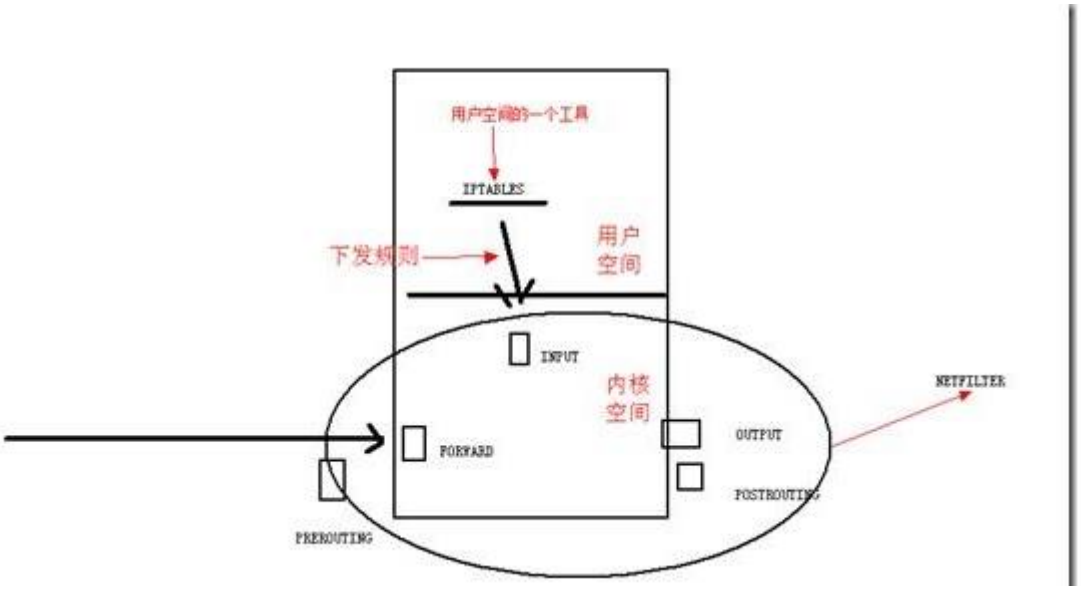
# 0x00iptables 介绍

linux 的包过滤功能，即 linux 防火墙，它由 netfilter 和 iptables 两个组件组成。

netfilter 组件也称为内核空间，是内核的一部分，由一些信息包过滤表组成，这些表包含内核用来控制信息包过滤处理的规则集。

iptables 组件是一种工具，也称为用户空间，它使插入、修改和除去信息包过滤表中的规则变得容易。

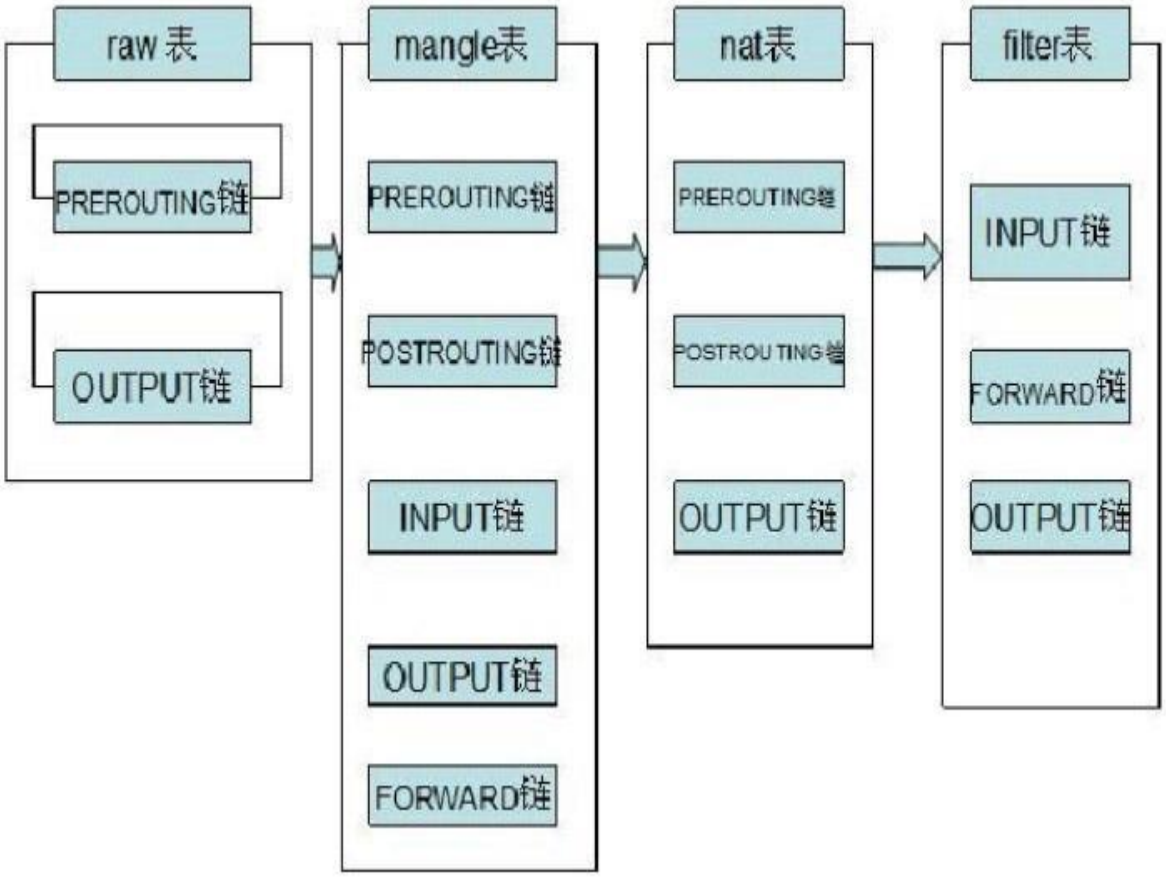



# 0x01iptables 的结构

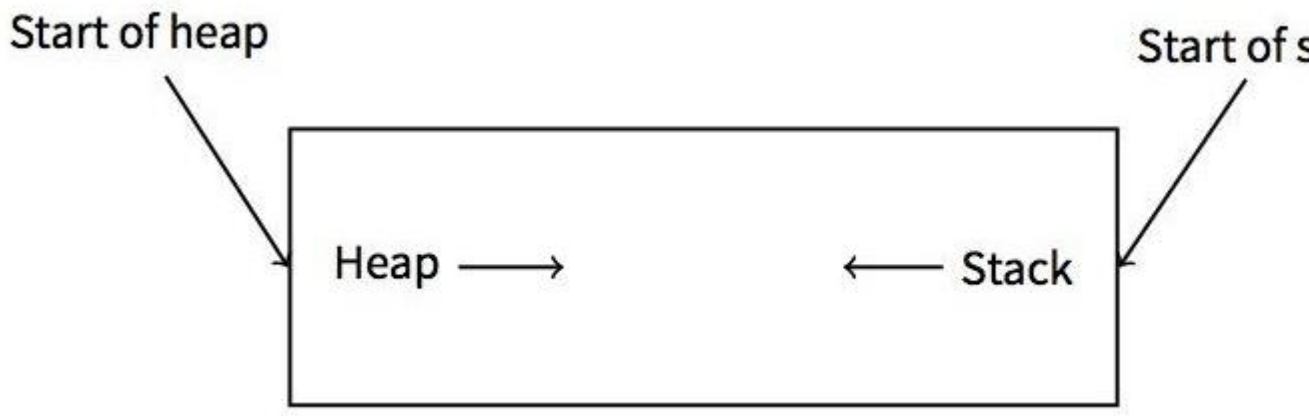
iptables 的结构：

iptables->Tables->Chains->Rules

简单地讲，tables 由 chains 组成，而 chains 又由 rules 组成。iptables 默认有四个表 Filter,NAT,Mangle,Raw，其对于的链如下图。




# 0x02iptables 工作流程




# 0x03filter 表详解

**1.在 iptables 中，filter 表起过滤数据包的功能，它具有以下三种内建链：**

> INPUT 链 - 处理来自外部的数据。
>
> OUTPUT 链 - 处理向外发送的数据。
>
> FORWARD 链 - 将数据转发到本机的其他网卡设备上。

**2.数据流向场景**

> 访问本机：在 INPUT 链上做过滤
>
> 本机访问外部：在 OUTPUT 链上做过滤
>
> 通过本机访问其他主机:在 FORWARD 链上做过滤

**3.Iptables 基本操作**

```
启动 iptables：serviceiptablesstart

关闭 iptables：serviceiptablesstop

重启 iptables：serviceiptablesrestart

查看 iptables 状态：serviceiptablesstatus

保存 iptables 配置：serviceiptablessave

Iptables 服务配置文件：/etc/sysconfig/iptables-config

Iptables 规则保存文件：/etc/sysconfig/iptables

打开 iptables 转发：echo"1">/proc/sys/net/ipv4/ip_forward
```

