

Re: interfaces lo:1 lo:2 lo:3? (for remote ssh tunnels)

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2004-06/3772.html>

From: Will Trillich (will_at_serensoft.com)

Date: 06/25/04

Date: Fri, 25 Jun 2004 09:47:38 -0500

To: debian-user@lists.debian.org

On Fri, Jun 25 at 09:56PM +0800, John Summerfield wrote:

> *Will Trillich wrote:*
> >turns out the vast majority of these connections will be coming
> >from beyond a remote firewall (remote from where the server is
> >located on the 'net):
>
> *Cool. That's the problem tunneling (port forwarding) solves. So does
> openvpn, but more generally: it can make two lans separated by the
> hostile Internet seem to be one.*

vpn is a very clever use of resources, and an amazing boost in convenience 1) once it's set up [much heavy lifting there requiring much expertise when things aren't Just Quite Right] and 2) even tho it provides lots more functionality [i.e. security issues] than most folks usually need, and is certainly the case here when we only need one tcp port to do the dirty work and 3) are typically better suited for long-term lan-to-lan connections than transient solitary-pc-to-lan connections.

> >*the server can't open a port on the client machine, cuz it
> >can't get past the client firewall. the client CAN ssh past
> >the server virewall (that's how the latter is set up) to the
> >server itself and establish a remote-to-local forwarding
> >rule. if the server can be made to chat with a localhost
> >interface using a port to match the forwarding setup, it will
> >work -- for one user per loopback interface.*
> >
> *I don't understand why the server would be making the
> connexion request. By definition, the client does that.*

aha -- suddenly i become the teacher.

it's not "by definition" -- it's "in the VAST majority of cases".
as in "very seldom, and it's surely suspicious behavior that
should be investigated by at least three government agencies at

Debian–User: Re: interfaces lo:1 lo:2 lo:3? (for remote ssh tunnels)

the highest level, there will be a case for forwarding server ports to the client, not that there's anything wrong with that."

MOST traffic, by far, is initiated by a client that connects to a server. but sometimes there's an instance (quickmate from janzabar in this case) where after the main connection is established, the user activates a function on the server, and the server initiates another connection to the client — in this instance to activate the quickmate menu. quickmate opens the local/client port, listening for instructions from the server; when the server says (at the user's request) "do this menu" it pops up and away we go.

in fact, until yesterday, i myself wondered when you would possibly ever need a remote–to–local connection. voila! here's one (perhaps the very single only one ever, in the entire history of the universe, since the dawn of time, ever).

cases like this one is why the bright folks who came up with port forwarding for ssh decided to not only have locate–to–remote tunnels, but remote–to–local tunnels as well.

that is, not "-L" but "-R". see the ssh manpage.

even brighter, the ssh virtuosi also managed to allow for specifying a HOST to beam the remote end to. in our case we don't need another hop, but the option is there and it's an awesome one to have available when it's needed. i never would have been able to implement that kind of genius, but i'm glad someone did.

smart folks, there. :)

```
> Here's what openvpn does:
> traceroute to 192.168.1.252 (192.168.1.252), 30 hops max, 38 byte packets
> 1 ns (192.168.9.4) 0.359 ms 0.226 ms 0.209 ms
> 2 gw (192.168.9.1) 0.413 ms 192.168.7.254 (192.168.7.254) 0.929 ms
> 0.552 ms
> 3 192.168.1.252 (192.168.1.252) 1058.580 ms 1103.616 ms 1066.529 ms
> summer@Dolphin:~$
>
> The internet is between 2 & 3. I can see all hosts on 1.x and
> other networks it can route to, and they can see me. Of
> course, I can add rules to the firewalls, and I could use
> NAT.
```

vpn is way cool, no doubt. if we had one in this case, you're right — this would all be moot. and maybe someday in the future, politics permitting, that will happen. i hope so.

for now, we ssh with tcp ports tunnelled all over creation. :)

Re: interfaces lo:1 lo:2 lo:3? (for remote ssh tunnels)

