packets sent from external computer | |
| 5 | Verify that all packets destined for the firewall host from outside are dropped | hping3, wireshark | ● iptables listing on firewall host should show that default policy for both **INPUT** and **OUTPUT** chain are set to **DROP** | **Pass** |
| 6 | Verify that any packets with a source address from the outside matching the internal network are dropped | hping3, wireshark | ● External computer should **not** receive any reply from the internal host<br>● iptable listing should show the packets sent from external computer hit the **FORWARD** and go to **DROP** | **Pass** |
| 7 | Verify that inbound SYN packet to high port are dropped | hping3, wireshark | ● External computer should **not** receive any reply from the internal host<br>● iptables listing should show that packets sent from the external computer hit the **FORWARD** chain and go to **DROP** | **Pass** |

| | | | | |
|---|---|---|---|---|
| 8 | Accepts all TCP packets that belongs to an existing connection (on allowed port) | ncat, wireshark | ● The internal host should receive packets from the external computer after the three-way handshake is completed.<br>● Wireshark capture on internal host should should that sequence of packets received from external computer after the three way handshake | **Pass** |
| 9 | Verify that all incoming telnet packets are dropped | hping3, wireshark | ● External computer should **not** receive any reply from the internal host<br>● iptables listing on firewall host should show that packets sent from external computer hit the **TCP_TRAFFIC** chain and get **DROP**<br>● Wireshark capture on firewall host should show telnet packets sent from external computer | **Pass** |
| 10 | Verify that all external traffic directed to port<br>● 32768 - 32775<br>● 137 - 139<br>● TCP 111, 515<br>are blocked | hping3, wireshark | ● External computer should **not** receive any reply from the internal host<br>● iptable listing on firewall hosts should show that packets sent from external computers hit the **TCP_TRAFFIC** and **FORWARD** that go to **DROP**.<br>● Wireshark capture on firewall host should show packets sent | **Pass** |

| | | | | |
|---|---|---|---|---|
| | | | from external computer | |
| 11 | Verify that inbound packets with SYN\FIN bit set are dropped | hping3, wireshark | ● External computer should **not** receive any reply from the internal host<br>● Wireshark capture on firewall host should show packets sent from the external computer | **Pass** |

## Support evidence

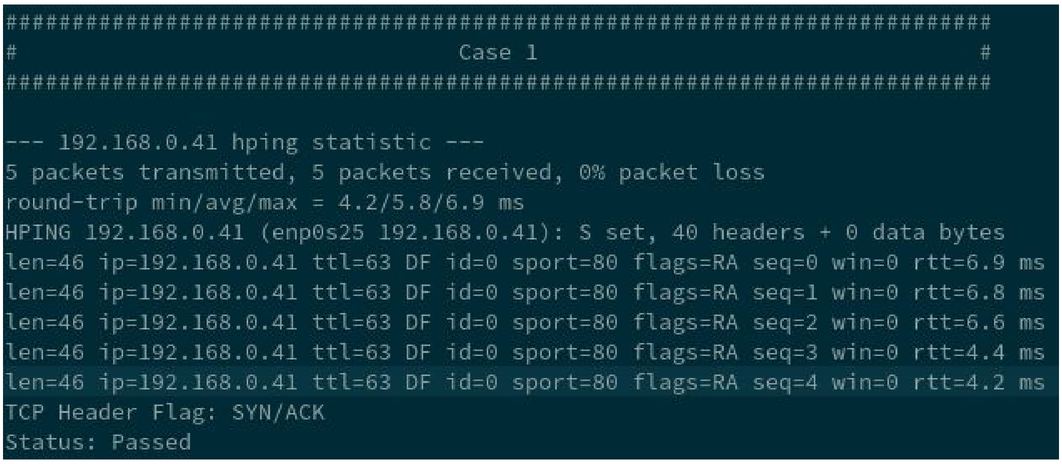
(*The wireshark captures can be found in the “external-test-captures” and “internal-test-captures” folder, the automatic test results are printed to test-result.txt)

### Internal test Case# 1

firewall host ip: 192.168.0.40
external computer ip: 192.168.0.41
internal host ip: 10.0.0.2

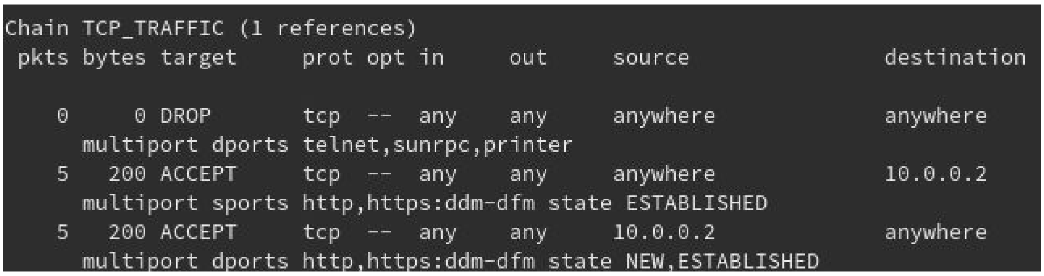
internal host -> external computer
**Detail**: Internal host probs external computer with TCP packets five times and go responses. A total of 10 packets showed up in the **TCP_TRAFFIC** that went to **ACCEPT** chain. The wireshark captures on the external computer should show TCP SYN requests from the internal host.

(hping3 output on internal host)



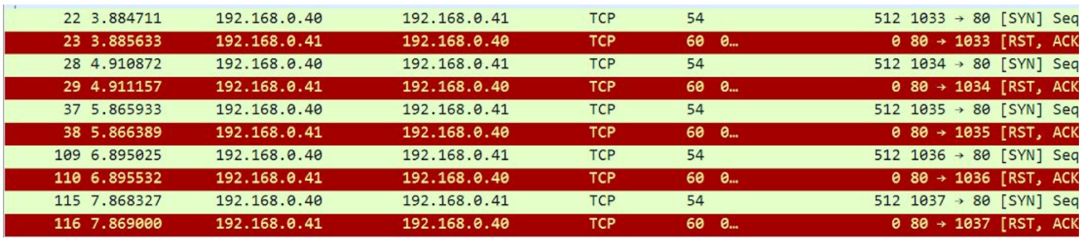
```
##########################################################################
#                                  Case 1                                #
##########################################################################

--- 192.168.0.41 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.2/5.8/6.9 ms
HPING 192.168.0.41 (enp0s25 192.168.0.41): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.41 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=6.9 ms
len=46 ip=192.168.0.41 ttl=63 DF id=0 sport=80 flags=RA seq=1 win=0 rtt=6.8 ms
len=46 ip=192.168.0.41 ttl=63 DF id=0 sport=80 flags=RA seq=2 win=0 rtt=6.6 ms
len=46 ip=192.168.0.41 ttl=63 DF id=0 sport=80 flags=RA seq=3 win=0 rtt=4.4 ms
len=46 ip=192.168.0.41 ttl=63 DF id=0 sport=80 flags=RA seq=4 win=0 rtt=4.2 ms
TCP Header Flag: SYN/ACK
Status: Passed
```

(iptable listing on firewall host)



```
Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       tcp  --  any    any     anywhere             anywhere
      multiport dports telnet,sunrpc,printer
    5   200 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2
      multiport sports http,https:ddm-dfm state ESTABLISHED
    5   200 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere
      multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
```

(wireshark capture on the external computer)

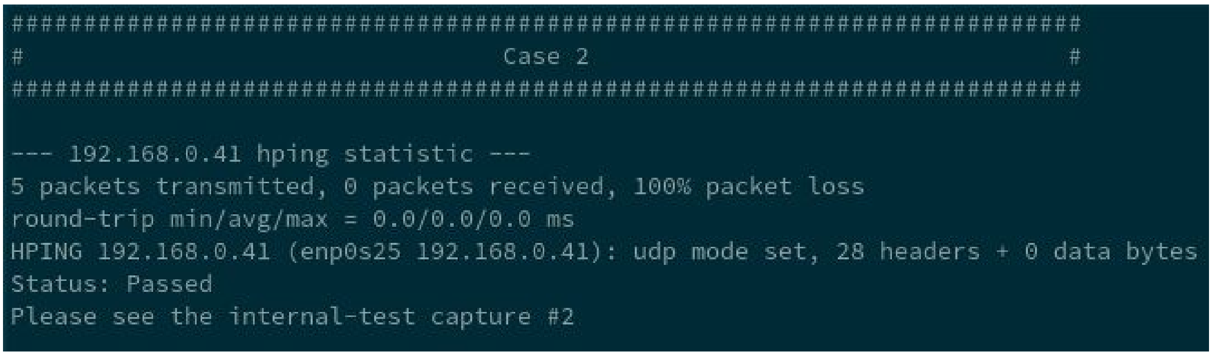


```
 22 3.884711   192.168.0.40   192.168.0.41   TCP   54         512 1033 → 80 [SYN] Seq
 23 3.885633   192.168.0.41   192.168.0.40   TCP   60  0…       0 80 → 1033 [RST, ACK
 28 4.910872   192.168.0.40   192.168.0.41   TCP   54         512 1034 → 80 [SYN] Seq
 29 4.911157   192.168.0.41   192.168.0.40   TCP   60  0…       0 80 → 1034 [RST, ACK
 37 5.865933   192.168.0.40   192.168.0.41   TCP   54         512 1035 → 80 [SYN] Seq
 38 5.866389   192.168.0.41   192.168.0.40   TCP   60  0…       0 80 → 1035 [RST, ACK
109 6.895025   192.168.0.40   192.168.0.41   TCP   54         512 1036 → 80 [SYN] Seq
110 6.895532   192.168.0.41   192.168.0.40   TCP   60  0…       0 80 → 1036 [RST, ACK
115 7.868327   192.168.0.40   192.168.0.41   TCP   54         512 1037 → 80 [SYN] Seq
116 7.869000   192.168.0.41   192.168.0.40   TCP   60  0…       0 80 → 1037 [RST, ACK
```

**Internal test Case# 2**
firewall host ip: 192.168.0.40
external computer ip: 192.168.0.41
internal host ip: 10.0.0.2

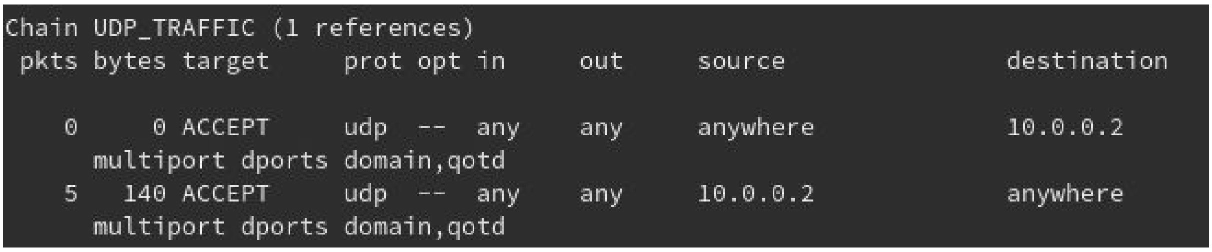
internal host -> external computer
**Detail**: Internal host probs external computer with UDP packets five times and got no response. A total of 5 packets showed up in the **UDP_TRAFFIC** that went to **ACCEPT** chain. The wireshark captures on the external computer should show 5 packets received from the internal host.

