SSH端口转发详解及实例

**目录**

* 1.1 SSH端口转发的两大功能
* 实验一：实现SSH端口转发——本地转发
* 实验二、实现SSH端口转发——远程转发
* 实验三、实现SSH端口转发——动态转发

**正文**

# 一、SSH端口转发简介

　　SSH会自动加密和解密所有SSH客户端与服务端之间的网络数据。但是，SSH还能够将其他TCP端口的网络数据通SSH链接来转发，并且自动提供了相应的加密及解密服务。这一过程也被叫做"**隧道**"（tunneling），这是因为SSH为其他TCP链接提供了一个安全的通道来进行传输而得名。例如，Telnet ，SMTP ，LDAP这些TCP应用均能够从中得益，避免了用户名，密码以及隐私信息的明文传输。而与此同时，如果工作环境许中的防火墙限制了一些网络端口的使用，但是允许SSH的连接，也能够将通过将TCP用端口转发来使用SSH进行通讯。

## 1.1 SSH端口转发的两大功能

* 加密SSH Client端至SSH Server端之间的通讯数据。
* 突破防火墙的简直完成一些之前无法建立的TCP连接。

# 二、本地转发

**命令：-L localport:remotehost:remotehostport sshserver**

**说明：**localport　　　　　　 本机开启的端口号

      remotehost　　　　　　最终连接机器的IP地址

      remotehostport        转发机器的端口号

      sshserver　　　　　　 转发机器的IP地址

**选项：**

-f 后台启用

-N 不打开远程shell，处于等待状态（不加-N则直接登录进去）

-g 启用网关功能

    接下来，我们通过实验来详细的说明一下如何实现本地转发：

## 实验一：实现SSH端口转发——本地转发

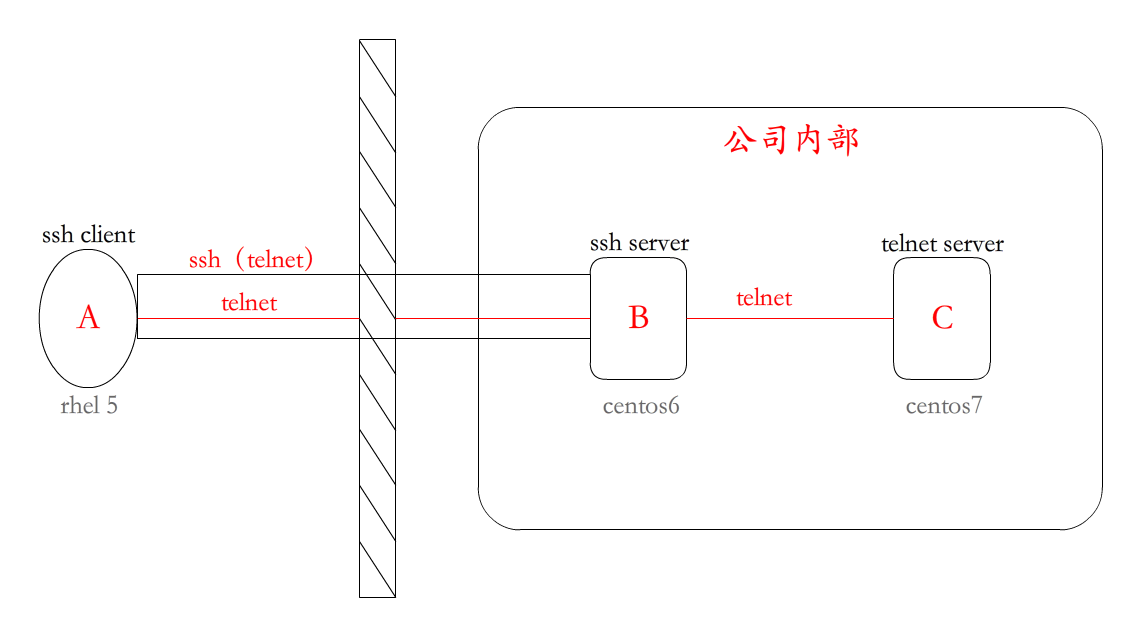
**背景：**企业内部C服务器只允许telnet连接（23端口）访问，不允许外部直接访问，B服务器是一个ssh服务器；有一个用户需要从外部连接到企业内部的C服务器。

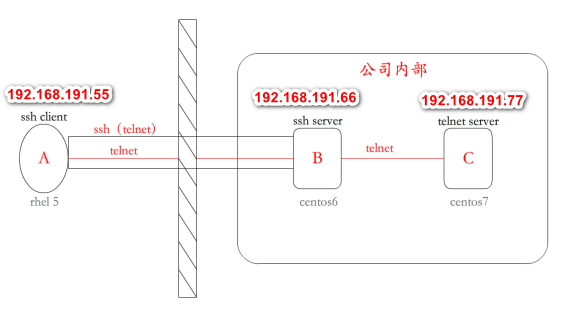
**前提：**防火墙允许22端口进来（或者企业内部有一个堡垒机，ssh -t通过堡垒机进去）。

