

Testing:

The testing during the implementation of the script was not documented. After completion it was tested using some applications from a phone. The test script for hping testing has its results on a text document in the folder.

TEST LIST

Test #	Test Description / Tool Used	Excepted Result	Pass / Fail	Figure
1	Verify that pinging types 0 and 8 work inbound/ freeping	Ports should be open	Pass	Fig 1
2	Verify that pinging types 0 and 8 work outbound / ping	Ping should be Succesful	Pass	Fig 2
3	Test for Inbound ssh / serverauditor	Firewall should allow it and connect	Pass	Fig 3
4	Test for Outbound ssh packets / ssh	Firewall should allow it	Pass	Fig 4
5	Test for Inbound http / safari	Firewall should allow it	Pass	Fig 5
6	Test for outbound http/https / browser	Firewall should allow it	Pass	Fig 6
7	Test for Inbound pinging (firewall blocked)/ freeping	Firewall should drop it	Pass	Fig 7
8	Test for Inbound ssh(firewall blocked) / serverauditor	Firewall should drop it	Pass	Fig 8
9	Test for Inbound http(firewall blocked) / safari	Firewall should drop it	Pass	Fig 9
10	Test for Inbound/Outbound DNS / browser	It should resolve address	Pass	Fig 6
11	Check for Accounting of the chain / verbose mode	It should show all the total transfer during the test	Pass	Fig 10
12	Check GUI for chains and accounting / GUI	It should show the chain and counts for each	Pass	Fig 11
13	Check GUI for changes applied / GUI	New Rule should be on top	Pass	Fig 12

