

## Re: iptables & tcp wrappers

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-10/0008.html>

---

**From:** Matthew Baker ([m\\_at\\_netgates.co.uk](mailto:m_at_netgates.co.uk))

**Date:** 10/05/04

Date: Tue, 05 Oct 2004 18:26:55 +0100

To: [focus-linux@securityfocus.com](mailto:focus-linux@securityfocus.com)

Luis M wrote:

*>I know this has been answered in many ways already, but this is yet  
>another approach.*

*>*

*and another.....*

I have rewritten a perl module into a script which is actually used on our mail server (MailScanner [www.mailscanner.info](http://www.mailscanner.info)) credit to Julian Field for that. What it does is monitor the output from auth logs (using swatch) and takes the IP addresses of failed/invalid attempts and records the number of attempts made from that IP in a database file. Then when the counter goes above a configured threshold (which can be different for a single host or CIDR network) the IP is inserted as a DROP rule into custom chain using IPtables.

No need for reloading all the chains. The script is only called when the fail pattern is matched in swatch and the IPtables insert is only done once when the threshold is reached.

I have documented it more on a little web page here:

<http://www.gwork.org/authwatch>

Although I still get failed logins I will only get a max of 6 attempts as opposed to 1000's. The script can also be taylorred to work with other log output combining failures from ftp, smtp auth, etc...

I've not released any of my scripts before so any feedback would be welcome,

Hope it helps.

Matt