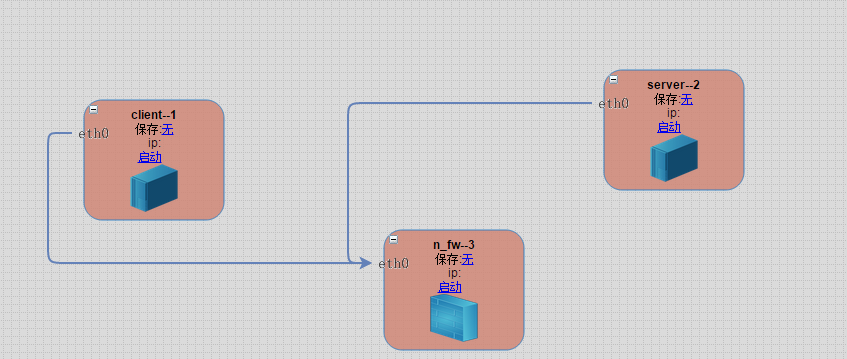
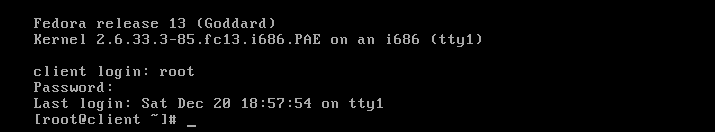
1、  单击“网络拓扑”，启动并进入目标主机，进入实验环境，如图

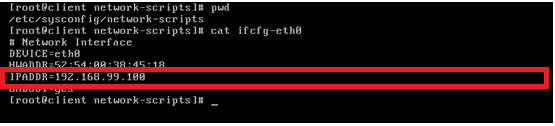


2、  启动系统并修改ip 地址

启动client(密码123456)



