|  |
| --- |
| iptables面试20道 |
| **作者：张亚**  **归档：学习笔记**  **2017/4/15** |
| **快捷键：**  Ctrl + 1 标题1  Ctrl + 2 标题2  Ctrl + 3 标题3  Ctrl + 4 实例  Ctrl + 5 程序代码  Ctrl + 6 正文 |
| **格式说明：**  蓝色字体：注释  黄色背景：重要  绿色背景：注意 |

****

**老男孩教育教学核心思想6重：重目标、重思路、重方法、重实践、重习惯、重总结**

**学无止境，老男孩教育成就你人生的起点！**

**联系方式:**

|  |  |
| --- | --- |
| **网站运维QQ交流群：** | |
| Linux 385168604 | 架构师 390642196 |
| Python 29215534 | 大数据 421358633 |
| **官方网站:** | |
| [**http://www.oldboyedu.com**](http://www.oldboyedu.com) |  |

目 录

[第1章 （一）企业面试口试题 1](#_Toc480023686)

[1、详述iptales工作流程以及规则过滤顺序？ 1](#_Toc480023687)

[2、iptables有几个表以及每个表有几个链？ 1](#_Toc480023688)

[3、iptables的几个表以及每个表对应链的作用，对应企业应用场景？ 1](#_Toc480023689)

[4、画图讲解iptables包过滤经过不同表和链简易流程图并阐述。 1](#_Toc480023690)

[5、请写出查看iptables当前所有规则的命令。 1](#_Toc480023691)

[6、禁止来自10.0.0.188 ip地址访问80端口的请求 1](#_Toc480023692)

[7、如何使在命令行执行的iptables规则永久生效？ 1](#_Toc480023693)

[8、实现把访问10.0.0.3:80的请求转到172.16.1.17:80 1](#_Toc480023694)

[9、实现172.16.1.0/24段所有主机通过124.32.54.26外网IP共享上网。 1](#_Toc480023695)

[10、描述tcp 3次握手及四次断开过程？ 1](#_Toc480023696)

[11.详细描述HTTP工作原理？ 1](#_Toc480023697)

[12.请描述iptables的常见生产应用场景。 2](#_Toc480023698)

[13、请描述下面iptables命令的作用 2](#_Toc480023699)

[14、企业WEB应用较大并发场景如何优化iptables? 2](#_Toc480023700)

[第2章 （二）企业运维经验面试题： 2](#_Toc480023701)

[15、写一个防火墙配置脚本，只允许远程主机访问本机的80端口（奇虎360面试题） 2](#_Toc480023702)

[16、请描述如何配置一个linux上网网关？ 2](#_Toc480023703)

[17、请描述如何配置一个专业的安全的WEB服务器主机防火墙？ 2](#_Toc480023704)

[18、企业实战题6：请用至少两种方法实现！ 2](#_Toc480023705)

[19、/var/log/messages日志出现kernel: nf\_conntrack: table full, dropping packet.请问是什么原因导致的？如何解决？ 3](#_Toc480023706)

[20、压轴上机实战iptables考试题  注：本试题全部摘自老男孩教育运维班课堂讲过的内容，课程不断，精彩不断，老男孩教育国内最优秀的教育机构，教学效果全国NO1。 3](#_Toc480023707)

# （一）企业面试口试题

## 1、详述iptales工作流程以及规则过滤顺序？

iptables采用数据包过滤机制工作的,他会对请求的数据包的包头数据进行分析,并根据预先设定的规则决定是否可以进入主机.

过滤顺序是层层过滤,从上到下,从前到后进行过滤.

