iptables的5条‘链’（chains）

： 作为关口进行把关 （我把这五条链看作墙）

**PREROUTING : 路由前**

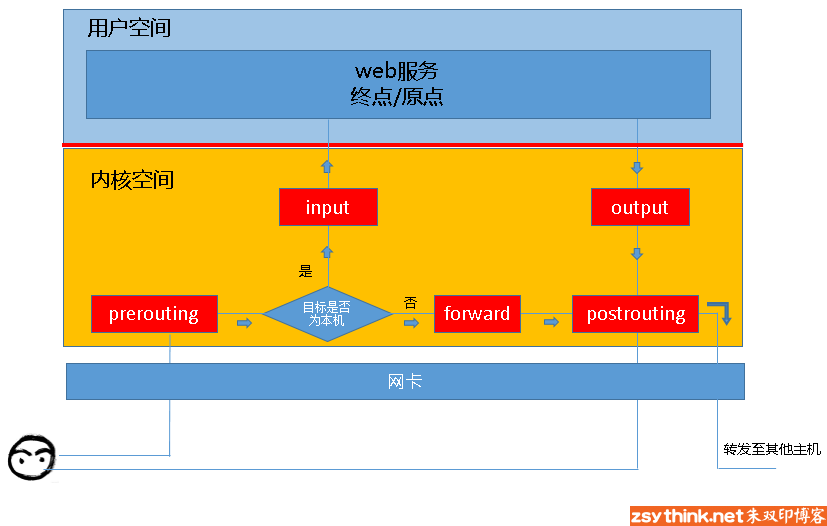
**INPUT : 收包**

**FORWARD : 转发**

**OUTPUT : 发包**

**POSTROUTING : 路由后**

（如图，五条链分别对应在甚么位置）



iptables的4张‘表’ （tables）

： 作为不同功能规则的集合

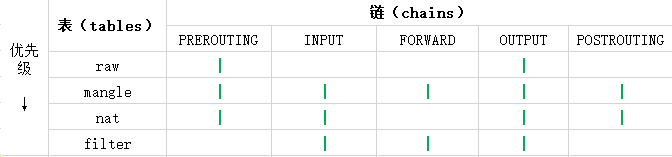
filter表: 和主机自身相关。负责过滤本机流入、流出数据包;

nat表: 和主机自身无关。是网络地址转换，负责来源与目的IP地址和port的转换;

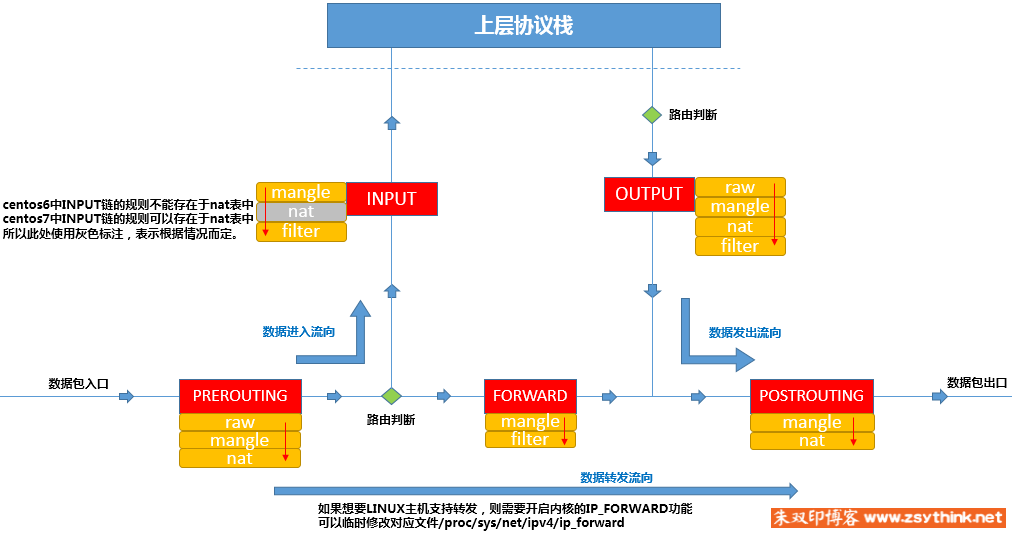
mangle表: 主要负责修改数据包中特殊的路由标记，如TTL、TOS、MARK;

raw表: 优先级最高，设置raw时一般是为了不再让iptables做数据包的链接跟踪处理，提高性能;

(如图，不同表的规则可用于哪些链)



Iptables的综合图示



Iptables命令

命令

|  |  |
| --- | --- |
| 命令 | 释义 |
| -A (append) | 向某链中追加规则 |
| -D (delete) | 删除某链中与指定规则匹配或指定编号的条目 |
| -R (replace) | 替换某链中第i条或第一条为当前规则 |
| -I (insert) | 在某链第i条规则前插入一条规则之后的规则后移，默认i=1 |
| -L (list) | 列出某链（所有链）的第i条规则（所有规则） |
| -N (new) | 创建一个新链（chain name） -- 自定义 |
| -S (list-rules) | 同-L |
| -F (flush) | 清空某链（所有链）中的规则 |
| -X (delete-chain) | 删除用户自定义的某链(所有链)，该指令不影响5链 |
| -P (policy) | 改变某链的策略 |
| -E (rename-chain) | 将 old-chain 名称更改为 new-chain。这样做可以使所有引用 old-chain 的规则失效 |

规则参数

|  |  |
| --- | --- |
| **参数** | **释义** |
| **-P (protocol)** | 网络协议，如：tcp、udp、icmp |
| **-S (source)** | 源地址， ip |
| **-D (destination)** | 目的地址，ip |
| **-J (jump)** | 满足指定规则时跳转到处理规则，如ACCEPT（接受）、DROP（丢弃）、QUEUE（进入队列）、RETURN（跳出）、REJECT（明示拒绝）、SNAT（地址转换） |
| **-I (in interface)** | 入站接口 |
| **-O (out interface)** | 出站接口 |
| **-SPORT (source port)** | 源端口，默认匹配所有端口。用于-p tcp 或 –p udp |
| **-DPORT (destination port)** | 目的端口，用于-p tcp 或 –p udp |
| **-TCP-FLAGS** | Tcp标志，例如SYN、ACK、FIN等，可以使用因为半角逗号(,)来制定多个TCP标识 |
| **-ICMP-TYPE** | ICMP类型，用于-P ICMP |