|  |
| --- |
|  |
| Stand Alone Firewall |
|  |
| Testing Document |

February 1, 2016

Authored by: Marc Vouve and Eric Tsang

Stand Alone Firewall

Testing Document

Contents

[Definitions 2](#_Toc442305933)

[Methodology 2](#_Toc442305934)

[Results 3](#_Toc442305935)

[Fig1: TCP Should be Allowed Inbound/Outbound on Allowed Ports 4](#_Toc442305936)

[Fig 2: Inbound/Outbound UDP Packets on allowed ports 6](#_Toc442305937)

[Fig 3: ICMP Inbound/Outbound based on type numbers 8](#_Toc442305938)

[Fig 4: All packets that fall through default rule will be dropped 9](#_Toc442305939)

[Fig 5: Do not accept any packets with a source address from the outside matching your internal network 10](#_Toc442305940)

[Fig 6: Reject Packets Coming the Wrong Way 11](#_Toc442305941)

[Fig 7: Accept Fragments 13](#_Toc442305942)

[Fig 8: Accept all TCP packets that belong to an existing connection (on allowed ports) 14](#_Toc442305943)

[Fig 9: Drop all Packets with SYN/FIN bit set 16](#_Toc442305944)

[Fig 10: Do not not allow Telnet packets at all 17](#_Toc442305945)

[Fig 11: Block all on ports 32768-32775, 137 – 139 TCP 111 and 515 18](#_Toc442305946)

[32768-32775 18](#_Toc442305947)

[137-139 19](#_Toc442305948)

[111 20](#_Toc442305949)

[515 21](#_Toc442305950)

[Fig 12: For FTP and SSH set control connections to minimum delay and maximum throughput for data. 22](#_Toc442305951)

# Definitions

Host: Machine protected by the firewall

Attacker: Machine outside the network.

Firewall: The machine running the firewall.

# Methodology

We tested our stand alone firewall using hping3 and iptables. Commands were crafted to test each of the firewalls requirements and then ran from either the host machine which was inside the local network, the attacker machine which was outside the personal network, or both.

For each assignment constraint the following was done:

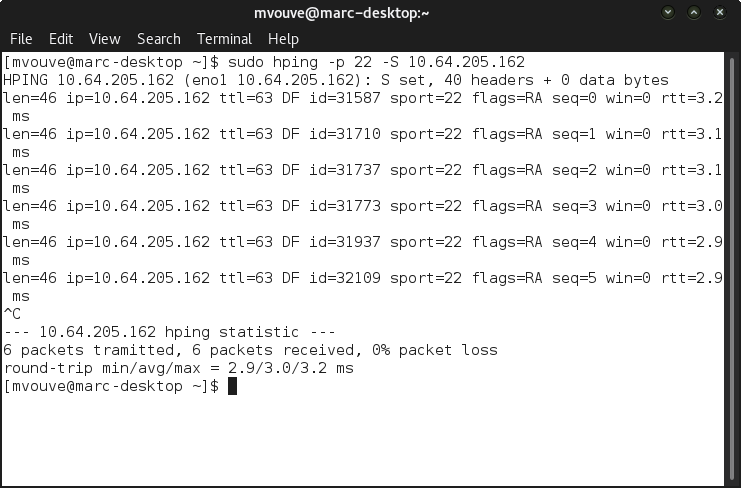
1. Firewall accounting was flushed
2. Rule was run on the appropriate machine
3. Results were recorded using screenshots and iptables accounting

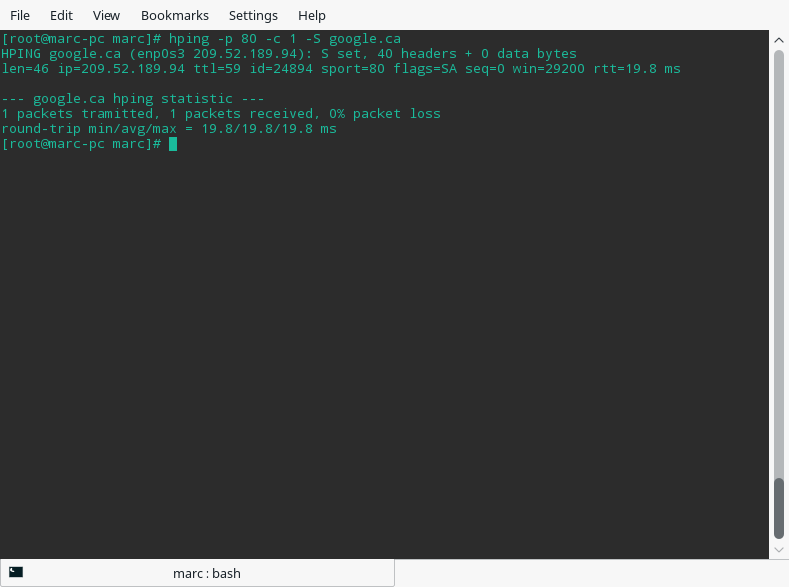
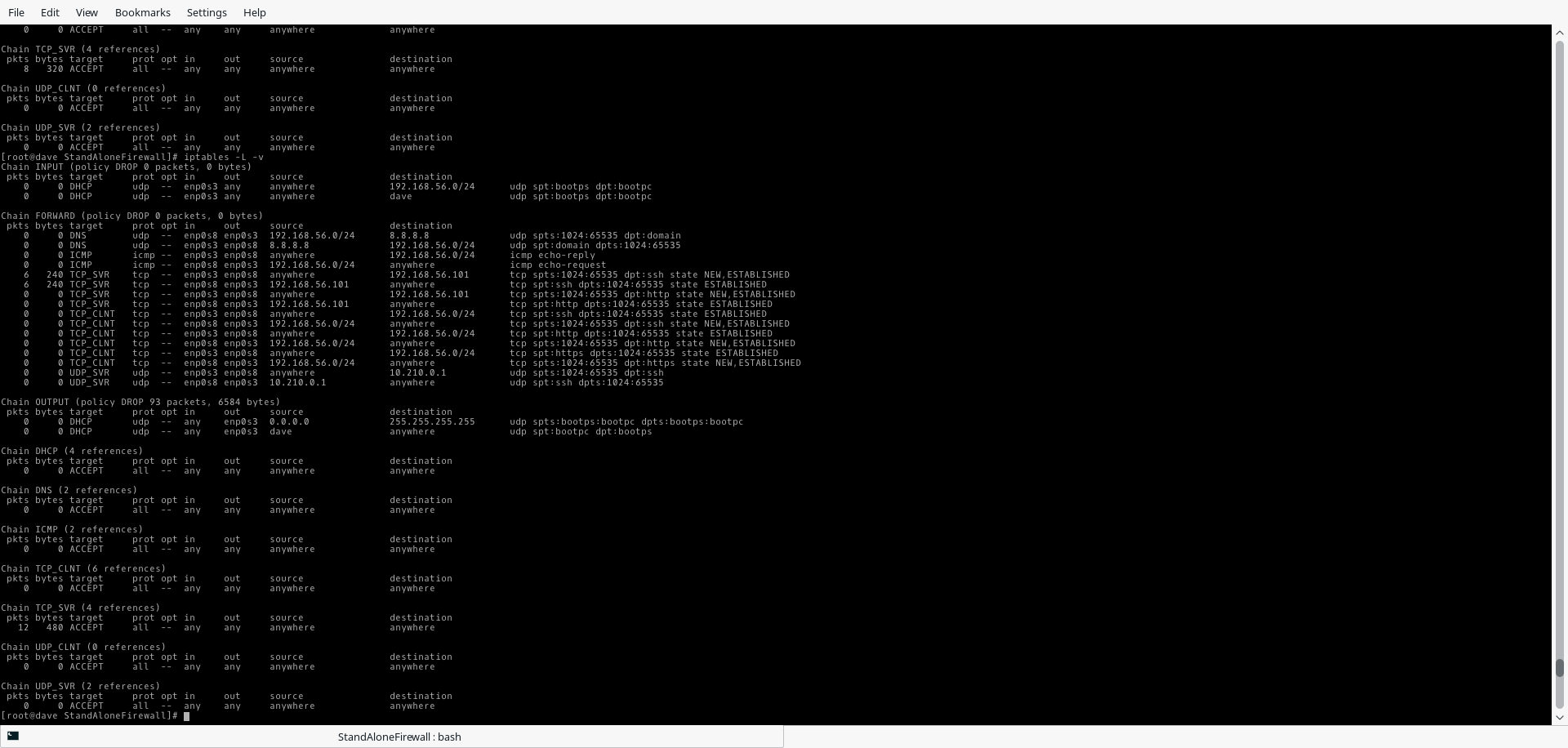
# Results

