

---

Subject: \*SOLVED\* Is OpenVZ in Parallels vm known to work?

Posted by [kermit](#) on Sun, 29 Apr 2007 13:02:41 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

I've just installed OpenVZ inside a Parallels virtual machine on a Mac. I ran into problems with networking. Since I don't have a spare physical box around I can't check whether the problem also occurs on a "real" machine.

Did anyone manage to get OpenVZ networking to work in a Parallels (or VMWare) virtual machine?

Thanks

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [Vasily Tarasov](#) on Wed, 02 May 2007 07:53:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

In VMware it works without problems. And it should work in Parallels too, if usual linux distribution can work with network in it. Check routing, iptables and other network settings.

Vasily.

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [dev](#) on Fri, 04 May 2007 13:12:50 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Yes, it works in Parallels 100% (though not tested on MAC by me).

Can you check the link in OpenVZ plz:

# ip a l

# dmesg

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [kermit](#) on Sat, 05 May 2007 20:16:19 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

OK, it was obviously not Parallels, but some "feature" of the network I was trying it in (Wifi with 802.1x authentication). After moving to a simpler network, I get a network connection from the VPS.

Now I'm struggling with the firewall within the VPS. I've set the HN's firewall to be transparent for the VPS, which works fine. If I now switch on the firewall in the VPS (which is CentOS 4), I can't connect to the VPS via SSH, despite allowing SSH traffic in system-config-securitylevel. It looks like the rule generated by system-config-securitylevel for allowing incoming ssh connections is

never matched (so the next rule REJECTs the incoming connection). If I simplify the rule (in /etc/sysconfig/iptables)

```
-A RH-Firewall-1-INPUT -m STATE --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

as generated by system-config-securitylevel to

```
-A RH-Firewall-1-INPUT -p tcp --dport 22 -J ACCEPT
```

and restart the firewall, I can connect to the VPS via SSH. However, I have about 5s delay after entering the password before I get the shell. This delay just goes away when I'm shutting down the firewall within the VPS.

I'm using kernel 2.6.18-8.el5.028stab031.1 and vzctl 3.0.16 on CentOS 5 on the HN and a CentOS 4 template on the VPS.

Any ideas whether this is a problem of the kernel or some mis-configuration?

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [dev](#) on Sun, 06 May 2007 16:53:59 GMT

[View Forum Message](#) <> [Reply to Message](#)

not sure from your description where you setup these iptables rules in HN or inside VE?

if on HN, then you need to you FORWARD chain, not INPUT.

if in VE, then please check that all the required conntrack modules were loaded \*before\* VE start.

Use iptables -L -v to see counters which help to understand where packets were matched.

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [kermit](#) on Sun, 06 May 2007 18:10:32 GMT

[View Forum Message](#) <> [Reply to Message](#)

I'm setting the iptables rule for ssh in the VE. I have the exact same rule also in the HN (and there, in the HN, the very same rule works as expected and allows access via SSH to the HN), thus I believe that I have all necessary netfilter modules loaded in the kernel when the VE is started. Note that I do not get any error message in the VE when doing a

```
# service iptables restart
```

which is an additional indication that all necessary modules are available to the VE.

The package counters shown when doing a

```
# iptables -L -v -n
```

give a clear indication that the SSH rule is `_not_ matched`, but instead the following REJECT rule is matched.

This, and the fact that I `_can_` connect to the VE when stopping the firewall in the VE shows that the package forwarding from the HN to the VE is working correctly.

I should also stress that the rule definition is not a hand crafted one but one that is automatically generated by Redhat's `system-config-securitylevel` script.

Any ideas?

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [Vasily Tarasov](#) on Mon, 07 May 2007 07:41:10 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hello,

can you tell me, please, what distribution are you using on HN? For me (centos 4.4), the rule generated by your ``system-config-securitylevel`` doesn't work:

