Iptables-NAT

一、NAT 的作用

1. 网络地址的转换（隐藏内网主机的 IP 地址）
2. 网络地址端口的转换
3. Iptables 表中存在的链路：prerouting，output，postrouting（有的版本中还有 input）

二、NAT 表的解读

```
# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
mercku_nat_port_fw  all  --  anywhere             anywhere
mercku_nat_dmz  all  --  anywhere             anywhere

MINIUPNPD  all  --  anywhere             192.168.100.100

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere

Chain MINIUPNPD (1 references)
target     prot opt source               destination
DNAT       udp  --  anywhere             anywhere            udp dpt:36983 to:192.168.127.103:36983

Chain mercku_nat_dmz (1 references)
target     prot opt source               destination
DNAT       all  --  anywhere             192.168.100.100     to:192.168.127.100

Chain mercku_nat_port_fw (1 references)
target     prot opt source               destination
#
```

1. Chain 后面跟的都是链路的名称
2. 链路后面括号中的代表默认执行的操作
3. Traget 下方为处理动作
   (1) SNAT：源地址转换
   (2) DNAT：目标地址转换
   (3) MASQUURADE：SNAT 的加强版，适用于动态的，临时会变得 IP 上
      a. SNAT 需要指明将报文的源地址改为哪个 IP，而 MASQUERADE 则不用指定明确的 IP
      b. MASQUERADE 会动态的将报文的源地址修改为指定网卡上可用的 IP

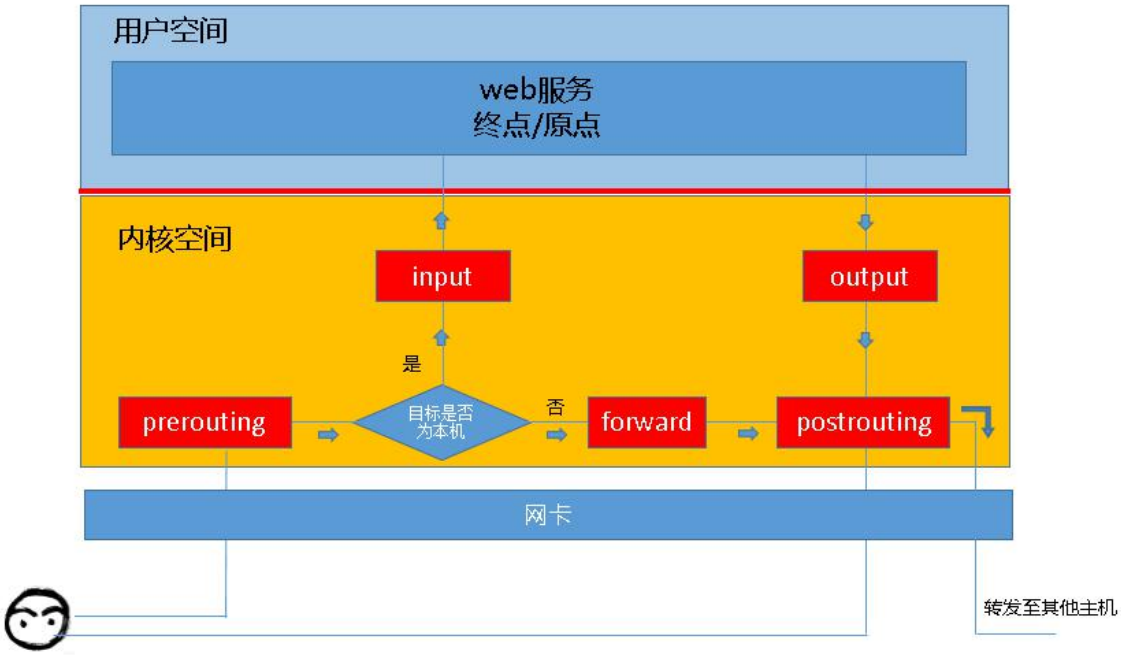
地址（如：将内网的 IP 地址动态的转化为路由器 eth1 的 IP 地址）

(4) 链路中还存在的信息有，使用的协议，源端口号和 IP，目的端口号和 IP

(5) 还有自己定义的其他链路

(6) 自己定义的链路必须被默认的链路调用才能生效

三、数据的流向



1. 数据首先经过 prerouting 链路
2. 路由器判断数据是否发送到本机
3. 到本机的数据通过 input 链路到达用户空间
4. 不是到本机的数据则通过 forward 链路和 postrouting 发送到其他主机

四、DNAT 和 SNAT 发挥作用的链路

1. DNAT 发挥作用存在于 prerouting 链路
2. SNAT 发挥作用存在于 postrouting 链路
3. DNAT 和 SNAT 的作用都是为了隐藏私网中的主机 IP

五、扩展

1. Chain MINIUPNPD 的作用就是实现点对点的传输，实现网络之间的透传（如迅雷）
2. 使用 UPNP 后，直接访问对应的端口号进行传输，不需要经过服务器。一定程度上加快传输速率