Subject: Script to delete VM IP on DDoS attack?
Posted by postcd on Wed, 25 Sep 2013 13:37:41 GMT
View Forum Message <> Reply to Message

Hi,

on my OpenVZ some VM was under ddos attack and this attack was overloading the node server, unsure what would happen if i was not noticed about this attack.

So my question is if we can setup some bash script, which will get some value like high load on VM or excessive connections to some VPS, some evidence and then automatically remove IP from that VPS by command: vzctl set VMID --ipdel IPADDRESS --save and send mail to admin?

Any idea how and what value to extract as to be a sign of DDoS?

---
in my case i temporarilly set a script which will delete one VPS IP when load on node is above 30.00 (8 cpus) and send me an email:

```
#!/bin/bash
THRESHOLD="30.00"
LOAD=$(uptime | sed -e "s/^.*[a-z]: //; s/,.*//")
echo "One minute load average = $LOAD"
if test $(echo "$LOAD > $THRESHOLD" | bc -l) == 1 ; then
        vzctl set VMID --ipdel IPADDRESS --save
        mail -s "Server load is $LOAD, VMID IP deleted" myemail@gmail.com
else
        echo "Load average not too high "
fi
exit 0
```

then cronjob every half minute (crontab -e):

```
*/1 * * * * /foo/delip440vmonload.sh >/dev/null 2>&1
* * * * * sleep 30; /foo/delip440vmonload.sh >/dev/null 2>&1
```