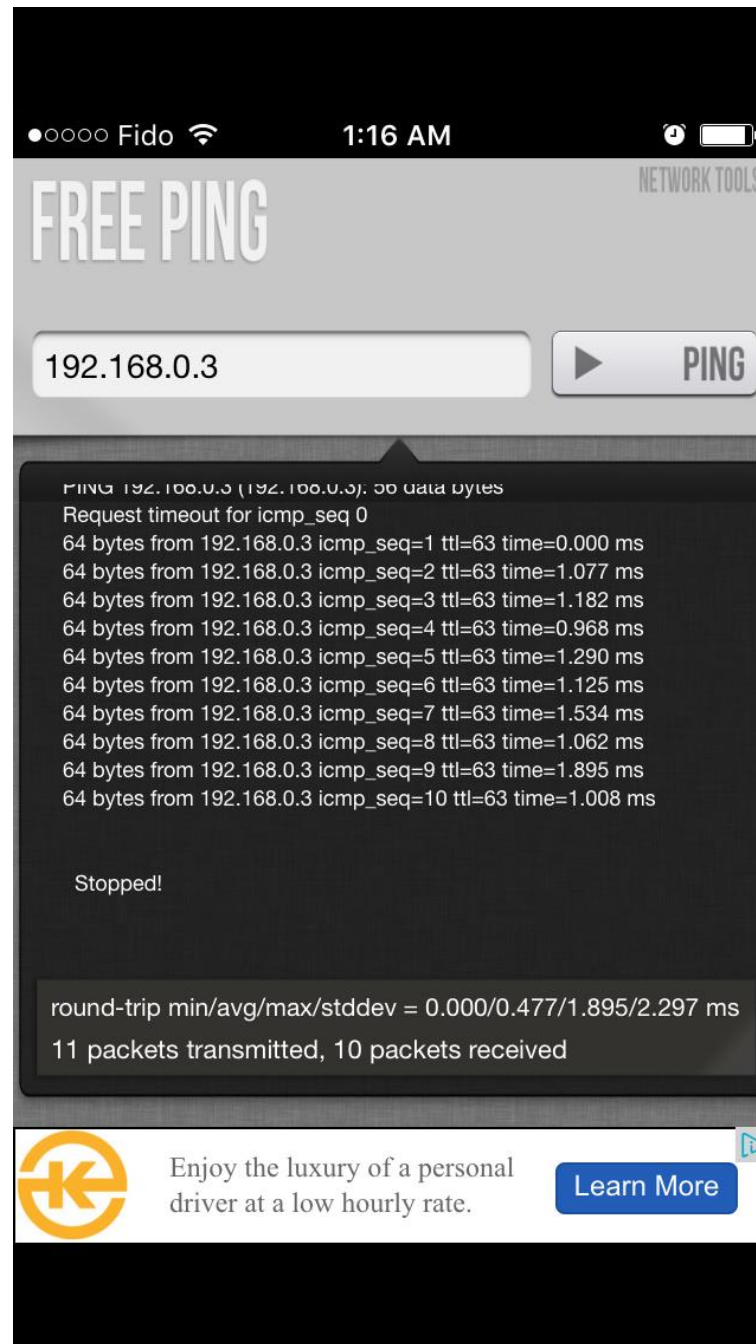


Figure 1

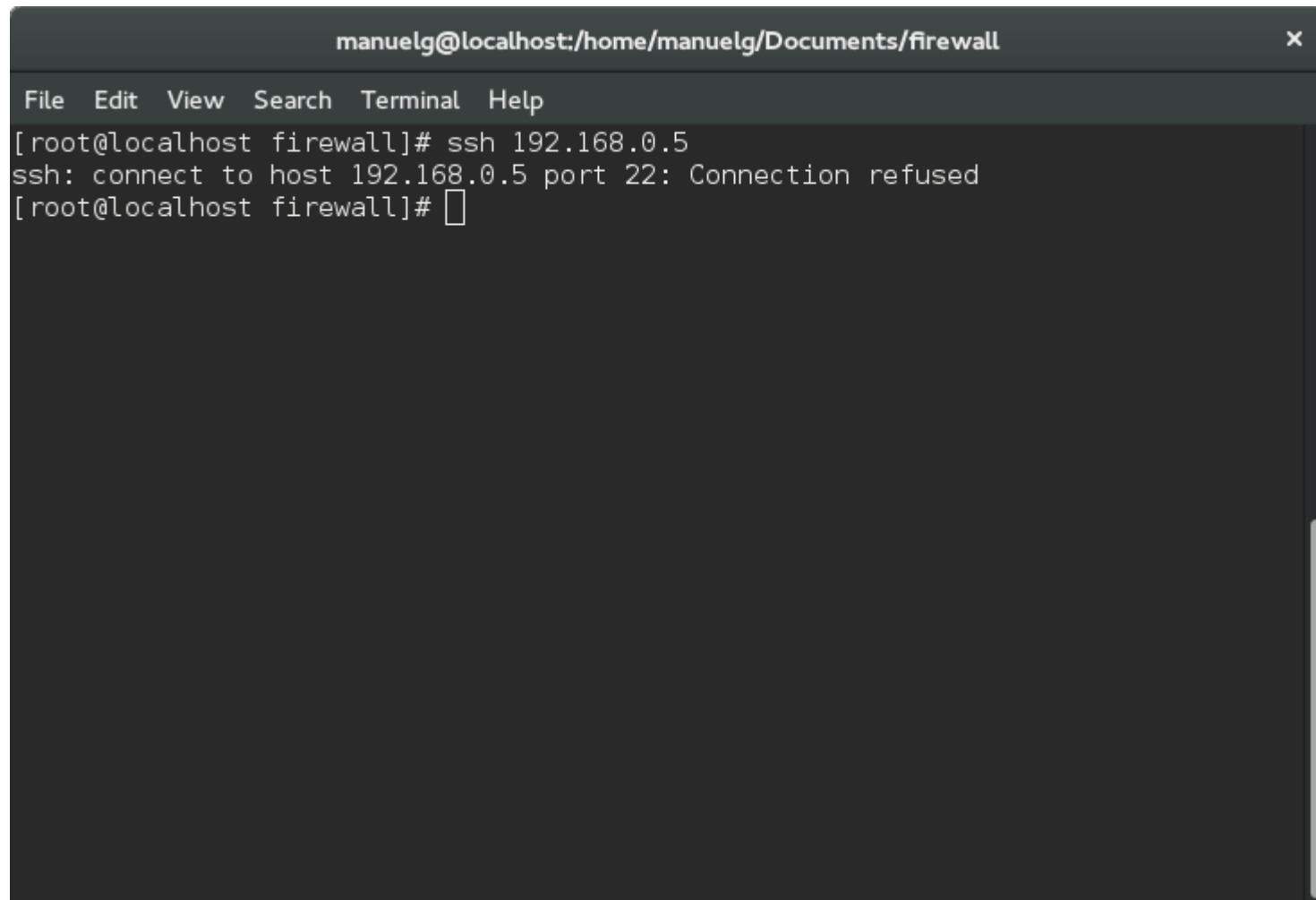
```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=17.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=15.9 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 15.977/17.478/18.225/0.898 ms
[root@localhost firewall]#
```

