Subject: *SOLVED* ipt_owner within a VE
Posted by nksupport on Fri, 15 Jun 2007 21:46:33 GMT
View Forum Message <> Reply to Message

Trying to get the subject working. Works for the host OS, but vzctl enter and even vzlist say

Warning: Unknown iptable module: ipt_owner, skipped

I believe everything is configured OK:

grep owner /etc/vz/vz.conf
IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_owner"

lsmod | grep owner
ipt_owner 6400 0
ip_tables 35096 12
ipt_owner,iptable_nat,ipt_length,ipt_ttl,ipt_tcpmss,ipt_TCPMSS,iptable_mangle,iptable_filter,ipt_multiport,ipt_limit,ipt_tos,ipt_REJECT

Host OS is RHEL 4 update 5 x86_64
kernel 2.6.9-023stab044.4-smp, also tried development and 2.6.18 with same effect
vzctl 3.0.16.1, already tried recompiling the source RPM running under the specified kernel with no effect.

Googling did not give me the exact answer if the feature is working in OpenVZ. Is it so? Does anybody have an example of a working setup?

UPDATE: now i have a working installation as well)

Subject: Re: ipt_owner within a VE
Posted by curx on Sun, 17 Jun 2007 08:33:25 GMT
View Forum Message <> Reply to Message

Hi,

iptables "OWNER" module isn't virtualized,
only listed iptables modules can be used in VE context:
(see man-page of vzctl)

iptable_filter,iptable_mangle, ipt_limit, ipt_multiport,
ipt_tos, ipt_TOS,ipt_REJECT, ipt_TCPMSS, ipt_tcpmss,
ipt_ttl, ipt_LOG, ipt_length, ip_conntrack, ip_conntrack_ftp,

ip_conntrack_irc, ipt_conntrack, ipt_state, ipt_helper,
iptable_nat, ip_nat_ftp, ip_nat_irc, ipt_REDIRECT xt_mac.

Subject: Re: ipt_owner within a VE
Posted by nksupport on Sun, 17 Jun 2007 16:33:25 GMT
View Forum Message <> Reply to Message

Sure, that makes sense. What puzzles me is this:
http://git.openvz.org/?p=linux-2.6.16-openvz;a=commit;h=02b2da381654f72b8be867f9f695a14e51d35165

and this:

http://lists.swsoft.co.jp/pipermail/virtuozzo/2006-November/ 000011.html

However, as you correctly mentioned, the source tarball contains the same static manpage and the module is not listed. So, the question remains: what is the current status of ipt_owner in the kernel?

Subject: Re: ipt_owner within a VE
Posted by Vasily Tarasov on Tue, 19 Jun 2007 14:42:44 GMT
View Forum Message <> Reply to Message

Hello,

I've just tried ipt_owner on 2.6.18-028stab033 and it works for me. I still have "Warning: Unknown iptable module: ipt_owner, skipped", but it works. Can you explain (with command examples), how do you check, that ipt_owner doesn't work?

Thanks,
Vasily.

Subject: Re: ipt_owner within a VE
Posted by nksupport on Tue, 19 Jun 2007 18:46:57 GMT
View Forum Message <> Reply to Message

root@x2 ~ # lsmod | grep own
ipt_owner 6400 0
ip_tables 35096 12

ipt_owner,iptable_nat,ipt_length,ipt_ttl,ipt_tcpmss,ipt_TCPMSS,iptable_mangle,iptable_filter,ipt_multiport,ipt_limit,ipt_tos,ipt_REJECT
root@x2 ~ # vzctl enter 103
Warning: Unknown iptable module: ipt_owner, skipped
entered into VE 103

2.6.9-023stab044.4-smp

18:37:34 up 3 days, 21:24, 0 users, load average: 0.26, 0.23, 0.14

LANG=C
root@p4 / # iptables -I OUTPUT -m owner --uid-owner=110 -j ACCEPT
iptables: No chain/target/match by that name

/lib/iptables/libipt_owner.so exists within the VE.

Subject: Re: ipt_owner within a VE
Posted by nksupport on Tue, 19 Jun 2007 21:22:29 GMT
View Forum Message <> Reply to Message

Recompiled 2.6.18 and got it working. Thanks for the tip.

Subject: Re: ipt_owner within a VE
Posted by Vasily Tarasov on Wed, 20 Jun 2007 06:34:19 GMT
View Forum Message <> Reply to Message

Actually, thank you! While trying iptables owner module, I have discovered a problem in current OpenVZ iptables management. The bug was filled:
http://bugzilla.openvz.org/show_bug.cgi?id=626

Thank you,
Vasily.

Subject: Re: *SOLVED* ipt_owner within a VE
Posted by GameOver on Fri, 06 Jul 2007 09:30:48 GMT
View Forum Message <> Reply to Message

Hi nightkid,

What did you do to enable iptables owner module? In the patch for kernel 2.6.18, I don't see anything for ipt_owner. Did you just enable it in kernel config and recompile? Also, do you any problem with your server after enabling ipt_owner?

To OpenVZ developers: could you virtualize ipt_owner and enable it by default in stable kernel? We need this module to restrict outgoing connections to specific UIDs/GIDs to help prevent our users from bypassing MTA to connect directly to remote mail server to send spam. I think many people especially those operating hosting servers will need it too.

Many thanks,

Subject: Re: *SOLVED* ipt_owner within a VE
Posted by nksupport on Wed, 25 Jul 2007 16:56:18 GMT
View Forum Message <> Reply to Message

Yes, I simply enabled it in the kernel config and rebuilt the kernel SRPM. There was one problem, though: an attempt to unload the iptables modules from the node's kernel causes a panic - I ignored it, as there is no need to unload those. I did not apply patches.