只要匹配上就不再往下进行匹配

## 2、iptables有几个表以及每个表有几个链？

4个表

5个链

## 3、iptables的几个表以及每个表对应链的作用，对应企业应用场景？

3个表

Filter表 真正的防火墙功能

Nat表 负责数据包改写,网关共享,端口映射

Mangle表 路由相关,用的不多

5个链

INPUT 过滤进入主机的数据包

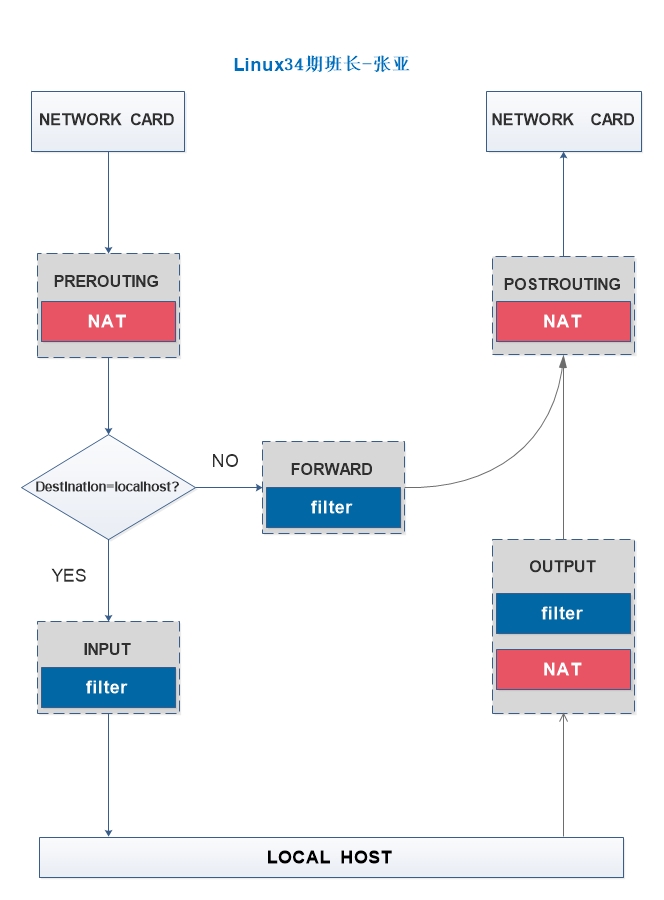
FORWARD 负责转发流经主机的数据包

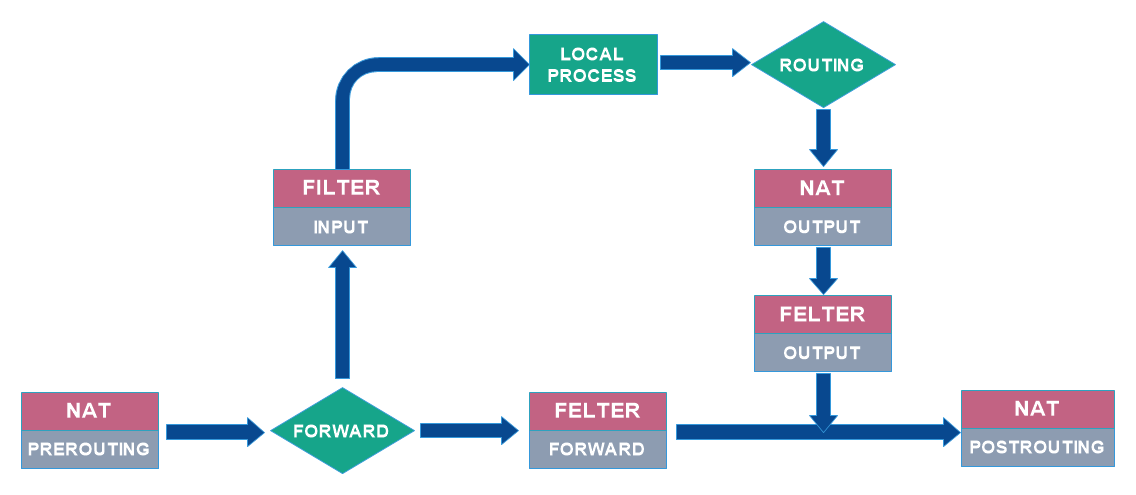
OUTPUT 处理从主机发出去的数据包

PREROUTING 数据包到达防火墙时进行路由判断之前执行的规则,适合的工作场景是端口映射

POSTROUTING 数据包离开防火墙时进行路由判断之后执行的规则,适合的工作场景是共享上网

## 4、画图讲解iptables包过滤经过不同表和链简易流程图并阐述。





说明:

1.到数据包到达防火墙的时候,首先检测有没有匹配NAT规则这里是NAT表的PREROUTING控制,如果匹配上就进入下一步,假设没有配置NAT表规则的话默认是放行的.

