1-Linux 防火墙基础概念

作者：Carey
原文链接：https://ld246.com/article/1611571699841
来源网站：链滴

1 安全技术和防火墙

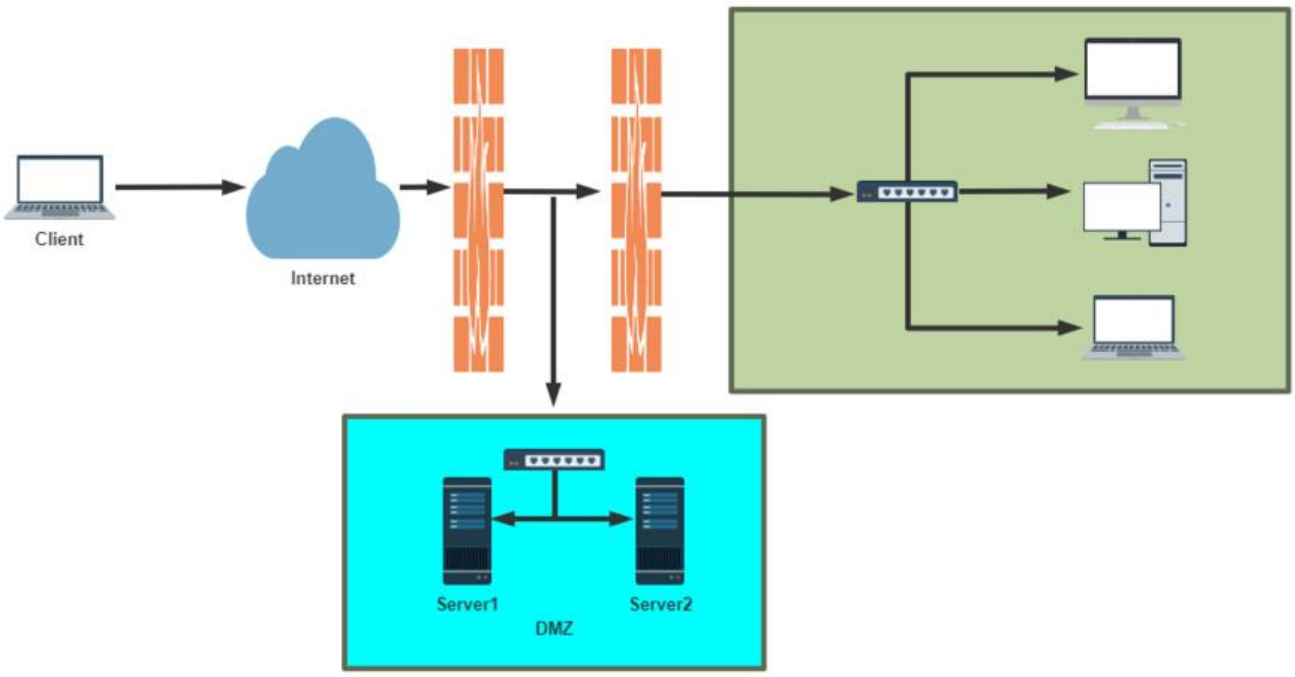
1.1 安全技术

● 入侵检测系统（Intrusion Detection Systems）：特点是不阻断任何网络访问，量化、定位来自内网络的威胁情况，主要以提供报告和事后监督为主，提供有针对性的指导措施和安全决策依据。一般用旁路部署方式

● 入侵防御系统（Intrusion Prevention System）：以透明模式工作，分析数据包的内容如：溢出击、拒绝服务攻击、木马、蠕虫、系统漏洞等进行准确的分析判断，在判定为攻击行为后立即予以阻，主动而有效的保护网络的安全，一般采用在线部署方式

