
Subject: iptables with nat inside guest
Posted by [tpso](#) on Sun, 28 Oct 2007 21:42:49 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

I trying to use iptables inside a guest, to do some port-forwarding.

The host has a lot of ip-tables running to separate access from the different guests, so all iptables kernel modules should be loaded.

When I run : iptables -L
inside the guest it shows empty chain - which I expect.

When I try to run the following command:

```
/sbin/iptables -t nat -A PREROUTING -p tcp -i venet0 -d  
192.168.217.200 --dport 25 -j DNAT --to 192.168.217.200:1025
```

it fails with an error :

```
iptables v1.2.11: can't initialize iptables table `nat': Table does not exist (do you need to insmod?)  
Perhaps iptables or your kernel needs to be upgraded.
```

Any hint's on what is wrong?

Host is running: vmlinuz-2.6.18-8.1.4.el5.028stab035
guest is a contos 5.

regards
Thomas

Subject: Re: iptables with nat inside guest
Posted by [Valmont](#) on Mon, 29 Oct 2007 14:44:09 GMT
[View Forum Message](#) <> [Reply to Message](#)

man and search your best friends. Laziness - not.

```
# vzctl --help | grep iptables  
  [--iptables <name>] [--disabled <yes|no>]
```

From vzctl man page:

Iptables control parameters

--iptables name

Restrict access to iptables modules inside a VE (by default all iptables modules that are loaded in the host system are accessible inside a VE).

You can use the following values for name: iptable_filter, iptable_mangle, ipt_limit, ipt_multiport, ipt_tos, ipt_TOS, ipt_REJECT, ipt_TCPMSS, ipt_tcpmss, ipt_ttl, ipt_LOG, ipt_length, ip_conntrack, ip_conntrack_ftp, ip_conntrack_irc, ipt_conntrack, ipt_state, ipt_helper, iptable_nat, ip_nat_ftp, ip_nat_irc, ipt_REDIRECT, xt_mac.

Please, be assured, that all necessary iptables modules are loaded before the start of vps

Subject: Re: iptables with nat inside guest
Posted by [tpso](#) on Tue, 30 Oct 2007 19:05:14 GMT
[View Forum Message](#) <> [Reply to Message](#)

I have already found the same quote in the man-pages.

It states that : by default all iptables modules that are loaded in the host system are accessible inside a VE.

As mentioned in my first post, I already have iptables running on the host (including NAT), why I assume that all necessary kernel modules should be loaded.

I have tried to stop and restart the VPS so the iptables modules is loaded before VPS start.

So i'm still interesting in any hints.

Most post (and wiki documentation) is about iptables on the host handling VPS access - and I have it all up and running.

But I can't run iptables inside the VPS.

Is there any non standard modules required ?

Regards Thomas

Subject: Re: iptables with nat inside guest
Posted by [Valmont](#) on Wed, 31 Oct 2007 11:18:49 GMT
[View Forum Message](#) <> [Reply to Message](#)

```
# grep -i iptables /etc/vz/vz.conf
## IPv4 iptables kernel modules
IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS
ipt_tcpmss ipt_ttl ipt_length"

# lsmod | grep nat
iptables_nat      13188  1
ip_nat            22288  2 vzrst,iptables_nat
ip_conntrack     60356  7
vzrst,vzcpt,ip_conntrack_netbios_ns,xt_conntrack,xt_state,iptables_nat,ip_nat
nfnetlink        10648  2 ip_nat,ip_conntrack
ip_tables        18760  3 iptable_filter,iptable_mangle,iptables_nat
x_tables         19204  18
xt_length,ipt_ttl,xt_tcpmss,ipt_TCPMSS,xt_multiport,xt_limit,ipt_tos,ipt_recent,xt_conntrack,ipt_R
EJECT,ipt_LOG,xt_state,xt_MARK,iptables_nat,ip_tables,ip6t_REJECT,xt_tcpudp,ip6_tables
# vzctl start 115
...
# vzctl enter 115
# iptables -t nat -nvL
iptables v1.3.5: can't initialize iptables table `nat': Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.
^D
# vzctl set 115 --iptables "iptables iptable_nat iptable_filter iptable_mangle ip_conntrack ipt_conntrack
ipt_REDIRECT ipt_REJECT ipt_multiport ipt_helper ipt_LOG ipt_state" --save
Saved parameters for VE 115

# vzctl restart 115
...
# vzctl enter 115
# iptables -t nat -nvL
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in  out  source          destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in  out  source          destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in  out  source          destination
```

Subject: Re: iptables with nat inside guest
Posted by [Valmont](#) on Wed, 31 Oct 2007 11:27:54 GMT
[View Forum Message](#) <> [Reply to Message](#)

certainly, you can add iptable_nat into /etc/vz/vz.conf &&
service vz restart.

It should work too, but I didn't try it

Subject: Re: iptables with nat inside guest
Posted by [tpso](#) on Thu, 01 Nov 2007 14:18:32 GMT
[View Forum Message](#) <> [Reply to Message](#)

Valmont wrote on Wed, 31 October 2007 12:27 certainly, you can add iptable_nat into
/etc/vz/vz.conf &&
service vz restart.

It should work too, but I didn't try it

It Does !! - or actually I know it works if all the iptables parameters from you vzctl ... --iptables
command is moved top vz.conf . The contrack parameters was allso missing.

Thanks a lot. Maybe the docs should be change, so the paragraph stating that "by default all
iptables modules that are loaded in the host system are accessible inside a VE" is changed to a
reference to the vz.conf file.

That was the point that got me off the track.

I know I haven't modified my vz.conf, so i mistakensly believed i could reley on default settings.

Thanks again.

/Thomas

Subject: Re: iptables with nat inside guest
Posted by [Valmont](#) on Thu, 01 Nov 2007 14:25:25 GMT
[View Forum Message](#) <> [Reply to Message](#)

You are welcome

tpso wrote on Thu, 01 November 2007 17:18
Maybe the docs should be change, so the paragraph stating that "by default all iptables modules
that are loaded in the host system are accessible inside a VE" is changed to a reference to the
vz.conf file.

/Thomas

Yeah, in this point I will agree with you. After your post I was wondering about availability of all modules in docs.
