Subject: Traffic Limiting
Posted by atomic on Sun, 19 Feb 2006 12:54:24 GMT
View Forum Message <> Reply to Message

Hi,

i like to introduce a small and dirty script to limit the traffic amount for a vps. Besides iptables, the ipt_quota module is needed, its not included in the official ovz kernel, so you have to build you own from vanilla sources and patch it with the ovz enhancements.

Linux 2.6.8: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.8.tar. bz2
OVZ Patches: http://download.openvz.org/kernel/022stab064.1/patches/patch -022stab064-combined.gz

(Actual version on http://openvz.org/download/kernel/)

Download, extract and patch the Kernel source (2.6.8) with the combined ovz patch, then copy a ovz configfile for the desired system to /usr/src/linux/.config. Now, you'll need the ipt_quota module which is shipped with the netfilter patch-o-matic.

Note: ipt_quota is available for uniprocessor systems without SMP support only at the moment.

Grab patch-o-matic here: ftp://ftp.netfilter.org/pub/patch-o-matic-ng/
Grab netfilter sources here: ftp://ftp.netfilter.org/pub/iptables/

Extract patch-o-matic and the iptables sources. Now execute "runme" + Module in the patch-o-matic source directory. You will be asked for the kernel and iptables source directory.

./runme quota
Hey! KERNEL_DIR is not set.
Where is your kernel source directory? [/usr/src/linux]
Hey! IPTABLES_DIR is not set.
Where is your iptables source code directory? [/usr/src/iptables]

After patching the ipt_quota module, customize and compile your kernel with the module "ipt_quota".

Via .config file directly:

CONFIG_IP_NF_MATCH_QUOTA=m

Via menuconfig:

Device Drivers --->
  Networking support --->
    Networking options --->
      Network packet filtering (replaces ipchains) --->
        IP: Netfilter Configuration --->
          <M> quota match support

Note: I had some serious problems compiling the 2.6.8 Kernel with a actual version of gcc/cpp but it worked fine with gcc-Version 3.3.2 20031022. Thats the gcc version shipped with fc1, the ovz rpm kernels are build against that gcc version too.

You get this specific version of gcc and cpp here:
  http://mirrors.kernel.org/fedora/core/1/i386/os/Fedora/RPMS/ gcc-3.3.2-1.i386.rpm
  http://mirrors.kernel.org/fedora/core/1/i386/os/Fedora/RPMS/ cpp-3.3.2-1.i386.rpm

Compile, install and boot the patched kernel.

When the new kernel is loaded you should be able to modprobe ipt_quota to load the module (if it has not been loaded automaticly).
Check with lsmod:

ip_tables   20624 11   ipt_quota,ipt_length,ipt_ttl,ipt_tcpmss,ipt_TCPMSS,iptable_mangle [...]

Now you are able to set network traffic quotas for each ip adress on your system (a vps may have more than one ip adress).

I use this crapy piece of iptables configuration to limit the traffic:

```
iptables -N vn1-virtual01
iptables -A vn1-virtual01 -m quota --quota 107374182400 -j ACCEPT
iptables -A vn1-virtual01 -d vps.ipa.ddr.ess -j REJECT --reject-with host-prohib
iptables -A vn1-virtual01 -s vps.ipa.ddr.ess -j REJECT --reject-with host-prohib

iptables -A INPUT -d vps.ipa.ddr.ess -j vn1-virtual01
iptables -A OUTPUT -s vps.ipa.ddr.ess -j vn1-virtual01
iptables -A FORWARD -s vps.ipa.ddr.ess -j vn1-virtual01
```

Asuming that the VPS "vn1-virtual01" has the IP "vps.ipa.ddr.ess", this script monitors the traffic that is recieved, sent and forwarded by the VPS. The quota is set to 107374182400Bytes which is equivalent to 100GBytes. If the traffic limit is reached, all connections to/from the VPS will be terminated and rejected with the ICMP message "Host prohibited".

I'm looking forward to your comments and suggestions for improvement.