2.此时防火墙判断数据包是请求的地址是否为局域网内的机器,是的话就由FITER表控装的INPUT链指定的规则来匹配,如果合规,那么就交给要处理的机器.如果不合规就丢弃

3.数据包由机器处理完成之后,交给NAT表的OUTPUT链处理,如果没有配置NAT表的OUTPUT规则,默认为放行,紧接着交给FELTER表的OUTPUT链去处理.

4.经过NAT表OUTPUT链处理完成之后数据包来到了FELTER表的OUTPUT链,如果合规就放行,如果不合规就丢弃.

5.最后数据包来到了最后一个关卡,也就是NAT表的POSTROUTING链,当然如果没有配置的话默认也是全部放行.

## 5、请写出查看iptables当前所有规则的命令。

iptables -nL

iptables -nL -t nat

iptables -nL -t mangle

## 6、禁止来自10.0.0.188 ip地址访问80端口的请求

ipttables -A INPUT -p tcp -s 10.0.0.188 --dport 80 -j DROP

## 7、如何使在命令行执行的iptables规则永久生效？

/etc/init.d/iptables save

iptables-save >/etc/sysconfig/iptables

## 8、实现把访问10.0.0.5:9000的请求转到172.16.1.8:80

iptables -t nat -A PREROUTING -d 10.0.0.5 -p tcp --dport 9000 -j DNAT --to-destination 172.16.1.8:80

## 9、实现172.16.1.0/24段所有主机通过124.32.54.26外网IP共享上网。

iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -o eth0 -j SNAT --to-source 10.0.0.8

## 10、描述tcp 3次握手及四次断开过程？

（课外参考：<http://user.qzone.qq.com/49000448/blog/1426987479>）

三次握手:

第一次握手：建立连接时,客户端发送SYN（seq=x）包到服务器,并进入SYN\_SENT状态,等待服务器的确认.SYN：同步序列编号（Synchronize Sequence Numbers）。

第二次握手：服务器收到SYN包,必须确认客户的SYN（ack=x+1）,同时自己也发送一个SYN包（seq=y）,即发送SYN+ACK包,此时服务器进入SYN\_RECV状态;

第三次握手：客户端收到SYN+ACK包,向服务器发送ACK(ack=y+1）包,此包发送完毕,客户端和服务器进入ESTABLISHED状态,完成三次握手.

完成三次握手，客户端与服务器开始传送数据

四次挥手:

tcp/ip协议的四次断开的过程

注：挥手动作可由客户端或服务器任意一方发起。

　第一次挥手：客户端发送FIN+ACK包（序号为seq=a,确认序号ack=b）给服务端,用来关闭客户端到服务端的数据传送,客户端进入FIN\_WAIT\_1状态.

　第二次挥手：服务端收到FIN+ACK包后,发送ACK包给客户端进行确认,服务端进入CLOSE\_WAIT状态.客户端收到ACK包后进入FIN\_WAIT\_2状态.到这里,关闭一个单向通道.

　第三次挥手：服务端发送FIN+ACK包给客户端,服务端进入LAST\_ACK状态.

　第四次挥手：客户端收到FIN+ACK包后,发送ACK包给服务端进行确认,客户端进入TIME\_WAIT状态,在等待30秒（可修改）后进入CLOSED状态.服务端收到ACK包后进入CLOSED状态,关闭另一个单向通道.

