文章编号:1001 - 9081(2003)02 - 0105 - 02

Netfilter 功能框架及其在校园网中的应用

刘建彪 ,杨寿保
(中国科学技术大学 计算机科学技术系 ,安徽 合肥 230026)

摘 要:讨论了 Linux 2.4 内核的 Netfilter 功能框架 ,并对基于 Netfilter 框架的包过滤、网络地址转换(NAT)进行了讨论 ,最后给出了一个在校园网环境下用 Netfilter 实现的防火墙的具体实例。

关键词:Netfilter ;防火墙 ;包过滤 ;网络地址转换(NAT)
中图分类号: TP393.08 **文献标识码**:A

Function Framework of Netfilter and Application on Campus Network

LIU Jian-biao , YANG Shou-bao
(*Department of Computer Science and Technology , University of Science and Technology of China , Hefei Anhui* 230026 ,*China*)

Abstract: In this article , we have a discussion on the function framework of Netfilter embeded in linux kernel 2.4 , then we give a further discussion on the framework's packet filter and NAT ,finally ,we show an application that using Netfilter as firewall in the campus network.

Key words: Netfilter ;firewall ;packet filter ;Net Address Transfer(NAT)

1 Netfilter 基础和概念

Netfilter 是 Linux 2.4 内核实现数据包过滤、网络地址转换(NAT)、数据包处理等的功能框架。相对于原来的 ipchains 防火墙 ,Netfilter 防火墙以更好的结构重新构造 ,并实现了许多新功能。

1.1 什么是 Netfilter

Netfilter 比以前任何一版 Linux 内核的防火墙子系统都要完善强大 ,它提供了一个抽象、通用化的框架 ,该框架定义的一个子功能的实现就是包过滤子系统。在 Linux 2.4 中架设一个防火墙或者伪装网关只是 Netfilter 功能的一部分。Netfilter 框架包含以下三部分:

1) 为每种网络协议(IPv4、IPv6 等)定义一套钩子函数(IPv4 定义了 5 个钩子函数) ,这些钩子函数在数据包流过协议栈的几个关键点被调用。在这几个点中 ,协议栈将把数据包及钩子函数标号作为参数调用 Netfilter 框架。

2) 内核的任何模块可以对每种协议的一个或多个钩子进行注册 ,实现挂接 ,这样 ,当某个数据包被传递给 Netfilter 框架时 ,内核能检测是否有模块对该协议和钩子函数进行了注册。若注册了 ,则调用该模块注册的回调函数 ,这样这些模块就有机会检查(可能还会修改)该数据包、丢弃该数据包及指示 Netfilter 将该数据包传入用户空间的队列。

3) 那些排队的数据包是被传递给用户空间的异步地进行处理。一个用户进程能检查数据包、修改数据包 ,甚至可以重新将该数据包通过离开内核的同一个钩子函数中注入到内核中。

1.2 Netfilter 对数据包的处理流程

一个数据包按照如图 1 所示的过程通过 Netfilter 系统:

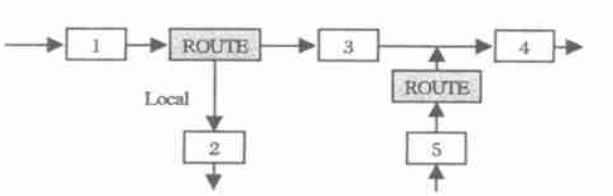

图 1 Netfilter 对数据包的处理流程

从图中可以看到一共有 5 个钩子函数 ,分别为: 1) NF-IP-PRE-ROUTING; 2) NF-IP-LOCAL-IN ; 3) NF-IP-FORWARD; 4) NF-IP-POST-ROUTING; 5) NF-IP-LOCAL-OUT。

数据包从左边进入系统 ,进行 IP 校验以后 ,数据包经过第一个钩子函数 NF-IP-PRE-ROUTING 进行处理 ;然后就进入路由代码 ,决定该数据包是需要转发还是发给本机的 ;若该数据包是发给本机的 ,则经过钩子函数 NF-IP-LOCAL-IN 处理后传递给上层协议 ;若该数据包应该被转发 ,则它被 NF-IP-FORWARD 处理 ;转发的数据包经过最后一个钩子函数 NF-IP-POST-ROUTING 处理以后 ,再传输到网络上。

