How to defend against slowloris Webserver Denial of Service Attack

Author : admin

Like you can read in my previous post, there is a terrible DoS attack dating back,
from the previous year. It's a real shit and it was really annoying for me to figure out
that my Apache running on top of FreeBSD is vulnerable as well.
Therefore I needed desperately a fix, I was not really keen at the idea of installing
mod_qos, because I really hate third party software to mess up my Apache official module list.
Therefore I needed another approach, after some walk through google I found the following
How to best defend against a "slowloris" attack against Apache web server There are a couple of pathways
to follow as you can read in the post above. However the one that fit me best was through:
Varnish state-of-the-art high-performance HTTP accelerator (proxy) , it's truely a wonderful piece of soft.
Installing it on FreeBSD was a piece of cake:
All I had to do was:

# cd /usr/ports/www/varnish# make install clean# echo 'varnishd_enable="YES"' >> /etc/rc.confAnd last but not least, I had to alter my **/usr/local/etc/apache2/httpd.conf**
and change everywhere the Listen port to 8080 instead of the default 80, the same
procedure goes for VirtualHosts ports as well.

Last thing to do was:
Restart Apache# /usr/local/etc/rc.d/apache2 restartStart varnishd# /usr/local/etc/rc.d/varnishd startThat's it now varnishd handles the incoming connections to my Port 80, and passes whatever thinks appropriateto the apache server. Hip, Hip Hooray no more slowloris worries!
Another possible approach to Apache Denial of Service issues is to limit the maximum
allowed connections per host to be no more than 20.

On GNU/Linux this could be done with the following iptables rule:
# iptables -I INPUT -p tcp --dport 80 -m connlimit --connlimit-above 20 --connlimit-mask 40 -j DROP
On FreeBSD or OpenBSD with packet filter, you might bother to take a look at the following:
Howto: Basic Denial of Service Protection Using PF

But wait there is even more options to handle the slowloris DoS attack. It looks some enthusiast
has created even Apache module that handles the loris attack, sources of the non-official
mod_antiloris module release as well asprecompiled binaries in rpm can be obtained here.