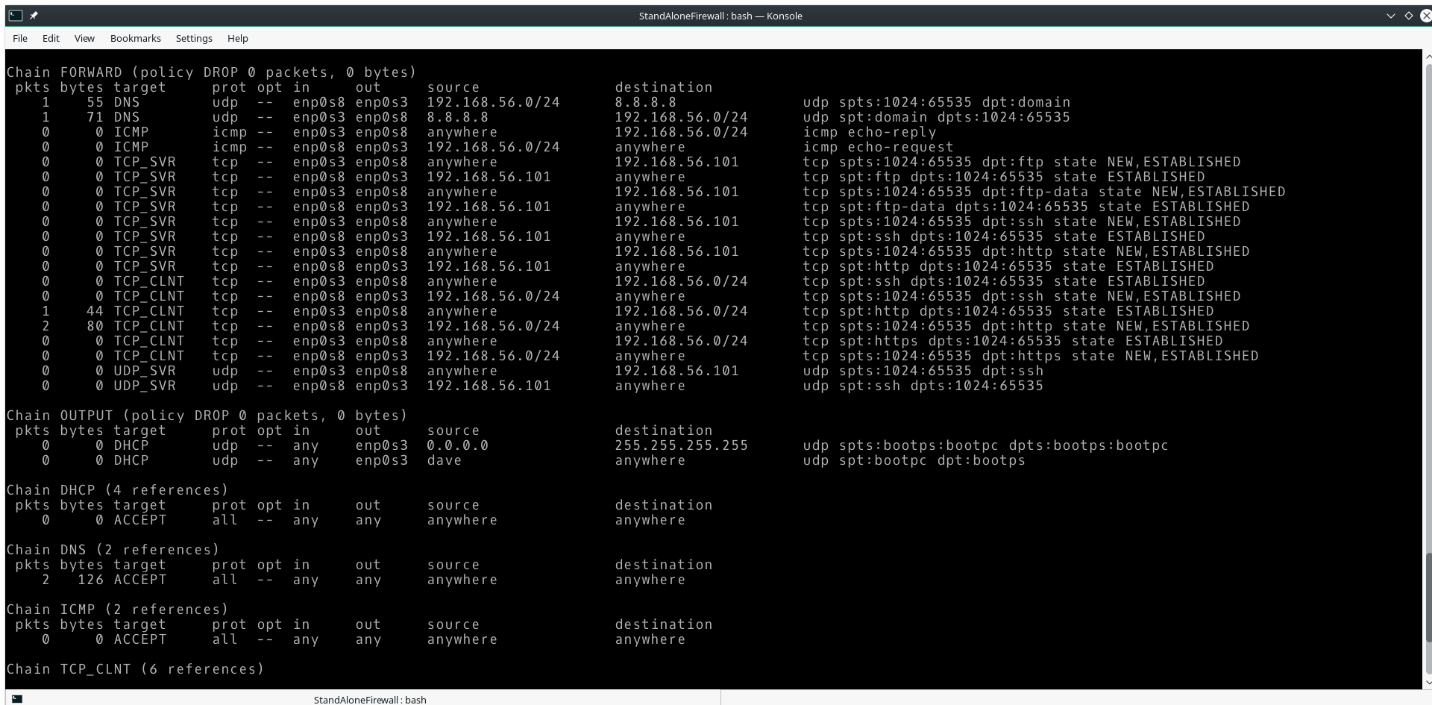
|  |  |  |  |
| --- | --- | --- | --- |
| Constraint | Tool | Status | Evidence |
| TCP Should be allowed Inbound/Outbound on Allowed ports | Hping3/iptables | passed | Fig 1 |
| UDP Should be allowed Inbound/Outbound on allowed ports | Hping3/iptables | Passed | Fig 2 |
| ICMP Should be allowed Inbound/Outbound on allowed Types | Ping/iptables | Passed | Fig 3 |
| All Packets not following the default rule should be dropped | Hping/iptables | Passed \* | Fig 4 |
| Drop all packets destine for the firewall from outside | Hping/iptables | Passed \* | Fig 5 |
| Do not accept any packets with a source address from the outside matching your internal network | Hping/iptables | Passed \* | Fig 6 |
| Reject connections going the “wrong” way i.e. high port SYN numbers | Hping/iptables | Passed \* | Fig 7 |
| Accept Fragments | Hping/iptables | Passed | Fig 8 |
| Drop all packets with the SYN/FIN bits set | Hping/iptables | Passed | Fig 9 |
| Do not allow telnet packets at all | Hping/iptables | Passed | Fig 10 |
| Block external traffic to 32768-32775, TCP 137-139, 111, 515 | Hping/iptables | Passed\* | Fig 11 |
| FTP (control) and SSH should have minimum delay FTP (data) should have maximum throughput | Hping/iptables | Passed | Fig 12 |

