COMP 8006
Assignment 2

Chris Hunter A00833669

Geoff Dabu A00817395

Document Contents

Disk Contents

- firewall.sh
- internalTestScript.rb
- externalTestScript.rb
- Packet Captures
  - ...
- Documentation
  - readme.txt
  - documentation.pdf

Summary

The purpose of this assignment was to create a stand-alone linux firewall with specified rules. Six user defined chains were created; tcpIN, tcpOUT, udpIN, udpOUT, icmpIN, icmpOUT. These chains are used to track packets in and out of ports specified by the user. Each track only tcp, udp, or icmp. These chains are attached to the FORWARD chain. Fragmented packets are passed through the FORWARD chain.

The chains PREROUTING and POSTROUTING were used to transfer packets from the public interface to the internal network, or vice versa.

The user has the option to change the name and location of the utility, IP addresses and interfaces for both internal and external devices, services allowed for TCP, UDP, and ICMP.

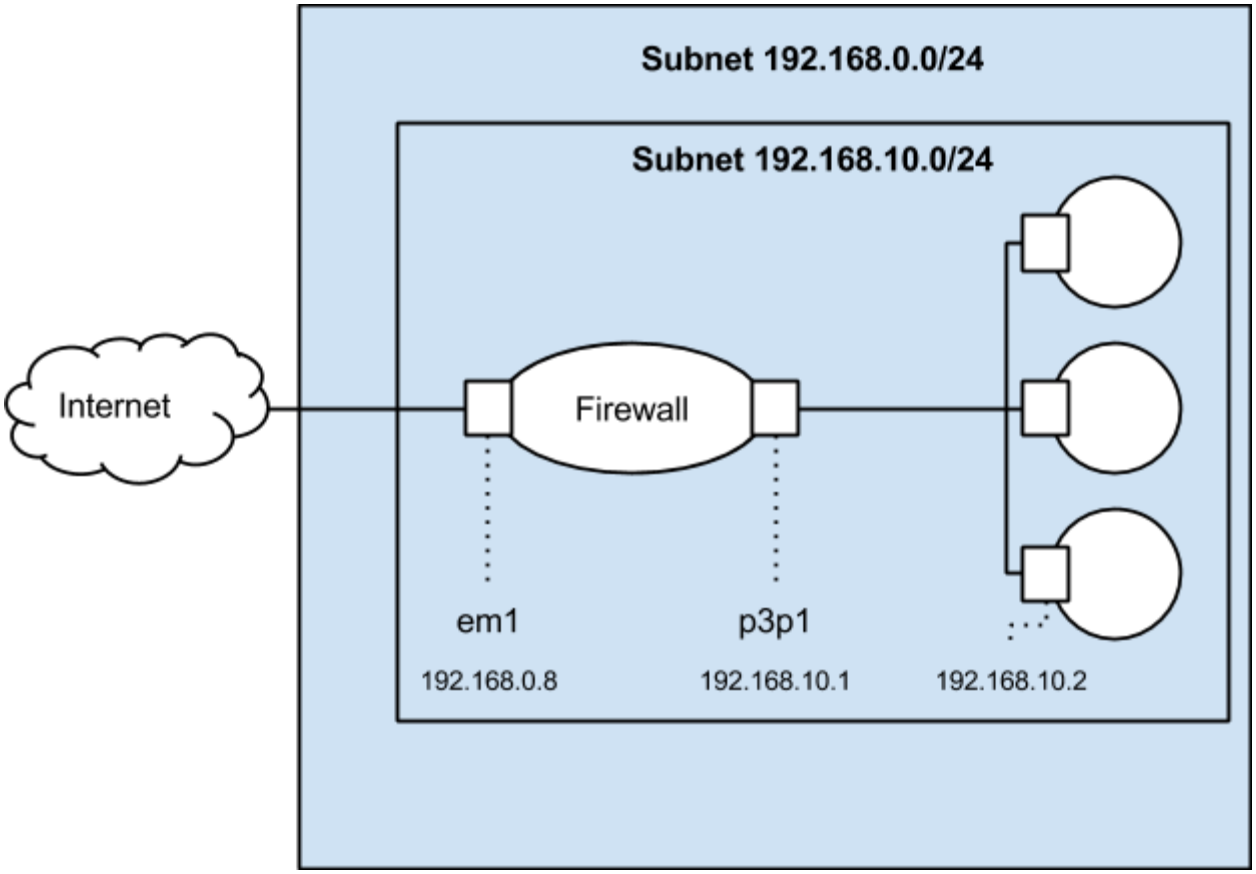
Two test scripts were created; one for internal(outbound) tests, and one for external(inbound tests). These test scripts create a log file where the user can easily read the desired and actual results.