**0x04iptables 命令参考**

命令：

```
iptables[-t 表名]命令选项[链名][条件匹配][-j 目标动作或跳转]
```

1.表名

表名：Filter,NAT,Mangle,Raw

起包过滤功能的为表 Filter，可以不填，不填默认为 Filter

2.命令选项　选项名

功能及特点

| | |
|---|---|
| -A | 在指定链的末尾添加（--append）一条新的规则 |
| -D | 删除（--delete）指定链中的某一条规则，按规则序号或内容确定要删除的规则 |
| -I | 在指定链中插入（--insert）一条新的规则，默认在链的开头插入 |
| -R | 修改、替换（--replace）指定链中的一条规则，按规则序号或内容确定 |
| -L | 列出（--list）指定链中的所有的规则进行查看，默认列出表中所有链的内容 |
| -F | 清空（--flush）指定链中的所有规则，默认清空表中所有链的内容 |
| -N | 新建（--new-chain）一条用户自己定义的规则链 |
| -X | 删除指定表中用户自定义的规则链（--delete-chain） |
| -P | 设置指定链的默认策略（--policy） |
| -n | 用数字形式（--numeric）显示输出结果，若显示主机的 IP地址而不是主机名 |
| -P | 设置指定链的默认策略（--policy） |
| -v | 查看规则列表时显示详细（--verbose）的信息 |
| -V | 查看iptables命令工具的版本（--Version）信息 |
| -h | 查看命令帮助信息（--help） |
| --line-number | 查看规则列表时，同时显示规则在链中的顺序号 |

### 3.链名

可以根据数据流向来确定具体使用哪个链，在 Filter 中的使用情况如下：

> INPUT 链 - 处理来自外部的数据。
>
> OUTPUT 链 - 处理向外发送的数据。
>
> FORWARD 链 - 将数据转发到本机的其他网卡设备上。

### 4.条件匹配

条件匹配分为基本匹配和扩展匹配，拓展匹配又分为隐式扩展和显示扩展。

a)基本匹配包括：

匹配参数

说明

| | |
|---|---|
| -p | 指定规则协议，如tcp, udp,icmp等，可以使用all来指定所有协议 |
| -s | 指定数据包的源地址参数，可以使IP地址、网络地址、主机名 |
| -d | 指定目的地址 |
| -i | 输入接口 |
| -o | 输出接口 |

b)隐式扩展包括：

| 隐含扩展条件 | 需包含 | 扩展项 | 说明 |
| --- | --- | --- | --- |
| -m tcp | -p tcp | --sport | 源端口 |
| | | --dport | 目标端口 |
| | | --tcp-flags | 示例（SYN,ACK,RST,FIN SYN） |
| | | --syn | 第一次握手 |
| -m udp | -p udp | --sport | 源端口 |
| | | --dport | 目标端口 |
| -m icmp | -p icmp | --icmp-type | 8:echo-request 0:echo-reply |

c)常用显式扩展

| 显式扩展条件 | 扩展项 | 说明 |
| --- | --- | --- |
| -m state | --state | 用于实现连接的状态检测 NEW,ESTABLISHED,RELATED,INVALID |
| -m multiport | --source-ports | 多个源端口 |
| | --destination-ports | 多个目的端口 |
| | --ports | 源和目的端口 |
| -m limit | --limit | 速率(如3/minute 表示每分钟3个数据包) |
| | --limit -burst | 峰值速率(如100 最大不能超过100个数据包) |
| -m connlimit | --connlimit-above n | 多于n个表示满足条件取反要在选项前加! |
| -m iprange | --src-range ip-ip | 源ip范围 |
| | --dst-range ip-ip | 目的ip范围 |
| -m mac | --mac-source | mac地址限制 |
| -m string | --algo [bm\|kmp] | 匹配算法 |
| | --string “Pattern” | 要匹配的字符串 |
| | --name | 设定列表名称，默认为DEFAULT |
| | --rsource | 源地址，此为默认 |
| | --rdest | 目的地址 |
| | --set | 添加源地址的包到列表中 |

5.目标值

数据包控制方式包括四种为：

```
ACCEPT：允许数据包通过。

DROP：直接丢弃数据包，不给出任何回应信息。

REJECT：拒绝数据包通过，必须时会给数据发送端一个响应信息。

LOG：在/var/log/messages 文件中记录日志信息，然后将数据包传递给下一条规则。

QUEUE：防火墙将数据包移交到用户空间

RETURN：防火墙停止执行当前链中的后续 Rules，并返回到调用链(thecallingchain)
```

