# 一、防火墙的概念

防火墙技术是用于安全管理的软件和硬件设备，在计算机内/外网之间构建一道相对隔绝的保护屏障，以保护数据和信息安全性的一种技术。

防火墙分为网络防火墙和主机防火墙。

网络防火墙由软件和硬件组成，可以保护整个网络，价格也很贵，从几万到几十万的都有，功能非常强大，主要包括[入侵检测](https://baike.baidu.com/item/%E5%85%A5%E4%BE%B5%E6%A3%80%E6%B5%8B/326615)、网络地址转换、网络操作的审计监控、强化网络安全服务等功能。

主机防火墙只有软件部分（操作系统和杀毒软件自带），用于保护本操作系统，功能比较简单，只能防范简单的攻击。

本文将介绍主机防火墙（CentOS7以上版本）的使用和配置。

# 二、防火墙配置

CentOS7的防火墙比CentOS6的功能更强大，配置方法和操作命令也完全不同。

CentOS7的防火墙规则既可以是端口，也可以是服务。

防火墙查看和配置以下介绍的命令，如果没有特别说明就表示需要管理员权限执行。

## 1、查看防火墙的命令

1）查看防火墙的版本。

firewall-cmd --version

2）查看firewall的状态。

firewall-cmd --state

3）查看firewall服务状态（普通用户可执行）。

systemctl status firewalld

4）查看防火墙全部的信息。

firewall-cmd --list-all

5）查看防火墙已开通的端口。

firewall-cmd --list-port

6）查看防火墙已开通的服务。

firewall-cmd --list-service

7）查看全部的服务列表（普通用户可执行）。

firewall-cmd --get-services

8）查看防火墙服务是否开机启动。

systemctl is-enabled firewalld

## 2、配置防火墙的命令

 1）启动、重启、关闭防火墙服务。

# 启动

systemctl start firewalld

# 重启

systemctl restart firewalld

# 关闭

systemctl stop firewalld

2）开放、移去某个端口。

# 开放80端口

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

# 移去80端口

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

3）开放、移去范围端口。

# 开放5000-5500之间的端口

firewall-cmd --zone=public --add-port=5000-5500/tcp --permanent

# 移去5000-5500之间的端口

firewall-cmd --zone=public --remove-port=5000-5500/tcp --permanent

4）开放、移去服务。

# 开放ftp服务

firewall-cmd --zone=public --add-service=ftp --permanent

# 移去http服务

firewall-cmd --zone=public --remove-service=ftp --permanent

5）重新加载防火墙配置（修改配置后要重新加载防火墙配置或重启防火墙服务）。

firewall-cmd --reload

6）设置开机时启用、禁用防火墙服务。

# 启用服务

systemctl enable firewalld

# 禁用服务

systemctl disable firewalld

# 三、centos7以下版本

1）开放80，22，8080 端口。

/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

2）保存。

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

3）查看打开的端口。

/etc/init.d/iptables status

4）启动、关闭防火墙服务。

# 启动服务

service iptables start

# 关闭服务

service iptables stop

5）设置开机时启用、禁用防火墙服务。

# 启用服务

chkconfig iptables on

# 禁用服务

chkconfig iptables off

# 四、云平台访问策略配置

如果您购买的是云服务器，除了配置云服务器的防火墙，还需要登录云服务器提供商的管理平台配置访问策略（或安全组）。

不同云服务器提供商的管理平台操作方法不同，具体方法请查阅云服务器提供商的操作手册、或者百度，或者咨询云服务器提供商的客服。