(hping3 output on internal host)



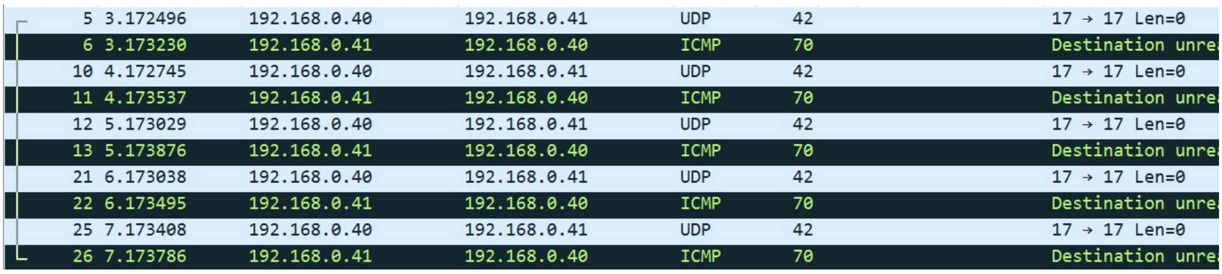
```
##########################################################################
#                                 Case 2                                 #
##########################################################################

--- 192.168.0.41 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.41 (enp0s25 192.168.0.41): udp mode set, 28 headers + 0 data bytes
Status: Passed
Please see the internal-test capture #2
```

(iptable listing on firewall host)



```
Chain UDP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     udp  --  any    any     anywhere             10.0.0.2
      multiport dports domain,qotd
    5   140 ACCEPT     udp  --  any    any     10.0.0.2             anywhere
      multiport dports domain,qotd
```

(wireshark capture on external computer)

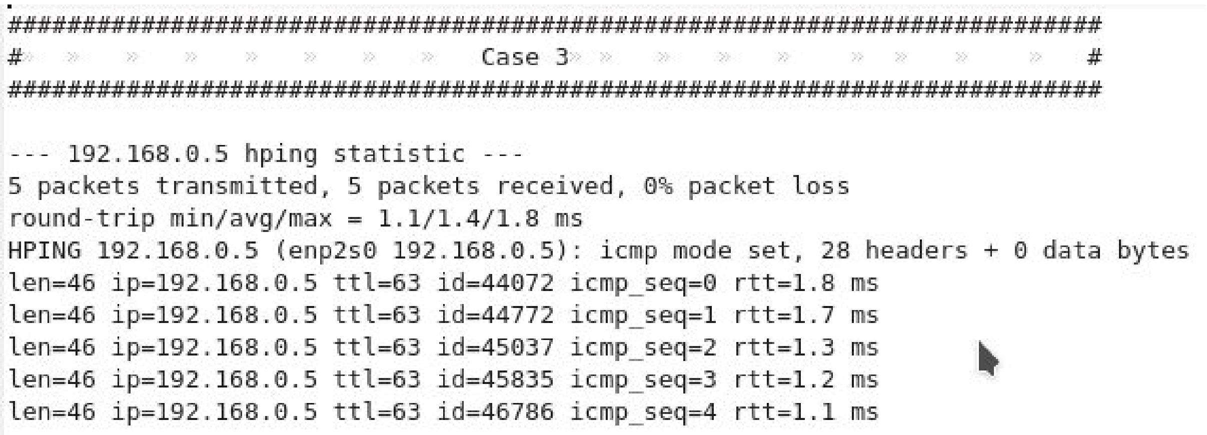


```
  5 3.172496   192.168.0.40   192.168.0.41   UDP    42     17 → 17 Len=0
  6 3.173230   192.168.0.41   192.168.0.40   ICMP   70     Destination unre
 10 4.172745   192.168.0.40   192.168.0.41   UDP    42     17 → 17 Len=0
 11 4.173537   192.168.0.41   192.168.0.40   ICMP   70     Destination unre
 12 5.173029   192.168.0.40   192.168.0.41   UDP    42     17 → 17 Len=0
 13 5.173876   192.168.0.41   192.168.0.40   ICMP   70     Destination unre
 21 6.173038   192.168.0.40   192.168.0.41   UDP    42     17 → 17 Len=0
 22 6.173495   192.168.0.41   192.168.0.40   ICMP   70     Destination unre
 25 7.173408   192.168.0.40   192.168.0.41   UDP    42     17 → 17 Len=0
 26 7.173786   192.168.0.41   192.168.0.40   ICMP   70     Destination unre
```

**Internal test Case# 3**
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

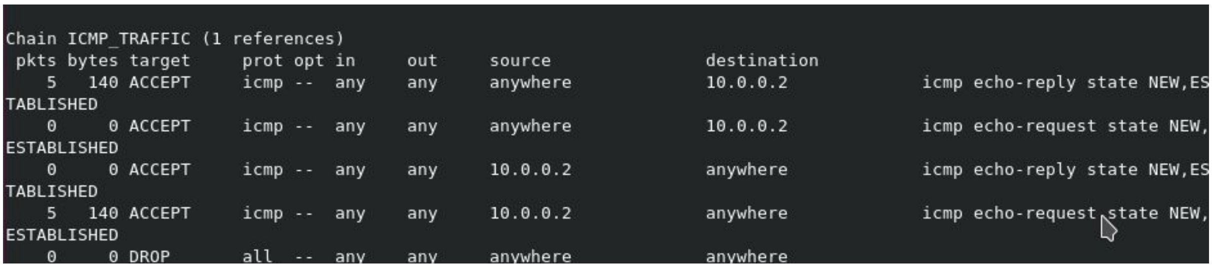
internal host -> external computer
**Detail**: Internal host probs external computer with ICMP packets five times and got response. A total of 10 packets showed up in the **ICMP_TRAFFIC** that went to **ACCEPT** chain. The wireshark captures on the internal host show 5 echo requests (from internal host) and 5 echo reply (from external computer).

(hping3 output on internal host)



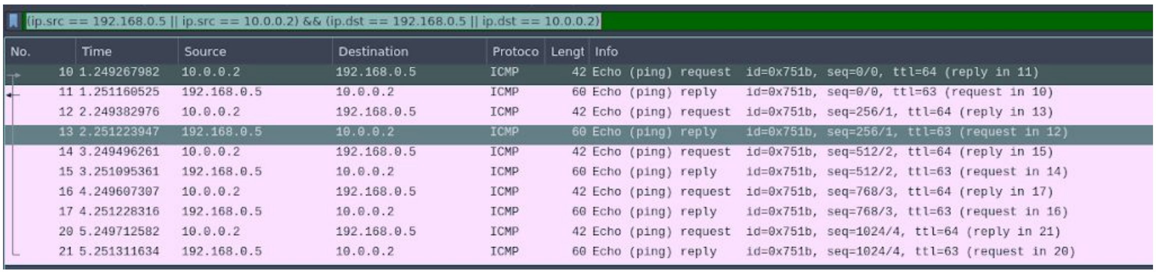
```
############################################################################
#                               Case 3                                     #
############################################################################

--- 192.168.0.5 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.4/1.8 ms
HPING 192.168.0.5 (enp2s0 192.168.0.5): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.5 ttl=63 id=44072 icmp_seq=0 rtt=1.8 ms
len=46 ip=192.168.0.5 ttl=63 id=44772 icmp_seq=1 rtt=1.7 ms
len=46 ip=192.168.0.5 ttl=63 id=45037 icmp_seq=2 rtt=1.3 ms
len=46 ip=192.168.0.5 ttl=63 id=45835 icmp_seq=3 rtt=1.2 ms
len=46 ip=192.168.0.5 ttl=63 id=46786 icmp_seq=4 rtt=1.1 ms
```

(iptable listing on firewall host)



```
Chain ICMP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    5   140 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-reply state NEW,ES
TABLISHED
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-request state NEW,
ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-reply state NEW,ES
TABLISHED
    5   140 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-request state NEW,
ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere
```

(wireshark capture on internal host)



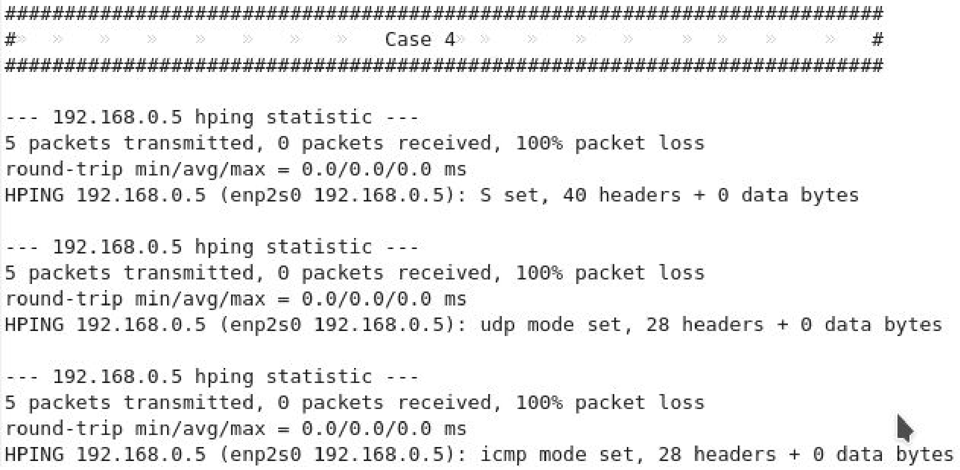
(ip.src == 192.168.0.5 || ip.src == 10.0.0.2) && (ip.dst == 192.168.0.5 || ip.dst == 10.0.0.2)

| No. | Time | Source | Destination | Protoco | Lengt | Info |
|---|---|---|---|---|---|---|
| 10 | 1.249267982 | 10.0.0.2 | 192.168.0.5 | ICMP | 42 | Echo (ping) request  id=0x751b, seq=0/0, ttl=64 (reply in 11) |
| 11 | 1.251160525 | 192.168.0.5 | 10.0.0.2 | ICMP | 60 | Echo (ping) reply    id=0x751b, seq=0/0, ttl=63 (request in 10) |
| 12 | 2.249382976 | 10.0.0.2 | 192.168.0.5 | ICMP | 42 | Echo (ping) request  id=0x751b, seq=256/1, ttl=64 (reply in 13) |
| 13 | 2.251223947 | 192.168.0.5 | 10.0.0.2 | ICMP | 60 | Echo (ping) reply    id=0x751b, seq=256/1, ttl=63 (request in 12) |
| 14 | 3.249496261 | 10.0.0.2 | 192.168.0.5 | ICMP | 42 | Echo (ping) request  id=0x751b, seq=512/2, ttl=64 (reply in 15) |
| 15 | 3.251095361 | 192.168.0.5 | 10.0.0.2 | ICMP | 60 | Echo (ping) reply    id=0x751b, seq=512/2, ttl=63 (request in 14) |
| 16 | 4.249607307 | 10.0.0.2 | 192.168.0.5 | ICMP | 42 | Echo (ping) request  id=0x751b, seq=768/3, ttl=64 (reply in 17) |
| 17 | 4.251228316 | 192.168.0.5 | 10.0.0.2 | ICMP | 60 | Echo (ping) reply    id=0x751b, seq=768/3, ttl=63 (request in 16) |
| 20 | 5.249712582 | 10.0.0.2 | 192.168.0.5 | ICMP | 42 | Echo (ping) request  id=0x751b, seq=1024/4, ttl=64 (reply in 21) |
| 21 | 5.251311634 | 192.168.0.5 | 10.0.0.2 | ICMP | 60 | Echo (ping) reply    id=0x751b, seq=1024/4, ttl=63 (request in 20) |

