**北京科技大学实验报告**

学院：计算机与通信工程学院 专业： 信息安全 班级： 信安192

姓名： 霍炟 学号：41824147 实验日期： 2022年 4月 20日

**实验名称：网络防火墙初级实验**

## 实验目的

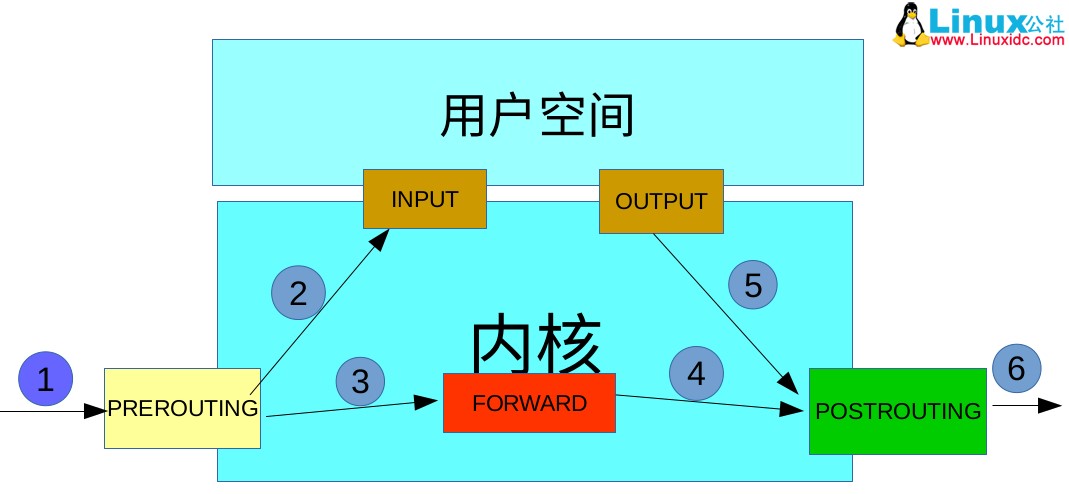
iptables常用规则示例，这些例子为您提供了些基本的iptables使用方法。通过本实验了解iptables的基本使用方法。

## 实验仪器

ubuntu • g++

## 实验原理

iptables实现防火墙功能的原理是：在数据包经过内核的过程中有五处关键地方，分别是PREROUTING、INPUT、OUTPUT、FORWARD、POSTROUTING，称为钩子函数，iptables这款用户空间的软件可以在这5处地方写规则，对经过的数据包进行处理，规则一般的定义为“如果数据包头符合这样的条件，就这样处理数据包”。 数据包先经过PREOUTING，由该链确定数据包的走向： 1、目的地址是本地，则发送到INPUT，让INPUT决定是否接收下来送到用户空间，流程为①--->②; 2、若满足PREROUTING的nat表上的转发规则，则发送给FORWARD，然后再经过POSTROUTING发送出去，流程为： ①--->③--->④--->⑥ 主机发送数据包时，流程则是⑤--->⑥



