Assignment #2

Clemens Lo A00863045

Charles Kevin Tan A00896299

COMP 8006 February 4, 2016

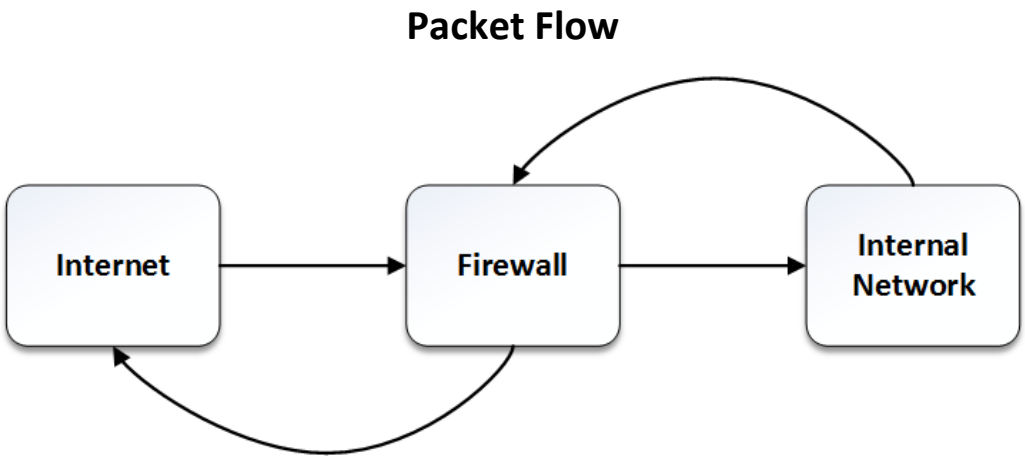
TABLE OF CONTENTS

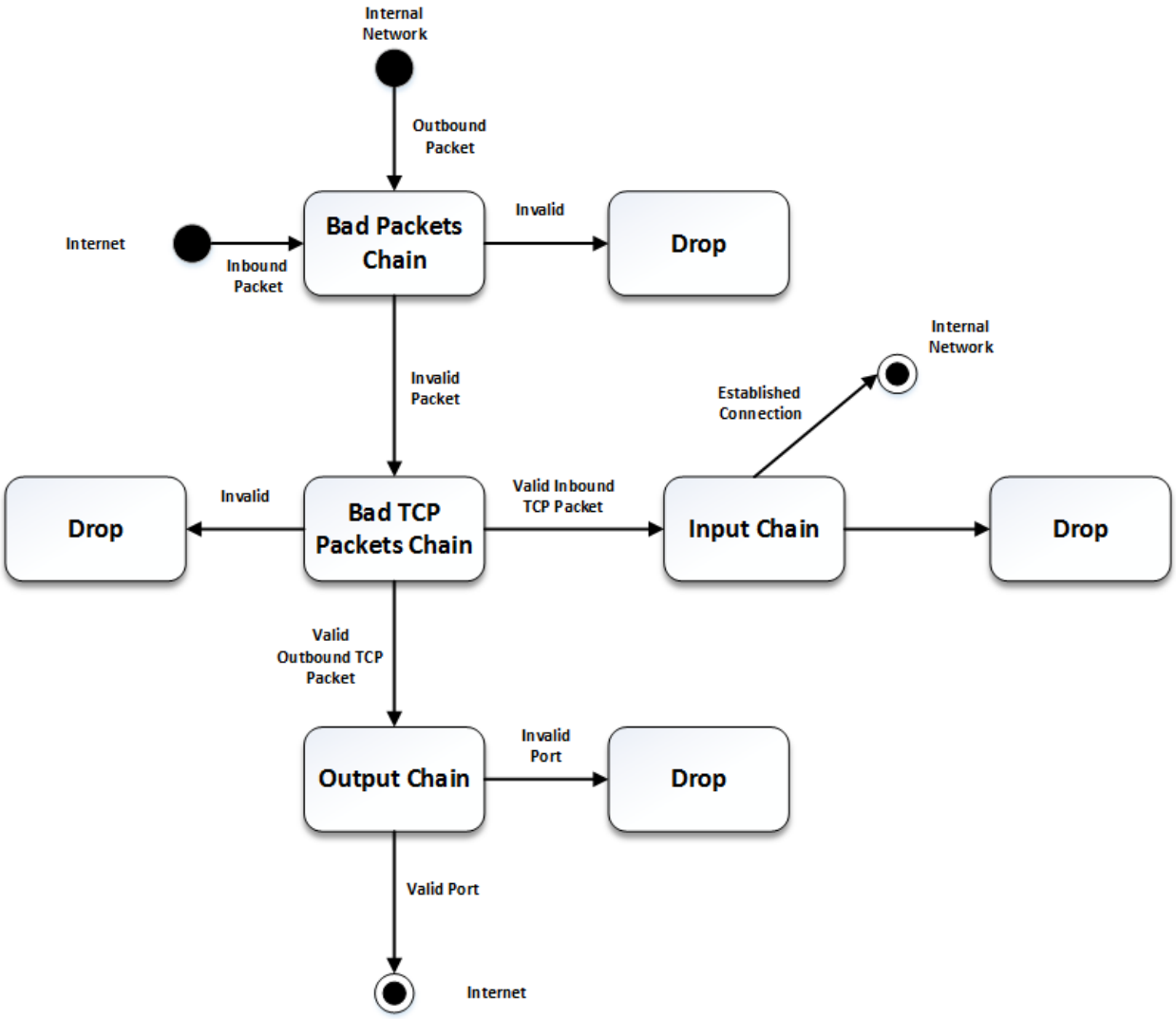
Overview

The purpose of this assignment is to create a iptables firewall that manages traffic through two Ethernet interfaces. One interface is the external interface, which connection to the internet, and the other one is the internal interface, which connected to the local network. All packets come from/in the external interface will go through the firewall. The firewall is reacting like a gateway and flit all traffic based on the specific rules.

Design Diagrams

Both inbound and outbound network packets will go through the firewall for inspection. Therefore the internal network is protected and isolated from the internet.




Internal Network
Outbound Packet
Internet
Inbound Packet
Bad Packets Chain
Invalid
Drop
Invalid Packet
Internal Network
Established Connection
Drop
Invalid
Bad TCP Packets Chain
Valid Inbound TCP Packet
Input Chain
Drop
Valid Outbound TCP Packet
Output Chain
Invalid Port
Drop
Valid Port
Internet

Testing

External to Computer behind Firewall

Test #	Description	Test Action	Result	Pass/Fail
1	Allow inbound packets on port 80 and 443 as specified by user	hping3 using test.sh script	Successfully showed the traffic being passed	Passed. Check the screenshot.
2	Drop inbound packets on ports 111 and 515, 137 – 139, 32768 – 32775	hping3 using test.sh script	Successfully shows the traffic being dropped.	Passed. Check the screenshot.
3	Telnet blocked	hping3 using test.sh script	Successfully shows that packets going to port 23 are dropped	Passed. Check the screenshot.
4	SYN packets to high ports dropped	hping3 using test.sh script	Successfully shows packets are dropped.	Passed. Check the screenshot.
5	SYN, FIN packets are dropped	hping3 using test.sh script.	Successfully shows the packets are dropped.	Passed. Check the screenshot.
6	Fragmented packets are allowed	hping3 using test.sh script.	Successfully shows the packets are accepted	Passed. Check the screenshot.
7	SSH connected	hping3 using test.sh script	Successfully shows packets being accepted in port 22	Passed. Check the screenshot.

Test Case 1: Allow packets to port 80 and 441

Results:

```
#Initializing TCP ports 80, 443 that is allowed by user

'80,' being added


--- 192.168.0.8 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.8 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=0.8 ms
'443' being added


--- 192.168.0.8 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.8 ttl=63 DF id=52973 sport=443 flags=RA seq=0 win=0 rtt=0.8 ms
```

Test Case 2: Drop packets to ports 111, 137, 138, 139, 515, 32768 – 32775

Results:

```
#Initializing TCP ports 111, 137, 138, 139, 515, 32768, 32769, 32770, 32771, 32772, 32773, 32774, 32775 that is dropped by user

'111,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'137,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'138,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'139,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
```

```
'515,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32768,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32769,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32770,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32771,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32772,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32773,' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32774,' being dropped
```

```
--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
'32775' being dropped

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
```

Test Case 3: Drop telnet packets

Results:

```
# Will 192.168.0.8 drop telnet packets


--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
```