**0x05Iptables 常见命令**

a)1.删除 iptables 现有规则

```
iptables-F
```

b)2.查看 iptables 规则

```
iptables - L（iptables - L - v-n）
```

c)3.增加一条规则到最后

```
    iptables-AINPUT-ieth0-ptcp--dport80-mstate--stateNEW,E
STABLISHED-jACCEPT
```

d)4.添加一条规则到指定位置

```
    iptables-IINPUT2-ieth0-ptcp--dport80-mstate--stateNEW,
ESTABLISHED-jACCEPT
```

e)5.删除一条规则

```
    iptabels-DINPUT2
```

f)6.修改一条规则

```
    iptables-RINPUT3-ieth0-ptcp--dport80-mstate--stateNEW,
ESTABLISHED-jACCEPT
```

g)7.设置默认策略

```
    iptables-PINPUTDROP
```

h)8.允许远程主机进行 SSH 连接

```
    iptables-AINPUT-ieth0-ptcp--dport22-mstate--stateNEW,E
STABLISHED-jACCEPT

    iptables-AOUTPUT-oeth0-ptcp--sport22-mstate--stateESTA
BLISHED-jACCEPT
```

i)9.允许本地主机进行 SSH 连接

```
   iptables-AOUTPUT-oeth0-ptcp--dport22-mstate--stateNEW,
ESTABLISHED-jACCEPT

   iptables-AINTPUT-ieth0-ptcp--sport22-mstate--stateESTA
BLISHED-jACCEPT
```

j)10.允许 HTTP 请求

```
   iptables-AINPUT-ieth0-ptcp--dport80-mstate--stateNEW,E
STABLISHED-jACCEPT

   iptables-AOUTPUT-oeth0-ptcp--sport80-mstate--stateESTA
BLISHED-jACCEPT
```

k)11.限制 ping192.168.146.3 主机的数据包数，平均 2/s 个，最多不能超过 3 个

```
   iptables-AINPUT-ieth0-d192.168.146.3-picmp--icmp-type8
-mlimit--limit2/second--limit-burst3-jACCEPT
```

l)12.限制 SSH 连接速率(默认策略是 DROP)

```
   iptables-IINPUT1-ptcp--dport22-d192.168.146.3-mstate--
stateESTABLISHED-jACCEPT

   iptables-IINPUT2-ptcp--dport22-d192.168.146.3-mlimit--
limit2/minute--limit-burst2-mstate--stateNEW-jACCEPT
```

**0x06 如何正确配置 iptables**

a)1.删除现有规则

```
    iptables-F
```

b)2.配置默认链策略

```
    iptables-PINPUTDROP

    iptables-PFORWARDDROP

    iptables-POUTPUTDROP
```

c)3.允许远程主机进行 SSH 连接

```
    iptables-AINPUT-ieth0-ptcp-dport22-mstate-stateNEW,EST
ABLISHED-jACCEPT

    iptables-AOUTPUT-oeth0-ptcp-sport22-mstate-stateESTABL
ISHED-jACCEPT
```

d)4.允许本地主机进行 SSH 连接

```
    iptables-AOUTPUT-oeth0-ptcp-dport22-mstate-stateNEW,ES
TABLISHED-jACCEPT

    iptables-AINPUT-ieth0-ptcp-sport22-mstate-stateESTABLI
SHED-jACCEPT
```

e)5.允许 HTTP 请求

```
    iptables-AINPUT-ieth0-ptcp-dport80-mstate-stateNEW,EST
ABLISHED-jACCEPT

    iptables-AOUTPUT-oeth0-ptcp-sport80-mstate-stateESTABL
ISHED-jACCEPT
```

**0x07 使用 iptables 抵抗常见攻击**

1.防止 syn 攻击

思路一：限制 syn 的请求速度（这个方式需要调节一个合理的速度值，不然会影响正常用户的请求）

```
    iptables-Nsyn-flood

    iptables-AINPUT-ptcp--syn-jsyn-flood

    iptables-Asyn-flood-mlimit--limit1/s--limit-burst4-jRE
TURN

    iptables-Asyn-flood-jDROP
```

思路二：限制单个 ip 的最大 syn 连接数

```
    iptables-AINPUT-ieth0-ptcp--syn-mconnlimit--connlimit-
above15-jDROP
```

2.防止 DOS 攻击

利用 recent 模块抵御 DOS 攻击

```
    iptables-IINPUT-ptcp-dport22-mconnlimit--connlimit-abo
ve3-jDROP
```

单个 IP 最多连接 3 个会话

```
    iptables-IINPUT-ptcp--dport22-mstate--stateNEW-mrecent
--set--nameSSH
```

只要是新的连接请求，就把它加入到 SSH 列表中

```
    Iptables-IINPUT-ptcp--dport22-mstateNEW-mrecent--updat
e--seconds300--hitcount3--nameSSH-jDROP
```

5 分钟内你的尝试次数达到 3 次，就拒绝提供 SSH 列表中的这个 IP 服务。被限制 5 分钟后即可恢复访问。

3.防止单个 ip 访问量过大

```
    iptables-IINPUT-ptcp--dport80-mconnlimit--connlimit-ab
ove30-jDROP
```

4.木马反弹

```
    iptables-AOUTPUT-mstate--stateNEW-jDROP
```

5.防止 ping 攻击

```
    iptables-AINPUT-picmp--icmp-typeecho-request-mlimit--l
imit1/m-jACCEPT
```