Figure 2

```
Last login: Thu Feb  4 01:17:19 2016 from 192.168.0.5
[root@localhost ~]# cd Documents/
[root@localhost Documents]# ls
[root@localhost Documents]# cs /home/manuelg/Documents/firewall/
bash: cs: command not found...
Similar commands are::
'ss'
'cc'
[root@localhost Documents]# cd /home/manuelg/Documents/firewall/
[root@localhost firewall]# ls
firewall.sh gateway.sh host.sh
[root@localhost firewall]#
```



Figure 3

A terminal window titled 'manuelg@localhost:/home/manuelg/Documents/firewall' with a close button in the top right corner. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows a root user at localhost in the 'firewall' directory attempting to connect via SSH to 192.168.0.5. The connection is refused, and the prompt returns to the root user.

```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# ssh 192.168.0.5
ssh: connect to host 192.168.0.5 port 22: Connection refused
[root@localhost firewall]#
```

Figure 4

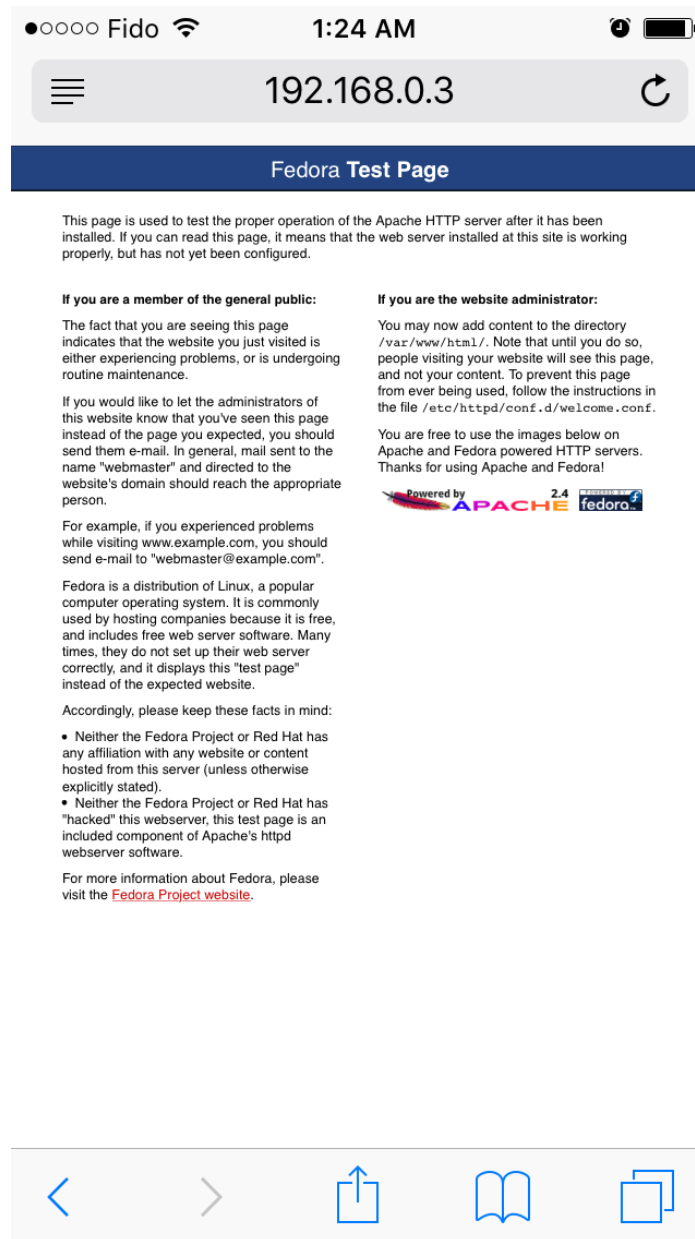


Figure 5

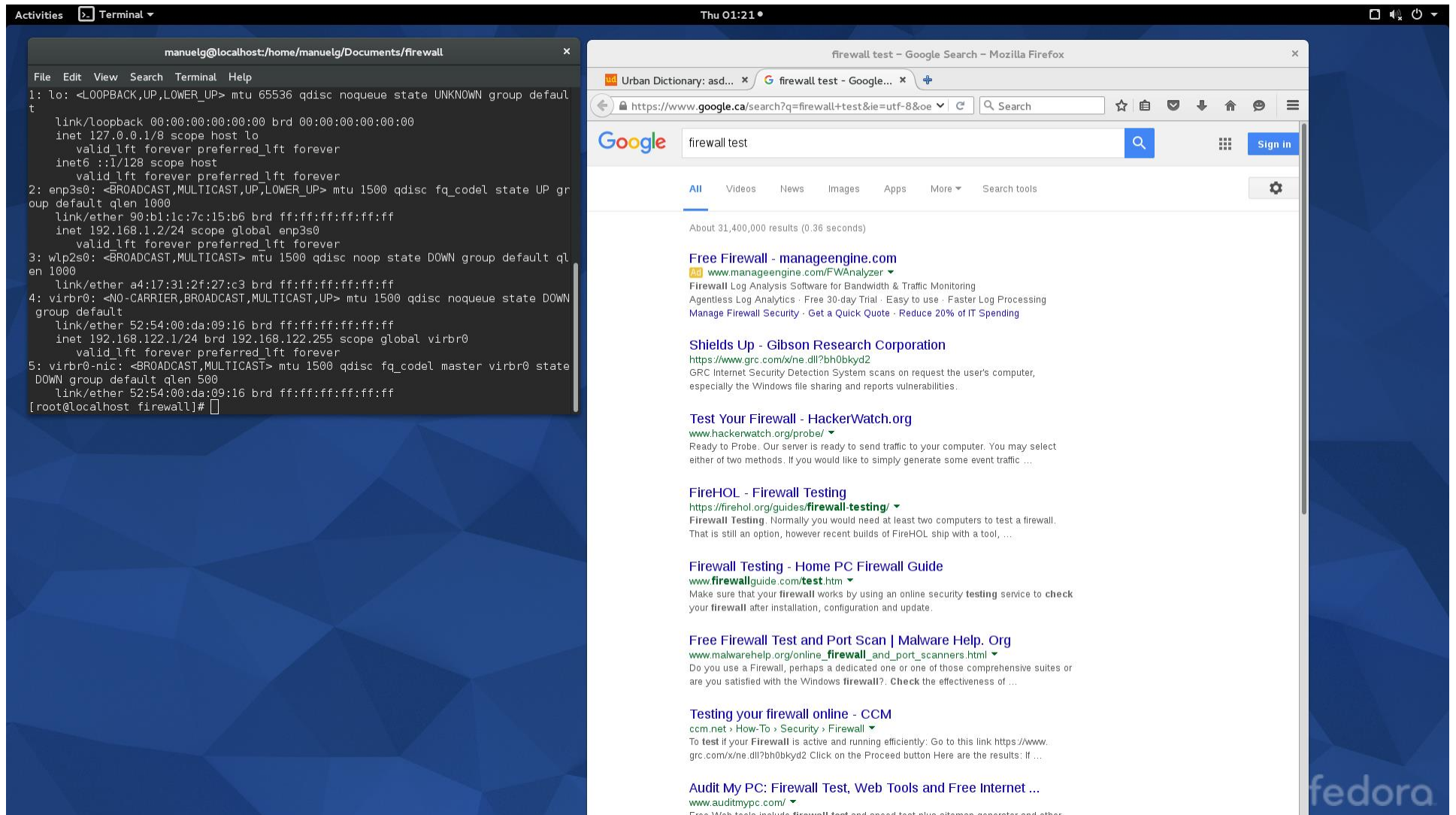


Figure 6

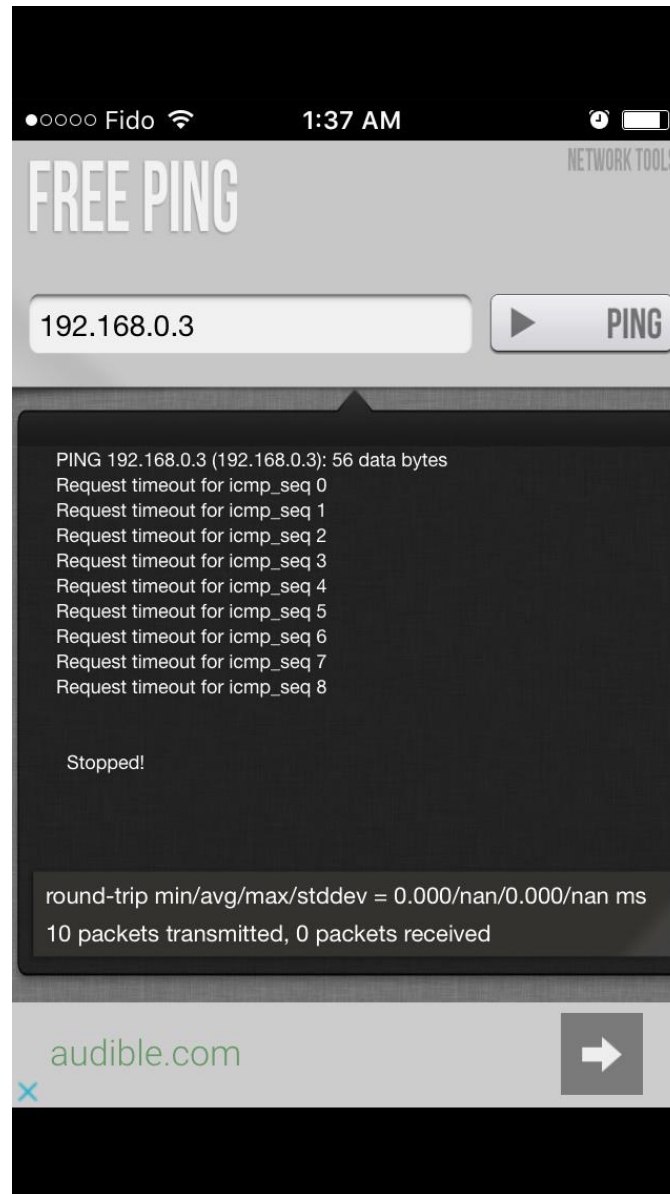


Figure 7

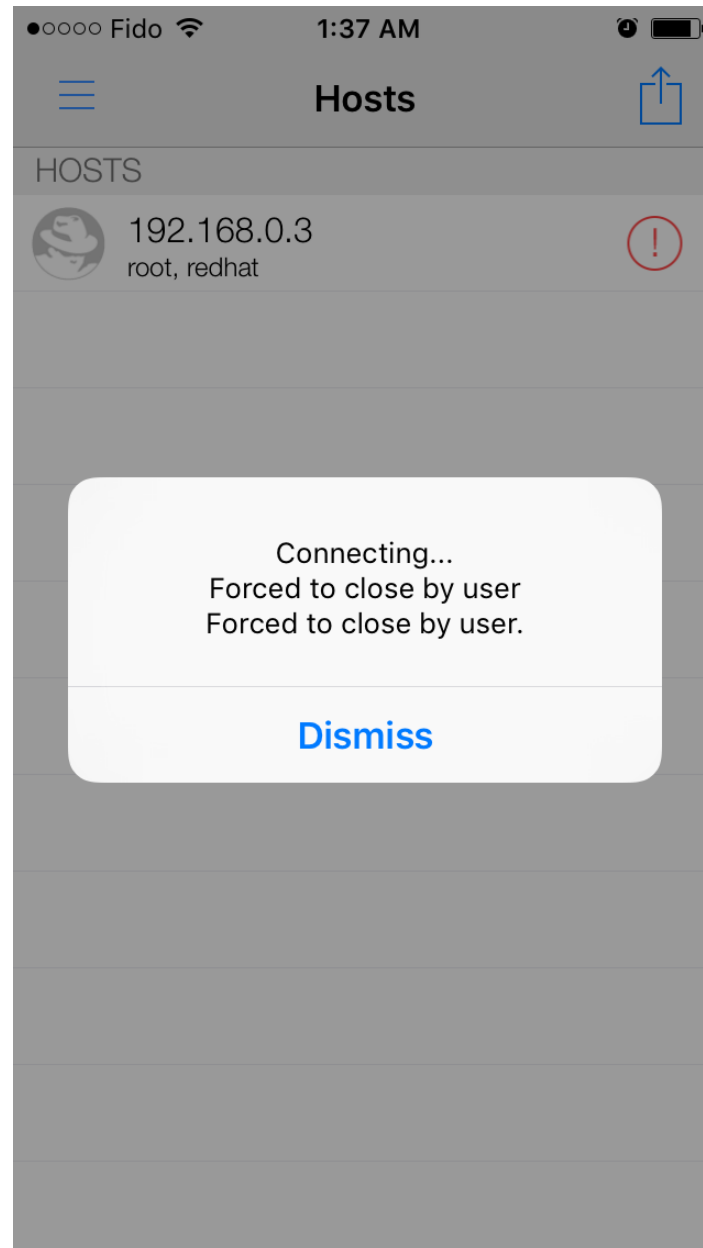
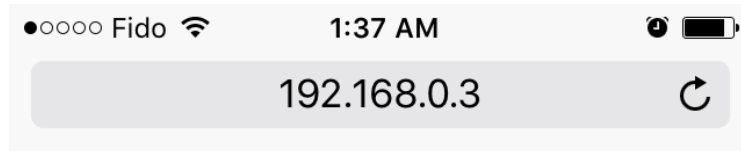