```
[root@white ~]# CentOS release 4.4 (Final)
[root@white ~]# iptables -A RH-Firewall-1-INPUT -m STATE --state NEW -m tcp -p tcp --dport 22
-j ACCEPT
iptables v1.2.11: Couldn't load match `STATE':/lib64/iptables/libipt_STATE.so: cannot open
shared object file: No such file or directory
```

Try ``iptables -h`` or `'iptables --help'` for more information.

Thank you,  
Vasily.

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [kermit](#) on Sat, 12 May 2007 12:04:16 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Regarding the versions I am using:

Kernel 2.6.18-8.el5.028stab031.1 and vzctl 3.0.16 on CentOS 5 on the HN and a CentOS 4 template on the VPS.

Regarding the firewall rule that behaves unexpectedly in the VE:

Sorry, I have just realized that I had an error in the capitalization of the firewall rule. The correct line is:

```
iptables -A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

that is: "state" is not in capitals. (When using "STATE" in the command line above I get the same error message as you.)

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [Vasily Tarasov](#) on Mon, 14 May 2007 10:11:10 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hello,

I've just tried to reproduce the problem:

HN: Centos 4.4

VE: Centos 4.4

vzctl: 3.0.16

kernel: 2.6.18-028stab031

I added ipt\_state module to vz.conf file and loaded this module on HN, then I started VE and used system-config-securitylevel utility in VE to mark venet0 as trusted interface and allow ssh traffic. It resulted in the following /etc/sysconfig/iptables file:

```
[root@VE /]# cat /etc/sysconfig/iptables
```

```
# Firewall configuration written by system-config-securitylevel
```

```
# Manual customization of this file is not recommended.
```

```
*filter
```

```
:INPUT ACCEPT [0:0]
```

```
:FORWARD ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [0:0]
```

```
:RH-Firewall-1-INPUT - [0:0]
```

```
-A INPUT -j RH-Firewall-1-INPUT
```

```
-A FORWARD -j RH-Firewall-1-INPUT
```

```
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -i venet0 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
```

After that I was able to ssh to VE from HN and from other nodes. But note, that I have no any firewall rules in VE0 (including SNAT/DNAT rules)

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [kermit](#) on Mon, 14 May 2007 16:42:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hi,

> After that I was able to ssh to VE from HN and from other nodes. But note, that I have no any firewall rules in VE0 (including SNAT/DNAT rules)

Note that this is what I want to do: let the VE admin set their own firewall rules. And that is what doesn't work for me, at least not with the rules that are automatically generated.

So if you would try to switch on the firewall in the VE (using the same procedure as for the HN) and there, too, allow SSH traffic, then you should see the problem.

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [Vasily Tarasov](#) on Tue, 15 May 2007 06:09:12 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

I think you undestood my last post incorrectly: VE0 == HN, so I setuped firewall only `_in_ _VE_`, but no any firewall rules on HN.

Thanks,  
Vasily.

---

---

Subject: Re: Is OpenVZ in Parallels vm known to work?

Posted by [kermit](#) on Sat, 19 May 2007 12:51:04 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

OK, I see: the resolution is to add `ipt_state` to the `IPTABLES` variable of `/etc/vz/vz.conf`. I was under the (wrong) impression that this is only necessary if the HN hasn't the module already loaded.

I consider the issue solved. Thanks a lot for your help and patience.

I've two suggestions:

\* Since `ipt_state` is used by the default firewall configuration of Redhat (and CentOS) and since Redhat is kind of the primary distribution you support, what about adding `libipt_state` to the list of allowed iptables libraries by default?

\* The OpenVZ-Users-Guide on page 70 advises to add iptables modules to the variable `IPTABLES_MODULES` of file `/etc/sysconfig/iptables-config`. That should be corrected to refer to the variable `IPTABLES` of file `/etc/vz/vz.conf`.

---

Subject: Re: Is OpenVZ in Parallels vm known to work?  
Posted by [Vasily Tarasov](#) on Mon, 21 May 2007 06:44:58 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Thank you for the suggestions, I offer you to post them as separate bug reports with enhancement severity to [bugzilla.openvz.org](http://bugzilla.openvz.org).

Thank you,  
Vasily.

---