\* tested a small subset to verify results

## Fig1: TCP Should be Allowed Inbound/Outbound on Allowed Ports

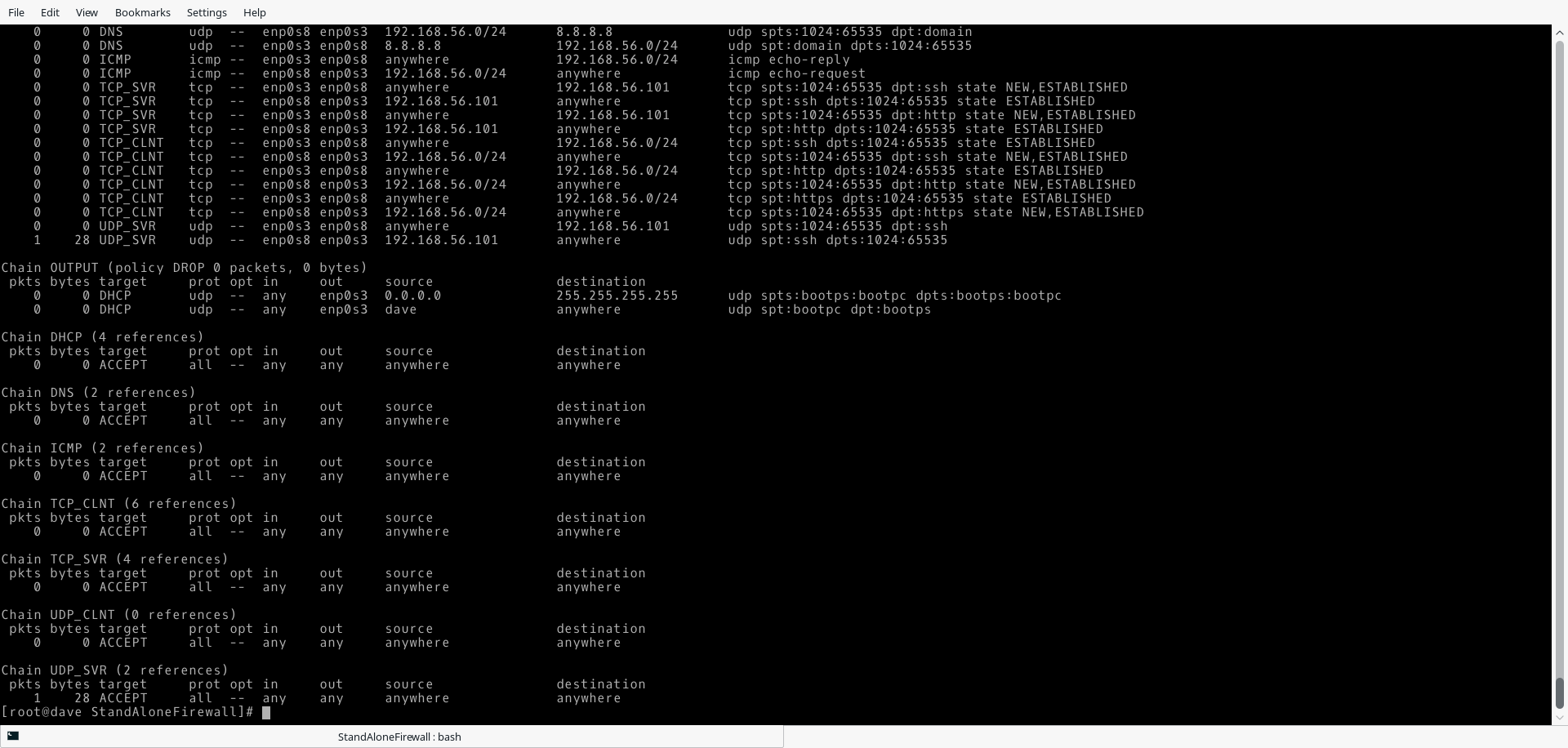


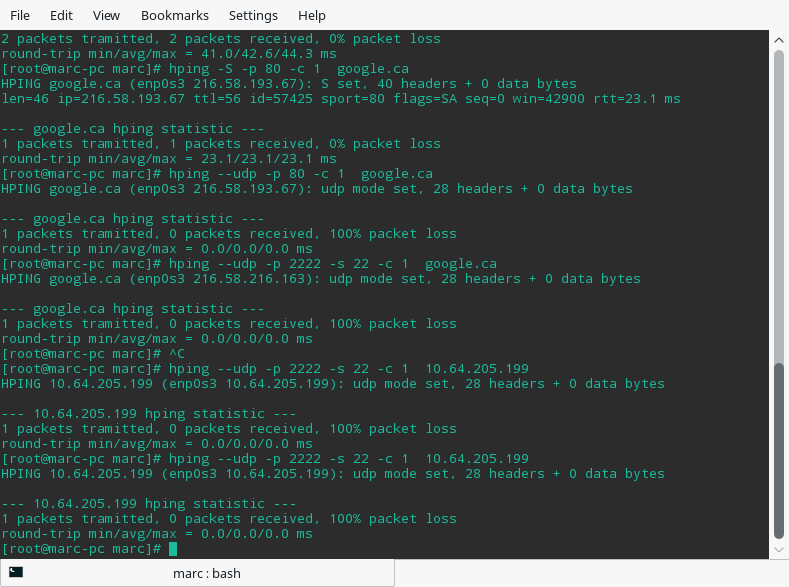


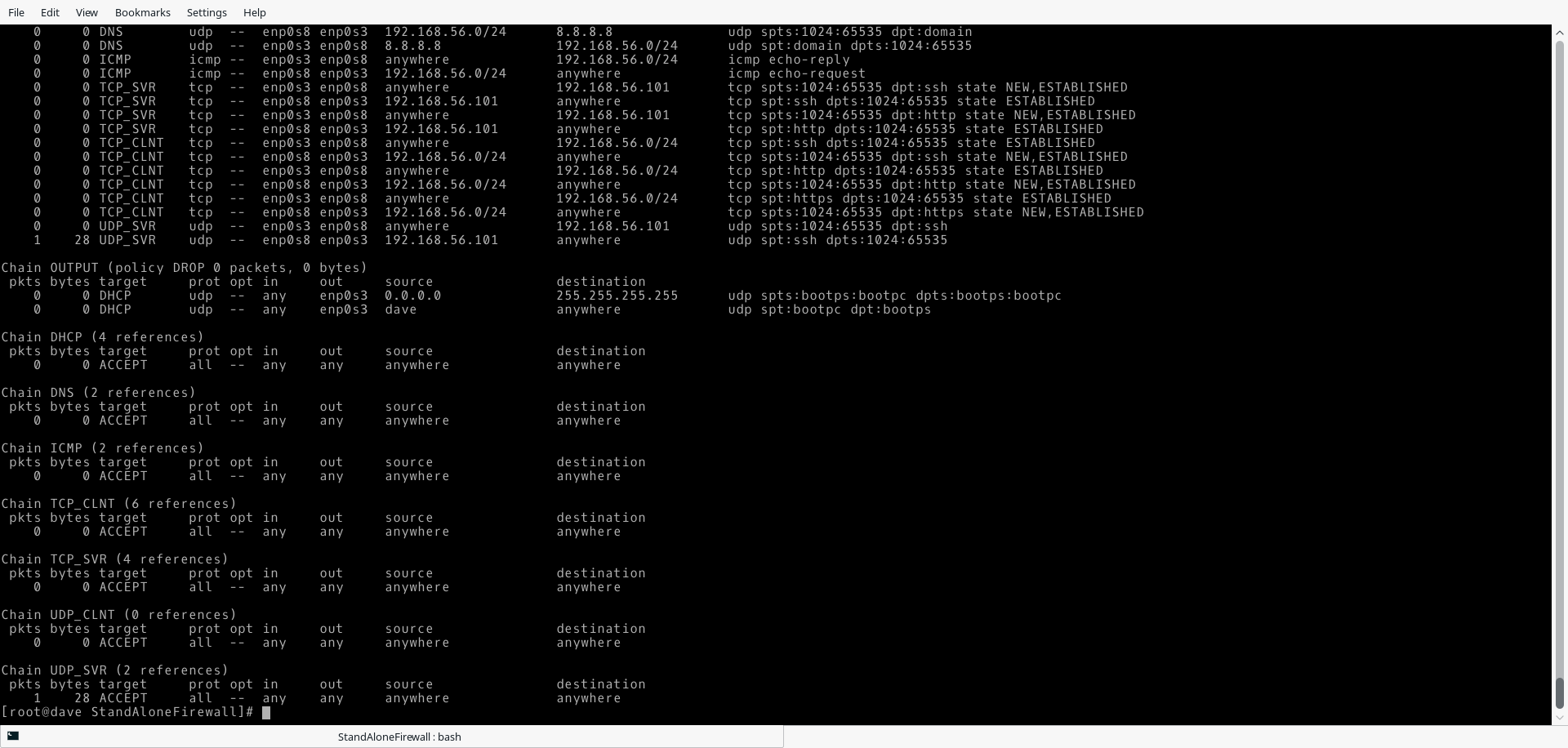


## Fig 2: Inbound/Outbound UDP Packets on allowed ports

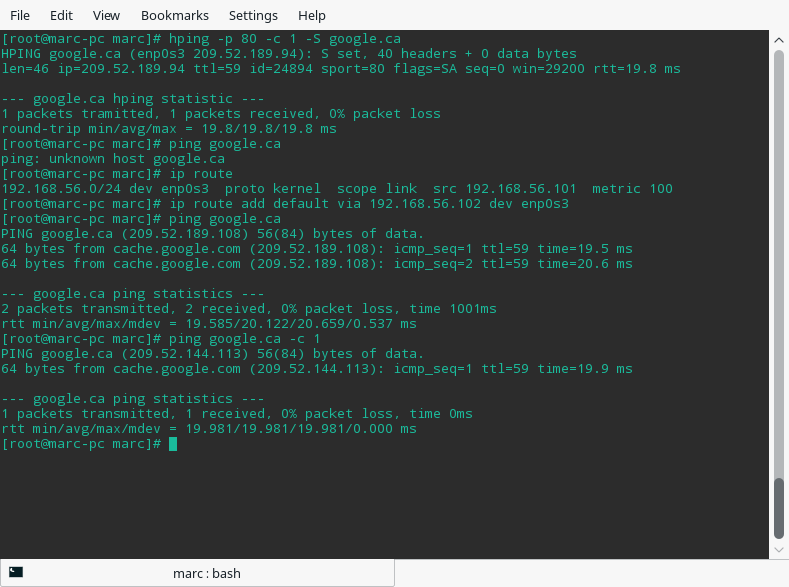


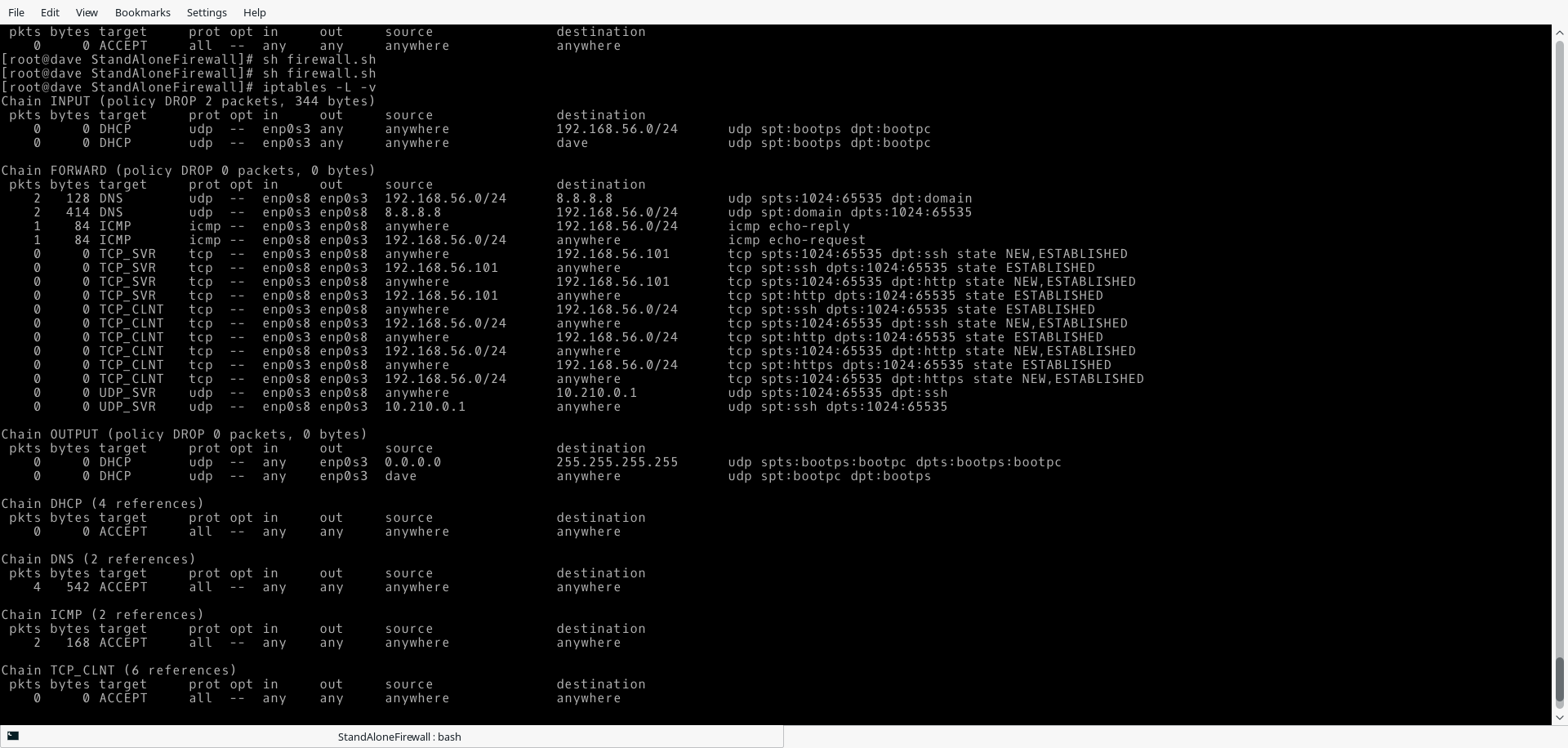




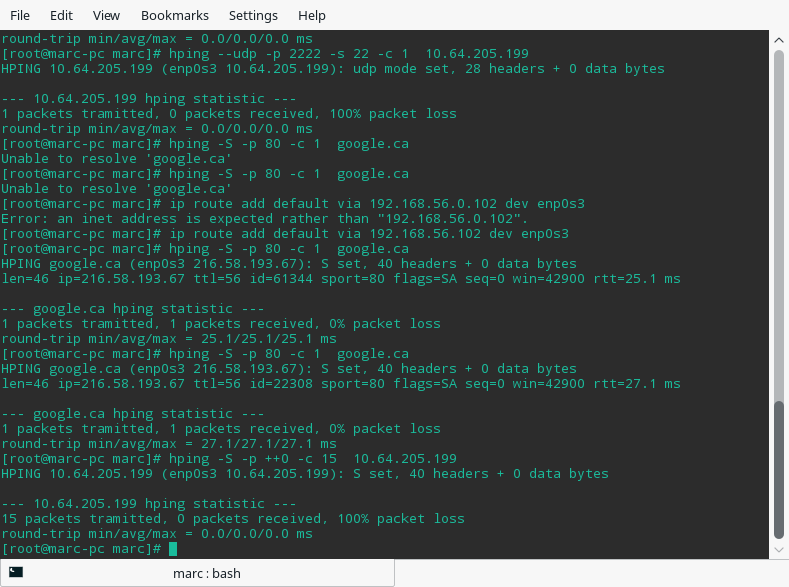