● 防火墙（FireWall）：隔离功能，工作在网络或主机边缘，对进出网络或主机的数据包基于一定规则检查，并在匹配某规则时由规则定义的行为进行处理的一组功能的组件，基本上的实现都是默认况下关闭所有的通过型访问，只开放允许访问的策略,会将希望外网访问的主机放在DMZ(demilitarize zone)网络中

防水墙
广泛意义上的防水墙：防水墙（Waterwall），与防火墙相对，是一种防止内部信息泄漏的安全产品网络、外设接口、存储介质和打印机构成信息泄漏的全部途径。防水墙针对这四种泄密途径，在事前事中、事后进行全面防护。其与防病毒产品、外部安全产品一起构成完整的网络安全体系。



1.2 防火墙的分类

按保护范围划分：

- 主机防火墙：服务范围为当前一台主机
- 网络防火墙：服务范围为防火墙一侧的局域网

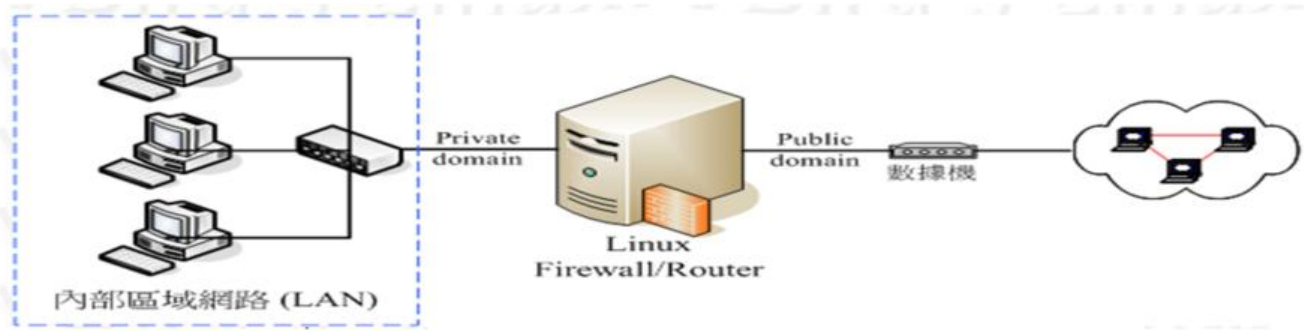
按实现方式划分：

- 硬件防火墙：在专用硬件级别实现部分功能的防火墙；另一个部分功能基于软件实现，如：华为，融信，启明星辰，绿盟，深信服, Checkpoint，NetScreen(Juniper2004年40亿美元收购)等
- 软件防火墙：运行于通用硬件平台之上的防火墙的应用软件，Windows 防火墙 ISA --> Forefront MG

