

RE: [fw-wiz] Issues opeing firewall for SSH/SecureFTP?

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-08/0048.html>

From: David West (davedub_at_yahoo.com)

Date: 08/19/04

To: firewall-wizards@honor.icsalabs.com

Date: Thu, 19 Aug 2004 15:32:49 +1000 (EST)

I've recently been looking at a similar request.

Has anyone on the list looked at using a restricted shell such as rssh or sponly to restrict scp or sftp without a remote shell?

rssh – <http://www.pizzashack.org/rssh/>

sponly – <http://sublimation.org/sponly/>

David

- > *From: "Bill Royds" <broyds@rogers.com>*
- > *To: <firewall-wizards@honor.icsalabs.com>*
- > *Subject: RE: [fw-wiz] Issues opeing firewall for*
- > *SSH/SecureFTP?*
- > *Date: Thu, 12 Aug 2004 15:44:39 -0400*
- >
- > *Whether VPN or SSH is appropriate really depends on*
- > *the situation. A contractor*
- > *needing access to a particular server on your*
- > *internal network would be better*
- > *served by a VPN directly to that server with a stack*
- > *that blocks splitting the*
- > *routing when the VPN is up (no access to internal*
- > *network when VPN is working).*
- > *They can look at the server fully including using*
- > *something like Terminal Server*
- > *to run installs and diagnostics. This VPN would be*
- > *through your firewall, not*
- > *terminated at your firewall.*
- > *But if all they needed was a single purpose*
- > *access, such as file transfer then*
- > *SFTP over SSH generally is appropriate. But remember*
- > *that SSH is Secure SHELL.*
- > *It gives command line access to the remote machine,*

Firewall-Wizards: RE: [fw-wiz] Issues opening firewall for SSH/SecureFTP?

- > *which means a lot of control*
- > *over your server. Some clients and servers can*
- > *control it to only allow SFTP,*
- > *but one has to set things up carefully to avoid*
- > *giving access to the system.*
- >
- > -----Original Message-----
- > *From: firewall-wizards-admin@honor.icsalabs.com*
- > *[mailto:firewall-wizards-admin@honor.icsalabs.com]*
- > *On Behalf Of Chris Conacher*
- > *Sent: Monday, August 09, 2004 3:35 PM*
- > *To: firewall-wizards@honor.icsalabs.com*
- > *Subject: [fw-wiz] Issues opening firewall for*
- > *SSH/SecureFTP?*
- >
- > *Dear List*
- >
- > *I am currently trying to move an organization's*
- > *current solution of VPN for*
- > *external contractors performing file transfer, to*
- > *SecureFTP.*
- >
- > *My belief has always been that SecureFTP is the*
- > *appropriate solution for*
- > *secure file transfer and the aim should always be to*
- > *avoid giving remote*
- > *access to internal networks [especially*
- > *non-employee] where it is not*
- > *specifically required.*
- >
- > *My question is are there any other issues that I*
- > *should be aware of with*
- > *allowing SecureFTP/SSH through the firewall as one*
- > *of the standard pushes*
- > *(read knee jerk reactions) against this appears to*
- > *be that another port is*
- > *opened on the firewall?*
- >
- > *1. I have worked in a lot of different organizations*
- > *where VPN seems to be*
- > *the norm for everyone even where the only*
- > *requirement is file transfer*
- > *2. My belief is that this is because the*
- > *organization does not appreciate*
- > *the implications of allowing non-employees access to*
- > *the internal network*
- > *and does not understand that SecureFTP is an*
- > *appropriate solution*
- > *3. I understand that SSH is a great opportunity for*
- > *tunneling attacks if an*
- > *exploit is discovered, but I feel that there is it*

RE: [fw-wiz] Issues opening firewall for SSH/SecureFTP?

Firewall-Wizards: RE: [fw-wiz] Issues opening firewall for SSH/SecureFTP?

- > *possible to manage this*
- > *exposure through the existence of a DMZ based*
- > *bastion host, rather than*
- > *providing external people with access to the VPN.*
- >
- > *Comments appreciated.*
- >
- > *Chris*
- >
- >

-
- > *It's fast, it's easy and it's free. Get MSN*
 - > *Messenger today!*
 - > *<http://www.msn.co.uk/messenger>*
 - >

Find local movie times and trailers on Yahoo! Movies.
<http://au.movies.yahoo.com>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>