Subject: Re: VEs with different subnets
Posted by ugo123 on Mon, 09 Jul 2007 12:51:19 GMT
View Forum Message <> Reply to Message

n00b_admin wrote on Mon, 09 July 2007 08:35I know i'm not much of an expert but i'm learning too from your experience...

Why do you need public addresses on the VE's ?

You assign public addresses to the HN's and private to the VE's.. what you need to do that cannot be done because of NAT-ing the VE's ?

You setup the VE's with venet0 and that's all you need to do.

Hello,

I need public addresses on the VEs because those VEs are the one who are providing Internet services, and I want one public IP per VE.

I don't want to assign a single public IP to the HN because it's a waste of IP (and being in Europe, we are tight on public IP with the RIPE), it's also useless in my case and it exposes the HN to the Internet (even with a firewall, I don't like the idea).
The HN should be for me the most secured box (because if compromised, everything is going down), and a private subnet is ideal to answer both of my problems : no public IP wasted, impossible to reach from the Internet.

I don't want to do NAT either, because NAT is less than ideal both in terms of performance and configuration, it would be of course okay if I had a single HN and a single IP.
like set the port 25 to my mail_ve, 80 to my web_ve, etc..etc..

But it's not my case and I want a full network capacity on each VE... and to configure each VE the most easy way, like a real box.... and to don't mind any above configuration.... like NATing and so on... so if a HN dies, I can migrate the VE to the HN, launch it again, and it directly works... no configuration involved.

Finally I could have tweaked my main gateway 10.1.1.1 for my internal network to provide a kind of mixed routing to support my case, but it would have meant that the WHOLE network would have relied and transited on a single machine aka a SPoF (Single Point of Failure), whereas my ISP is providing me a nice IP gateway, with full redondancy, heavy reliability, etc..etc....

So I guess for most simple cases or when you can't trust your VE, venet is definitively the way to go....
But when you need to create more complex infrastructure, it has some limitations, it has nothing to do with the way OpenVZ is built, it's just the limitation of Layer 3 IP routing.... you sometimes need to a Level 2 (with MAC addresses and so on) to do more tricky things.

Hope it answers your questions.

Ugo