The iptable created is as follows:

```
Chain INPUT (policy ACCEPT 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 tcpIN      tcp  --  any    any     anywhere             anywhere
    0     0 tcpOUT     tcp  --  any    any     anywhere             anywhere
    0     0 udpIN      tcp  --  any    any     anywhere             anywhere
    0     0 udpOUT     tcp  --  any    any     anywhere             anywhere
    0     0 icmpIN     tcp  --  any    any     anywhere             anywhere
    0     0 icmpOUT    tcp  --  any    any     anywhere             anywhere
    0     0 ACCEPT     all  -f  any    any     anywhere             anywhere

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

```
Chain icmpIN (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  em1    p3p1    anywhere             anywhere             icmp echo-request

Chain icmpOUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  p3p1   em1     anywhere             anywhere             icmp echo-request

Chain tcpIN (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  em1    p3p1    192.168.10.0/24      anywhere
    0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp dpts:!0:1024 flags:FIN,SYN,RST,ACK/SYN
    0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp flags:FIN,SYN/FIN,SYN
    0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp spt:telnet
    0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             multiport dports filenet-tms:filenet-pch,netbios-ns:netbios-ssn,sunrpc,sftp
    0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             state NEW tcp spts:0:1023 multiport dports domain,bootps,bootpc,http,https
    0     0 ACCEPT     tcp  --  em1    p3p1    anywhere             anywhere             state NEW,ESTABLISHED multiport dports domain,bootps,bootpc,http,https
    0     0 ACCEPT     tcp  --  em1    p3p1    anywhere             anywhere             state NEW,ESTABLISHED multiport sports domain,bootps,bootpc,http,https

Chain tcpOUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  p3p1   em1     anywhere             anywhere             tcp dpt:telnet
    0     0 DROP       tcp  --  p3p1   em1     anywhere             anywhere             tcp spt:telnet
    0     0 ACCEPT     tcp  --  p3p1   em1     anywhere             anywhere             multiport dports domain,bootps,bootpc,http,https
    0     0 ACCEPT     tcp  --  p3p1   em1     anywhere             anywhere             multiport sports domain,bootps,bootpc,http,https

Chain udpIN (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       udp  --  em1    p3p1    anywhere             anywhere             udp spts:0:1023 multiport dports domain,bootps,bootpc,http,https
    0     0 ACCEPT     udp  --  em1    p3p1    anywhere             anywhere             multiport dports domain,bootps,bootpc,http,https
    0     0 ACCEPT     udp  --  em1    p3p1    anywhere             anywhere             multiport sports domain,bootps,bootpc,http,https

Chain udpOUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  p3p1   em1     anywhere             anywhere             multiport dports domain,bootps,bootpc,http,https
    0     0 ACCEPT     udp  --  p3p1   em1     anywhere             anywhere             multiport sports domain,bootps,bootpc,http,https
[root@DataComm ~]#
```

Network Architecture



Testing & Results

Test Procedure

2 tests scripts were created, one for internal testing(outbound traffic), one for external testing(inbound traffic). The test files were written in ruby. They create a log file which offers the reader the ability to understand which tests should receive acks back and which will not.

The user has the ability to change the ports and ip addresses being tested.

Shown below are the test results from this experiment. For every test case the corresponding hping command, expected results and actual results have been listed. Also, to validate our test cases, screenshots of the iptables and wireshark packet captures have been included as well. This document only includes the screenshots of the wireshark packet captures, but the wireshark .pcapng files have been included as well on the disk.

Constaints

Test Case	Description	Hping Command	Expected Results	Actual Results
TCP				
1a	Permit **inbound** TCP packets (ports 22, 53, 80)	hping 192.168.0.15 -S -s 2000 -p 22 -c 20 -i u500	20 Ack backs	Success, 20 Ack backs
1b	Permit **outbound** TCP packets (ports 22, 53, 80)	hping3 192.168.0.22 -S -s 2000 -p 22 -c 20 -i u500	20 Ack backs	Success, 20 Ack backs
Test Screenshots				

1a

Before Hping Packet Craft (tcpIN CHAIN):

```
0    0 ACCEPT    tcp  --  em1   p3p1   anywhere         anywhere         state NEW,ESTABLISHED multiport dports ssh,domain,bootps,bootpc,http,https
```

Hping Packet Craft (from Host B):

