第十九章：iptables高级应用

一、SNAT源地址转换；

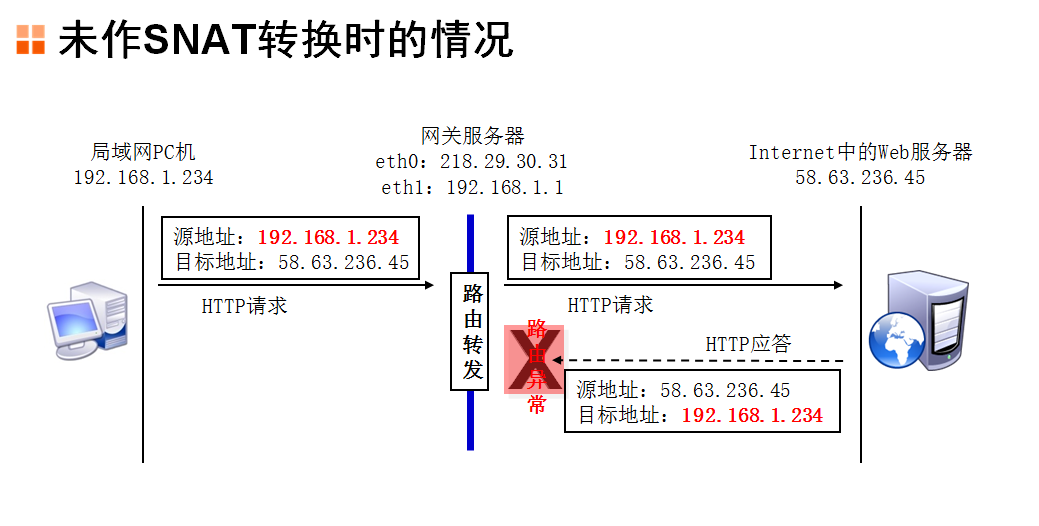
二、DNAT目的地址转换；

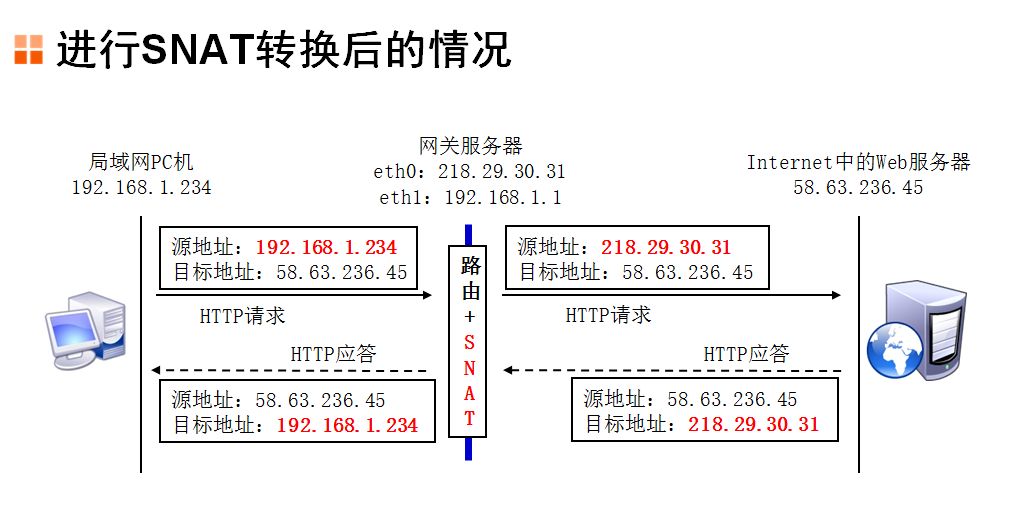
三、SNAT和DNAT实战案例；

一、SNAT源地址转换；

1.原理：在路由后链POSTROUTING将内网主机的ip地址转换成外网网卡的ip地址；

2.应用场景：共享内部主机上网，在网关主机上设置；





3.设置SNAT：

a.设置内外网网卡的网络参数；

b.开启路由转发功能；

sed -i '/ip\_forward/s/0/1/g' /etc/sysctl.conf

sysctl -p

c.编写规则；

iptables -t nat -I POSTROUTING -o 外网网卡 -s 内网的网段/24 -j SNAT --to-source 外网网卡的ip地址 ##适用于 外网ip地址固定的环境

iptables -t nat -I POSTROUTING -o 外网网卡 -s 内网的网段/24 -j MASQUERADE ##适用于网关服务器外网网卡 地址不是固定的环境