按网络协议划分：

- 网络层防火墙：OSI模型下四层，又称为包过滤防火墙
- 应用层防火墙/代理服务器：proxy 代理网关，OSI模型七层

包过滤防火墙



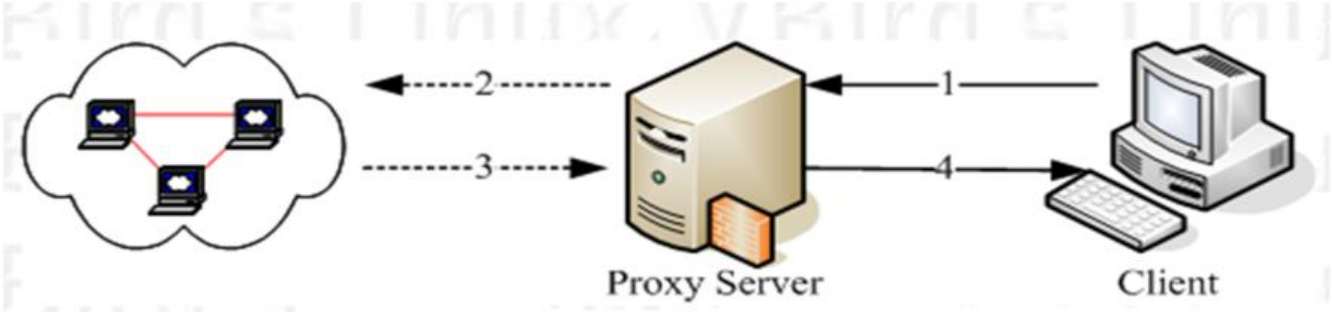
原文链接：1-Linux 防火墙基础概念

网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，被称为访问控制列表（ACL），通检查数据流中每个数据的源地址，目的地址，所用端口号和协议状态等因素，或他们的组合来确定是允许该数据包通过