**Internal test Case# 4**
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

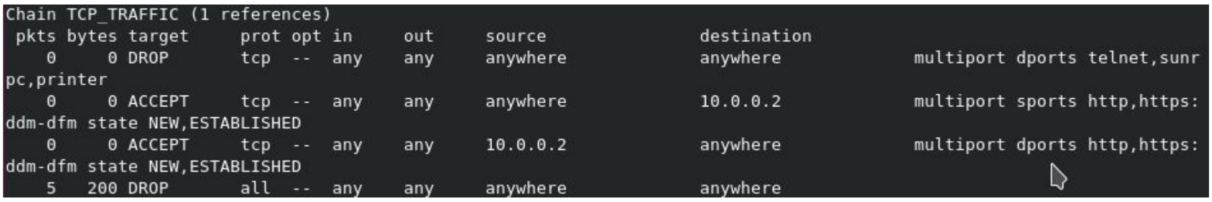
internal host -> external computer
**Detail**: Internal host probes the external computer with 5 TCP, 5 UDP and 5 ICMP packets got no response. A total of 15 packets should show up in each of the **TCP_TRAFFIC, UDP_TRAFFIC** and **ICMP_TRAFFIC** chains that go to **DROP** (15 packets dropped in total). The wireshark captures on the firewall host shows that 15 incoming traffic (UDP, TCP and ICMP)

(hping3 output on internal host)

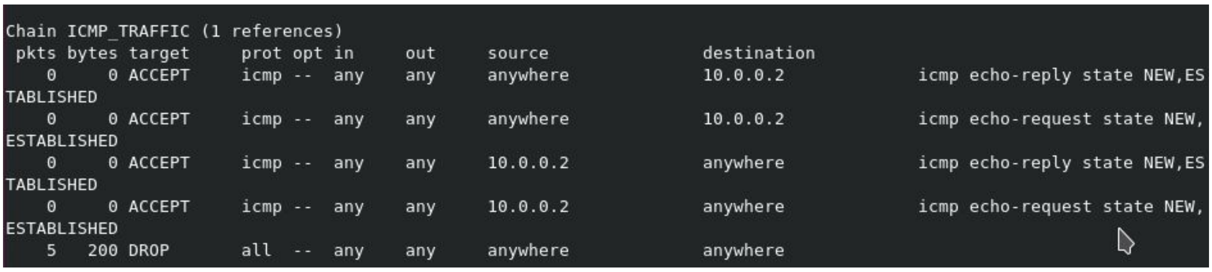


```
##########################################################################
#»  »   »   »   »   »   »   »   Case 4» »   »   »   »    »  »   »    »   #
##########################################################################

--- 192.168.0.5 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.5 (enp2s0 192.168.0.5): S set, 40 headers + 0 data bytes

--- 192.168.0.5 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.5 (enp2s0 192.168.0.5): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.5 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.5 (enp2s0 192.168.0.5): icmp mode set, 28 headers + 0 data bytes
```

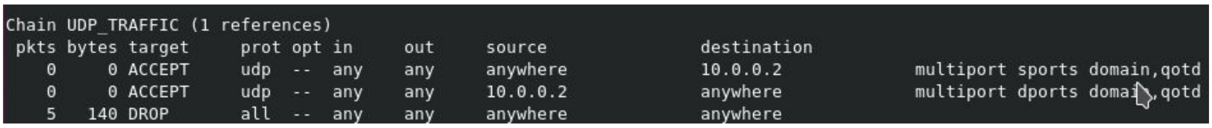
(iptable listing on firewall host)



```
Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             multiport dports telnet,sunr
pc,printer
    0     0 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2             multiport sports http,https:
ddm-dfm state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere             multiport dports http,https:
ddm-dfm state NEW,ESTABLISHED
    5   200 DROP       all  --  any    any     anywhere             anywhere
```

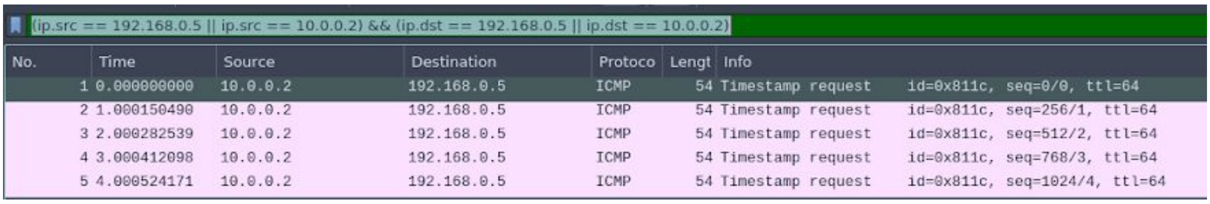


```
Chain ICMP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-reply state NEW,ES
TABLISHED
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-request state NEW,
ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-reply state NEW,ES
TABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-request state NEW,
ESTABLISHED
    5   200 DROP       all  --  any    any     anywhere             anywhere
```

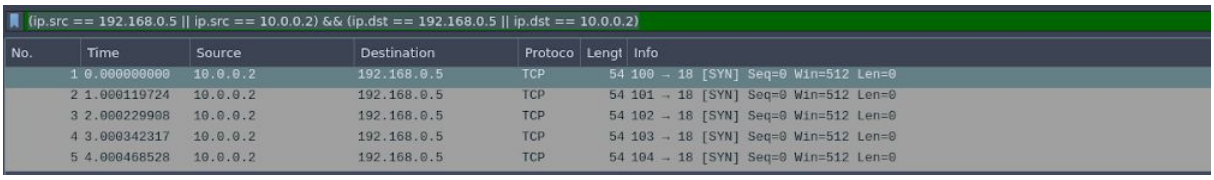


```
Chain UDP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  any    any     anywhere             10.0.0.2             multiport sports domain,qotd
    0     0 ACCEPT     udp  --  any    any     10.0.0.2             anywhere             multiport dports domain,qotd
    5   140 DROP       all  --  any    any     anywhere             anywhere
```

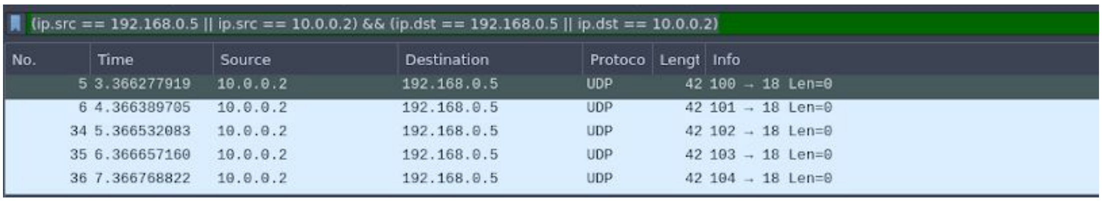
(wireshark capture on firewall host)



```
(ip.src == 192.168.0.5 || ip.src == 10.0.0.2) && (ip.dst == 192.168.0.5 || ip.dst == 10.0.0.2)
No.    Time           Source      Destination    Protoco Lengt Info
     1 0.000000000    10.0.0.2    192.168.0.5    ICMP       54 Timestamp request    id=0x811c, seq=0/0, ttl=64
     2 1.000150490    10.0.0.2    192.168.0.5    ICMP       54 Timestamp request    id=0x811c, seq=256/1, ttl=64
     3 2.000282539    10.0.0.2    192.168.0.5    ICMP       54 Timestamp request    id=0x811c, seq=512/2, ttl=64
     4 3.000412098    10.0.0.2    192.168.0.5    ICMP       54 Timestamp request    id=0x811c, seq=768/3, ttl=64
     5 4.000524171    10.0.0.2    192.168.0.5    ICMP       54 Timestamp request    id=0x811c, seq=1024/4, ttl=64
```



```
(ip.src == 192.168.0.5 || ip.src == 10.0.0.2) && (ip.dst == 192.168.0.5 || ip.dst == 10.0.0.2)
No.    Time           Source      Destination    Protoco Lengt Info
     1 0.000000000    10.0.0.2    192.168.0.5    TCP        54 100 → 18 [SYN] Seq=0 Win=512 Len=0
     2 1.000119724    10.0.0.2    192.168.0.5    TCP        54 101 → 18 [SYN] Seq=0 Win=512 Len=0
     3 2.000229908    10.0.0.2    192.168.0.5    TCP        54 102 → 18 [SYN] Seq=0 Win=512 Len=0
     4 3.000342317    10.0.0.2    192.168.0.5    TCP        54 103 → 18 [SYN] Seq=0 Win=512 Len=0
     5 4.000468528    10.0.0.2    192.168.0.5    TCP        54 104 → 18 [SYN] Seq=0 Win=512 Len=0
```

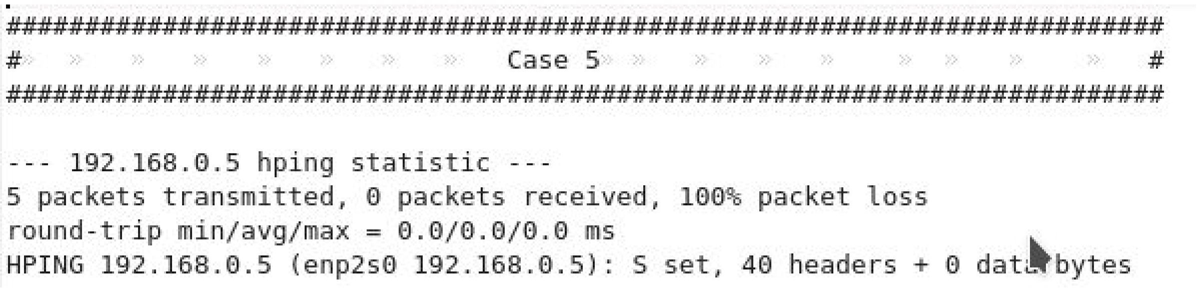


```
(ip.src == 192.168.0.5 || ip.src == 10.0.0.2) && (ip.dst == 192.168.0.5 || ip.dst == 10.0.0.2)
No.    Time           Source      Destination    Protoco Lengt Info
     5 3.366277919    10.0.0.2    192.168.0.5    UDP        42 100 → 18 Len=0
     6 4.366389705    10.0.0.2    192.168.0.5    UDP        42 101 → 18 Len=0
    34 5.366532083    10.0.0.2    192.168.0.5    UDP        42 102 → 18 Len=0
    35 6.366657160    10.0.0.2    192.168.0.5    UDP        42 103 → 18 Len=0
    36 7.366768822    10.0.0.2    192.168.0.5    UDP        42 104 → 18 Len=0
```

**Internal test Case# 5**
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

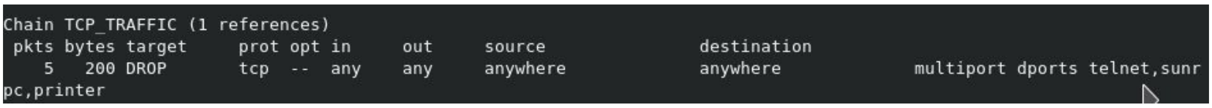
internal host -> external computer
**Detail**: Internal host probe the external computer with telnet packets five times. A total of 5 packets should show up in the **TCP_TRAFFIC** chain that go to **DROP**. The wireshark captures on the firewall host shows that 5 incoming traffic (port 23 to port 23) was received from the network

(hping3 output on internal host)



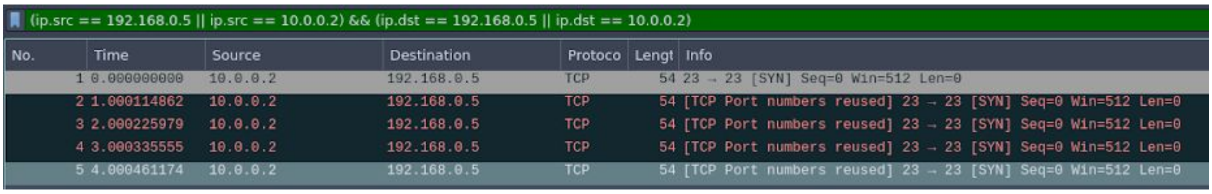
```
#############################################################################
#                                Case 5                                     #
#############################################################################

--- 192.168.0.5 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.5 (enp2s0 192.168.0.5): S set, 40 headers + 0 data bytes
```