**原理：**A用户通过ssh协议连接到B机器上，再通过B机器做跳板，连接至C机器。

**机器：**rhel5模拟A用户，centos6模拟B机器，centos7模拟C机器

**图示如下：**





**实验步骤：**

1）模拟C机器不允许A用户连接，并且开启B机器的telnet服务端口23。

在centos7上输入以下口令：

**iptables -A INPUT -s 192.168.191.55 -j REJECT**

IMG_257

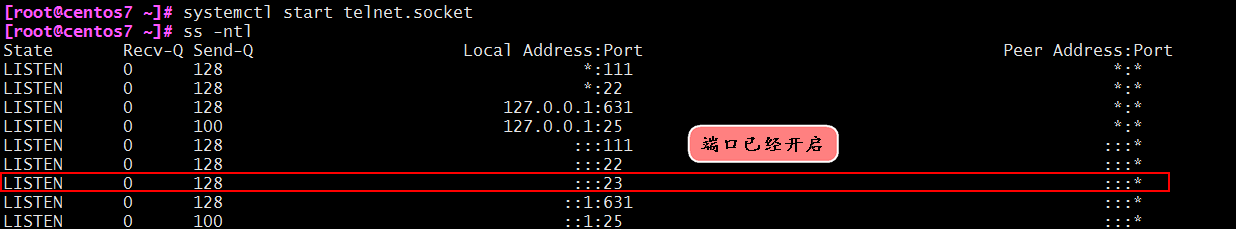
此时，从rhel5用ssh命令连接centos7，是拒绝的：

IMG_258

同时，我们还要开启7的telnet服务端口23：

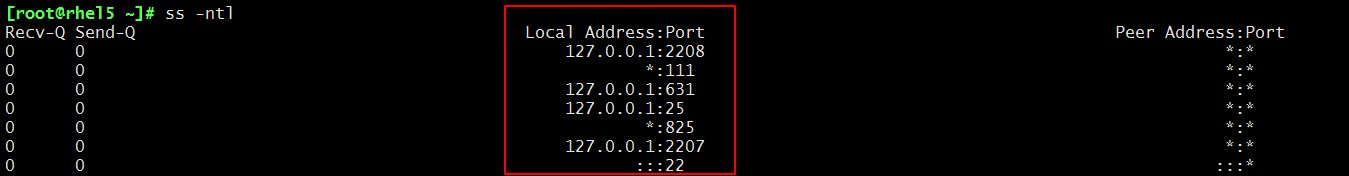
**systemctl start telnet.socket**

用**ss -ntl**命令可以查看的服务端口是否已开启



2）开启端口转发（telnet隧道）

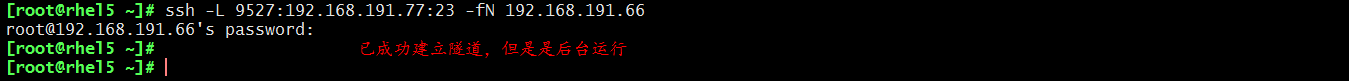
    首先，我们在5机器上确认已经开启的端口有哪些：



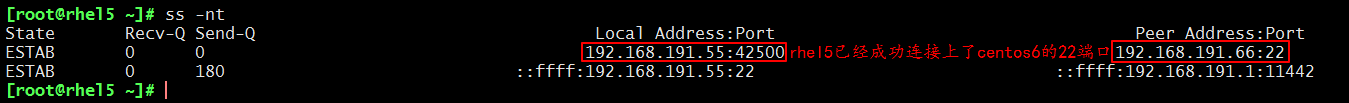
我们使用的端口是9527端口，从上图中我么已经看出，9527端口没有被占用，所以我们可以使用~

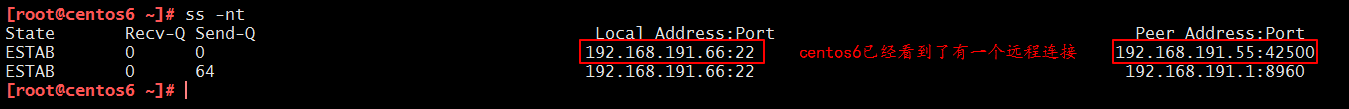
接着我们建立本地转发的隧道（5上输入以下命令）：

**ssh -L 9527:192.168.191.77:23 -fN 192.168.191.66**



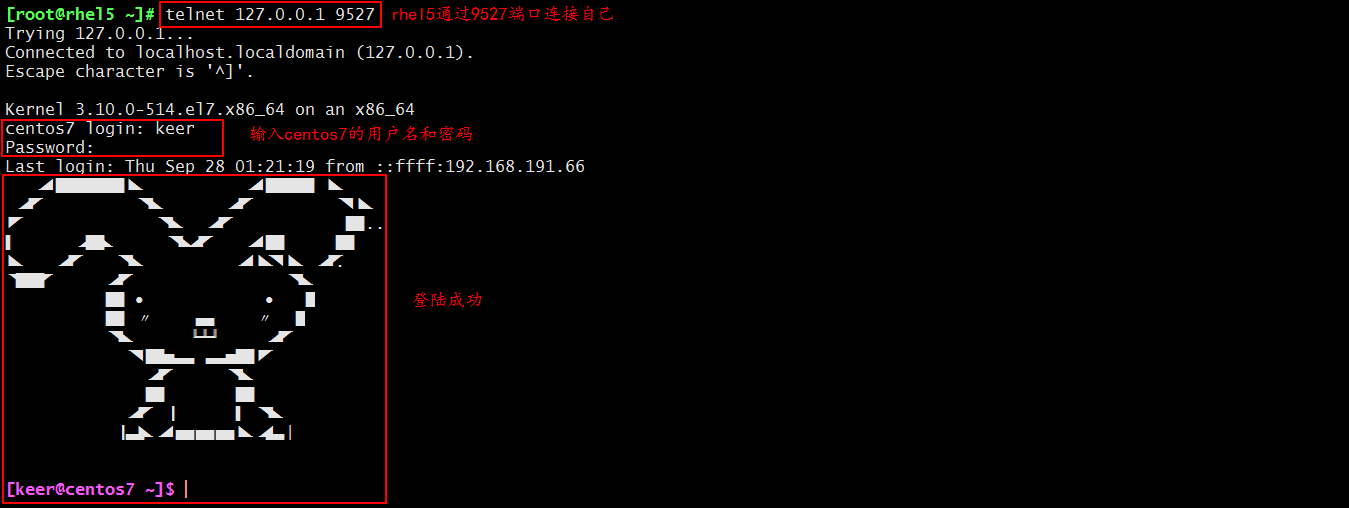
    在这里，我们可以使用**ps aux**来查询后台运行的进程。也可以通过**ss -nt**查看接口连接情况：



