大家都知道SSH是一种安全的传输协议，用在连接服务器上比较多。不过其实除了这个功能，它的隧道转发功能更是吸引人。下面是个人根据自己的需求以及在网上查找的资料配合自己的实际操作所得到的一些心得。  
首先先贴些一些关于ssh在端口转发方面的三个比较重要的命令的基本资料：

首先，认识下这三个非常强大的命令：

ssh -C -f -N -g -L listen\_port:DST\_Host:DST\_port user@Tunnel\_Host  
ssh -C -f -N -g -R listen\_port:DST\_Host:DST\_port user@Tunnel\_Host  
ssh -C -f -N -g -D listen\_port user@Tunnel\_Host

相关参数的解释：  
-f Fork into background after authentication.  
后台认证用户/密码，通常和-N连用，不用登录到远程主机。

-L port:host:hostport  
将本地机(客户机)的某个端口转发到远端指定机器的指定端口. 工作原理是这样的, 本地机器上分配了一个 socket 侦听 port 端口, 一旦这个端口上有了连接, 该连接就经过安全通道转发出去, 同时远程主机和 host 的 hostport 端口建立连接. 可以在配置文件中指定端口的转发. 只有 root 才能转发特权端口. IPv6 地址用另一种格式说明: port/host/hostport

-R port:host:hostport  
将远程主机(服务器)的某个端口转发到本地端指定机器的指定端口. 工作原理是这样的, 远程主机上分配了一个 socket 侦听 port 端口, 一旦这个端口上有了连接, 该连接就经过安全通道转向出去, 同时本地主机和 host 的 hostport 端口建立连接. 可以在配置文件中指定端口的转发. 只有用 root 登录远程主机才能转发特权端口. IPv6 地址用另一种格式说明: port/host/hostport  
  
-D port  
指定一个本地机器 “动态的’’ 应用程序端口转发. 工作原理是这样的, 本地机器上分配了一个 socket 侦听 port 端口, 一旦这个端口上有了连接, 该连接就经过安全通道转发出去, 根据应用程序的协议可以判断出远程主机将和哪里连接. 目前支持 SOCKS4 协议, 将充当 SOCKS4 服务器. 只有 root 才能转发特权端口. 可以在配置文件中指定动态端口的转发.

-C Enable compression.  
压缩数据传输。

-N Do not execute a shell or command.  
不执行脚本或命令，通常与-f连用。

-g Allow remote hosts to connect to forwarded ports.  
在-L/-R/-D参数中，允许远程主机连接到建立的转发的端口，如果不加这个参数，只允许本地主机建立连接。注：这个参数我在实践中似乎始终不起作用。

**实例说明：**  
一台服务器提供ftp服务（其实任何服务都可以），因为ftp传输是明文密码，如果不做ssh端口之前，我们可以通过tcpdump命令很容易的捕捉到明文信息。所以我们要对21端口进行转发：

（注：**我这里要使用的功能是鉴于这个理由，比如有三台电脑主机，A、B和C，它们有这样的访问规则：A<------>B<------>C-----x-----A。所以如果想从C登录到A，必须先登录到B在登录到A上，如果上传下载文件的话，也是非常麻烦，这使我们想到用ssh转发，使A的22端口转发到B的8822，然后再把B的8822端口转发到B本身的9944端口，端口号只要不被占用大于1024即可。这样，我们直接连接B的9944端口实际上就相当于连接A的22端口，就像是可以直接互联一样。这是我们要进行端口转发的出发点**）

ftp-server# ssh -CNfg -R 2121:localhost:21 root@100.0.0.50  
（注：**不用root也可以，只是通常情况下，非root用户限定端口不能使用1024以下的，但是以上的可以，所以，对于上面我所要求的情况。首先我们用传统的方式登录到A服务器上，然后可以使用如下命令：**  
**ssh -CNfg -R 8822:localhost:22 usernameinB@ipB**  
**然后会让你输入密码，输入完之后就消失到后台了**  
**PS:这里的localhost其实指的A服务器本身**  
）

