**Centos 7 firewall 命令：**

查看已经开放的端口：

firewall-cmd --list-ports

开启端口

firewall-cmd --zone=public --add-port=80/tcp --permanent

命令含义：

–zone #作用域

–add-port=80/tcp #添加端口，格式为：端口/通讯协议

–permanent #永久生效，没有此参数重启后失效

重启防火墙

firewall-cmd --reload #重启firewall

systemctl stop firewalld.service #停止firewall

systemctl disable firewalld.service #禁止firewall开机启动  
**firewall-cmd --state** #查看默认防火墙状态（关闭后显示notrunning，开启后显示running）

**CentOS 7 以下版本 iptables 命令**

如要开放80，22，8080 端口，输入以下命令即可

/sbin/iptables -I INPUT -p tcp --dport 80 -j ACCEPT

/sbin/iptables -I INPUT -p tcp --dport 22 -j ACCEPT

/sbin/iptables -I INPUT -p tcp --dport 8080 -j ACCEPT

然后保存：

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

查看打开的端口：

/etc/init.d/iptables status

关闭防火墙   
1） 永久性生效，重启后不会复原

开启： chkconfig iptables on

关闭： chkconfig iptables off

2） 即时生效，重启后复原

开启： service iptables start

关闭： service iptables stop

查看防火墙状态： service iptables status

**下面说下CentOS7和6的默认防火墙的区别**

CentOS 7默认使用的是firewall作为防火墙，使用iptables必须重新设置一下

1、直接关闭防火墙

systemctl stop firewalld.service #停止firewall

systemctl disable firewalld.service #禁止firewall开机启动

2、设置 iptables service

yum -y install iptables-services

如果要修改防火墙配置，如增加防火墙端口3306

vi /etc/sysconfig/iptables

增加规则

-A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT

保存退出后

systemctl restart iptables.service #重启防火墙使配置生效

systemctl enable iptables.service #设置防火墙开机启动

最后重启系统使设置生效即可。

systemctl start iptables.service #打开防火墙

systemctl stop iptables.service #关闭防火墙

**解决主机不能访问虚拟机CentOS中的站点**

前阵子在虚拟机上装好了CentOS6.2，并配好了apache+php+mysql，但是本机就是无法访问。一直就没去折腾了。

具体情况如下

1. 本机能ping通虚拟机

2. 虚拟机也能ping通本机

3.虚拟机能访问自己的web

4.本机无法访问虚拟机的web

后来发现是**防火墙将80端口屏蔽了的缘故。**

检查是不是服务器的80端口被防火墙堵了，可以通过命令：telnet server\_ip 80 来测试。

解决方法如下：

/sbin/iptables -I INPUT -p tcp --dport 80 -j ACCEPT

然后保存：

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

重启防火墙

/etc/init.d/iptables restart

CentOS防火墙的关闭，关闭其服务即可：

查看CentOS防火墙信息：/etc/init.d/iptables status

关闭CentOS防火墙服务：/etc/init.d/iptables stop