Subject: Re: Openvpn Internet issue
Posted by kir on Thu, 21 May 2009 20:56:00 GMT
View Forum Message <> Reply to Message

sammy08 wrote on Thu, 21 May 2009 23:40IPTables is running on the hardware node and I have it running in the VE.

OK, a little longer explanation.

Functionality of iptables is implemented in kernel, by the kernel modules (named ip_*, ipt_*, iptables_* nf_* etc.). Such modules are loaded during system bootup, and they provide different iptables filters, policies, etc. For example, SNAT functionality is provided by ip_nat, ip_conntrack, iptable_nat and probably some other modules.

OpenVZ functionality is also (partially) provided by the kernel modules (named vz*). Those modules are loaded by /etc/init.d/vz script during system bootup.

If you need to use functionality of some iptables modules from inside a VE, you need to make sure the modules you need are loaded before /etc/init.d/vz is started.

How to implement that depends on your distro. In most cases /etc/init.d/vz script itself contains code to (pre)load needed iptables modules. In that case the list of modules to be loaded is set by IPTABLES variable in /etc/vz/vz.conf file. So what you need to do is

1. Find out what modules do you need. You can do so by running lsmod on the host system, then running the iptables command that you try to run in VE (and it will load the required modules automatically), and the running lsmod again for the second time. Now, compare the output of two lsmod runs and find out the new modules which has just been loaded. Most probably this is ip_nat, but YMMV.
2. Add the names of those modules into IPTABLES in /etc/vz/vz.conf
3. Run /etc/init.d/vz restart.
4. Check in VE that it's working.

Finally, the error you see is caused by the fact that iptables utility is smart enough so it tries to load some iptables modules if those are not yet loaded. Of course you can not do that from within a VE (for security reasons) so iptables tries to load modules and it fails. (Note that this explanation is a little simplified but correct).