Netfilter开发概况

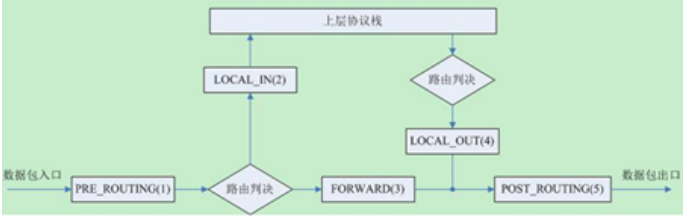
2013-04-17 23:35 by zmkeil, 734 阅读, 0 评论, 收藏, 编辑

关于Netfilter的资料网上很多，这里仅描述一些概况，把流程讲清楚，具体的细节可以很方便地跟踪到代码中去看。这个模块是构建在网络栈的网络层的，与底层架构基本没多大关系，所以要做平台间的移植也基本不需要做修改。

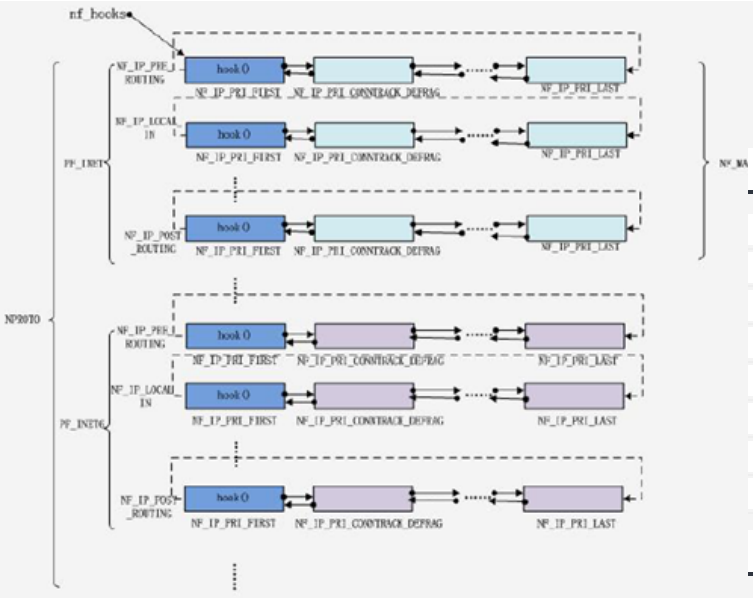
1.Netfilter框架简述

1.1框架

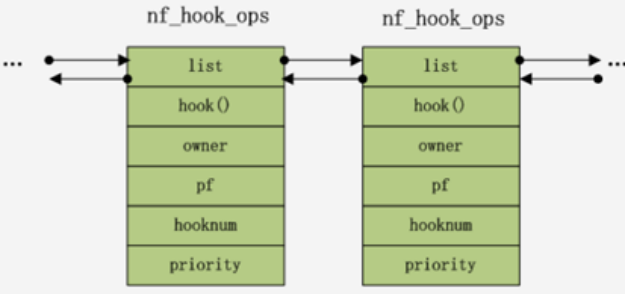
Netfilter框架的主要思想是：在网络层数据包的传递路径中，插入一些点，执行额外的功能。如下图所示：



在每个点上注册一串函数，当数据包到达该点时，依次执行这些函数，以完成filter、nat、track、mangle等功能。如下图所示：



每种协议（IPX,IPv4,IPv6,X.25等）都有自己独立的5个挂载点的函数流，它们共同构成上图所示的二维表，并以内核全局变量nf_hook来指示。表中每个节点都是一个nf_hook_ops结构，该结构中包含了协议、挂载点等信息，以及最重要的执行函数的入口。如下图所示：



1.2简易开发

内核提供一个hook注册函数nf_register_hook(struct nf_hook_ops* ops)。

下面做一个最简单的开发：然主机不接受任何IPv4的包。编写一个module，准备好一个执行函数，内容是丢弃包；然后再module_init()函数中，准备一个nf_hook_ops结构，填写其中内容：hook函数就是之前的函数，协议IPv4，挂载点LOCAL_IN；最后注册它。

编译好该module，直接insomd后，主机就不能再接受任何包了。

1.3小结

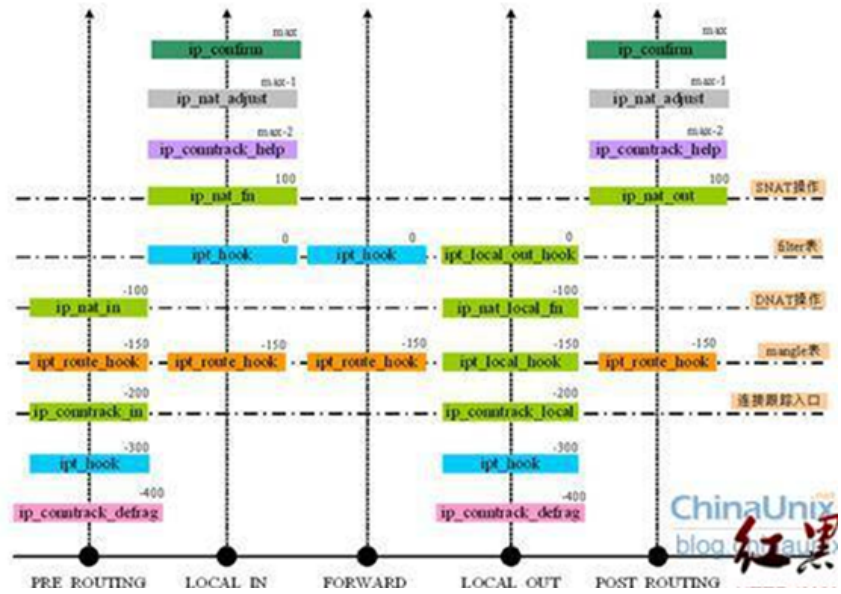
这套框架建立在网络层中间，很好地和上下协议层隔离，并且在网络层中，它也做了协议分离，即不同的协议（IP,X.25等）有不同的一套hook。这使得该框架的实现比较简单，同时也保证了很好的开放、可扩展性。对它的开发扩展也比较简单。

