
Subject: Re: IP Conntrack /DST Cache Overflow issue
Posted by [pavel.odintsov](#) on Sun, 10 Nov 2013 22:30:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello, KevinH!

I will recommend you to enlarge a buffer for conntrack buckets up to 1-3 millions (it's ok for modern systems).

You can do it by a following commands:
edit /etc/sysctl.conf and fix:
net.ipv4.netfilter.ip_conntrack_max=1548576

Apply changes:

sysctl -p

You can entirely disable connection tracking for certain CT with following commands:

```
iptables -t raw -A PREROUTING -d VPS_IP -j NOTRACK  
iptables -t raw -A PREROUTING -s VPS_IP -j NOTRACK
```

Be aware about using last command, it result to completely disable RELATED/ESTABLISHED flags to working inside container.

In addition I recommend you to upgrade from pretty old kernels 2.6.18 to modern 2.6.32 kernel series. Oh, sorry, I forgot to specify link, it's here https://openvz.org/028_to_042_kernel_upgrade
