

端口转发

1. IPtables

(1) IPtables 中存在 4 个表：

Filter：一般的过滤功能

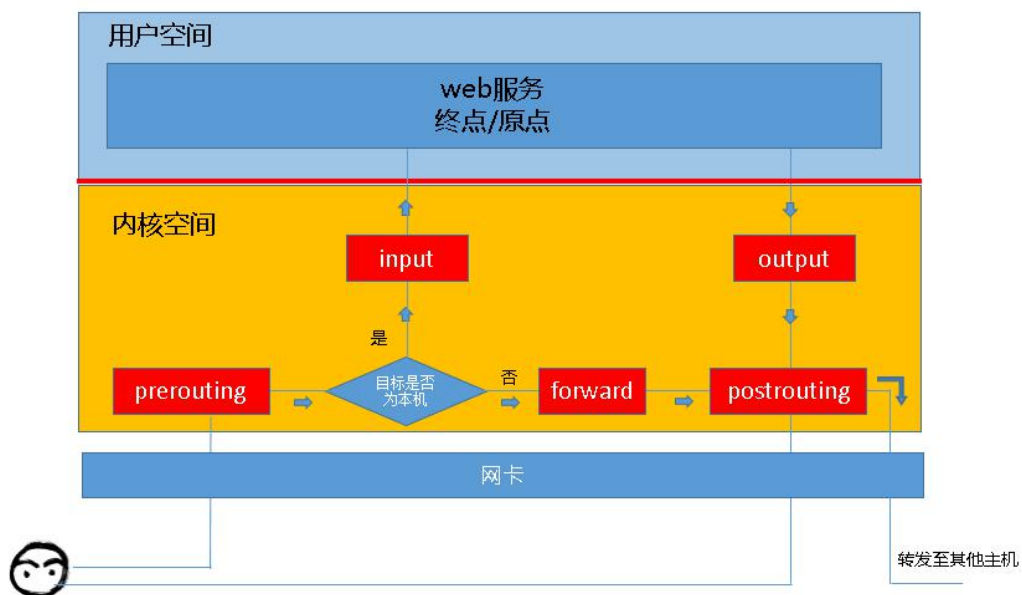
Nat：网络地址转换功能（端口映射，地址映射等）

Nat 表中存在 snat, dnat, pnat

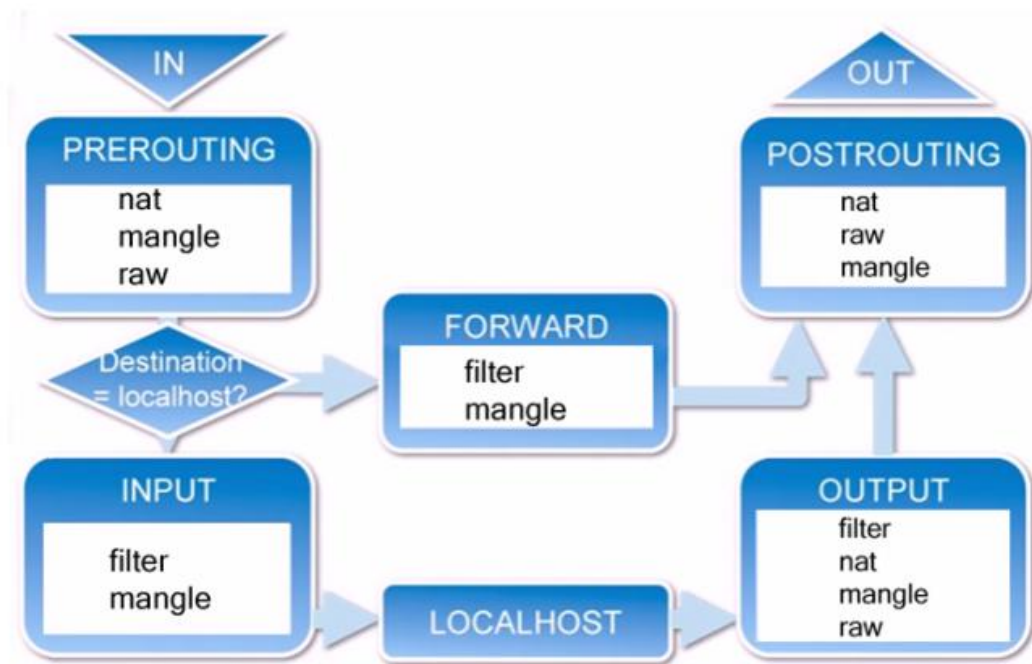
Mangle：拆解报文，做出修改并重新封装的功能

Raw：优先级最高，关闭 nat 表上的连接追踪机制。

(2) IPtables 的链路



iptables的原理主要是对数据包的控制，看下图：



报文流向

1. 到本机某进程的报文： prerouting->input
2. 由本机转发的报文： prerouting->forward->postrouting
3. 由本机某进程发出的报文（通常为响应报文） output->postrouting

(3) iptables 中的表和链路的对应关系

Filter: INPUT FORWARD OUTPUT

NAT: PREROUTING OUTPUT POSTROUTING

Mangle: PREROUTING INPUT FORWARD OUTPUT POSTROUTING

Raw: PREROUTING OUTPUT