Debian–User: Re: interfaces lo:1 lo:2 lo:3? (for remote ssh tunnels)

- > *I'm running openvpn on gw at my end (my firewall, a Powermac running*
- > *Woody) and the host at the other end is inside the firewall, a*
- > *commercial ADSL router.*
- >
- > *Using ssh the way _I_ described. I can connect from my system at home to*
- > *hosts at work. In the specific example I gave, I could connect to the*
- > *webserver on 127.0.0.1.*
- >
- > *With this command:*
- > *ssh -L 8088:192.168.4.254:80 192.168.1.252*
- > *if I open my browser on <http://127.0.0.1:8088/> then ssh forwards the*
- > *connexion request to 1.252 and from there makes a connexion request to*
- > *port 80 on 192.168.4.254 which could be an ADSL router. The router would*
- > *see the request as coming from 1.252.*

aha! but, as you said:

- > *You don't want loopback devices. The loopback device is*
- > *for me to send messages to myself: the client and server*
- > *are on the same box.*

"i'm talking to myself"! 127.0.0.1 is the loopback interface, so you "don't want that"... :) unless you've got the port forwarded elsewhere. right? yes? hmm?

:)

similarly to your setup, i've got my firewall at home set to forward ssh requests to my debian server; then i have my roving ssh laptop configured to connect to the mother ship (server in my basement) port-forwarding :8888 back to the firewall for seeming-to-be-from-inside-the-lan administrative configuration.

```
ssh -L:8888:192.168.0.1:80 home.server.net.addr
```

then i <http://localhost:8888/> and administer my firewall "from inside" even tho i'm miles from home. tres kewl!

- > *>about those dummy interfaces... can they be made into loopback*
- > *>devices? and if so, how?*
- >
- > *You don't want loopback devices. The loopback device is for me to send*
- > *messages to myself: the client and server are on the same box.*

unless the server port is forwarded elsewhere, in which case the server THINKs it's talking to itself (just as the client normally does) but the traffic actually wormholes through to the client end of the connection.

just like "ssh -L port:host:port" but in reverse -- instead, it's "ssh -R port:host:port". instead of the client forwarding

Re: interfaces lo:1 lo:2 lo:3? (for remote ssh tunnels)

Debian-User: Re: interfaces lo:1 lo:2 lo:3? (for remote ssh tunnels)

its local ports to the server, we get the server to forward its local ports to the client. grok?

> *_I_ would use the IP address of an existing interface. Servers can generally accept many requests to the one port and IP address.*

just as the client can accept many incoming request to any particular port. but only one process can open the port for listening purposes. the port is open for listening on the client, and there's no way to have the server contact the client (right now) except via ssh port-forwarding technology. we tried local-to-remote forwarding, but only one could listen for connections on that port -- ssh or quickmate. once we figured it was remote-to-local, all was well: the server initiates the connection to the client (when the user requests it) and if we have the server look to 127.*.* with port forwarding, it winds up in the client's lap just as we want it to.

you're quite right in that a vpn would be much more convenient and a more universal solution. but politics is a problem, not to mention age of technology and knowledge levels of current staff. :)

for now, ssh -R:10001:localhost:10001 works a treat.

[this has been an interesting discussion -- i've learned a lot and hope you have too...]

--

I use Debian/GNU Linux version 3.0;
Linux boss 2.4.18-bf2.4 #1 Son Apr 14 09:53:28 CEST 2002 i586 unknown

DEBIAN NEWBIE TIP #7 from Will Trillich <will@serensoft.com>

:

Wondering what COMMANDS you have at your disposal? Try pressing the TAB key at the command line. For example, "apt<TAB>" will show you all the commands that start with "apt". (This is called "completion" if you want to look it up in your shell's manpage.) (Different implementations have the <TAB> completion set up differently -- you may need to press <TAB> twice.) Also see <http://newbieDoc.sourceforge.net/> ...

--

To UNSUBSCRIBE, email to debian-user-REQUEST@lists.debian.org with a subject of "unsubscribe". Trouble? Contact listmaster@lists.debian.org