iptables详解

来自：<https://www.cnblogs.com/metoy/p/4320813.html>

文件位于：/etc/sysconfig/iptables

# 一、iptables简介

netfilter/iptables（简称为iptables）组成Linux平台下的包过滤防火墙，与大多数的Linux软件一样，这个包过滤防火墙是免费的，它可以代替昂贵的商业防火墙解决方案，完成封包过滤、封包重定向和网络地址转换（NAT）等功能。

# 二、iptables基础

规则（rules）其实就是网络管理员预定义的条件，规则一般的定义为“如果数据包头符合这样的条件，就这样处理这个数据包”。规则存储在内核空间的信息 包过滤表中，这些规则分别指定了源地址、目的地址、传输协议（如TCP、UDP、ICMP）和服务类型（如HTTP、FTP和SMTP）等。当数据包与规 则匹配时，iptables就根据规则所定义的方法来处理这些数据包，如放行（accept）、拒绝（reject）和丢弃（drop）等。配置防火墙的 主要工作就是添加、修改和删除这些规则。

# 三、iptables和netfilter的关系：

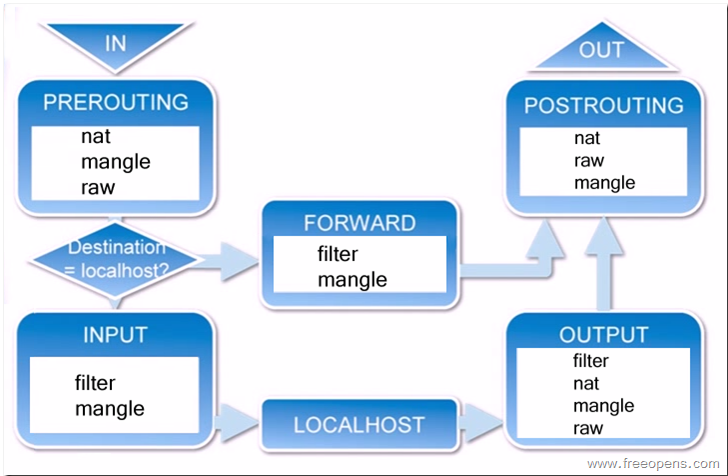
这是第一个要说的地方，Iptables和netfilter的关系是一个很容易让人搞不清的问题。很多的知道iptables却不知道 netfilter。其实iptables只是Linux防火墙的管理工具而已，位于/sbin/iptables。真正实现防火墙功能的是 netfilter，它是Linux内核中实现包过滤的内部结构。

iptables传输数据包的过程

① 当一个数据包进入网卡时，它首先进入PREROUTING链，内核根据数据包目的IP判断是否需要转送出去。

② 如果数据包就是进入本机的，它就会沿着图向下移动，到达INPUT链。数据包到了INPUT链后，任何进程都会收到它。本机上运行的程序可以发送数据包，这些数据包会经过OUTPUT链，然后到达POSTROUTING链输出。

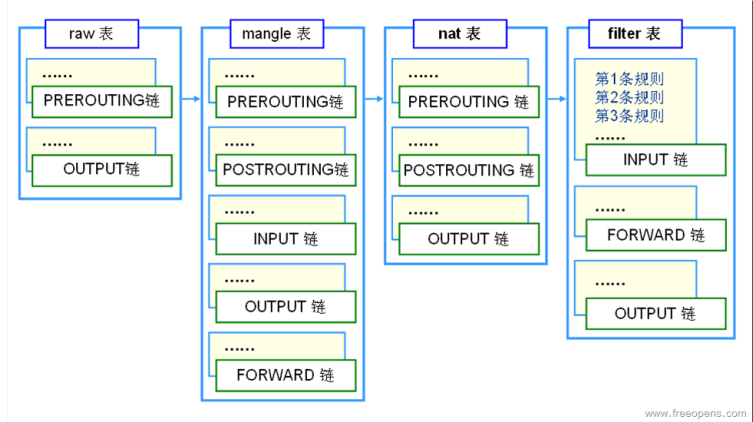
③ 如果数据包是要转发出去的，且内核允许转发，数据包就会如图所示向右移动，经过FORWARD链，然后到达POSTROUTING链输出。



# 四、iptables的规则表和链：

      表（tables）提供特定的功能，iptables内置了4个表，即filter表、nat表、mangle表和raw表，分别用于实现包过滤，网络地址转换、包重构(修改)和数据跟踪处理。

