
Subject: *SOLVED* DNS Problem

Posted by [goeldi](#) on Tue, 04 Jul 2006 21:21:20 GMT

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

Is this problem ([http://forum.openvz.org/index.php?t=tree&th=717&mid= 3736&&rev=&reveal=](http://forum.openvz.org/index.php?t=tree&th=717&mid=3736&&rev=&reveal=)) solved? Because I am experiencing the exact same problem.

BTW: stopping iptables on the host system solves the symptom: I can do a ping google.com and the ping works. When I start iptables on the host, it doesn't work anymore. Same for wget etc. In my opinion, stopping iptables is not a professional solution, or did I miss something about openvz security?

These are the iptables rules on the host (no iptables on the ve yet):

```
# /sbin/service iptables status
```

```
Table: nat
```

```
Chain PREROUTING (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Chain POSTROUTING (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Table: mangle
```

```
Chain PREROUTING (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Chain INPUT (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Chain FORWARD (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Chain POSTROUTING (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Table: filter
```

```
Chain INPUT (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
RH-Firewall-1-INPUT all -- 0.0.0.0/0            0.0.0.0/0
```

```
Chain FORWARD (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
RH-Firewall-1-INPUT all -- 0.0.0.0/0 0.0.0.0/0
```

Chain OUTPUT (policy ACCEPT)

```
target prot opt source destination
```

Chain RH-Firewall-1-INPUT (2 references)

```
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 icmp type 255
ACCEPT esp -- 0.0.0.0/0 0.0.0.0/0
ACCEPT ah -- 0.0.0.0/0 0.0.0.0/0
ACCEPT udp -- 0.0.0.0/0 224.0.0.251 udp dpt:5353
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:631
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:19150
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:10000
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited
```

Subject: Re: DNS Problem

Posted by [dev](#) on Wed, 05 Jul 2006 04:58:50 GMT

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

1. kernel

2. can you please check that you have conntracks enabled in the host (should list conntracks, not empty):

```
# cat /proc/net/ip_conntracks
```

3. can you please answer the questions those in thread:

<http://forum.openvz.org/index.php?t=tree&th=717&mid=3770&&rev=&reveal=>

4. have you changed something in your default RH rules?

the rule "ACCEPT all -- 0.0.0.0/0 0.0.0.0/0" looks strange for me... google shows that it should be a rule for lo interface...

5. I don't see any rules for port 53. why have you decided that DNS should not be filtered out?

6. check iptables -L -v output, as it gets you number of matched packets and you can find number of dropped packets. this can help you to resolve where your packets are dropped.

7. please note one BIG difference. these rules are created by redhat for a single host. where INPUT and OUTPUT chains are for the host node itself. Your VEs are however using FORWARD chain when go outside and inside, i.e. RH-Firewall-1-INPUT rules are implied on VE on both directions, while on host on INPUT only. Do you see why it is so different now?

Subject: Re: DNS Problem

Posted by [goeldi](#) on Wed, 05 Jul 2006 06:56:22 GMT

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

1. kernel = 2.6.8-022stab077.1
2. this file does not exist in /proc, but ip_contracks is loaded.
3. the 2 getent commands give no answer
4. Shall I remove this rule?
5. DNS works on the host

6. This is what I get:

```
# /sbin/iptables -L -v
```

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
```

pkts	bytes	target	prot	opt	in	out	source	destination	
296	20652	RH-Firewall-1-INPUT	all	--	any	any	anywhere	anywhere	

```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

pkts	bytes	target	prot	opt	in	out	source	destination	
21	1312	RH-Firewall-1-INPUT	all	--	any	any	anywhere	anywhere	

```
Chain OUTPUT (policy ACCEPT 190 packets, 16970 bytes)
```

pkts	bytes	target	prot	opt	in	out	source	destination	
------	-------	--------	------	-----	----	-----	--------	-------------	--

```
Chain RH-Firewall-1-INPUT (2 references)
```

