Subject: iptables - host node or VPSes?
Posted by GameOver on Thu, 03 Nov 2005 11:17:47 GMT
View Forum Message <> Reply to Message

Hi there,

I have a couple of VPSes and want to use iptables to protect them, I'll use the same rules for all VPSes anyway. Should I apply my iptables rules to the hostnode or to each individual VPS? I think the former method is better because it reduces the number of rules in the kernel and it is more stable as it can load/unload iptables modules but I could be wrong.

By the way, using OpenVZ instructions I could not load iptables modules automatically on a RHEL4 based hostnode. Is it just me or the instructions are incorrect? Of cource I can load them through rc.local.

Subject: Re: iptables - host node or VPSes?
Posted by dim on Thu, 03 Nov 2005 12:17:15 GMT
View Forum Message <> Reply to Message

Typical VPS' packet travel looks like:
1) to VPS: sender, network, HN's input interface, ip stack with HN context, forward to venet interface, venet interface, IP stack with VPS context, receiver inside VPS.
2) from VPS: sender inside VPS, IP stack with VPS context, venet interface, IP stack with HN context, forward to HN's output interface, output, network, receiver.

Both ways have their advantages and disadvantages.

If you apply rules on HN, you avoid travel of bad packets through the system, but this way slows down all VPSs network performance.

If you apply iptables rules in VPS, they will be checked only if packet context equals to this VPS. But you need to load iptables modules before VPS start and permit them in VPS config (or in global vz config, if you need the same set for all VPSs).

So, for hosting purposes where HN administrator and VPS owners are different identities, I'd prefer iptable rules on HN - thus I'll be sure, that at least these rules will work as expected

About second question - we have common UserGuide for all distros and it is likely that its instructions are not quite correct for some of them.