Subject: Re: How to disable raw sockets
Posted by eugeniopacheco on Sun, 11 Jun 2006 21:59:38 GMT
View Forum Message <> Reply to Message

Hi,

I believe I am using venet, not veth. Below I have used ifconfig to show the interfaces.

```
[root@server ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr x:x:x:x:x:x
          inet addr:x.x.x.x  Bcast:x.x.x.x Mask:255.255.255.252
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23591161 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23587373 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1651199768 (1.5 GiB)  TX bytes:1656101486 (1.5 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:32613 (31.8 KiB)  TX bytes:32613 (31.8 KiB)

venet0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
          RX packets:33669 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33412 errors:0 dropped:6 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3803369 (3.6 MiB)  TX bytes:3193558 (3.0 MiB)
```

The way it is, people are still able to ddos from the vps. Also, even though I have capped their connection by using the following script:

```
#!/bin/bash

DEV=eth0
tc qdisc del dev $DEV root
tc qdisc add dev $DEV root handle 1: cbq avpkt 1000 bandwidth 10mbit
tc class add dev $DEV parent 1: classid 1:1 cbq rate 512kbit 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 10mbit
```

tc class add dev $DEV2 parent 1: classid 1:1 cbq rate 512kbit 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

They are still able to use more than 512kbps (I don't know why). I know this script works, because if I use wget from inside a vps, I will download things at 512kbps = 64kbytes/sec. Also, if I try to download stuff from this vps to another machine, I will only get 512kbps. So I'm sure the script works fine, but not for ddos. And I have no clue why that's happening.

Also the folowing is my settings for the vps:

ONBOOT="yes"

NUMPROC="400:400"
AVNUMPROC="372:372"
NUMTCPSOCK="1860:1860"
NUMOTHERSOCK="1860:1860"
VMGUARPAGES="10365:2147483647"

# Secondary parameters
KMEMSIZE="24434836:26878319"
TCPSNDBUF="2497985:8144945"
TCPRCVBUF="2497985:8144945"
OTHERSOCKBUF="1248992:6895952"
DGRAMRCVBUF="1248992:1248992"
OOMGUARPAGES="10365:2147483647"
PRIVVMPAGES="331095:354204"

# Auxiliary parameters
LOCKEDPAGES="357:357"
SHMPAGES="3109:3109"
PHYSPAGES="0:2147483647"
NUMFILE="11904:11904"
NUMFLOCK="1000:1100"
NUMPTY="186:186"
NUMSIGINFO="512:512"
DCACHESIZE="5325595:5485363"
NUMIPTENT="200:200"
DISKSPACE="1320140:1452155"
DISKINODES="1600924:1761017"
CPUUNITS="19658"

Any idea how much I should use on NUMTCPSOCK, NUMOTHERSOCK, TCPSNDBUF, TCPRCVBUF, OTHERSOCKBUF and DGRAMRCVBUF so that the vps is not allowed to ddos?

Thanks for your help.

Regards,