

---

Subject: conntrack in OpenVZ 7  
Posted by [iblinger](#) on Mon, 09 Jul 2018 08:06:24 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hello.

In OpenVZ 6 when we use conntrack in container, connections are tracked in container and do not appear in `/proc/net/nf_conntrack` on node.

In OpenVZ 7 when we use conntrack in container, connections appear in `/proc/net/nf_conntrack` on node.

Is it normal that connections which are tracked in container appear in `/proc/net/nf_conntrack` on OpenVZ 7 node?

On OpenVZ 6 we can execute on node `iptables -j NOTRACK` for some user's connections to container and in container definition of state of these connections continued to work.

If we execute NOTRACK on OpenVZ 7, we will not be able to use conntrack for these connections in container.

Example.

After adding this rule to node:

```
iptables -t nat -A PREROUTING ! -d NODE.IP.ADDR.ES -i br0 -p tcp -m multiport ! --sports 25,465,587 -j NOTRACK
```

on OpenVZ 6 node we can use conntrack in container for ports that are not equal 25,465,587 and we can't use conntrack in container on OpenVZ 7 node.

Is there any way to execute NOTRACK and after that track these connections in container?

Thank you.

---