## 实验内容与步骤

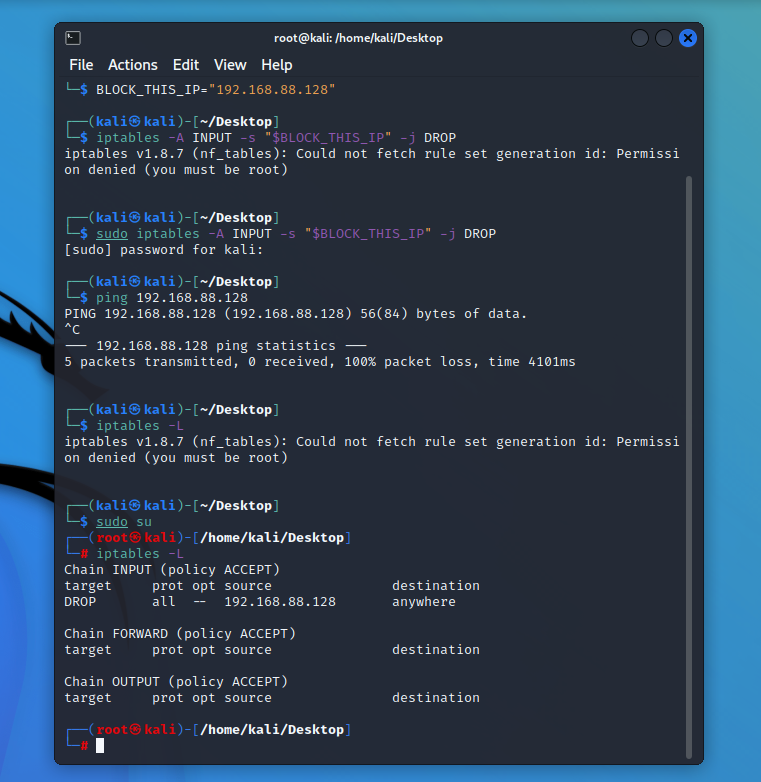
工作目录 访问IPtables方式如下： • 桌面右键打开终端命令行 • 输入iptables进入iptables客户端

1、阻止指定的IP地址

丢弃来自IP地址 192.168.88.128的包

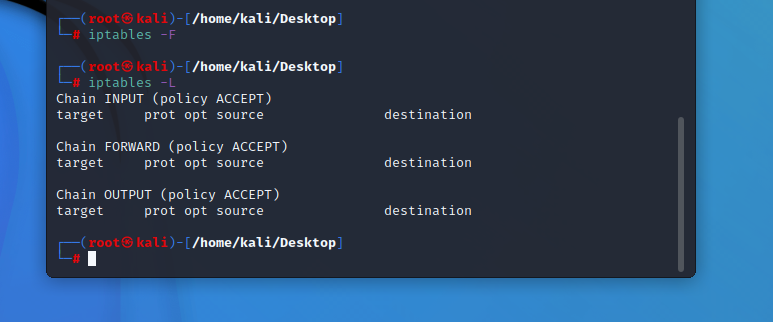
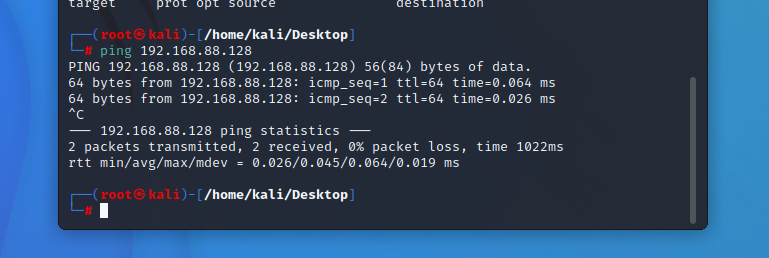
BLOCK\_THIS\_IP="192.168.88.128"

