

## RE: SSH Security

**Source:** <http://linux.derkeiler.com/Mailing-Lists/RedHat/2004-10/0011.html>

---

**From:** Michael Anaya ([mianaya\\_at\\_edatatrace.com](mailto:mianaya_at_edatatrace.com))

**Date:** 10/01/04

To: "'General Red Hat Linux discussion list'" <[redhat-list@redhat.com](mailto:redhat-list@redhat.com)>

Date: Fri, 1 Oct 2004 10:31:07 -0700

From: [redhat-list-bounces@redhat.com](mailto:redhat-list-bounces@redhat.com) [<mailto:redhat-list-bounces@redhat.com>]

On Behalf Of Alexey Fadyushin

Sent: Thursday, September 30, 2004 10:02 AM

To: [ddelao@oucpm.org](mailto:ddelao@oucpm.org); General Red Hat Linux discussion list

Subject: Re: SSH Security

You should use option AllowUsers in file /etc/ssh/sshd\_config. This option lists the names of users which are allowed to connect via ssh and host from which they are allowed to connect. For example:

AllowUsers: \*@192.168.11.1

should allow any user to connect from host 192.168.11.1. Connections from other addresses will not succeed.

Also you can use files /etc/hosts.allow and/or /etc/hosts.deny which define restrictions for connections to daemons which use libwrap (SSH does use it).

It is also possible to filter incoming connections to port ssh with iptables, so the packets from any hosts not allowed to connect to SSH will be dropped.

Alexey Fadyushin.

Brainbench MVP for Linux

<http://www.brainbench.com>

Darryl W. DeLao Jr. wrote:

> *How can I tell the SSH server to only allow certain IP's the ability to*  
> *login?*

AllowUsers is a list of local user accounts allowed to ssh in.

AllowUsers: username1 username2 username3

The option you are looking for:

ListenAddress ###.###.###.###:port

Both supported using protocol 2

RedHat: RE: SSH Security

HTH

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@redhat.com?subject=unsubscribe>

<https://www.redhat.com/mailman/listinfo/redhat-list>