

## Re: Jail support for mac\_portacl(4).

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-05/0095.html>

---

**From:** Samy Al Bahra ([samy\\_at\\_kerneled.org](mailto:samy_at_kerneled.org))

**Date:** 05/29/05

To: Robert Watson <[rwatson@FreeBSD.org](mailto:rwatson@FreeBSD.org)>

Date: Sun, 29 May 2005 17:21:03 +0300

On Sun, 2005-05-29 at 15:02 +0100, Robert Watson wrote:

> On Tue, 24 May 2005, Pawel Jakub Dawidek wrote:

>

>> *This patch gives another option, so one don't need to use firewall for*

>> *this purpose. It adds new idtype - 'jid'. With this patch, one can*

>> *configure that jail with the given JID can use only defined ports:*

>>

>> *# sysctl security.mac.portacl.rules="jid:1:tcp:80"*

>>

>> *Patch is here:*

>>

>> [http://people.freebsd.org/~pjd/patches/mac\\_portacl.c.patch](http://people.freebsd.org/~pjd/patches/mac_portacl.c.patch)

>>

>> *Any objections?*

>

> *This sounds fine to me, especially since it doesn't break forwards*

> *compatibility from older mac\_portacl rule sets.*

>

> *However, I've CC'd Samy Al Bahra, who has a set of outstanding mac\_portacl*

> *patches that are similar, and might have some comments on your proposed*

> *changes. My primary concern with his changes was that they changed the*

> *syntax in a way that broke backwards compatibility to older defined rules;*

That was fixed.

I think pjd@'s syntax changes are not that flexible (and well, as useful). Please take a look at

<http://samy.kerneled.org/patches/portacl.patch>

Support for an "add" and "none" keyword was added as well (except for the uid/gid field). This is copy I sent to Robert a couple of months ago. If pjd@ wishes, he can modify this patch to his style and apply the "all" keyword to the uid/gid identifier in order to bind all processes in a jail to a rule (if he wishes).

Thanks.

--

Re: Jail support for mac\_portacl(4).

FreeBSD-Security: Re: Jail support for mac\_portacl(4).

Samy Al Bahra

|----- <http://samy.kerneled.org>

|----- <http://www.FreeBSD.org>

|----- <http://www.arabeyes.org>

---

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"