

Re: Openssh Port Forwarding Confusion

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-12/0205.html>

From: Darren Tucker (dtucker_at_dodgy.net.au)

Date: 12/23/03

Date: Tue, 23 Dec 2003 13:58:22 +0000 (UTC)

In article <7e15f9e1.0312230057.4e07cfa4@posting.google.com>, Hank <william.quiter@sylvania.com> wrote:
>Now for my Port forwarding question. I have read every man page, and
>every Howto I can get my hands on – they just end up confusing me. I
>figured out that I am missing something very fundamental, but I don't
>know what it is. So far what I have extracted about ssh port
>forwarding is:
>I can forward ports

As far as SSH is concerned, at the simplest level there are 2 types of port forwarding:

- * Local forwarding: You connect to a port on the SSH client. The data is sent over the SSH data stream to the server, sshd makes a connection the target of the forward (which may or may not be on the SSH server itself).
- * Remote forwarding: You connect to a port on the SSH server. The data is sent over the SSH data stream to the client, which connects to the target of the forward (which, again, may or may not be on the client itself).

To use a forward, you configure whatever software you want to tunnel the traffic of to use "localhost" or "127.0.0.1" [1] as the address to connect to. Your software connects to the port that ssh or sshd is listening to, which then forwards the data over the SSH connection where at the other end the SSH software connects to the target of the forward on your behalf.

Now, adding to this, there are some special cases:

- * X11 Forwarding: A special case of Remote forwarding where the port is 6000 + N, the \$DISPLAY environment variable is set to something like localhost:N.0 [3] and xauth is used to restrict access to this pseudo-display managed by ssh. When an X client runs, it connects to the port specified by \$DISPLAY and the connection is sent back through the SSH channel and to the X Server (which, confusingly, is running on the SSH client in this case).

comp.security.ssh: Re: Openssh Port Forwarding Confusion

* Dynamic Forwarding. A special case of Local forwarding where instead of connecting to a fixed port on the SSH client to be forwarded via the SSH channel, the SOCKS protocol is used to determine which host and port the forwarded connection is destined for. In this case, the SSH *client* is behaving as a SOCKS *server*.

Hopefully this helps. I glossed over some details and it's still longer than I thought it would be (perhaps a candidate for an FAQ entry?)

-Daz.

[1] Most of the time, the ports that are forwarded are listening only on the loopback interface (ie 127.0.0.1) and thus only processes on the forwarding machine may use the forward. This can be overridden and a bound to all addresses (for OpenSSH, this is the GatewayPorts [2] directive, most SSH software has something similar).

[2] Whether or not you can specify GatewayPorts on a remote port forward varies with the software and server settings.

[3] Actually on OpenSSH this varies with the setting of X11UseLocalhost.

--

Darren Tucker (dtucker at 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.