Subject: *CLOSED* Good way to isolate VE networks.
Posted by sebastian on Sun, 04 Mar 2007 16:44:58 GMT
View Forum Message <> Reply to Message

Hi,

first of all: I'm new to OpenVZ and it well may be that i overlooked some obvious thing addressing my issue. But i searched the forum and the wiki but didn't found a concrete answer. So sorry if this is a typical newbie question.

I've set up some VE's in a Debian Etch HN (It's a VMWare-Machine for testing purposes). I'm using the VENET approach for networking (because of security concerns) and so far it's working fine. The VE's can access the internet and DNAT works too, but: I've found no nice way to restrict networking access between the VE's. I'm currently thinking of the following setup on the HN:

General Purpose VE's
- Database Server
- MTA
- DNS
- APT-Proxy

User VE's
- User VE 1
- ...
- User VE n

The User VE's should be able to access the general purpose VE's but should not be able to interconnect between them. Of course can i add matching firewall entries to all VE's but this seems like a classical case for building two networks. My problem is: I found no way to add netmasks or something similar through vzctl. What approach would you recommend in such a szenario?

Thanks very much in advance,
Sebastian