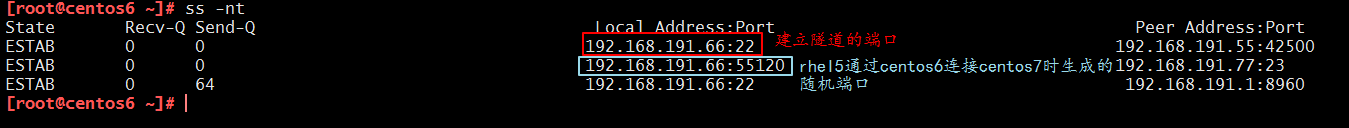


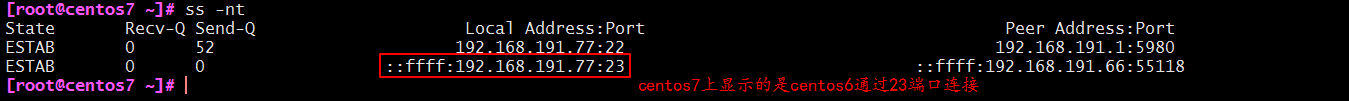
3）在rhel5上输入以下命令，用9527端口连接自己：

**telnet 127.0.0.1 9527**



    此时，我们可以查看一下centos6和centos7的连接情况：





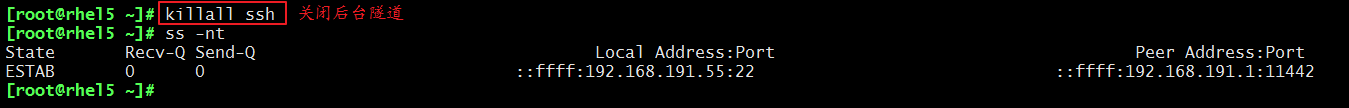
    至此，我们已经实现了A用户在公司外部远程连接C机器的需求，接下来我们就来讲一讲实现过程：

    data <- -> localhost:9527端口 <- -> localhost:XXXXX（随机在客户端6开一个端口） <- -> sshsrv:22（通过ssh封装） <- -> sshsrv:YYYYY（服务器解封装，开一个端口，代表telnet客户端） <- -> telnetsrv:23

　　用大白话来解释就是：当rhel5（A用户）连接自己的9527端口时，该请求自然会通过ssh协议封装发送给centos6（B机器），然后在centos6（C机器）上解封装,形成telnet流量，发送给centos7（C机器）。

　　实验做完了，如果我们想要停止这个隧道，直接把后台的隧道进程杀死就可以了，命令如下：

**killall ssh**



　　我们的实验圆满完成ヾ(✿ﾟ▽ﾟ)ノ

# 三、远程转发

　　在我们实验一的场景下，首先要满足的是防火墙上必须打开22端口，但是在现实生活中，企业处于安全考虑，一般是不会打开防火墙，只允许出不允许进。所以，当防火墙的端口没有打开的时候，我们要怎么办呢？这就要用到我们接下来要说的远程转发了：

