Home » Blog » Programming » Linux » TCP Connection Limiting on Sarge

TCP Connection Limiting on Sarge

By Roger Keays, 1 March 2007

One of the reasons Debian is such a great operating system is because of the huge amount of software tested, ready and available with apt-get. Every now and then though, you have to get your hands dirty and build something yourself and installing connlimit was one of these cases. Here's how I got connlimit working on Sarge.

connlimit, or more correctly ipt_connlimit, is a netfilter module which allows you to add rules to your firewall based on the number of connections a client has made to your server. It's very handy when you get some defective client program making hundreds of requests and unintentionally sapping your server's resources.

On sarge, there is no package for connlimit although the iptables binary is built with support for the module. When you try to use it you'll get this error message:

```
iptables: No chain/target/match by that name
```

The secret to connlimit-on-sarge is to fetch an old version of netfilter's patch-o-matic which includes a version of connlimit that works on the 2.6.8 kernel. It's tagged as patch-o-matic/pre_2611 in the netfilter subversion repository [1]. Conceptually you have to do the following steps:

1. download the kernel source
2. download the netfilter (iptables) source
3. download netfilter's patch-o-matic which contains the connlimit module
4. install the connlimit patch
5. configure the kernel
6. rebuild the kernel and reboot
7. configure your new firewall

Here are the commands I used on this system for these steps:

```
## 1. download the kernel source
$ apt-get install kernel-source-2.6.8
$ cd /usr/src
$ tar -xjf kernel-source-2.6.8.tar.bz2
```

```
## 2. download the netfilter (iptables) source
$ wget http://ftp.netfilter.org/pub/iptables/iptables-1.3.7.tar.bz2
$ tar -xjf iptables-1.3.7.tar.bz2

## 3. download netfilter's patch-o-matic
$ svn co https://svn.netfilter.org/netfilter/tags/patch-o-matic-ng/pre_2611/ pa

## 4. install connlimit patch
$ cd patch-o-matic-ng-pre_2611
$ export KERNEL_DIR=/usr/src/kernel-source-2.6.8
$ export IPTABLES_DIR=/usr/src/iptables-1.3.7
$ ./runme connlimit

## 5. configure the kernel
$ cd /usr/src/kernel-source-2.6.8
$ cp /boot/config-2.6.8-2-686 .config
$ make menuconfig
```

The new connlimit module can be selected from Device Drivers > Networking Support > Networking Options > Network Packet Filtering > IP: Netfilter Configuration > IP Connection Limiting.

Fortunately iptables doesn't have to be rebuilt since the binary distributed in sarge already has support for connlimit.

The kernel is recompiled, installed into grub and the system rebooted:

```
## 6. rebuild kernel and reboot
$ make
$ make modules_install
$ make install
$ mkinitrd -o /boot/initrd.img-2.6.8 2.6.8
$ vim /boot/grub/menu.lst
$ init 6
```

Now the fun part (building your firewall) is up to you. Here's a simple use of connlimit to limit the number of HTTP connections to 25 per client IP address:

```
$ iptables -A INPUT -j REJECT --reject-with tcp-reset -m connlimit
               --connlimit-above 25 -p tcp --dport http
```

References

[1] https://svn.netfilter.org/netfilter/tags/patch-o-matic-ng/pre_2611/

About Roger Keays

Roger Keays is an artist, an engineer, and a student of life. He has no fixed addressand has leftfootprints on 40-something different countries around the world. Roger is addicted to surfing. His other interests are music, psychology, languages, the proper use of semicolons, and finding good food.