iptables -A INPUT -s "$BLOCK\_THIS\_IP" -j DROP

阻止192.168.88.128之后，ping 192.168.88.128失败  使用iptables –L命令之后，发现本机进入了DROP列表

2、删除已有规则

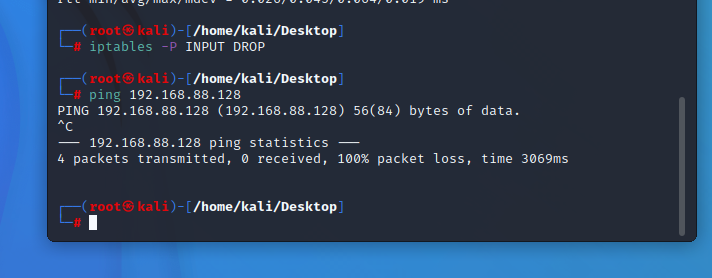
iptables –F

删除已有的规则之后，192.168.88.128没有出现在DROP列表当中  重新ping 192.168.88.128可以ping通 

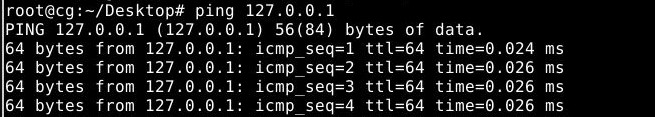
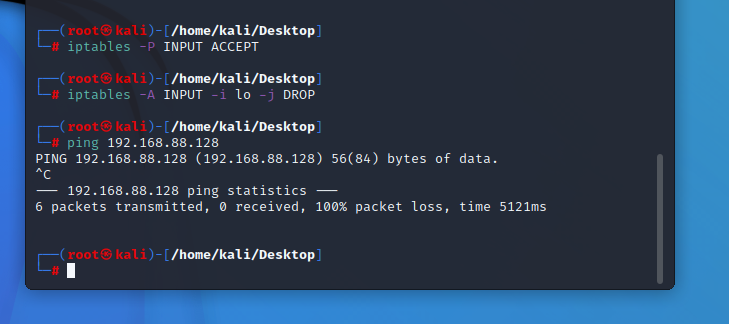
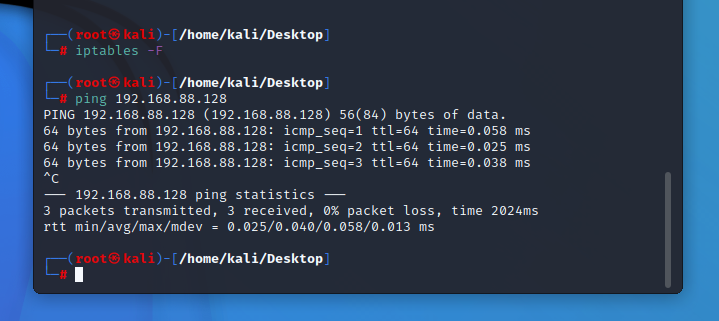
3、设置链的默认策略

链的默认政策设置为”ACCEPT”（接受），若要将INPUT链设置成”DROP”（拒绝）

iptables -P INPUT DROP

输入命令之后ping本机失败 

4、设置阻止回环访问

设置之前默认是允许回环访问的  设置不允许回环访问，ping 127.0.0.1失败  修改回允许回环访问，可以ping成功 

5、关闭所有终端，点击提交评测

## 实验数据

见上图

## 实验数据处理

无

## 实验结果与分析

**iptables**

　　iptables是什么？

* iptables不是防火墙，是防火墙用户代理
* 用于把用户的安全设置添加到安全框架中
* 安全框架是防火墙
* 安全框架的名称为netfilter
* netfilter位于内核空间中，是Linux操作系统核心层内部的一个数据包处理模块
* iptables是用于在用户空间对内核空间的netfilter进行操作的命令行工具
* **netﬁlter/iptables功能**

　　netﬁlter/iptables可简称为iptables，为Linux平台下的包过滤防火墙，是开源的，内核自带的，可以代替成本较高的 企业级硬件防火墙，能够实现如下功能：

* 数据包过滤，即防火墙
* 数据包重定向，即转发
* 网络地址转换，即可NAT

　　注：

　　平常我们使用iptables并不是防火墙的“服务”，而服务是由内核提供的。

**iptables概念**

　　iptables工作依据------规则(rules）

　　iptables是按照规则(rules)来办事的，而规则就是运维人员所定义的条件；规则一般定义为“如果数据包头符合这样的 条件，就这样处理这个数据包”。

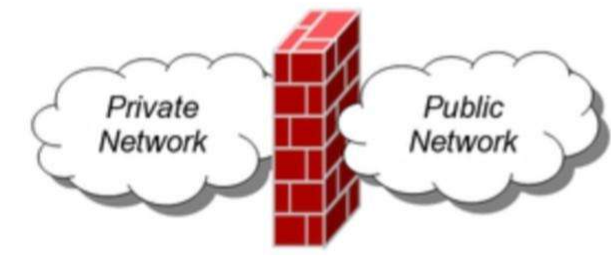
　　规则存储在内核空间的数据包过滤表中，这些规则分别指定了源地址、目的地址，传输协议(TCP、UDP、ICMP)和服 务类型(HTTP、FTP)等。  
　　当数据包与规则匹配时，iptables就根据规则所定义的方法来处理这些数据包，比如放行(ACCEPT)、拒绝(REJECT)、 丢弃(DROP)等