```
[root@DataComm ~]# hping3 192.168.0.23 -S -c 5 -k -p 50
HPING 192.168.0.23 (em1 192.168.0.23): S set, 40 headers + 0 data bytes

--- 192.168.0.23 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@DataComm ~]# hping 192.168.0.15 -S -s 2000 -p 22 -c 20 -i u500
HPING 192.168.0.15 (em1 192.168.0.15): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=1.6 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=1.5 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=5 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=6 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=7 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=8 win=29200 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=9 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=10 win=29200 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=11 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=12 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=13 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=14 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=15 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=16 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=17 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=18 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.15 ttl=63 DF id=0 sport=22 flags=SA seq=19 win=29200 rtt=1.1 ms

--- 192.168.0.15 hping statistic ---
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.9/1.6 ms
```

After Hping Packet Craft (tcpIN CHAIN):

```
40  1600 ACCEPT    tcp  --  em1   p3p1   anywhere         anywhere         state NEW,ESTABLISHED multiport dports ssh,domain,bootps,bootpc,http,https
```

1b

Before Hping Packet Craft (tcpOut CHAIN):

```
 0     0 ACCEPT     tcp  --  p3p1   em1     anywhere            anywhere            multiport sports ssh,domain,bootps,bootpc,http,https
```

Hping Packet Craft (from Host A):

```
round trip min/avg/max = 3.6/7.6/12.2 ms
[root@DataComm ~]# hping3 192.168.0.22 -S -s 2000 -p 22 -c 20 -i u500
HPING 192.168.0.22 (p3p1 192.168.0.22): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=1.5 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=1.5 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=5 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=6 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=7 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=8 win=29200 rtt=0.5 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=9 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=10 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=11 win=29200 rtt=0.9 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=12 win=29200 rtt=1.4 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=13 win=29200 rtt=0.9 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=14 win=29200 rtt=1.4 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=15 win=29200 rtt=0.8 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=16 win=29200 rtt=1.4 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=17 win=29200 rtt=0.9 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=18 win=29200 rtt=1.6 ms
len=46 ip=192.168.0.22 ttl=63 DF id=0 sport=22 flags=SA seq=19 win=29200 rtt=1.1 ms
```

After Hping Packet Craft (tcpOUT CHAIN):

```
 41  1652 ACCEPT     tcp  --  p3p1   em1     anywhere            anywhere            multiport dports ssh,domain,bootps,bootpc,http,https
```

Packet Capture

10	2.675251000	192.168.0.20	192.168.0.17	TCP	60 http > cisco-sccp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	2.675338000	192.168.0.17	192.168.0.20	TCP	54 dc > http [SYN] Seq=0 Win=512 Len=0
12	2.675603000	192.168.0.20	192.168.0.17	TCP	60 http > dc [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	2.675867000	192.168.0.17	192.168.0.20	TCP	54 globe > http [SYN] Seq=0 Win=512 Len=0
14	2.676176000	192.168.0.20	192.168.0.17	TCP	60 http > globe [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	2.676400000	192.168.0.17	192.168.0.20	TCP	54 brutus > http [SYN] Seq=0 Win=512 Len=0
16	2.676668000	192.168.0.20	192.168.0.17	TCP	60 http > brutus [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	2.676930000	192.168.0.17	192.168.0.20	TCP	54 mailbox > http [SYN] Seq=0 Win=512 Len=0
18	2.677217000	192.168.0.20	192.168.0.17	TCP	60 http > mailbox [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	2.677446000	192.168.0.17	192.168.0.20	TCP	54 berknet > http [SYN] Seq=0 Win=512 Len=0
20	2.677726000	192.168.0.20	192.168.0.17	TCP	60 http > berknet [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	2.677966000	192.168.0.17	192.168.0.20	TCP	54 invokator > http [SYN] Seq=0 Win=512 Len=0
22	2.678200000	192.168.0.20	192.168.0.17	TCP	60 http > invokator [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	2.678495000	192.168.0.17	192.168.0.20	TCP	54 dectalk > http [SYN] Seq=0 Win=512 Len=0
24	2.678825000	192.168.0.20	192.168.0.17	TCP	60 http > dectalk [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

This packet capture was taken from the external machine. For this scenario, packets were sent to 192.168.0.20 port 22. Port 22 is an allowed port and the packet capture illustrates that packets were successfully coming back after reaching the inner host machine.

Test Case	Description	Hping Command	Expected Results	Actual Results
UDP				
2 A	Permit **inbound** UDP packets (ports 22, 53, 80)	hping 192.168.0.15 --udp -s 2000 -k -p 22-c 20 -i u500	iptables show transmission, no ack backs	Success
2 B	Permit **outbound** UDP packets (ports 22, 53, 80)	hping3 192.168.0.22 --udp -s 2000 -k -p 22-c 20 -i u500	iptables show transmission, no ack backs	Success

Test Screenshots

2 A

Before Hping Packet Craft (udpIN CHAIN):