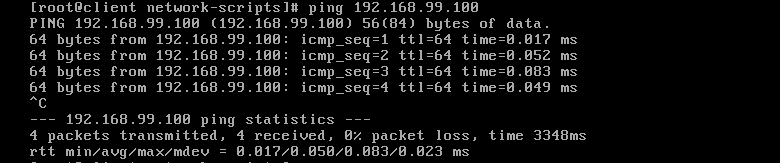
修改eth0 的地址



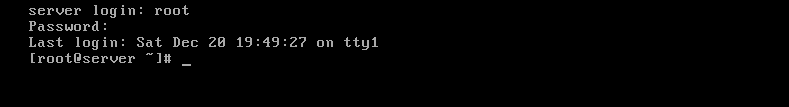
地址生效

service  network restart

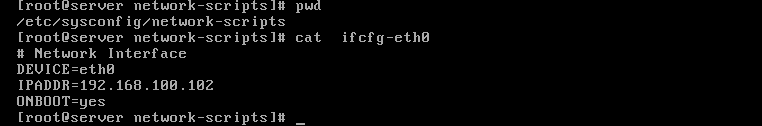
ping 192.168.99.100



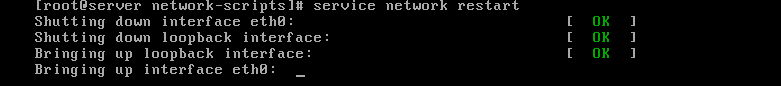
启动服务器



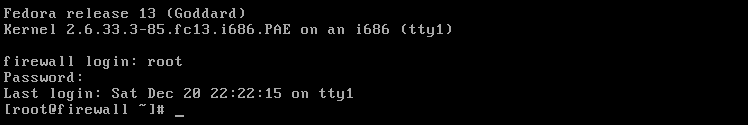
修改地址



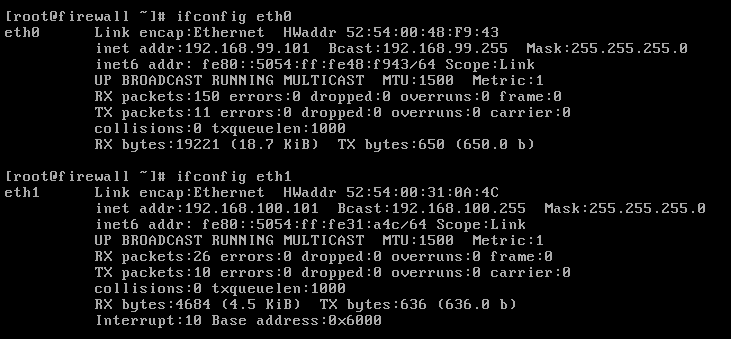
修改生效



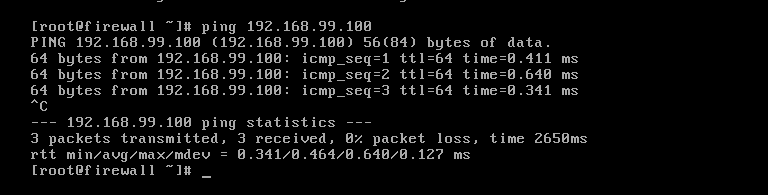
3、  启动防火墙



查看防火墙地址

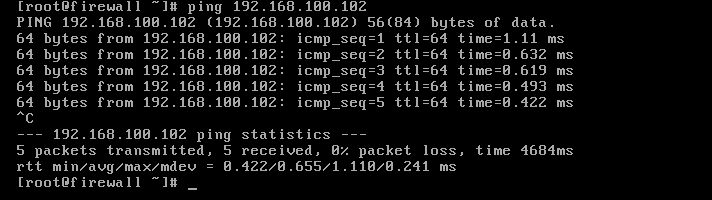


ping 192.168.99.100



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

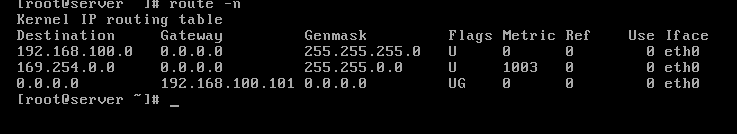
增加缺省路由

#route add default gw 192.168.100.101

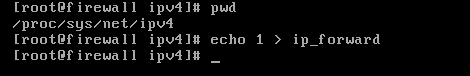
http://10.144.53.6/api/attachment?type=courseDocument&id=4926

查看路由信息

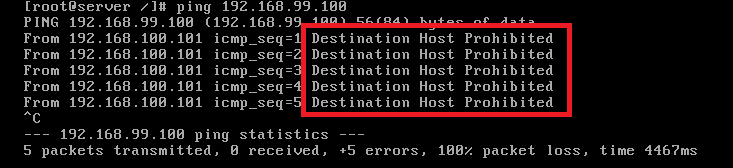
#route -n



防火墙增加转发功能



然后在内网ping外网地址 192.168.99.100



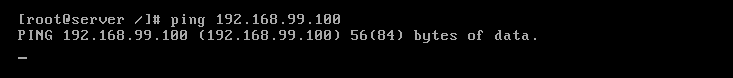
说明防火墙规则不让转发ping 的

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

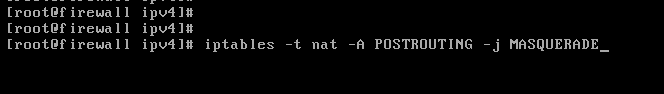
然后在内网ping 外网地址

ping 192.168.100.99



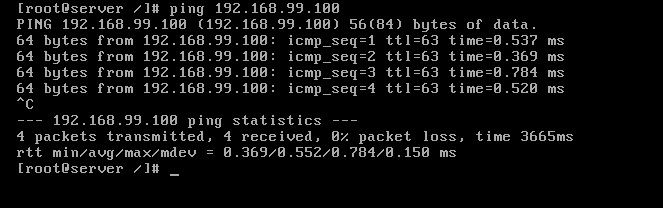
发现这次不同是因为路由问题,同时为了隐藏内网地址.