**命令：**-R sshserverport:remotehost:remotehostport sshserver

**说明：**sshserverport         被转发机器开启的端口号

      remotehost       　　 最终连接机器的IP地址

      remotehostport        被转发机器的端口号

      sshserver             被转发机器的IP地址

　　同样的，我们以实验来具体说明我们的远程转发：

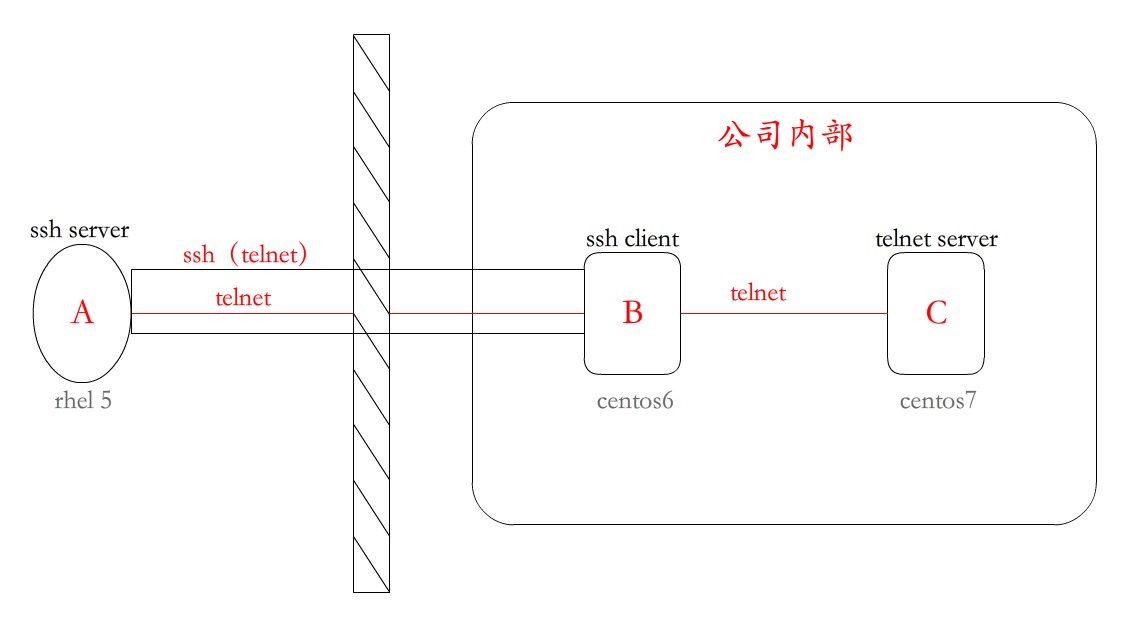
## 实验二、实现SSH端口转发——远程转发

**背景：**企业内部C服务器只允许telnet连接（23端口）访问，不允许外部直接访问，B服务器是一个ssh服务器；有一个用户需要从外部连接到企业内部的C服务器。

**原理：**B机器访问A用户，给A用户转发

**机器：**rhel5模拟A用户，centos6模拟B机器，centos7模拟C机器

**图示如下：**



**实验步骤：**

1）模拟C机器不允许A用户连接，并且开启B机器的telnet服务端口23。

　　在centos7上输入以下口令：

**iptables -A INPUT -s 192.168.191.55 -j REJECT**

IMG_269

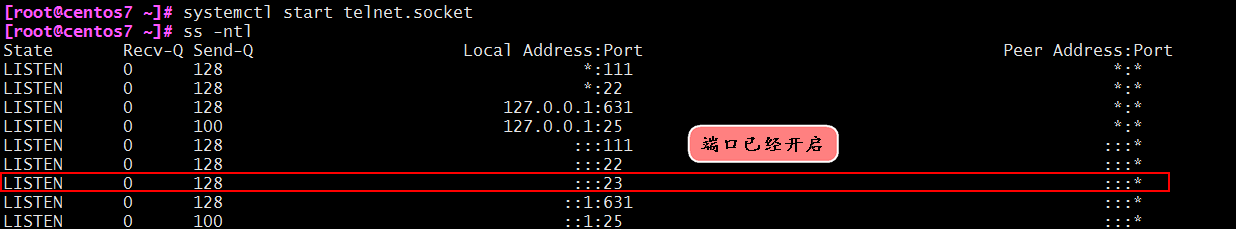
　　此时，从rhel5用ssh命令连接centos7，是拒绝的：

IMG_270

　　同时，我们还要开启7的telnet服务端口23：

**systemctl start telnet.soc ket**

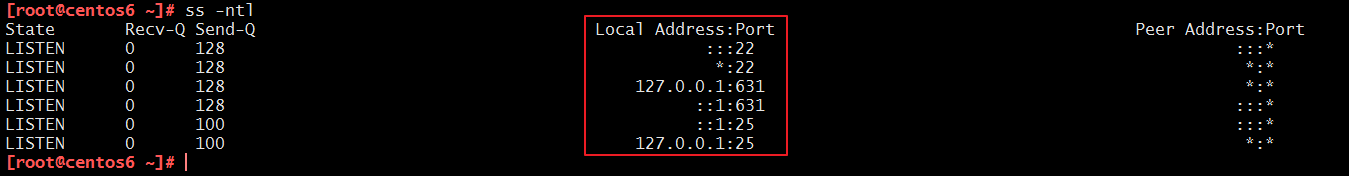
　　用**ss -ntl**命令可以查看的服务端口是否已开启



