Subject: *SOLVED* How to disable raw sockets
Posted by eugeniopacheco on Sat, 10 Jun 2006 10:59:04 GMT
View Forum Message <> Reply to Message

Hi,

Does anyone know how to block raw sockets inside a VPS? I'm asking this because I would like to avoid a ddos attack to come from a VPS of mine. Is it possible? Or is there any other way to do it besides disabling raw sockets?

Regards,

Eugenio Pacheco

Subject: Re: How to disable raw sockets
Posted by Vasily Tarasov on Sun, 11 Jun 2006 10:22:37 GMT
View Forum Message <> Reply to Message

You can set paramters numothersock, numtcpsock, othersockbuf, tcpsndbuf, tcprcvbuf of the VPS to values, that are only enough to work "legaly" with VPS.

HTH.

Subject: Re: How to disable raw sockets
Posted by dev on Sun, 11 Jun 2006 11:25:35 GMT
View Forum Message <> Reply to Message

if you are using venet network device for VPS networking (not veth), then DDoS attacks from inside VPS are impossible.
This is why we recommend to use venet device and do care about security.

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,

Eugenio Pacheco

Subject: Re: How to disable raw sockets
Posted by Vasily Tarasov on Thu, 15 Jun 2006 13:28:29 GMT
View Forum Message <> Reply to Message

Finally I've got the reason...

Hunk 1:

Quote: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

Hunk 2:
Quote: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

Note, that both hunks work at egress of VE0!

Here is why wget is limited by traffic and ddos-atack tools aren't:

wget downloads from some node to VPS, for VE0 it's egress, so hunk 1 or hunk 2 work.

But ddos-atack tools emit(!) traffic. Thus for VE0 it's ingress traffic. Consequently hunk2 doesn't catch it!

If you want to solve your problem you can use this hunk 3 in addition to hunk2, hunk1:

Quote:DEV=venet0
tc filter add dev $DEV parent 1: protocol ip prio 20 u32 match u32 1 0x0000 police rate 2kbit buffer 10k drop flowid :1

Subject: Re: How to disable raw sockets
Posted by eugeniopacheco on Thu, 15 Jun 2006 13:49:13 GMT
View Forum Message <> Reply to Message

Hi,

Thanks for your help, but it still didn't work. In 30 seconds 2500MB limiting the connection of the ip on the vps to 512kbps and adding your line. I also tried adding it to the eth0 interface and it didn't work. I tried with both interfaces and it still didn't work. Also, I noticed you mentioned that the upload is not being limited, but it is. If someone try to download something FROM the VPS, he will be limited, if he tries to upload something TO the VPS, he will be limited, only the ddos is not being limited... And that I have no clue as to why.

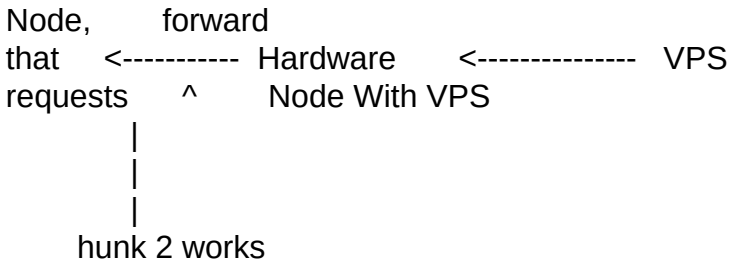
Regards,

Eugenio Pacheco

Subject: Re: How to disable raw sockets
Posted by Vasily Tarasov on Thu, 15 Jun 2006 14:19:11 GMT
View Forum Message <> Reply to Message

Quote:Also, I noticed you mentioned that the upload is not being limited, but it is. If someone try to download something FROM the VPS, he will be limited, if he tries to upload something TO the VPS, he will be limited,

If somebody tries to download smth from VPS (it is uploading for VPS), IP packet goes something like that:



So you are right.
In my previous post I meant that if upload goes to HN with VPS, then there is no forwarding - so no limiting and hunk 3 helps in such situation.

Anyway this isn't your case... And it's really strange why ddos tools aren't limited!..

Subject: Re: How to disable raw sockets
Posted by eugeniopacheco on Thu, 15 Jun 2006 15:18:25 GMT
View Forum Message <> Reply to Message

Hi,

I completely agree that it is strange ddos is not limited. Everything else is limited, only ddos is not. it is weird.

Thanks for your help though.

Regards,

Eugenio Pacheco

Subject: Re: How to disable raw sockets
Posted by Vasily Tarasov on Fri, 16 Jun 2006 12:04:58 GMT

View Forum Message <> Reply to Message

The reason is that ddos-atack utils generate a lot of packets of small size. So there are a LOT of PACKETS, but there only FEW MEGABYTES. So tc rules don't catch them: there is no traffic (Mb/sec) exceeding.

Subject: Re: How to disable raw sockets
Posted by Vasily Tarasov on Fri, 16 Jun 2006 13:04:23 GMT
View Forum Message <> Reply to Message

If you want to limit packages per second rate from VE you can use the following command on HN:

iptables -I FORWARD 1 -o eth0 -s x.x.x.x -m limit --limit 200/sec -j ACCEPT
iptables -I FORWARD 2 -o eth0 -s x.x.x.x -j DROP

x.x.x.x is the IP address of VE, you want to limit.

Good luck!