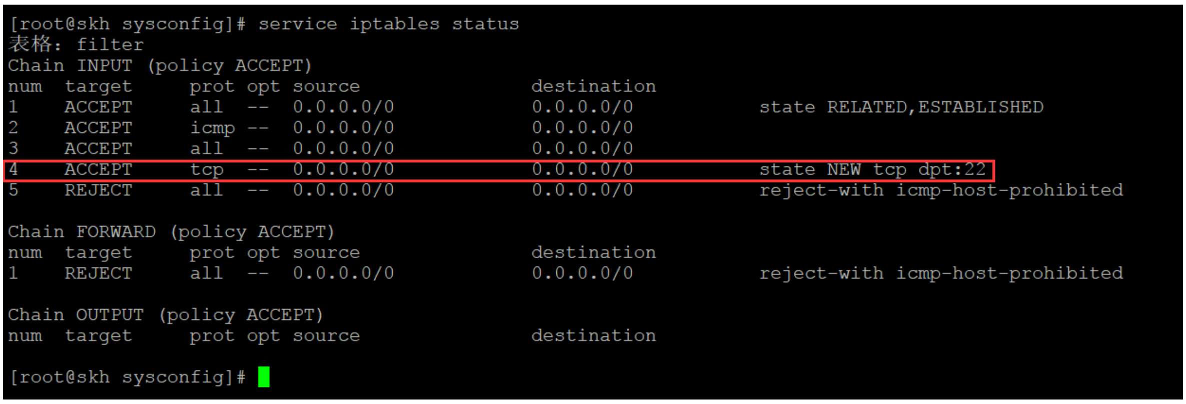
一、Centos6.8防火墙配置

1、基本操作

```
# 查看防火墙状态
service iptables status

# 停止防火墙(立即生效，开机重启,会重新打开)
service iptables stop

# 启动防火墙
service iptables start

# 重启防火墙
service iptables restart

# 永久关闭防火墙（关机重启才会生效）
chkconfig iptables off

# 永久关闭后重启
chkconfig iptables on
```

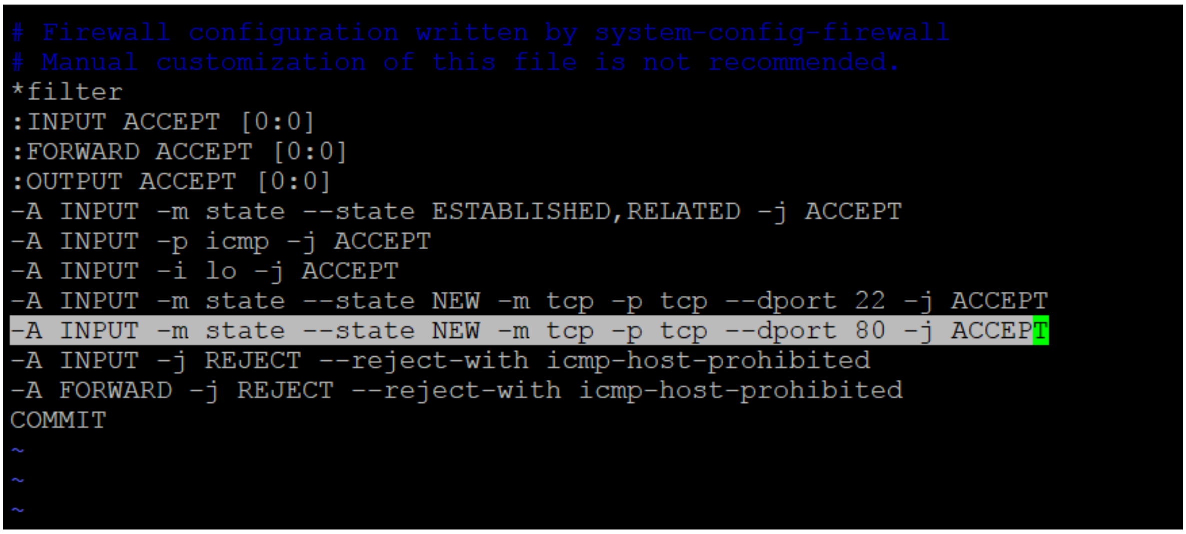
2、查看防火墙状态，防火墙处于开启状态并且只开放了22端口



```
[root@skh sysconfig]# service iptables status
表格: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
5    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

[root@skh sysconfig]#
```

3、开启80端口

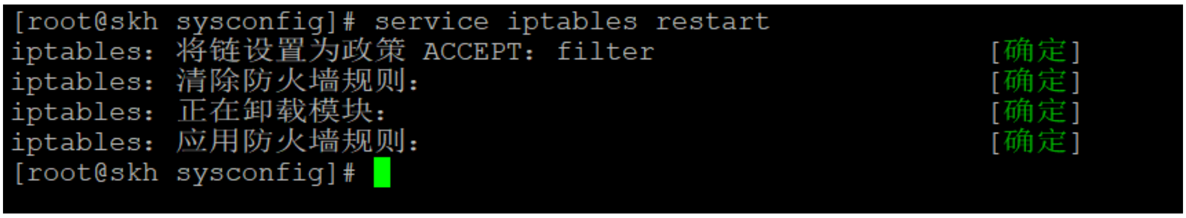
```
 vim /etc/sysconfig/iptables
# 加入如下代码，比着两葫芦画瓢 :)
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```



```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
~
~
```

4、保存退出后重启防火墙

```
service iptables restart
```



```
[root@skh sysconfig]# service iptables restart
iptables: 将链设置为政策 ACCEPT: filter                    [确定]
iptables: 清除防火墙规则:                                  [确定]
iptables: 正在卸载模块:                                    [确定]
iptables: 应用防火墙规则:                                  [确定]
[root@skh sysconfig]#
```

其他开启其他端口亦是如此。

二、Centos7以上防火墙配置

查看防火墙状态

```
firewall-cmd --state

 systemctl status firewalld
```

关闭防火墙

```
systemctl stop firewalld
```

打开防火墙

```
systemctl start firewalld
```

禁止firewall开机启动

```
systemctl disable firewalld
```

设置firewall开机自启

```
systemctl enable firewalld
```

查看开放的端口号

```
firewall-cmd --list-all #查看所有
firewall-cmd --list-ports #查看所有开放的端口
```

设置开放的端口号

```
firewall-cmd --zone=public --add-port=80/tcp --permanent #开放80端口
```

关闭端口

```
firewall-cmd --zone=public --remove-port=5672/tcp --permanent  #关闭5672端口
```

重启防火墙

```
firewall-cmd --reload # 开启或关闭端口需要重启，重启后配置立即生效
```

查看监听的端口

```
netstat -lnpt
```

检查端口被哪个进程占用

```
netstat -lnpt |grep 5672
```