本地产生的数据经过钩子函数 NF-IP-LOCAL-OUT[5] 处理后 ,进行路由选择处理 ,然后经过 NF-IP-POST-ROUTING 处理并发送到网络上。

内核模块可以对一个或多个这样的钩子函数进行注册挂接 ,并且在数据包经过这些钩子函数时被调用 ,从而模块可以修改这些数据包 ,并向 Netfilter 返回表示接受还是丢弃等的值。

2 使用 IPTables 进行数据包选择

2.1 Netfilter 的工具 IPTables

在 Linux 2.4 内核中应用了一个基于 Netfilter 框架的、称为 iptables 的数据包选择系统 ,其实它就是 ipchains 的后继工

收稿日期:2002 - 12 - 11(修改稿) **基金项目**:国家自然科学基金(90104030)
作者简介:刘建彪(1970 -) ,男 ,广东高州人 ,硕士研究生 ,主要研究方向:计算机网络及应用; 杨寿保 ,教授 ,博士生导师 ,主要研究方向:网络与信息安全、网络计算.

具,但却有更强的可扩展性。这种数据包选择系统用于实现数据包过滤(filter 表),网络地址转换(NAT 表)及数据包处理(mangle 表)。Linux 2.4 内核提供的这三种数据包处理功能都基于 Netfilter 的钩子函数和 IP 表。它们是独立的模块,相互之间是独立的,并都被完美地集成到由 netfileter 提供的框架中。

Linux2.4 提供了一个简洁强大的工具 iptables 来插入、删除、修改规则链中的规则。iptables 命令可以对所有的 IP 表进行处理,当前包括 filter,NAT 及 mangle 三个表,及以后扩展的表模块。

IPTables 命令基本上包含如下五部分,基本的语法为:

iptables - t table - Operation chain - j target match(es)

其中 table 是希望操作的表,Opetation 是具体的操作(插入、添加、删除、修改),chain 是具体的链,target 是对特定规则的目标动作,match(es)是匹配条件。

例如,希望添加一个规则,拒绝所有从任何地方到本地 SMTP 端口的连接:

iptables - t filter - A INPUT - j DROP - p tcp - - dport smtp

当然,还有其它的对规则进行操作的命令如清空表、设置表缺省策略、添加一个用户自定义的表等。

2.2 包过滤

filter 表不会对数据包进行修改,而只对数据包进行过滤。iptables 优于 ipchains 的一个方面就是它更为小巧和快速。它是通过钩子函数 NF-IP-LOCAL-IN, NF-IP-FORWARD 及 NF-IP-LOCAL-OUT 接入 Netfilter 框架的。因此,对于任何一个数据包只在一个地方对其进行过滤。这相对 ipchains 来说是一个巨大的改进,因为在 ipchains 中一个被转发的数据包会遍历三条链。

2.3 网络地址转换 NAT(Network Address Translation)

NAT 表监听三个 Netfilter 钩子函数:NF-IP-PRE-ROUTING、NF-IP-POST-ROUTING 及 NF-IP-LOCAL-OUT。NF-IP-PRE-ROUTING 实现对需要转发的数据包的目的地址进行转换。而 NF-IP-POST-ROUTING 则对需要转发的数据包的源地址进行转换。对于本地数据包的目的地址的转换则由 NF-IP-LOCAL-OUT 来实现。

NAT 表不同于 filter 表,因为只有新连接的第一个数据包将遍历表,而随后的数据包将根据第一个数据包的结果进行同样的转换处理。NAT 表被用在源 NAT、目的 NAT、伪装(是源 NAT 的一个特例)及透明代理(是目的 NAT 的一个特例)。

SNAT 可以变换数据包的源地址,例如:

iptables - t nat - A POSTROUTING - j SNAT - - to - source 1.2.3.4;

MASQUERADE 用于具有动态 IP 地址的拨号连接的 SNAT,类似于 SNAT,但是如果连接断开,所有的连接跟踪信息将被丢弃,而去使用重新连接以后的 IP 地址进行 IP 伪装,例如:

iptables - t nat - A POSTROUTING - j MASQUERADE - o ppp0;

DNAT 用于转换数据包的目的地址,这是在 NF-IP-PRE-ROUTING 钩子中处理的,也就是在数据包刚刚进入时。因此 Linux 随后的处理得到的都是新的目的地址,例如:

iptables - t nat - A PREROUTING - j DNAT - - to - destination 1.2.3.4:8080 - p tcp - - dport 80 - i eth1;

