

## Re: rate limiting sshd connections ?

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-05/0028.html>

---

**From:** Mark Johnston (*mjohnston\_at\_skyweb.ca*)

**Date:** 05/10/04

To: [freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org)

Date: Mon, 10 May 2004 11:17:32 -0500

Mike Tancsa <mike@sentex.net> wrote:

> *Does anyone know of a way to rate limit ssh connections from an IP address?*

I haven't used it myself, but ipfw (not sure whether it's ipfw2-only) has a limit directive:

```
limit {src-addr | src-port | dst-addr | dst-port} N
    The firewall will only allow N connections with the same set of
    parameters as specified in the rule. One or more of source and
    destination addresses and ports can be specified.
```

If you're getting lots of connects in parallel, that should improve things. Here's another thought, using dummynet:

```
ipfw pipe 1 config bw 1Kbit mask src-ip 0xffffffff
ipfw add 10 pipe 1 tcp from any to me 22 setup
```

1 kbit is 128 bytes/sec, which is roughly 2-3 average SYN packets per second. More than enough for a regular host, but fairly limiting against a flood. You can also implement this at the border:

```
ipfw pipe 1 config bw 1Kbit mask src-ip 0xffffffff dst-ip 0xffffffff
ipfw add 10 pipe 1 tcp from any to (LAN) 22 setup
```

(Dropping the dst-ip mask here would limit SYNs from any given IP to your whole LAN.)

These aren't tested, but they may give you some ideas.

Mark

---

[freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org) mailing list

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

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