优点：对用户来说透明，处理速度快且易于维护

缺点：无法检查应用层数据，如病毒等

应用层防火墙



应用层防火墙/代理服务型防火墙，也称为代理服务器（Proxy Server）

将所有跨越防火墙的网络通信链路分为两段

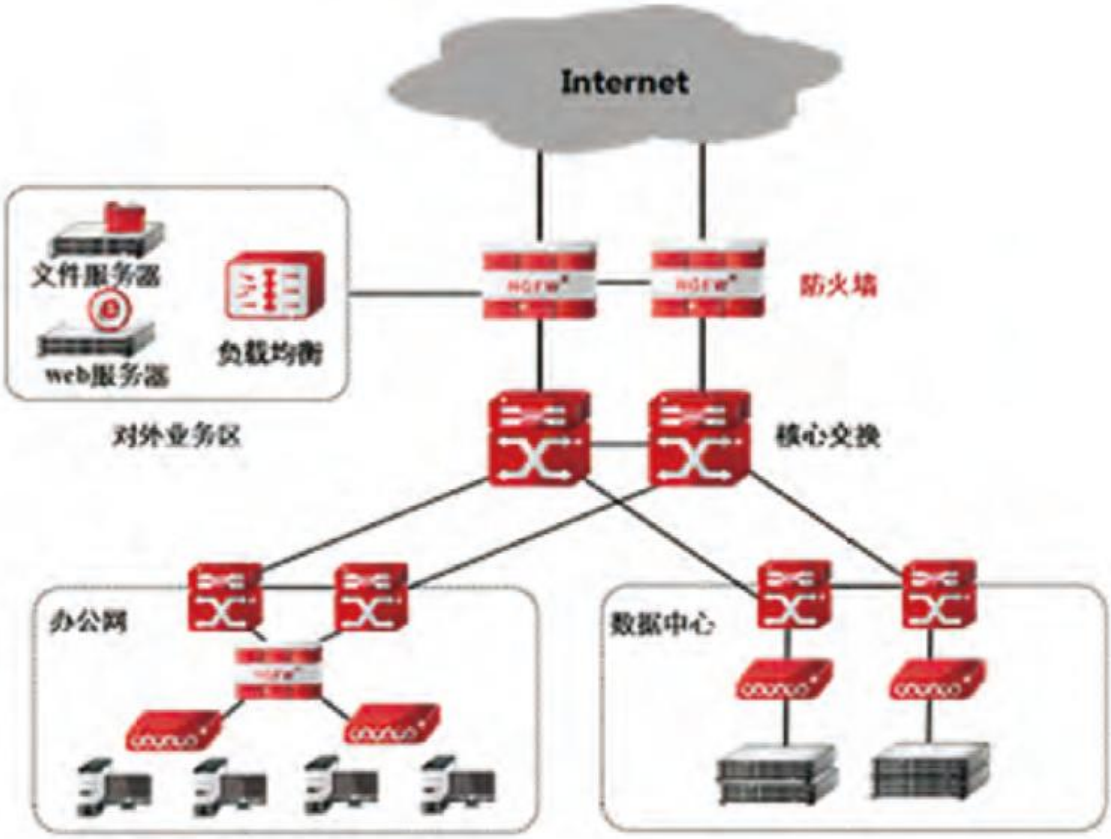
内外网用户的访问都是通过代理服务器上的“链接”来实现

优点：在应用层对数据进行检查，比较安全

缺点：增加防火墙的负载

提示：现实生产环境中所使用的防火墙一般都是二者结合体，即先检查网络数据，通过之后再送到应层去检查

1.3 网络架构



2 Linux 防火墙的基本认识

2.1 Netfilter

Linux防火墙是由Netfilter组件提供的，Netfilter工作在内核空间，集成在linux内核中Netfilter 是Linux 2.4.x之后新一代的Linux防火墙机制，是linux内核的一个子系统。Netfilter采用模块化设计，具有好的可扩充性，提供扩展各种网络服务的结构化底层框架。Netfilter与IP协议栈是无缝契合，并允许数据报进行过滤、地址转换、处理等操作

Netfilter官网文档：https://netfilter.org/documentation/

```
[17:28:01 root@centos8 ~]#grep -m 10 NETFILTER /boot/config-4.18.0-193.el8.x86_64
CONFIG_NETFILTER=y
CONFIG_NETFILTER_ADVANCED=y
CONFIG_BRIDGE_NETFILTER=m
CONFIG_NETFILTER_INGRESS=y
CONFIG_NETFILTER_NETLINK=m
CONFIG_NETFILTER_FAMILY_BRIDGE=y
CONFIG_NETFILTER_FAMILY_ARP=y
# CONFIG_NETFILTER_NETLINK_ACCT is not set
CONFIG_NETFILTER_NETLINK_QUEUE=m
CONFIG_NETFILTER_NETLINK_LOG=m
[17:35:40 root@centos7 ~]#grep -m 10 NETFILTER /boot/config-3.10.0-1127.el7.x86_64
CONFIG_NETFILTER=y
# CONFIG_NETFILTER_DEBUG is not set
CONFIG_NETFILTER_ADVANCED=y
```

CONFIG_BRIDGE_NETFILTER=m
CONFIG_NETFILTER_NETLINK=m
CONFIG_NETFILTER_NETLINK_ACCT=m
CONFIG_NETFILTER_NETLINK_QUEUE=m
