Subject: Bridging inside the CT, snort in-line?!
Posted by vitorallo on Sat, 31 Jan 2009 11:28:28 GMT
View Forum Message <> Reply to Message

Hello Folks,

nice to be part of the community, I just joined.
Few words about openvz. It's awesome. I started using it only one week ago and it already changed my life!!!! it is a great project and a tremendous contribution to the virtualization world....

I liked it so much that I decided to start a small project using it. Unfortunately I stuck with an architectural problem.

I read already that bridge-utils and bridging inside the ct is not possible. This makes perfectly sense. It is plenty of possibilities to bridge outside at the host machine level.

However, I am trying to install snort in-line inside the ct. I am so crazy to think about IPS inside CT. No problem with recompiling it; I just used a debootstrap minimal machine. The real problem is to let the traffic flowing into the VM, bridging inside and allowing iptable queue to grab it, in order for snort to process the analysis. Therefore, bridging cannot be out of the ct. Even working with a stick into the ct, after the learning phase the bridge will send the traffic directly out to the second interface (without taking care of the stick)

Let me explain. This what I would like to do:

```
eth0(host)--(bridge or...)--veth101.0----eth0(CT)
 ..................................................... .!
 ..................................................... .! bridge
 ..................................................... .! snort-inline
 ..................................................... .!
eth1(host)--(bridge2 or..)---veth101.1---eth1(CT)
```

Not that complicated architecture, but snort runs inside and needs to lookup the packets from the ct inner eb or iptables.

I looked around the internet but I did not find anything useful. Every efforts in bridging for openvz is done outside. Maybe I was not very good in searching around. I tried also some horizontal solution like using iptables to copy packets but I don't want to add so much overhead (affecting performances).

Right now, I am looking for something, modules and so on, something to compile as external pluggable module into the ovz kernel ... uhmm ... it wouldn't be very clean.

I don't think nobody tried to do something similar. So, I am posting here to grab your suggestions, idea or testing. I am pretty new and I might miss the way to do it help
I would like to go ahead with openvz - I don't want to switch on xen!!! I will be happy to share trough this forum any other further experience of mine .

talk to you soon guys,

vito