REDIRECT 重定向数据包的目的端口为 3128,和 DNAT 将目的地址修改为接到数据包的接口地址情况完全一样,例如:

iptables - t nat - A PREROUTING - j REDIRECT - - to - port 3128 - i eth1 - p tcp - - dport 80

2.4 数据包处理(Packet mangling)

mangle 表格在 NF-IP-PRE-ROUTING 和 NF-IP-LOCAL-OUT 钩子中进行注册。使用 mangle 表,可以实现对数据包的修改或给数据包附上一些额外数据。当前 mangle 表支持修改 TOS 位及设置 skb 的 nfmard 字段。

3 Netfilter 的具体应用实例

下面给出一个具体的例子来说明 Netfilter 的应用。网关由一台 PC 机充当,安装的操作系统是 RedHat 7.1,并装有两块网卡 eth0 与 eth1,其中 eth0 连接内部子网,其 IP 地址是一个内部地址 192.168.1.1,eth1 与外部 Internet 相连,eth1 的 IP 地址是 202.38.64.205。内部子网有三台 PC 机,其 IP 地址都是内部地址,分别是 192.168.1.2、192.168.1.3 与 192.168.1.4。

要实现的具体目标是内部子网的三台主机可以受限制访问外部 Internet,外部 Internet 可以访问位于 192.168.1.2 上的 WWW 服务器,但是不能访问其它两台内部子网的主机。脚本如下所示:

1) 首先清空 filter 与 NAT 表

iptables - t filter - F

iptables - t nat - F

2) 禁止内部主机在上班时上 QQ,QQ 服务器的端口号是 8000,在这里就是不转发目的端口号为 8000 的 UDP 数据包。假如想禁止内部用户访问其它服务,可以增加类似语句。

iptables - t filter - A FORWARD - p udp - - destination - port 8000 - j DROP

3) 在计算机安全领域,一种说法是阻塞所有的东西,然后当需要时才打开一些小洞小坑。就像古罗马的竞技场。下面这条语句设置网络地址转换的缺省策略为 DROP。当一个包没有找到合适的规则匹配,这时候缺省策略将会决定包的命运。

iptables - t nat - P POSTROUTING DROP

4) 内部主机通过源 NAT 访问外部 Internet,即经过防火墙的 POSTROUTING 表时数据包的源地址转换为一个合法的外部地址 202.38.64.205,这样外部连接看到的源地址都是 202.38.64.205。

iptables - t nat - A POSTROUTING - s 192.168.1.2 - j SNAT - - to 202.38.64.205

iptables - t nat - A POSTROUTING - s 192.168.1.3 - j SNAT - - to 202.38.64.205

iptables - t nat - A POSTROUTING - s 192.168.1.4 - j SNAT - - to 202.38.64.205

5) 把 192.168.1.2 这台机器设置为 WWW 服务器,外部 Internet 要想访问 WWW 服务,必须进行目的 NAT,即外部连接经过防火墙时,把目的地址与端口 202.38.64.205:80 转换为 192.168.1.2:80,这样,外部 Internet 用户在用浏览器访问 http://202.38.64.205/ 上的主页时,实际上访问的是 192.168.1.2 上的主页。

iptables - t nat - A PREROUTING - p tcp - d 202.38.64.205 - - destination - port 80 - j DNAT - - to 192.168.1.2

文章编号:1001 - 9081(2003)02 - 0107 - 03

用 RAS 拨号管理 DLL 管理拨入信息

熊 伟[1] ,丁宇征[3] ,孙 娜[2] ,钟毅芳[1]
(1. 华中科技大学 国家 CAD 支撑软件中心 ,湖北 武汉 430074 ;
2. 哈尔滨工程大学 电子与信息工程学院 ,黑龙江 哈尔滨 150001 ;
3. 中国国防科技信息中心 ,北京 100036)

摘 要:阐述了在 Windows NT4. 0/ 2000/ XP 系统下 ,通过编写 RAS 拨号管理动态链接库(DLL)对用户拨入信息进行管理的技术细节 ,并详细讨论了如何在系统服务程序中与桌面应用程序进行通信的问题。