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	lo	any	anywhere	anywhere	
2	184	ACCEPT	icmp	--	any	any	anywhere	anywhere	icmp any
0	0	ACCEPT	ipv6-crypt	--	any	any	anywhere	anywhere	
0	0	ACCEPT	ipv6-auth	--	any	any	anywhere	anywhere	
0	0	ACCEPT	udp	--	any	any	anywhere	224.0.0.251	udp dpt:5353
0	0	ACCEPT	udp	--	any	any	anywhere	anywhere	udp dpt:ipp
292	19340	ACCEPT	all	--	any	any	anywhere	anywhere	state
RELATED,ESTABLISHED									
0	0	ACCEPT	tcp	--	any	any	anywhere	anywhere	state NEW tcp
dpt:19150									
0	0	ACCEPT	tcp	--	any	any	anywhere	anywhere	state NEW tcp
dpt:10000									
0	0	ACCEPT	tcp	--	any	any	anywhere	anywhere	state NEW tcp
dpt:ssh									
23	2440	REJECT	all	--	any	any	anywhere	anywhere	reject-with
icmp-host-prohibited									

Subject: Re: DNS Problem
Posted by [dim](#) on Wed, 05 Jul 2006 07:40:40 GMT
[View Forum Message](#) <> [Reply to Message](#)

You need to add:

```
options ip_conntrack ip_conntrack_enable_ve0=1
```

to /etc/modprobe.conf file and reload ip_conntrack module. In 2.6.8 kernels conntrack functionality is prohibited on host node itself by default.

Subject: Re: DNS Problem
Posted by [dev](#) on Wed, 05 Jul 2006 10:40:57 GMT
[View Forum Message](#) <> [Reply to Message](#)

2) sorry, cat /proc/net/ip_conntrack, not cat /proc/net/ip_conntracks

check it once again please

Subject: Re: DNS Problem
Posted by [goeldi](#) on Wed, 05 Jul 2006 10:51:15 GMT
[View Forum Message](#) <> [Reply to Message](#)

it is not there:

```
ls /proc/net
```

```
arp dev_mcast      ip_tables_names  netlink packet route  rt_cache_stat sockstat udp  
dev ip_tables_matches ip_tables_targets netstat raw   rt_cache snmp      tcp   unix
```

Subject: Re: DNS Problem
Posted by [goeldi](#) on Wed, 05 Jul 2006 10:55:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

this is already in /etc/modprobe.conf. I created the file /etc/modules.conf with this line, but it didn't change anything (after restarting iptables and vz).

Subject: Re: DNS Problem
Posted by [dim](#) on Wed, 05 Jul 2006 11:13:14 GMT
[View Forum Message](#) <> [Reply to Message](#)

Please:

- 1) dmesg | grep conntrack
- 2) lsmod
- 3) cat /etc/modprobe.conf
- 3) make sure that ip_conntrack module were reloaded with above option:
service vz stop, service iptables stop, lsmod | grep ip_conntrack

Subject: Re: DNS Problem

Posted by [goeldi](#) on Wed, 05 Jul 2006 12:59:19 GMT

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

dmesg|grep conntrack

ip_conntrack version 2.1 (2033 buckets, 16264 max) - 300 bytes per conntrack

lsmod:

/sbin/lsmod

Module	Size	Used by
vznetdev	12480	7
vzmon	41664	4 vznetdev
af_packet	16360	0
iptable_nat	26492	0
ipt_state	1632	4
ip_conntrack	35752	2 iptable_nat,ipt_state
simfs	3324	3
vzdquota	38736	3 [permanent]
ipt_length	1504	3
ipt_ttl	1632	3
ipt_tcpmss	1920	3
ipt_TCPMSS	3648	3
ipt_multiport	1760	3
ipt_limit	1952	3
ipt_tos	1408	3
lm85	20452	0
i2c_sensor	2144	1 lm85
i2c_isa	1440	0
i2c_i801	6704	0
i2c_dev	7872	0
i2c_core	18416	5 lm85,i2c_sensor,i2c_isa,i2c_i801,i2c_dev
vzdev	1792	3 vznetdev,vzmon,vzdquota
iptable_mangle	4256	3
ipt_REJECT	5568	4
iptable_filter	4096	4
ip_tables	20880	12 iptable_nat,ipt_state,ipt_length,ipt_ttl,ipt_tcpmss,ipt_TCPMSS,ipt_multiport,ipt_limit,ipt_tos,iptable_mangle,ipt_REJECT ,iptable_filter
thermal	10096	0

```
processor      10244 1 thermal
fan            2668 0
button        4408 0
battery       7052 0
asus_acpi     8920 0
ac            3084 0
uhci_hcd      28656 0
ehci_hcd      25604 0
usbcore       100356 4 uhci_hcd,ehci_hcd
pciehp        90476 0
eepro100      25644 0
mii           4384 1 eepro100
natsemi       24704 0
```

```
/etc/modprobe.conf:
/etc/modprobe.conf
alias eth0 natsemi
alias snd-card-0 snd-via82xx
options snd-card-0 index=0
install snd-via82xx /sbin/modprobe --ignore-install snd-via82xx && /usr/sbin/alsactl restore
>/dev/null 2>&1 || :
remove snd-via82xx { /usr/sbin/alsactl store >/dev/null 2>&1 || : ; } /sbin/modprobe -r
--ignore-remove snd-via82xx
alias usb-controller uhci-hcd
options ip_conntrack ip_conntrack_enable_ve0=1
```

```
then:
# /sbin/service vz stop
Shutting down VPS 194
Shutting down VPS 193
Shutting down VPS 192
Stopping OpenVZ: [ OK ]
# /sbin/service iptables stop
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: nat mangle filter [ OK ]
Unloading iptables modules: [ OK ]
# /sbin/lsmmod | grep ip_conntrack
```

