
Subject: *SOLVED* iptables: DNAT with --dport option inside ve
Posted by [rudiross](#) on Fri, 08 Sep 2006 00:22:06 GMT

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

Hi all!

I am trying to forward some ports from inside a VE to another host.

The following works:

```
root@srv03:~# iptables -t nat -A PREROUTING -p tcp -i venet0 -j DNAT --to 10.4.0.2
```

The following does not:

```
root@srv03:~# iptables -t nat -A PREROUTING -p tcp --dport 80 -i venet0 -j DNAT --to 10.4.0.2:80
```

Error message:

```
iptables: No chain/target/match by that name
```

Following modules are loaded via <vpsid>.conf:

```
IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS  
ipt_tcpmss ipt_ttl ipt_length iptable_nat ip_conntrack ip_conntrack_ftp ipt_conntrack ipt_helper  
ipt_state"
```

Can anyone tell me whether it is possible to perform DNAT with selected ports from inside a VE?

TIA

Rudi

Subject: Re: iptables: DNAT with --dport option inside ve
Posted by [Vasily Tarasov](#) on Fri, 08 Sep 2006 07:14:45 GMT

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

Hello,

For me both these commands work fine...

What kernel version do you use?

One more trick. Try to do the following:

- 1) do the command you need (... --dport ...) on HN
- 2) remove this rule on HN
- 3) enter VE and do the same command in VE

HTH,

vass.

Subject: Re: iptables: DNAT with --dport option inside ve
Posted by [rudiross](#) on Fri, 08 Sep 2006 08:18:21 GMT

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

Hi Vass,

your trick made it work. Thank you very much. After loading the rule on the HW node and removing it again, it worked inside the VE (with both tcp and udp).

After rebooting the HW node, it stopped working again, so for now I add and remove one rule with the --dport option in it via startup script.

Does anybody have an explanation why this is necessary?

BTW, I am running 2.6.16-026test017 with iptables v1.3.3.

Regards,

Rudi

Subject: Re: iptables: DNAT with --dport option inside ve
Posted by [Vasily Tarasov](#) on Fri, 08 Sep 2006 08:37:45 GMT

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

Quote:Does anybody have an explanation why this is necessary?

Explanation is very easy

To add rule in VE - appropriate modules should be loaded on HN.

If you give the same iptables command on HW - needed modules are loaded. =)

So, actually you can just manually load needed modules on HW, and that's all.

Good luck!

Subject: Required module for DNAT with --dport option inside ve
Posted by [rudiross](#) on Sat, 09 Sep 2006 15:03:21 GMT

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

Just as a sidenote:

The required module seems to be xt_tcpudp.