CONFIG_NETFILTER_NETLINK_LOG=m
CONFIG_NETFILTER_NETLINK_QUEUE_CT=y
CONFIG_NETFILTER_SYNPROXY=m
各种Linux发行版本都有

2.2 防火墙工具介绍

2.2.1 iptables

由软件包iptables提供的命令行工具，工作在用户空间，用来编写规则，写好的规则被送往netfilter
告诉内核如何去处理信息包

```
[17:34:38 root@centos8 ~]#rpm -qi iptables
Name        : iptables
Version     : 1.8.4
Release     : 10.el8
Architecture: x86_64
Install Date: Thu 17 Dec 2020 05:01:47 PM CST
Group       : Unspecified
Size        : 1974473
License     : GPLv2 and Artistic 2.0 and ISC
Signature   : RSA/SHA256, Sun 26 Apr 2020 10:09:33 AM CST, Key ID 05b555b38483c65d
Source RPM  : iptables-1.8.4-10.el8.src.rpm
Build Date  : Fri 24 Apr 2020 09:51:59 PM CST
Build Host  : x86-01.mbox.centos.org
Relocations : (not relocatable)
Packager    : CentOS Buildsys
Vendor      : CentOS
URL         : http://www.netfilter.org/projects/iptables
Summary     : Tools for managing Linux kernel packet filtering capabilities
Description :
The iptables utility controls the network packet filtering code in the
Linux kernel. If you need to set up firewalls and/or IP masquerading,
you should either install nftables or this package.

Note: This package contains the nftables-based variants of iptables and
ip6tables, which are drop-in replacements of the legacy tools.
```