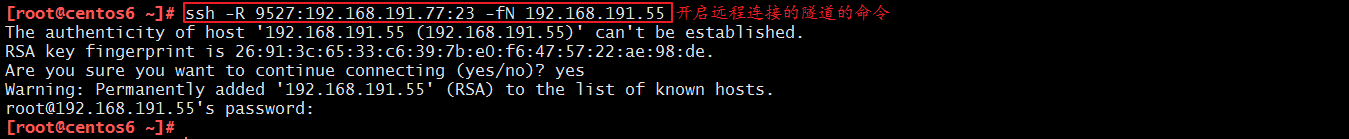
2）开启隧道转发（telnet隧道）

    这一次，由于防火墙完全关闭，外部的设备连接不进来，所以我们要通过B机器去连接A用户的机器，因此，我们的开启隧道命令要在B机器（centos6）上运行：

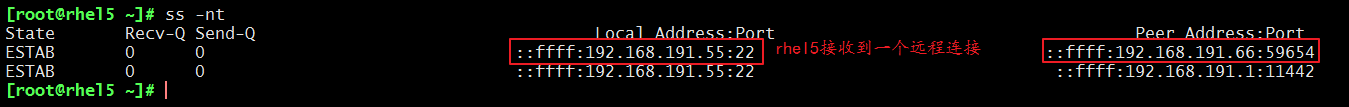
    首先，我们要确定一下centos6上开启了哪些端口：

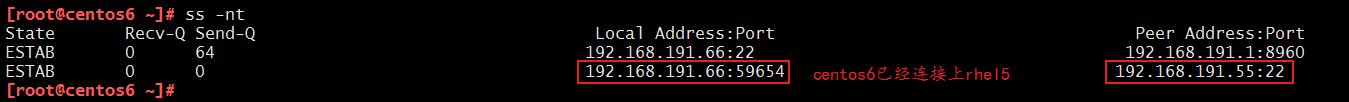


    然后，我们选择一个没有被开启的端口开启隧道，进行实验：



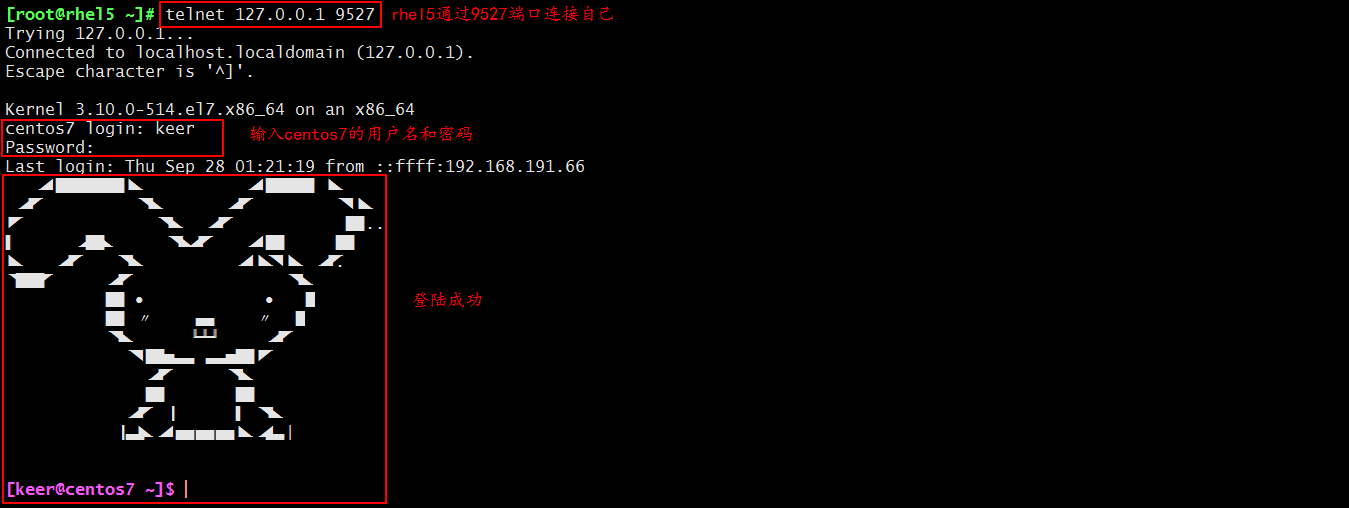
　　同样的，在这里，我们可以使用**ps aux**来查询后台运行的进程。也可以通过**ss -nt**查看接口连接情况：



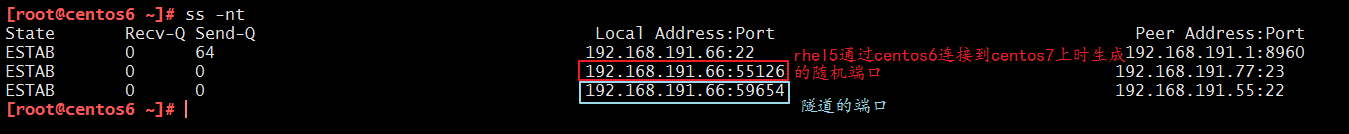


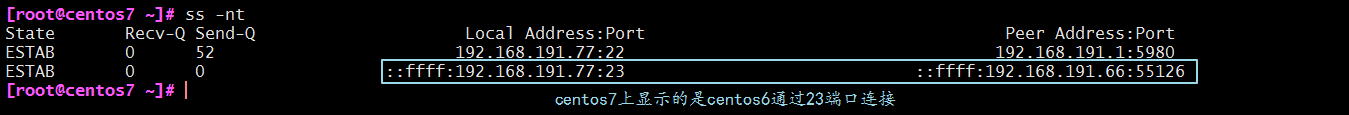
3）在rhel5上输入以下命令，用9527端口连接自己：

**telnet 127.0.0.1 9527**



    此时，我们可以查看一下centos6和centos7的连接情况：





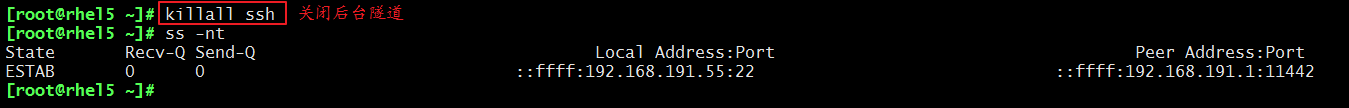
    至此，我们已经实现了A用户在公司外部远程连接C机器的需求，接下来我们就来讲一讲实现过程：

　　data <- -> sshsrv:9527端口 <- -> sshsrv:22（通过ssh封装） <- -> localhost:XXXXX（随机在客户端6开一个端口） <- -> localhost:YYYYY（服务器解封装，开一个端口，代表telnet客户端） <- -> telnetsrv:23