链（chains）是数据包传播的路径，每一条链其实就是众多规则中的一个检查清单，每一条链中可以有一 条或数条规则。当一个数据包到达一个链时，iptables就会从链中第一条规则开始检查，看该数据包是否满足规则所定义的条件。如果满足，系统就会根据 该条规则所定义的方法处理该数据包；否则iptables将继续检查下一条规则，如果该数据包不符合链中任一条规则，iptables就会根据该链预先定 义的默认策略来处理数据包。  
  
       Iptables采用“表”和“链”的分层结构。在REHL4中是三张表五个链。现在REHL5成了四张表五个链了，不过多出来的那个表用的也不太多，所以基本还是和以前一样。下面罗列一下这四张表和五个链。注意一定要明白这些表和链的关系及作用。



## 1、规则表：

1.filter表——三个链：INPUT、FORWARD、OUTPUT  
作用：过滤数据包  内核模块：iptables\_filter.

2.Nat表——三个链：PREROUTING、POSTROUTING、OUTPUT  
作用：用于网络地址转换（IP、端口） 内核模块：iptable\_nat

3.Mangle表——五个链：PREROUTING、POSTROUTING、INPUT、OUTPUT、FORWARD  
作用：修改数据包的服务类型、TTL、并且可以配置路由实现QOS内核模块：iptable\_mangle(别看这个表这么麻烦，咱们设置策略时几乎都不会用到它)

4.Raw表——两个链：OUTPUT、PREROUTING  
作用：决定数据包是否被状态跟踪机制处理  内核模块：iptable\_raw  
(这个是REHL4没有的，不过不用怕，用的不多)

## 2、规则链：

1.INPUT——进来的数据包应用此规则链中的策略

2.OUTPUT——外出的数据包应用此规则链中的策略

3.FORWARD——转发数据包时应用此规则链中的策略

4.PREROUTING——对数据包作路由选择前应用此链中的规则  
（记住！所有的数据包进来的时侯都先由这个链处理）

5.POSTROUTING——对数据包作路由选择后应用此链中的规则  
（所有的数据包出来的时侯都先由这个链处理）

3、规则表之间的优先顺序：

Raw——mangle——nat——filter  
规则链之间的优先顺序（分三种情况）：

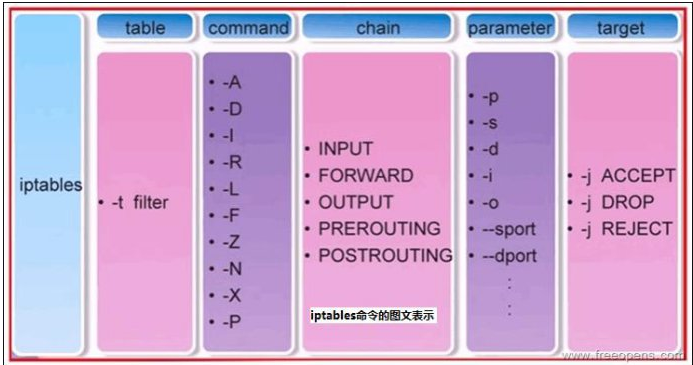
**第一种情况：入站数据流向**

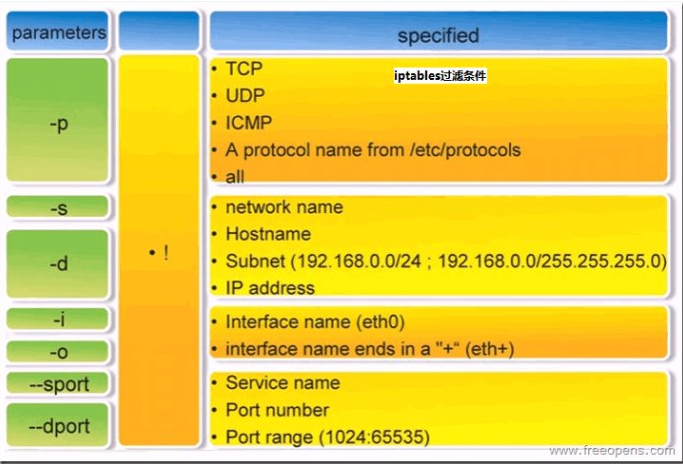
       从外界到达防火墙的数据包，先被PREROUTING规则链处理（是否修改数据包地址等），之后会进行路由选择（判断该数据包应该发往何处），如果数据包 的目标主机是防火墙本机（比如说Internet用户访问防火墙主机中的web服务器的数据包），那么内核将其传给INPUT链进行处理（决定是否允许通 过等），通过以后再交给系统上层的应用程序（比如Apache服务器）进行响应。

