Linux 新型内核防火墙组网分析与应用设计

刘源源

(清华大学信息网络工程研究中心,北京 100084)

摘 要: 本文首先简单地介绍了防火墙的概念及其分类,然后深入地分析了 Linux2. 4 版新型内核防火墙 netfilter 框架的工作机制及其采用 iptables 实现的方式。最后提出了用 netfilter 组建校园网络的防火墙的实现方法和实施方案。

关键词: 防火墙;Linux;netfilter;iptables

中图分类号: TP393. 08 **文献标识码**: B **文章编号**: 1002 - 4956(2003)06 - 0066 - 04

1 引言

防火墙是一种安全有效的防范技术,是访问控制机制、安全策略和防入侵措施。从狭义上来讲,防火墙是指安装了防火墙软件的主机或路由器系统;从广义上讲,防火墙还包括了整个网络的安全策略和安全行为。它是通过在网络边界上建立起来的相应网络安全监测系统来隔离内部和外部网络,以确定哪些内部服务允许外部访问,以及允许哪些外部服务访问内部服务,阻挡外部网络的入侵。随着技术的发展,防火墙的技术也在不断发展,到今天,防火墙的分类和功能也在不断细化,但总的来说,可以分为以下两大类:包过滤防火墙、应用级防火墙。

(1) 包过滤型防火墙 又叫网络级防火墙,因为它是工作在网络层。它一般是通过检查单个包的地址、协议、端口等信息来决定是否允许此数据通过。路由器便是一个"传统"的网络级防火墙。网络级防火墙简洁、速度快、费用低,并且对用户透明,但是对网络的保护很有限,因为它只检查地址和端口,对网络更高协议层的信息无理解能力。

(2) 应用级防火墙 应用级防火墙主要工作在应用层。应用级防火墙往往又称为应用级网关,它此时也起到一个网关的作用。应用级防火墙检查进出的数据包,通过自身(网关)复制传递数据,防止在受信主机与非受信主机间直接建立联系。常用应用级防火墙已有了相应的代理服务软件,如 HTTP、SMTP、FTP、Telnet 等等,但是对于新开发的应用,尚没有相应的代理服务,它们将通过网络级防火墙和一般的代理服务(如 sock 代理)。显然可知,应用级防火墙每一种协议需要相应的代理软件,使用时工作量大,效率明显不如网络级防火墙。在现在的防火墙分类中,还有"电路级网关"、"规则过滤防火墙"、"监测型防火墙"等等,但这些只是以上两大种防火墙中某一种技术上具体实现时的一种说法或

收稿日期: 2002-12-31

作者简介: 刘源源(1959—),女,工程师.

者是两种防火墙的融合。

2 Linux2.4 版新型内核防火墙的工作机制

近几年来 Linux 得到了迅速的发展,这既得益于它的自由软件属性和稳定、高效、健壮的内核,也与 Linux 是一个高性能的网络操作系统密不可分。作为一个高性能的网络操作系统,Linux 内核所内嵌的防火墙扮演着重要的角色。防火墙允许网络管理员定义一个中心"控制点"来防止非法用户,如黑客、网络破坏者等进入内部网络,还可以作为部署 NAT(Network Address Translator,网络地址变换)的逻辑地址,来隐蔽私有网络,缓解 IP 地址的短缺。在 Linux2.0 版内核中防火墙被称为 ipforward,在 2.2 版内核中为 IPchains,而在新的 2.4 版内核中则是 netfiler。

Netfilter 比以前任何一版 Linux 内核的防火墙子系统都要完善强大。Netfilter 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。Netfilter 作为中间件在协议栈中提供了一些钩子函数(Hooks),用户可以利用钩子函数插入自己的程序,扩展所需的功能。目前,基于 IPv4、IPv6 和 IPX 的 netfiter 钩子函数都已开发完成。我们在这里仅以 IPv4 为例加以说明,其它的与此类似。图 1 说明了 IPv4 中数据包经过 netfilter 的过程,从图中可以看到 IPv4 中 5 个钩子函数的放置位置,函数定义在内核头文件 linux/ netfilter-ipv4.h 中。

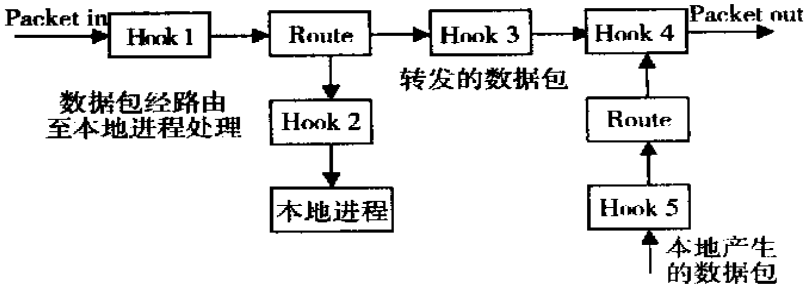

图 1 数据包经过 netfilter 的过程

图中数据包从左边进入 netfilter 框架,进行 IP 校验以后,数据包经过第一个钩子函数 Hook1(NF-IP-PRE-ROUTING),进行目的地址转换;然后就进入路由代码,其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,则该数据经过钩子函数 Hook2(NF-IP-LOCAL-IN)处理以后然后传递给上层协议;若该数据包应该被转发则它被 Hook3(NF-IP-FOR- WARD)处理;经过转发的数据包经过最后一个钩子函数 Hook4(NF-IP-POST-ROUTING),进行源地址转换,再传输到网络上。本地产生的数据经过钩子函数 Hook5(HF-IP-LO - CAL-OUT)进行 OUTPUT 包过滤,进行路由选择处理,然后经过 Hook4(NF-IP-POST-ROUTING)处理以后发送到网络上。