## 11.详细描述HTTP工作原理？

## 12.请描述iptables的常见生产应用场景。

1.局域网共享上网(适合做企业内部局域网上网网关,以及IDC机房内网的上网网关)(nat POSTROUTING)

 2.服务器防火墙功能(适合IDC机房具有外网IP的服务器)(主要是filter INPUT的控制)

3.把外部IP及端口映射到局域网内部(可以一对一IP映射,也可以针对某一端口映射).也可能是IDC把网站的外网VIP及网站端口映射到负载均衡器上(硬件防火墙).(nat PREROUTING)

4.办公路由器+网关功能(zebra路由+iptables过滤及NAT+squid正向透明代理80+ntop/iftop/iptraf流量查看+tc流量控制限速)

5.邮件的网关

## 13、请描述下面iptables命令的作用

iptables -N syn-flood

iptables -A INPUT -i eth0 -syn -j syn-flood

iptables -A syn-flood -m limit -limit 5000/s -limit-burst 200 -j RETURN

iptables -A syn-flood -j DROP

## 14、企业WEB应用较大并发场景如何优化iptables?

net.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 180

net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120

net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60

net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120

# （二）企业运维经验面试题：

## 15、写一个防火墙配置脚本，只允许远程主机访问本机的80端口（奇虎360面试题）

（<http://user.qzone.qq.com/49000448/blog/1429755081>）

iptables -A INPUT --dport 80 -j ACCEPT

iptables -P INPUT DROP

## 16、请描述如何配置一个linux上网网关？

route -net 172.16.1.0/24 gw 192.168.1.1

## 17、请描述如何配置一个专业的安全的WEB服务器主机防火墙？

#首先设置允许ssh连接

iptables -F

iptables -X

iptables -Z

iptables -A INPUT -p tcp -s 10.0.0.0/24 --dport 22 -j ACCEPT

iptables -P INPUT DROP

iptables -nL

#设置允许本机lo通信规则

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

#修改默认规则

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

#开启信任网段

iptables -A INPUT -s 124.43.62.96/27 -p all -j ACCEPT <---办公室固定IP段

iptables -A INPUT -s 192.168.1.0/24 -p all -j ACCEPT <---IDC机房的内网网段

iptables -A INPUT -s 10.0.0.0/24 -p all -j ACCEPT <---其他机房的内网网段

iptables -A INPUT -s 203.83.24.0/24 -p all -j ACCEPT <---IDC机房的外网网段

iptables -A INPUT -s 201.82.34.0/24 -p all -j ACCEPT <---其他IDC机房的外网网段

#允许业务服务端口对外访问(允许http服务无条件通过)

iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT

#允许icmp类型协议通过

iptables -A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT

提示:如果不想开,就不执行此命令

如果对内开,对外不开就用下面的方式

iptables -A INPUT -p icmp -s 10.0.0.0/24 -m icmp --icmp-type any -j ACCEPT

#允许关联的状态包通过(web服务不要使用FTP服务)

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

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

##查看最终结果

[root@nginx-8 ~]# iptables -nL

Chain INPUT (policy DROP)

target prot opt source destination

ACCEPT tcp -- 10.0.0.0/24 0.0.0.0/0

ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22

ACCEPT all -- 0.0.0.0/0 0.0.0.0/0

ACCEPT all -- 124.43.62.96/27 0.0.0.0/0

ACCEPT all -- 192.168.1.0/24 0.0.0.0/0

ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:80

ACCEPT icmp -- 10.0.0.0/24 0.0.0.0/0 icmp type 255

Chain FORWARD (policy DROP)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- 0.0.0.0/0 0.0.0.0/0

ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED

#将iptables临时配置保存为配置文件的方法

[root@nginx-8 ~]# /etc/init.d/iptables save

iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]

## 18、企业实战题6：请用至少两种方法实现！

写一个脚本解决DOS攻击生产案例

提示：根据web日志或者或者网络连接数，监控当某个IP并发连接数或者短时内PV达到100，即调用防火墙命令封掉对应的IP，监控频率每隔3分钟。防火墙命令为：iptables -A INPUT -s 10.0.1.10 -j DROP。

