

Re: per-interface packet filters, design approach

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-12/0185.html>

From: Bruce M Simpson (*bms_at_spc.org*)

Date: 12/14/04

Date: Tue, 14 Dec 2004 06:13:07 -0800
To: Andre Oppermann <andre@freebsd.org>

On Tue, Dec 14, 2004 at 03:03:27PM +0100, Andre Oppermann wrote:

> *Let's take a high level view of the issue at hand and the consider*

> *some alternative approaches to the situation.*

[snip]

I'm wrapping up in Berkeley for the holidays, but I wanted to drop my 2c into this discussion.

What I'm really missing in IPFW is the ability to maintain one or more 'shadow rulesets'. These rulesets may not be the active rulesets, but I can manipulate them as tables, independently of the active ruleset(s), push rules into them, flush them, and then atomically switch them to be the active ruleset, using a single syscall.

IPF and PF have such functionality, IPFW does not. The lack of a documented ABI/API for access to IPFW by applications other than ipfw(8) is something which I'm leaving out of the picture for the moment.

I don't really consider using 'skipto' and separate sections of rule index number space a valid answer here, because we should have the ability to independently flush each ruleset.

When extended to stateful rules (I am talking here purely about the simple stateless packet filter case), this comes in even more useful.

Regards,
BMS

-
- application/pgp-signature attachment: [stored](#)