# 使用iptables配置nat服务器

## 概念：

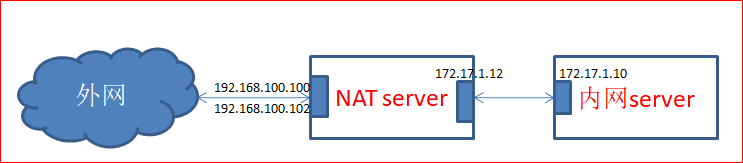
SNAT：nat服务器修改报文中的源IP地址后，将报文转发到目的地址。

DNAT：nat服务器修改报文中的目的IP地址，然后将报文转发到目的服务器

## 组网：

Nat服务器：提供两个网卡，一个接外部网络，一个接内部网络。

内网服务器：一个网卡，接内部网络。



## 要求：

内网服务器可以通过nat服务器的中转可以访问外部网络，外部网络通过nat服务器的中转可以访问内网服务器。

## 配置：

假定外部网络地址段为192.168.100.0/24，内部网络IP地址段为172.17.1.0/24

1：为内网服务器网卡配置内网IP地址172.17.1.10

2：为NAT服务器的内网网卡配置IP地址为172.17.1.12

3：为NAT服务器的外网网卡配置多个IP地址，192.168.100.100，192.168.100.102

4：为内网服务器配置默认网关，网关地址为NAT服务器内网地址

route add default gw 172.17.1.12

5：NAT服务器打开服务器路由功能

echo 1 > /proc/sys/net/ipv4/ip\_forward

6：NAT服务器上配置SNAT功能，将源地址为172.17.1.10的包源地址修改为192.168.100.100

iptables -t nat -A POSTROUTING -s 172.17.1.10  -j SNAT --to-source 192.168.100.100

7：NAT服务器上配置DNAT功能，将目的地址为192.168.100.100的报文地址修改为172.17.1.10

iptables -t nat -A PREROUTING -d 192.168.100.100 -j DNAT --to-destination 172.17.1.10