SSH 三种端口转发测试

# 环境介绍：

服务器 A

52.97.16.21

服务器 B

52.97.16.18

服务器 C

52.97.16.17

# 本地端口转发

**####命令：**

ssh -Nf -L [local\_A\_address]:local\_A\_port:target\_C\_server:target\_C\_port via\_B\_server

ssh -Nf -p 57613 -L 20880:52.97.16.17:80 root@52.97.16.18

**####参数：**

-N,不执行命令

-f,后台执行

-L,local本地端口转发

local\_A\_address:

127.0.0.1 - 默认，只能本机使用这个端口转发

也可以是本机的IP地址，同时其他人可以使用这个IP来使用这个端口转发

via\_B\_server:中间服务器

**####应用：**

A---能访问------>B-------能访问------>C

A---不能访问----------------------------->C

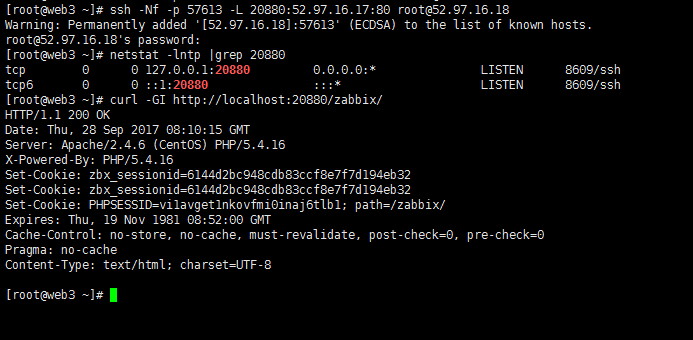
A---通过本机端口,以B的名义访问-->C

**####关闭：**

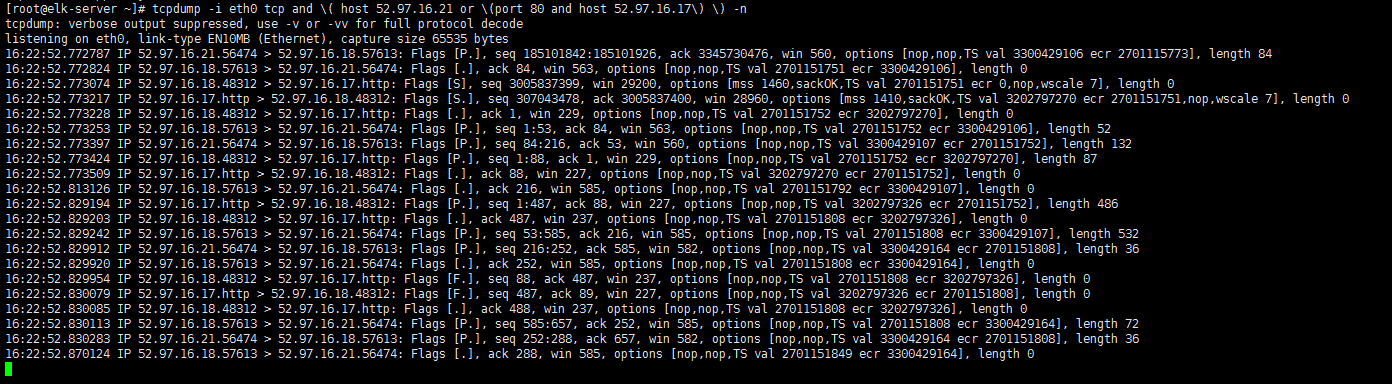
直接kill -9 建立的SSH连接，下同



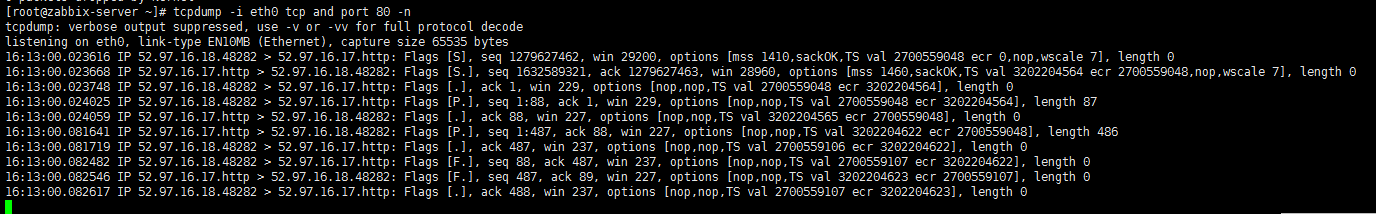
在A服务器上访问A的20880 端口成功返回信息



在B服务器上抓包，显示是B服务器去访问C的80，然后把返回的数据转发给A服务器



在C服务器上抓包，显示访问C的80端口的服务器是B



# 2 远程端口转发

**在B上执行**

**####命令：**

ssh -Nf -R [local\_A\_address]:local\_A\_port:target\_C\_server:target\_C\_port local\_A\_address

**####参数：**

-R,remote,远程端口转发

local\_A\_address,这个地址为A的IP

**####应用：**

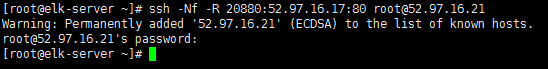
环境和目的 与 本地端口转发是一样的，这里只是不在本地服务器A上执行命令，而是在中间服务器B上执行；

