|  |  |
| --- | --- |
| 实验步骤： | 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  http://10.144.53.6/api/attachment?type=courseDocument&id=8131  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=8148  修改eth0 的地址  http://10.144.53.6/api/attachment?type=courseDocument&id=8116  地址生效  service  network restart  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=8132  启动服务器server  http://10.144.53.6/api/attachment?type=courseDocument&id=8141  修改地址  http://10.144.53.6/api/attachment?type=courseDocument&id=8145  修改生效  http://10.144.53.6/api/attachment?type=courseDocument&id=8118  第三步、启动防火墙n\_fw  http://10.144.53.6/api/attachment?type=courseDocument&id=8142  查看防火墙地址  http://10.144.53.6/api/attachment?type=courseDocument&id=8129  ping 192.168.99.100  http://10.144.53.6/api/attachment?type=courseDocument&id=8134  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=8136  第四步、客户端ping 防火墙  http://10.144.53.6/api/attachment?type=courseDocument&id=8117  客户端ping 防火墙的eth1 接口  http://10.144.53.6/api/attachment?type=courseDocument&id=8128  route add default gw 192.168.99.101  http://10.144.53.6/api/attachment?type=courseDocument&id=8138  ping 192.168.100.101  http://10.144.53.6/api/attachment?type=courseDocument&id=8124  Ping 防火墙后面的服务器地址  http://10.144.53.6/api/attachment?type=courseDocument&id=8126  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=8139  2）  防火墙增加转发功能  http://10.144.53.6/api/attachment?type=courseDocument&id=8122  然后再客户端ping 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=8127  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=8144  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  –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=8119  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=8130  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=8140  #iptables –A test –p tcp --dport 21 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=8137  #iptables –I  INPUT 4 –j test  http://10.144.53.6/api/attachment?type=courseDocument&id=8133  第六步、配置防火墙的地址映射规则  #iptables –t nat –A PREROUTING –d 192.168.99.101 –j DNAT --to-destination 192.168.100.102  http://10.144.53.6/api/attachment?type=courseDocument&id=8121  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=8143  原来是同时需要增加允许防护墙对21端口的转发  #iptables –N myforward  #iptables –I FORWARD 2 –j myforward  #iptables –A myforward –p tcp --dport 21 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=8135  同时需要配置防火墙允许转发对 21端口的防问  这时在客户端ftp访问192.168.99.101  http://10.144.53.6/api/attachment?type=courseDocument&id=8149  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  因此,需要增加  # iptables –A myforward –p tcp --sport 21 –j ACCEPT  http://10.144.53.6/api/attachment?type=courseDocument&id=8125  这时在客户端访问外网地址  http://10.144.53.6/api/attachment?type=courseDocument&id=8123  则能够访问  在防火墙上查看转发规则  #iptables –L FORWARD  http://10.144.53.6/api/attachment?type=courseDocument&id=8120  #iptables –L  myforward  http://10.144.53.6/api/attachment?type=courseDocument&id=8146  #iptables –t nat –L  http://10.144.53.6/api/attachment?type=courseDocument&id=8147  第七步、实验完毕，关闭实验窗口和网络拓扑图。 |
|  |