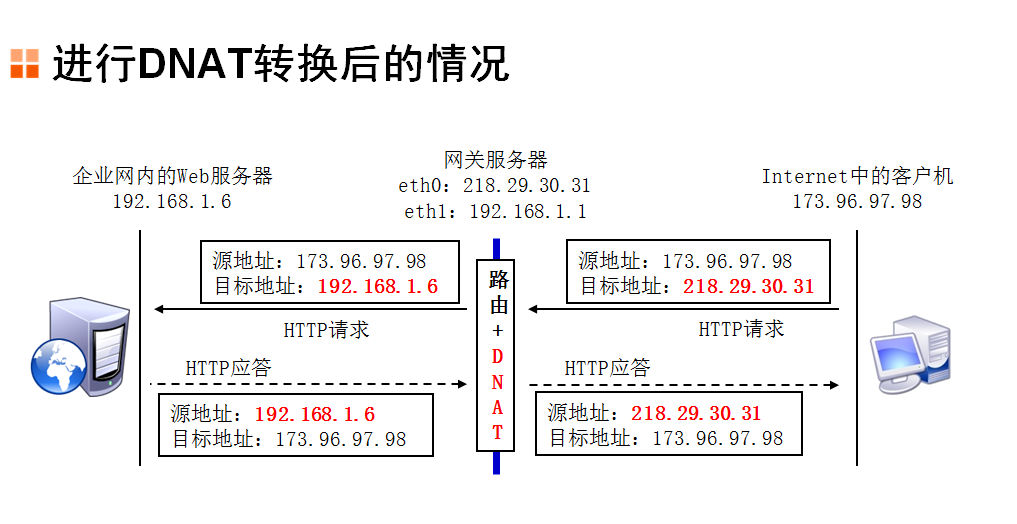
d.做好安全控制：使用FORWARD时机进行控制，严格设置INPUT规则；

e.配置客户端网关；

二、DNAT目的地址转换；

1.原理：在路由前链PREROUTING将来自外网访问网关公网ip及对应端口的目的ip及端口修改为内部服务器的ip及端口，实现发布内网服务器；

2.应用场景：发布内网主机到公网



3.设置DNAT：网关主机上设置

a.设置ip地址，开启路由，设置SNAT，保证内部主机和内部服务器可以连接公网；

b.编写防火墙规则；

iptables -t nat -I PREROUTING -i 外网网卡名 -d 外网网卡的ip地址 -p tcp --dport 发布的端口 -j DNAT --to-destination 内网服务器ip地址 ##将内网服务器发布到网关主机的外网ip地址并对应其端口，后边的端口可以省略；

c.外网客户端访问网关外网ip地址进行测试；

三、SNAT和DNAT的实战案例：

1.需求：共享公网ip上网，发布ftp和httpd服务，控制网关安全；

2.配置过程：

a.配置好ip地址等参数后，开启路由转发功能；

b.编写规则：

编写SNAT和DNAT规则：

[root@lwh ~]# /etc/init.d/iptables stop

[root@lwh ~]# iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o eth1 -j MASQUERADE

[root@lwh ~]# iptables -t nat -A PREROUTING -d 192.168.50.101 -i eth1 -p tcp -m multiport --dports 21,20,40000:45000,80,443 -j DNAT --to-destination 192.168.100.153

编辑网关安全控制规则：

[root@lwh ~]# iptables -A INPUT -i lo -j ACCEPT ##允许本地网卡访问

[root@lwh ~]# iptables -A INPUT -s 192.168.100.0/24 -i eth0 -p icmp -j ACCEPT ##允许内网ping

[root@lwh ~]# iptables -A INPUT -s 192.168.100.250 -p tcp --dport 22 -j ACCEPT ##允许主机100.250远程登陆主机

[root@lwh ~]# iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT ##允许放行主机已经建立的连接

[root@lwh ~]# iptables -A FORWARD -s 192.168.100.0/24 -j ACCEPT ##转发源地址为内网地址的流量

[root@lwh ~]# iptables -A FORWARD -d 192.168.100.0/24 -j ACCEPT ##转发目的地址为内网地址的流量

[root@lwh ~]# iptables -P INPUT DROP

[root@lwh ~]# iptables -P FORWARD DROP

d.保存规则：

[root@lwh ~]# /etc/init.d/iptables save

[root@lwh ~]# chkconfig iptables on

[root@lwh ~]# iptables-save >/root/1.txt ##将iptables规则导入到某文件中

[root@lwh ~]# iptables-restore </root/1.txt ##恢复文件中的防火墙规则