zllong

随笔 - 2, 文章 - 0, 评论 - 0, 引用 - 0

导航

博客园
首页
新随笔
联系
订阅 XML
管理

< 2021年1月 >

日	一	二	三	四	五	六
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

随笔分类

Linux(2)

随笔档案

2017年7月(2)

阅读排行榜

1. Linux之iptables原理详解(2749)
2. iptables基础实战练习(160)

Linux之iptables原理详解

目录：

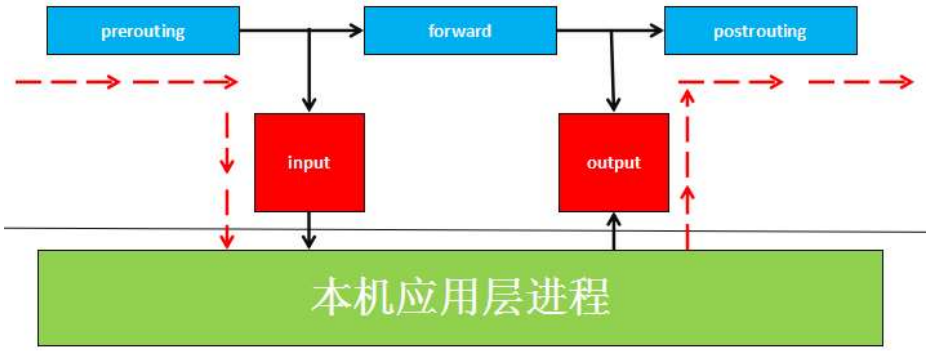
一、netfilter与iptables

（1）Netfilter是由Rusty Russell提出的Linux 2.4内核防火墙框架，该框架既简洁又灵活，可实现安全策略应用中的许多功能，如数据包过滤、数据包处理、地址伪装、透明代理、动态网络地址转换(Network Address Translation，NAT)，以及基于用户及媒体访问控制(Media Access Control，MAC)地址的过滤和基于状态的过滤、包速率限制等。Iptables/Netfilter的这些规则可以通过灵活组合，形成非常多的功能、涵盖各个方面，这一切都得益于它的优秀设计思想。

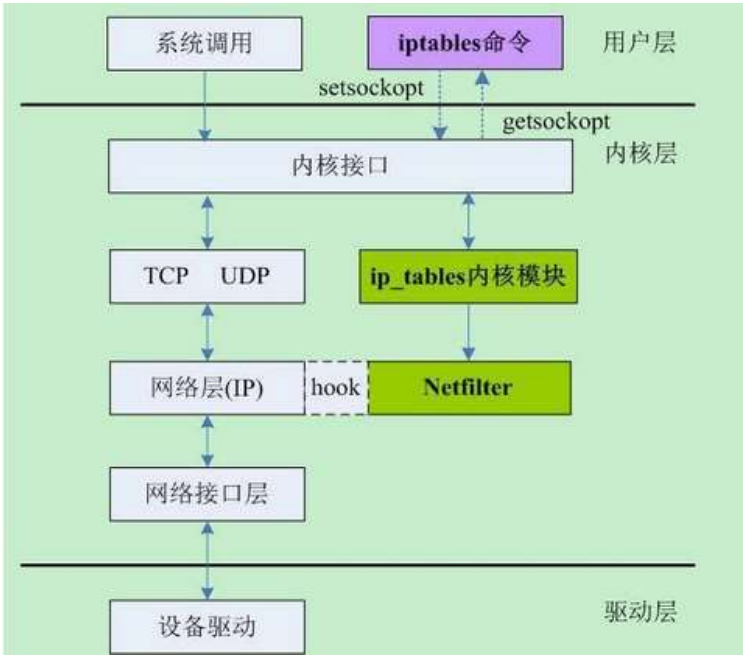
Netfilter是Linux操作系统核心层内部的一个数据包处理模块，它具有如下功能：

- 网络地址转换(Network Address Translate)
- 数据包内容修改
- 数据包过滤防火墙

（2）Netfilter 平台中制定了数据包的五个挂载点（Hook Point，我们可以理解为回调函数点，数据包到达这些位置的时候会主动调用我们的函数，使我们有机会能在数据包路由的时候改变它们的方向、内容），这5个挂载点分别是PRE_ROUTING、INPUT、OUTPUT、FORWARD、POST_ROUTING。