配置防火墙主要工作就是对iptables规则进行添加、修改、删除等  
　　小结：

* 工作依据是规则
* 规则存在表中
* 规则指定了什么？源地址或目的地址或传输协议的类型
* 如果数据包备匹配到，按照规则指定的动作去执行

**iptables中链的概念**

　　当客户端访问服务器端的web服务时，客户端发送访问请求报文至网卡，而tcp/ip协议栈是属于内核的一部分，  
所 以，客户端的请求报文会通过内核的TCP协议传输到用户空间的web服务，而客户端报文的目标地址为web服务器  
所 监听的套接字(ip:port)上，当web服务器响应客户端请求时，web服务所回应的响应报文的目标地址为客户端地址，  
我们说过，netﬁlter才是真正的防火墙，属于内核的一部分，所以，我们要想让netﬁlter起到作用，我们就需要在内  
核中设置“关口”，所以进出的数据报文都要通过这些关口，经检查，符合放行条件的准允放行，符合阻拦条件的则被  
阻止，于是就出现了input和output关口，然而在iptables中我们把关口叫做“链”。

　　在计算机领域，防火墙是用于保护信息安全的设备，其会依照用户定义的规则，允许或限制数据的传输。  
　　

* 用于保护内网安全的一种设备
* 依据规则进行防护
* 用户定义规则
* 允许或拒绝外部用户访问

**防火墙分类**

　　逻辑上划分，防火墙可以大体分为主机防火墙和网络防火墙  
　　主机防火墙：针对于单个主机进行防护  
　　网络防火墙：针对网络进行防护，处于网络边缘，防火墙背后是本地局域网  
　　网络防火墙主外(服务集体)，主机防火墙主内(服务个人)

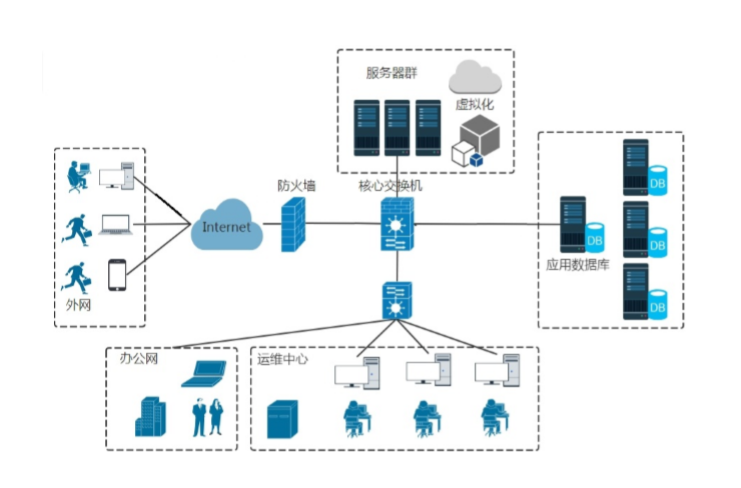
　　物理上划分，防火墙可分为硬件防火墙和软件防火墙  
　　硬件防火墙：在硬件级别实现防火墙功能，另一部分基于软件实现，其性能高，硬件成本高

　　软件防火墙：应用软件处理逻辑运行于通用硬件平台之上的防火墙，其性能相较于硬件防火墙低，成本较低，对于 Linux系统已自带，直接使用即可

**防火墙性能**

* 吞吐量
* 并发连接
* 新建连接
* 时延
* 抖动

**硬件防火墙**



**软件防火墙**

　　软件防火墙是单独使用具备配置数据包通过规则的软件来实现数据包过滤。多见于单主机系统或个人计算机。

**Web应用防火墙(WAF）**

　　Web应用防火墙是对web防护(网页保护)的安全防护设备(软件)，主要用于截获所有HTTP数据或仅仅满足某些规则的 会话。多见于云平台中。

**硬件防火墙和软件防火墙对比**

　　硬件防火墙有独立的硬件设备，运算效率较高，价格略高，可为计算机网络提供安全防护。  
　　软件防火墙必须部署在主机系统之上，相较于硬件防火墙运算效率低，在一定程度上会影响到主机系统性能，一般用 于单机系统或个人计算机中，不直接用于计算机网络中。

