Subject: Re: Bandwidth limiting crashes the machine
Posted by eugeniopacheco on Sat, 06 May 2006 10:22:17 GMT
View Forum Message <> Reply to Message

Hi,

Thanks a lot for all the answers, it really helped me.

Right after I posted this problem with bandwidth limit, I also thought of using the device venet0, but it only limited the incoming bandwidth, not the outgoing, so I had the idea of making another script and it's running 3 days ago with no problems (at least up to now) Here it goes:

```
#!/bin/bash

DEV=eth0

tc qdisc del dev $DEV root
tc qdisc add dev $DEV root handle 1: cbq avpkt 1000 bandwidth 100mbit
tc class add dev $DEV parent 1: classid 1:1 cbq rate 1024kbit allot 1500 prio 5 bounded isolated
tc filter add dev $DEV parent 1: protocol ip prio 16 u32 match ip src x.x.x.x flowid 1:1
tc qdisc add dev $DEV parent 1:1 sfq perturb 10


DEV2=venet0

tc qdisc del dev $DEV2 root
tc qdisc add dev $DEV2 root handle 1: cbq avpkt 1000 bandwidth 100mbit
tc class add dev $DEV2 parent 1: classid 1:1 cbq rate 1024kbit allot 1500 prio 5 bounded isolated
tc filter add dev $DEV2 parent 1: protocol ip prio 16 u32 match ip dst x.x.x.x flowid 1:1
tc qdisc add dev $DEV2 parent 1:1 sfq perturb 10
```

This script limits the bandwidth for the ip x.x.x.x to 1024kbit/s both incoming and outgoing. It really works... Even if a client of yours use their vps to ddos, it will be stopped at 1024kbit/s, so if your machine has a 100mbit port it won't even affect your machine. Even if he gets ddos, it will also slow down the packages that comes to the machine and goes to the VPS. WARNING: From my own experience, I got one ip that was being ddosed, and it was slowing the entire VPS down, only the VPS, for it was limited. The problem is, I made the most stuppid thing and tried to delete the ip address. It wasn't a good choice, for the incoming ddos now was going to the host machine, for the ip address was already routed to go through the host machine. The packets went to the host machine and stopped there since they couldn't find the ip address they were originally going to. RESULT: the entire machine was affected... So if you guys get ddosed to 1 ip, just limit the bandwidth to 32kbit/s let's say and ask the DC to block it on the router, DO NOT delete the ip address or your entire machine will be affected.

Now, there is another script I'm using to check bandwidth used (incoming and outgoing). It's by using ip tables and thanks to someone else that have posted it.

You run it on the host machine...

```
#!/bin/bash
DEV=eth0
iptables -A FORWARD -o $DEV -s x.x.x.x
iptables -A FORWARD -i $DEV -d x.x.x.x
```

This will set the iptables to log the bandwidth used. Then it can be seen by using:

```
#!/bin/bash
iptables -L FORWARD -v -x
iptables -L FORWARD -v
```

The first line shows the real numbers in bytes, expanded. The second one shows the numbers in Kbyte or Mbyte... It will show something like:
pkts-bytes-target-prot-opt-in-out---source---destination
117K-18M----------all- -- -any-eth0-x.x.x.x--anywhere
114K-17M----------all- -- -eth0-any-anywhere-x.x.x.x

As you can see the second line shows outgoing bandwidth while the third line shows incoming bandwidth.

If you want to reset the counters, just use:
iptables -Z

Hope this helped... And thanks for everything:)

Regards,

Eugenio Pacheco