然后登录到100.0.0.50机器，我们可以通过netstat -an|grep :2121查看端口已经侦听

（**这里我们登录到ipB的机器，然后就可以直接使用下面的命令：**

**ssh -l usernameinA localhost -p 8822**

**然后就可以登录到A服务器上了。**

**PS：这里的localhost其实指的是B机器，原理就是在B上连自己的8822，其实就是连A上的22端口，这都是由于上面第一步的转发形成的。注意与第一步的比较**）

100.0.0.50# ftp localhost 2121

就可以登录到ftp-server了，而且tcpdump无法捕获到有效的信息。  
2121端口任意选择，只要是机器上没有占用的端口就行

**来一个稍微复杂一点的，做网关的例子：**

（注**：它这里所说的复制的离子，其实就是我们要达到的目的，从C直接联到A，当然是通过B。**）  
假如内网有一台提供ftp(linux，port is 2121，称为A机器)的机器，通过网关服务器(linux，port is 8888，称为B机器)进去，现在外网有一台C机器需要访问网关服务器的某个端口(port is 21)来访问内网的ftp服务器。大家可以看到，其实这就像是一个基于ssh的防火墙程序，好，下面我们来具体操作：  
**1、login A 机器**

# ssh -CNfg -R 8888:localhost:2121 root@B机器IP  
（注：**同上，执行命令**  
**ssh -CNfg -R 8822:localhost:22 usernameinB@B机器IP**  
)

这样我们就在B机器上开了一个8888->2121的端口转换，但是由于8888端口只能侦听在localhost主机上，因此，虽然我们已经可以在B机器上使用

(注：**上面其实我们也解释了：这样我们就在B机器上开了一个B机器上的8822端口->A机器的22端口转换，但是由于8822端口只能侦听在localhost主机上，因此，虽然我们已经可以在B机器上使用**

**ssh -l usernameinA localhost -p 8822 来访问A机器，但仍然无法提供给外网的机器访问，下面正要解决直接C--->B  
  
  
PS：第一步其实就是上面实例时的那种情况**）

# ftp localhost 8888

来访问真正的ftp服务器，但仍然无法提供给外网的机器访问

**2、login B机器**

**（注：登上B）**

# ssh -CNfg -L 21:localhost:8888 root@localhost  
（**注：执行命令：**  
**ssh -CNfg -L 9944:localhost:8822 usernameinB@localhost**  
**在这里插播一个情况就是可能在登录的过程中会出现一个这样的问题：**

**ssh\_exchange\_identification: Connection closed by remote host**

**出现这种错误的原因是/etc/hosts.allow和/etc/hosts.deny阻止了你的登录，你要检查下。没有出现这个问题当然是最好。做完之后就在B机器上完成了9944--->8822的端口转换，可以侦听在任何地址上的请求。**）

这样做，是做本地机器上的21->8888端口转换，可以侦听在任何地址上的请求。

2(1)  
如果C机器也是一台linux机器，那也可以这样设置：

# ssh -CNfg -R 21:localhost:8888 root@C机器IP  
（**注：在我们这里就是执行 ssh -CNfg -R 9944:localhost:8822 usernameinC@C机器IP**）

**3。使用C机器，**  
可以是linux下的ftp命令，也可以是windows下的客户端软件都可以访问B机器的21端口来连接后台真正的ftp服务器(真正的端口是2121)

（**注：对于我们的情况，访问的就是B机器的9944端口，使用C机器上的帐户**）

如果是按照2(1)中的设置，则访问的地址为本机IP。

（**注：对于2（1）的情况，可以使用**

**ssh -l usernameinC localhost -p 9944**

**这里使用的localhost，实际上对应的C机器**）

至此，通常情况下用端口转发就可以实现。

再补充一点，其实对于2（1）的情况，有些软件也可以实现，比如putty，这方面的设置可以参考：我这里就不赘述了（http://www.lupaworld.com/batch.download.php?aid=1199）

简单介绍一个在linux下使用的设置ssh端口转换的程序  
[http://gstm.sourceforge.net/?page\_id=5](http://www.lupaworld.com/page_id=5.html)  
[p\_w\_upload=1197]  
  
在windows机器下使用putty也可以建立端口转发  
假设从windows机器上将本地的8888端口转发到B的21端口，可以做如下设置  
Connection->SSH-Tunnels中可以设置putty的端口转发，Source port为listen\_port，填8888，Destionation为DST\_Host:DST\_port，填写B机器IP:21，设置完了点Add.  
注意是local还是remote？  
[p\_w\_upload=1198]  
设置好后，我们可以在dos下用netstat命令看一下是否开启了本地的转发端口  
[p\_w\_upload=1199]  
接下来我们访问localhost的8888端口来访问ftp服务器了