
Subject: ip_conntrack_ftp Not Working in Container
Posted by [ichilton](#) on Fri, 09 Apr 2010 14:52:25 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

I'm trying to connect out from a Debian container to an external FTP server.

It works fine from the host node (with the same firewall) and it works fine from the container when I take down the firewall, but with the firewall up, it connects but will not do the directory listing:

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> ls
200 PORT command successful. Consider using PASV.
425 Failed to establish connection.
ftp>
```

It looks like the ip_conntrack_ftp module doesn't seem to be working.

It's in both vz.conf and the container's own config file - 101.conf:

```
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
ip_conntrack ipt_helper ipt_state iptable_nat ip_nat_ftp ip_nat_irc ipt_TOS"
```

Host and container are both running Debian:

Host Node:

```
# uname -a
Linux 2.6.26-2-openvz-amd64 #1 SMP Tue Mar 9 23:10:10 UTC 2010 x86_64 GNU/Linux
```

```
# lsmod |grep ftp
nf_nat_ftp          7296  0
nf_nat             22548  3 nf_nat_irc,nf_nat_ftp,iptable_nat
nf_conntrack_ftp  12728  1 nf_nat_ftp
nf_conntrack       82688  10
nf_nat_irc,nf_nat_ftp,iptable_nat,nf_nat,xt_helper,xt_conntrack,nf_conntrack_irc,nf_conntrack_ftp,
xt_state,nf_conntrack_ipv4
```

Container:

```
$ uname -a  
Linux 2.6.26-2-openvz-amd64 #1 SMP Tue Mar 9 23:10:10 UTC 2010 i686 GNU/Linux
```

Any ideas why it's not working?

Thanks,

Ian

Subject: Re: ip_conntrack_ftp Not Working in Container
Posted by [ddpaul](#) on Wed, 14 Apr 2010 12:23:35 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi.

The same thing on Centos 5.4 and x86_64 host node

```
# uname -a  
Linux vz.hostnode.tld 2.6.18-164.15.1.el5.028stab068.9 #1 SMP Tue Mar 30 18:07:38 MSD 2010  
x86_64 x86_64 x86_64 GNU/Linux
```

ip_conntrack_ftp is loaded but doesn't work inside 32-bit container:

```
# uname -a  
Linux ct.container.tld 2.6.18-164.15.1.el5.028stab068.9 #1 SMP Tue Mar 30 18:07:38 MSD 2010  
i686 i686 i386 GNU/Linux
```

```
# ftp ftp.bgbilling.ru  
Connected to ftp.bgbilling.ru (81.30.195.156).  
220 (vsFTPd 2.0.5)  
Name (ftp.bgbilling.ru:root): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
227 Entering Passive Mode (81,30,195,156,26,135)  
ftp: connect: No route to host  
ftp> quit  
221 Goodbye.
```

There are some dropped packets by iptables and only one record in /proc/net/ip_contrack:

```
# cat /var/log/iptables.log
Apr 14 15:58:08 vz kernel: IN=venet0 OUT=eth0 SRC=10.0.0.213 DST=81.30.195.156 LEN=60
TOS=0x00 PREC=0x00 TTL=64 ID=19868 DF PROTO=TCP SPT=45315 DPT=6791
WINDOW=5840 RES=0x00 SYN URGP=0
Apr 14 15:58:11 vz kernel: IN=venet0 OUT=eth0 SRC=10.0.0.213 DST=81.30.195.156 LEN=60
TOS=0x00 PREC=0x00 TTL=64 ID=19869 DF PROTO=TCP SPT=45315 DPT=6791
WINDOW=5840 RES=0x00 SYN URGP=0
```

```
# cat /proc/net/ip_contrack | grep 81.30.195.156
tcp 6 431995 ESTABLISHED src=10.0.0.213 dst=81.30.195.156 sport=40642 dport=21
packets=12 bytes=673 src=81.30.195.156 dst=10.0.0.213 sport=21 dport=40642 packets=8
bytes=582 [ASSURED] mark=0 secmark=0 use=1
```

At the same time it works while connecting from HN:

```
# ftp ftp.bgbilling.ru
Connected to bgbilling.ru.
220 (vsFTPD 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (ftp.bgbilling.ru:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (81,30,195,156,170,167)
150 Here comes the directory listing.
drwxr-xr-x 3 500 100 4096 Mar 10 18:28 pub
226 Directory send OK.
ftp>
```

There are no dropped packets by iptables and two corresponding records in /proc/net/ip_contrack in this case:

```
# cat /proc/net/ip_contrack | grep 81.30.195.156
tcp 6 431903 ESTABLISHED src=10.0.0.196 dst=81.30.195.156 sport=42787 dport=21
packets=17 bytes=970 src=81.30.195.156 dst=10.0.0.196 sport=21 dport=42787 packets=13
bytes=982 [ASSURED] mark=0 secmark=0 use=1
tcp 6 23 TIME_WAIT src=10.0.0.196 dst=81.30.195.156 sport=59495 dport=43687 packets=4
bytes=216 src=81.30.195.156 dst=10.0.0.196 sport=43687 dport=59495 packets=4 bytes=277
```

[ASSURED] mark=0 secmark=0 use=1

Also ip_contrack_ftp works fine on 32-bit host nodes in both cases (from HN and container).
Do you have any clues?

Thanks in advance,
Pavel