```
0     0 ACCEPT     udp  --  em1    p3p1    anywhere            anywhere            multiport dports ssh,domain,bootps,http,https
```

Hping Packet Craft (from Host B):

```
[root@DataComm ~]# hping 192.168.0.15 --udp -s 2000 -p 22 -c 20 -i u5000
HPING 192.168.0.15 (em1 192.168.0.15): udp mode set, 28 headers + 0 data bytes

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

After Hping Packet Craft (udpIN CHAIN):

```
20   560 ACCEPT     udp  --  em1    p3p1    anywhere            anywhere            multiport dports ssh
```

2 B

Before Hping Packet Craft (udpOUT CHAIN):

```
0     0 ACCEPT     udp  --  p3p1   em1     anywhere            anywhere            multiport dports ssh
0     0 ACCEPT     udp  --  p3p1   em1     anywhere            anywhere            multiport sports ssh
```

Hping Packet Craft (from Host A):

```
[root@DataComm ~]# hping 192.168.0.22 --udp -s 2000 -k -p 22 -c 20 -i u500
HPING 192.168.0.22 (p3p1 192.168.0.22): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.22 hping statistic ---
20 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@DataComm ~]#
```

After Hping Packet Craft (udpOUT CHAIN):

```
20   560 ACCEPT     udp  --  p3p1   em1     anywhere            anywhere            multiport dports ssh
 0     0 ACCEPT     udp  --  p3p1   em1     anywhere            anywhere            multiport sports ssh
```

Packet Capture

462	30.951020000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
463	30.951568000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
464	30.952107000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
465	30.952637000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
466	30.953174000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
467	30.953743000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
468	30.954305000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
469	30.954837000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
470	30.955400000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
471	30.955933000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
472	30.956494000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
473	30.957037000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
474	30.957592000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
475	30.958135000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
476	30.958688000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
477	30.959246000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh
478	30.959791000	192.168.0.17	192.168.0.20	UDP	42	Source port: cisco-sccp Destination port: ssh

This packet capture was taken from the external machine. For this scenario, packets were sent to 192.168.0.20 port 22 (udp).

Test Case	Description	Hping Command	Expected Results	Actual Results
ICMP				
3 A	Permit **inbound** ICMP packets (type 8)	hping 192.168.0.15 --icmpcode 8 -c 20 -i u500	iptables show transmission, no ack backs	Success
3 B	Permit **outbound** ICMP packets (type 8)	hping3 192.168.0.22 --icmpcode 8 -c 20 -i u500	iptables show transmission, no ack backs	Success
Test Screenshots				

3 A	**Before Hping Packet Craft (icmpIN CHAIN):**
	`0 0 ACCEPT icmp -- em1 p3p1 anywhere anywhere`
	Hping Packet Craft (from Host B):
	`[root@DataComm ~]# hping 192.168.0.15 --icmpcode 8 -c 20 -i u500`
	`HPING 192.168.0.15 (em1 192.168.0.15): icmp mode set, 28 headers + 0 data bytes`
	
	`--- 192.168.0.15 hping statistic ---`
	`20 packets transmitted, 0 packets received, 100% packet loss`
	`round-trip min/avg/max = 0.0/0.0/0.0 ms`
	`[root@DataComm ~]#`
	
	After Hping Packet Craft (icmpIN CHAIN):
	`20 560 ACCEPT icmp -- em1 p3p1 anywhere anywhere icmp echo-request`			

3 B	**Before Hping Packet Craft (icmpOUT CHAIN):** `0 0 ACCEPT icmp -- p3p1 em1 anywhere anywhere`			

Hping Packet Craft (from Host A):

```
[root@DataComm ~]# hping3 192.168.0.22 --icmpcode 8 -c 20 -i u500
HPING 192.168.0.22 (p3p1 192.168.0.22): icmp mode set, 28 headers + 0 data bytes

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

After Hping Packet Craft (icmpOUT CHAIN):

