Subject: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by HHawk on Fri, 31 May 2019 08:03:44 GMT
View Forum Message <> Reply to Message

I understand this was never really possible under OpenVZ 6 (or Virtuozzo 6), however apparently it's possible with the new version of OpenVZ 7 (Virtuozzo 7).

I quote Konstantin Khorenko's post on https://bugs.openvz.org/browse/OVZ-5736:

Quote:By the way, Virtuozzo 7 with kernel 3.10.0-327.10.1.vz7.12.8 or later has support for ipset in Containers.

So @khorenko or someone else can explain how to do this correctly for CT's?
Would be great. Especially considering it works way faster (apparently) compared to using iptables.

Thank you in advance!

Subject: Re: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by khorenko on Fri, 31 May 2019 08:49:37 GMT
View Forum Message <> Reply to Message

Quote:how to do this correctly for CT's?

Just configure ipset inside a Container like you do this on a Hardware Node,
that should work.
Link to an example.

Subject: Re: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by HHawk on Fri, 31 May 2019 10:53:25 GMT
View Forum Message <> Reply to Message

Thank you khorenko! Highly appreciated.

ipset performance is better right, compared to iptables?
I think I read somewhere is can handle more IP's without performance issues. Is that true?

Subject: Re: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by khorenko on Fri, 31 May 2019 11:27:28 GMT
View Forum Message <> Reply to Message

i did not measure them myself, but
https://workshop.netfilter.org/2013/wiki/images/a/ab/Jozsef_ Kadlecsik_ipset-osd-public.pdf

Subject: Re: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by HHawk on Mon, 03 Jun 2019 08:00:29 GMT
View Forum Message <> Reply to Message

Thank you.

Subject: Re: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by wsap on Sun, 09 Jun 2019 01:21:31 GMT
View Forum Message <> Reply to Message

HHawk wrote on Fri, 31 May 2019 07:53Thank you khorenko! Highly appreciated.

ipset performance is better right, compared to iptables?
I think I read somewhere is can handle more IP's without performance issues. Is that true?

Yep! As long as you don't require more advanced control over the IP than block/allow type controls then it's much faster and does work with OpenVZ 7. Only had to install ipset and it worked right off the bat, but we also have NETFILTER=full enabled for all containers using ipset, which may help with that being so straightforward.

Subject: Re: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by HHawk on Mon, 17 Jun 2019 07:18:38 GMT
View Forum Message <> Reply to Message

Thank you websavers for the reply.

I do have one more question. I am planning to use on our bigger Plesk servers (which will be migrated from OpenVZ 6 to OpenVZ 7 before doing so ofcourse) Juggernaut Security and Firewall.
Now they state that OpenVZ 6 is not working correctly with it. I quote: "Virtuozzo is not the ideal VPS because it does not support ipset for high performance firewall blocking."

However this was based on OpenVZ 6. So it shouldn't apply to OpenVZ 7. Correct?

Furthermore; according to the (old) OpenVZ wiki and I quote: "Also, large numiptent cause considerable slowdown of processing of network packets. It is not recommended to allow containers to create more than 200300 numiptent."

Is it safe to increase the value to 10000 as stated here:
https://docs.danami.com/juggernaut/basics/virtuozzo-openvz-c onfig-tasks

Thanks in advance.

//edit 1: I just installed the Juggernaut firewall with 10000 numiptent, but the firewall crashes as it already hit the 10000 entries. So I am going to increase it to 100000 instead. This is a test server, but I am still wondering if this is allowed or not?

//edit 2: Okay, a small edit. Apparently with 3 block lists and 3 countries blocked (including China) it required 12629 numiptent setting. So I am guessing a value around 25000 for numiptent should be enough for servers. But is this a safe value with OpenVZ 7? I cannot seem any real information about this setting or modern values. So I am hoping someone can explain this a bit more.

Subject: Re: Can you use "ipset" with OpenVZ 7 / Virtuozzo 7?
Posted by wsap on Mon, 17 Jun 2019 11:18:59 GMT
View Forum Message <> Reply to Message

Hey HHawk,

I haven't specifically used Juggernaught before, but I have used a few other firewall solutions and, as long as NETFILTER=full is enabled on the container, they've all worked great.

Even with vz7 I *have* seen slowdowns when too many containers have too many standard iptables rules per node, however I haven't analyzed it in any great detail. This is the big advantage of ipset; you can use that to set up huge chains of rules without any such slowdowns. Hopefully juggernaught uses it too?

I generally try to keep my numiptent to under 5000 per container. I *think* when I ran into trouble it was around 20000 rules across all containers on a node. I'd suggest that juggernaught start using ipset instead. If that's not likely to happen, could always check out csf -- it uses ipset.