范例：安装iptables的service包

```
[17:36:01 root@centos7 ~]#yum install iptables-services.x86_64
[17:38:32 root@centos7 ~]#rpm -ql iptables-services
/etc/sysconfig/ip6tables
/etc/sysconfig/iptables
/usr/lib/systemd/system/ip6tables.service
/usr/lib/systemd/system/iptables.service
/usr/libexec/initscripts/legacy-actions/ip6tables
/usr/libexec/initscripts/legacy-actions/ip6tables/panic
/usr/libexec/initscripts/legacy-actions/ip6tables/save
```

/usr/libexec/initscripts/legacy-actions/iptables
/usr/libexec/initscripts/legacy-actions/iptables/panic
/usr/libexec/initscripts/legacy-actions/iptables/save
/usr/libexec/iptables
/usr/libexec/iptables/ip6tables.init
/usr/libexec/iptables/iptables.init

2.2.2 firewalld

从CentOS 7 版开始引入了新的前端管理工具

软件包：

- firewalld
- firewalld-config

管理工具：

- firewall-cmd 命令行工具
- firewall-config 图形工作

2.2.3 nftables（重点）

Netfilter在内核中选取五个位置放了五个hook(勾子) function(INPUT、OUTPUT、FORWARD、PREOUTING、POSTROUTING)，而这五个hook function向用户开放，用户可以通过一个命令工具（iptables）向其写入规则由信息过滤表（table）组成，包含控制IP包处理的规则集（rules），规则被分放在链（chain）上

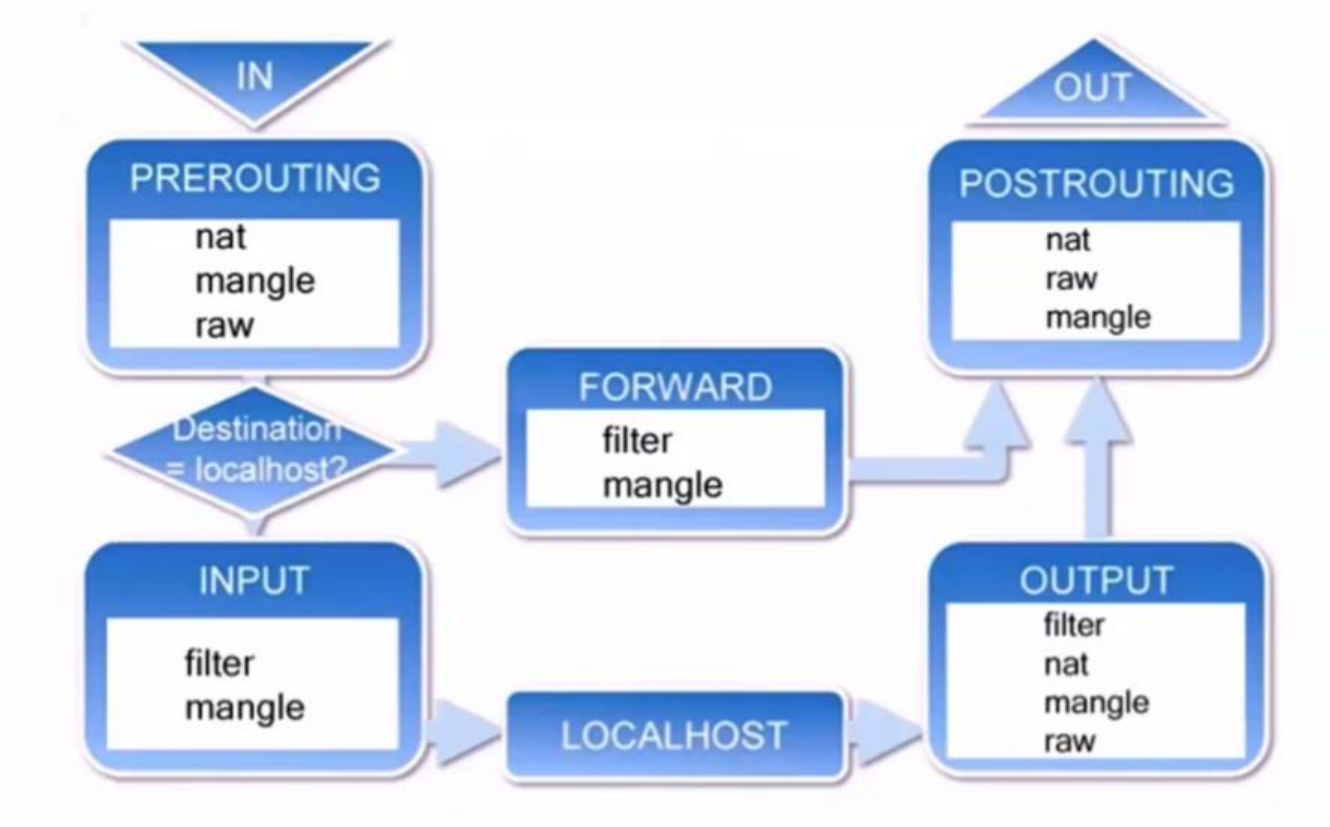
提示：从 Linux kernel 4.2 版以后，Netfilter 在prerouting 前加了一个 ingress 勾子函数。可以使这个新的入口挂钩来过滤来自第2层的流量，这个新挂钩比预路由要早，基本上是 tc 命令（流量控制具）的替代品

