```
#!/bin/sh
#
######################################################################
#
#   Name:           ddos_protection_my_build.sh
#   Author:         Chris Fedun 17/02/2017
#   Description:    IPTABLES DDoS Configuration for Call Manager
#   Based on:       https://javapipe.com/iptables-ddos-protection
#
#   Copyright (C) 2017  Christopher Fedun
#
#   This program is free software: you can redistribute it and/or modify
#   it under the terms of the GNU General Public License as published by
#   the Free Software Foundation, either version 3 of the License, or
#   (at your option) any later version.
#
#   This program is distributed in the hope that it will be useful,
#   but WITHOUT ANY WARRANTY; without even the implied warranty of
#   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#   GNU General Public License for more details.
#
#   You should have received a copy of the GNU General Public License
#   along with this program.  If not, see <http://www.gnu.org/licenses/>.
######################################################################
#####Constants#####
IPTABLES=/sbin/iptables
IP6TABLES=/sbin/ip6tables
MODPROBE=/sbin/modprobe
#INT_NET=192.168.10.0/24
IFACE_INT=eth1
IFACE_EXT=eth0
#DNS_SVR_IP=192.168.10.253
#WEB_SVR_IP=192.168.10.253
#EMAIL_SVR_IP=192.168.10.253
#CALL_MANAGER_IP=192.168.10.252
Setup_dir='/root/initial_setup/'


### 1: Drop invalid packets ###
$IPTABLES -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j LOG_DROP

### 2: Drop TCP packets that are new and are not SYN ###
$IPTABLES -t mangle -A PREROUTING -p tcp ! --syn -m conntrack --ctstate NEW -j LOG_DROP

### 3: Drop SYN packets with suspicious MSS value ###
$IPTABLES -t mangle -A PREROUTING -p tcp -m conntrack --ctstate NEW -m tcpmss ! --mss 536:65535
-j LOG_DROP

### 4: Block packets with bogus TCP flags ###
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN FIN,SYN -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags SYN,RST SYN,RST -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags SYN,FIN SYN,FIN -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags FIN,RST FIN,RST -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags FIN,ACK FIN -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ACK,URG URG -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ACK,FIN FIN -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ACK,PSH PSH -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ALL ALL -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ALL NONE -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ALL FIN,PSH,URG -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j LOG_DROP

### 5: Block spoofed packets ### ### CAUTION! MAY DISRUPT VPN ###
$IPTABLES -t mangle -A PREROUTING -s 224.0.0.0/3 ! -i $IFACE_INT -j LOG_DROP
```

```
$IPTABLES -t mangle -A PREROUTING -s 169.254.0.0/16 ! -i $IFACE_INT -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -s 172.16.0.0/12 ! -i $IFACE_INT -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -s 192.0.2.0/24 ! -i $IFACE_INT -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -s 192.168.0.0/16 ! -i $IFACE_INT -j LOG_DROP
#$IPTABLES -t mangle -A PREROUTING -s 10.0.0.0/8 ! -i $IFACE_INT -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -s 0.0.0.0/8 ! -i $IFACE_INT -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -s 240.0.0.0/5 ! -i $IFACE_INT -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -s 127.0.0.0/8 ! -i lo -j LOG_DROP

### 6: Drop ICMP (you usually don't need this protocol)  Limit Really ###
$IPTABLES -t mangle -A PREROUTING -p icmp -m icmp --icmp-type address-mask-request -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p icmp -m icmp --icmp-type timestamp-request -j LOG_DROP
$IPTABLES -t mangle -A PREROUTING -p icmp -m icmp --icmp-type 8 -m limit --limit 1/second -j
ACCEPT
$IPTABLES -t mangle -A PREROUTING -p icmp -j LOG_DROP

### 7: Drop fragments in all chains ### ### DO NOT USE IF USING VPN ###
#$IPTABLES -t mangle -A PREROUTING -f -j LOG_DROP

### 8: Limit connections per source IP ###
$IPTABLES -A INPUT -p tcp -m connlimit --connlimit-above 111 -j REJECT --reject-with tcp-reset

### 9: Limit RST packets ###
$IPTABLES -A INPUT -p tcp --tcp-flags RST RST -m limit --limit 2/s --limit-burst 2 -j ACCEPT
$IPTABLES -A INPUT -p tcp --tcp-flags RST RST -j LOG_DROP

### 10: Limit new TCP connections per second per source IP ###
$IPTABLES -A INPUT -p tcp -m conntrack --ctstate NEW -m limit --limit 60/s --limit-burst 20 -j
ACCEPT
$IPTABLES -A INPUT -p tcp -m conntrack --ctstate NEW -j LOG_DROP

### 11: Use SYNPROXY on all ports (disables connection limiting rule) ###
#$IPTABLES -t raw -A PREROUTING -p tcp -m tcp --syn -j CT --notrack
#$IPTABLES -A INPUT -p tcp -m tcp -m conntrack --ctstate INVALID,UNTRACKED -j SYNPROXY
--sack-perm --timestamp --wscale 7 --mss 1460
#$IPTABLES -A INPUT -m conntrack --ctstate INVALID -j LOG_DROP

### SSH brute-force protection ###
$IPTABLES -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --set
$IPTABLES -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --update --seconds 60
 --hitcount 10 -j LOG_DROP

### Protection against port scanning ###
$IPTABLES -N port-scanning
$IPTABLES -A port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s --
limit-burst 2 -j RETURN
$IPTABLES -A port-scanning -j LOG --log-prefix "DROP Port-Scanning" --log-tcp-options --
log-ip-options
$IPTABLES -A port-scanning -j DROP
$IPTABLES -A INPUT -j port-scanning

exit
#######END :) #######
```