实验虚拟主机各自用户名密码：

client主机

用户名：root  密码：123456

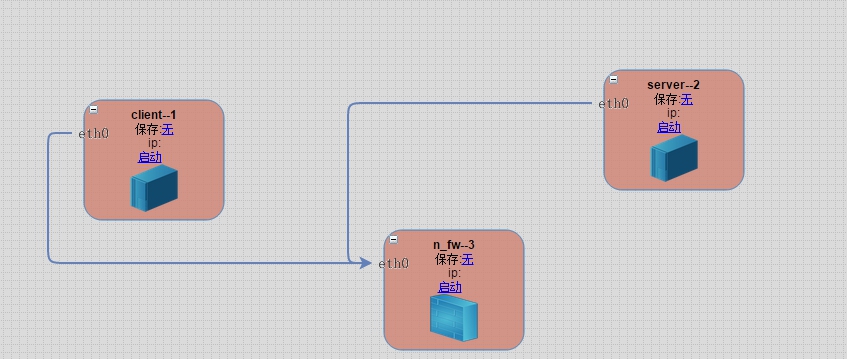
n\_fw主机

用户名：root  密码：123456

server

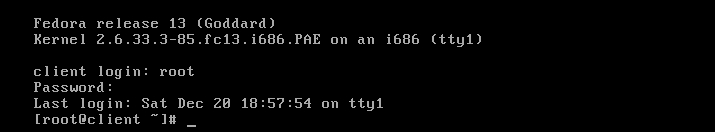
用户名：root  密码：123456

第一步、单击“网络拓扑”，启动并进入目标主机，进入实验环境，如图



第二步、启动系统并修改ip 地址

启动client(密码123456)



