# 25个最常用的iptables策略

## 1、清空存在的策略

当你开始创建新的策略，你可能想清除所有的默认策略，和存在的策略，可以这么做：iptables -F 或者iptables --flush

## 2，设置默认策略

默认链策略是ACCEPT，改变所有的链策略为DROP:iptables -P INPUT DROPiptables -P FORWARD DROPiptables -P OUTPUT DROP

## 3，阻止一个指定的ip

BLOCK\_THIS\_IP=“x.x.x.x"iptables -A INPUT -s ”$BLOCK\_THIS\_IP“ -j DROPiptables -A INPUT -i eth0 -s "$BLOCK\_THIS\_IP" -j DROPiptables -A INPUT -i eth0 -p tcp -s "$BLOCK\_THIS\_IP" -j DROP

## 4，允许SSH

允许所有通过eth0接口使用ssh协议连接本机：iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

## 5，允许某个网段通过ssh连接

iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

## 6，允许http和https

允许所有进来的web流量：http协议的80端口iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT允许所有进来的web流量：https协议的443端口iptables -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

## 7，多个策略联合一起

允许ssh，http，https：iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state ESTABLISHED -j ACCEPT

## 8，允许SSH连接其他主机

iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

## 9，允许SSH连接指定的网段

iptables -A OUTPUT -o eth0 -p tcp -d 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

## 10，允许https出去

iptables -A OUTPUT -o eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A INPUT -i eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

## 11，对web请求做负载均衡(每三个包，均衡到指定服务器，需要扩展iptables)

iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every 3 --packet 0 -j DNAT --to-destination 192.168.1.101:443iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every 3 --packet 1 -j DNAT --to-destination 192.168.1.102:443iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every 3 --packet 2 -j DNAT --to-destination 192.168.1.103:443

## 12，允许ping

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPTiptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

## 13，允许ping远程

iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPTiptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

## 14，允许本地回环

iptables -A INPUT -i lo -j ACCEPTiptables -A OUTPUT -o lo -j ACCEPT

## 15，允许内网访问外部网络

这个例子eth1 连接外部网络，eth0连接内部网络iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

## 16，允许DNS出去

iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPTiptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT

## 17，允许NIS连接

NIS端口是动态的，当ypbind启动时它分配端口。首先运行 rpcinfo -p 显示得到端口号，这个例子使用端口850,853。iptables -A INPUT -p tcp --dport 111 -j ACCEPTiptables -A INPUT -p udp --dport 111 -j ACCEPTiptables -A INPUT -p tcp --dport 853 -j ACCEPTiptables -A INPUT -p udp --dport 853 -j ACCEPTiptables -A INPUT -p tcp --dport 850 -j ACCEPTiptables -A INPUT -p udp --dport 850 -j ACCEPT上面的例子当ypbind重新启动时将失效，有2种解决方案：(1)分配nis服务静态ip(2) 使用精妙的脚本

## 18，允许指定网段连接Rsync

iptables -A INPUT -i eth0 -p tcp -s 192.168.101.0/24 --dport 873 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 873 -m state --state ESTABLISHED -j ACCEPT

## 19，允许mysql从指定的网段连接

iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 3306 -m state --state ESTABLISHED -j ACCEPT

## 20，允许sendmail或者postfix

iptables -A INPUT -i eth0 -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT

## 21，允许IMAP和IMAPS

IMAP:iptables -A INPUT -i eth0 -p tcp --dport 143 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPTIMAPS:iptables -A INPUT -i eth0 -p tcp --dport 993 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 993 -m state --state ESTABLISHED -j ACCEPT

## 22，允许POP3和POP3S

POP3：iptables -A INPUT -i eth0 -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPTPOP3S：iptables -A INPUT -i eth0 -p tcp --dport 995 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 995 -m state --state ESTABLISHED -j ACCEPT

## 23，预防DOS攻击

iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT-m ： 使用iptables扩展--limit 25/minute : 限制分钟连接请求数--limit-burst：触发阀值，一次涌入数据包数量

## 24，端口转发

来自442的都转到22端口iptables -t nat -A PREROUTING -p tcp -d 192.168.102.37 --dport 422 -j DNAT --to 192.168.102.37:22你还必须明确允许442端口iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state NEW,ESTABLISHED -j ACCEPTiptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state ESTABLISHED -j ACCEPT

## 25，包丢弃日志

你也许想查看所有丢弃包的日志。首先创建一个新链叫 LOGGINGiptables -N LOGGING确保所有的连接跳到LOGGINGiptables -A INPUT -j LOGGING记录这些包通过自定义名字 "log-prefix"iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables Packet Dropped:" --log-level 7最后丢弃这些数据包iptables -A LOGGING -j DROP