RHEL7 中使用了firewalld代替了原来的iptables，操作设置和原来有点不同：

查看防火墙状态：systemctl status firewalld

启动防火墙：systemctl start firewalld

停止防火墙：systemctl stop firewalld

防火墙中的一切都与一个或者多个区域相关联，下面对各个区进行说明：

Zone                                    Description   
-----------------------------------------------------  
drop (immutable)                 Deny all incoming connections, outgoing ones are accepted.   
block (immutable)                Deny all incoming connections, with ICMP host prohibited messages issued.   
trusted (immutable)             Allow all network connections   
public                            Public areas, do not trust other computers  
external                          For computers with masquerading enabled, protecting a local network   
dmz                               For computers publicly accessible with restricted access.    
work                              For trusted work areas   
home                              For trusted home network connections   
internal                          For internal network, restrict incoming connections  
  
drop（丢弃）  
任何接收的网络数据包都被丢弃，没有任何回复。仅能有发送出去的网络连接。  
  
block（限制）  
任何接收的网络连接都被 IPv4 的 icmp-host-prohibited 信息和 IPv6 的 icmp6-adm-prohibited 信息所拒绝。  
  
public（公共）  
在公共区域内使用，不能相信网络内的其他计算机不会对您的计算机造成危害，只能接收经过选取的连接。  
  
external（外部）  
特别是为路由器启用了伪装功能的外部网。您不能信任来自网络的其他计算，不能相信它们不会对您的计算机造成危害，只能接收经过选择的连接。  
  
dmz（非军事区）  
用于您的非军事区内的电脑，此区域内可公开访问，可以有限地进入您的内部网络，仅仅接收经过选择的连接。  
  
work（工作）  
用于工作区。您可以基本相信网络内的其他电脑不会危害您的电脑。仅仅接收经过选择的连接。  
  
home（家庭）  
用于家庭网络。您可以基本信任网络内的其他计算机不会危害您的计算机。仅仅接收经过选择的连接。  
  
internal（内部）  
用于内部网络。您可以基本上信任网络内的其他计算机不会威胁您的计算机。仅仅接受经过选择的连接。  
  
trusted（信任）  
可接受所有的网络连接。

**操作防火墙的一些常用命令：**

--显示防火墙状态  
[root@localhost zones]# firewall-cmd --state  
running  
  
  
--列出当前有几个zone  
[root@localhost zones]# firewall-cmd --get-zones  
block dmz drop external home internal public trusted work  
  
--取得当前活动的zones  
[root@localhost zones]# firewall-cmd --get-active-zones  
public  
  interfaces: ens32 veth4103622  
  
--取得默认的zone  
[root@localhost zones]# firewall-cmd --get-default-zone  
public  
  
--取得当前支持service  
[root@localhost zones]# firewall-cmd --get-service             
RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client smtp ssh telnet tftp tftp-client transmission-client vnc-server wbem-https  
  
--检查下一次重载后将激活的服务。  
[root@localhost zones]# firewall-cmd --get-service --permanent  
RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client smtp ssh telnet tftp tftp-client transmission-client vnc-server wbem-https  
  
--列出zone public 端口  
[root@localhost zones]# firewall-cmd --zone=public --list-ports  
  
--列出zone public当前设置  
[root@localhost zones]# firewall-cmd --zone=public --list-all  
public (default, active)  
  interfaces: eno16777736  
  sources:   
  services: dhcpv6-client ssh  
  ports:   
  masquerade: no  
  forward-ports:   
  icmp-blocks:   
  rich rules:

--增加zone public开放http service  
[root@localhost zones]# firewall-cmd --zone=public --add-service=http  
success  
[root@localhost zones]# firewall-cmd --permanent --zone=internal --add-service=http  
success  
  
  
--重新加载配置  
[root@localhost zones]# firewall-cmd --reload  
success  
  
  
--增加zone internal开放443/tcp协议端口  
[root@localhost zones]# firewall-cmd --zone=internal --add-port=443/tcp  
success  
  
  
--列出zone internal的所有service  
[root@localhost zones]# firewall-cmd --zone=internal --list-services  
dhcpv6-client ipp-client mdns samba-client ssh  
  
  
设置黑/白名单  
--增加172.28.129.0/24网段到zone trusted（信任）  
[root@localhost zones]# firewall-cmd --permanent --zone=trusted --add-source=172.28.129.0/24  
success  
  
  
--列出zone truste的白名单  
[root@localhost zones]# firewall-cmd --permanent --zone=trusted --list-sources  
172.28.129.0/24  
  
  
--活动的zone  
[root@localhost zones]# firewall-cmd --get-active-zones  
public  
  interfaces: eno16777736  
  
  
--添加zone truste后重新加载，然后查看--get-active-zones  
[root@localhost zones]# firewall-cmd --reload            
success  
[root@localhost zones]# firewall-cmd --get-active-zones  
public  
  interfaces: ens32 veth4103622  
trusted  
  sources: 172.28.129.0/24  
  
  
--列出zone drop所有规则  
[root@localhost zones]# firewall-cmd --zone=drop --list-all  
drop  
  interfaces:   
  sources:   
  services:   
  ports:   
  masquerade: no  
  forward-ports:   
  icmp-blocks:   
  rich rules:  
  
  
--添加172.28.13.0/24到zone drop  
[root@localhost zones]# firewall-cmd --permanent --zone=drop --add-source=172.28.13.0/24  
success  
  
  
--添加后需要重新加载  
[root@localhost zones]# firewall-cmd --reload  
success  
  
  
[root@localhost zones]# firewall-cmd --zone=drop --list-all  
drop  
  interfaces:   
  sources: 172.28.13.0/24  
  services:   
  ports:   
  masquerade: no  
  forward-ports:   
  icmp-blocks:   
  rich rules:   
  
  
[root@localhost zones]# firewall-cmd --reload  
success  
  
  
--从zone drop中删除172.28.13.0/24  
[root@localhost zones]# firewall-cmd --permanent --zone=drop --remove-source=172.28.13.0/24  
success  
  
  
--查看所有的zones规则  
[root@localhost ~]# firewall-cmd --list-all-zones

**最后再提几点：**

1、很多时候我们需要开放端口或开放某IP访问权限，我们需要先查看我们当前默认的zone是哪个，然后在对应的zone里面添加port和source，这样对外才会有作用。

     比如我当前的默认zone是public，我需要开放80端口对外访问，则执行如下命令：

     [root@localhost zones]# firewall-cmd --zone=public --permanent --add-port=80/tcp  
     success  
     [root@localhost zones]# firewall-cmd --reload  
     success

2、使用命令的时候加上 --permanent 是永久生效的意思，在重启防火墙服务后依然生效。否则，只对重启服务之前有效。

3、我们执行的命令，结果其实都体现在具体的配置文件中，其实我们可以直接修改对应的配置文件即可。

      以public zone为例，对应的配置文件是/etc/firewalld/zones/public.xml，像我们刚刚添加80端口后，体现在public.xml 中的内容为：

     [root@localhost zones]# cat public.xml  
     <?xml version="1.0" encoding="utf-8"?>  
     <zone>  
       <short>Public</short>  
       <description>For use in public areas. You do not trust the other computers on networks to not harm your computer. Only selected incoming      connections are accepted.</description>  
       <service name="dhcpv6-client"/>  
       <service name="ssh"/>  
       <port protocol="tcp" port="80"/>  
     </zone>

     这个大家可自己再进一步了解下配置文件的结构后，进行自行配置，不过记得要在配置后 --reload 或重启 firewall 服务。

-----------------------------------

（完）