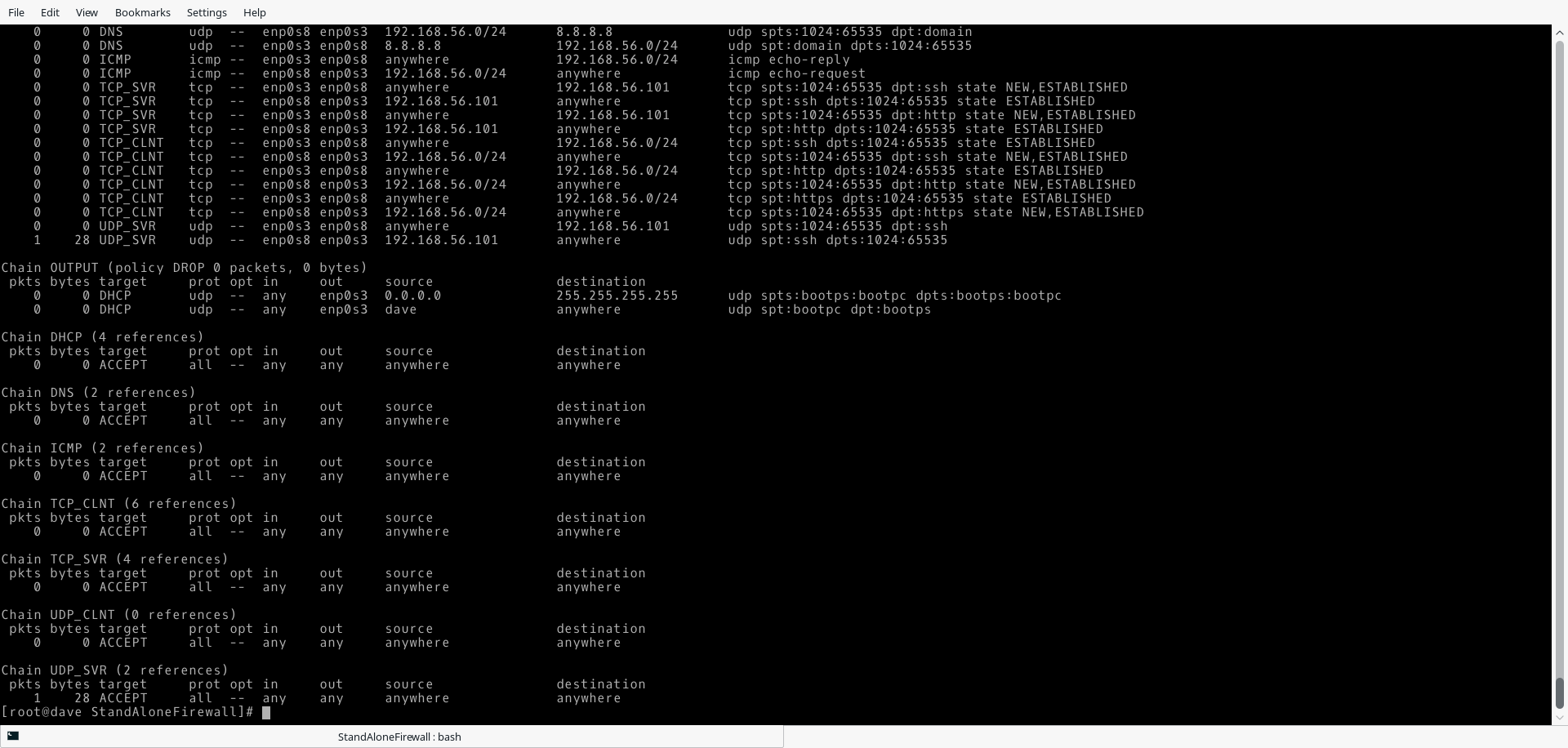
## Fig 3: ICMP Inbound/Outbound based on type numbers



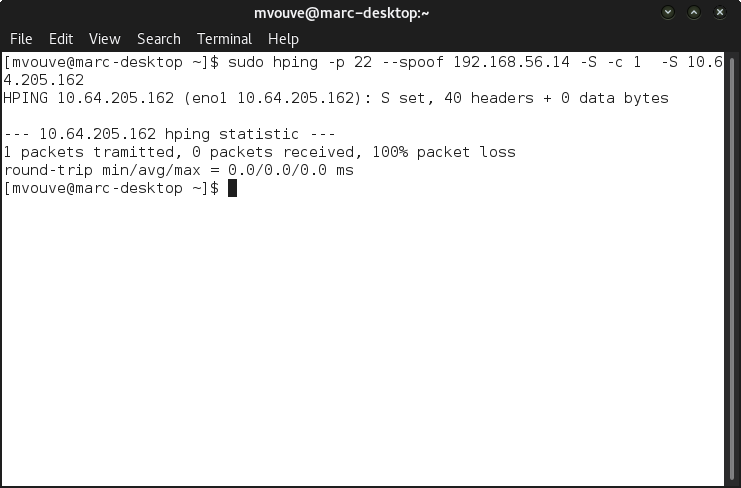


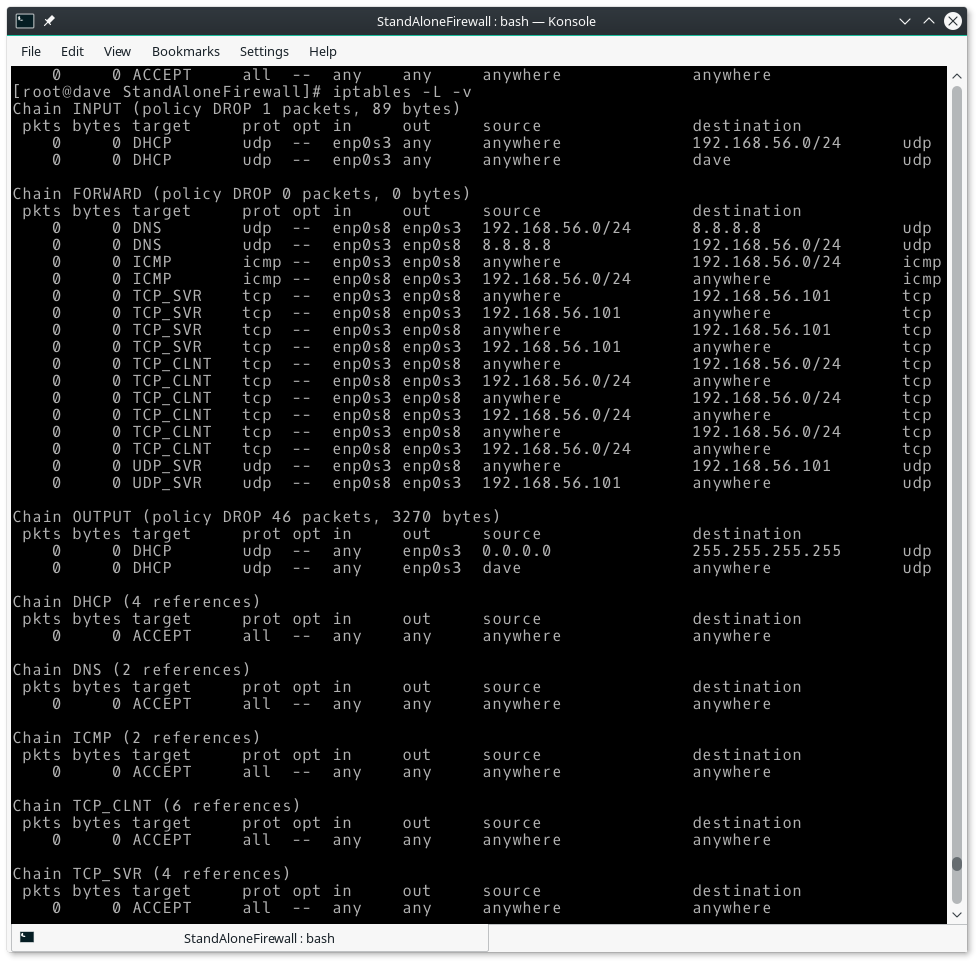
## Fig 4: All packets that fall through default rule will be dropped



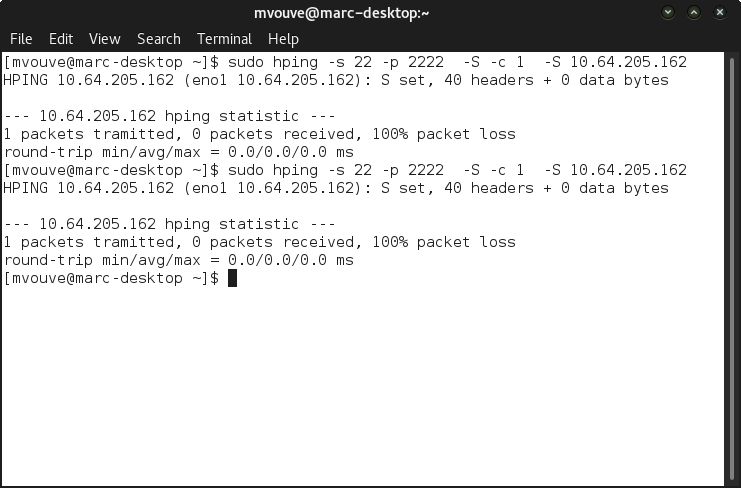


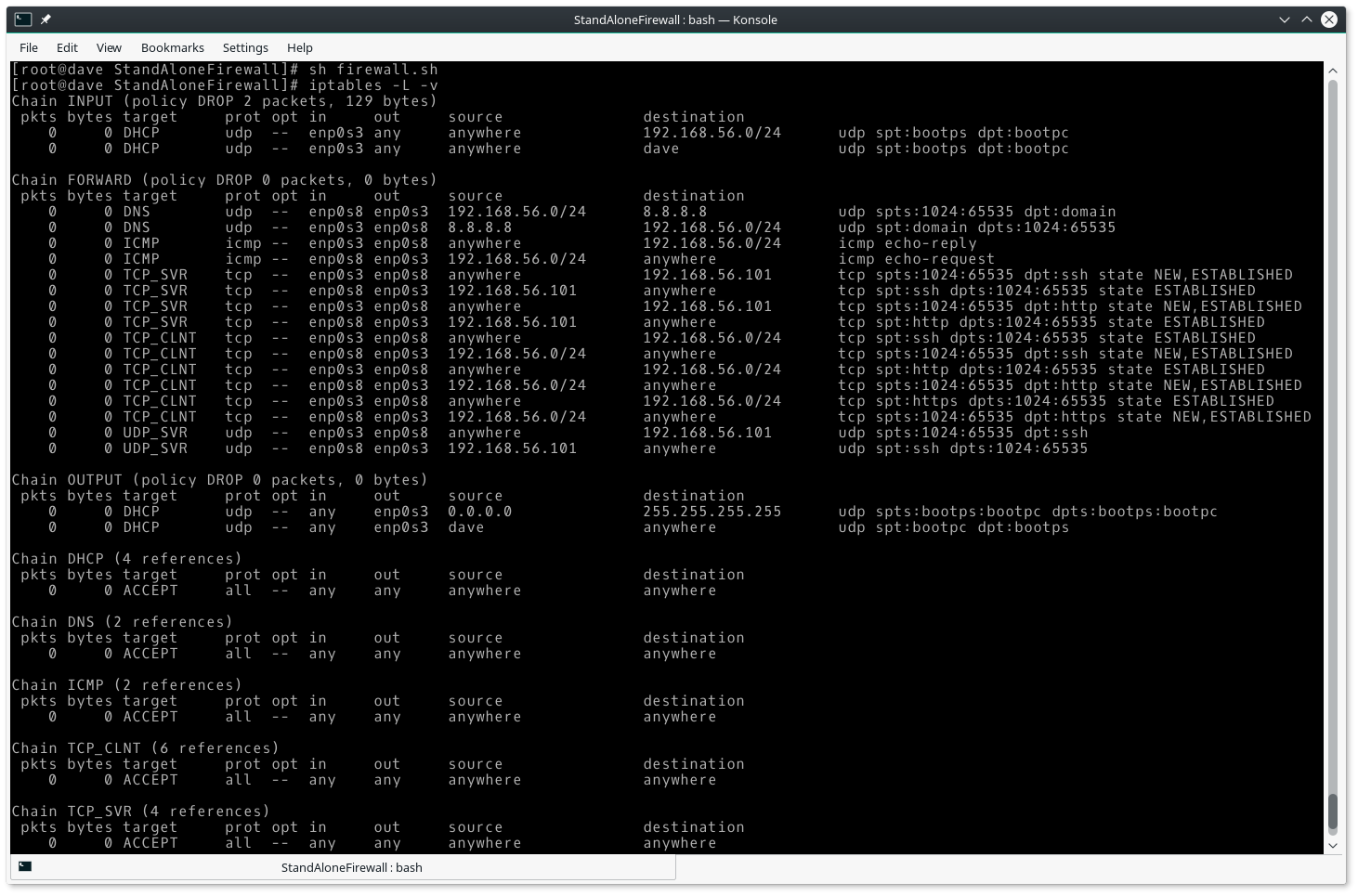
## Fig 5: Do not accept any packets with a source address from the outside matching your internal network