但正是由于这种协议隔离，也限制了它的使用范围，比如，若想实现IPv4和IPv6的互通转化，就不能用这套框架。

2.iptables简介

2.1功能介绍

Iptables是在netfilter框架下开发的，集多种功能于一身的产品，它在每个5个挂载点处挂载一些列hook，以IPv4协议为例，如下图所示：



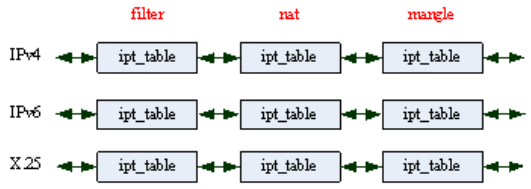
仔细去分析这些函数，联系数据包在网络层中传递的情况，可看出这些函数

3. Linux下的虚拟Bridge实现(3963)
4. OpenWRT平台搭建及简单应用(3162)
5. Linux下VLAN功能的实现(1967)

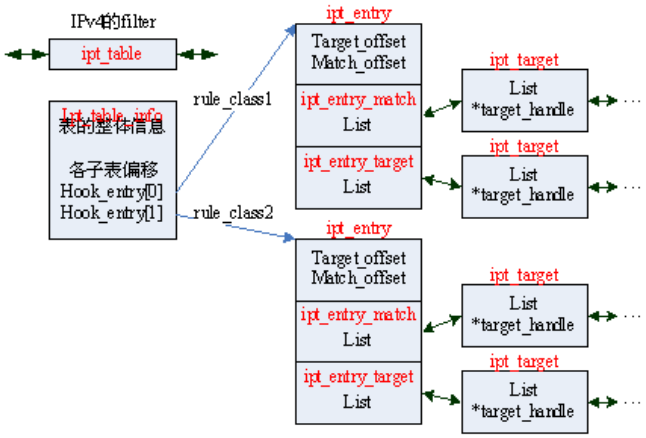
能很好地配合，同时完成数据包过滤filter，网络地址转化NAT，数据包修改mangle，链接跟踪truck等功能。

2.2规则表数据结构

光有这些函数还不行，就比如拿filter功能来说，内核还必须有数据结构来维护许许多多的规则（那些包能走，那些包不能通过等），该数据结构还要有很好的删除修改性能。Iptables是这样做的，仍然按协议分离的原则，并且每种功能的规则表独立开来。

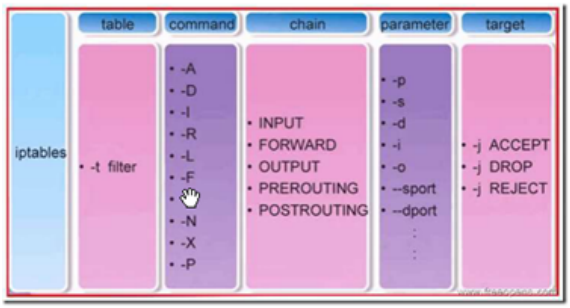


这里每个ipt_table结构中最主要的就是name，af，指明它是哪个协议、哪个功能的，另外还包含指向实际规则表的指针。这里还要注意的是，对一个功能如filter，其规则也分为不同类，如按IP地址的规则，还有按端口的规则等，这些通过下面的结构完成。



2.3用户空间命令

以上是iptables在内核空间所做的工作，它同时也提供用户空间接口，主要方便用户添加、删除规则。接口函数封转在libiptc库中。



2.4小结

Iptables的功能做得很完善了，可以在它的基础上，利用它提供的一些内核函数即数据结构，扩展一些功能，即添加ipt_table。

zmkeil
关注 - 0
粉丝 - 37

0 0

+加关注

« 上一篇：OpenWRT平台搭建及简单应用
» 下一篇：操作系统小结-Linux0.11

分类：网络相关

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 登录 或 注册，访问网站首页。

最新IT新闻：
· 华为企业云发布一年考
· 大老板的焦虑、寂寞和人才困境
· 穷游网十二年，一个老社区的演变和它的新生意
· 微软推出Android测试版Flow自动化事务处理应用
· IM企业热衷推出实体商品：Slack开售美式纹身贴纸
» 更多新闻...

最新知识库文章：
· 程序猿媳妇儿注意事项
· 可是姑娘，你为什么要编程呢？
· 知其所以然（以算法学习为例）
· 如何给变量取个简短且无歧义的名字
· 编程的智慧
» 更多知识库文章...