(iptables output on firewall host)



```
Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    5   200 DROP       tcp  --  any    any     anywhere             anywhere             multiport dports telnet,sunr
pc,printer
```

(wireshark capture on firewall host)

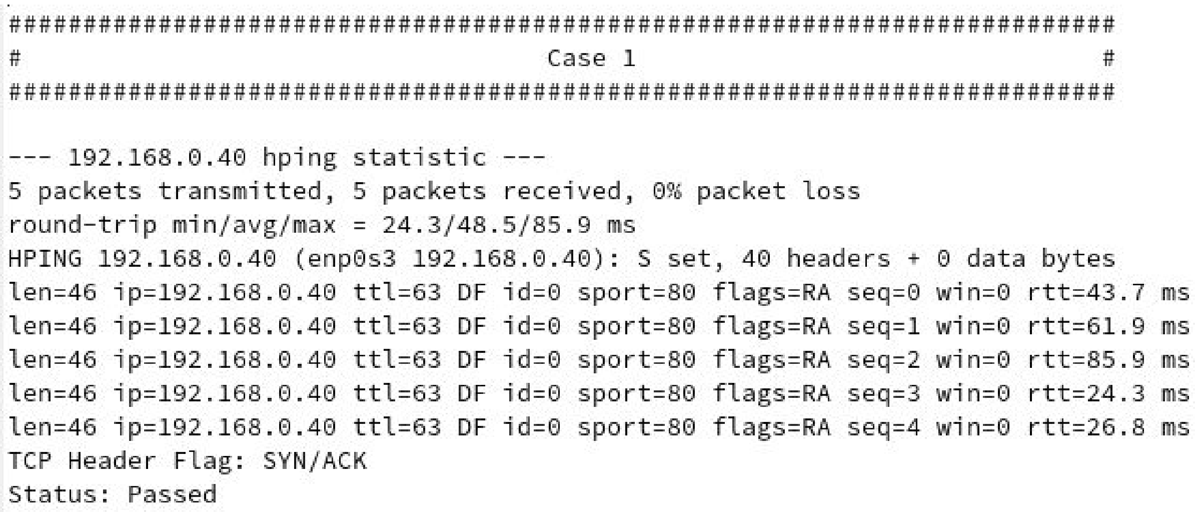


```
(ip.src == 192.168.0.5 || ip.src == 10.0.0.2) && (ip.dst == 192.168.0.5 || ip.dst == 10.0.0.2)
No.     Time            Source          Destination     Protoco Lengt Info
      1 0.000000000     10.0.0.2        192.168.0.5     TCP       54 23 → 23 [SYN] Seq=0 Win=512 Len=0
      2 1.000114862     10.0.0.2        192.168.0.5     TCP       54 [TCP Port numbers reused] 23 → 23 [SYN] Seq=0 Win=512 Len=0
      3 2.000225979     10.0.0.2        192.168.0.5     TCP       54 [TCP Port numbers reused] 23 → 23 [SYN] Seq=0 Win=512 Len=0
      4 3.000335555     10.0.0.2        192.168.0.5     TCP       54 [TCP Port numbers reused] 23 → 23 [SYN] Seq=0 Win=512 Len=0
      5 4.000461174     10.0.0.2        192.168.0.5     TCP       54 [TCP Port numbers reused] 23 → 23 [SYN] Seq=0 Win=512 Len=0
```

**External test Case# 1**
firewall host ip: 192.168.0.40
external computer ip: 192.168.0.41
internal host ip: 10.0.0.2

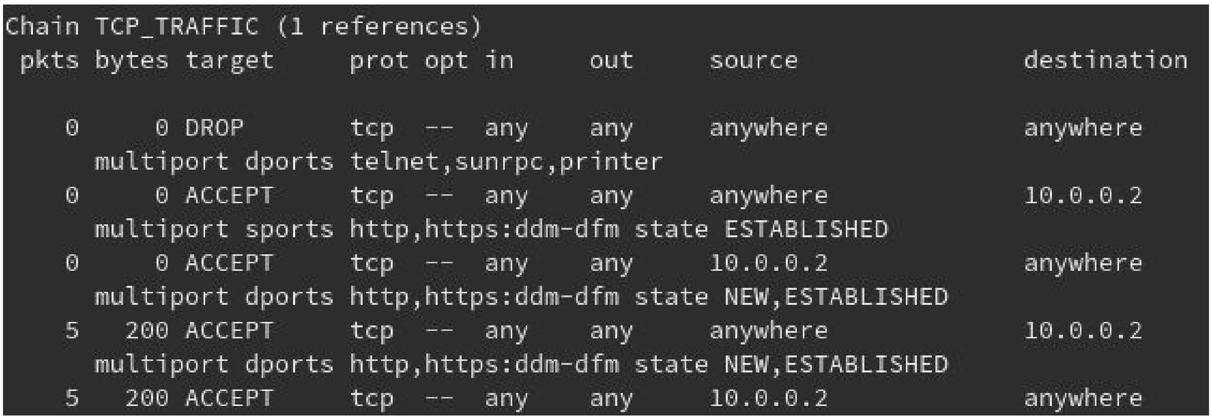
external computer -> firewall host
**Detail**: External computer probes firewall host with TCP packets five times and got response. So a total of 10 packets should show up in the **TCP_TRAFFIC** chain that goes to **ACCEPT** (request and reply). The wireshark captures on the internal host shows that 5 incoming traffic (port 443 to port 443) was received from the network.

(hping3 output on external computer)



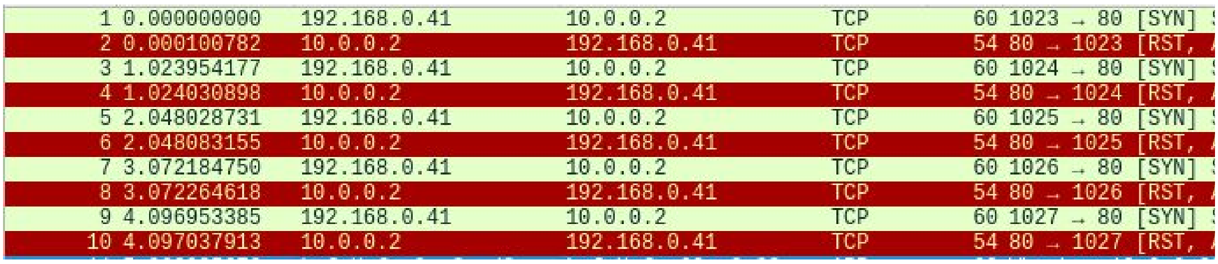
```
###########################################################################
#                                    Case 1                               #
###########################################################################

--- 192.168.0.40 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 24.3/48.5/85.9 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.40 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=43.7 ms
len=46 ip=192.168.0.40 ttl=63 DF id=0 sport=80 flags=RA seq=1 win=0 rtt=61.9 ms
len=46 ip=192.168.0.40 ttl=63 DF id=0 sport=80 flags=RA seq=2 win=0 rtt=85.9 ms
len=46 ip=192.168.0.40 ttl=63 DF id=0 sport=80 flags=RA seq=3 win=0 rtt=24.3 ms
len=46 ip=192.168.0.40 ttl=63 DF id=0 sport=80 flags=RA seq=4 win=0 rtt=26.8 ms
TCP Header Flag: SYN/ACK
Status: Passed
```

(iptable listing on firewall host)



```
Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       tcp  --  any    any     anywhere             anywhere
      multiport dports telnet,sunrpc,printer
    0     0 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2
      multiport sports http,https:ddm-dfm state ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere
      multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
    5   200 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2
      multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
    5   200 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere
```

(wireshark capture on internal host)

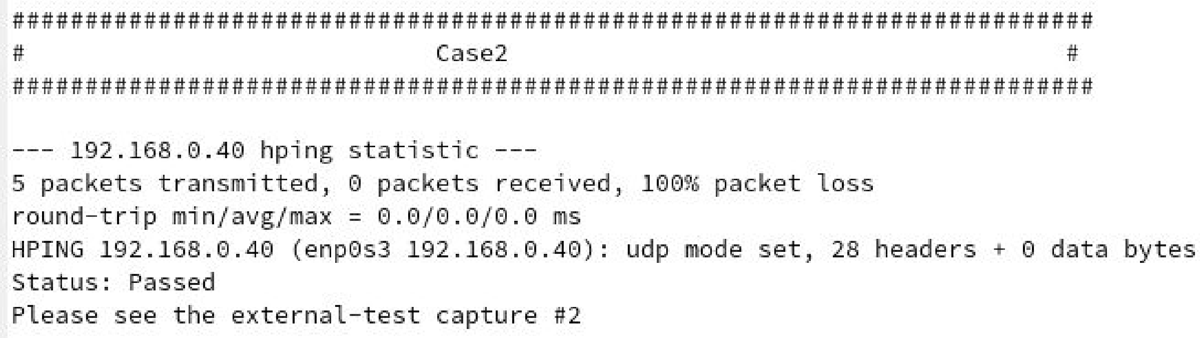


```
      1 0.000000000   192.168.0.41     10.0.0.2         TCP      60 1023 → 80 [SYN]
      2 0.000100782   10.0.0.2         192.168.0.41     TCP      54 80 → 1023 [RST,
      3 1.023954177   192.168.0.41     10.0.0.2         TCP      60 1024 → 80 [SYN]
      4 1.024030898   10.0.0.2         192.168.0.41     TCP      54 80 → 1024 [RST,
      5 2.048028731   192.168.0.41     10.0.0.2         TCP      60 1025 → 80 [SYN]
      6 2.048083155   10.0.0.2         192.168.0.41     TCP      54 80 → 1025 [RST,
      7 3.072184750   192.168.0.41     10.0.0.2         TCP      60 1026 → 80 [SYN]
      8 3.072264618   10.0.0.2         192.168.0.41     TCP      54 80 → 1026 [RST,
      9 4.096953385   192.168.0.41     10.0.0.2         TCP      60 1027 → 80 [SYN]
     10 4.097037913   10.0.0.2         192.168.0.41     TCP      54 80 → 1027 [RST,
```

**External test Case# 2**
firewall host ip: 192.168.0.40
external computer ip: 192.168.0.41
internal host ip: 10.0.0.2

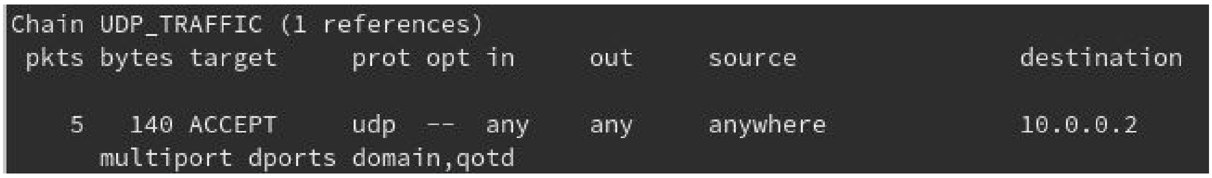
external computer -> firewall host
**Detail**: External computer probes firewall host with UDP packets five times and got response. So a total of 5 packets should show up in the **UDP_TRAFFIC** chain that goes to **ACCEPT** (incoming only). The wireshark captures on the internal host shows that 5 incoming traffic (port 17 to port 17) was received from the network.