**iptables**

　　iptables是什么？

* iptables不是防火墙，是防火墙用户代理
* 用于把用户的安全设置添加到安全框架中
* 安全框架是防火墙
* 安全框架的名称为netfilter
* netfilter位于内核空间中，是Linux操作系统核心层内部的一个数据包处理模块
* iptables是用于在用户空间对内核空间的netfilter进行操作的命令行工具
* **netﬁlter/iptables功能**

　　netﬁlter/iptables可简称为iptables，为Linux平台下的包过滤防火墙，是开源的，内核自带的，可以代替成本较高的 企业级硬件防火墙，能够实现如下功能：

* 数据包过滤，即防火墙
* 数据包重定向，即转发
* 网络地址转换，即可NAT

　　注：

　　平常我们使用iptables并不是防火墙的“服务”，而服务是由内核提供的。

**iptables概念**

　　iptables工作依据------规则(rules）

　　iptables是按照规则(rules)来办事的，而规则就是运维人员所定义的条件；规则一般定义为“如果数据包头符合这样的 条件，就这样处理这个数据包”。

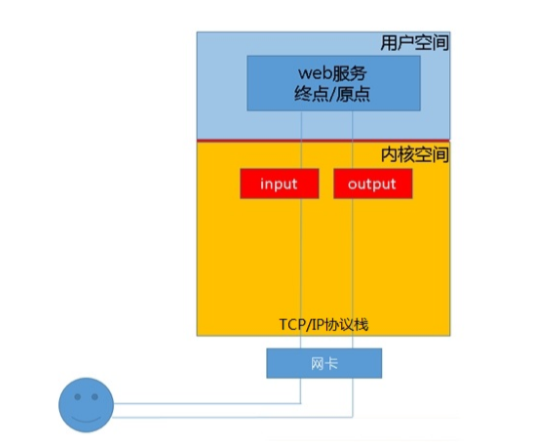
　　规则存储在内核空间的数据包过滤表中，这些规则分别指定了源地址、目的地址，传输协议(TCP、UDP、ICMP)和服 务类型(HTTP、FTP)等。  
　　当数据包与规则匹配时，iptables就根据规则所定义的方法来处理这些数据包，比如放行(ACCEPT)、拒绝(REJECT)、 丢弃(DROP)等

配置防火墙主要工作就是对iptables规则进行添加、修改、删除等  
　　小结：

* 工作依据是规则
* 规则存在表中
* 规则指定了什么？源地址或目的地址或传输协议的类型
* 如果数据包备匹配到，按照规则指定的动作去执行

**iptables中链的概念**

　　当客户端访问服务器端的web服务时，客户端发送访问请求报文至网卡，而tcp/ip协议栈是属于内核的一部分，  
所 以，客户端的请求报文会通过内核的TCP协议传输到用户空间的web服务，而客户端报文的目标地址为web服务器  
所 监听的套接字(ip:port)上，当web服务器响应客户端请求时，web服务所回应的响应报文的目标地址为客户端地址，  
我们说过，netﬁlter才是真正的防火墙，属于内核的一部分，所以，我们要想让netﬁlter起到作用，我们就需要在内  
核中设置“关口”，所以进出的数据报文都要通过这些关口，经检查，符合放行条件的准允放行，符合阻拦条件的则被  
阻止，于是就出现了input和output关口，然而在iptables中我们把关口叫做“链”。



