命令表　用来增加(-A、-I)删除(-D)修改(-R)查看(-L)规则等；
常用参数　用来指定协议(-p)、源地址(-s)、源端口(--sport)、目的地址(-d)、目的端口(--dport)、进入网卡(-i)、出去网卡(-o)等设定包信息（即什么样的包）；
用来描述要处理包的信息。 常用处理动作用 -j 来指定对包的处理(ACCEPT、DROP、REJECT、REDIRECT等)。
1. 清除所有已经存在的规则
iptables -F
2. 设定预设政策，除了 INPUT 预设为 DROP 其它为预设 ACCEPT；
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
3. 开放本机的 lo (loopback)可以自由放行；
iptables -A INPUT -i lo -j ACCEPT
4. 设定有相关的封包状态可以联机进入本机
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -nL --line-numbers 显示规则
==========
vim /etc/sysconfig/iptables

iptables -P INPUT DROP 进入服务器全部禁止
iptables -P INPUT ACCEPT 进入服务器全部允许
iptables -A INPUT -p tcp -s 127.0.0.1 -j ACCEPT 允许自己所有请求
iptables -A INPUT -p tcp -s 10.221.124.0/24 --dport 80 -j ACCEPT 增加80端口
iptables -A INPUT -p tcp -s 10.221.124.0/24 --dport 80 -j ACCEPT 删除80端口这条规则
iptables -A INPUT -p tcp --dport 22 -j ACCEPT 增加22端口
iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -j DROP 禁ping
iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -j ACCEPT 解ping
/etc/init.d/iptables save && /etc/init.d/iptables restart

/etc/init.d/iptables status --line-numbers 查看编号
iptables -D INPUT 1 删除指定编号的规则
iptables -I INPUT -s 10.0.0.0/8 -j DROP 屏蔽10.*.*.*
iptables -I INPUT -s 10.204.0.0/16 -j DROP 屏蔽10.204.*.*
iptables -I INPUT -s 10.204.237.0/24 -j DROP 屏蔽10.204.237.*

iptables -A INPUT -p tcp -s 10.0.0.0/8 --dport 3306 -j ACCEPT 先允许后屏蔽
iptables -A INPUT -p tcp --dport 3306 -j DROP 屏蔽3306端口
==========领团-web==========
iptables -I INPUT -s 14.17.0.0/16 -j DROP
iptables -I INPUT -s 101.226.0.0/16 -j DROP
iptables -I INPUT -s 112.64.235.0/24 -j DROP
iptables -I INPUT -s 112.64.193.0/24 -j DROP
iptables -I INPUT -s 112.90.11.0/24 -j DROP

iptables -I INPUT -s 112.90.78.0/24 -j DROP
iptables -I INPUT -s 113.105.95.0/24 -j DROP
iptables -I INPUT -s 113.108.0.0/16 -j DROP
iptables -I INPUT -s 163.177.69.0/24 -j DROP
iptables -I INPUT -s 180.153.0.0/16 -j DROP
iptables -I INPUT -s 183.60.0.0/16 -j DROP
iptables -I INPUT -s 157.55.0.0/16 -j DROP
iptables -I INPUT -s 207.46.0.0/16 -j DROP
==========

/etc/init.d/iptables save
/etc/init.d/iptables restart