Subject: Iptables logging on VPS not working
Posted by Martijn on Tue, 28 Feb 2006 20:57:43 GMT

View Forum Message <> Reply to Message

For some extra protection I'd like to have iptables run on the VPS's or the host system. Since the FAQ tells that stateful inspection on the host is "highly not recommended" I'd like to run iptables on the VPS's.

More info on the setup:
Host: CentOS 4.2; 2.6.8-022stab070.1
VPS: CentOS 4.2

Modules loaded with the VPS taken from the configfile:

```
IPTABLES="iptable_filter iptable_mangle ipt_limit ipt_REJECT ipt_LOG ipt_length "
```

/etc/sysconfig/iptables part:

```
...
-A INPUT -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -j LOG --log-prefix "INPUT-DENIED: "
-A RH-Firewall-1-INPUT -j DROP
COMMIT
```

As you can see, above is just an altertion of a stock firewall with CentOS 4.2.

The iptables is running and working but it doesn't log any dropped packets in syslog. Anybody a clue?

Thanks in advance,
Martijn

Subject: Re: Iptables logging on VPS not working
Posted by dev on Tue, 28 Feb 2006 22:33:54 GMT

View Forum Message <> Reply to Message

Where have you tried to see logged packets? in host system or in VPS?
Have you tried 'dmesg' in VPS?

Subject: Re: Iptables logging on VPS not working
Posted by Martijn on Fri, 03 Mar 2006 11:06:37 GMT

View Forum Message <> Reply to Message

dev wrote on Tue, 28 February 2006 17:33Where have you tried to see logged packets? in host system or in VPS?

Have you tried 'dmesg' in VPS?
Dev, sorry that it took a while but here we go:
- Looked in both files (messages/dmesg) on the host and VPS, nothing in regard to blocked packets for the VPS;
- The host blocks and logs the dropped packages fine but only uses the INPUT table (for access to the host). No FORWARD rules are applied on the host.

There must be something I overlook, the rules are there and the counters increase after an attempt which triggers the logging and the reject as seen below:

```
$vps> iptables -L -n -v
Chain RH-Firewall-1-INPUT (2 references)
 pkts bytes target prot opt in out source     destination
    0     0 ACCEPT all  --  lo *   0.0.0.0/0 0.0.0.0/0
    0     0 ACCEPT icmp --  *  *   0.0.0.0/0 0.0.0.0/0 icmp type 255
...
   82 11917 ACCEPT tcp  --  *  *   0.0.0.0/0 0.0.0.0/0 tcp dpt:80
   14  1188 LOG    all  --  *  *   0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 4 prefix `INPUT-DENIED: '
   14  1188 REJECT all  --  *  *   0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited
```

Bottom line is that the rules *DO WORK* but nothing is logged when packets are dropped of rejected.

Strange... any help is appreciated!

Subject: Re: Iptables logging on VPS not working

Posted by dev on Fri, 03 Mar 2006 15:41:16 GMT
View Forum Message <> Reply to Message

I meant command 'dmesg', not file messages/dmesg
simply execute:

```
$vps> dmesg
```

Also please provide the output of

```
cat /proc/sys/kernel/printk
```

Maybe your log level doesn't allow such messages

Subject: Re: Iptables logging on VPS not working

Posted by Martijn on Fri, 03 Mar 2006 21:54:01 GMT
View Forum Message <> Reply to Message

My fault, thought you were talking about logfiles. The dmesg definately gave the right answers.

Here is the output of printk

```
bash-3.00# cat /proc/sys/kernel/printk
6       4       1       7
bash-3.00#
```

Subject: Re: Iptables logging on VPS not working

Posted by dev on Sat, 04 Mar 2006 09:14:36 GMT

View Forum Message <> Reply to Message

ok. So I suppose the whole issue is resolved?
or you want to log them to some file?
then you need to start syslog/klogd which will save dmesg output to /var/log/messages

Subject: Re: Iptables logging on VPS not working

Posted by Martijn on Sat, 04 Mar 2006 14:21:37 GMT

View Forum Message <> Reply to Message

dev wrote on Sat, 04 March 2006 04:14ok. So I suppose the whole issue is resolved?
or you want to log them to some file?
then you need to start syslog/klogd which will save dmesg output to /var/log/messages

Dev, the only issue is the logging to /var/log/messages. On the host is syslogd running but no klogd.

```
bash-3.00# ps aux|grep logd|grep -v grep
root     27895  0.0  0.0  1520  592 ?        Ss   16:15   0:00 syslogd -m 0
bash-3.00#
```

A restart of the syslog service didn't help for the logging to the file but dmesg did show the dropped packets.

Idea is that the VPS runs just like a standard out-of-the-box installation of CentOS.

Subject: Re: Iptables logging on VPS not working

Posted by Martijn on Fri, 10 Mar 2006 13:01:25 GMT

View Forum Message <> Reply to Message

Dev, do you have any tips how to turn on the "default CentOS" logging so the iptables logging ends up in the /var/log/messages file?

Thanks in advance!

Subject: Re: Iptables logging on VPS not working
Posted by kir on Fri, 10 Mar 2006 15:45:51 GMT

View Forum Message <> Reply to Message

For the historical reasons klogd was disabled in template. In your case you need to enable it. If you use precreated template, the best way to do it is to take the original /etc/init.d/syslog file from sysklogd rpm and put it into your VPS.

If you use template tools and use vzpkgcache to create a template, edit the /vz/template/centos/4/(your-arch)/config/install-post file and remove (or comment out) these lines:

```
# Disable klogd
$VZCTL exec2 $VEID \
        "sed -i -e 's/daemon\\ klogd/passed\\ klogd\\ skipped/' \
                -e 's/killproc\\ klogd/passed\\ klogd\\ skipped/' \
                        /etc/init.d/syslog"
# FIXME: fix '/etc/init.d/syslog status' to return 0
# even if klogd is not running
```

After that, run vzpkgcache -f to forcibly recreate the template cache, and then create a new VPS. It will have klogd running.

Subject: Re: Iptables logging on VPS not working
Posted by Martijn on Tue, 14 Mar 2006 17:57:37 GMT

View Forum Message <> Reply to Message

kir wrote on Fri, 10 March 2006 10:45After that, run vzpkgcache -f to forcibly recreate the template cache, and then create a new VPS. It will have klogd running.
Kir, thanks a lot for clearing it!

Subject: Re: Iptables logging on VPS not working
Posted by RapidVPS on Wed, 15 Mar 2006 23:24:22 GMT

View Forum Message <> Reply to Message

This is an informative post. Martijn, is the iptables log finally printed to /var/log/messages? It is not clear based on your response.

Subject: Re: Iptables logging on VPS not working
Posted by gralex on Tue, 29 Mar 2011 12:17:06 GMT

View Forum Message <> Reply to Message

That's working solution for me:

```
rm -f /etc/init.d/syslog
```

```
yum reinstall sysklogd
/etc/init.d/syslog restart
```

Thanks.

p.s. iptables logs both in dmesg in /var/log/messages. Is it how the things should be?