官方文档地址：[https://access.redhat.com/documentation/en-US/Red\_Hat\_Enterprise\_Linux/7/html/Security\_Guide/sec-Using\_Firewalls.html#sec-Introduction\_to\_firewalld](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html" \l "sec-Introduction_to_firewalld" \t "_blank)

1、firewalld简介

firewalld是centos7的一大特性，最大的好处有两个：支持动态更新，不用重启服务；第二个就是加入了防火墙的“zone”概念

firewalld有图形界面和工具界面，由于我在服务器上使用，图形界面请参照官方文档，本文以字符界面做介绍

firewalld的字符界面管理工具是 **firewall-cmd**

firewalld默认配置文件有两个：/usr/lib/firewalld/ （系统配置，尽量不要修改）和 /etc/firewalld/ （用户配置地址）

zone概念：

硬件防火墙默认一般有三个区，firewalld引入这一概念系统默认存在以下区域（根据文档自己理解，如果有误请指正）：

drop：默认丢弃所有包

block：拒绝所有外部连接，允许内部发起的连接

public：指定外部连接可以进入

external：这个不太明白，功能上和上面相同，允许指定的外部连接

dmz：和硬件防火墙一样，受限制的公共连接可以进入

work：工作区，概念和workgoup一样，也是指定的外部连接允许

home：类似家庭组

internal：信任所有连接

对防火墙不算太熟悉，还没想明白public、external、dmz、work、home从功能上都需要自定义允许连接，具体使用上的区别还需高人指点

2、安装firewalld

root执行 **# yum install firewalld firewall-config**

3、运行、停止、禁用firewalld

启动：**# systemctl start  firewalld**

查看状态：**# systemctl status firewalld** 或者**firewall-cmd --state**

停止：**# systemctl disable firewalld**

禁用：**# systemctl stop firewalld**

4、配置firewalld

查看版本：**$ firewall-cmd --version**

查看帮助：**$ firewall-cmd --help**

查看设置：

                显示状态：**$ firewall-cmd --state**

                查看区域信息:**$ firewall-cmd --get-active-zones**

                查看指定接口所属区域：**$ firewall-cmd --get-zone-of-interface=eth0**

拒绝所有包：**# firewall-cmd --panic-on**

取消拒绝状态：**# firewall-cmd --panic-off**

查看是否拒绝：**$ firewall-cmd --query-panic**

更新防火墙规则：**# firewall-cmd --reload**

**# 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

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

设置默认接口区域

**# firewall-cmd --set-default-zone=public**

立即生效无需重启

打开端口（貌似这个才最常用）

查看所有打开的端口：

**# firewall-cmd --zone=dmz --list-ports**

加入一个端口到区域：

**# firewall-cmd --zone=dmz --add-port=8080/tcp**

若要永久生效方法同上

打开一个服务，类似于将端口可视化，服务需要在配置文件中添加，/etc/firewalld 目录下有services文件夹，这个不详细说了，详情参考文档

**# firewall-cmd --zone=work --add-service=smtp**

移除服务

**# firewall-cmd --zone=work --remove-service=smtp**