

comp.security.ssh: Re: Restrict tunnels?

## Re: Restrict tunnels?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-12/0192.html>

---

**From:** Darren Tucker ([dtucker\\_at\\_dodgy.net.au](mailto:dtucker_at_dodgy.net.au))

**Date:** 12/21/04

Date: 21 Dec 2004 12:20:02 GMT

In article <41c6e81d\$3@e-post.inode.at>, Hannes Erven <h.e@gmx.at> wrote:

>Darren Tucker wrote:

>> *Otherwise, no, the functionality doesn't exist in the vanilla*

>> *distribution.*

>

>*I wonder why this isn't something more asked for -- am I missing some*

>*more or less obvious workaround or reason why one wouldn't want to*

>*restrict tunneling?*

If you allow interactive logins people can do their own forwarding whether or not sshd lets the (eg with tools like netcat), and some platforms have kernel-based restrictions on outgoing connections (eg Linux/iptables "owner match" rules or "user" rules in OpenBSD's pf).

--

Darren Tucker ([dtucker@zip.com.au](mailto:dtucker@zip.com.au))

GPG key 8FF4FA69 / D9A3 86E9 7EEE AF4B B2D4 37C9 C982 80C7 8FF4 FA69

Good judgement comes with experience. Unfortunately, the experience usually comes from bad judgement.