（3）Netfilter 所设置的规则是存放在内核内存中的，而 iptables 是一个应用层的应用程序，它通过 Netfilter 放出的接口来对存放在内核内存中的 XXtables（Netfilter的配置表）进行修改。这个XXtables由表tables、链chains、规则rules组成，iptables在应用层负责修改这个规则文件。类似的应用程序还有 firewalld 。



二、filter、nat、mangle等规则四表

（1）table有 filter、nat、mangle等规则表；

filter表

主要用于对数据包进行过滤，根据具体的规则决定是否放行该数据包（如DROP、ACCEPT、REJECT、LOG）。filter 表对应的内核模块为iptable_filter，包含三个规则链：

- INPUT**链：**INPUT针对那些目的地是本地的包
- FORWARD**链：**FORWARD过滤所有不是本地产生的并且目的地不是本地(即本机只是负责转发)的
- OUTPUT**链：**OUTPUT是用来过滤所有本地生成的包

nat表

主要用于修改数据包的IP地址、端口号等信息（网络地址转换，如SNAT、DNAT、MASQUERADE、REDIRECT）。属于一个流的包(因为包的大小限制导致数据可能会被分成多个数据包)只会经过

这个表一次。如果第一个包被允许做NAT或Masqueraded，那么余下的包都会自动地被做相同的操作，也就是说，余下的包不会再通过这个表。表对应的内核模块为 iptable_nat，包含三个链

- PREROUTING**链：**作用是在包刚刚到达防火墙时改变它的目的地址
- OUTPUT**链：**改变本地产生的包的目的地址
- POSTROUTING**链：**在包就要离开防火墙之前改变其源地址

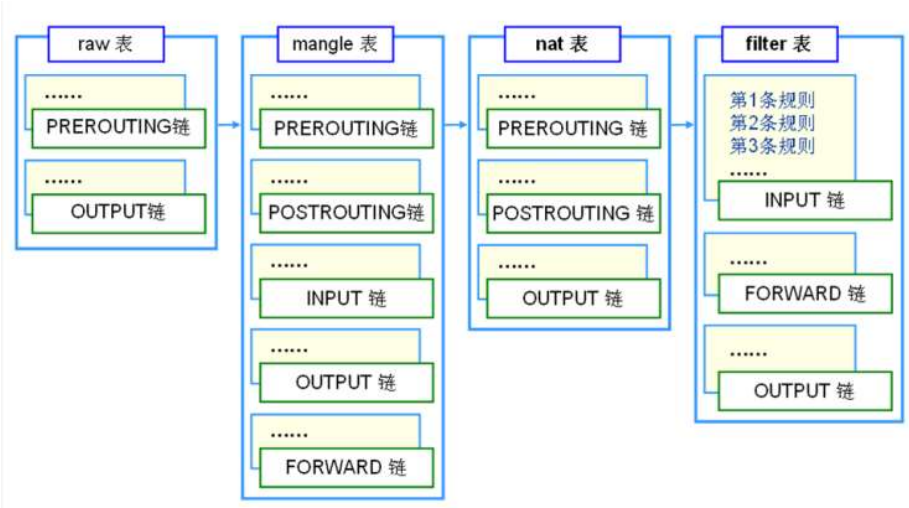
mangle表

主要用于修改数据包的TOS（Type Of Service，服务类型）、TTL（Time To Live，生存周期）指以及为数据包设置Mark标记，以实现Qos(Quality Of Service，服务质量)调整以及策略路由等

应用，由于需要相应的路由设备支持，因此应用并不广泛。包含五个规则链——PREROUTING，POSTROUTING，INPUT，OUTPUT，FORWARD。

raw表

是自1.2.9以后版本的iptables新增的表，主要用于决定数据包是否被状态跟踪机制处理。在匹配数据包时，raw表的规则要优先于其他表。包含两条规则链——OUTPUT、PREROUTING



（2）iptables中数据包和**4种被跟踪连接**的4种不同**状态：**

- NEW：该包想要开始一个连接（重新连接或将连接重定向）
- RELATED：该包是属于某个已经建立的连接所建立的新连接。例如：FTP的数据传输连接就是控制连接所 RELATED出来的连接。--icmp-type 0 (ping 应答) 就是--icmp-type 8 (ping 请求)所RELATED出来的。
- ESTABLISHED：只要发送并接到应答，一个数据连接从NEW变为ESTABLISHED,而且该状态会继续匹配这个连接的后续数据包。
- INVALID：数据包不能被识别属于哪个连接或没有任何状态比如内存溢出，收到不知属于哪个连接的ICMP错误信息，一般应该DROP这个状态的任何数据。