三种报文流向

- 流入本机：PREROUTING --> INPUT-->用户空间进程
- 流出本机：用户空间进程 -->OUTPUT--> POSTROUTING
- 转发：PREROUTING --> FORWARD --> POSTROUTING

2.3 iptables的组成

iptables由五个表table和五个链chain以及一些规则组成



链 chain：

- 内置链：每个内置链对应于一个钩子函数
- 自定义链：用于对内置链进行扩展或补充，可实现更灵活的规则组织管理机制；只有Hook钩子调自定义链时，才生效

五个内置链chain:

INPUT,OUTPUT,FORWARD,PREROUTING,POSTROUTING

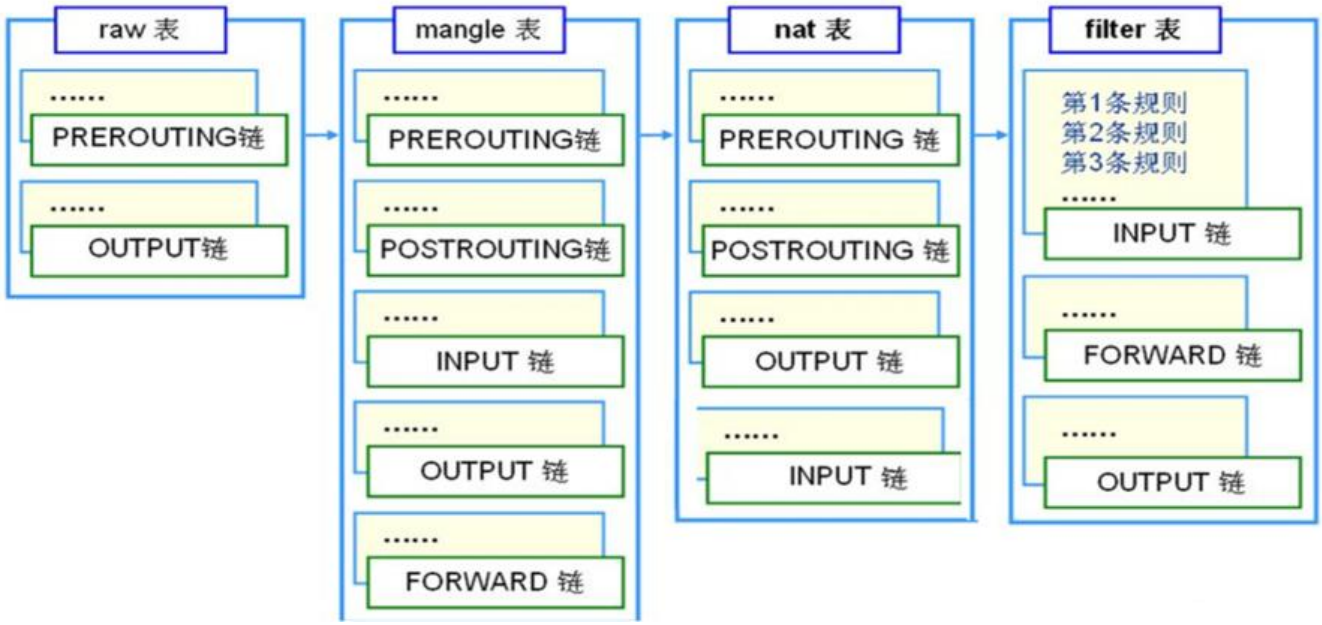
五个表table：filter、nat、mangle、raw、security

- filter：过滤规则表，根据预定义的规则过滤符合条件的数据包,默认表
- nat：network address translation 地址转换规则表
- mangle：修改数据标记位规则表
- raw：关闭启用的连接跟踪机制，加快封包穿越防火墙速度
- security：用于强制访问控制（MAC）网络规则，由Linux安全模块（如SELinux）实现

