SSH relay server with OpenSSH

Asked 13 years, 5 months ago Modified 2 years, 3 months ago Viewed 25k times

11

Is it possible to use OpenSSH to relay to other SSH-enabled devices such as routers switches etc? Is this something that can be done without creating a bespoke application on Linux to do it?

linux ssh

Share Improve this question

Follow

edited Dec 2, 2020 at 8:19

Overmind

3,018 ● 2 ● 16 ● 24

asked Oct 7, 2009 at 23:01

aHunter

314 ● 1 ● 6 ● 21

4 Answers

Sorted by:

Highest score (default)

11

Sure; just use SSH port forwarding/tunneling. Start an ssh connection to the "proxy" machine using the following command:

```
ssh -L$LOCALPORT:$REMOTEHOST:$SSHPORT $PROXYHOST
```

- `$PROXYHOST`: the machine you've got SSH access to
- `$REMOTEHOST`: the machine that $PROXYHOST can connect to, but you can't. Use a hostname or IP that `$PROXYHOST` can use to refer to the machine
- `$SSHPORT`: the port that sshd is listening for on remotehost; most likely 22
- `$LOCALPORT`: the local outbound port SSH is opening up on your local machine that forwards to port 22 on `$REMOTEHOST`

Leave that connection up to keep the tunnel working. You might want to also add `-N` to the command so that this connection won't bring up a remote shell and you won't accidentally close it later.

Once the tunnel is established, do the following:

```
ssh -p $LOCALPORT localhost
```

This attempts an SSH connection to your local machine on the port that's forwarded to the `$REMOTEHOST`'s SSH port.

Share Improve this answer Follow

edited Jan 8, 2014 at 6:11

bahamat
6,243 ● 24 ● 28

answered Oct 8, 2009 at 0:09

Brad Beyenhof
544 ● 2 ● 7

4

Of the presented answers, Zordache's is the the best overall solution. However for posterity, if you simply want to connect ad-hoc without editing your config, use the `-t` flag to allocate a pseudo terminal along with executing ssh directly on the relay.

```
ssh -t relay.example.com ssh internal.example.com
```

Share Improve this answer Follow

answered Jan 8, 2014 at 6:20

bahamat
6,243 ● 24 ● 28

simplest solution without edit files – Kartoch Jul 5, 2014 at 8:03

3

If you are willing to update the configuration on your client you can setup your client to use your gateway box as a proxy. Your relay box will need netcat installed, and for the best results you'll want to have key-based authentication setup.

Here is what I use in my .ssh/config to connect through another host.

```
Host internal-ssh-host-proxy
    ProxyCommand /usr/bin/ssh username@ssh-relay-host "/bin/netcat -w 1 internal-ssh-
host 22"
```

With the above you can simply run the command **ssh internal-ssh-host-proxy** from your client machine.

If the proxy SSH host is has the OpenSSH client 5.4 or above you do not need netcat, and instead you can use the built in netcat mode.

```
Host internal-ssh-host-proxy
    ProxyCommand /usr/bin/ssh username@ssh-relay-host -W internal-ssh-host:22
```

建议使用这种方式，不仅`ssh`命令可以直接使用，`sftp`命令也支持该配置。

其中，`.ssh`目录下的`config`文件中添加如下配置项目即可

```
Host test
    User root
    ProxyCommand ssh root@10.21.22.29  -i C:\Users\user\.ssh\data_id_rsa -p443 -W
10.21.22.28:22
```

使用`ssh test`或`sftp test`即可直接在客户机上通过中转机器`10.21.22.29`直接连接到目标机器`10.21.22.28`

Share Improve this answer Follow edited Jan 8, 2014 at 0:33

answered Oct 7, 2009 at 23:19

Zoredache
130k ● 40 ● 273 ● 415

Sorry but this is not using OpenSSH you are using netcat to do the relay between client server and server? – aHunter Oct 7, 2009 at 23:38

It is using OpenSSH combined with a very common utility that is available almost everywhere. It is not pure ssh, but I wouldn't call it bespoken. – Zoredache Oct 7, 2009 at 23:49

No I agree it is not bespoke but I wanted to know if it is possible to relay using OpenSSH so that you use a standard ssh client and ssh to a box running OpenSSH that then automatically then provides ssh access to another machine or multiple machines. Thanks – aHunter Oct 7, 2009 at 23:57

1 @aHunter, for the record there is now a 'netcat mode' built into openssh 5.4 which makes offers a pure openssh connection - blog.rootshell.be/2010/03/08/openssh-new-feature-netcat-mode no external tools are needed. – Zoredache Mar 30, 2010 at 0:03

2

You can forward connections automatically using OpenSSH. In your `~/.ssh/authorized_keys` file, you can specify a command to execute, which could be an SSH to a second machine.

```
[ssh client] ----> [ssh relay server] ----> [ssh target server]
    you          modified authorized_keys      target machine
```

What you will end up seeing is two prompts for `Password:`: one for the relay server and one for the target server. You can always remove this behaviour by using certificates.

Share Improve this answer Follow

answered Oct 8, 2009 at 0:20

sybreon
7,385 ● 1 ● 20 ● 20

that sounds perfect how would you configure the sshd in openssh? – aHunter Oct 8, 2009 at 2:43

Refer to the section on [Forced Commands][1] at [1] eng.cam.ac.uk/help/jpmg/ssh/authorized_keys_howto.html – sybreon Oct 8, 2009 at 5:35

this is an amazing idea. The last thing I want to do is open 100 discrete ports in my firewall with routes. Then repeat for redundancy. This suggests I can create 100 ssh keys and link each to it's own server. This also suggests that I can completely lockdown the relay server. Some might call this a VPN but I see it differently. – Richard Jan 31, 2020 at 16:48