(hping3 output on external computer)



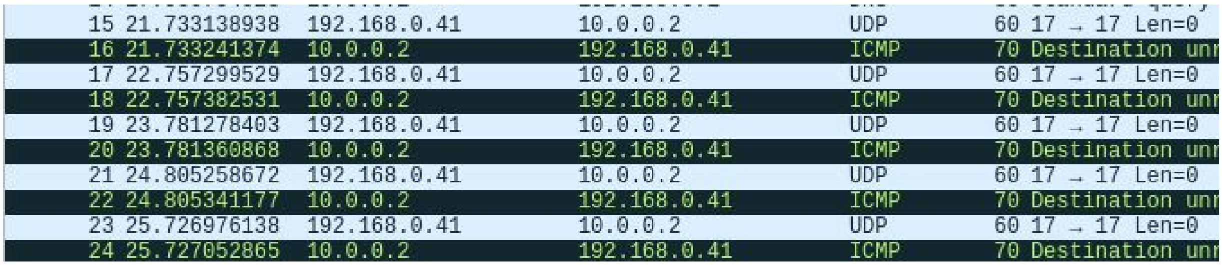
```
##########################################################################
#                            Case2                                       #
##########################################################################

--- 192.168.0.40 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): udp mode set, 28 headers + 0 data bytes
Status: Passed
Please see the external-test capture #2
```

(iptable listing on firewall host)



```
Chain UDP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination

    5   140 ACCEPT     udp  --  any    any     anywhere             10.0.0.2
      multiport dports domain,qotd
```

(wireshark capture on internal host)

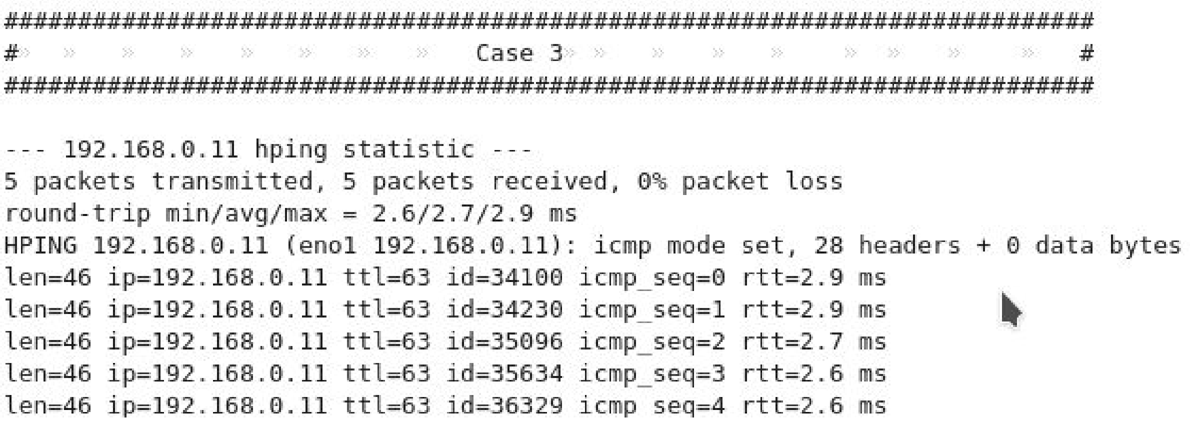


```
15 21.733138938  192.168.0.41       10.0.0.2           UDP        60 17 → 17 Len=0
16 21.733241374  10.0.0.2           192.168.0.41       ICMP       70 Destination unr
17 22.757299529  192.168.0.41       10.0.0.2           UDP        60 17 → 17 Len=0
18 22.757382531  10.0.0.2           192.168.0.41       ICMP       70 Destination unr
19 23.781278403  192.168.0.41       10.0.0.2           UDP        60 17 → 17 Len=0
20 23.781360868  10.0.0.2           192.168.0.41       ICMP       70 Destination unr
21 24.805258672  192.168.0.41       10.0.0.2           UDP        60 17 → 17 Len=0
22 24.805341177  10.0.0.2           192.168.0.41       ICMP       70 Destination unr
23 25.726976138  192.168.0.41       10.0.0.2           UDP        60 17 → 17 Len=0
24 25.727052865  10.0.0.2           192.168.0.41       ICMP       70 Destination unr
```

**External test Case# 3**
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

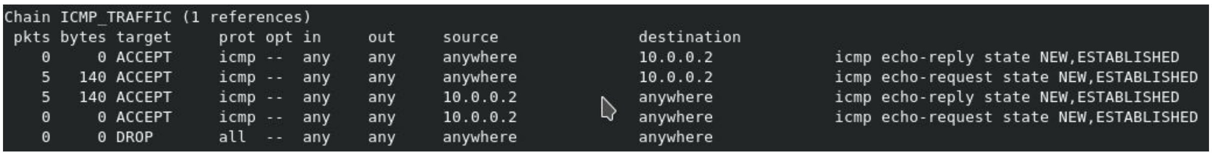
external computer -> firewall host
**Detail**: External computer probes firewall host with ICMP packets five times and got response. So a total of 10 packets should show up in the **ICMP_TRAFFIC** chain that goes to **ACCEPT** (request and reply). The wireshark captures on the internal host shows that 5 echo reply sent from the internal host.

(hping3 output on external computer)



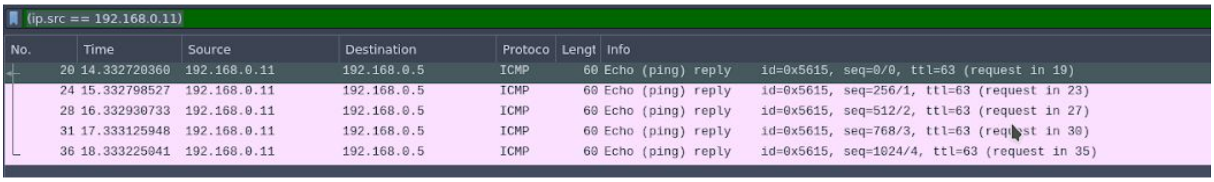
```
##########################################################################
#»  »   »   »   »   »   »   »    Case 3» »   »   »   »    »  »   »    »   #
##########################################################################

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.6/2.7/2.9 ms
HPING 192.168.0.11 (eno1 192.168.0.11): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.11 ttl=63 id=34100 icmp_seq=0 rtt=2.9 ms
len=46 ip=192.168.0.11 ttl=63 id=34230 icmp_seq=1 rtt=2.9 ms
len=46 ip=192.168.0.11 ttl=63 id=35096 icmp_seq=2 rtt=2.7 ms
len=46 ip=192.168.0.11 ttl=63 id=35634 icmp_seq=3 rtt=2.6 ms
len=46 ip=192.168.0.11 ttl=63 id=36329 icmp seq=4 rtt=2.6 ms
```

(iptable listing on firewall host)



```
Chain ICMP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-reply state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-request state NEW,ESTABLISHED
    5   140 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-request state NEW,ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere
```

(wireshark capture on internal host)



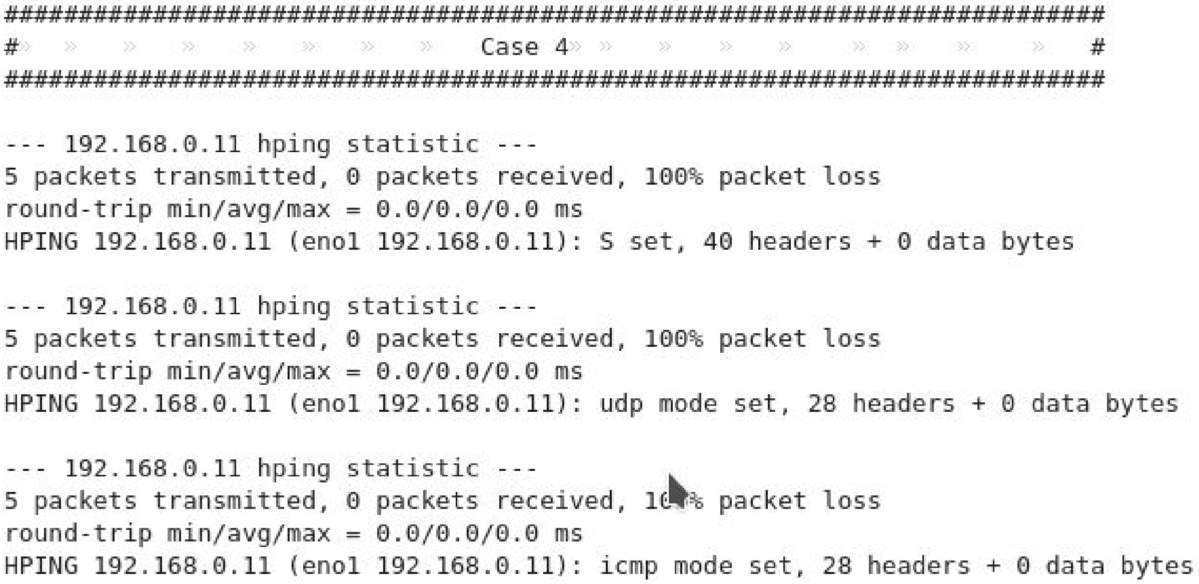
(ip.src == 192.168.0.11)

| No. | Time | Source | Destination | Protoco | Lengt | Info |
|---|---|---|---|---|---|---|
| 20 | 14.332720360 | 192.168.0.11 | 192.168.0.5 | ICMP | 60 | Echo (ping) reply id=0x5615, seq=0/0, ttl=63 (request in 19) |
| 24 | 15.332798527 | 192.168.0.11 | 192.168.0.5 | ICMP | 60 | Echo (ping) reply id=0x5615, seq=256/1, ttl=63 (request in 23) |
| 28 | 16.332930733 | 192.168.0.11 | 192.168.0.5 | ICMP | 60 | Echo (ping) reply id=0x5615, seq=512/2, ttl=63 (request in 27) |
| 31 | 17.333125948 | 192.168.0.11 | 192.168.0.5 | ICMP | 60 | Echo (ping) reply id=0x5615, seq=768/3, ttl=63 (request in 30) |
| 36 | 18.333225041 | 192.168.0.11 | 192.168.0.5 | ICMP | 60 | Echo (ping) reply id=0x5615, seq=1024/4, ttl=63 (request in 35) |

**External test Case# 4**
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

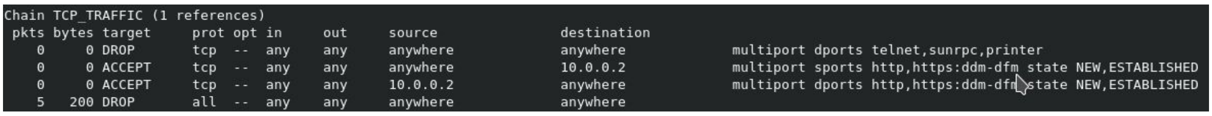
external computer -> firewall host
**Detail**: External computer probes firewall host with 5 TCP, 5 UDP and 5 ICMP packets got no response. A total of 15 packets should show up in each of the **TCP_TRAFFIC, UDP_TRAFFIC** and **ICMP_TRAFFIC** chains that go to **DROP** (15 packets dropped in total). The wireshark captures on the internal host shows that 5 incoming traffic (port 17 to port 17) was received from the network.