Subject: Re: DNS Problem
Posted by [dev](#) on Wed, 05 Jul 2006 17:22:19 GMT
[View Forum Message](#) <> [Reply to Message](#)

uhhh.... can you simply give me a temporary root access to your node (dev @ openvz org)? I feel there is something really simple happening.

if module ip_conntrack is loaded properly there MUST be /proc/net/ip_conntrack file in host

system.

you can recheck it on any other std Linux system yourself and load ip_conntrack on openvz manually with modprobe argument:

```
# modprobe ip_conntrack ip_conntrack_enable_ve0=1
```

Subject: Re: DNS Problem

Posted by [goeldi](#) on Wed, 05 Jul 2006 18:49:46 GMT

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

I did a reboot and now there is /proc/net/ip_conntrack:

```
# cat /proc/net/ip_conntrack
```

```
tcp    6 431999 ESTABLISHED src=195.141.143.41 dst=195.141.143.42 sport=56959 dport=22
src=195.141.143.42 dst=195.141.143.41 sport=22 dport=56959 [ASSURED] use=1
```

195.141.143.42 is the ip of the host. .41 is one of the hosts that can log in via ssh (I restricted ssh logins via iptables, because I am paranoid . I don't know, why this IP (.41) shows up in /proc/net/ip_conntrack. But perhaps this gives you a hint?

Subject: Re: DNS Problem

Posted by [dev](#) on Thu, 06 Jul 2006 04:46:20 GMT

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

fine. now you have ip_conntrack module loaded correctly and can check your iptables rules to find the bad one.

first, I would check that if the only FORWARD chain rule is removed everything starts to work fine in your VE (dns resolve):

```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

```
pkts bytes target prot opt in out source destination
```

```
21 1312 RH-Firewall-1-INPUT all -- any any anywhere anywhere
```

Subject: Re: DNS Problem

Posted by [goeldi](#) on Thu, 06 Jul 2006 06:18:29 GMT

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

Yes, this was the last problem. Now resolving works in the VE.

Thank you very much!

Subject: Re: DNS Problem
Posted by [dev](#) on Thu, 06 Jul 2006 10:15:28 GMT
[View Forum Message](#) <> [Reply to Message](#)

I hope now your question about OpenVZ security model is answered?

Subject: Re: DNS Problem
Posted by [goeldi](#) on Thu, 06 Jul 2006 17:53:25 GMT
[View Forum Message](#) <> [Reply to Message](#)

Yes, it is.

But this should be available in the installation guide too. There is written to simply deactivate firewall and selinux.

Thank you again for your 1st class help!

Subject: Re: ***SOLVED*** DNS Problem
Posted by [AandM_Hosting](#) on Wed, 20 Sep 2006 19:35:54 GMT
[View Forum Message](#) <> [Reply to Message](#)

I apologize for bringing back an old thread but I am having the same problem and rather than open a new one i figured it would be better to just reopen this one. I have tried all of the steps and I still do not have an ip_contrack file I tried a reboot like the op did and fixed it for him but i still do not have it. Are there any other ways to resolve this?