**第二冲情况：转发数据流向**  
       来自外界的数据包到达防火墙后，首先被PREROUTING规则链处理，之后会进行路由选择，如果数据包的目标地址是其它外部地址（比如局域网用户通过网 关访问QQ站点的数据包），则内核将其传递给FORWARD链进行处理（是否转发或拦截），然后再交给POSTROUTING规则链（是否修改数据包的地 址等）进行处理。

**第三种情况：出站数据流向**  
       防火墙本机向外部地址发送的数据包（比如在防火墙主机中测试公网DNS服务器时），首先被OUTPUT规则链处理，之后进行路由选择，然后传递给POSTROUTING规则链（是否修改数据包的地址等）进行处理。

**管理和设置iptables规则**





## 4、iptables的基本语法格式

iptables [-t 表名] 命令选项 ［链名］ ［条件匹配］ ［-j 目标动作或跳转］  
说明：表名、链名用于指定 iptables命令所操作的表和链，命令选项用于指定管理iptables规则的方式（比如：插入、增加、删除、查看等；条件匹配用于指定对符合什么样 条件的数据包进行处理；目标动作或跳转用于指定数据包的处理方式（比如允许通过、拒绝、丢弃、跳转（Jump）给其它链处理。

## 5、iptables命令的管理控制选项

-A 在指定链的末尾添加（append）一条新的规则  
-D 删除（delete）指定链中的某一条规则，可以按规则序号和内容删除  
-I 在指定链中插入（insert）一条新的规则，默认在第一行添加  
-R 修改、替换（replace）指定链中的某一条规则，可以按规则序号和内容替换  
-L 列出（list）指定链中所有的规则进行查看  
-E 重命名用户定义的链，不改变链本身  
-F 清空（flush）  
-N 新建（new-chain）一条用户自己定义的规则链  
-X 删除指定表中用户自定义的规则链（delete-chain）  
-P 设置指定链的默认策略（policy）  
-Z 将所有表的所有链的字节和数据包计数器清零  
-n 使用数字形式（numeric）显示输出结果  
-v 查看规则表详细信息（verbose）的信息  
-V 查看版本(version)  
-h 获取帮助（help）

## 6、防火墙处理数据包的四种方式

ACCEPT 允许数据包通过  
DROP 直接丢弃数据包，不给任何回应信息  
REJECT 拒绝数据包通过，必要时会给数据发送端一个响应的信息。  
LOG在/var/log/messages文件中记录日志信息，然后将数据包传递给下一条规则

## 7、iptables防火墙规则的保存与恢复

iptables-save把规则保存到文件中，再由目录rc.d下的脚本（/etc/rc.d/init.d/iptables）自动装载

使用命令iptables-save来保存规则。一般用

iptables-save > /etc/sysconfig/iptables

生成保存规则的文件 /etc/sysconfig/iptables，

也可以用

service iptables save

它能把规则自动保存在/etc/sysconfig/iptables中。

当计算机启动时，rc.d下的脚本将用命令iptables-restore调用这个文件，从而就自动恢复了规则。

**删除INPUT链的第一条规则**

iptables -D INPUT 1

**iptables防火墙常用的策略**

1.拒绝进入防火墙的所有ICMP协议数据包

iptables -I INPUT -p icmp -j REJECT

2.允许防火墙转发除ICMP协议以外的所有数据包

iptables -A FORWARD -p ! icmp -j ACCEPT

说明：使用“！”可以将条件取反。

3.拒绝转发来自192.168.1.10主机的数据，允许转发来自192.168.0.0/24网段的数据

iptables -A FORWARD -s 192.168.1.11 -j REJECT   
iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT

说明：注意要把拒绝的放在前面不然就不起作用了啊。

4.丢弃从外网接口（eth1）进入防火墙本机的源地址为私网地址的数据包

iptables -A INPUT -i eth1 -s 192.168.0.0/16 -j DROP   
iptables -A INPUT -i eth1 -s 172.16.0.0/12 -j DROP   
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP