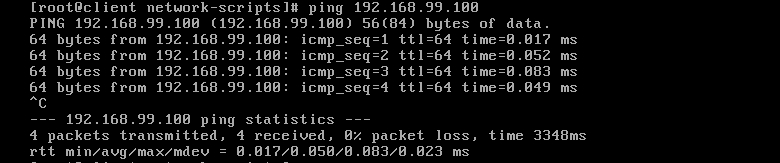
修改eth0 的地址



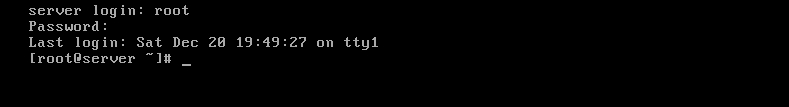
地址生效

service  network restart

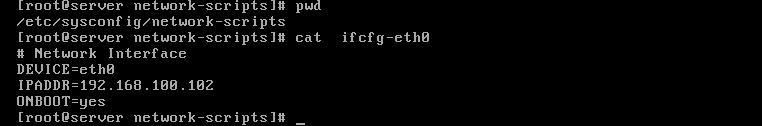
ping 192.168.99.100



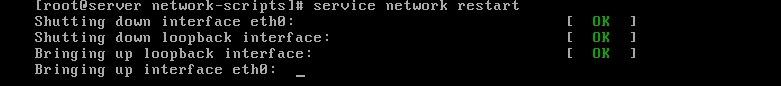
启动服务器



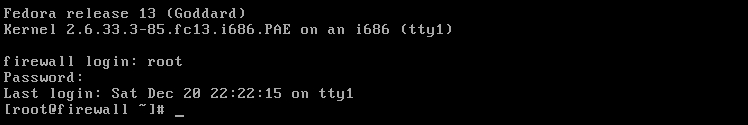
修改地址



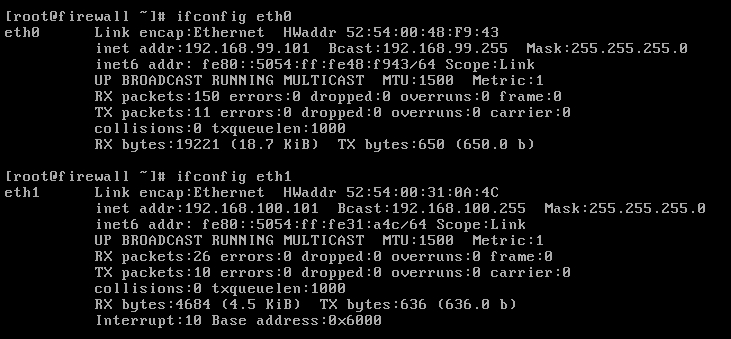
修改生效



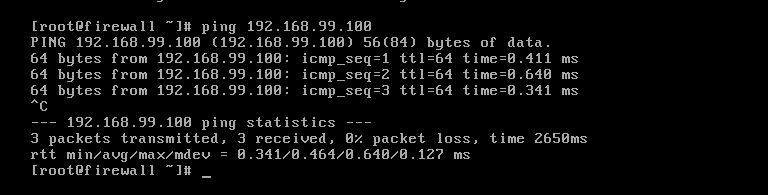
第三步、启动防火墙



查看防火墙地址

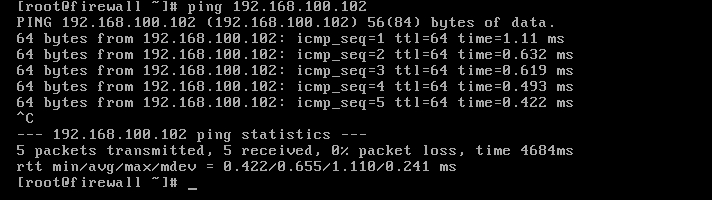


ping 192.168.99.100



从防火墙到客户端是通的

ping 192.168.100.102



从防火墙ping 内网是通的

需要内网地址能访问外网地址需要

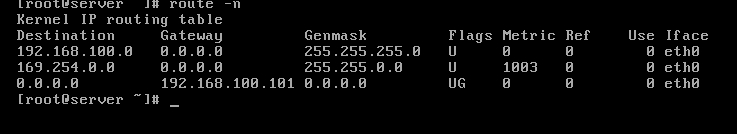
增加缺省路由

#route add default gw 192.168.100.101

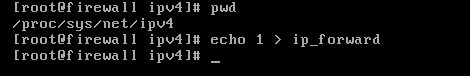
http://10.144.53.6/api/attachment?type=courseDocument&id=9012

查看路由信息

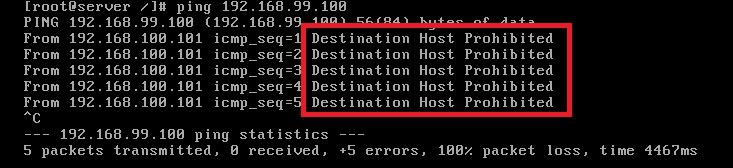
#route -n



防火墙增加转发功能



然后在内网ping外网地址 192.168.99.100



发现不通

然后再到防火墙上，查看防火墙的缺省规则

iptables -L



发现转发被禁止

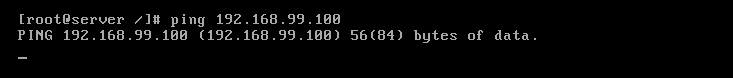
说明防火墙规则不让转发ping

我们增加一条允许 ping 的规则，此规则必须在红线圈定的规则之前

#iptables –I FORWARD 1 –p icmp   –j ACCEPT

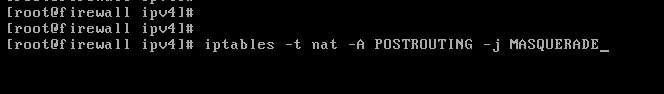
然后在内网ping 外网地址

ping 192.168.99.100



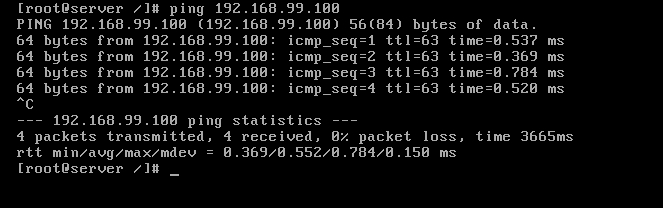
发现这次不同是因为路由问题,同时为了隐藏内网地址.

