# **[centos7 firewall 防火墙 命令](http://www.cnblogs.com/phpshen/p/5842118.html)**

为了架设ss在vultr上买了一个日本的vps 用的是centos7的系统 防火墙是 firewall 捣鼓了两天 在这里总结一下。

如果小伙伴也准备在vultr上买vps  在注册是 可以使用这个优惠连接   http://www.vultr.com/?ref=6972993-3B  会的到 20$ 的优惠  也就可以免费使用4个月

如果你的系统上没有安装使用命令安装

#yum install firewalld //安装firewalld 防火墙

开启服务

# systemctl start firewalld.service

关闭防火墙

# systemctl stop firewalld.service

开机自动启动

# systemctl enable firewalld.service

关闭开机制动启动

# systemctl disable firewalld.service

查看状态

#systemctl status firewalld

得到到的结果如果是

● firewalld.service - firewalld - dynamic firewall daemon  
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)  
Active: active (running) since Mon 2016-09-05 02:34:07 UTC; 15min ago  
Main PID: 3447 (firewalld)  
CGroup: /system.slice/firewalld.service  
└─3447 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Sep 05 02:34:07 vultr.guest systemd[1]: Starting firewalld - dynamic firewall daemon...  
Sep 05 02:34:07 vultr.guest systemd[1]: Started firewalld - dynamic firewall daemon.

这样的说明没有问题

设置 firwall

使用firewall-cmd 命令

查看状态

#firewall-cmd --state //running 表示运行

获取活动的区域

#firewall-cmd --get-active-zones

这条命令将用以下格式输出每个区域所含接口：

<zone1>: <interface1> <interface2> ..<zone2>: <interface3> ..

 获取所有支持的服务

#firewall-cmd --get-service

每个服务以空格分隔  例如：

RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns freeipa-ldap freeipa-ldaps freeipa-replication ftp high-availability http https imaps ipp ipp-client ipsec iscsi-target 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 rsyncd samba samba-client smtp ssh telnet tftp tftp-client transmission-client vdsm vnc-server wbem-http

获取永久选项所支持的服务   就是重启后也支出的

#firewall-cmd --get-service --permanent //在 0.3.0 之前的 FirewallD版本中, panic 选项是 –enable-panic 与 –disable-panic

开启应急模式阻断所有网络连接

#firewall-cmd --panic-on //在 0.3.0 之前的 FirewallD版本中, panic 选项是 –enable-panic 与 –disable-panic

关闭应急模式

#firewall-cmd --panic-off

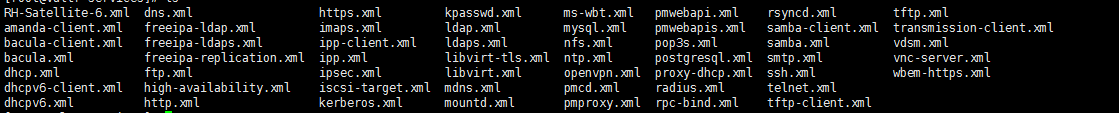
 查看应急模式的状态

#firewall-cmd --query-panic

 在不改变状态的条件下重新加载防火墙：

#firewall-cmd --reload

防火墙预定义的服务配置文件是xml文件 目录在 /usr/lib/firewalld/services/



在 /etc/firewalld/services/ 这个目录中也有配置文件    但是/etc/firewalld/services/目录 优先于 /usr/lib/firewalld/services/  目录

修改配置文件后 使用命令重新加载

#firewall-cmd --reload

启用某个服务

# firewall-cmd --zone=public --add-service=https //临时

# firewall-cmd --permanent --zone=public --add-service=https //永久

开启某个端口

#firewall-cmd --permanent --zone=public --add-port=8080-8081/tcp //永久

#firewall-cmd --zone=public --add-port=8080-8081/tcp //临时

使用命令加载设置

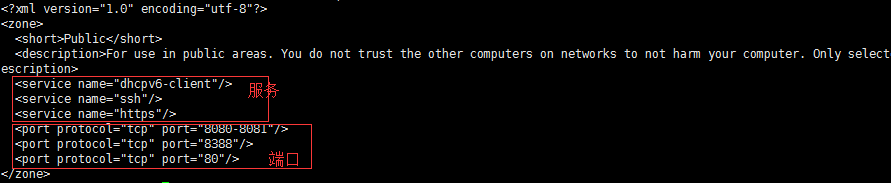
#firewall-cmd --reload

查看开启的端口和服务

#firewall-cmd --permanent --zone=public --list-services //服务空格隔开 例如 dhcpv6-client https ss

#firewall-cmd --permanent --zone=public --list-ports //端口空格隔开 例如 8080-8081/tcp 8388/tcp 80/tcp

在每次修改 端口和服务后  /etc/firewalld/zones/public.xml  文件就会被修改   所以也可以在文件中之间修改  然后重新加载

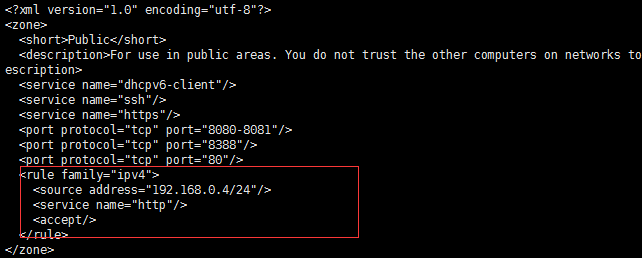


 设置某个ip 访问某个服务

#firewall-cmd --permanent --zone=public --add-rich-rule="rule family="ipv4" source address="192.168.0.4/24" service name="http" accept"

ip 192.168.0.4/24 访问 http

设置后 public.xml 就会出现变化



 删除上面设置的规则

#firewall-cmd --permanent --zone=public --remove-rich-rule="rule family="ipv4" source address="192.168.0.4/24" service name="http" accept"

启动服务

[IMG_259](http://www.cnblogs.com/phpshen/p/javascript:void(0);" \o "复制代码)

#systemctl start firewalld.service //开启服务  
#systemctl enable firewalld.service //开机制动启动  
  
#systemctl stop firewalld.service //关闭服务

#systemctl disable firewalld.service //禁止开机启动