

RE: ssh from public internet and firewalls

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2005-01/0329.html>

From: Michael Velez (mikev777_at_hotmail.com)

Date: 01/19/05

To: "'General Red Hat Linux discussion list'" <redhat-list@redhat.com>

Date: Wed, 19 Jan 2005 05:55:57 -0500

Hello Donald,

Thanks for the reply. It has helped me to understand what I need to do.

I believe I have figured out how to be able to log in without a password or passphrase while using a machine on my lan and how to force using private key and passphrase when connecting from outside the lan. Is the below solution valid/security feasible?

I could have two ssh daemons listening on two different ports:

- a local sshd listening on port 22 using sshd_config, requiring public/private key authentication with no passphrase. Using your MAC info, the RHEL Firewall could then restrict port 22 messages to those machines connecting from my LAN.

- a remote sshd listening on port XXXX using a file I would call remotesshd_config, requiring authentication with a key that has a passphrase associated with it. I would then have to create a new service called remotesshd listening on port XXXX, and create its associated init.d script. The RHEL Firewall would accept all remote sshd requests connecting to this port and would let sshd do the authentication.

This would allow me to connect to machines from within my LAN using batch scripts without having to enter a password; and it would give me good security when connecting from the public internet, using something I have (soft token private key) and something I know (passphrase).

Can I run two sshd daemons at the same time? Am I opening myself up to security vulnerabilities?

Michael

> -----Original Message-----

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

> bounces@redhat.com] On Behalf Of O'Neill, Donald (US - Deerfield)

> Sent: Tuesday, January 18, 2005 6:40 PM

RedHat: RE: ssh from public internet and firewalls

> *To: General Red Hat Linux discussion list*
> *Subject: RE: ssh from public internet and firewalls*
>
> *You are somewhat correct. The MAC option will only work for local*
> *computers located on the LAN, otherwise your remote connections will use*
> *the MAC address from the last router hop.*
>
> *If your going to be connecting from a particular subnet on the Internet,*
> *setup your /etc/hosts.allow /etc/host.deny or iptables to only accept*
> *connections from a particular subnet.*
>
> -----Original Message-----
> *From: redhat-list-bounces@redhat.com*
> *[mailto:redhat-list-bounces@redhat.com] On Behalf Of Michael Velez*
> *Sent: Tuesday, January 18, 2005 5:26 PM*
> *To: redhat-list@redhat.com*
> *Subject: ssh from public internet and firewalls*
>
> *Hello all,*
>
>
>
> *I have set up sshd on my RHEL 3 box to be able to ssh to it from the*
> *internet. All rules on the modem, router, and RHEL work fine. However,*
> *I*
> *would like to add a rule to my firewall that only certain MAC addresses*
> *can*
> *actually make a request to sshd, thereby limiting ssh's from the public*
> *internet to two trusted laptops.*
>
>
>
> *I have set up my firewall with the mac address option and have put in*
> *the*
> *mac addresses of those laptops. The problem is that this works fine*
> *when*
> *the laptops are connecting from within my LAN (i.e. firewall*
> *accepts/rejects*
> *specific MAC addresses – not a great help there but I guess I'm*
> *protected*
> *from any devious family member) but it does not work when my laptop is*
> *connecting from the public internet? Is there a reason? Will the MAC*
> *address reflect the one from the latest hop; that is, will my Linux box*
> *only*
> *see the router MAC address? There seems to be a MAC option in the*
> *sshd_config; is that the answer and how do I use that?*
>
>
>
> *Also, can I set up two different authentication mechanisms for whether*
> *I'm*

RE: ssh from public internet and firewalls

RedHat: RE: ssh from public internet and firewalls

> logging in from within my LAN or from the internet? There is a HOST
> keyword
> for the sshd_config file. Can I set up two pseudo-hosts to go verify
> two
> different identities with one of the hosts only accepting local IP
> addresses
> or something else that's local that I can define? The reason I ask is
> that
> I would rather just have to enter a password or no password (with RSA
> authentication – no passphrase) from within my lan but on the public
> internet, I would set up an authentication with password and RSA
> public/private key with passphrase and then only allow that from two
> laptops. Is this possible and/or is this overkill?
>
>
>
> Last but not least, I imagine I can change the port on which sshd
> listens.
> Do I only have to change the relevant line in /etc/services or is there
> something else I need to look at?
>
>
>
> If somebody can point me in the right direction, or suggest/advise the
> best
> way of doing this, I would appreciate it. I'll then go figure out the
> details.
>
>
>
> Thanks,
>
> Michael
>
>
>
>
>
> --
> redhat-list mailing list
> unsubscribe <mailto:redhat-list-request@redhat.com?subject=unsubscribe>
> <https://www.redhat.com/mailman/listinfo/redhat-list>
>
>
> This message (including any attachments) contains confidential information
> intended for a specific individual and purpose, and is protected by law.
> If you are not the intended recipient, you should delete this message.
> Any disclosure, copying, or distribution of this message, or the taking of
> any action based on it, is strictly prohibited.
>
> --

RedHat: RE: ssh from public internet and firewalls

- > *redhat-list mailing list*
- > *unsubscribe mailto:redhat-list-request@redhat.com?subject=unsubscribe*
- > *<https://www.redhat.com/mailman/listinfo/redhat-list>*

--

redhat-list mailing list
unsubscribe mailto:redhat-list-request@redhat.com?subject=unsubscribe
<https://www.redhat.com/mailman/listinfo/redhat-list>