　　用大白话来解释就是：当rhel5（A用户）连接自己的9527端口时，该请求自然会通过ssh协议封装发送给centos6（B机器），然后在centos6（C机器）上解封装,形成telnet流量，发送给centos7（C机器）。

　　实验做完了，如果我们想要停止这个隧道，直接把后台的隧道进程杀死就可以了，命令如下：

**killall ssh**



　　我们的实验圆满完成ヾ(✿ﾟ▽ﾟ)ノ

# 四、动态转发

　　众所周知，我国有一个功能强大的防火墙，用来避免我们访问谷歌等外国的部分网站，嗯。。。FQ的方法有很多，相信大家不比小编懂的少，所以我们就不一一举例说明了。接下来，小编就给大家说一说如何通过ssh转发技术实现FQ~

　　这里，就要用到我们的动态转发技术了：

　　当用firefox 访问internet 时，本机的1080 端口做为代理服务器，firefox 的访问请求被转发到sshserver 上，由sshserver替之访问internet。

　　接下来，我们还是以实验进行说明：

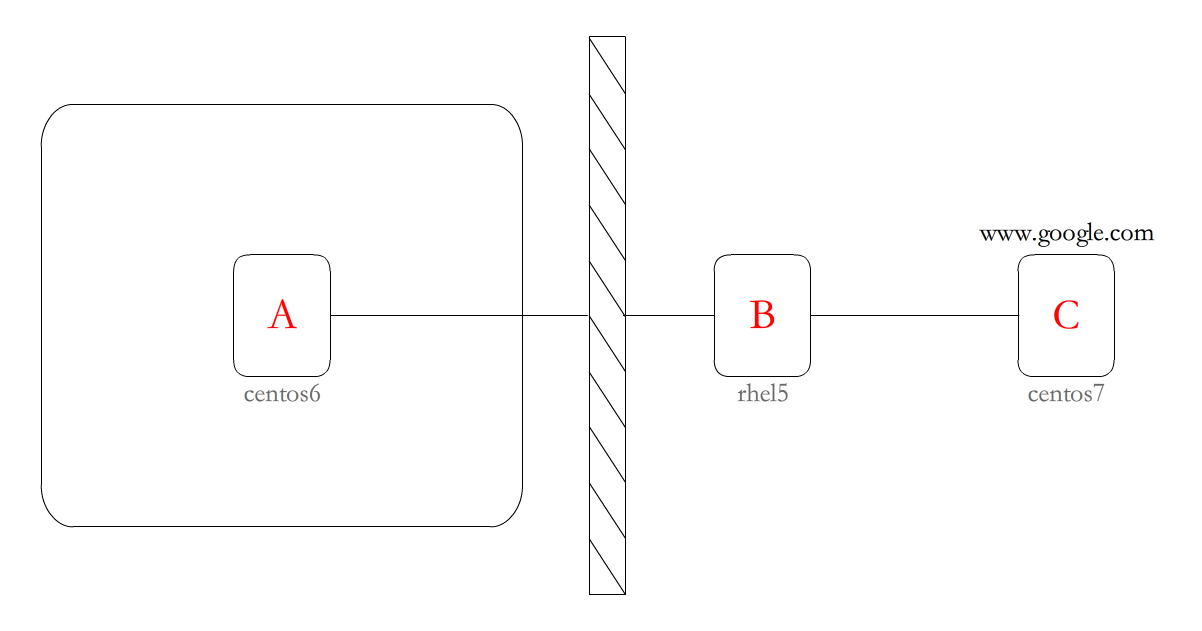
## 实验三、实现SSH端口转发——动态转发

**背景：**模拟Google的服务器C不允许国内网站A直接访问，B服务器是国外的一个小型的学习用的服务器；国内网站A可以访问国外学习服务器B；实现国内网站A访问模拟Google服务器C。

**原理：**国内网站A通过ssh协议连接到国外学习服务器B上，再通过国外学习服务器B做跳板，连接至Google服务器C。

**机器：**centos6模拟国内网站A，rhel5模拟国外学习服务器B，centos7模拟Google服务器C

**图示如下：**



**实验步骤：**

1）在模拟google服务器C上搭建一个网页，从互联网上访问centos7时，页面显示"Welcome to www.google.com"

　　命令如下：

[root@centos7 ~]# cd /var/www/html/

[root@centos7 html]# vim index.html<h1> Welcome to www.google.com </h1>

    编写完文件以后，记得重启一下httpd服务：

[root@centos7 html]# systemctl restart httpd

2）模拟Google服务器C不允许国内网站A连接

在centos7上输入以下口令：

**[root@centos7 ~]# iptables -A INPUT -s 192.168.191.66 -j REJECT**

此时，我们来测试一下centos6和rhel5能否访问centos7，命令为：

**curl 192.168.191.77** 或 **links 192.168.191.77**

[root@rhel5 ~]# curl 192.168.191.77

<h1> Welcome to www.google.com </h1>

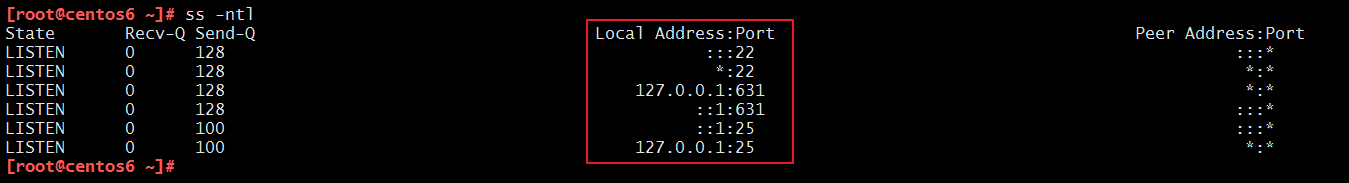
[root@centos6 ~]# curl 192.168.191.77

curl: (7) couldn't connect to host

　　可以看出，rhel5可以连接到centos7，但是centos6不能连接到centos7。我们现在的需求就是希望centos6可以借助于rhel5访问centos7，方法也很简单，接下来就给大家说一说。

