

## RE: FreeBSD bridge + filtering, BIG problem

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-12/0002.html>

---

**From:** Clément MOULIN ([cmoulin\\_at\\_simplerezo.com](mailto:cmoulin_at_simplerezo.com))

**Date:** 12/01/04

To: <[yongari@kt-is.co.kr](mailto:yongari@kt-is.co.kr)>

Date: Wed, 1 Dec 2004 14:20:40 +0100

Pyun YongHyeon wrote:

>Both pf and ipf can't create *\*states\** in bridge mode. That restriction comes from bridge(4). Since pf/ipf couldn't create states it will drop the packet when it thinks the packet is in out of TCP window.

>

>If you want to use pf/ipf in bridge mode, don't use stateful inspection.

>One more note: filtering works only for inbound traffics in bridge mode.

If you're right, it SHOULD really be specified in bridge(4), but I'm not very sure about this, since I see states with pfctl and no packets are dropped in my case (except maybe in scp from internet to sr01) !

Finally, I have found the main problem. Both for ipf/pf, I have to set sysctl "net.link.ether.bridge.ipf" to 1... That doesn't exist on FreeBSD 4X. After that, incoming traffic is filtered (accounting works, blocking rules too).

We REALLY need to specify this in FreeBSD handbook (sections 14.9 – firewalls and 24.5.4 – bridging) and Migration Guide of 5X, since it could be a big security hole.

My last problem is that scp from sr01 to internet that stalled after 144KB exactly (internet to sr01 works) ! This is a pf issue, since it occurs only when pf is enabled.

--

Clement Moulin

SimpleRezo - Simplifiez-vous le reseau !

Web: <http://www.simplerezo.com/>

---

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"