|  |
| --- |
| 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主机  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  http://10.144.53.6/api/attachment?type=courseDocument&id=4723  第二步、启动系统并修改ip 地址  启动client(密码123456)  http://10.144.53.6/api/attachment?type=courseDocument&id=4728  修改eth0 的地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4733  地址生效  service  network restart  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4743  启动服务器  http://10.144.53.6/api/attachment?type=courseDocument&id=4736  修改地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4739  修改生效  http://10.144.53.6/api/attachment?type=courseDocument&id=4730  第三步、 启动防火墙  http://10.144.53.6/api/attachment?type=courseDocument&id=4725  查看防火墙地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4731  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=4719  从防火墙到客户端是通的  ping 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=4713  第四步、 客户端ping 防火墙  http://10.144.53.6/api/attachment?type=courseDocument&id=4734  客户端ping 防火墙的eth1 接口  http://10.144.53.6/api/attachment?type=courseDocument&id=4729  route add default gw 192.168.99.101  http://10.144.53.6/api/attachment?type=courseDocument&id=4722  ping 192.168.100.101  http://10.144.53.6/api/attachment?type=courseDocument&id=4717  Ping 防火墙后面的服务器地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4715  如果需要防火墙后面的数据包能返回，必须  1）  给服务器增加返回的路由  http://10.144.53.6/api/attachment?type=courseDocument&id=4741  2）  防火墙增加转发功能  http://10.144.53.6/api/attachment?type=courseDocument&id=4720  然后再客户端ping 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=4716  发现不通  然后再到防火墙上，查看防火墙的缺省规则  iptables -L  http://10.144.53.6/api/attachment?type=courseDocument&id=4724  发现转发被禁止  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 --icmp-type echo-request  –j ACCEPT  然后在客户端ping 服务端  ping 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=4732  这是因为:icmp-type echo-reply 没有被允许转发  这时,可以增加一条状态检测的规则,  #iptables –I FORWARD 2 –m state --state RELATED,ESTABLISHED –j ACCEPT  再在客户端ping 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=4718  第五步、 配置服务器端,允许提供ftp 服务  #iptables –N test  http://10.144.53.6/api/attachment?type=courseDocument&id=4727  #iptables –A test –p tcp --dport 21 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=4744  在这里,我们只配置了对服务器的dport 21 端口的访问,为何能够访问到  #iptables –I  INPUT 4 –j test  http://10.144.53.6/api/attachment?type=courseDocument&id=4726  第六步、 配置防火墙的端口映射规则  #iptables –t nat –A PREROUTING  –d 192.168.99.101 –p tcp --dport 21  –j DNAT –to 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=4746  这时在客户端访问外网口的21 端口.发现不通  http://10.144.53.6/api/attachment?type=courseDocument&id=4745  原来是同时需要增加允许防护墙对21端口的转发  #ipta bles –N myforward  #iptables –I FORWARD 3 –j myforward  #iptables –A myforward –p tcp --dport 21 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=4721  http://10.144.53.6/api/attachment?type=courseDocument&id=4714  这时在客户端ftp访问192.168.99.101  http://10.144.53.6/api/attachment?type=courseDocument&id=4735  发现依旧不能访问.  这时因为转发只增加了对目的端口是21的访问,回来的数据没能转发  由于linux 的netfilter 防火墙是支持 状态检测的,所以可以增加以下一条规则  # iptables –A myforward –m state –state RELATED,ESTABLISHED –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=4740  这时在客户端访问外网地址  http://10.144.53.6/api/attachment?type=courseDocument&id=4737  则能够访问  在防火墙上查看转发规则  #iptables –L FORWARD  在防火墙上查看转发规则  #iptables –L FORWARD  http://10.144.53.6/api/attachment?type=courseDocument&id=4738  #iptables –L  myforward  http://10.144.53.6/api/attachment?type=courseDocument&id=4742  #iptables –t nat -L  http://10.144.53.6/api/attachment?type=courseDocument&id=4747  第七步、实验完毕，关闭实验窗口和网络拓扑图。 |
|