Subject: *SOLVED * iptables apf moblock veth0
Posted by locutius on Thu, 20 Mar 2008 11:29:00 GMT
View Forum Message <> Reply to Message

i have moblock installed in the HN and apf installed in a CT

this is my moblock start script for a non-OpenVZ kernel

please, how to add veth0 to the start script to make iptables in the HN filter packets for the CT?

```
#!/bin/sh
#
# MoBlock.sh - MoBlock start script
# --------------------------------

ACTIVATE_CHAINS=1
WHITE_TCP_IN=""
WHITE_UDP_IN=""
WHITE_TCP_OUT=""
WHITE_UDP_OUT=""
WHITE_TCP_FORWARD=""
WHITE_UDP_FORWARD=""


PIDF=/var/run/moblock.pid

FNAME=`basename $0 .sh`
MODE=`echo $FNAME|awk -F-  '{print $2}'`

if [ -f $PIDF  ]; then
 PID=`cat $PIDF`
 if [ `ps -p $PID|wc -l` -gt 1 ]; then
  echo "$0: $PIDF exists and processs seems to be running. Exiting."
  exit 1;
 fi;
fi;

if [ $MODE == "ipq" ]; then
 modprobe ip_queue
 TARGET="QUEUE"
elif [ $MODE == "nfq" ]; then
 modprobe ipt_NFQUEUE
 TARGET="NFQUEUE"
fi;

modprobe ipt_state
```

```
# Filter all traffic, edit for your needs

iptables -N MOBLOCK_IN
iptables -N MOBLOCK_OUT
iptables -N MOBLOCK_FW

if [ $ACTIVATE_CHAINS -eq 1 ]; then
 iptables -I INPUT -p all -m state --state NEW -j MOBLOCK_IN
 iptables -I OUTPUT -p all -m state --state NEW -j MOBLOCK_OUT
 iptables -I FORWARD -p all -m state --state NEW -j MOBLOCK_FW
fi;


iptables -I MOBLOCK_IN -p all -j $TARGET
#iptables -I MOBLOCK_IN -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -I MOBLOCK_OUT -p all -j $TARGET
#iptables -I MOBLOCK_OUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -I MOBLOCK_FW -p all -j $TARGET
#iptables -I MOBLOCK_FW -m state --state ESTABLISHED,RELATED -j ACCEPT

for PORT in $WHITE_TCP_OUT; do
 iptables -I MOBLOCK_OUT -p tcp --dport $PORT -j ACCEPT
done
for PORT in $WHITE_UDP_OUT; do
 iptables -I MOBLOCK_OUT -p udp --dport $PORT -j ACCEPT
done

for PORT in $WHITE_TCP_IN; do
 iptables -I MOBLOCK_IN -p tcp --dport $PORT -j ACCEPT
done
for PORT in $WHITE_UDP_IN; do
 iptables -I MOBLOCK_IN -p udp --dport $PORT -j ACCEPT
done

for PORT in $WHITE_TCP_FORWARD; do
 iptables -I MOBLOCK_FW -p tcp --dport $PORT -j ACCEPT
done
for PORT in $WHITE_UDP_FORWARD; do
 iptables -I MOBLOCK_FW -p udp --dport $PORT -j ACCEPT
done


# Loopback traffic fix

iptables -I INPUT -p all -i lo -j ACCEPT
```

```
iptables -I OUTPUT -p all -o lo -j ACCEPT

# Here you can change block list and log files
./moblock -p /etc/guarding.p2p ./moblock.log

# On exit delete the rules we added

if [ $ACTIVATE_CHAINS -eq 1 ]; then
 iptables -D INPUT -p all -m state --state NEW -j MOBLOCK_IN
 iptables -D OUTPUT -p all -m state --state NEW -j MOBLOCK_OUT
 iptables -D FORWARD -p all -m state --state NEW -j MOBLOCK_FW
fi;

iptables -D INPUT -p all -i lo -j ACCEPT
iptables -D OUTPUT -p all -o lo -j ACCEPT

iptables -F MOBLOCK_IN
iptables -X MOBLOCK_IN
iptables -F MOBLOCK_OUT
iptables -X MOBLOCK_OUT
iptables -F MOBLOCK_FW
iptables -X MOBLOCK_FW

if [ -f $PIDF ]; then
 rm $PIDF;
fi
```

many thanks in advance to the network guru who knows how to add veth0 to this script