5.封堵网段（192.168.1.0/24），两小时后解封。

# iptables -I INPUT -s 10.20.30.0/24 -j DROP   
# iptables -I FORWARD -s 10.20.30.0/24 -j DROP   
# at now 2 hours at> iptables -D INPUT 1 at> iptables -D FORWARD 1

说明：这个策略咱们借助crond计划任务来完成，就再好不过了。  
[1]   Stopped     at now 2 hours

6.只允许管理员从202.13.0.0/16网段使用SSH远程登录防火墙主机。

iptables -A INPUT -p tcp --dport 22 -s 202.13.0.0/16 -j ACCEPT   
iptables -A INPUT -p tcp --dport 22 -j DROP

说明：这个用法比较适合对设备进行远程管理时使用，比如位于分公司中的SQL服务器需要被总公司的管理员管理时。

7.允许本机开放从TCP端口20-1024提供的应用服务。

iptables -A INPUT -p tcp --dport 20:1024 -j ACCEPT   
iptables -A OUTPUT -p tcp --sport 20:1024 -j ACCEPT

8.允许转发来自192.168.0.0/24局域网段的DNS解析请求数据包。

iptables -A FORWARD -s 192.168.0.0/24 -p udp --dport 53 -j ACCEPT   
iptables -A FORWARD -d 192.168.0.0/24 -p udp --sport 53 -j ACCEPT

9.禁止其他主机ping防火墙主机，但是允许从防火墙上ping其他主机

iptables -I INPUT -p icmp --icmp-type Echo-Request -j DROP   
iptables -I INPUT -p icmp --icmp-type Echo-Reply -j ACCEPT   
iptables -I INPUT -p icmp --icmp-type destination-Unreachable -j ACCEPT

10.禁止转发来自MAC地址为00：0C：29：27：55：3F的和主机的数据包

iptables -A FORWARD -m mac --mac-source 00:0c:29:27:55:3F -j DROP

说明：iptables中使用“-m 模块关键字”的形式调用显示匹配。咱们这里用“-m mac –mac-source”来表示数据包的源MAC地址。

11.允许防火墙本机对外开放TCP端口20、21、25、110以及被动模式FTP端口1250-1280

iptables -A INPUT -p tcp -m multiport --dport 20,21,25,110,1250:1280 -j ACCEPT

说明：这里用“-m multiport –dport”来指定目的端口及范围

12.禁止转发源IP地址为192.168.1.20-192.168.1.99的TCP数据包。

iptables -A FORWARD -p tcp -m iprange --src-range 192.168.1.20-192.168.1.99 -j DROP

说明：此处用“-m –iprange –src-range”指定IP范围。

13.禁止转发与正常TCP连接无关的非—syn请求数据包。

iptables -A FORWARD -m state --state NEW -p tcp ! --syn -j DROP

说明：“-m state”表示数据包的连接状态，“NEW”表示与任何连接无关的，新的嘛！

14.拒绝访问防火墙的新数据包，但允许响应连接或与已有连接相关的数据包

iptables -A INPUT -p tcp -m state --state NEW -j DROP   
iptables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

说明：“ESTABLISHED”表示已经响应请求或者已经建立连接的数据包，“RELATED”表示与已建立的连接有相关性的，比如FTP数据连接等。

15.只开放本机的web服务（80）、FTP(20、21、20450-20480)，放行外部主机发住服务器其它端口的应答数据包，将其他入站数据包均予以丢弃处理。

[IMG_256](https://www.cnblogs.com/metoy/p/javascript:void(0);)

iptables -I INPUT -p tcp -m multiport --dport 20,21,80 -j ACCEPT   
iptables -I INPUT -p tcp --dport 20450:20480 -j ACCEPT   
iptables -I INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT   
iptables -P INPUT DROP

****文章参考****

**http://netfilter.org/ iptables官方网站  
　　http://www.linux.gov.cn/netweb/iptables.htm iptables配置手册  
　　http://man.chinaunix.net/  
　　http://man.chinaunix.net/network/iptables-tutorial-cn-1.1.19.html iptables配置手册  
　　http://blog.csdn.net/thmono/archive/2010/04/08/5462043.aspx  
　　http://netsecurity.51cto.com/art/200512/14457.htm  
　　http://blog.sina.com.cn/s/blog\_40ba724c0100jz12.html  
　　http://qiliuping.blog.163.com/blog/static/1023829320105245337799/**