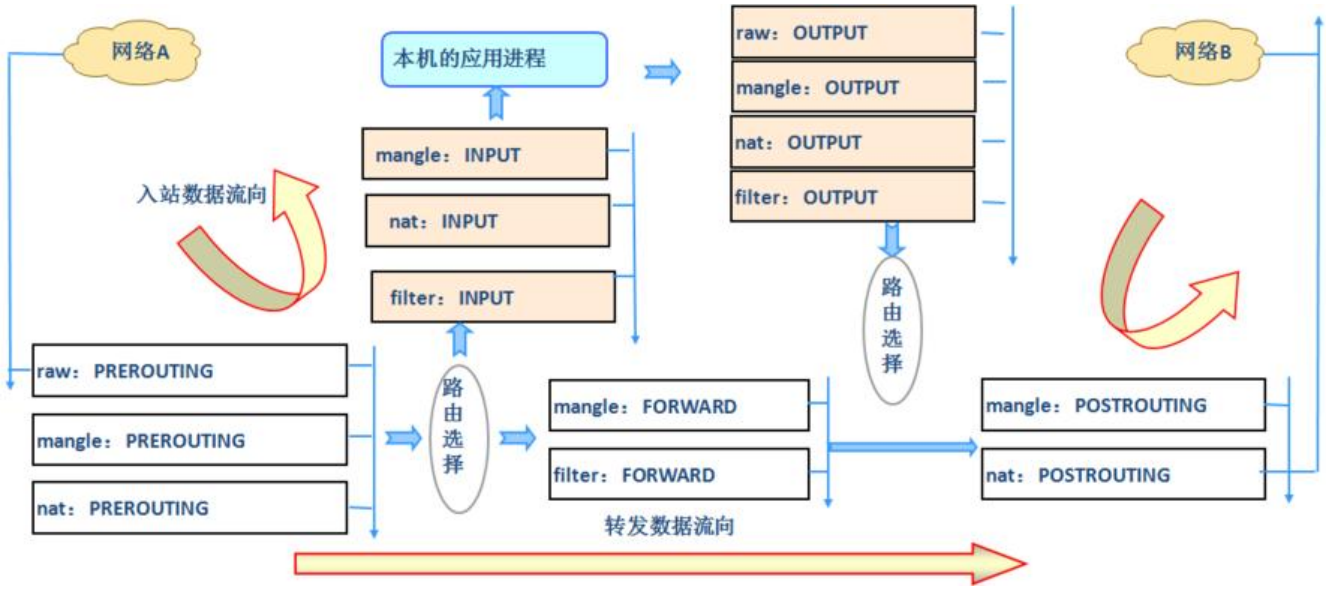
优先级由高到低的顺序为：

security -->raw-->mangle-->nat-->filter

表和链对应关系



数据包过滤匹配流程



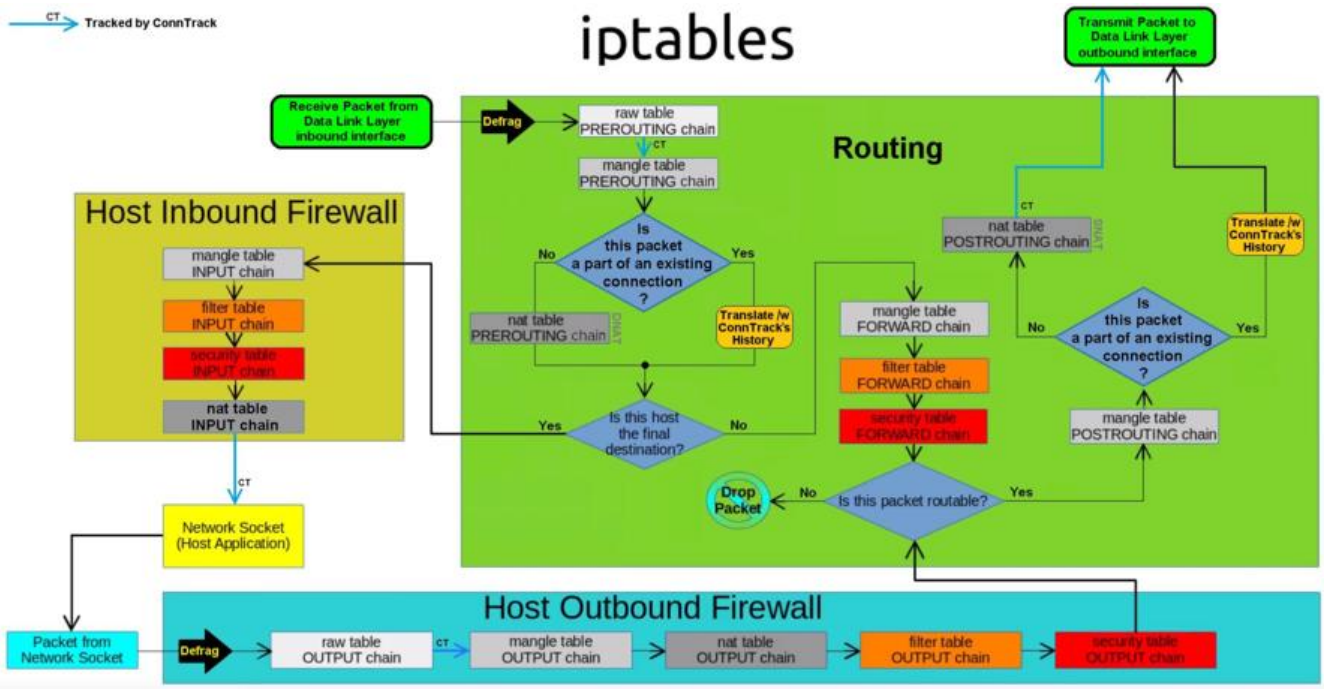
内核中数据包的传输过程

● 当一个数据包进入网卡时，数据包首先进入PREROUTING链，内核根据数据包目的IP判断是否需转送出去

● 如果数据包是进入本机的，数据包就会沿着图向下移动，到达INPUT链。数据包到达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，这些数据包经过OUTPUT链，然后到达POTROUTING链输出

● 如果数据包是要转发出去的，且内核允许转发，数据包就会向右移动，经过FORWARD链，然后到POSTROUTING链输出

2.4 netfilter 完整流程



原文链接：1-Linux 防火墙基础概念