Subject: Can't use IPTables inside a VE - still broken
Posted by jarcher on Wed, 11 Apr 2007 09:52:22 GMT
View Forum Message <> Reply to Message

Hi All...

I'm running Debian Etch AMD64 with kernel 2.6.18. I am unable to use IPTables inside a VPS. IPTables seems to work fine on the HN. If I try to use IPTables inside a VPS I see this:

Quote:
vps1001:/# iptables -t nat -L -v --line-number
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.

I looked at the wiki entry for using NAT with VE for private IPs here:

http://wiki.openvz.org/Using_NAT_for_VE_with_private_IPs

But it was not much help.

Is it possible to use IPTables inside a VPS and if so, what am I missing? Thanks.

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by curx on Wed, 11 Apr 2007 12:16:08 GMT
View Forum Message <> Reply to Message

Hi,

kernel iptables_nat module is loaded in VE0 (HN) ...?
VE0_# lsmod | grep ^iptable_nat

when not load it:
VE0_# modprobe iptable_nat

enable iptable_nat in VE
VE0_# vzctl set <VEID> --iptables iptable_nat --save

restart your VE
VE0_# vzctl restart <VEID>

check it
VE0_# vzctl exec <VEID> iptables -t nat -L -v --line-number

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by jarcher on Wed, 11 Apr 2007 19:43:48 GMT
View Forum Message <> Reply to Message

Thanks Thorsten, that did it!

The only anomoly was that it refused to make the changes while the VPS was running, so I just put it down, made the change then started it.

Thanks very much! Maybe I'll make a wiki entry on that, once I review it a bit more.

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by jarcher on Wed, 11 Apr 2007 21:41:44 GMT
View Forum Message <> Reply to Message

Well, as it turns out, this worked to get the list of chains to work, but I am unable to add rules. Here is the error I get when I try:

iptables -t nat -A PREROUTING -d 72.46.65.43 -p tcp --dport 43 -j REDIRECT --to-ports 10043
iptables: No chain/target/match by that name

I get the same thing if I try for the filters table:

iptables -A PREROUTING -p tcp -m tcp -d 72.46.65.43 --dport 43 -j DNAT --to 72.46.65.43:10043
iptables: No chain/target/match by that name

I did a little searching and found another thread with this problem:

http://forum.openvz.org/index.php?t=msg&goto=8384&#m sg_8384

I tried:

modprobe xt_tcpudp
modprobe ip_conntrack ip_conntrack_enable_ve0=1

That didn't work. I then ran:

depmode –a

But that didn't help either. And I restarted the VPS after each step.

I am now running the latest Debian AMD64 kernel (Dated April 10):

2.6.18-openvz-amd64 #1 SMP Tue Apr 10 19:34:07 MSD 2007 x86_64 GNU/Linux

Thanks very much...

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by jarcher on Fri, 13 Apr 2007 06:42:53 GMT
View Forum Message <> Reply to Message

Guys, any other ideas on this?

Thanks...

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by jarcher on Wed, 18 Apr 2007 06:33:13 GMT
View Forum Message <> Reply to Message

Well I have tried some more things and still no luck. Anyone have any more suggestions? Pretty please?

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by Vasily Tarasov on Wed, 18 Apr 2007 06:56:31 GMT
View Forum Message <> Reply to Message

Can you give me an access to the node?

Vasily.

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by jarcher on Fri, 20 Apr 2007 02:28:15 GMT
View Forum Message <> Reply to Message

Vasily Tarasov wrote on Wed, 18 April 2007 02:56Can you give me an access to the node?

Vasily.

Yes, I'll PM you tonight, thank you!!

Subject: Re: Can't use IPTables inside a VE, here iptable_nat
Posted by chase on Thu, 03 May 2007 23:26:53 GMT
View Forum Message <> Reply to Message

jarcher wrote on Wed, 11 April 2007 17:41Well, as it turns out, this worked to get the list of chains to work, but I am unable to add rules. Here is the error I get when I try:

iptables -t nat -A PREROUTING -d 72.46.65.43 -p tcp --dport 43 -j REDIRECT --to-ports 10043
iptables: No chain/target/match by that name

Not sure (worked for me) but I think if you want to do REDIRECT you need to make sure that iptables module is loaded. Edit:

/etc/vz/vz.conf
IPTABLES="ipt_REDIRECT ....."

/etc/sysconfig/iptables-config
IPTABLES_MODULES="ipt_REDIRECT ....."

After I did that I could run my rule of
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 2525 -j REDIRECT --to-ports 25