

Re: Agent Forwarding Question for the list

Source: http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2006-10/msg00019.html

- *From:* Jason Powers <jpowers@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 05 Oct 2006 13:39:57 -0400
-

Sorry, you are correct. So much of the information I find is about Port Forwarding, which I know is not the same as Agent Forwarding, which is what I am asking about. After years of Sun boxes and NCD terminals, I can already do the Port Forwarding stuff in my sleep.

- > By default (at least as shipped by some vendors), agent forwarding is
- > turned off. You need to explicitly enable it, either by modifying
- > /etc/ssh/ssh_config, ~/.ssh/config, or by specifying `-A` on the ssh
- > command line.
- >
- > If you want to make this the default (not recommended), look in
- > one of the aforementioned config files for the following:
- >
- > # Host *
- > # ForwardAgent no

This is the part I assumed I had configured correctly after reading the manual, though it does not specify if I do or do not also have to activate X11 forwarding to just get agent forwarding to work, so I did not include the x11 directives. By default usepam is yes on fedora.

My /etc/ssh/ssh_config on every box in question contains:

```
Host *
ForwardAgent yes
```

I want to go from desktop to server1 to server2 without typing a password. ssh-agent is on the desktop, I put my key in with ssh-add, ssh someuser@server1 lets me in. Now whether I use ssh username@server2 or ssh -A username@server2 it asks me for a password. It does not change if it is the same or a different username. It asks for the password so quickly, and does not show up in the other server's logs (unless I type the password), that I suspect it is in fact pam on server1 which is requesting the password instead of sshd on server2.

Thanks for your help

Jason Powers

Derek Martin wrote:

Re: Agent Forwarding Question for the list

On Wed, Oct 04, 2006 at 06:18:02PM -0400, Jason Powers wrote:

I have looked through the archives and googled this pretty thoroughly, I'm having a tough time finding someone else who has asked the same question previously. There's a lot of information about openssh, but surprisingly little detail about port forwarding.

Er, your e-mail doesn't appear to be about port forwarding at all... It seems to be about connecting with ssh-agent. Presumably this was just a think-o and you didn't really mean to ask about port forwarding?

Now let's say that I have a linux desktop and two linux servers, assuming I've configured things correctly, then from the desktop box I should be able to:

Trouble is, "assuming I've configured things correctly" is rather a big assumption. ;-)

```
me@desktop> ssh-add  
(type pass for key)  
me@desktop> ssh someuser@server1
```

```
now from that terminal  
someuser@server1> ssh otheruser@server2
```

It asks me for a password when I try to jump to the second server. I can put the password in and it works, but I think at this point it should be forwarding the key.

By default (at least as shipped by some vendors), agent forwarding is turned off. You need to explicitly enable it, either by modifying `/etc/ssh/ssh_config`, `~/.ssh/config`, or by specifying `-A` on the ssh command line.

If you want to make this the default (not recommended), look in one of the aforementioned config files for the following:

```
# Host *  
# ForwardAgent no
```

Re: Agent Forwarding Question for the list

Uncomment and change that to yes. But this is not recommended because it means that ALL ssh agents will be forwarded to ALL servers to which people are connecting to from that machine (where you made the config change). This is generally a bad idea, because IIUC it means that an unencrypted copy of your ssh keys will be available on machines outside your organization's control. While the risk is probably low if you only ever connect to "trusted" sites, in theory a malicious site/admin could hack sshd to record such keys or otherwise snoop them. This is why it's turned off by default.