3）动态端口转发

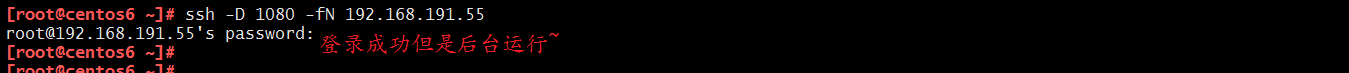
    首先，我们在6机器上确认已经开启的端口有哪些：



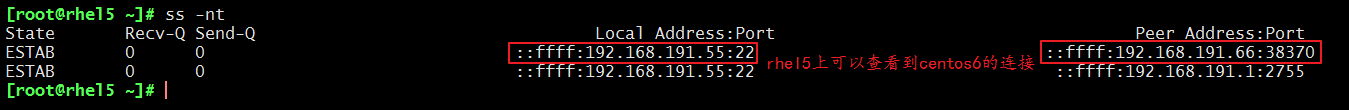
　　我们使用1080端口，从上图中我么已经看出，1080端口没有被占用，所以我们可以使用~

　　接着我们建立动态转发的隧道（6上输入以下命令）：

**ssh -D 1080 -fN 192.168.191.55**

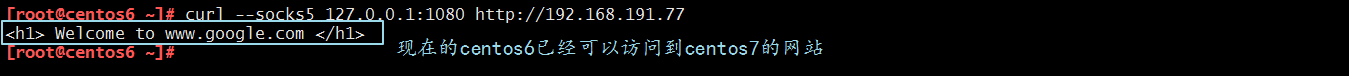


    在这里，我们可以在rhel5上查看到centos6的连接：

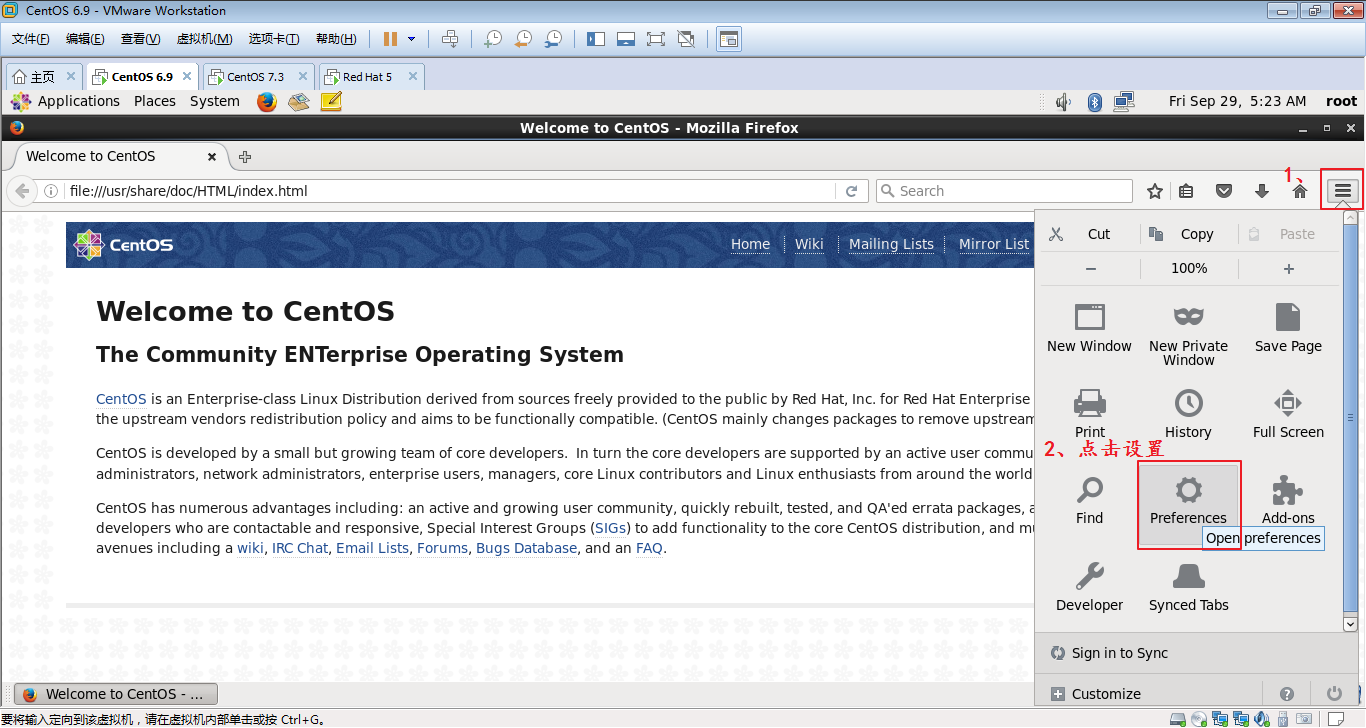


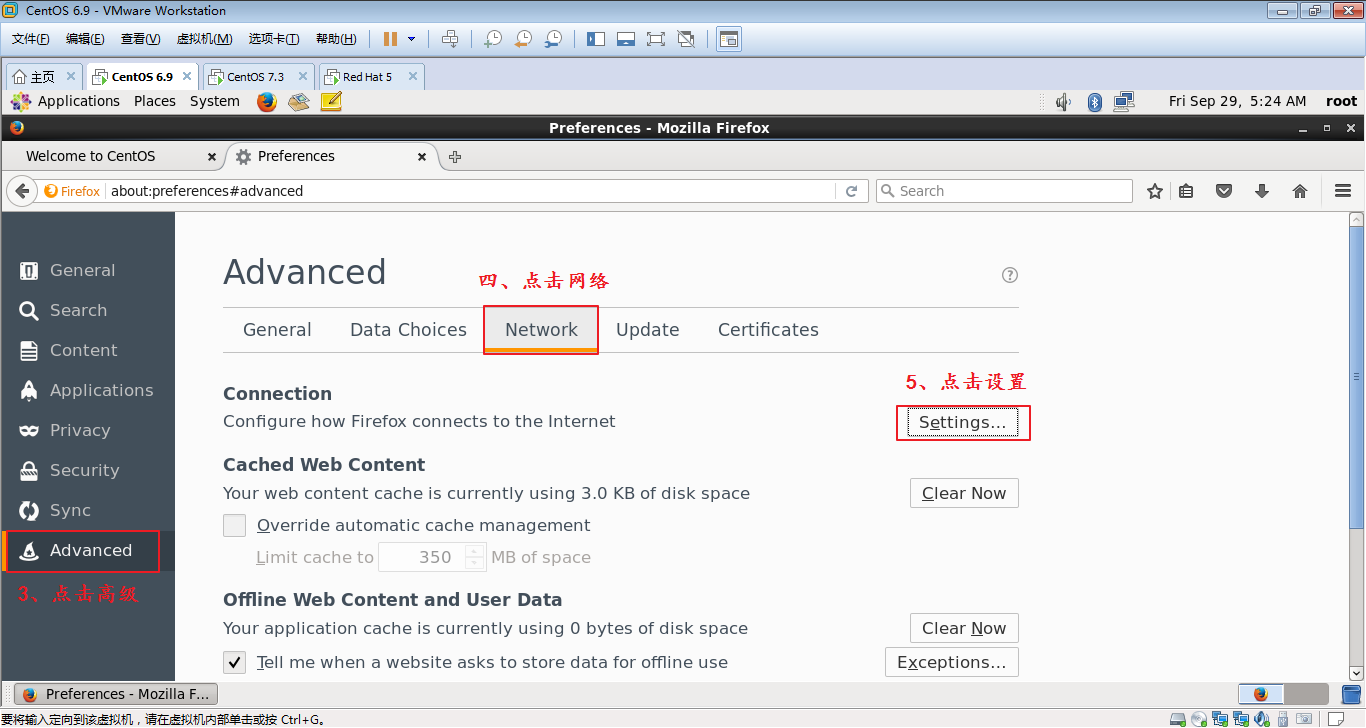
4）设置代理rhel5访问centos7，命令如下（在centos6上输入）：

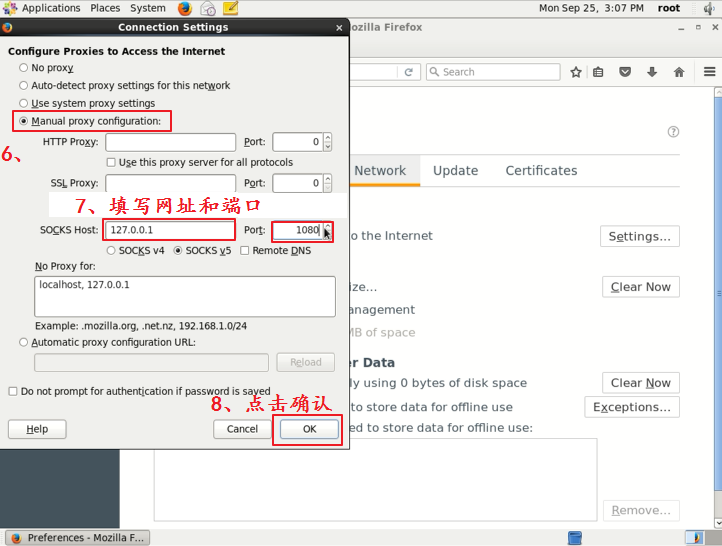
**curl --socks5 127.0.0.1:1080 http://192.168.191.77**



5）在图形化界面，在centos6上的firefox浏览器设置代理：









　　我们的实验圆满完成ヾ(✿ﾟ▽ﾟ)ノ

作者：[珂儿吖](http://www.cnblogs.com/keerya/" \t "https://www.cnblogs.com/keerya/p/_blank)

出处：[http://www.cnblogs.com/keerya/](http://www.cnblogs.com/keerya/" \t "https://www.cnblogs.com/keerya/p/_blank)

本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。   
大家写文都不容易，希望尊重劳动成果哟~

标签: [ssh](http://www.cnblogs.com/keerya/tag/ssh/)