```
 20   560 ACCEPT     icmp --  p3p1   em1     anywhere             anywhere
```

Packet Capture

11	2.733343000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=768/3, ttl=64
12	2.733880000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=1024/4, ttl=64
13	2.734432000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=1280/5, ttl=64
14	2.734969000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=1536/6, ttl=64
15	2.735502000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=1792/7, ttl=64
16	2.736061000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=2048/8, ttl=64
17	2.736593000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=2304/9, ttl=64
18	2.737152000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=2560/10, ttl=64
19	2.737683000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=2816/11, ttl=64
20	2.738242000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=3072/12, ttl=64
21	2.738777000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=3328/13, ttl=64
22	2.739337000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=3584/14, ttl=64
23	2.739894000	192.168.0.17	192.168.0.20	ICMP	42	Echo (ping) request id=0x5f0c, seq=3840/15, ttl=64

This packet capture was taken from the external machine. For this scenario, packets were sent to 192.168.0.20 port 22 (icmp).

Test Case	Description	Command	Expected Results	Actual Results
Specific Drop Rules				
4 A	Default to drop packets	hping 192.168.0.15 -s 2000 -k -S -p 900 -c 20 -i u500	iptables drop packets, no ack backs	Success, packets dropped by policy
4 B	Drop all packets destined for the firewall host from outside	Passive inbound packets	iptables drop packet	Success, packets dropped on INPUT policy
4 C	Drop packets with internal source address,	hping 192.168.0.15 -a 192.168.10.2 -s 2000 -k -S -p 80 -c 20 -i u500	iptables drop packets, no ack backs	Success, packets were

	coming from outside the network			dropped by the firewall
4 D	Drop incoming SYN packets with destination port > 1024	hping 192.168.0.15 -s 2000 -k -S -p 2222 -c 20 -i u500	iptables drop packets, no ack backs	Success, packets dropped at rule
4 E	Drop packets with SYN & FIN	hping 192.168.0.24 -S -F -s 2000 -k -p 80 -c 20 -i u500	iptables drop packets, no ack backs	Success, packets dropped by the firewall
4 F	Drop telnet packets	hping 192.168.0.24 -S -s 2000 -k -p 23 -c 20 -i u500	iptables drop packets, no ack backs	Success, packets dropped at rule
4 G	Drop incoming packets coming to ports 111, 137, 138, 139, 32768-32775	hping 192.168.0.24 -S -s 2000 -k -p {111,137-139,32768-32775} -c 20 -i u500	iptables drop packets, no ack backs	Success, packets dropped at rule

Test Screenshots

4 A

Before Hping Packet Craft (FORWARD CHAIN):

```
Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

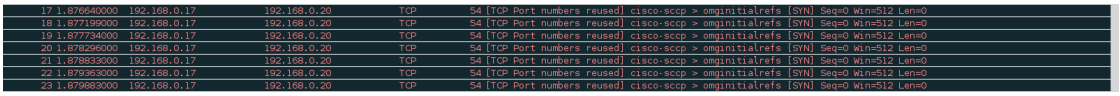
Hping Packet Craft (from Host B):

```
[root@DataComm ~]# hping 192.168.0.15 -s 2000 -k -S -p 900 -c 20 -i u500
HPING 192.168.0.15 (em1 192.168.0.15): S set, 40 headers + 0 data bytes

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

After Hping Packet Craft (FORWARD CHAIN):