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

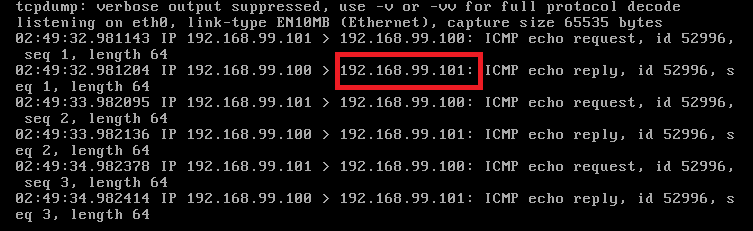
#tcpdump –i eth0 icmp

http://10.144.53.6/api/attachment?type=courseDocument&id=4921

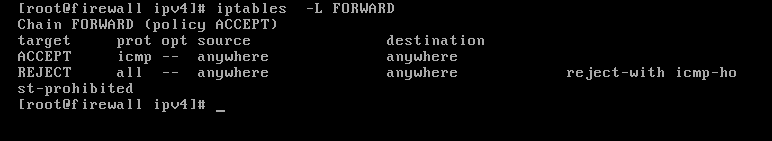
在内网ping 外网地址

#ping 192.168.99.100

再回到外网,发现抓包的数据

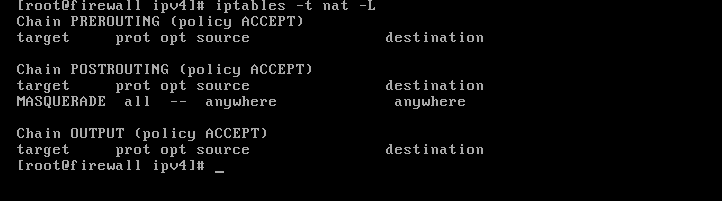


#Iptables –L FORWARD



查看nat 表的规则

#iptables –t nat –L



4、  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=4939

其次在防火墙设置记录规则

# iptables -I FORWARD 1 -p icmp -j ULOG

http://10.144.53.6/api/attachment?type=courseDocument&id=4923

在防火墙启动日志监控程序

# /usr/local/ulogd/sbin/ulogd  &

http://10.144.53.6/api/attachment?type=courseDocument&id=4941

在防火墙上

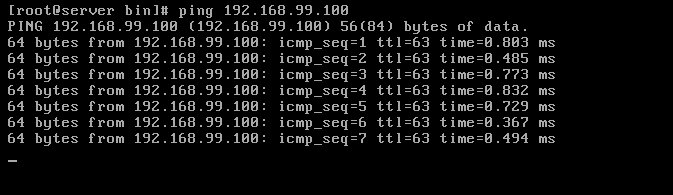
#iptables -I FORWARD 1 -p tcp --dport 21 -j ACCEPT

