
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/conntrack/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).
