

## RE: being DOSed

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2004-04/2353.html>

---

**From:** Thompson, Jimi (*JimiT\_at\_mail.cox.smu.edu*)

**Date:** 04/22/04

Date: Thu, 22 Apr 2004 14:03:35 -0500

To: "meimi" <meimi\_1@hotmail.com>

<SNIP>

I have found some IPs are opening 10 HTTP connection. Their IPs are Changing and all IPs are from different ISP network.

What should I do next?

Thanks

Meimi

</SNIP>

I'd suggest putting a firewall on another server, if you are being DDOS'd. Most people don't realize this, but your average old crunch Pentium I or MMX CPU has a lot more horse power than the average high end router that has nearly the same name as my vegetable shortening. Take anything you have and make it into something running a firewall or proxy which can filter the traffic to your web server. IMHO if you web server is already straining under a load from all the inbound traffic, you might not want to add a firewall to that box since it might not handle the additional load of inspecting all the packets/network connections.

I would suggest making some changed to your httpd.conf as well. Since you're posting to the FreeBSD list, I'm assuming that you're using Apache.

While what I'm suggesting won't help with making the actual DDOS'ing stop but it can help to keep your server from crashing due to the load. Most DDOS's against a web site occur by having a utility that opens a connection to your web server and then leave it hanging – waiting for an additional response from the client connection. That being the case, there are quite a few things you can do to change how your web server responds and processes those requests.

In this situation, your best friends are the Timeout & KeepAliveTimeout directives – turn those puppies down. You'll cause some legit users to get timed out but it will also cause the DDOS requests to time out faster as well. That said, you'll also probably want to edit some of the other directives in your httpd.conf as well. I didn't see a mention

freebsd-questions: RE: being DOSed

of which version of apache you are running, so I'm going to mention things I've found useful in the past.

You can set the MaxClients directive down so that your server will stop accepting so many incoming sessions. When you go to set it back up (after all this is over), be careful not to set it to something over 256 unless you have compiled special options in to your apache installation. If you don't know what I'm talking about, you haven't done it.

You can also set the MaxKeepAliveRequests to something low. Setting the MaxRequestsPerChild to something low will cause the spawned child processes to be killed off and restarted fairly frequently. If you are seeing anything involving escalating memory usage, this can be quite helpful. You should also probably MaxSpareServers so that any unused processes are dying on their own. I've found that limiting the MinSpareServers to be useful in stopping more children from spawning when the server is under an undesirable high load.

Depending on your version, you may also be able to set ThreadsPerChild, RLimitNPROC directive, RLimitMEM directive, RLimitCPU directive to limit system resource utilization.

If you're already being DOS'd, you may also want to consider setting the port directive to something other than 80 as least for now.

HTH,

Jimi

---

freebsd-questions@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@freebsd.org"