
Subject: IP Contrack FTP in VE

Posted by [ulver](#) on Wed, 30 Sep 2009 15:49:58 GMT

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

Hello everybody,

I'm trying to have ftp access (in passive mode) to a VE protected by iptables. On a physical server, i can get this working by enabling ip_contrack & ip_contrack_ftp but i doesn't work in the VE.

I've already read this :

<http://forum.openvz.org/index.php?t=msg&goto=13133&>

But it doesn't work for me

```
# uname -r
2.6.26-2-openvz-amd64
# cat /etc/debian_version
5.0.2
# grep IPTABLES /etc/vz/vz.conf
IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS
ipt_tcpmss ipt_ttl ipt_length ipt_state ip_contrack_ftp ip_contrack"
# cat /etc/modules
[...]
loop
ip_contrack
ip_contrack_ftp
# lsmod | grep connt
nf_contrack_ftp      12728  0
nf_contrack_ipv4    24352  16 iptable_nat,nf_nat
nf_contrack         82688  5 nf_contrack_ftp,iptable_nat,nf_nat,nf_contrack_ipv4,xt_state
```

I manage to connect to the VE by ftp, but the DIR command doesn't work (the port is blocked on the VE by the firewall : the ip contrack ftp doesn't seem to work).

If you have any idea...

Thanks in advance

Subject: Re: IP Contrack FTP in VE

Posted by [Erdbeergulasch](#) on Tue, 16 Mar 2010 21:29:44 GMT

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

I have currently the same Problem, is there now a solution for this?

I think this is, because the module is now named nf_contrack_ftp and not ip_contrack_ftp anymore.

but when i enter in IPTABLES the name nf_contrack_ftp, then, i get, that this is not a valid module.

greetz

Subject: Re: IP Contrack FTP in VE
Posted by [curx](#) on Wed, 17 Mar 2010 18:37:11 GMT
[View Forum Message](#) <> [Reply to Message](#)

ip_contrack_ftp is an alias for nf_contrack_ftp, see:

```
$ modinfo nf_contrack_ftp
filename:      /lib/modules/2.6.26-2-openvz-amd64/kernel/net/netfilter/nf_c ontrack_ftp.ko
alias:        ip_contrack_ftp <----!!!
(...)
```

Are the container(s) restarted after changeing the vz.conf ?

Bye,
Thorsten

Subject: Re: IP Contrack FTP in VE
Posted by [Erdbeergulasch](#) on Thu, 18 Mar 2010 00:44:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

thx for answer,
this is true, that nf_contrack_ftp is a alias, but i think it is not loaded into the ct.

yes, the ct was restartet, after manually loading the nf_contrack_ftp package.

and you can't set in the /etc/vz/vz.conf at the section IPTABLES, the new name of the module (nf_contrack_ftp), because when i enter nf_contrack_ftp to this file, than i get the error,
Warning: Unknown iptable module: nf_contrack_ftp, skipped

i think, that the problem is, that openvz thinks, the modules name is ip_contrack_ftp and so it looks for it, but openvz doesn't find it (because it is a alias and aliases are ignored in openvz) and so it could not be loaded.

I have looked up in the file ip_tables_matches but i haven't found the module ip_contrack_ftp
root@ct101:/# cat /proc/net/ip_tables_matches
owner
owner
mac
state

helper
conntrack
conntrack
length
ttl
tcpmss
multiport
multiport
limit
tos
tos
dscp
udplite
udp
tcp
icmp

what can i do?

Subject: Re: IP Conntrack FTP in VE
Posted by [curx](#) on Thu, 18 Mar 2010 08:19:13 GMT
[View Forum Message](#) <> [Reply to Message](#)

found your post on:

<http://www.linux-forum.de/iptables-und-ftp-und-logprobleme-b-er-openvz-auf-hn-deb-lenny-34622.html>

```
> IPTABLES="ip_tables ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle  
ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ip_conntrack ip_conntrack_ftp ip_conntrack_irc ipt_LOG  
ipt_conntrack ipt_helper ipt_state iptable_nat ip_nat_ftp ip_nat_irc ipt_TOS ipt_REDIRECT  
xt_mac ipt_owner"
```

esp. ipt_state is an alias, too

```
# modinfo xt_state  
filename:      /lib/modules/2.6.26-2-openvz-amd64/kernel/net/netfilter/xt_state.ko  
alias:        ip6t_state  
alias:        ipt_state  
(...)
```

but a xt_state is not show in you ct config, but used (ip_targets_match : state)

loaded kmod module in ct0 (=hardwarenode) can be used in ct without configuration.

for debugging:

- load ipt ruleset in ct
- make a connection to your ct via ftp:
- track entries on ct0 and ct in the /proc/net/ip_contrack

Bye,
Thorsten

Subject: Re: IP Contrack FTP in VE
Posted by [ilass](#) on Sun, 21 Mar 2010 11:50:29 GMT
[View Forum Message](#) <> [Reply to Message](#)

Confirm.

