Subject: Re: How to assign a public IP to a VE ? (SOLVED)
Posted by U.Mutlu on Sun, 30 Oct 2011 16:04:49 GMT
View Forum Message <> Reply to Message

U.Mutlu wrote, On 2011-10-30 13:12:
> Problem solved!
> (problem was how to assign a public IP to a VE)
>
> It was a firewall issue on the HN, because in my firewall script
> the default iptables target for FORWARD was set to DROP. After changing
> this to ACCEPT things work fine.
> (now I must recheck my security guidelines on whether and which other
> implications this change can have...)
>
> Ie. the solution was to change this from
> iptables -P FORWARD DROP
> to
> iptables -P FORWARD ACCEPT
> (for testing one can of course also completeley disable the iptables firewall)

Now I improved the above solution to this more secure solution:
  iptables -P FORWARD DROP
  iptables -A FORWARD -s w.x.y.z -j ACCEPT
  iptables -A FORWARD -d w.x.y.z -j ACCEPT

where w.x.y.z is the IP for the VE.
(I could have also make it "w.x.y.z/24" but IMO it's not neccessary
since no broadcasts are supposed to go over that link).

> And do not assign the IP in question to the HN, rather just
> let it assign/manage by vzctl when it creates/starts the VE.
>
> This solution uses the default venet0 only, ie. no veth, no bridging etc.,
> no "source routing via kernel routing table" etc., not even any additional normal routing! :-)
> (Beware: there is much garbage info floating around on the net about the venet0 device;
> maybe this is due to very old versions of vzctl used...)
>
> My environment:
> HN: Debian 6 (squeeze), but using a newer vzctl from either the upcoming Debian 7
(wheezy/testing)
> or from http://download.openvz.org/utils/vzctl/current/; I've vzctl version 3.0.29.3.
> Kernel: 2.6.32-5-openvz-amd64 (linux-image-2.6.32-5-openvz-amd64 from the debian
repository)
> VE: debian-6.0-i386-minimal from http://wiki.openvz.org/Download/template/precreated
> (I so far tested only this one, the other ones should work too I think)
>
> People still having problems setting up openvz can contact me (help @ mutluit.com)
> if having a similar environment (ie. Debian 6 on HN+VE, using venet, not veth),

> maybe I can help if time permits...
>
> --
> U.Mutlu
> www.mutluit.com