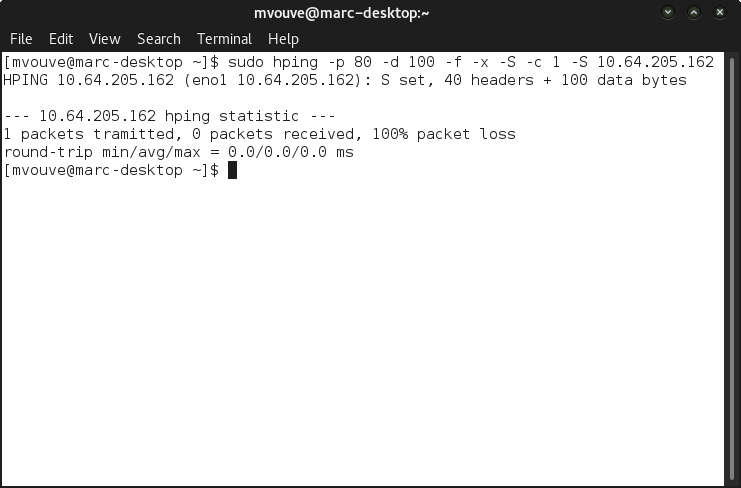


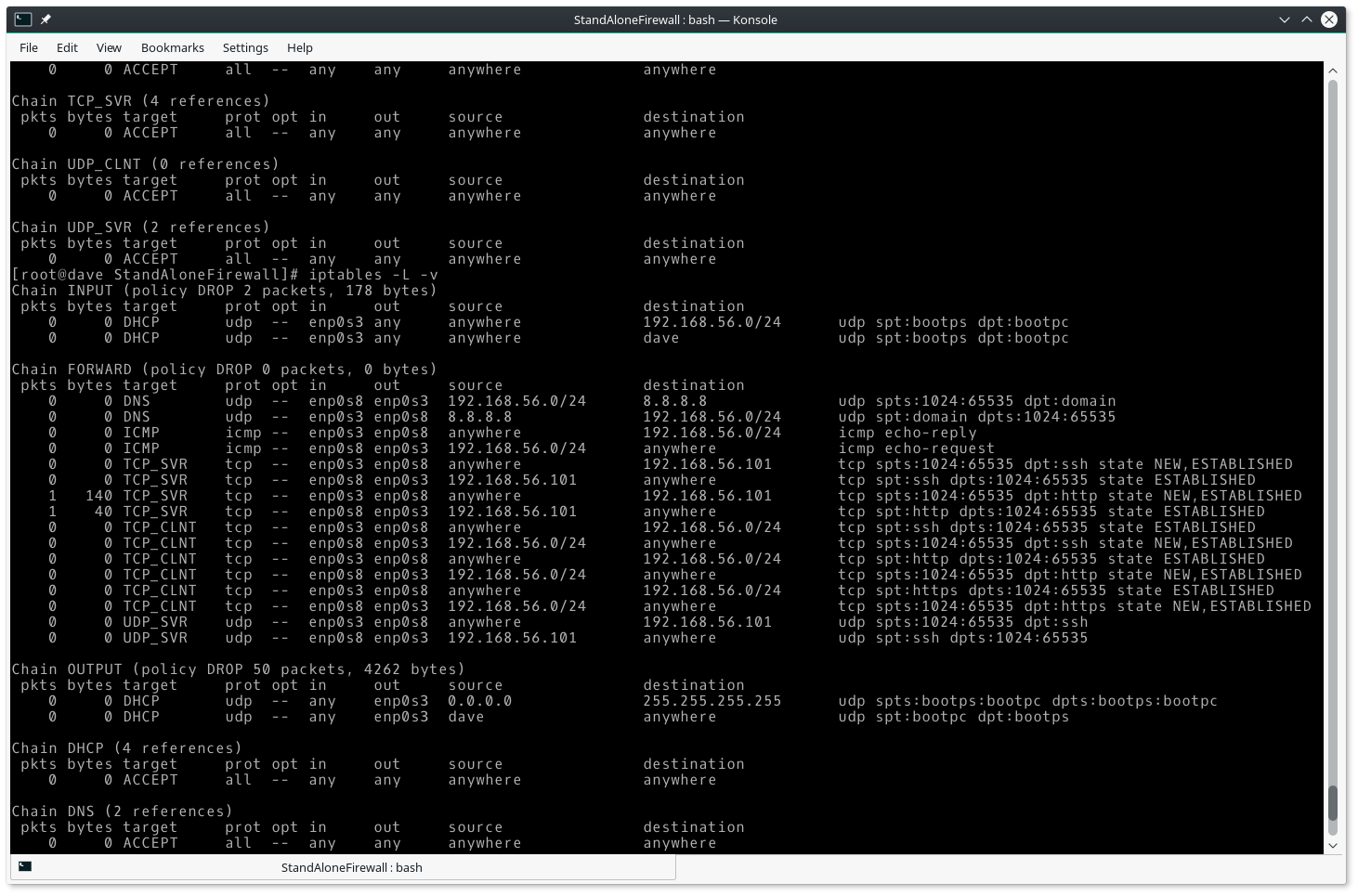
## Fig 6: Reject Packets Coming the Wrong Way



