Firewall iptables script

```
# Interfaces
WAN="ens3"
LAN="ens9"

#ifconfig $LAN up
#ifconfig $LAN 192.168.1.1 netmask 255.255.255.0

echo 1 > /proc/sys/net/ipv4/ip_forward
sysctl -w net.ipv4.ip_forward=1

iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -X

# Default to drop packets
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Allow all local loopback traffic
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Allow output on $WAN and $LAN if. Allow input on $LAN if.
iptables -A INPUT -i $LAN -j ACCEPT
iptables -A OUTPUT -o $WAN -j ACCEPT
iptables -A OUTPUT -o $LAN -j ACCEPT

iptables -A INPUT -p tcp -i $WAN --dport 22 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -o $LAN -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -i $LAN -o $WAN -j ACCEPT
iptables -t nat -A POSTROUTING -o $WAN -j MASQUERADE
```

```
# Allow ICMP echo reply/echo request/destination unreachable/time exceeded
iptables -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
iptables -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT


# WWW
iptables -t nat -A PREROUTING -p tcp -i $WAN -m multiport --dports 80,443 -j DNAT --to 10.1.1.11
iptables -A FORWARD -p tcp -i $WAN -o $LAN -d 10.1.1.11 -m multiport --dports 80,443 -j ACCEPT


exit 0 #report success
```