(hping3 output on external computer)

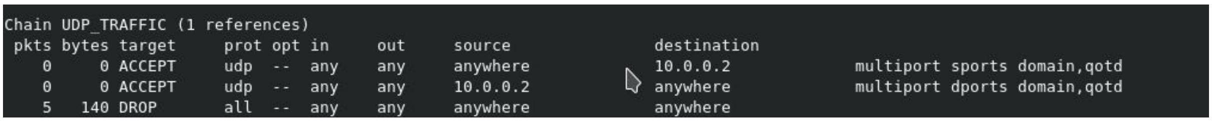


```
##########################################################################
#    »     »     »     »     »     »     »    Case 4»  »     »     »     »     »  »    »     »    #
##########################################################################

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enol 192.168.0.11): S set, 40 headers + 0 data bytes

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enol 192.168.0.11): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enol 192.168.0.11): icmp mode set, 28 headers + 0 data bytes
```

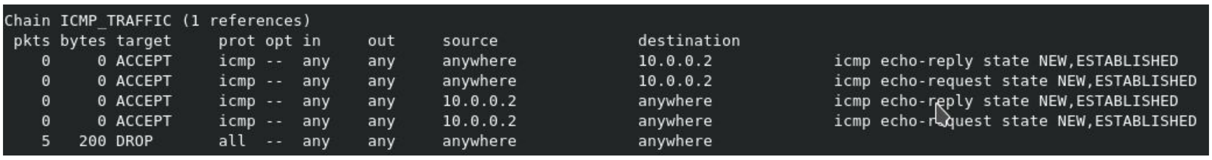
(iptable listing on firewall host)



```
Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             multiport dports telnet,sunrpc,printer
    0     0 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2             multiport sports http,https:ddm-dfm state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere             multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
    5   200 DROP       all  --  any    any     anywhere             anywhere
```



```
Chain UDP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  any    any     anywhere             10.0.0.2             multiport sports domain,qotd
    0     0 ACCEPT     udp  --  any    any     10.0.0.2             anywhere             multiport dports domain,qotd
    5   140 DROP       all  --  any    any     anywhere             anywhere
```



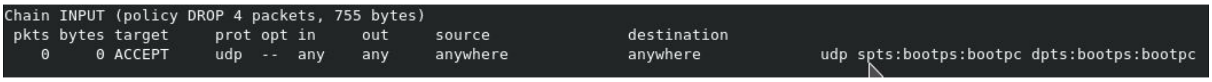
```
Chain ICMP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     anywhere             10.0.0.2             icmp echo-request state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-reply state NEW,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     10.0.0.2             anywhere             icmp echo-request state NEW,ESTABLISHED
    5   200 DROP       all  --  any    any     anywhere             anywhere
```

## External test Case# 5

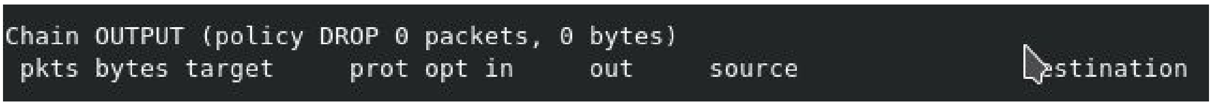
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

**Detail**: All packets destined for firewall host will be pre routed to internal host. By default, the input and output chain are set to **DROP**.

(iptable listing on firewall host)



```
Chain INPUT (policy DROP 4 packets, 755 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spts:bootps:bootpc dpts:bootps:bootpc
```



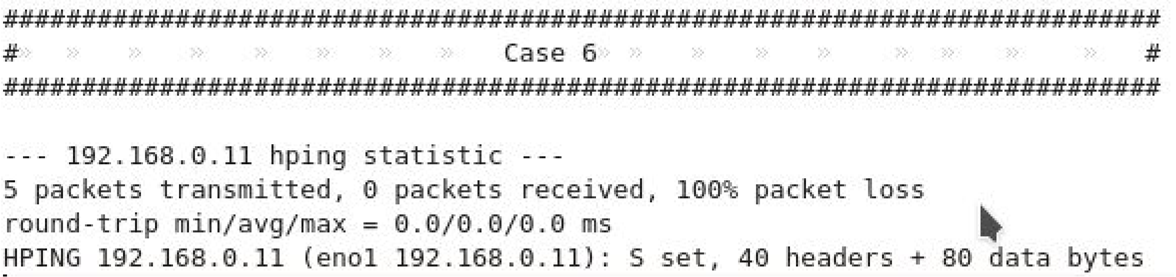
```
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

## External test Case# 6

firewall host ip: 192.168.0.11
external computer ip: 10.0.0.3 (spoof)
internal host ip: 10.0.0.2

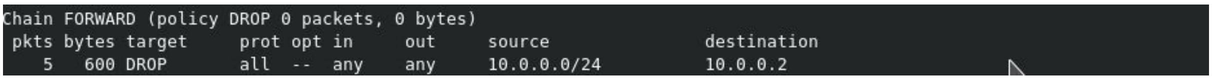
external computer -> firewall host
**Detail**: External computer probes firewall host with TCP packets five times. A total of 5 packets should show up **FORWARD** chain that go to **DROP**.

(hping3 output on external computer)



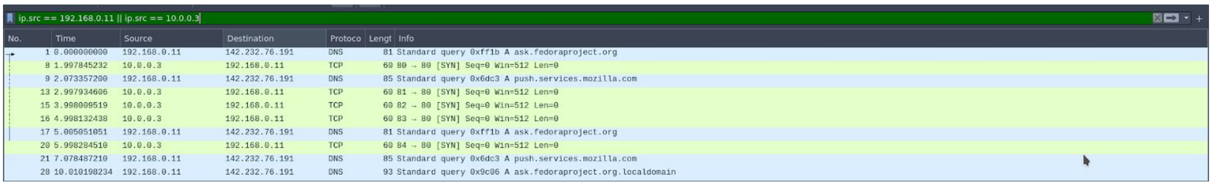
```
##########################################################################
#                                 Case 6                                 #
##########################################################################

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (eno1 192.168.0.11): S set, 40 headers + 80 data bytes
```

(iptable listing on firewall host)



```
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    5   600 DROP       all  --  any    any     10.0.0.0/24          10.0.0.2
```

(wireshark capture on internal host)



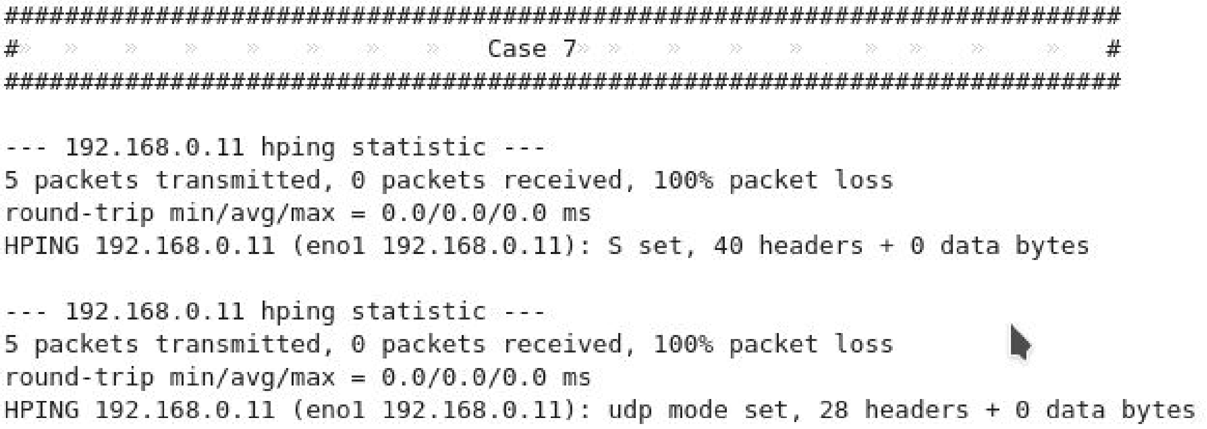
ip.src == 192.168.0.11 || ip.src == 10.0.0.3

| No. | Time | Source | Destination | Protoco | Lengt | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 192.168.0.11 | 142.232.76.191 | DNS | 81 | Standard query 0xff1b A ask.fedoraproject.org |
| 8 | 1.997845232 | 10.0.0.3 | 192.168.0.11 | TCP | 60 | 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 9 | 2.073357200 | 192.168.0.11 | 142.232.76.191 | DNS | 85 | Standard query 0x6dc3 A push.services.mozilla.com |
| 13 | 2.997934606 | 10.0.0.3 | 192.168.0.11 | TCP | 60 | 81 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 15 | 3.998009519 | 10.0.0.3 | 192.168.0.11 | TCP | 60 | 82 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 16 | 4.998132438 | 10.0.0.3 | 192.168.0.11 | TCP | 60 | 83 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 17 | 5.005051051 | 192.168.0.11 | 142.232.76.191 | DNS | 81 | Standard query 0xff1b A ask.fedoraproject.org |
| 20 | 5.998284510 | 10.0.0.3 | 192.168.0.11 | TCP | 60 | 84 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 21 | 7.078487210 | 192.168.0.11 | 142.232.76.191 | DNS | 85 | Standard query 0x6dc3 A push.services.mozilla.com |
| 28 | 10.010198234 | 192.168.0.11 | 142.232.76.191 | DNS | 93 | Standard query 0x9c06 A ask.fedoraproject.org.localdomain |

**External test Case# 7**

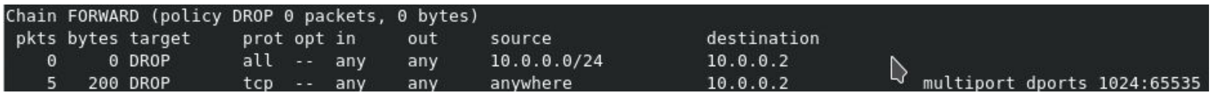
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

external computer -> firewall host
**Detail**: External computer probes firewall host with 5 TCP packets and 5 UDP packets with high source port. A total of 10 packets should show up **FORWARD** chain that go to **DROP**.
(hping3 output on external computer)

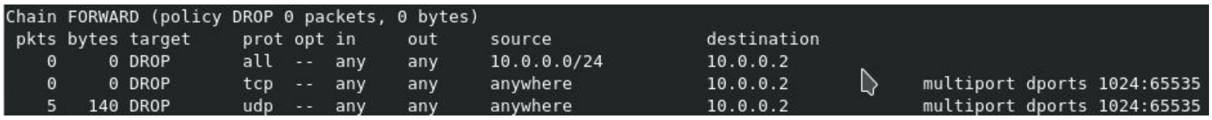


```
##########################################################################
#                                      Case 7                            #
##########################################################################

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (eno1 192.168.0.11): S set, 40 headers + 0 data bytes

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (eno1 192.168.0.11): udp mode set, 28 headers + 0 data bytes
```

(iptable listing on firewall host)

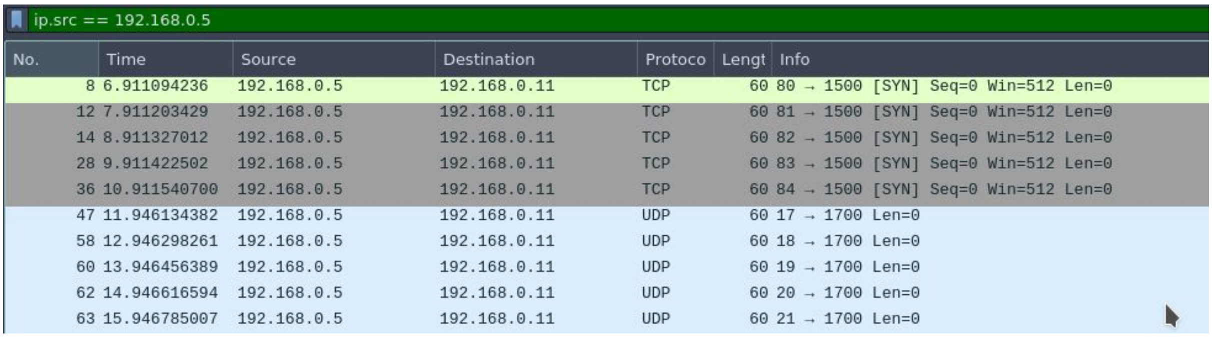


```
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  any    any     10.0.0.0/24          10.0.0.2
    5   200 DROP       tcp  --  any    any     anywhere             10.0.0.2             multiport dports 1024:65535
```