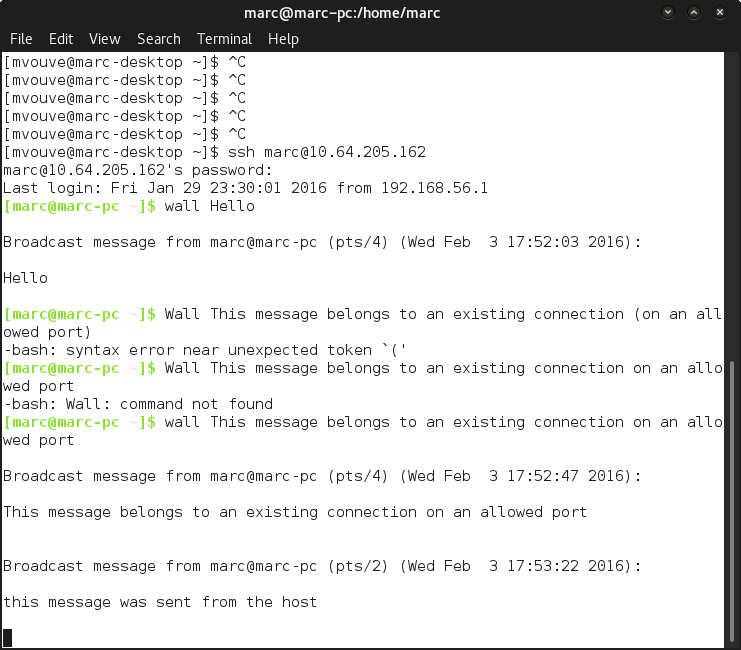


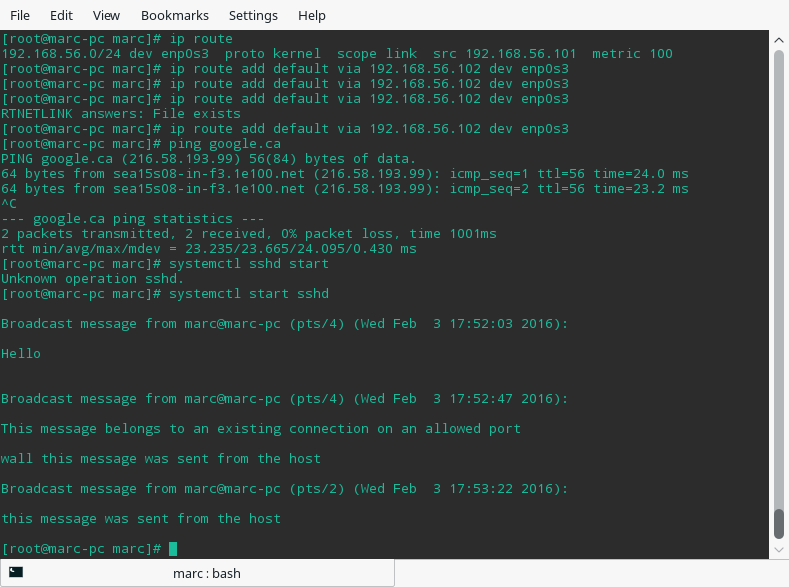
## Fig 7: Accept Fragments

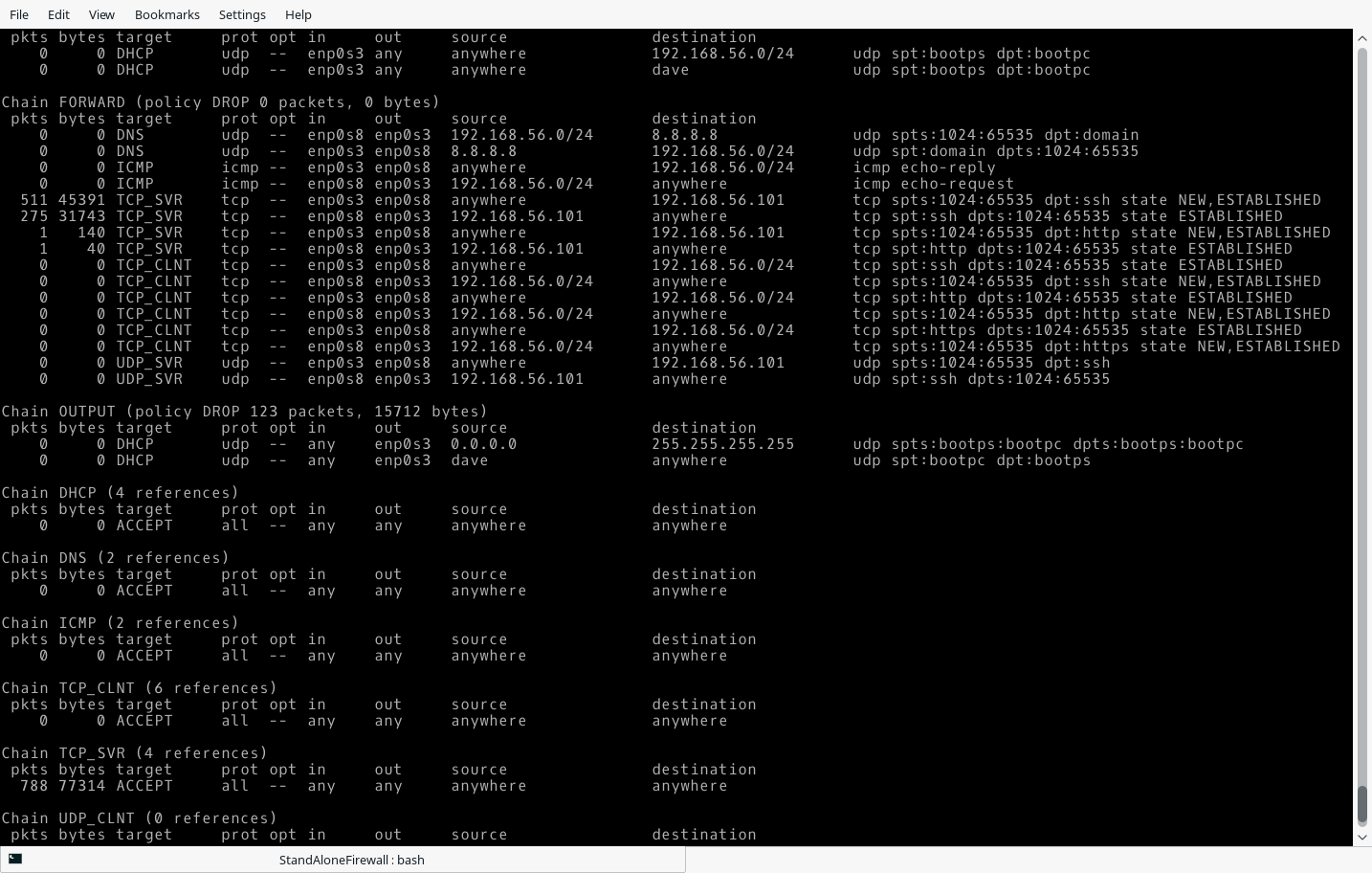




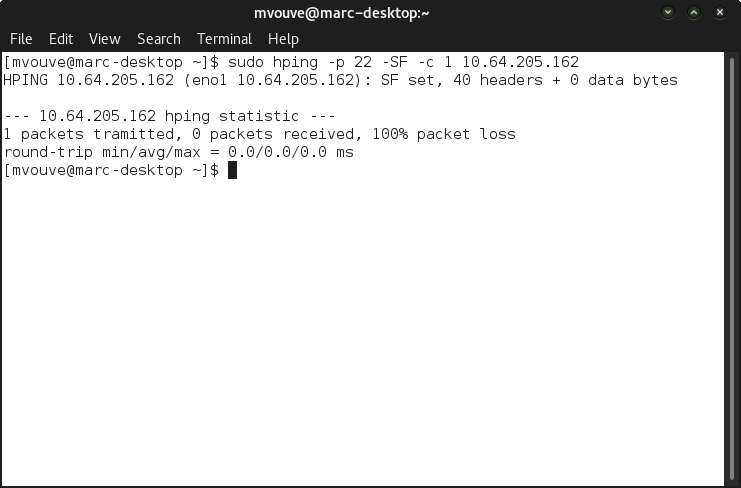
## Fig 8: Accept all TCP packets that belong to an existing connection (on allowed ports)