关键词:RAS;DLL ;系统服务
中图分类号: TP391 **文献标识码**:A

Management Dial-in Information with RAS Administration DLL

XIONG Wei[1] , DING Yu-zheng[3] , SUN Na[2] , ZHONG Yi-fang[1]
(1. *National Research Center of CAD Supporting Software , Huazhong University of Science and Technology , Wuhan Hubei* 430074 *, China;*
2. *College of Electronics and Information Engineering , Harbin Engineering University , Haerbin Heilongjiang* 150001 *, China;*
3. *Defense Science and Technology Center of China , Beijing* 100036 *, China)*

Abstract: In many cases , dial-up connection as a kind of network connection approach still is very useful. This paper explains how to manage user's dial-in information by RAS administration dynamic linked library (DLL) on Windows NT4. 0/ 2000/ XP system. Beside that the problem of communicating with desktop applications in system service is discussed.

Key words: RAS;DLL ;system service

拨号连接作为进行网络连接的一种途径 ,在很多领域 ,仍然起着重要的作用。对于 RAS 服务器而言 ,如何对用户拨入信息进行管理 ,也就成了一个值得关注的问题。本文结合笔者编程实践 ,阐述了通过编写 RAS 拨号管理动态连接库(RAS Administration DLL)对用户拨入信息进行管理的技术细节 ,并详细讨论了如何在系统服务程序中与桌面应用进行通信的问题。

1 概述

从 Windows NT4. 0 开始 ,Windows 允许通过编写第三方的拨号管理 DLL 来获取拨号连接通知 ,当有客户请求接入或断开连接时 ,系统服务在进行必要的验证和连接处理后 ,会及时通知拨号管理 DLL 作进一步的处理 ,这时拨号管理 DLL 就可以通过系统服务调用 DLL 时的传入参数 ,获得拨入用户的基本信息 ,如用户名、拨入主机名等 ,对其进行管理了。

通过编写 RAS 拨号管理 DLL ,可以实现以下管理功能:

1) 在进行基本 RAS 用户认证的基础上 ,对用户拨入进行管理 ,决定是否允许该用户与 RAS 服务器建立连接。比如 ,可以通过编写拨号管理 DLL 对用户信息进行验证 ,禁止所有登录用户名第一个字符为“A”的用户的登录 ,这通过拨

收稿日期:2002 - 09 - 03
作者简介:熊伟(1978 -) ,男 ,湖北赤壁人 ,硕士研究生 ,主要研究方向:CAD、分布式系统、组件技术; 孙娜(1978 -) ,女 ,辽宁大连人 ,硕士研究生 ,主要研究方向:计算机网络与数据通信; 丁宇征(1966 -) ,男 ,江苏无锡人 ,博士后 ,主要研究方向:软件工程、计算机仿真、网络安全; 钟毅芳(1936 -) ,男 ,广西北海人 ,教授 ,博士生导师 ,主要研究方向:机械设计理论和方法、数字化设计、优化设计.

6) 允许网关上的外部地址 202. 38. 64. 205 通过防火墙访问任何地址。

```
iptables - t nat - A POSTROUTING - s 202. 38. 64. 205 - j
  ACCEPT
```

7) 最后在操作系统内核打开包转发。

```
echo 1 > /proc/ sys/ net/ ipv4/ ip-forward
```

4 结束语

Netfilter 是 Linux 2. 4 内核实现新一代的数据包过滤、数据包处理、NAT 等的功能框架 ,以更好的结构重新构造 ,并实现了许多新功能。用这样框架提供的具体工具 iptables 可以实现内部局域网和外部 Internet 之间的网关和防火墙 ,是一种简单、快速、高效 ,而且是经济的方法 ,可以广泛应用在学校、机关、中小型公司的局域网上。

参考文献

[1] 毛德操 ,胡希明. Linux 内核源代码情景分析[M]. 杭州:浙江大学出版社 ,2002.
[2] (美) Toxen B. Linux 安全 ——入侵防范、检测和恢复[M]. 前导工作室 ,译. 北京:机械工业出版社 ,2002.
[3] (美) Ross S. Linux 系统安全工具[M]. 前导工作室 ,译. 北京:机械工业出版社 ,2000.
[4] (美) Hare C ,Siyan K. Internet 防火墙与网络安全[M]. 北京:机械工业出版社 , 1998.
[5] (美) Andreasson O. Iptables Tutorial 1. 1. 9 ,2001
[6] (美) Russell. Linux iptables HOWTO ,CST ,1999.