Figure 8



Safari could not open the page because the server stopped responding.



Figure 9

```
manuelg@localhost:/home/manuelg/Documents/fire
File Edit View Search Terminal Help
[root@localhost fire]# iptables -L -vxn
Chain INPUT (policy DROP 80 packets, 2798 bytes)
  pkts    bytes target     prot opt in     out     source            destination
Chain FORWARD (policy DROP 9 packets, 648 bytes)
  pkts    bytes target     prot opt in     out     source            destination
  0        0 DROP      all  --  wlp8s0 *      192.168.1.2      0.0.0.0/0
  0        0 DROP      tcp  --  *      *      0.0.0.0/0         0.0.0.0/0         multiport dports 1024:65535 tcp flags:0x3F/0x02
  0        0 DROP      tcp  --  *      *      0.0.0.0/0         0.0.0.0/0         tcp flags:0x3F/0x03
  0        0 DROP      tcp  --  *      *      0.0.0.0/0         0.0.0.0/0         tcp flags:0x3F/0x3F
  0        0 ACCEPT    all  -f  *      *      0.0.0.0/0         192.168.1.2
441      36182 ACCEPT    tcp  --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         state NEW,ESTABLISHED tcp dpt:22
263      32126 ACCEPT    tcp  --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         state ESTABLISHED tcp spt:22
44       10296 ACCEPT    tcp  --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         state ESTABLISHED tcp spt:80
58       6027  ACCEPT    tcp  --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         state NEW,ESTABLISHED tcp dpt:80
583     692414 ACCEPT    tcp  --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         state ESTABLISHED tcp spt:443
608     89890  ACCEPT    tcp  --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         state NEW,ESTABLISHED tcp dpt:443
2        80  ACCEPT    tcp  --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         state ESTABLISHED tcp spt:22
2       120  ACCEPT    tcp  --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         state NEW,ESTABLISHED tcp dpt:22
0        0  ACCEPT    udp  --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         state NEW,ESTABLISHED udp dpt:53
0        0  ACCEPT    udp  --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         state ESTABLISHED udp spt:53
55     6359  ACCEPT    udp  --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         state ESTABLISHED udp spt:53
55     3509  ACCEPT    udp  --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         state NEW,ESTABLISHED udp dpt:53
10       840  ACCEPT    icmp --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         icmp type 8
13     1092  ACCEPT    icmp --  wlp8s0 enp7s0 0.0.0.0/0         0.0.0.0/0         icmp type 0
13     1092  ACCEPT    icmp --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         icmp type 8
10       840  ACCEPT    icmp --  enp7s0 wlp8s0 0.0.0.0/0         0.0.0.0/0         icmp type 0
Chain OUTPUT (policy DROP 18 packets, 3076 bytes)
  pkts    bytes target     prot opt in     out     source            destination
[root@localhost fire]#
```