```
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  any    any     10.0.0.0/24          10.0.0.2
    0     0 DROP       tcp  --  any    any     anywhere             10.0.0.2             multiport dports 1024:65535
    5   140 DROP       udp  --  any    any     anywhere             10.0.0.2             multiport dports 1024:65535
```

(wireshark on firewall host)



ip.src == 192.168.0.5

| No. | Time | Source | Destination | Protoco | Lengt | Info |
|---|---|---|---|---|---|---|
| 8 | 6.911094236 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | 80 → 1500 [SYN] Seq=0 Win=512 Len=0 |
| 12 | 7.911203429 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | 81 → 1500 [SYN] Seq=0 Win=512 Len=0 |
| 14 | 8.911327012 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | 82 → 1500 [SYN] Seq=0 Win=512 Len=0 |
| 28 | 9.911422502 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | 83 → 1500 [SYN] Seq=0 Win=512 Len=0 |
| 36 | 10.911540700 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | 84 → 1500 [SYN] Seq=0 Win=512 Len=0 |
| 47 | 11.946134382 | 192.168.0.5 | 192.168.0.11 | UDP | 60 | 17 → 1700 Len=0 |
| 58 | 12.946298261 | 192.168.0.5 | 192.168.0.11 | UDP | 60 | 18 → 1700 Len=0 |
| 60 | 13.946456389 | 192.168.0.5 | 192.168.0.11 | UDP | 60 | 19 → 1700 Len=0 |
| 62 | 14.946616594 | 192.168.0.5 | 192.168.0.11 | UDP | 60 | 20 → 1700 Len=0 |
| 63 | 15.946785007 | 192.168.0.5 | 192.168.0.11 | UDP | 60 | 21 → 1700 Len=0 |

**External test Case# 8**

firewall host ip: 192.168.0.11

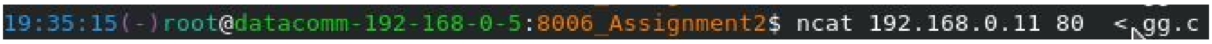
external computer ip: 192.168.0.5

internal host ip: 10.0.0.2

external computer -> firewall host

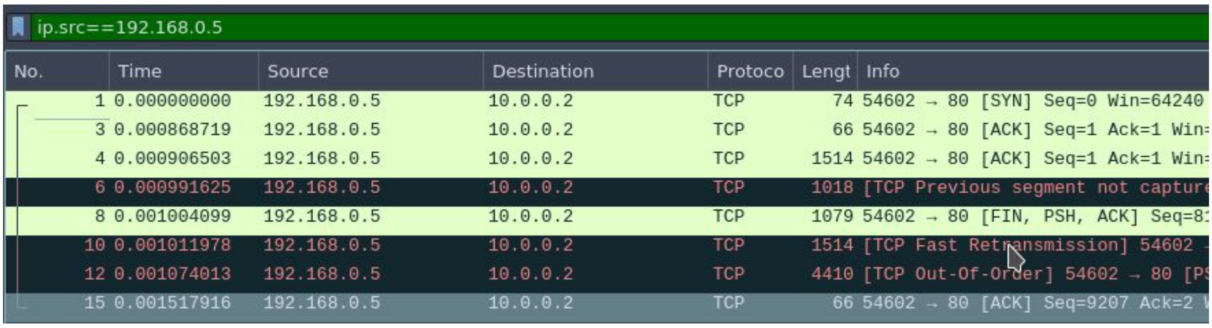
**Detail**: While the internal host is listening for incoming ncat request, the external computer ran ncat to transfer a text file to internal host. The wireshark below shows that after the connection was established, the external computer continued to send packets over to the internal host.

(ncat command line output)



```
19:35:15(-)root@datacomm-192-168-0-5:8006_Assignment2$ ncat 192.168.0.11 80  < gg.c
```

(wireshark capture on internal host)



ip.src==192.168.0.5

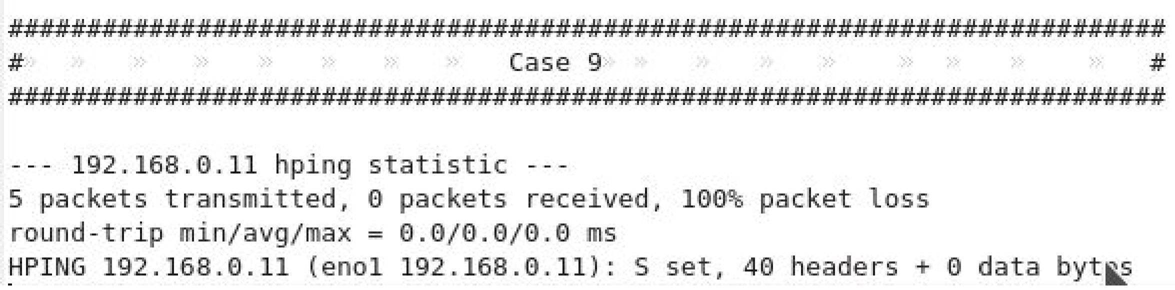
| No. | Time | Source | Destination | Protoco | Lengt | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 192.168.0.5 | 10.0.0.2 | TCP | 74 | 54602 → 80 [SYN] Seq=0 Win=64240 |
| 3 | 0.000868719 | 192.168.0.5 | 10.0.0.2 | TCP | 66 | 54602 → 80 [ACK] Seq=1 Ack=1 Win= |
| 4 | 0.000906503 | 192.168.0.5 | 10.0.0.2 | TCP | 1514 | 54602 → 80 [ACK] Seq=1 Ack=1 Win= |
| 6 | 0.000991625 | 192.168.0.5 | 10.0.0.2 | TCP | 1018 | [TCP Previous segment not capture |
| 8 | 0.001004099 | 192.168.0.5 | 10.0.0.2 | TCP | 1079 | 54602 → 80 [FIN, PSH, ACK] Seq=8 |
| 10 | 0.001011978 | 192.168.0.5 | 10.0.0.2 | TCP | 1514 | [TCP Fast Retransmission] 54602 |
| 12 | 0.001074013 | 192.168.0.5 | 10.0.0.2 | TCP | 4410 | [TCP Out-Of-Order] 54602 → 80 [P |
| 15 | 0.001517916 | 192.168.0.5 | 10.0.0.2 | TCP | 66 | 54602 → 80 [ACK] Seq=9207 Ack=2 |

### External test Case# 9

firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

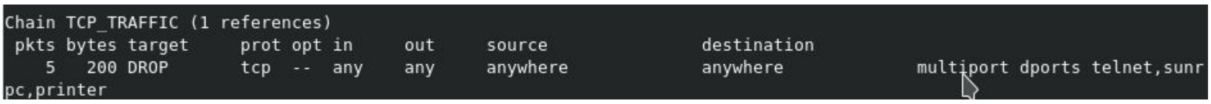
external computer -> firewall host
**Detail**: External computer probes firewall host with telnet packets five times. A total of 5 packets should show up in the TCP_TRAFFIC chain that go to **DROP**. The wireshark captures on the firewall host shows that 5 incoming traffic (port 23 to port 23) was received from the network

(hping3 output on external computer)



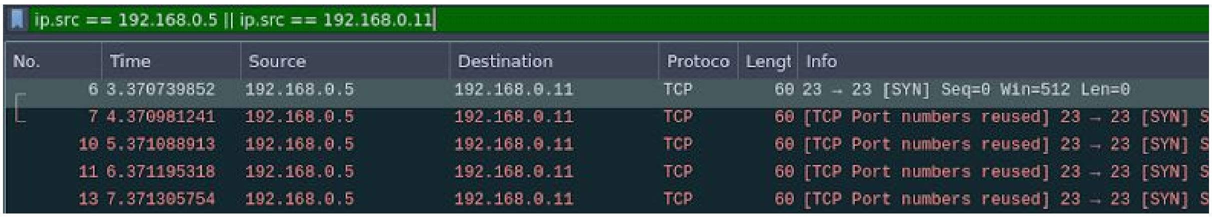
```
############################################################################
#»   »   »   »   »   »   »   »   Case 9»  »   »   »   »   »   »   »   #
############################################################################

--- 192.168.0.11 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (eno1 192.168.0.11): S set, 40 headers + 0 data bytes
```

(iptable listing on firewall host)