这时候需要在防火墙上增加地址伪装规则



这时再在内网ping 外网地址

#ping 192.168.99.100

这时在外网抓包

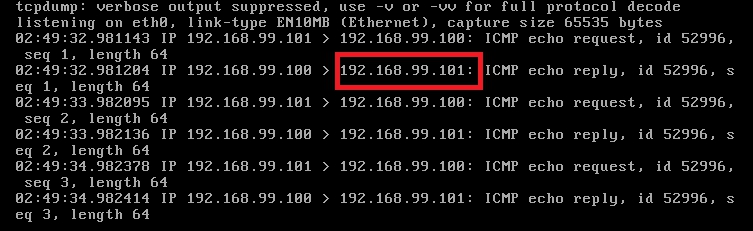
#tcpdump –i eth0 icmp

http://10.144.53.6/api/attachment?type=courseDocument&id=9018

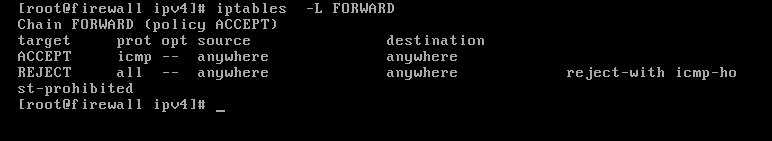
在内网ping 外网地址

#ping 192.168.99.100

再回到外网,发现抓包的数据

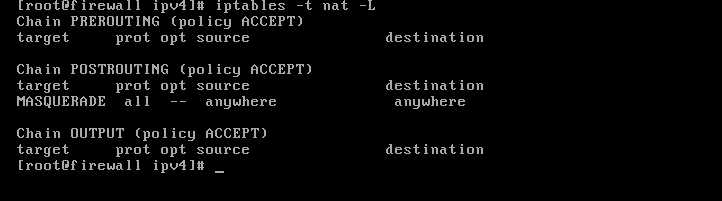


#Iptables –L FORWARD



查看nat 表的规则

#iptables –t nat –L



第四步、如果外网有ftp服务器,配置规则,允许内网访问

首先配置外网规则,允许ftp 服务可以被访问

#iptables –I INPUT 5 –p tcp --dport 21 –j ACCEPT

http://10.144.53.6/api/attachment?type=courseDocument&id=9031

其次在防火墙上配置允许内网访问的规则

#iptables –I FORWARD 2 –s 192.168.100.0/24 –j ACCEPT

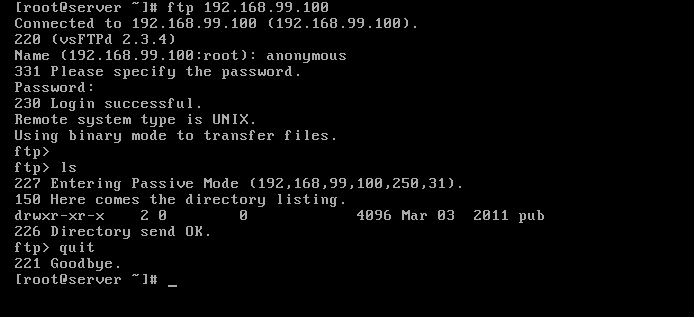
#iptables –I FORWARD 3 –d 192.168.100.0/24 –j ACCEPT

#iptables –L FORWARD



在内网ftp 外网地址

#ftp 192.168.99.100



第五步、实验完毕，关闭实验窗口和网络拓扑图。