```
Chain FORWARD (policy DROP 20 packets, 800 bytes)
```

Packet Capture



17	1.876640000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > omginitialrefs [SYN] Seq=0 Win=512 Len=0
18	1.877199000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > omginitialrefs [SYN] Seq=0 Win=512 Len=0
19	1.877734000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > omginitialrefs [SYN] Seq=0 Win=512 Len=0
20	1.878296000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > omginitialrefs [SYN] Seq=0 Win=512 Len=0
21	1.878833000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > omginitialrefs [SYN] Seq=0 Win=512 Len=0
22	1.879363000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > omginitialrefs [SYN] Seq=0 Win=512 Len=0
23	1.879883000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > omginitialrefs [SYN] Seq=0 Win=512 Len=0

This packet capture illustrates that packets were not being successfully ACKed and therefore not successfully reaching the host on the subnet.

4 B	**Before Hping Packet Craft (INPUT CHAIN):**
	`Chain INPUT (policy DROP 0 packets, 0 bytes)`
	
	After Hping Packet Craft (INPUT CHAIN):
	`Chain INPUT (policy DROP 42 packets, 4576 bytes)`

4 C	**Before Hping Packet Craft (tcpIN CHAIN):**
	`0 0 DROP all -- em1 p3p1 192.168.10.0/24 anywhere`
	Hping Packet Craft (from Host B):
	`[root@DataComm ~]# hping 192.168.0.15 -a 192.168.10.2 -s 2000 -k -S -p 80 -c 20 -i u500`
	`HPING 192.168.0.15 (em1 192.168.0.15): S set, 40 headers + 0 data bytes`
	
	`--- 192.168.0.15 hping statistic ---`
	`20 packets transmitted, 0 packets received, 100% packet loss`
	`round-trip min/avg/max = 0.0/0.0/0.0 ms`
	`[root@DataComm ~]#`
	
	After Hping Packet Craft (tcpIN CHAIN):
	`0 0 DROP all -- em1 p3p1 192.168.10.0/24 anywhere`
	Packet Capture
	`9 1.505859000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	`10 1.506433000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	`11 1.507011000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	`12 1.507538000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	`13 1.508061000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	`14 1.508589000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	`15 1.509113000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	`16 1.509642000 192.168.10.2 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0`
	This packet capture illustrates that packets were not being successfully ACKed and therefore not successfully reaching the host on the subnet.

4 D	**Before Hping Packet Craft (tcpIN CHAIN):**
	`0 0 DROP tcp -- em1 p3p1 anywhere anywhere tcp dpts:!0:1024 flags:FIN,SYN,RST,ACK/SYN`
	
	Hping Packet Craft (from Host B):
	`[root@DataComm ~]# hping 192.168.0.15 -s 2000 -k -S -p 2222 -c 20 -i u500`
	`HPING 192.168.0.15 (em1 192.168.0.15): S set, 40 headers + 0 data bytes`
	
	`--- 192.168.0.15 hping statistic ---`
	`20 packets transmitted, 0 packets received, 100% packet loss`
	`round-trip min/avg/max = 0.0/0.0/0.0 ms`
	`[root@DataComm ~]#`
	
	After Hping Packet Craft (tcpIN CHAIN):
	`40 1600 DROP tcp -- em1 p3p1 anywhere anywhere tcp dpts:!0:1024 flags:FIN,SYN,RST,ACK/SYN`
	Packet Capture
	`93 2.293015000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`94 2.293538000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`95 2.294060000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`96 2.294587000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`97 2.295117000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`98 2.295643000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`99 2.296158000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`100 2.296704000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	`101 2.297224000 192.168.0.17 192.168.0.20 TCP 54 [TCP Port numbers reused] cisco-sccp > EtherNet-IP-1 [SYN] Seq=0 Win=512 Len=0`
	This packet capture illustrates that packets were not being successfully ACKed and therefore not successfully reaching the host on the subnet.

4 E	**Before Hping Packet Craft (tcpIN CHAIN):** `0 0 DROP tcp -- em1 p3p1 anywhere anywhere tcp flags:FIN,SYN/FIN,SYN`

Hping Packet Craft (from Host B):

```
[root@DataComm ~]# hping 192.168.0.24 -S -F -s 2000 -k -p 80 -c 20 -i u500
HPING 192.168.0.24 (em1 192.168.0.24): SF set, 40 headers + 0 data bytes

--- 192.168.0.24 hping statistic ---
20 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@DataComm ~]#
```

After Hping Packet Craft (tcpIN CHAIN):

```
 0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp flags:FIN,SYN/FIN,SYN
```

Packet Capture

10	2.007484000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
11	2.008038000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
12	2.008568000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
13	2.009105000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
14	2.009649000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
15	2.010201000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
16	2.010734000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
17	2.011304000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
18	2.011836000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0
19	2.012396000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > http [FIN, SYN] Seq=0 Win=512 Len=0

This packet capture illustrates that packets were not being successfully ACKed and therefore not successfully reaching the host on the subnet.

4 F

Before Hping Packet Craft (tcpIN CHAIN):

```
 0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp dpt:telnet
 0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp spt:telnet
```

Hping Packet Craft (from Host B):

```
[root@DataComm ~]# hping 192.168.0.24 -S -s 2000 -k -p 23 -c 20 -i u500
HPING 192.168.0.24 (em1 192.168.0.24): S set, 40 headers + 0 data bytes

--- 192.168.0.24 hping statistic ---
20 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@DataComm ~]#
```

After Hping Packet Craft (tcpIN CHAIN):