Test Case 4: SYN packets to high ports are dropped

Results:

```
# Check the SYN to port 15000 on 192.168.0.8


--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
```

Test Case 5: Drop SYN/FIN packets

Results:

```
# Waiting if 192.168.0.8 will accept or drop SYN/FIN packets


--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): SF set, 40 headers + 0 data bytes

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.8 (eno1 192.168.0.8): SF set, 40 headers + 0 data bytes
```

Test 6: Fragments allowed

Results:

```
# Check the fragments in 192.168.0.8


--- 192.168.0.8 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.9/0.9/0.9 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 888 data bytes
len=46 ip=192.168.0.8 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=0.9 ms

--- 192.168.0.8 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 888 data bytes
len=46 ip=192.168.0.8 ttl=63 DF id=61 sport=443 flags=RA seq=0 win=0 rtt=0.8 ms
```

Test 7: SSH connected

Results:

```
# Will 192.168.0.8 drop or accpet ssh packets


--- 192.168.0.8 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.7/0.7 ms
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.8 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=0.7 ms
```

Computer Behind Firewall to External

Test #	Description	Test Action	Result	Pass/Fail
1	Allow inbound packets on port 80 and 443 as specified by user	hping3 using test.sh script	Successfully showed the traffic being passed	Passed. Check the screenshot.
2	Drop inbound packets on ports 111 and 515, 137 – 139, 32768 – 32775	hping3 using test.sh script	Successfully shows the traffic being dropped.	Passed. Check the screenshot.
3	Telnet blocked	hping3 using test.sh script	Successfully shows that packets going to port 23 are dropped	Passed. Check the screenshot.
4	SYN packets to high ports dropped	hping3 using test.sh script	Successfully shows packets are dropped.	Passed. Check the screenshot.
5	SYN, FIN packets are dropped	hping3 using test.sh script.	Successfully shows the packets are dropped.	Passed. Check the screenshot.
6	Fragmented packets are allowed	hping3 using test.sh script.	Successfully shows the packets are accepted	Passed. Check the screenshot.
7	SSH connected	hping3 using test.sh script	Successfully shows packets being accepted in port 22	Passed. Check the screenshot.

Test Case 1: Allow inbound packets on port 80 and 443

Results:

```
#Initializing TCP ports 80, 443 that is allowed by user

'80,' being added


--- 192.168.0.11 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/0.6 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.11 ttl=63 DF id=29128 sport=80 flags=RA seq=0 win=0 rtt=0.6 ms
'443' being added


--- 192.168.0.11 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.7/0.7 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.11 ttl=63 DF id=29138 sport=443 flags=RA seq=0 win=0 rtt=0.7 ms
```

Test Case 2: Drop packets to ports 111, 137, 138, 139, 515, 32768 – 32775

Results:

```
#Initializing TCP ports 111, 137, 138, 139, 515, 32768, 32769, 32770, 32771, 32772, 32773, 32774, 32775 that is dropped by user

'111,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'137,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'138,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'139,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'515,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'32768,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
```

```
'32769,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'32770,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'32771,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'32772,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'32773,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'32774,' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
'32775' being dropped

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
```

Test Case 3: Drop telnet packets

Results:

```
# Will 192.168.0.11 drop telnet packets


--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
```

Test Case 4: SYN packets to high ports are dropped

Results:

```
# Check the SYN to port 15000 on 192.168.0.11


--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
```

Test Case 5: Drop SYN/FIN packets

Results:

```
# Waiting if 192.168.0.11 will accept or drop SYN/FIN packets


--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): SF set, 40 headers + 0 data bytes

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): SF set, 40 headers + 0 data bytes
```

Test Case 6: Fragments allowed

Results:

```
# Check the fragments in 192.168.0.11


--- 192.168.0.11 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.0/1.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 888 data bytes
len=46 ip=192.168.0.11 ttl=63 DF id=41156 sport=80 flags=RA seq=0 win=0 rtt=1.0 ms

--- 192.168.0.11 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.0/1.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 888 data bytes
len=46 ip=192.168.0.11 ttl=63 DF id=41191 sport=443 flags=RA seq=0 win=0 rtt=1.0 ms
```

Test 7: SSH connected

Results:

```
# Will 192.168.0.11 drop or accpet ssh packets


--- 192.168.0.11 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.0/1.0 ms
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.11 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1.0 ms
```