
Subject: Re: APF not logging on openVZ VE
Posted by [Vasily Tarasov](#) on Wed, 06 Jun 2007 11:52:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello,

I've just found time to check ipt_LOG module in VE. It works for me, please, look at the transcript:

```
# lsmod | grep ipt_LOG
# modprobe ipt_LOG          # !!!! Loading ipt_LOG kernel module before VE start!
# lsmod | grep ipt_LOG
ipt_LOG          8192 0
x_tables        17928 13
ipt_LOG,xt_tcpudp,xt_state,xt_length,ipt_ttl,xt_tcpmss,ipt_TCPMSS,xt_multiport,xt_limit,ipt_tos,ipt
_REJECT,ip_tables_nat,ip_tables
# cat /etc/vz/conf/4.conf | grep ipt_LOG
# cat /etc/vz/vz.conf | grep ipt_LOG
# vim /etc/vz/vz.conf # !!!! Aadding ipt_LOG to the list of available in VE
# cat /etc/vz/vz.conf | grep ipt_LOG
IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS
ipt_tcpmss ipt_ttl ipt_length ipt_state ipt_LOG"
# vzctl start 4
Starting VE ...
VE is mounted
Adding IP address(es): 10.0.1.2
Setting CPU units: 1000
Setting devices
File resolv.conf was modified
VE start in progress...
# vzctl enter 4
entered into VE 4
# dmesg
# iptables -A OUTPUT -j LOG
# echo $?
0
# ping mail.ru
PING mail.ru (194.67.57.126) 56(84) bytes of data.
64 bytes from mail.ru (194.67.57.126): icmp_seq=0 ttl=119 time=18.2 ms
64 bytes from mail.ru (194.67.57.126): icmp_seq=1 ttl=119 time=17.8 ms

--- mail.ru ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 17.815/18.056/18.297/0.241 ms, pipe 2
# dmesg
IN= OUT=venet0 SRC=10.0.1.2 DST=192.168.1.1 LEN=53 TOS=0x00 PREC=0x00 TTL=64
ID=59520 DF PROTO=UDP SPT=32768 DPT=53 LEN=33
IN= OUT=venet0 SRC=10.0.1.2 DST=194.67.57.126 LEN=84 TOS=0x00 PREC=0x00 TTL=64
ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=15423 SEQ=0
```

IN= OUT=venet0 SRC=10.0.1.2 DST=192.168.1.1 LEN=72 TOS=0x00 PREC=0x00 TTL=64
ID=59539 DF PROTO=UDP SPT=32768 DPT=53 LEN=52
IN= OUT=venet0 SRC=10.0.1.2 DST=194.67.57.126 LEN=84 TOS=0x00 PREC=0x00 TTL=64
ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=15423 SEQ=1

So, two important points:

- 1) Load ipt_LOG kernel module on VE0 _before_ VE start
- 2) Add ipt_LOG to the list of available modules in vz.conf

HTH,
Vasily
