Subject: Filter container traffic
Posted by cheetah on Tue, 19 Jun 2012 02:10:14 GMT
View Forum Message <> Reply to Message

Hi Guys,

I just setup my openvz environment. What I need to do now is to write a firewall to check each flow from container and decide if it is allowed.

I noticed that for each container there is vmnet device. I am wondering can I use open vswitch with this vmnet device? (It seems not from what is mentioned here http://wiki.openvz.org/Virtual_network_device). If not, does that mean I have to use netfilter/contrack/iptables to implement my firewall? Could you please recommend some tutorials/readings?

Thanks a lot!

Regards,
Peter

Subject: Re: [Devel] Filter container traffic
Posted by kir on Tue, 26 Jun 2012 19:44:22 GMT
View Forum Message <> Reply to Message

On 06/19/2012 06:10 AM, cheetah wrote:
> Hi Guys,
>
>
> I just setup my openvz environment.

Can you please stop cross-posting to two mailing lists? This is kinda impolite and is counter-productive.

Please stick to users@ list, unless you have a patch or smth.

Thank you.

Subject: Re: [Devel] Filter container traffic
Posted by cheetah on Wed, 27 Jun 2012 03:03:57 GMT
View Forum Message <> Reply to Message

Sorry for my misuse. Will follow the advice next time.

Could you please give some hints on the questions? Thanks.

Peter

On Wed, Jun 27, 2012 at 3:44 AM, Kir Kolyshkin <kir@openvz.org> wrote:

> On 06/19/2012 06:10 AM, cheetah wrote:
>
>> Hi Guys,
>>
>>
>> I just setup my openvz environment.
>>
>
> Can you please stop cross-posting to two mailing lists? This is kinda
> impolite and is counter-productive.
>
> Please stick to users@ list, unless you have a patch or smth.
>
> Thank you.
>

Subject: Re: [Devel] Filter container traffic
Posted by kir on Wed, 27 Jun 2012 08:36:10 GMT
View Forum Message <> Reply to Message

On 06/19/2012 06:10 AM, cheetah wrote:
> Hi Guys,
>
>
> I just setup my openvz environment. What I need to do now is to write
> a firewall to check each flow from container and decide if it is allowed.
>
> I noticed that for each container there is vmnet device.

You probably mean venet or veth. We do not have vmnet.

> I am wondering can I use open vswitch with this vmnet device?

It will be possible later, we have just finished porting OpenVSwitch to
our RHEL6 kernel. Now, it is not possible.

> (It seems not from what is mentioned here
> http://wiki.openvz.org/Virtual_network_device). If not, does that mean
> I have to use netfilter/contrack/iptables to implement my firewall?

Yes, you can use iptables. For venet case, you can use iptables on the
host system and/or inside CT. For veth case, you can only use iptables

inside containers (and on the host you can use ebtables I guess).

Subject: Re: [Devel] Filter container traffic
Posted by kir on Wed, 27 Jun 2012 08:41:11 GMT
View Forum Message <> Reply to Message

On 06/19/2012 06:10 AM, cheetah wrote:
> Hi Guys,
>
>
> I just setup my openvz environment. What I need to do now is to write
> a firewall to check each flow from container and decide if it is allowed.
>
> I noticed that for each container there is vmnet device. I am
> wondering can I use open vswitch with this vmnet device? (It seems not
> from what is mentioned here
> http://wiki.openvz.org/Virtual_network_device). If not, does that mean
> I have to use netfilter/contrack/iptables to implement my firewall?
> Could you please recommend some tutorials/readings?

I guess most of what we have is available from here:
http://wiki.openvz.org/Category:Networking