三、INPUT、FORWARD等规则五链和规则

（1）在处理各种数据包时，根据防火墙规则的不同介入时机，iptables供涉及5种默认规则链，从应用时间点的角度理解这些链：

- INPUT**链：**当接收到防火墙本机地址的数据包（入站）时，应用此链中的规则。
- OUTPUT**链：**当防火墙本机向外发送数据包（出站）时，应用此链中的规则。
- FORWARD**链：**当接收到需要通过防火墙发送给其他地址的数据包（转发）时，应用此链中的规则。
- PREROUTING**链：**在对数据包作路由选择之前，应用此链中的规则，如DNAT。
- POSTROUTING**链：**在对数据包作路由选择之后，应用此链中的规则，如SNAT。

```
-->PREROUTING-->[ROUTE]-->FORWARD-->POSTROUTING-->
    mangle        |       mangle        ^ mangle
     nat          |       filter        |  nat
                  |                     |
                  |                     |
                  v                     |
                INPUT                 OUTPUT
                  | mangle              ^ mangle
                  | filter              |  nat
                  v ------>local------->| filter
```

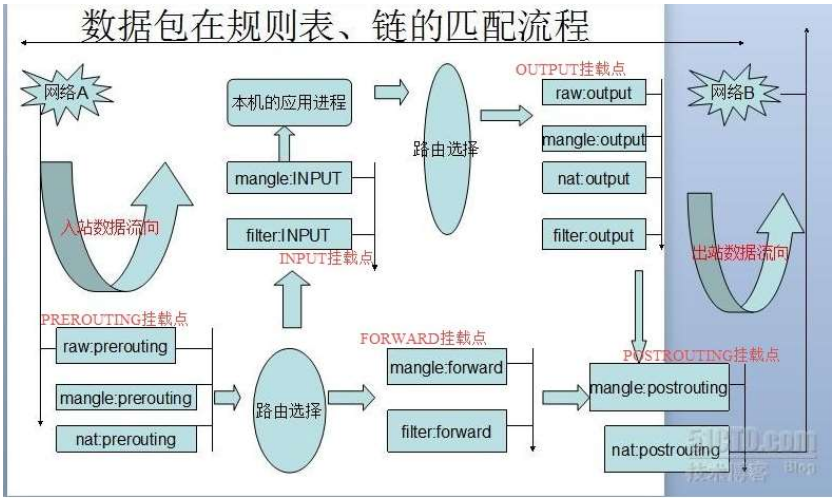
（2）其中中INPUT、OUTPUT链更多的应用在“主机防火墙”中，即主要针对服务器本机进出数据的安全控制；而FORWARD、PREROUTING、POSTROUTING链更多的应用在“网络防火 墙”中，特别是防火墙服务器作为网关使用时的情况。

四、Linux数据包路由原理

（1）理解了Netfilter和Iptables的架构和作用，并且学习了控制Netfilter行为的Xtables表的结构，那么这个Xtables表是怎么在内核协议栈的数据包路由中起作用的呢?

工作流程：网口数据包由底层的网卡NIC接收，通过数据链路层的解包之后(去除数据链路帧头)，就进入了TCP/IP协议栈(本质就是一个处理网络数据包的内核驱动)和Netfilter混合的数据包处理流程中了。数据包的接收、处理、转发流程构成一个有限状态向量机，经过一些列的内核处理函数、以及Netfilter Hook点，最后被转发、或者本次上层的应用程序消化掉。

如图：



从上图中，我们可以总结出以下规律：

- 当一个数据包进入网卡时，数据包首先进入**PREROUTING链**，在PREROUTING链中我们有机会修改数据包的DestIP(目的IP)，然后内核的"路由模块"根据"数据包目的IP"以及"内核中的路由表"判断是否需要转送出去(注意，这个时候数据包的DestIP有可能已经被我们修改过了)
- 如果数据包就是进入本机的(即数据包的目的IP是本机的网口IP)，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
- 本机上运行的程序也可以发送数据包，这些数据包经过**OUTPUT链，**然后到达**POSTROTING链输出**(注意，这个时候数据包的SrcIP有可能已经被我们修改过了)
- 如果数据包是要转发出去的(即目的IP地址不再当前子网中)，且内核允许转发，数据包就会向右移动，经过**FORWARD链**，然后到达**POSTROUTING链输出**(选择对应子网的网口发送出去)

