Subject: ufw support in OpenVZ ubuntu container.
Posted by piplite on Tue, 11 Aug 2009 20:00:01 GMT

I have been googling problem with setting up ufw (Ubuntu FireWall) for hours now and no success answer anywaere.
I also searched this place and no answer so far.
So heres a problem.
Installation goes perfectly fine. Im able to add rules and so on but problem comes when im trying to enable firewall:
root@piplite:/# ufw enable
ERROR: problem running init script
and more

root@piplite:/# ufw enable
Firewall started and enabled on system startup
root@piplite:/# sudo /etc/init.d/ufw force-reload
 * Stopping firewall: ufw...
    [OK]
 * Starting firewall: ufw...
        iptables-restore: line 71 failed
 * Problem running '/etc/ufw/before.rules'...
                iptables-restore: line 34 failed
 * Problem running '/etc/ufw/after.rules'...
                error: "Operation not permitted" setting key "net.ipv6.conf.all.accept_redirects"
error: "Operation not permitted" setting key "net.ipv6.conf.default.accept_redirects"
error: "Operation not permitted" setting key "net.ipv4.icmp_echo_ignore_broadcasts"
error: "Operation not permitted" setting key "net.ipv4.icmp_ignore_bogus_error_responses"
error: "Operation not permitted" setting key "net.ipv4.icmp_echo_ignore_all"
error: "Operation not permitted" setting key "net.ipv4.tcp_syncookies"
error: "Operation not permitted" setting key "net.ipv4.tcp_sack"

[fail]

Its also been asked here: https://answers.launchpad.net/ufw/+question/63832   but no answer.
If anybody knows how to make it work, please advice.

Beforehand thanks.

Subject: Re: ufw support in OpenVZ ubuntu container.
Posted by curx on Wed, 12 Aug 2009 22:25:54 GMT

Hi,

the ufw set some settings via the sysctl interface, but in OpenVZ Container this action is not

permitted.

so check /etc/default/ufw, Variable IPT_SYSCTL
or
comment the sysctl entries in /etc/ufw/sysctl.conf

Bye,
 Thorsten

Subject: Re: ufw support in OpenVZ ubuntu container.
Posted by piplite on Thu, 13 Aug 2009 04:46:29 GMT
View Forum Message <> Reply to Message

I did try doing that.
Here is a result:

root@piplite:/# ufw disable
Firewall stopped and disabled on system startup
root@piplite:/# ufw enable
ERROR: problem running init script
root@piplite:/# ufw enable
Firewall started and enabled on system startup
root@piplite:/# /etc/init.d/ufw restart
 * Skipping restart (not enabled)
root@piplite:/# ufw enable
Firewall started and enabled on system startup
root@piplite:/# /etc/init.d/ufw restart
 * Stopping firewall: ufw...
    [OK]
 * Starting firewall: ufw...
        iptables-restore: line 71 failed
 * Problem running '/etc/ufw/before.rules'...
             iptables-restore: line 34 failed
 * Problem running '/etc/ufw/after.rules'...
        [fail]
don't delete the 'COMMIT' line or these rules won't be processed
COMMIT   <-- line number 71 and 34

Thanks.

Subject: Re: ufw support in OpenVZ ubuntu container.
Posted by Nepa on Sun, 30 Aug 2009 08:41:47 GMT
View Forum Message <> Reply to Message

I am having a trouble to start ufw on ubuntu server in openvz container as well

@ curx

I dont have any sysctl entries in /etc/ufw/sysctl.conf

so do I need to comment out this line:
IPT_SYSCTL=/etc/ufw/sysctl.conf

in /etc/default/ufw instead?

Subject: Re: ufw support in OpenVZ ubuntu container.
Posted by bodhi.zazen on Mon, 10 May 2010 16:07:20 GMT
View Forum Message <> Reply to Message

UFW does not seem to run properly in openvz (Ubuntu) templates.

Part of the problem is that ufw calls modprobe, which will fail.

As a partial work around you can remove modprobe and replace it with a link to /bin/true.

rm /sbin/modprobe
ln -s /bin/true /sbin/modprobe

A second problem is that rsyslog does not run well in openvz templates (rsyslog will not log iptables or ufw). A potential work around is to use syslog-ng

apt-get purge rsyslog
apt-get install syslog-ng

syslog-ng will log to /var/log/messages and /var/log/kern.log but not /var/log/ufw.log

With those work arounds, you can try ufw. You will still get some error messages from ufw-init re: iptables-restore. I do not know how to fix that.

That is about as far as I can get you if you want to use UFW as I personally use iptables.

Others have suggested using shorewall as an alternate (to ufw).

http://www.shorewall.net/OpenVZ.html

With ufw you sometimes need to toggle the defaults, then ufw will start:

ufw default allow
ufw default deny
ufw enable

I highly suggest you use iptables (keep in mind you may need to edit /etc/vz/vz.conf on the HOST) and iptables is not fully functional in openvz guests (the basic functions and logging work, but some functions such as conntrack may not).

To log use iptables + syslog-ng (/var/log/kern.log is fairly clean).

If you have a busy server, and do not want to review hundreds of thousands of logs, consider using snort or psad.

Subject: Re: ufw support in OpenVZ ubuntu container.
Posted by bodhi.zazen on Tue, 11 May 2010 20:29:41 GMT
View Forum Message <> Reply to Message

OK, I found a "fix" for ufw in openvz templates.

Basically the issues are :

1. modprobe does not work

2. iptables is not fully functional in openvz templates, so ufw writes iptables rules the can not be used in openvz templates.

Sorry for the external link, but see this blog for details:

http://blog.bodhizazen.net/uncategorized/how-to-use-ufw-in-o penvz-templates/