**[centos 防火墙设置](https://www.cnblogs.com/bugs/p/3587915.html)**

**1、安装iptables防火墙**怎么知道系统是否安装了iptables?执行iptables -V，如果显示如：   
iptables v1.3.5   
说明已经安装了iptables。   
如果没有安装iptables需要先安装，执行：   
yum install iptables   
在Linux中设置防火墙，以CentOS为例，打开iptables的配置文件：   
vi /etc/sysconfig/iptables   
通过/etc/init.d/iptables status命令查询是否有打开80端口，如果没有可通过两种方式处理：   
1.修改vi /etc/sysconfig/iptables命令添加使防火墙开放80端口   
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT   
2.关闭/开启/重启防火墙   
/etc/init.d/iptables stop #start 开启 #restart 重启   
3.永久性关闭防火墙   
chkconfig --level 35 iptables off /etc/init.d/iptables stop iptables -P INPUT DROP   
4.打开主动模式21端口   
iptables -A INPUT -p tcp --dport 21 -j ACCEPT   
5.打开被动模式49152~65534之间的端口   
iptables -A INPUT -p tcp --dport 49152:65534 -j ACCEPT   
iptables -A INPUT -i lo -j ACCEPT   
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT   
全部修改完之后重启iptables:   
service iptables restart   
你可以验证一下是否规则都已经生效：   
iptables -L   
通过文章的介绍，我们清楚的知道了CentOS下配置iptables防火墙的过程，希望大家都能掌握它！   
**2、清除已有iptables规则**iptables -F 清除预设表filter中的所有规则链的规则   
iptables -X 清除预设表filter中使用者自定链中的规则   
iptables -Z   
**3、开放指定的端口**#允许本地回环接口(即运行本机访问本机)   
iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT   
# 允许已建立的或相关连的通行   
iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT   
#允许所有本机向外的访问   
iptables -A OUTPUT -j ACCEPT   
# 允许访问22端口   
iptables -A INPUT -p tcp –dport 22 -j ACCEPT   
#允许访问80端口   
iptables -A INPUT -p tcp –dport 80 -j ACCEPT   
#允许FTP服务的21和20端口   
iptables -A INPUT -p tcp –dport 21 -j ACCEPT   
iptables -A INPUT -p tcp –dport 20 -j ACCEPT   
#如果有其他端口的话，规则也类似，稍微修改上述语句就行   
#禁止其他未允许的规则访问   
iptables -A INPUT -j REJECT （注意：如果22端口未加入允许规则，SSH链接会直接断开。）   
iptables -A FORWARD -j REJECT   
执行完后，这些配置就像用命令配置IP一样,重起就会失去作用。必须执行以下命令进行保存。   
/etc/rc.d/init.d/iptables save   
**4、屏蔽IP**#如果只是想屏蔽IP的话“3、开放指定的端口”可以直接跳过。   
#屏蔽单个IP的命令是   
iptables -I INPUT -s 123.45.6.7 -j DROP   
#封整个段即从123.0.0.1到123.255.255.254的命令   
iptables -I INPUT -s 123.0.0.0/8 -j DROP   
#封IP段即从123.45.0.1到123.45.255.254的命令   
iptables -I INPUT -s 124.45.0.0/16 -j DROP   
#封IP段即从123.45.6.1到123.45.6.254的命令是   
iptables -I INPUT -s 123.45.6.0/24 -j DROP   
**5、查看已添加的iptables规则**iptables -L -n   
v：显示详细信息，包括每条规则的匹配包数量和匹配字节数   
x：在 v 的基础上，禁止自动单位换算（K、M）   
n：只显示IP地址和端口号，不将ip解析为域名   
**6、删除已添加的iptables规则**将所有iptables以序号标记显示，执行：   
iptables -L -n –line-numbers   
比如要删除INPUT里序号为8的规则，执行：   
iptables -D INPUT 8   
**7、iptables的开机启动及规则保存**CentOS上可能会存在安装好iptables后，iptables并不开机自启动，可以执行一下：   
chkconfig –level 345 iptables on   
将其加入开机启动。   
CentOS上可以执行：service iptables save保存规则。