#iptables -I FORWARD 2 -m state --state RELATED,ESTABLISHED -j ACCEPT

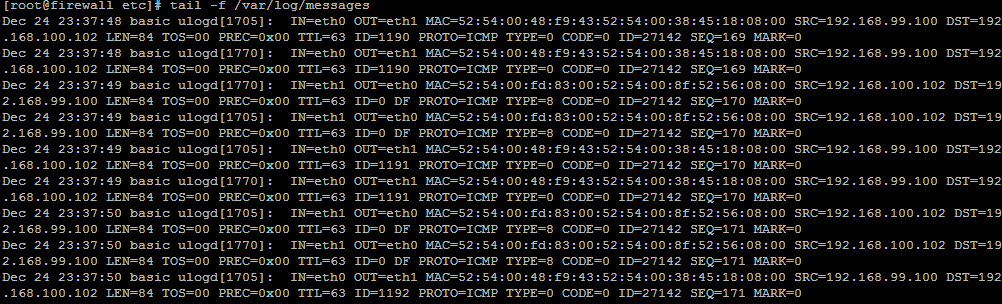
#tail –f /var/log/messages

在内网

#ping 192.168.99.100



再回到防火墙



发现在messages 里已经记录了很多日志

#iptables –I FORWARD 2 –p tcp –j ULOG

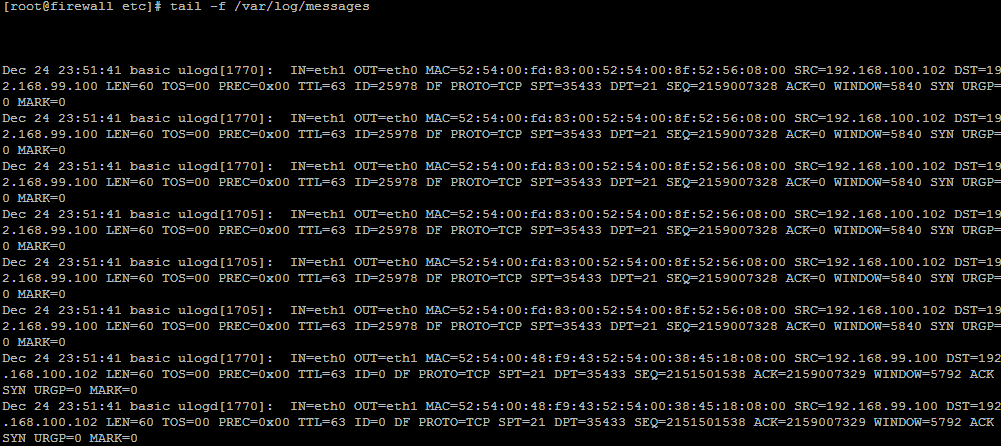
http://10.144.53.6/api/attachment?type=courseDocument&id=4912

在防火墙上

#tail –f /var/log/messages

在服务器里

#ftp 192.168.99.100



按CTRL+C 可以停止

下面我们实现只记录被拒绝的数据包

在防火墙上，我们设计如下的场景

1）  不允许内网ftp 访问外网

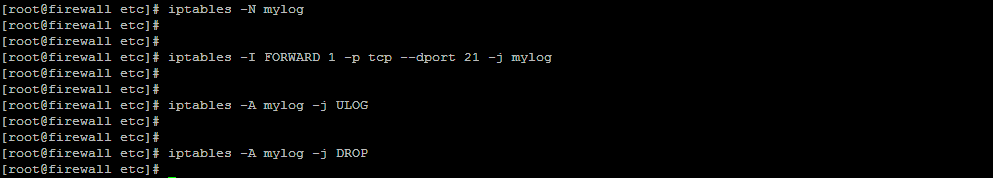
2）  记录被拒绝的ftp 访问

#iptables –N mylog

#iptables –I FORWARD 1 –p tcp –dport 21 –j mylog

#iptables –A mylog –j ULOG

#iptables –A mylog –j DROP



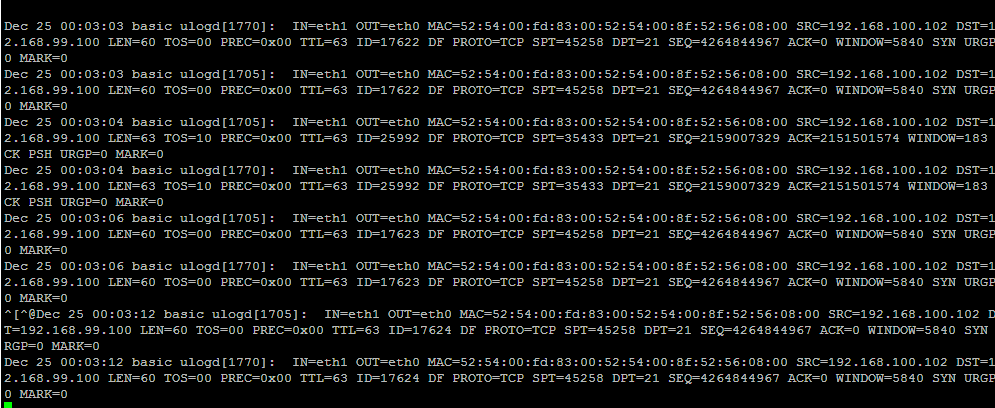
在防火墙

#tail –f /var/log/messages

在内网

#ftp 192.168.99.100

回到防火墙



按CTRL+C 可以终止

5、  实验完毕，关闭实验窗口和网络拓扑图。