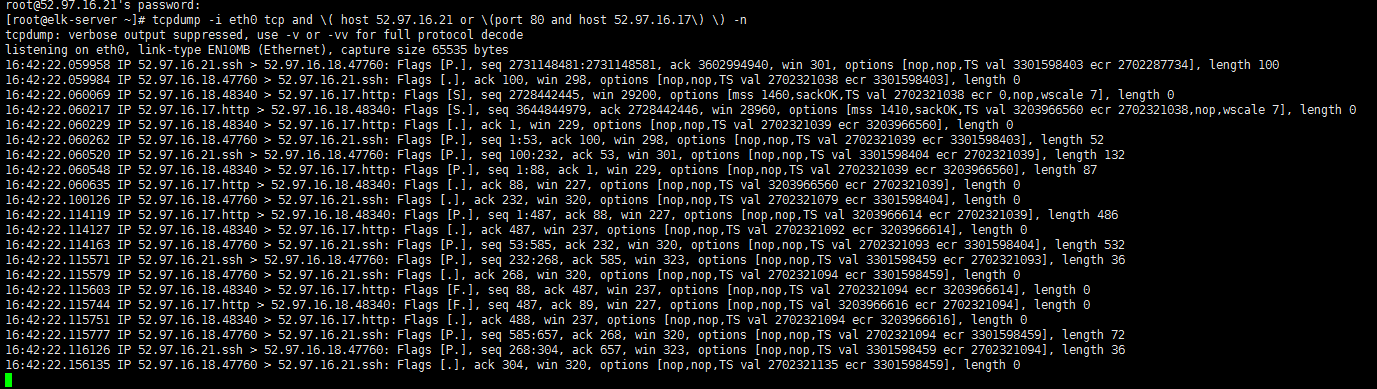
为什么不直接在服务器A自己身上执行命令呢？这个场景有别于本地端口转发的地方在于A不能主动连接B但反之可以，比如A在外网，B在内网；

而A去访问的时候，同样都是通过自己的IP和端口，同样首先建立AB之间的SSH通道，以服务器B的名义来访问目标服务器C。

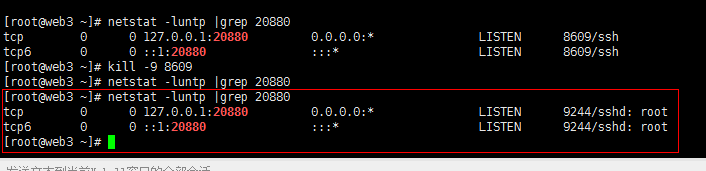


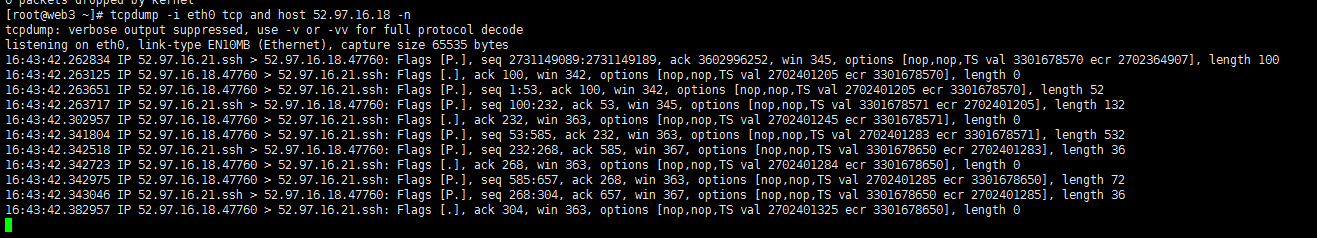
服务器B



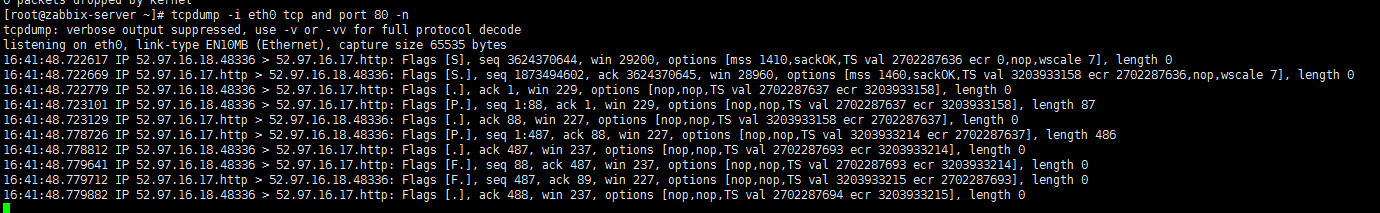


服务器A





在C服务器上抓包，显示访问C的80端口的服务器是B



# 3 动态端口转发

**####命令：**

ssh -Nf -D [local\_A\_address]:local\_A\_port via\_B\_server

ssh -Nf -p B\_SSH\_PORT 10.10.1.200:8080 B\_User@10.10.1.201

**####参数：**

-D,dynamic,动态端口转发

**####应用：**

本地和远程端口转发，都限定了目标服务器以及目标服务器的端口；

而动态端口转发，A把B作为了自己的全权代理，不限定目标服务器及其端口；

这里要求在A上，做下代理设置，比如浏览器的代理设定为自己的IP:PORT；

本地端口转发和远程端口转发，其实都可看着是动态端口转发(代理)的子集；

三者和一般代理的目的和场景都一致，区别在于这里自己A和代理服务器B之前的所有连接都是基于加密的SSH。