```
#!/bin/bash

# Usage:
#   $ source my_firewall.sh
#   $ fw_start_and_open_our_services

EXTIF=eth2

# Enable/disable routing (1 => enable, 0 => disable). By default enable it.
function set_routing {
 local DEFAULT=1
 echo ${1:-$DEFAULT} > /proc/sys/net/ipv4/ip_forward
}

# Uncomment the following two lines to print the commands that would be executed, without executing them (for
debugging):
#function iptables    { echo iptables "$@"; }
#function set_routing { echo set_routing "$@"; }

function fw_stop {
 # Disable routing:
 set_routing 0

 # Clean tables:
 iptables -t filter -F
 iptables -t nat -F

 # Restore policies (if needed):
 iptables -P FORWARD ACCEPT
 iptables -P INPUT ACCEPT
}

function fw_start {
 # Start from a clean state:
 fw_stop

 # Activate routing:
 set_routing 1

 # Activate SNAT:
 iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

 # Policies:
 iptables -P FORWARD ACCEPT
 iptables -P INPUT ACCEPT

 # Stop initiatives from the external interface:
 iptables -A FORWARD -i $EXTIF -m state --state NEW -j DROP
 iptables -A INPUT   -i $EXTIF -m state --state NEW -j DROP

}

# Examples:
#
#   fw_open_port tcp 22
#   fw_open_port tcp 22 192.168.1.2
#   fw_open_port tcp 22 192.168.1.2 50022
#
function fw_open_port {
 local PROTOCOL=$1
 local PORT=$2
 local SERVER=$3
 local SERVER_PORT=${4:-$PORT}

 if [[ -n $SERVER ]]; then
   iptables -I FORWARD 1 -i $EXTIF -p $PROTOCOL --dport $PORT -d $SERVER -j ACCEPT
   iptables -t nat -A PREROUTING -i $EXTIF -p $PROTOCOL --dport $PORT -j DNAT --to $SERVER:$SERVER_PORT
 else
   # SERVER is undefined => open the port on the router itself (INPUT):
```

```
   iptables -I INPUT 1 -i $EXTIF -p $PROTOCOL --dport $PORT -j ACCEPT
 fi
}

function fw_close_port {
 local PROTOCOL=$1
 local PORT=$2
 local SERVER=$3
 local SERVER_PORT=${4:-$PORT}

 if [[ -n $SERVER ]]; then
   iptables -D FORWARD -i $EXTIF -p $PROTOCOL --dport $PORT -d $SERVER -j ACCEPT
   iptables -t nat -D PREROUTING -i $EXTIF -p $PROTOCOL --dport $PORT -j DNAT --to $SERVER:$SERVER_PORT
 else
   # SERVER is undefined => open the port on the router itself (INPUT):
   iptables -D INPUT -i $EXTIF -p $PROTOCOL --dport $PORT -j ACCEPT
 fi
}

# MAIN: our rules
function fw_start_and_open_our_services {

 # Basic rules:
 fw_start

 # open HTTP/m1
 fw_open_port tcp 80 192.168.1.2

 # open SSH/m3
 fw_open_port tcp 22 10.0.0.3

}
```