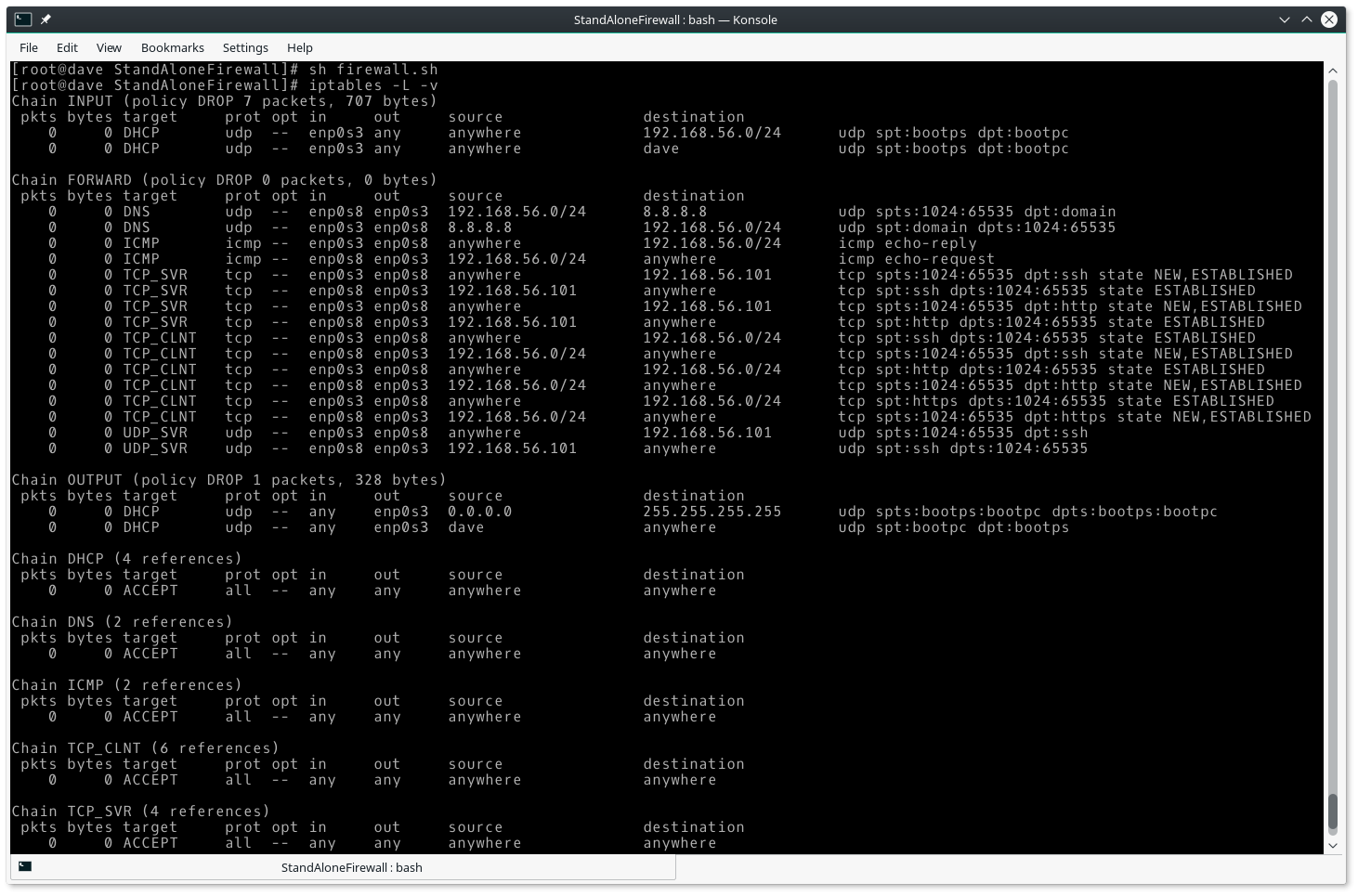




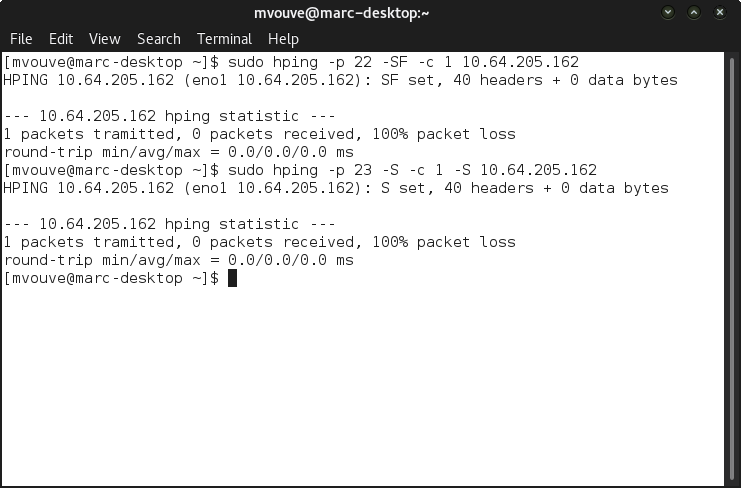


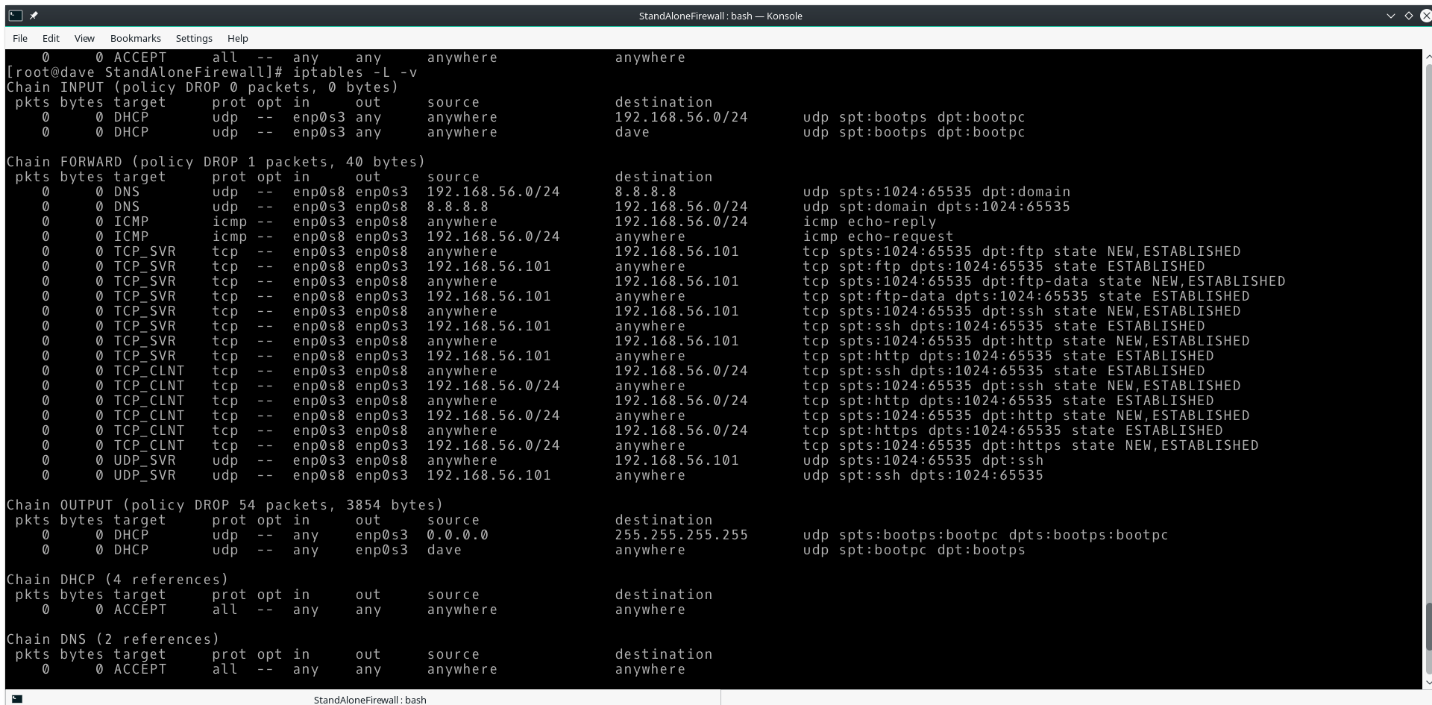
## Fig 9: Drop all Packets with SYN/FIN bit set





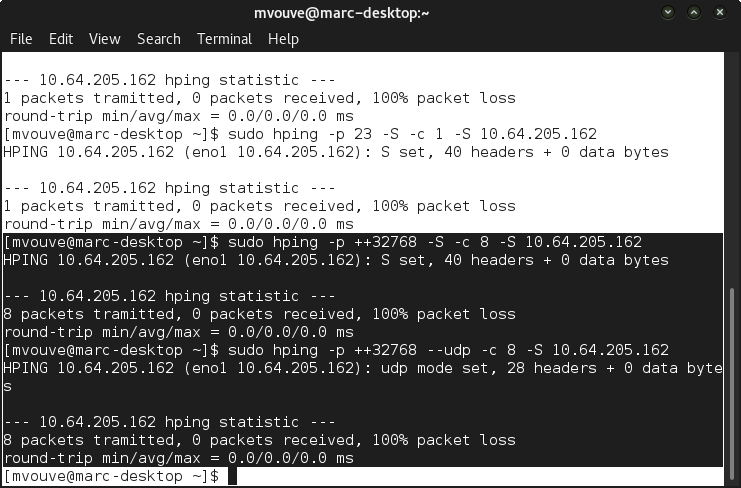
## Fig 10: Do not not allow Telnet packets at all

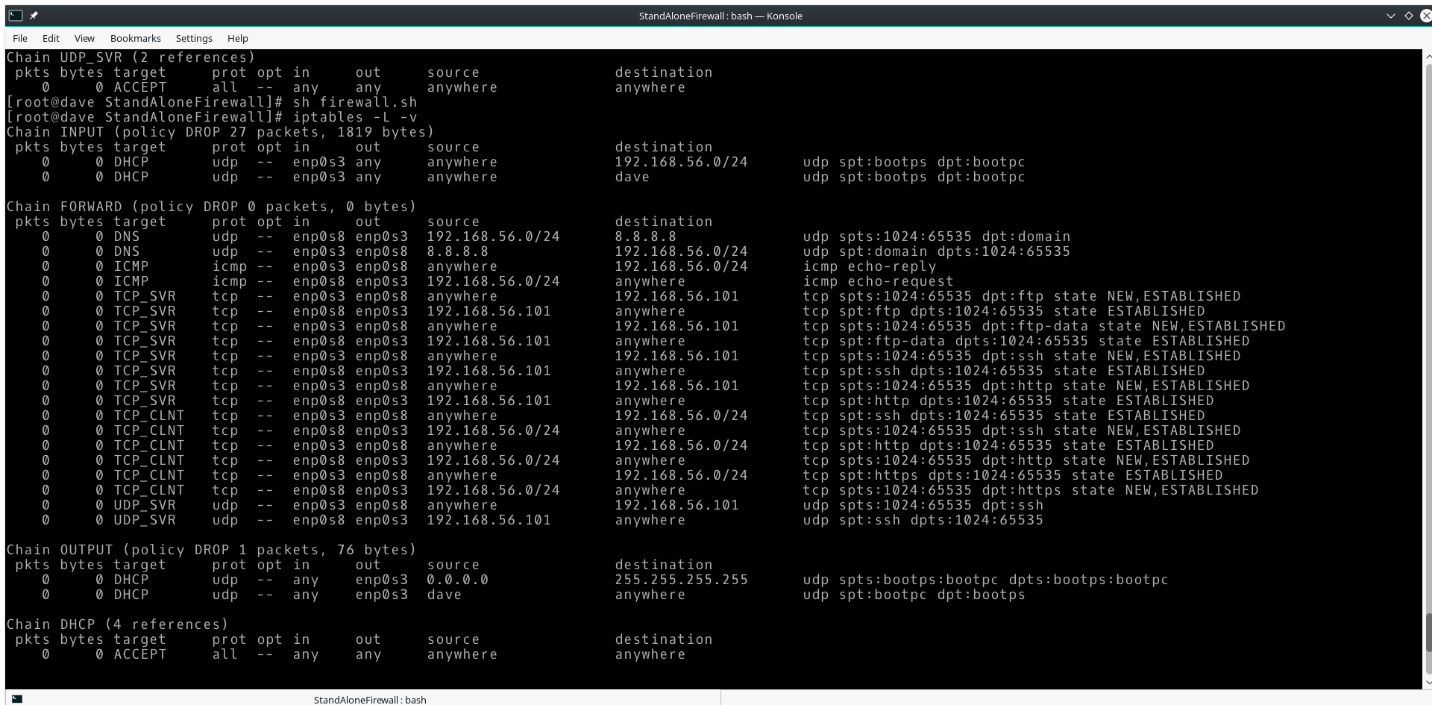




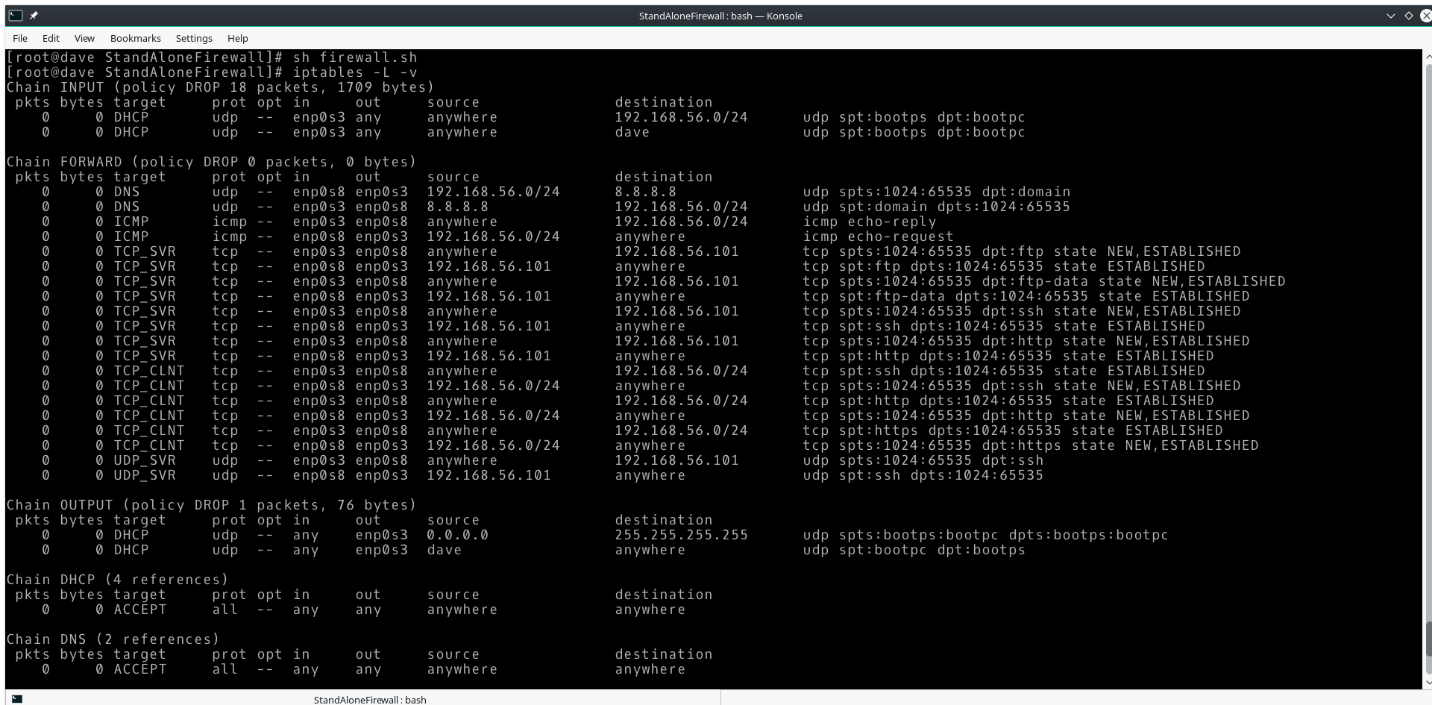
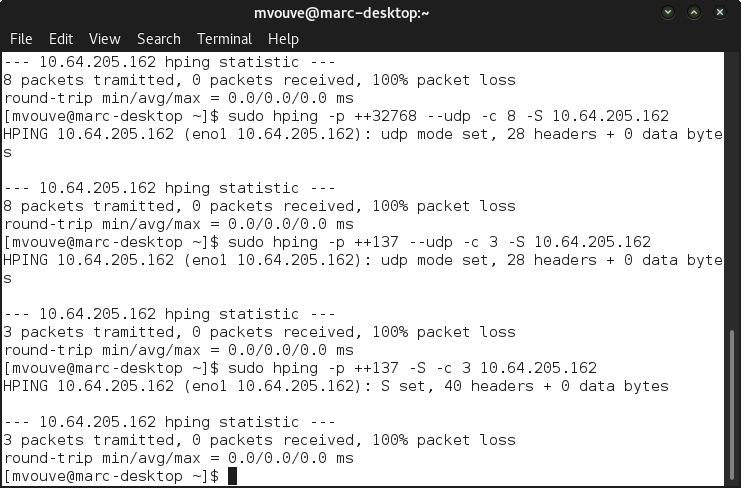
## Fig 11: Block all on ports 32768-32775, 137 – 139 TCP 111 and 515

