

Firewall Script Guide

The script has 2 modes “reset” or “set”

By executing it as `./firewall reset`. It would flush all the tables and set the default policies back to ACCEPT.

By executing it as `./firewall set`. It would set all the specified changes from the user defined fields into its respective tables.

The user Defined Fields looks like this:

```
*F:\fire\firewall.sh - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
firewall.sh
4 # Author : Manuel Gonzales
5 # Date : Feb 02, 2016
6 # Script to set up the gateway firewall
7
8 #####
9 #USER DEFINED VARIABLES
10
11 #UTILITY PATH
12 IPT="iptables"
13
14 #CURRENT NETWORK INTERFACE
15 NETWORK_INTERFACE="wlp8s0"
16
17 #FIREWALL GATEWAY INTERFACE
18 GATEWAY_INTERFACE="enp7s0"
19
20 #CLIENT IP ADDRESS
21 CLIENT_IP_ADDR="192.168.1.2"
22
23 #GATEWAY IP ADDRESS
24 IP_ADDR="192.168.1.1"
25
26 #NETWORK SUBNET
27 NET_SUBNET_ADDR="192.168.0.0/24"
28 GATE_SUBNET_ADDR="192.168.0.0/24"
length: 5010 lines: 150 Ln: 9 Col: 14 Sel: 0|0 UNIX ANSI as UTF-8 INS
```

IPT – stands for the tool used and its path. In this example the tool to use is **iptables** and the path is already part of the environment.

Network Interface – The name of the interface that is connected to the internet **wlp8s0** in this case when a wireless interface was used.

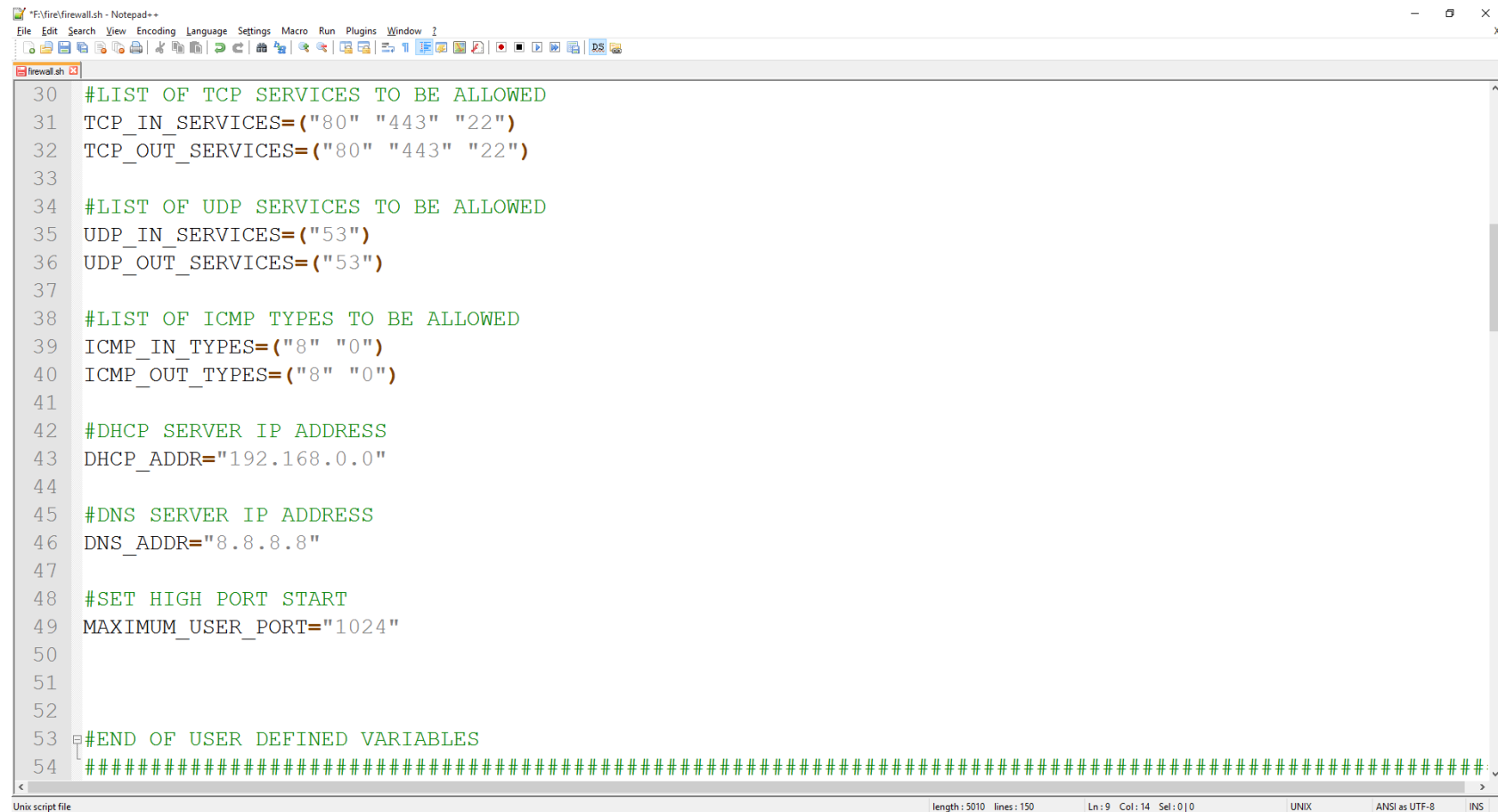
Gateway Interface - The name of the interface that is connected to the client **enp7s0** in this case connected in Ethernet

Client IP address - The IP address of the firewall client **192.168.1.2** in this example. Used for port post-routing and pre-routing

IP address- The IP address of the firewall in the gateway interface **192.168.1.1** in this example

Net subnet address- The subnet and its mask for the network interface.

Gate subnet address- The subnet and its mask for the gateway interface.



```
*F:\fire\firewall.sh - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
firewall.sh
30 #LIST OF TCP SERVICES TO BE ALLOWED
31 TCP_IN_SERVICES=("80" "443" "22")
32 TCP_OUT_SERVICES=("80" "443" "22")
33
34 #LIST OF UDP SERVICES TO BE ALLOWED
35 UDP_IN_SERVICES=("53")
36 UDP_OUT_SERVICES=("53")
37
38 #LIST OF ICMP TYPES TO BE ALLOWED
39 ICMP_IN_TYPES=("8" "0")
40 ICMP_OUT_TYPES=("8" "0")
41
42 #DHCP SERVER IP ADDRESS
43 DHCP_ADDR="192.168.0.0"
44
45 #DNS SERVER IP ADDRESS
46 DNS_ADDR="8.8.8.8"
47
48 #SET HIGH PORT START
49 MAXIMUM_USER_PORT="1024"
50
51
52
53 #END OF USER DEFINED VARIABLES
54 #####
Unix script file length: 5010 lines: 150 Ln: 9 Col: 14 Sel: 0 | 0 UNIX ANSI as UTF-8 INS
```

For the following the services need to be added into the “()” inside quotes (“”) and separated by single spaces.

TCP in services- The TCP services/ports that should be open for inbound connections.

TCP out services- The TCP service/ports that should be open for outbound connections.

UDP in services- The UDP services/ports that should be open for inbound connections.

UDP out services- The UDP services/ports that should be open for outbound connections.

ICMP in types- The type that should be accepted for inbound connections.

ICMP out types- The type that should be accepted for outbound connections.

DHCP address- IP address of the DHCP server

DNS address- IP address of the DNS server

Maximum User Port- The highest allowed port for common services, any port higher than this would be blocked from incoming traffic.