Figure 10

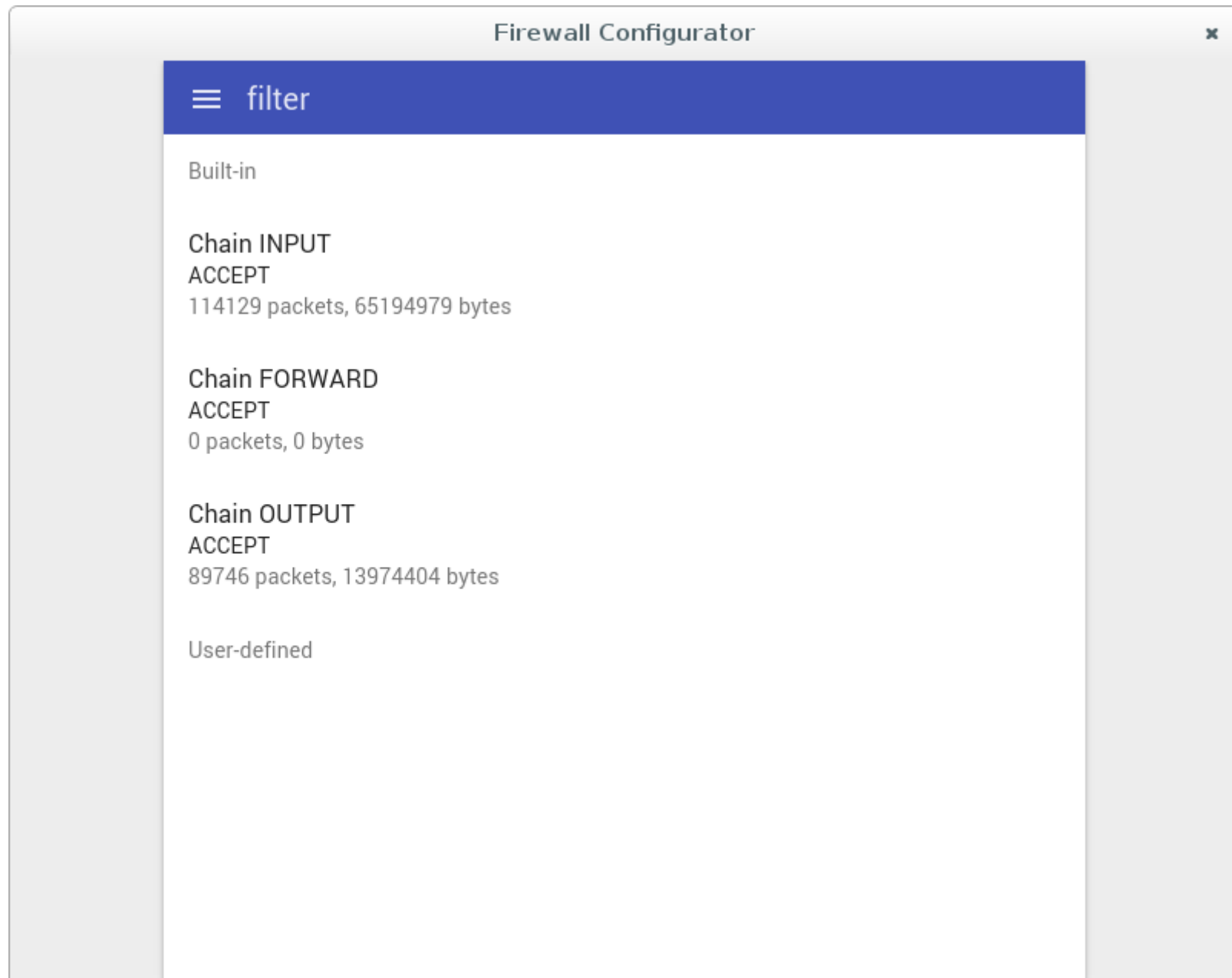


Figure 11

Firewall Configurator

← FORWARD



Policy

ACCEPT

New Rule

Note: Rules are appended to the top of the rules list.

Direction	Protocol	Port No.	Permission
Inbound ▼	TCP ▼	23 ▼	Allow ▼
IP Address	Network Interface	Gateway Interface	
192.168.1.1	eth0	wlan0	

CLEAR

CREATE

Rules

-A FORWARD -p tcp --dport 23 -m state --state NEW,ESTABLISHED -i wlan0 -o

New rule created

Figure 12