Subject: DMZ VPS on LAN HN ?
Posted by bards1888 on Sun, 14 Jan 2007 05:13:19 GMT
View Forum Message <> Reply to Message

I have a 3 legged firewall with INTERNET, LAN and DMZ segments/legs. The LAN and DMZ have their own switches.

I have openvz stable 2.6.9-023stab037.3-smp running on a 'LAN' server that is Centos 4.4 x86_64. Everything is working well and I can create VEs successfully.

I'm now trying to consolidate my physical DMZ host (mail/web server) onto a VPS running on this 'LAN' server. The LAN server has 2 nics eth0 (LAN) and eth1 (DMZ). I have physically connected eth1 to the DMZ switch and eth0 is connected to the LAN switch.

I've brought eth1 up with an IP address of the DMZ segement and also assigned a VE with another DMZ segment IP address. I had to changed the vz.conf so that;

VE_ROUTE_SRC_DEV="eth1"

This works perfectly and the VE looks like it lives in the DMZ.

From a security point of view I'm a bit worried that it would appear as though I *have* to bring up eth1 on the HN with an IP address for this to work. Obviously I'd like if I could run this without need an IP on eth1.

I brought eth1 up without an IP to see if that would work bu it appears not to.

Do I need to enable proxy arp for this work ?

Do I need to use iptables to restrict access to the eth1 interface but allow access to the VE's IP address ?

Or am I trying to do something that wont work the way I want it to ?

Any help or assistance would be appreciated.

Cheers.

Subject: Re: DMZ VPS on LAN HN ?
Posted by bards1888 on Sun, 14 Jan 2007 11:58:02 GMT
View Forum Message <> Reply to Message

I appear to have fixed this and answered my own questions by doing this;

vzctl set 112 --netdev_add eth1 --save

This passed the eth1 interface directly into the VE. I then used the standard CENTOS network interface file /etc/sysconfig/network-scripts/ifcfg-eth1 and brought the interface up with a DMZ address. However, the default gateway was always being set. I found this address in two places;

/etc/sysconfig/network

and

/etc/sysconfig/network-scripts/route-venet0

I commented those bits out of each file and then had to add a 'GATEWAY=' section in my;

/etc/sysconfig/network-scripts/ifcfg-eth1

This worked a treat and the VE comes up perfectly.

Now, eth1 on the HN is deliberately not configured, it does not have an IP and is not UP. In fact a 'ifconfig -a' doesn't show the device and an 'ifconfig eth1' produces;

eth1: error fetching interface information: Device not found

I did some tests with tcpdump and and the VE cannot, as you would expect, see any traffic on HN eth0. Also, as eth1 is sort of invisible the HN cannot see any traffic on it.

I added a firewall rule that allows by VE to talk SMTP to a server on my LAN. This connection came from the DMZ to the LAN server, it did not use any local interface on the HN.

This is exactly what I wanted.

Another thing, I did not have to set proxy_arp sysctl variables to 1 or do anything with ipfilter.

Can anyone see any issues with this setup ?

Cheers,

Bards.