### 32768-32775

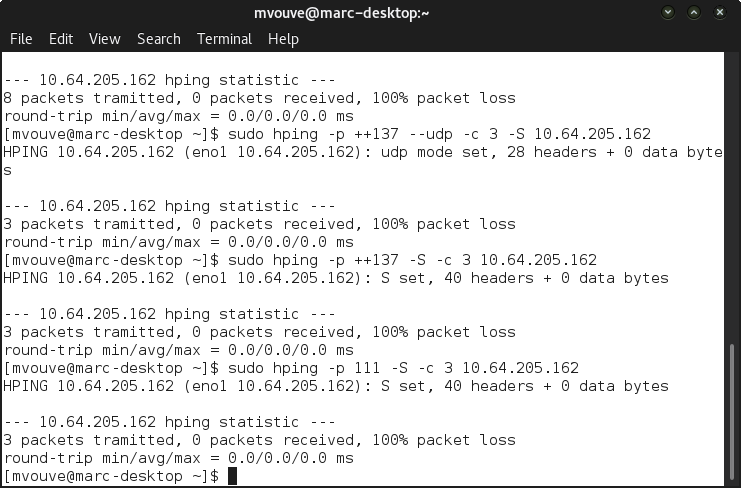


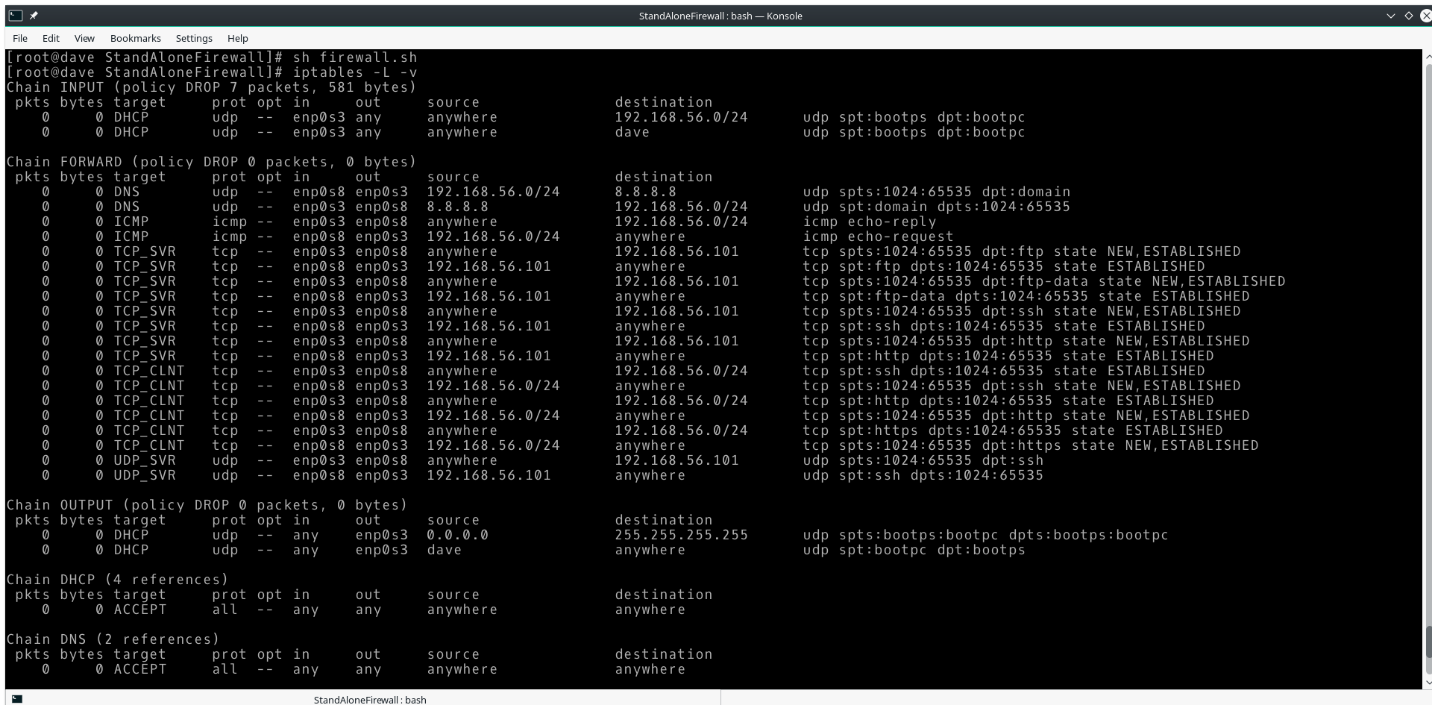


### 137-139

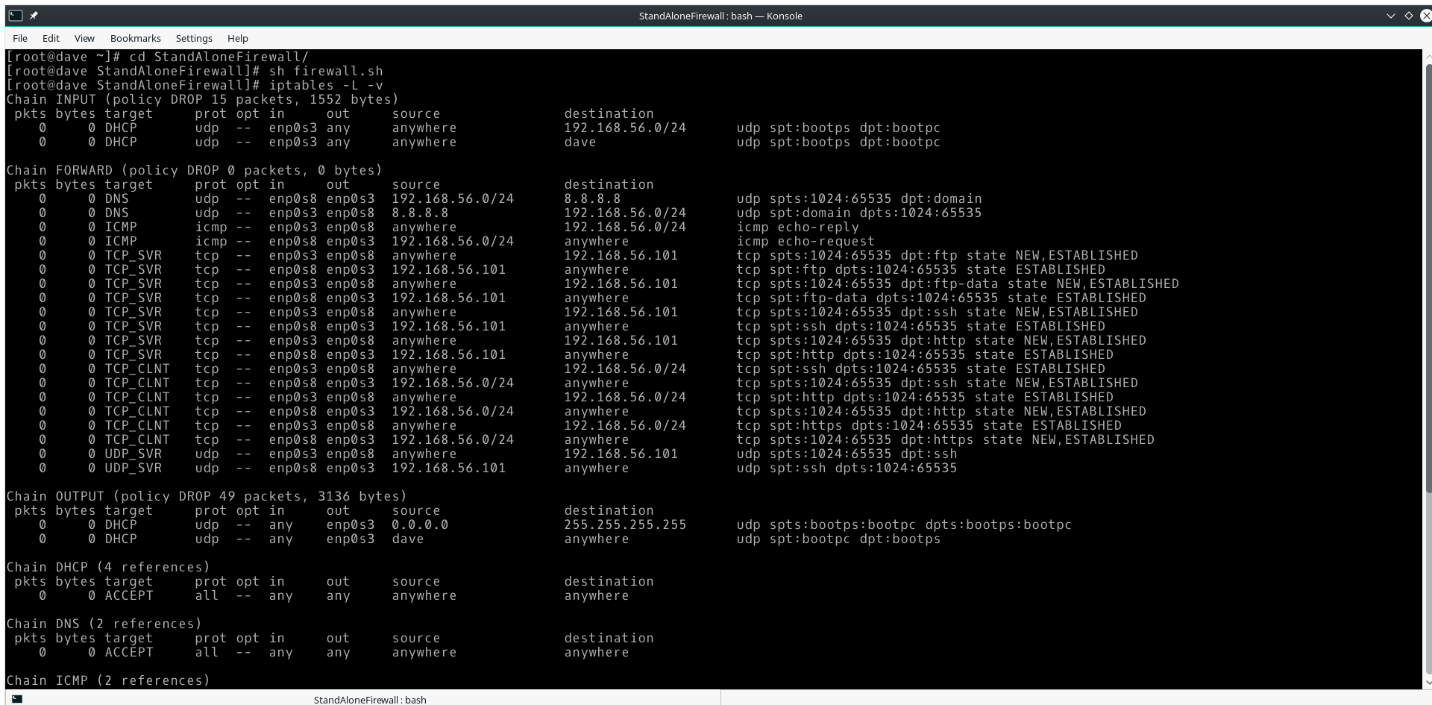
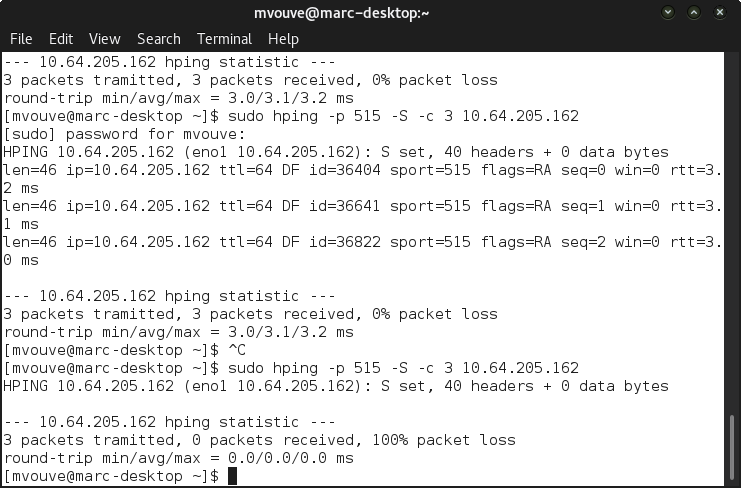


### 111





### 515



## Fig 12: For FTP and SSH set control connections to minimum delay and maximum throughput for data.

