**一、iptables**

1.打开/关闭/重启防火墙

开启防火墙(重启后永久生效)：chkconfig iptables on

关闭防火墙(重启后永久生效)：chkconfig iptables off

开启防火墙(即时生效，重启后失效)：service iptables start

关闭防火墙(即时生效，重启后失效)：service iptables stop

重启防火墙:service iptables restartd

2.查看打开的端口

/etc/init.d/iptables status

3.打开某个端口(以8080为例)

（1）开启端口

iptables -A INPUT -p tcp --dport 8080 -j ACCEPT

（2）保存并重启防火墙

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

/etc/init.d/iptables restart

4.打开49152~65534之间的端口

iptables -A INPUT -p tcp --dport 49152:65534 -j ACCEPT

同样，这里需要对设置进行保存，并重启防火墙。

5.其他打开方式

我们还可以通过修改/etc/sysconfig/iptables文件的方式开启端口，如下

vi /etc/sysconfig/iptables

然后在文件中增加一行

-A RH-Firewall-1-INPUT -m state –state NEW -m tcp -p tcp –dport 8080 -j ACCEPT

参数说明:

–A 参数就看成是添加一条规则  
–p 指定是什么协议，我们常用的tcp 协议，当然也有udp，例如53端口的DNS  
–dport 就是目标端口，当数据从外部进入服务器为目标端口  
–sport 数据从服务器出去，则为数据源端口使用  
–j 就是指定是 ACCEPT -接收 或者 DROP 不接收

**二、firewalld**

Centos7默认安装了firewalld，如果没有安装的话，可以使用 yum install firewalld firewalld-config进行安装。

1.启动防火墙

systemctl start firewalld

2.禁用防火墙

systemctl stop firewalld

3.设置开机启动

systemctl enable firewalld

4.停止并禁用开机启动

sytemctl disable firewalld

5.重启防火墙

firewall-cmd --reload

6.查看状态

systemctl status firewalld或者 firewall-cmd --state

7.查看版本

firewall-cmd --version

8.查看帮助

firewall-cmd --help

9.查看区域信息

firewall-cmd --get-active-zones

10.查看指定接口所属区域信息

firewall-cmd --get-zone-of-interface=eth0

11.拒绝所有包

firewall-cmd --panic-on

12.取消拒绝状态

firewall-cmd --panic-off

13.查看是否拒绝

firewall-cmd --query-panic

14.将接口添加到区域(默认接口都在public)

firewall-cmd --zone=public --add-interface=eth0(永久生效再加上 --permanent 然后reload防火墙)

15.设置默认接口区域

firewall-cmd --set-default-zone=public(立即生效，无需重启)

16.更新防火墙规则

firewall-cmd --reload或firewall-cmd --complete-reload(两者的区别就是第一个无需断开连接，就是firewalld特性之一动态

添加规则，第二个需要断开连接，类似重启服务)

17.查看指定区域所有打开的端口

firewall-cmd --zone=public --list-ports

18.在指定区域打开端口（记得重启防火墙）

firewall-cmd --zone=public --add-port=80/tcp(永久生效再加上 --permanent)