# iptables策略

<https://www.cnblogs.com/lixin012007/p/15769078.html>

<https://codeantenna.com/a/x02npw28oW>

<https://www.hostarr.com/iptables-basic-config/>

<https://www.fengnayun.com/news/content/62280.html>

### 实战部署

#### 删除策略:各种清零

iptables -F  
iptables -X  
iptables -Z  
iptables -F -t nat  
iptables -X -t nat  
iptables -Z -t nat

#### 允许自己 的网段及22端口通过

1 iptables -A INPUT -s 10.0.0.0/24 -j ACCEPT  
2 iptables -A INPUT -s 203.81.18.0/24 -j ACCEPT  
3 iptables -A INPUT -p tcp --dport 22 -j ACCEPT ##工作中根据自己情况，一般不用

#### 设置默认规则策略

iptables -P INPUT DROP  
iptables -P FORWARD DROP  
iptables -P OUTPUT ACCEPT

以上命令配置将接收、转发和发出分组均丢弃，施行比较严格的分组管理。由于接收和发分组均被设置为丢弃，当进一步配置其他规则的时候，需要注意针对 INPUT和OUTPUT分别配置

#### 设置其他允许

1 iptables -A INPUT -i lo -j ACCEPT #允许回环地址  
2 iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT #设置80端口转发  
3 iptables -A INPUT -s 172.16.1.0/24 -j ACCEPT   
4 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT#连接状态设置

### 保存配置

service iptables save

### 重启

systemctl restart iptables.service

### 开机自启

systemctl enable iptables.service