在写iptables规则的时候，要时刻牢记这张路由次序图，根据所在Hook点的不同，灵活配置规则

五、iptables编写规则

命令格式：

	table	command	chain	Parameter & Xmatch	target
iptables	-t filter nat	-A -D -L -F -P -I -R -n	INPUT FORWARD OUTPUT PREROUTING POSTROUTING	-p tcp -s -d --sport --dport --dports -m tcp state multiport	-j ACCEPT DROP REJECT DNAT SNAT

示例：

```
1 iptables -I INPUT -s 0/0 -d 192.168.42.153 -p tcp -m multiport --dports 22,80,3306 -j ACCEPT
```

```
1 iptables -t filter -I INPUT -d 192.168.42.153 -p tcp --dport 80 -j ACCEPT
```

1.[-t 表名]：**该规则所操作的哪个表，可以使用filter、nat等，如果没有指定则默认为filter**

- -A：新增一条规则，到该规则链列表的最后一行
- -I：插入一条规则，原本该位置上的规则会往后顺序移动，没有指定编号则为1
- -D：从规则链中删除一条规则，要么输入完整的规则，或者指定规则编号加以删除
- -R：替换某条规则，规则替换不会改变顺序，而且必须指定编号。
- -P：设置某条规则链的默认动作
- -nL：-L、-n，查看当前运行的防火墙规则列表

2.chain名：**指定规则表的哪个链，如INPUT、OUPUT、FORWARD、PREROUTING等**

- [规则编号]：插入、删除、替换规则时用，--line-numbers显示号码
- [-i|o 网卡名称]：i是指定数据包从哪块网卡进入，o是指定数据包从哪块网卡输出
- [-p 协议类型]：可以指定规则应用的协议，包含tcp、udp和icmp等
- [-s 源IP地址]：源主机的IP地址或子网地址
- [--sport 源端口号]：数据包的IP的源端口号
- [-d目标IP地址]：目标主机的IP地址或子网地址
- [--dport目标端口号]：数据包的IP的目标端口号

3.-m：**extend matches，这个选项用于提供更多的匹配参数，如：**

- -m state --state ESTABLISHED,RELATED
- -m tcp --dport 22
- -m multiport --dports 80,8080
- -m icmp --icmp-type 8

4.<-j 动作>：**处理数据包的动作，包括ACCEPT、DROP、REJECT等**

- ACCEPT：允许数据包通过

- DROP：直接丢弃数据包，不给任何回应信息
- REJECT：拒绝数据包通过，必要时会给数据发送端一个响应的信息。
- SNAT：源地址转换。在进入路由层面的route之后，出本地的网络栈之前，改写源地址，目标地址不变，并在本机建立NAT表项，当数据返回时，根据NAT表将目的地址数据改写为数据发送出去时候的源地址，并发送给主机。解决内网用户用同一个公网地址上网的问题。
  MASQUERADE，是SNAT的一种特殊形式，适用于像adsl这种临时会变的ip上
- DNAT:目标地址转换。和SNAT相反，IP包经过route之前，重新修改目标地址，源地址不变，在本机建立NAT表项，当数据返回时，根据NAT表将源地址修改为数据发送过来时的目标地址，并发给远程主机。可以隐藏后端服务器的真实地址。（感谢网友提出之前这个地方与SNAT写反了）
  REDIRECT：是DNAT的一种特殊形式，将网络包转发到本地host上（不管IP头部指定的目标地址是啥），方便在本机做端口转发。
- 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

除去最后一个LOG，前3条规则匹配数据包后，该数据包不会再往下继续匹配了，所以编写的规则顺序极其关键。

分类: Linux

» 下一篇： iptables基础实战练习

posted on 2017-07-25 22:27 zllong 阅读(2750) 评论(0) 编辑 收藏

相关博文：
· linux-iptables增、删、改、保存
· Linux防火墙设置——iptables
· iptables
· Linux中的防火墙(Netfilter、Iptables、Firewalld)
· iptables详解（1）：iptables概念
» 更多推荐...

最新 IT 新闻:
· 耳朵大战，迫在眉睫
· 网传蔚来包下宁德时代磷酸铁锂电池生产线？官方回应
· OpenAI推DALL-E模型：能根据文字描述生成图片
· NASA新太空望远镜SPHEREx将揭开大爆炸的秘密
· 充不满、掉电快..."怕冷"的磷酸铁锂Model 3如何帮车主们熬过冬天?
» 更多新闻...