（此题来自老男孩教育SHELL编程必会考试题之一）

#学长的脚本注释版

[root@nginx-8 ~]# cat drop\_ip3.sh

#!/bin/bash

. /etc/init.d/functions

conut=10 #访问次数的阀值，超过10次就禁止掉这个IP

Path=/server/scripts/access.log

function ipt(){ #iptables 的设置

awk '{print $1}'$Path|sort|uniq -c|sort -rn >/tmp/tmp.log #统计IP访问次数

exec < /tmp/tmp.log

while read line

do

ip=echo $line|awk '{print $2}'

if [ echo $line|awk '{print $1}' -ge $conut -a iptables -L -n|grep "$ip"|wc -l -lt 1 ]

#如果IP访问次数大于等于10并且在iptables禁止列表里没有这个IP。

then

iptables -I INPUT -s $ip -j DROP

#把这个IP写进iptables禁止列表里

RETVAL=$?

if [ $RETVAL -eq 0 ]

#如果上一条命令执行没有出错

then

action "iptables -I INPUT -s $ip -j DROP" /bin/true

echo "$ip" >>/tmp/ip\_$(date +%F).log

#把这个ip写进一个IP地址黑名单

else

action "iptables -I INPUT -s $ip -j DROP" /bin/false

fi

fi

done

}

function del(){

[ -f /tmp/ip\_$(date +%F -d '-1 day').log ]||{

#如果存在这个黑名单日志

echo "log is not exist"

exit 1}

exec </tmp/ip\_$(date +%F -d '-1 day').log

while read line

do

if [ iptables -L -n|grep "$line"|wc -l -ge 1 ]

#如果IP地址存在黑名单里

then

iptables -D INPUT -s $line -j DROP

#就把他放出来

fi

done

}

function main(){

flag=0

#计数器

while true

do

sleep 180

#180秒运行一次下面的命令

((falg++))

#每执行一次，计数器自动加上1

ipt

[ $flag -ge 480 ] && del && flag=0

#超过1天的时候，就把黑名单里的IP给放出来并且把计数器归零

done

}

main

我的脚本:

#!/bin/bash

. /etc/init.d/functions

iptables\_list=$(iptables -n -L)

count=10

path=/server/scripts/access.log

function ipt(){

awk '{print $1}' $path|sort|uniq -c|sort -rn >/tmp/tmp.log

max\_line=$(cat /tmp/tmp.log|wc -l)

for ((i=1;i<=$max\_line;i++))

do

ip=$(awk 'NR=='"$i"'{print $2}' /tmp/tmp.log)

ip\_num=$(awk 'NR=='"$i"'{print $1}' /tmp/tmp.log)

iptables\_ip\_num=$(iptables -nL|grep "$ip"|wc -l)

if [ $ip\_num -ge $count -a $iptables\_ip\_num -lt 1 ]

then

iptables -I INPUT -s $ip -j DROP

RETVAL=$?

if [ $RETVAL -eq 0 ]

then

action "iptables -I INPUT -s $ip -j DROP" /bin/true

echo "$ip" >>/tmp/ip\_$(date +%F).log

else

action "iptables -I INPUT -s $ip -j DROP" /bin/false

fi

fi

done

}

function del(){

if [ -f /tmp/ip\_$(date +%F -d '-1 day').log ]

then

cat /tmp/ip\_$(date +%F -d '-1 day').log|awk '{print "iptables -D INPUT -s "$1" -j DROP"}'|bash

else

echo "log is not exist"

fi

}

function main(){

while true

do

sleep 10

((flag++))

ipt

[ $flag -ge 480 ] && del && flag=0

done

}

main

## 19、/var/log/messages日志出现kernel: nf\_conntrack: table full, dropping packet.请问是什么原因导致的？如何解决？

解答:

有两种可能,一是打开的端口太少导致不够用,修改ip\_conntrack文件为1024 65535

还有一个原因是nat连接真的达到了65535了,此时就把NAT映射表保持时间设置短一些.

以下参数是对iptables防火墙的优化,防火墙不开会提示,可以忽略不计

net.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 180

net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120

net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60

net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120

## 20、压轴上机实战iptables考试题 图片  **注：本试题全部摘自老男孩教育运维班课堂讲过的内容，课程不断，精彩不断，老男孩教育国内最优秀的教育机构，教学效果全国NO1。**