**iptables简介**

我们平常看到的iptables实现的linux平台防火墙功能其实是由iptables和netfilter共同完成的。而真正的iptables仅仅是linux上的防火墙管理工具

**iptables与netfilter的关系**

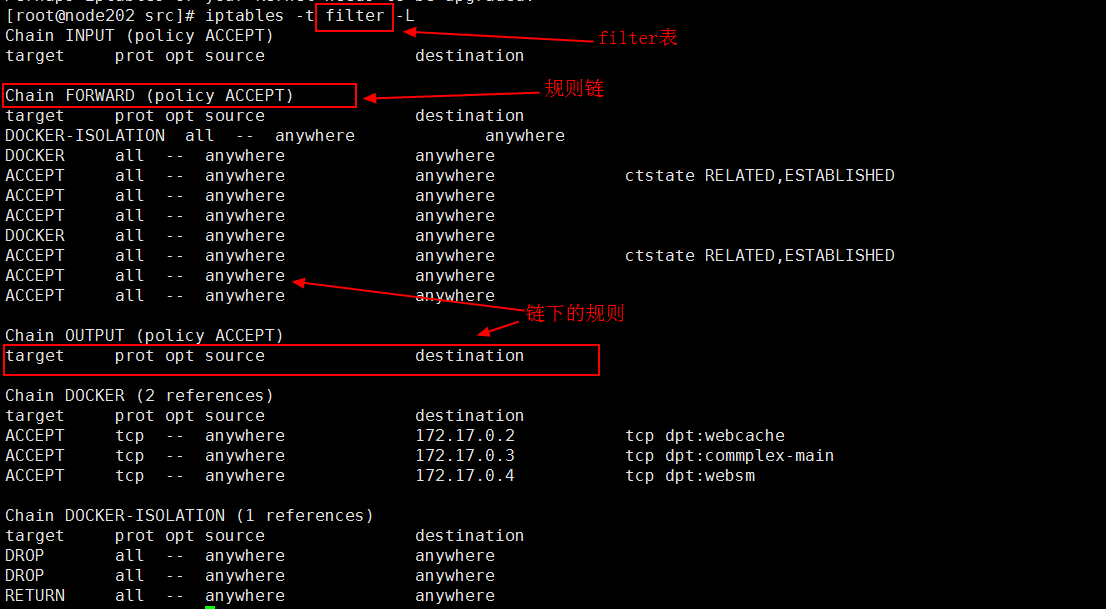
iptables对防火墙进行管理，而netfilter在真正意义上完成防火墙的功能。两者组合形成一个linux平台下免费的包过滤防火墙。两种结合可以实现封包过滤、封包重定向和网络亲地址转换。

netfilter是linux操作系统核心层内部的一个数据处理模块，它的功能有：网络地址转换，数据包内容修改，数据包过滤等。

iptables可以看做一个客户端，位于用户空间。而netfilter是一个防火墙的安全框架，位于内核空间。通过iptables将一些了的安全设定（例如规则）设定执行到netfilter中。

总结iptables是一个规则管理工具，通过iptables管理各种规则，使得内核中的netfilter能够读取相应规则并实现。

**iptables的基础概念**



1.规则

由管理员定义的条件。规则一般的定义为：“如果数据包头符合规则描述的条件，就如规则所述处理数据包”。规则存储在内核空间的信息包过滤表中。规则分别指定了源地址、目标地址、传输协议（TCP、UDP、ICMP）和服务类型等。以及规则定义的处理数据包方法，例如accept、reject、drop等。

所以配置防火墙主要就是对各种规则的管理

2、规则链

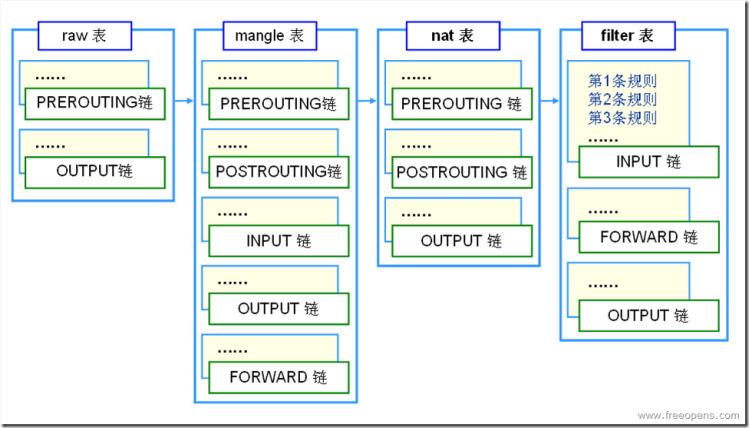
链是数据包传输的路径。一条链代表众多规则的检查清单，每条链表中可以有多条规则。一个数据包到达一个链时，iptables就会从链中第一条规则开始检查，看该数据包是否满足规则所定义的条件。如果满足，系统就会根据 该条规则所定义的方法处理该数据包；否则iptables将继续检查下一条规则，如果该数据包不符合链中任一条规则，iptables就会根据该链预先定 义的默认策略来处理数据包。

即一条链就是一系列规则组成的数据包检查与对应规则的数据包处理方法。

3、规则表

表是由多条链组成的，用于提供特定的功能，表内链的规则规则功能相近。iptables内部提供了4个表，分别是filter、nat、mangle和raw表，分别用于实现包过滤、网络地址转换、包重构、数据跟踪处理。

iptables采用了表和链分层的结构，如图所示

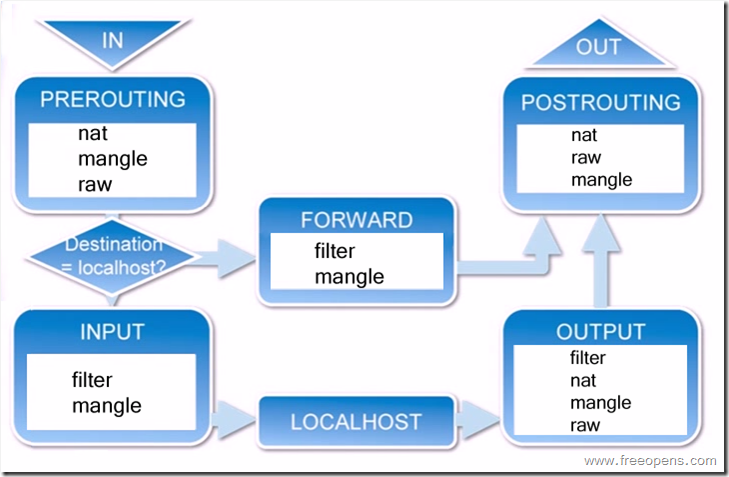


**iptables传输数据包的流程**

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。



**规则表与规则链的优先级**

4个人表的优先级由高到低依次为raw > mangle > nat > filter.

通过规则链的顺序如上图所示。

而在规则链内部次序很重要，越靠前的规则优先度越高。

在数据包经过主机时：

①首先经过prerouting规则链，而preroutinig规则链由多个表组成，若当前表不满足，则继续向下一个表的相同链匹配。

