



链滴

# iptables 规则脚本 - 生产环境使用

作者: [cuijianzhe](#)

原文链接: <https://ld246.com/article/1552644198015>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

## ##Centos Iptables 规则

### ####CentOS7安装iptables防火墙

CentOS7默认的防火墙不是iptables,而是firewalld.

### ####备份当前规则

```
iptables-save > iptables.rules
```

### ####禁用FireWallD, 安装和启用的iptables服务

```
systemctl stop firewalld
```

```
systemctl mask firewalld
```

```
yum install iptables-services -y
```

```
systemctl enable iptables
```

### #####先检查是否安装了iptables

```
service iptables status
```

### #####安装iptables

```
yum install -y iptables
```

### #####升级iptables

```
yum update iptables
```

### #####安装iptables-services

```
yum install iptables-services
```

### 禁用/停止自带的firewalld服务

### #####停止firewalld服务

```
systemctl stop firewalld
```

### #####禁用firewalld服务

```
systemctl mask firewalld
```

### 保存规则设定

### #####保存上述规则

```
service iptables save
```

### 注册iptables服务

### #####相当于以前的chkconfig iptables on

```
systemctl enable iptables.service
```

### #####开启服务

```
systemctl start iptables.service
```

### #####查看状态

```
systemctl status iptables.service
```

### 解决vsftpd在iptables开启后,无法使用被动模式的问题

首先在/etc/sysconfig/iptables-config中修改或者添加以下内容

### #####添加以下内容,注意顺序不能调换

```
IPTABLES_MODULES="ip_conntrack_ftp"
```

```
IPTABLES_MODULES="ip_nat_ftp"
```

### 2.重新设置iptables设置

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

### #####以下为完整设置脚本

```
#清空所有默认规则
```

```
iptables -F
```

```
iptables -t nat -F
```

```
iptables -t mangle -F
```

### #清空所有自定义规则

```
iptables -X
```

```
iptables -t nat -X
iptables -t mangle -X
```

```
#所有计数器归0
```

```
iptables -Z
iptables -A INPUT -i lo -j ACCEPT
```

```
#开放端口
```

```
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m udp -p udp --dport 21 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m udp -p udp --dport 20 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 5203 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 10050 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 10051 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 10389 -j ACCEPT ##ldap
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 389 -j ACCEPT ##ldap
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 3000 -j ACCEPT ##grafa
a
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 138 -j ACCEPT ##samba
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT ###samb

/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 137 -j ACCEPT ##samba
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT ##samba
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 514 -j ACCEPT ##syslog
/sbin/iptables -A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT ##sysl
g
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
/sbin/iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 30001:31000 -j ACCEPT
```

```
#####开启nat转发 (LDAP) , 源ip: 192.168.51.202 源端口: 10389 目的ip: 172.16.16.4 目的
口: 389
```

```
/sbin/iptables -t nat -A PREROUTING -d 192.168.51.202 -p tcp --dport 10389 -j DNAT --to-de
termination 172.16.16.4:389
/sbin/iptables -t nat -A POSTROUTING -d 172.16.16.4 -p tcp -m tcp --dport 389 -j SNAT --t
192.168.51.202
/sbin/iptables -t filter -A INPUT -p tcp -m state --state NEW -m tcp --dport 10389 -j ACCEPT
```

```
#test
```

```
#!/sbin/iptables -t nat -A PREROUTING -d 192.168.51.202 -p tcp --dport 8080 -j DNAT --to-de
termination 10.100.41.87:80
#!/sbin/iptables -t nat -A POSTROUTING -d 10.100.41.87 -p tcp -m tcp --dport 80 -j SNAT --
o 192.168.51.202
#!/sbin/iptables -t filter -A INPUT -p tcp -m state --state NEW -m tcp --dport 8080 -j ACCEPT
```

```
iptables -I FORWARD -j ACCEPT #####开启所有转发
iptables -I FORWARD -s 192.168.51.0/24 -j ACCEPT ##开启一个网段转发
```

```
#允许ping
```

```
iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
```

```
#允许接受本机请求之后的返回数据 RELATED,是为FTP设置的
```

```
/sbin/iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
#iptables -A INPUT -p tcp --dport 1024: -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_nat_ftp

#其他入站一律丢弃
iptables -P INPUT DROP
#iptables -P INPUT ACCEPT
#所有出站一律绿灯
iptables -P OUTPUT ACCEPT

#允许接受本机请求之后的返回数据 RELATED,是为FTP设置的
/sbin/iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#所有转发一律丢弃
#iptables -P FORWARD DROP

#如果要添加内网ip信任（接受其所有TCP请求）
#iptables -A INPUT -p tcp -s 45.96.174.68 -j ACCEPT

#iptables -I FORWARD -d 10.100.40.229/22 -j ACCEPT

#过滤所有非以上规则的请求
#iptables -P INPUT DROP

#要封停一个IP，使用下面这条命令：
#iptables -I INPUT -s 45.56.155.153 -j DROP

#要解封一个IP，使用下面这条命令：
#iptables -D INPUT -s *.*.*.*.*.*.*.* -j DROP

service iptables save
#centos6 重启iptables
#/etc/init.d/iptables restart
#centos7 重启iptables
systemctl restart iptables.service
/sbin/iptables -nvL
```