Subject: Re: Bridging inside the CT, snort in-line?!
Posted by maratrus on Mon, 02 Feb 2009 17:32:36 GMT

First of all, thank you for clarifications. So if I'm right, the main desire is not running two instances of snort inside CT. Instead it would be great to join interfaces and run only one instance of snort. But running two instances of snort is a solution anyway (and it's no so bad). What do you think?

Unfortunately it's impossible to create/delete bridges inside CT because they are not virtualized. There is a bug http://bugzilla.openvz.org/show_bug.cgi?id=831 (and you could describe the necessity of this feature from new point of view).

May be it worth trying the following (ugly) workaround: using only one eth0 interface inside CT and two ip addresses on it (alias) and appropriate routing rules on the HN.
To be more plain:

```
 eth0    eth1
+-|--------|-+
|| HN  ||
|        |
|    veth  |
| +---|---+ |
| | eth0 ||
| | eth0:0| |
| | VE  ||
| +-------+ |
+------------+
```

On the HN the following routing rules:

ip r add $CT_IP_1 dev $VETH
ip r add $CT_IP_2 dev $VETH