

## Re: packets with syn/fin vs pf\_norm.c

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-07/0011.html>

---

**From:** Darren Reed ([avalon\\_at\\_caligula.anu.edu.au](mailto:avalon_at_caligula.anu.edu.au))

**Date:** 07/05/05

To: [wollman@csail.mit.edu](mailto:wollman@csail.mit.edu) (Garrett Wollman)  
Date: Wed, 6 Jul 2005 00:28:45 +1000 (Australia/ACT)

In some mail from Garrett Wollman, sie said:

>  
> <<On Mon, 04 Jul 2005 02:53:33 +0200, [des@des.no](mailto:des@des.no) (Dag-Erling Smørgrav) said:  
>  
> > *It is not invalid for a TCP segment to have both SYN and FIN set. See  
> > for instance RFC 1644.*  
>  
> *RFC 793 is perhaps the better reference, followed by RFC 1025.*

No, you're wrong on this.

Packets for TCP with SYN + FIN set are valid under T/TCP.  
T/TCP is documented under RFC 1644. To claim that these, earlier, documents render it ... "dead" is to argue that SACK and all other TCP enhancements since also fall into that bucket.

Very few people use T/TCP, although I believe FreeBSD is the only one of the BSDs that has done anything serious with it. pf is wrong to unconditionally clear the FIN flag. So there are a number of options here:

- fix pf to not remove the FIN flag in FreeBSD
- don't use T/TCP
- don't use scrub in pf
- don't use pf

I think this is a bug in the scrub implementation and should be fixed.

Darren

---

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