Basic iptables router & firewall in Linux (Ubuntu)

Below is a simple script that I wrote when I was at University; it formed part of my dissertation.

The script allows a Linux box with 2 network interfaces to function as a router/firewall appliance, which is always handy to know how to do. This script is ready to go, all that needs to be changed is the interface definitions and a single line adding to /etc/sysctl.conf.

Hope it helps someone out:

```
 #!/bin/bash
#
#
#
# EXTIF - WAN Interface
# INTIF - LAN Interface
#
#
#
# Need to add net.ipv4.ip_forward=1 to /etc/sysctl.conf
# to allow iptables to work
#
```

```
# Define network interfaces
EXTIF="eth0"
INTIF="eth2"
#
# Flushing out existing iptables entries
iptables -P INPUT ACCEPT
iptables -F INPUT
iptables -P OUTPUT ACCEPT
iptables -F OUTPUT
iptables -P FORWARD DROP
iptables -F FORWARD
iptables -t nat -F
#
# Allow all outbound traffic and only allow established and related connections back in
iptables -A FORWARD -i $EXTIF -o $INTIF -m state --state ESTABLISHED, RELATED -j
ACCEPT
iptables -A FORWARD -i $INTIF -o $EXTIF -j ACCEPT
iptables -A FORWARD -j LOG
#
# Masquerade NAT functionality on $EXTIF
iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE
#
# Allows ssh inbound connections
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
#
# Allows lo interface to work
iptables -A INPUT -i lo -j ACCEPT
#
# Default DROP
iptables -A INPUT -i $EXTIF -j DROP
```