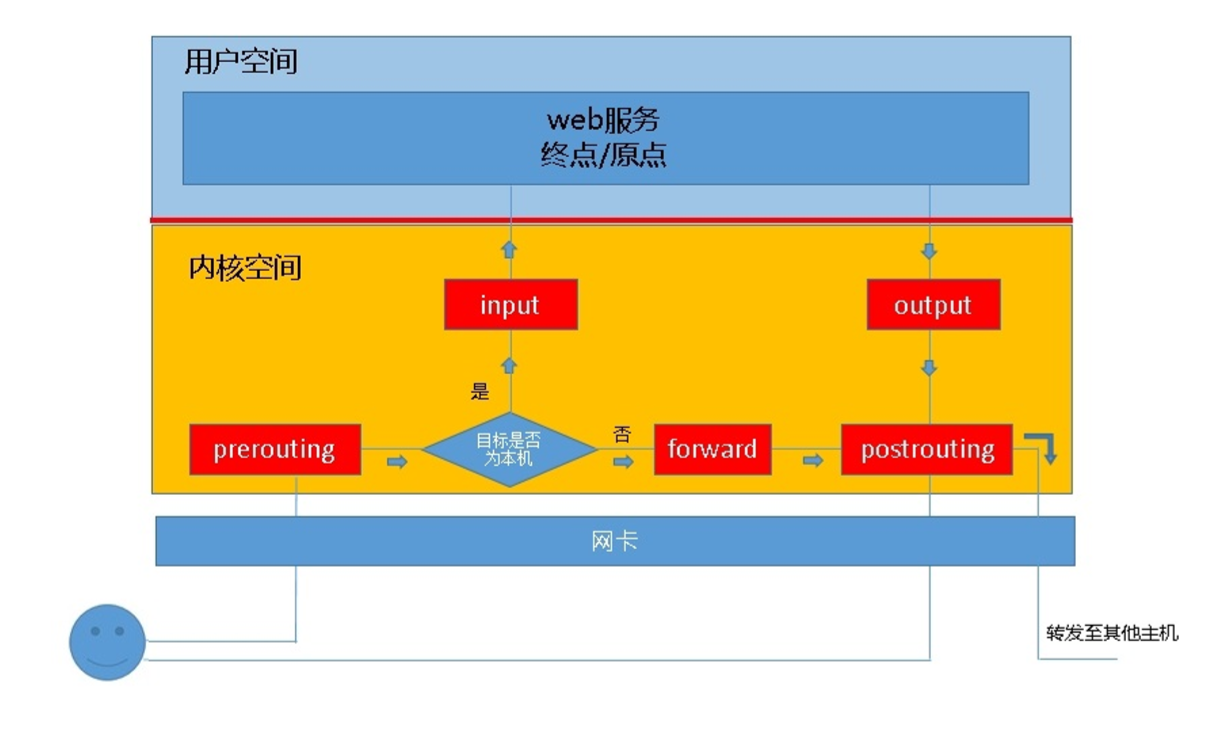
 　　上面的举例中，如果客户端发到本机的报文中包含的服务器地址并不是本机，而是其他服务器，此时本机就应该能够  
进行转发，那么这个转发就是本机内核所支持的IP\_FORWARD功能，此时我们的主机类似于路由器功能，所以我们会  
看到在iptables中，所谓的关口并只有上面所提到的input及output这两个，应该还有“路由前”，“转发”，“路由后”，  
它们所对应的英文名称分别为“PREROUTING”，“FORWARD”，“POSTROUTING”，这就是我们说到的5链  
　　INPUT

　　OUTPUT

　　PREROUTING

　　FORWARD

　　POSTROUTING



 　　通过上图可以看出，当我们在本地启动了防火墙功能时，数据报文需要经过以上关口，根据各报文情况，  
各报名经常 的“链”可能不同，如果报文目标地址是本机，则会经常input链发往本机用户空间，如果报  
文目标不是本机，则会直接 在内核空间中经常forward链和postrouting链转发出去。

