一、规则表

具有某一类相似用途的防火墙规则，按照不同处理时机区分到不同的规则链以后，被归置到不同的“表”中规则表是规则链的集合

默认4种规则表

raw表：是自1.2.9以后版本的iptables新增的表.debug测试，确认是否对该数据包进行状态跟踪.包含两个链.对应的内核模块为iptable\_raw

mangle表：主要用于修改数据包的TOS(Type Of Service，服务类型)、TTL(Time ToLive，生存周期)值以及为数据包设置Mark标记，以实现Qos (Quality of Service,服务质量)调整以及策略路由等应用，由于需要相应的路由设备支持，因此应用并不广泛。对应的内核模块为iptable\_mangle.包含五个链.

nat表：(Network Address Translation，网络地址转换)主要用于修改数据包的IP地址、端口号等信息。修改数据包中源地址和目标ip地址或端口，这是我们要学的重点，在nat表中定义的有prerouting\postrouting\output 三个规则链.内核模块为iptable nat

filer表：对数据包进行过滤,准许什么数据包通过,不许什么数据包通过.并且这个规则表也是默认的.这也是重点 在filter中 有INPUT FORWARD OUTPUT三个规则链.对应的内核模块为iptable\_ filter

二、规则链

规则的作用在于对数据包进行过滤或处理，根据处理时机的不同，各种规则被组织在不同的“链”中规则链是防火墙规则/策略的集合

默认的5种规则链

INPUT：处理入站数据包，当接收到访问防火墙本机地址的数据包(入站)时，应用此链中的规则。

OUTPUT：处理出站数据包，当防火墙本机向外发送数据包(出站)时，应用此链中的规则。

FORWARD：处理转发数据包.当接收到需要通过防火墙发送给其他地址的数据包(转发)时，应用此链中的规则。

PREROUTING链:在对数据包作路由选择之前，应用此链中的规则。

POSTROUTING链:在对数据包作路由选择之后，应用此链中的规则。

三、设定规则

iptables -p INPUT DROP

iptables -p OUTPUT ACCEPT

iptables -p FORWARD DROP

1、防止外网用内网IP欺骗

iptables -t nat -A PREROUTING -i eth0 -s 10.0.0.0/8 -j DROP

iptables -t nat -A PREROUTING -i eth0 -s 172.16.0.0/12 -j DROP

iptables -t nat -A PREROUTING -i eth0 -s 192.168.0.0/16 -j DROP

查看nat规则

iptables -t nat -L

2、如果想取消上面所加的规则：

iptables -F -t nat

iptables -X -t nat

iptables -Z -t nat

3、阻止一个IP连接本机

iptables -t filter -A INPUT -s 192.168.1.5 -i eth0 -j DROP

4、查看本机的IPTABLES的所填规则

iptables -L -n

5、清除filter中所有的规则连接

iptables -F

清除filter中使用者自定义连接中的规则

iptables -X

6、保存所修改的iptables规则

/etc/rc.d/init.d/iptables save

重新启动iptables服务

service iptables restart

7、关闭不安全的端口连接本机

iptables -A OUTPUT -p tcp --sport 31337 -j DROP

iptables -A OUTPUT -p tcp --dport 31337 -j DROP

8、开启所需要的端口

22

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

80

iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

9、禁止一个IP或者一个IP段访问服务器端口服务

80端口

iptables -t filter -I INPUT 2 -s 192.168.5.0/24 -p tcp --dport http -j DROP

FTP端口

iptables -t filter -I INPUT 2 -s 192.168.7.9 -p tcp --dport ftp -j DROP