Linux系统上Iptables实现端口转发的过程 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/278/2021_2022_Linux_E7_B3_BB_E7_BB_c103_278491.htm 看了不少关于用Iptables实现端口转发的文章,但感觉都没有把问题说得很清楚,现接合我自己设置和使用的经历,谈谈它的实现过程. 设我们有一台计算机,有两块网卡,eth0连外网,ip为1.2.3.4.eth1连内网,ip为192.168.0.1.现在需要把发往地址1.2.3.4的81端口的ip包转发到ip地址192.168.0.2的8180端口,设置如下: 1. Iptables -t nat -A PREROUTING -d 1.2.3.4 -p tcp -m tcp --dport 81 -j DNAT --to-destination192.168.0.2:8180 2. Iptables -t nat -A POSTROUTING -s 192.168.0.0/255.255.0.0 -d 192.168.0.2 -p tcp -m tcp --dport 8180 -j SNAT --to-source 192.168.0.1 真实的传输过程如下所示: 假设某客户机的ip地址为6.7.8.9,它使用本机的1080端口连接1.2.3.4的81端口,发出的ip包源地址为6.7.8.9,源端口为1080,目的地址为1.2.3.4,目的端口为81. 主机1.2.3.4接收到这个包后,根据nat表的第一条规则,将该ip包的目的地址更该为192.168.0.2,目的端口更该为8180,同时在连接跟踪表中创建一个条目,(可从/proc/net/ip_conntrack文件中看到),然后发送到路由模块,通过查路由表,确定该ip包应发送到eth1接口.在向eth1接口发送该ip包之前,根据nat表的第二条规则,如果该ip包来自同一子网,则将该ip包的源地址更该为 192.168.0.1,同时更新该连接跟踪表中的相应条目,然后送到eth1接口发出. 此时连接跟踪表中有一项: 连接进入: src=6.7.8.9 dst=1.2.3.4 sport=1080 dport=81 连接返回: src=192.168.0.2 dst=6.7.8.9 sport=8180 dport=1080 是否使用: use=1 而从192.168.0.2发回

的ip包,源端口为8180,目的地址为6.7.8.9,目的端口为1080,主机1.2.3.4的TCP/IP栈接收到该ip包后,由核心查找连接跟踪表中的连接返回栏目中是否有同样源和目的地址和端口的匹配项,找到后,根据条目中的记录将ip包的源地址由 192.168.0.2更该为1.2.3.4, 源端口由8180更该为81,保持目的端口号1080不变.这样服务器的返回包就可以正确的返回发起连接的客户机,通讯就这样开始. 还有一点, 在filter表中还应该允许从eth0连接192.168.0.2地址的8180端口: Iptables -A INPUT -d 192.168.0.2 -p tcp -m tcp --dport 8180 -i eth0 -j ACCEPT 