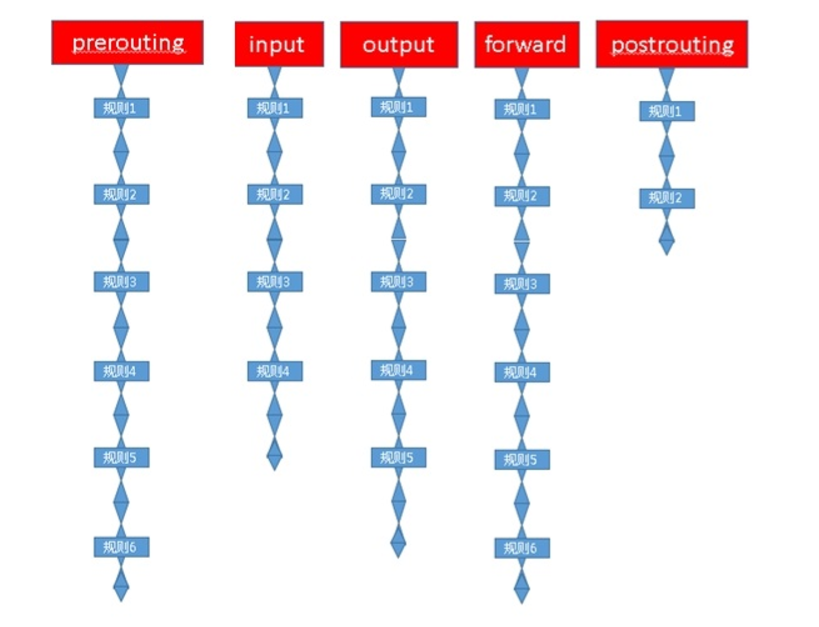
　　所以，根据上图，我们能够想象出某些常用场景中，报文的流向：

　　到本机某进程的报文：PREROUTING --> INPUT

　　由本机转发的报文：PREROUTING --> FORWARD --> POSTROUTING

　　由本机的某进程发出报文（通常为响应报文）：OUTPUT --> POSTROUTING

　　有的时候我们也经常听到人们在称呼input为“规则链”，这又是怎么回事呢？  
我们知道，防火墙的作用在于对经过的数 据报文进行规则匹配，然后执行  
对应的“动作”，所以数据包经过这些关口时，必须匹配这个关口规则，但是  
关口规则 可能不止一条，可能会有很多，当我们把众多规则放在一个关口  
上时，所有的数据包经常都要进行匹配，那么就形成 了一个要匹配的规则  
链条，因此我们也把“链”称作“规则链”。



 　　INPUT:处理入站数据包

　　OUTPUT:处理出站数据包  
　　FORWARD:处理转发数据包(主要是将数据包转发至本机其它网卡)

　　当数据报文经过本机时，网卡接收数据报文至缓冲区，内核读取报文ip首部，发现报文不是送到本机时（目的ip 不是本机），由内核直接送到forward链做匹配，匹配之后若符合forward的规则，再经由postrouting送往下一 跳或目的主机。  
　　PREROUTING:在进行路由选择前处理数据包，修改到达防火墙数据包的目的IP地址，用于判断目标主机

　　POSTROUTING:在进行路由选择后处理数据包，修改要离开防火墙数据包的源IP地址，判断经由哪一接口送往 下一跳

**iptables中表的概念**

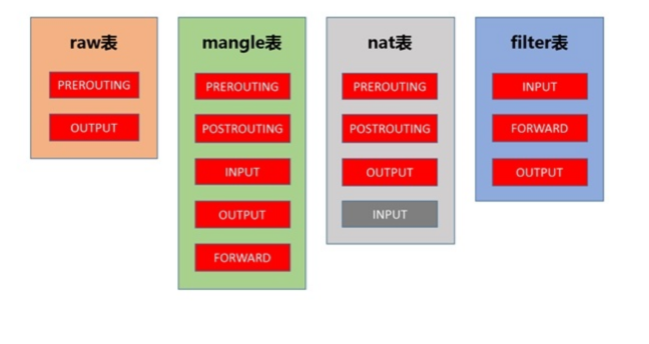
　　每个“规则链”上都设置了一串规则，这样的话，我们就可以把不同的“规则链”组合成能够完成某一特定功能集合分 类，而这个集合分类我们就称为表，iptables中共有5张表，学习iptables需要搞明白每种表的作用。

