

# Update: Alternate port randomization approaches

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-12/0324.html>

---

**From:** Mike Silbersack (*silby\_at\_silby.com*)

**Date:** 12/29/04

Date: Wed, 29 Dec 2004 03:02:20 -0600 (CST)

To: net@freebsd.org

On Sat, 18 Dec 2004, Mike Silbersack wrote:

> *There have been a few reports by users of front end web proxies and other  
> systems under FreeBSD that port randomization causes them problems under  
> load. This seems to be due to a combination of port randomization and rapid  
> connections to the same host causing ports to be recycled before the ISN has  
> advanced past the end of the previous connection, thereby causing the  
> TIME\_WAIT socket on the receiving end to ignore the new SYN.*

Based on testing done by Igor Sysoev, I've found that my original patch is insufficient; even as little as one randomizaion per second can cause problems for some users. As a result, I've created the attached patch (versions for both 6.x and 4.x are included). It implements a relatively simple algorithm: Port randomization is turned disable once the connection rate goes above 20 connections per second, and it is not reenabled until the connection rate falls below 20 cps for 5 seconds straight.

This appears to work for Igor, and it seems safe enough to commit before 4.11-RC2. But, if possible, I'd like a few more sets of eyes to doublecheck the concept and code; please take a look at it if you have a chance.

Thanks,

Mike "Silby" Silbersack

---

freebsd-net@freebsd.org mailing list

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

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

## freebsd-net: Update: Alternate port randomization approaches

---

- TEXT/PLAIN attachment: [portrandom-gen4-4x.patch](#)
- 

- TEXT/PLAIN attachment: [portrandom-gen4.patch](#)