Using kernel-PAE-2.6.27-kiprensky.1.i686.rpm from official page, using my distro supplied kernel, my own build using patch-kiprensky.1-combined.gz, i get same result as described. I also tried this on different HW (all x86 platform).

Some info about my system(s)/configs:

Hardware node

```
# uname -m  
i686
```

```
# uname -r  
2.6.27-kiprensky.1-PAE
```

```
# lsmod |egrep '(conn|state)'
```

```
xt_state          5896  4  
nf_conntrack_ipv4 14104  8 iptable_nat,nf_nat  
x_tables          15756  8  
ipt_ttl,ipt_REJECT,xt_tcpudp,xt_state,xt_hashlimit,iptable_nat,ip_tables,xt_multiport  
nf_conntrack_ftp  11060  0  
nf_conntrack      60820  5 xt_state,iptable_nat,nf_nat,nf_conntrack_ipv4,nf_conntrack_ftp
```

```
# egrep 'IPTABLES' /etc/vz/conf/1003.conf
```

```
IPTABLES="ip_tables iptable_filter iptable_nat iptable_mangle ip_contrack ip_contrack_ftp  
ipt_state ipt_multiport ipt_helper"
```

On hardware node no iptables rules configured in FORWARD chain and tables 'raw', 'mangle', 'nat'.

Please look at module refcount: it 0, but VE started. On 2.6.18 (production) everything is ok and refcount ~ 18. Is this normal?

VE

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p tcp -m multiport --dports 21,80,873 -m tcp --tcp-flags FIN,SYN,RST,ACK
```

```
SYN -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type 8 -m hashlimit
--hashlimit-upto 30/sec --hashlimit-mode dstip --hashlimit-name echo_request -j ACCEPT
```

```
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -p udp -m udp --sport 1024:65535 --dport 53
-j ACCEPT
```

```
# cat /proc/net/ip_tables_matches
ttl
udplite
udp
tcp
state
hashlimit
hashlimit
icmp
multiport
multiport
```

```
# cat /proc/net/ip_tables_names
mangle
filter
```

Using same rules on HN i get with working ftp in passive/active (production rules mostly identical), also using

```
# iptables -A FORWARD -m helper --helper ftp -j ACCEPT
```

on HN, and then connecting to ftp, i see packet count increment for this rule: so nf_conntrack_ftp matches packets. Tcpcdump on venet0 also confirms this.

I also try to establish connection from VE to ftp and get same result. Modes tried: passive, active.

Subject: Re: IP Conntrack FTP in VE
Posted by [ichilton](#) on Fri, 09 Apr 2010 14:25:49 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

Did anyone ever solve this? - i'm having exactly the same problem.

Thanks,

Ian

Subject: Re: IP Contrack FTP in VE
Posted by [ilass](#) on Tue, 13 Apr 2010 11:38:32 GMT
[View Forum Message](#) <> [Reply to Message](#)

This happens due to missed virtualization code in `nf_contrack_ftp`
(and probably others `nf_contrack_h323`, `nf_contrack_sip`, ..., `nf_nat_ftp` ...) in comparison with
2.6.18 kernels.

Probably 2.6.32 also affected. Can any one confirm this?

If in output of

```
$ lsmod | egrep 'nf_contrack_ftp'
```

you see `nf_contrack_ftp` refcount (Used by) equal to 0 or less than number of VE you run this
might indicate problem (testing true server in container is more welcome).

This is true BUG.

I will make detailed report in bugzilla in few days.

Subject: Re: IP Contrack FTP in VE
Posted by [ichilton](#) on Tue, 13 Apr 2010 11:45:25 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

ok, thanks.

Ian

Subject: Re: IP Contrack FTP in VE
Posted by [ilass](#) on Tue, 13 Apr 2010 12:34:48 GMT
[View Forum Message](#) <> [Reply to Message](#)

Bug report created.

http://bugzilla.openvz.org/show_bug.cgi?id=1491