* ﬁlter: 过滤功能，确定是否放行该数据包，属于真正防火墙，内核模块：iptables\_ﬁlter
* nat: 网络地址转换功能，修改数据包中的源、目标IP地址或端口；内核模块：iptable\_nat
* mangle: 对数据包进行重新封装功能，为数据包设置标记；内核模块：iptable\_mangle
* raw: 确定是否对数据包进行跟踪；内核模块：iptables\_raw
* security:是否定义强制访问控制规则；后加上的

**iptables中表链之间的关系**

　　我们在应用防火墙时是以表为操作入口的，只要在相应的表中的规则链上添加规则即可实现某一功能。那么我们就应 该知道哪张表包括哪些规则链，然后在规则链上操作即可。

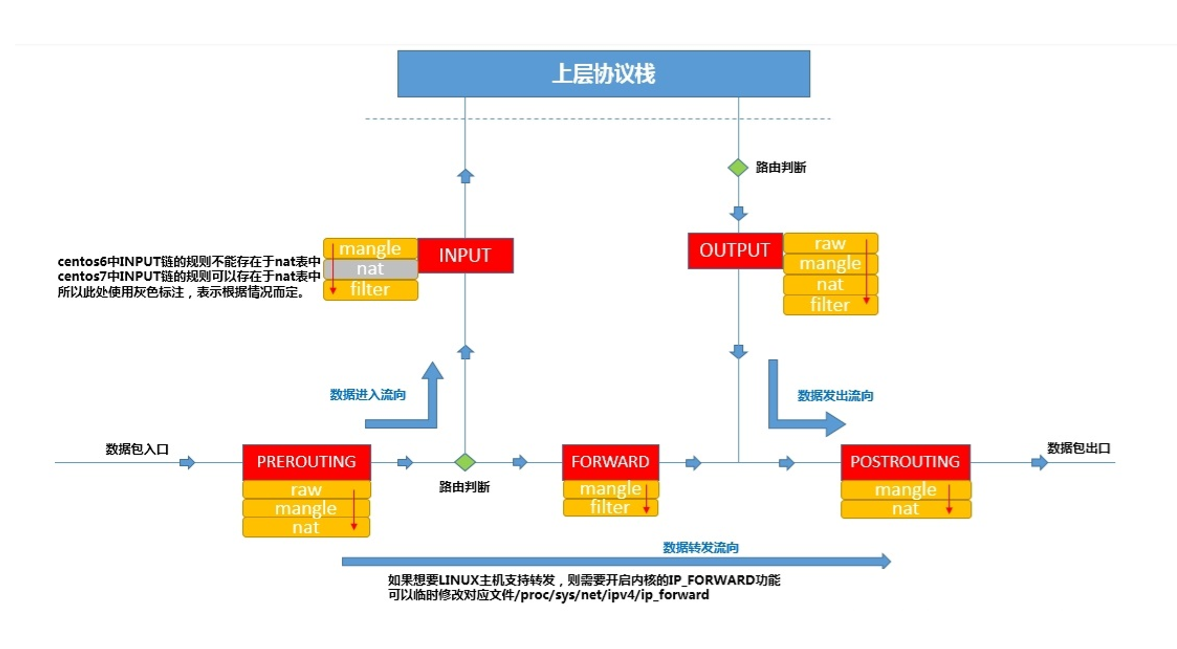
* ﬁlter表可以使用哪些链定义规则：INPUT,FORWARD,OUTPUT
* nat表中可以使用哪些链定义规则：PREROUTING,OUTPUT ,POSTROUTING,INPUT
* mangle 表中可以使用哪些链定义规则：PREROUTING,INPUT,FORWARD,OUTPUT,POSTROUTING
* raw表中可以使用哪些链定义规则：PREROUTING,OUTPUT



**iptables中表的优先级**

　　raw-mangle-nat-ﬁlter(由高至低)

**数据包经由iptables的流程**



资料来源：[一，Iptables详解(1):iptables概念 - minseo - 博客园 (cnblogs.com)](https://www.cnblogs.com/minseo/p/13595092.html)