
Subject: Re: The problem of iptables on FC4
Posted by [dev](#) on Sun, 19 Feb 2006 07:21:47 GMT
[View Forum Message](#) <> [Reply to Message](#)

I didn't fully got what doesn't work in your case.
First, you have the following rules in your iptables.sh

```
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP
...
$IPTABLES -A INPUT -p tcp -d 123.456.789.012/32 -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -s 123.456.789.012/32 -j ACCEPT
```

which means that only 123.456.789.012/32 subnetwork should work fine.

Next, VPS networking requires IP forwarding, so it won't work with this rule:
\$IPTABLES -P FORWARD DROP

Also, I would notice, that by default in OVZ kernel conntracks are disabled in host system. This is done so for performance reasons (no double conntracking). But if really needed you can enable it by:

```
/sbin/modprobe ip_conntrack "ip_conntrack_enable_ve0=1"
```