```
Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination         
    5   200 DROP       tcp  --  any    any     anywhere             anywhere             multiport dports telnet,sunr
pc,printer
```

(wireshark capture on firewall host)



ip.src == 192.168.0.5 || ip.src == 192.168.0.11

| No. | Time | Source | Destination | Protoco | Lengt | Info |
|---|---|---|---|---|---|---|
| 6 | 3.370739852 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | 23 → 23 [SYN] Seq=0 Win=512 Len=0 |
| 7 | 4.370981241 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | [TCP Port numbers reused] 23 → 23 [SYN] S |
| 10 | 5.371088913 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | [TCP Port numbers reused] 23 → 23 [SYN] S |
| 11 | 6.371195318 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | [TCP Port numbers reused] 23 → 23 [SYN] S |
| 13 | 7.371305754 | 192.168.0.5 | 192.168.0.11 | TCP | 60 | [TCP Port numbers reused] 23 → 23 [SYN] S |

**External test Case# 10**

firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

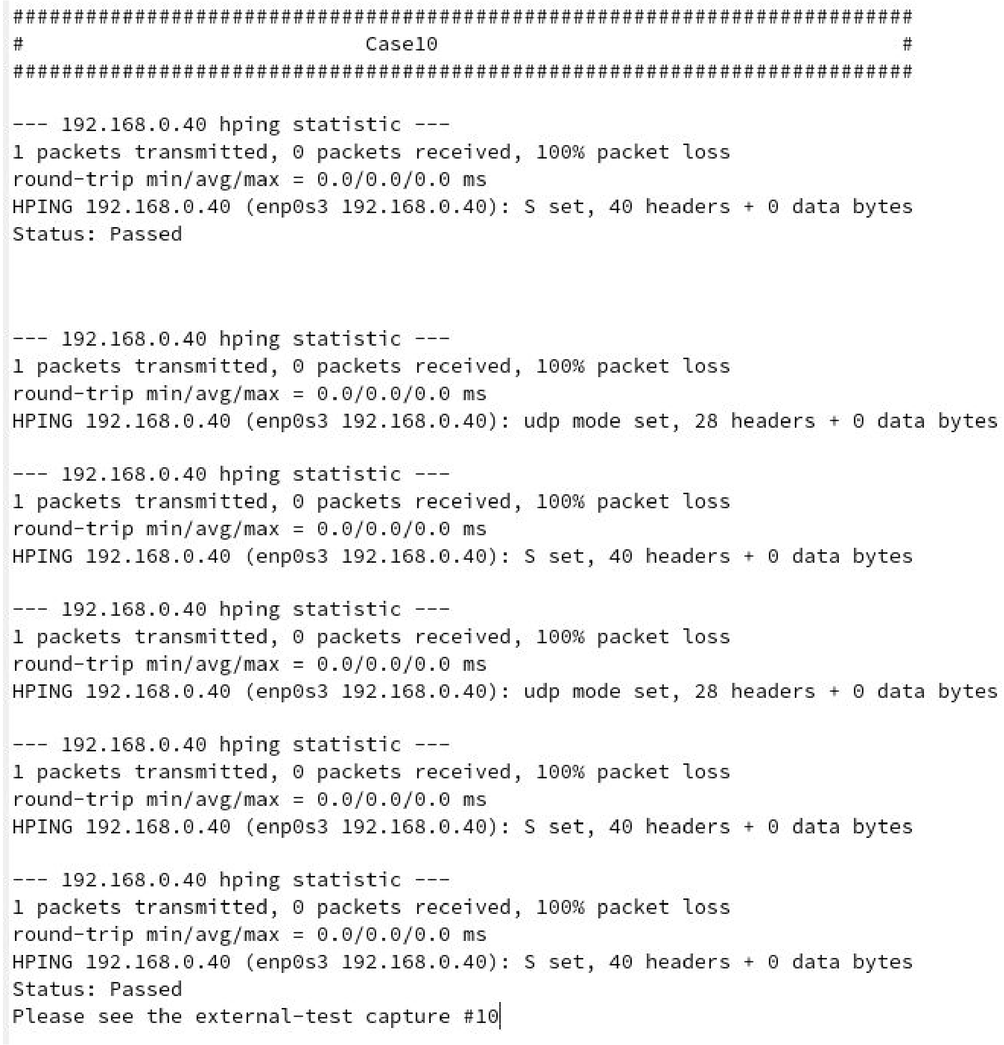
external computer -> firewall host

**Detail**: External computer probes firewall host

- with 2 TCP with port 111 and 515 packets.
- 3 TCP with port 137, 138, 139
- 3 UDP with port 147, 138, 139
- 8 UDP packets with port range from 32768 - 32775

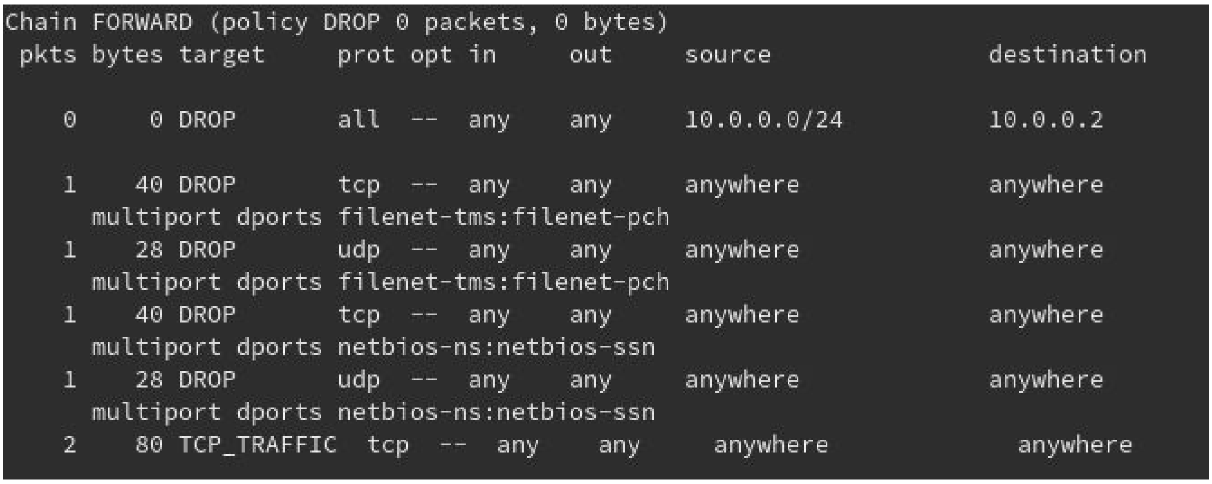
A total of 16 packets should show up in the **TCP_TRAFFIC** and **FORWARD** chain that go to **DROP**. The wireshark captures on the firewall host shows that 16 incoming traffic was received from the network (2 packets from port 80 - 111 and port 80 - 515, 6 packets from 137 - 139 and 8 packets from port 80 - 32768~32775)

(hping3 output on external computer)



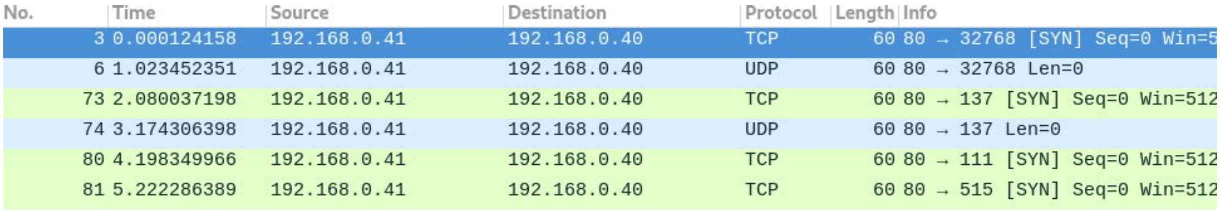
```
##########################################################################
#                             Case10                                     #
##########################################################################

--- 192.168.0.40 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): S set, 40 headers + 0 data bytes
Status: Passed



--- 192.168.0.40 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.40 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): S set, 40 headers + 0 data bytes

--- 192.168.0.40 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.40 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): S set, 40 headers + 0 data bytes

--- 192.168.0.40 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): S set, 40 headers + 0 data bytes
Status: Passed
Please see the external-test capture #10
```

(iptable listing on firewall host)



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

    0     0 DROP       all  --  any    any     10.0.0.0/24          10.0.0.2

    1    40 DROP       tcp  --  any    any     anywhere             anywhere
      multiport dports filenet-tms:filenet-pch
    1    28 DROP       udp  --  any    any     anywhere             anywhere
      multiport dports filenet-tms:filenet-pch
    1    40 DROP       tcp  --  any    any     anywhere             anywhere
      multiport dports netbios-ns:netbios-ssn
    1    28 DROP       udp  --  any    any     anywhere             anywhere
      multiport dports netbios-ns:netbios-ssn
    2    80 TCP_TRAFFIC  tcp  --  any    any     anywhere             anywhere
```

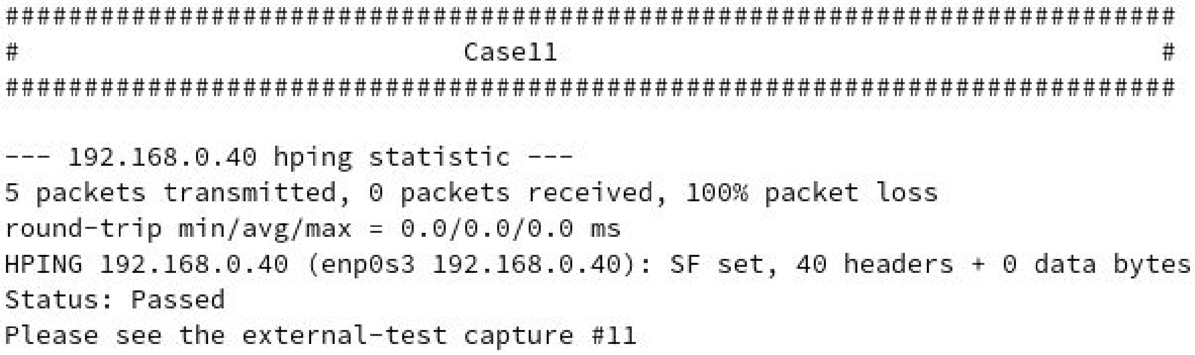
(wireshark capture on internal host)



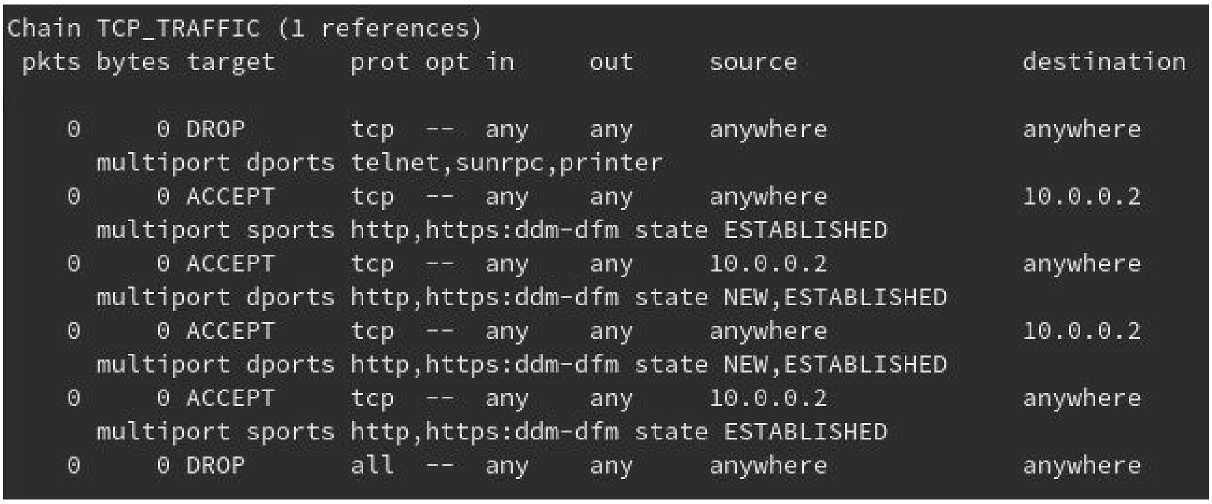
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 0.000124158 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 80 → 32768 [SYN] Seq=0 Win=5 |
| 6 | 1.023452351 | 192.168.0.41 | 192.168.0.40 | UDP | 60 | 80 → 32768 Len=0 |
| 73 | 2.080037198 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 80 → 137 [SYN] Seq=0 Win=512 |
| 74 | 3.174306398 | 192.168.0.41 | 192.168.0.40 | UDP | 60 | 80 → 137 Len=0 |
| 80 | 4.198349966 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 80 → 111 [SYN] Seq=0 Win=512 |
| 81 | 5.222286389 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 80 → 515 [SYN] Seq=0 Win=512 |

**External test Case# 11**
firewall host ip: 192.168.0.11
external computer ip: 192.168.0.5
internal host ip: 10.0.0.2

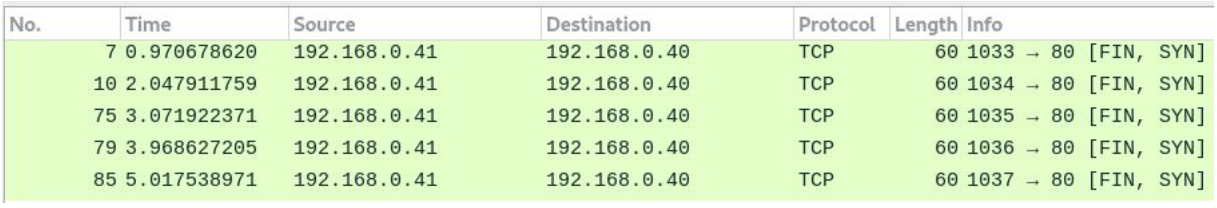
external computer -> firewall host
**Detail**: External computer probes firewall host with 5 TCP packets that have both SIN and FIN bit set. The iptable listing shows that the traffic neither accepted or dropped in **TCP_TRAFFIC** chain. The wireshark capture on the firewall host confirmed that those SIN\FIN packets indeed hit the firewall.



```
##########################################################################
#                            Case11                                      #
##########################################################################

--- 192.168.0.40 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.40 (enp0s3 192.168.0.40): SF set, 40 headers + 0 data bytes
Status: Passed
Please see the external-test capture #11
```



```
Chain TCP_TRAFFIC (1 references)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       tcp  --  any    any     anywhere             anywhere
      multiport dports telnet,sunrpc,printer
    0     0 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2
      multiport sports http,https:ddm-dfm state ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere
      multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     anywhere             10.0.0.2
      multiport dports http,https:ddm-dfm state NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.0.0.2             anywhere
      multiport sports http,https:ddm-dfm state ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere
```



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 7 | 0.970678620 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 1033 → 80 [FIN, SYN] |
| 10 | 2.047911759 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 1034 → 80 [FIN, SYN] |
| 75 | 3.071922371 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 1035 → 80 [FIN, SYN] |
| 79 | 3.968627205 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 1036 → 80 [FIN, SYN] |
| 85 | 5.017538971 | 192.168.0.41 | 192.168.0.40 | TCP | 60 | 1037 → 80 [FIN, SYN] |