
Subject: Problem with Traffic Accounting Tutorial.. bug?

Posted by [maxh](#) on Fri, 14 May 2010 10:46:28 GMT

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

Hi guys.

Here's the deal: Tonight one of my openvz-customer-vservers got hacked. The kid ran some DoS-Attack with a bunch of traffic. I can see in the accounting by my provider that I made ~200 GB+ more than I usually do. The traffic stopped by the time I killed the hack.

I have traffic accounting running for the vserver (used this tutorial.

http://wiki.openvz.org/Traffic_accounting_with_iptables)

The tool is running by cron every 10 min.

The problem is, that the hacker changed the ifconfig and a bunch of other bins in the vserver. Is anything in the vserver used for the accounting? That's pretty bad because customers that are familiar with linux might find that out, too.

Thank you for your help!

Max