```
20   800 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp dpt:telnet
 0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             tcp spt:telnet
```

Packet Capture

3	0.296249000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0
4	0.296776000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0
5	0.297317000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0
6	0.297854000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0
7	0.298412000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0
8	0.298941000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0
9	0.299475000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0
10	0.300012000	192.168.0.17	192.168.0.20	TCP	54	[TCP Port numbers reused] cisco-sccp > telnet [SYN] Seq=0 Win=512 Len=0

This packet capture illustrates that packets were not being successfully ACKed and therefore not successfully reaching the host on the subnet.

4 G

Before Hping Packet Craft (tcpIN CHAIN):

```
 0     0 DROP       tcp  --  em1    p3p1    anywhere             anywhere             multiport dports filenet-tms:filenet-pch,netbios-ns:netbios-ssn,sunrpc,sftp
```

Hping Packet Craft (from Host B):

```
[root@DataComm ~]# hping 192.168.0.24 -S -s 2000 -k -p 111 -c 20 -i u500
HPING 192.168.0.24 (em1 192.168.0.24): S set, 40 headers + 0 data bytes

--- 192.168.0.24 hping statistic ---
20 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@DataComm ~]#
```

After Hping Packet Craft (tcpIN CHAIN):

```
20   800 DROP       tcp  --  em1    p3p1    anywhere             anywhere             multiport dports filenet-tms:filenet-pch,netbios-ns:netbios-ssn,sunrpc,sftp
```

Packet Capture

9	2.498511000	192.168.0.17	192.168.0.20	TCP	54 cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
10	2.499063000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
11	2.499590000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
12	2.500126000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
13	2.500663000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
14	2.501200000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
15	2.501723000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
16	2.502289000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
17	2.502847000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
18	2.503380000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
19	2.503939000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
20	2.504470000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0
21	2.505031000	192.168.0.17	192.168.0.20	TCP	54 [TCP Port numbers reused] cisco-sccp > sunrpc [SYN] Seq=0 Win=512 Len=0

This packet capture illustrates that packets were not being successfully ACKed and therefore not successfully reaching the host on the subnet.

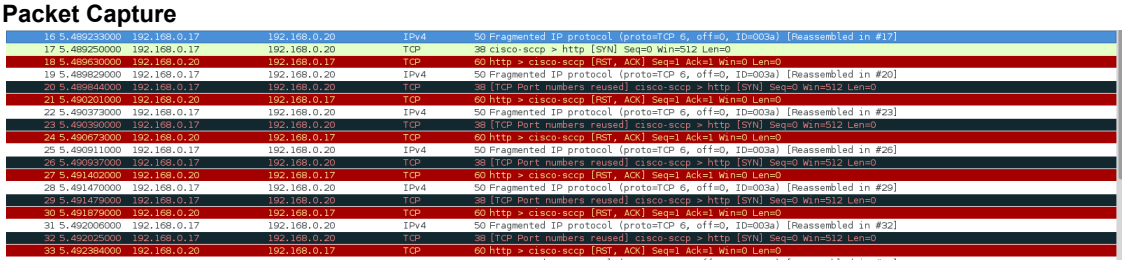
Test Case	Description	Command	Expected Results	Actual Results
Specific Accept Rules				
5 A	Accept fragments	hping 192.168.0.24 -f -s 2000 -k -p 80 -c 20 -i u500	fragmented packets accepted	Success, Ack backs
5 B	Accept packets from existing connections	Passive	connections aren't blocked after initial SYN	Success
Test Screenshots				
5 A	**Before Hping Packet Craft (FORWARD CHAIN):** `0  0 ACCEPT  all  -f  any  any  anywhere  anywhere` **Hping Packet Craft (from Host B):**			

```
HPING 192.168.0.24 (em1 192.168.0.24): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.24 ttl=63 DF id=37777 sport=80 flags=RA seq=0 win=0 rtt=1.0 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37778 sport=80 flags=RA seq=0 win=0 rtt=2.2 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37779 sport=80 flags=RA seq=0 win=0 rtt=2.2 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37780 sport=80 flags=RA seq=0 win=0 rtt=2.8 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37781 sport=80 flags=RA seq=0 win=0 rtt=2.8 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37782 sport=80 flags=RA seq=0 win=0 rtt=3.9 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37783 sport=80 flags=RA seq=0 win=0 rtt=3.9 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37784 sport=80 flags=RA seq=0 win=0 rtt=5.0 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37785 sport=80 flags=RA seq=0 win=0 rtt=5.0 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37786 sport=80 flags=RA seq=0 win=0 rtt=5.8 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37787 sport=80 flags=RA seq=0 win=0 rtt=6.8 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37788 sport=80 flags=RA seq=0 win=0 rtt=6.8 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37789 sport=80 flags=RA seq=0 win=0 rtt=7.9 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37790 sport=80 flags=RA seq=0 win=0 rtt=7.9 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37791 sport=80 flags=RA seq=0 win=0 rtt=8.9 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37792 sport=80 flags=RA seq=0 win=0 rtt=8.9 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37793 sport=80 flags=RA seq=0 win=0 rtt=10.0 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37794 sport=80 flags=RA seq=0 win=0 rtt=10.0 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37795 sport=80 flags=RA seq=0 win=0 rtt=11.2 ms
DUP! len=46 ip=192.168.0.24 ttl=63 DF id=37796 sport=80 flags=RA seq=0 win=0 rtt=11.2 ms

--- 192.168.0.24 hping statistic ---
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 1.0/6.2/11.2 ms
```

After Hping Packet Craft (FORWARD CHAIN):

```
0      0 ACCEPT      all   -f  any     any     anywhere            anywhere
```

Packet Capture



16 5.489233000	192.168.0.17	192.168.0.20	IPv4	50 Fragmented IP protocol (proto=TCP 6, off=0, ID=003a) [Reassembled in #17]
17 5.489250000	192.168.0.17	192.168.0.20	TCP	38 cisco-sccp > http [SYN] Seq=0 Win=512 Len=0
18 5.489630000	192.168.0.20	192.168.0.17	TCP	60 http > cisco-sccp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19 5.489829000	192.168.0.17	192.168.0.20	IPv4	50 Fragmented IP protocol (proto=TCP 6, off=0, ID=003a) [Reassembled in #20]
20 5.489844000	192.168.0.17	192.168.0.20	TCP	38 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0
21 5.490201000	192.168.0.20	192.168.0.17	TCP	60 http > cisco-sccp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 5.490373000	192.168.0.17	192.168.0.20	IPv4	50 Fragmented IP protocol (proto=TCP 6, off=0, ID=003a) [Reassembled in #23]
23 5.490390000	192.168.0.17	192.168.0.20	TCP	38 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0
24 5.490673000	192.168.0.20	192.168.0.17	TCP	60 http > cisco-sccp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25 5.490911000	192.168.0.17	192.168.0.20	IPv4	50 Fragmented IP protocol (proto=TCP 6, off=0, ID=003a) [Reassembled in #26]
26 5.490937000	192.168.0.17	192.168.0.20	TCP	38 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0
27 5.491402000	192.168.0.20	192.168.0.17	TCP	60 http > cisco-sccp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28 5.491470000	192.168.0.17	192.168.0.20	IPv4	50 Fragmented IP protocol (proto=TCP 6, off=0, ID=003a) [Reassembled in #29]
29 5.491479000	192.168.0.17	192.168.0.20	TCP	38 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0
30 5.491879000	192.168.0.20	192.168.0.17	TCP	60 http > cisco-sccp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 5.492006000	192.168.0.17	192.168.0.20	IPv4	50 Fragmented IP protocol (proto=TCP 6, off=0, ID=003a) [Reassembled in #32]
32 5.492025000	192.168.0.17	192.168.0.20	TCP	38 [TCP Port numbers reused] cisco-sccp > http [SYN] Seq=0 Win=512 Len=0
33 5.492384000	192.168.0.20	192.168.0.17	TCP	60 http > cisco-sccp [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

This packet capture illustrates that fragmented packets are being passed, through the fire wall.

5 B	Since tcpIN and tcpOUT accept packets with established connections. All packets that have already been established will be accepted.

Test Case	Description	Command	Expected Results	Actual Results
Delay & Throughput				
6 A	Minimum delay & maximum throughput for	hping 192.168.0.24 -S -s 2000 -k -p 22 -c 5000 -i u5000 hping 192.168.0.24 -S -s 2000 -k -p 80 -c 5000 -i u5000	Faster RTT on ports 20, 21, 22	Success, when packets sent at the

	FTP & SSH traffic			same time, port 22 was favoured
Test Screenshots				

6 A	**RTT on ports other than 20,21,22:**
	`--- 192.168.0.24 hping statistic ---`
	`5000 packets transmitted, 5000 packets received, 0% packet loss`
	`round-trip min/avg/max = 0.3/2.2/1001.5 ms`
	`[root@DataComm ~]#`
	
	RTT on ports 20,21,22:
	`--- 192.168.0.24 hping statistic ---`
	`5000 packets transmitted, 5000 packets received, 0% packet loss`
	`round-trip min/avg/max = 0.3/1.6/1001.5 ms`
	`[root@DataComm ~]#`			