3 Netfilter 的实现

一个基于 Netfilter 框架的、称为 iptables 的数据包选择系统在 Linux2.4 内核中被应用,其实它就是 ipchains 的后继工具,但却有更强的可扩展性。

(1) iptables 内置规则 Linux 内核中内置的 INPUT,OUTPUT,FORWARD 规则在

新的 iptables 中,任何一个包仅仅只在这三个规则中的任何一个上应用,或者被 INPUT 规则击中,或者被 FORWARD 规则或者 OUTPUT 规则击中,不象在 ipchains 中任何一个包如果是穿过这台防火墙总要同时击中三个规则。

首先,当一个包进来的时候,也就是从以太网卡进入防火墙,内核首先根据路由表决定包的目标。如果目标主机就是本机,则直接进入 INPUT 链,再由本地正在等待该包的进程接收,结束。否则,如果从以太网卡进来的包目标不是本机,再看是否内核允许转发包(可用 echo 1 > /proc/sys/net/ipv4/ip-forward 打开转发功能),如果不允许转发,则包被 DROP 掉,如果允许转发,则送出本机,结束。这当中决不经过 INPUT 或者 OUTPUT 链,因为路由后的目标不是本机,只被转发规则应用。最后,该 linux 防火墙主机本身能够产生包,这种包只经过 OUTPUT 链出去。注意 echo 1 > /proc/sys/net/ipv4/ip-forward 和 FORWARD 链的区别,前者的意思是是否打开内核的转发功能,后者是转发链规则只有内核打开转发功能,一个包才可能被送到转发链上去逐项检查规则。如果一台防火墙没有打开前者的 IP 转发功能,则跟防火墙相连的两边的网络是完全隔离的,如果是一端连到 Internet 上,则只能通过代理访问 Internet,不可能通过 IP 伪装的方式访问。

这样,任何一个包只可能应用 INPUT/OUTPUT/FORWARD 中的一个规则,这种巨大的改进同时也简单化了防火墙规则管理。

(2) iptables 的基本命令 一个 iptables 命令基本上包含如下 5 部分:希望工作在哪个表上、希望使用该表的哪个链、进行的操作(插入,添加,删除,修改)、对特定规则的目标动作、匹配数据包条件,分别见表 1—3。

表 1 iptables 基本操作表

- A	在链尾添加一条规则
- I	插入规则
- D	删除规则
- R	替代一条规则
- L	列出规则

表 2 iptables 基本目标动作

ACCEPT	接收该数据包
DROP	丢弃该数据包
QUEUE	排队该数据包到用户空间
RETURN	返回到前面调用的链
foobar	用户自定义链

表 3 iptables 基本匹配条件

- p	指定协议(tcp/ icmp/ udp/ . . .)
- s	源地址(ip address/ masklen)
- d	目的地址(ip address/ masklen)
- i	数据包输入接口
- o	数据包输出接口

4 Netfilter 在校园网中的应用设计

某大学校园网由于业务发展需要升级改造,由原来的 100Base - T 升级为目前的 1000Base - T,学生宿舍、新教学楼都进行了综合布线,新增 400 多个信息结点,可以访问校园内部的 Intranet 和通过校园网进入 Internet。随着校园网网络规模的增大,地址资源紧张、网络安全成为急需解决的问题。考虑到价格、实用性和灵活性等各方面的因素,最后采用 Redhat7. 2(内含新版 2. 4 版内核)构造了校园网包过滤防火墙,实现了 IP 伪装(NAT)、限制对外部地址的访问等功能。

(1) 防火墙工作环境 ①Interl 服务器,安装两个网卡,分别接入 Internet 和内部网。其中一块网卡 IP 地址为:202. XXX. 20. 6,网关地址为:202. XXX. 20. 1(路由器 IP)。另一块网卡 IP 地址为:192. 168. 100. 253。网关地址为:192. 168. 100. 254(核心交换机 IP)。②操作系统:Redhat Liunx7. 2。③启动服务:iptables,httpd,samba 等。

(2) 配置防火墙系统

①在/ etc/ rc. d/ rc. local 中做如下改变:

```
# ! / bin/ sh
# This script will be executed *after * all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
/ sbin/ route add - net 192. 168. 0. 0gw192. 168. 100. 254netmask255. 255. 0. 0
# 增加到内部网的静态路由
echo 1 > / proc/ sys/ net/ ipv4/ ip-forward
# 打开 IP 包转发
/ sbin/ modprobe ip-conntrack-ftp
/ sbin/ modprobeip- nat-ftp
# 加载 NAT 需要用到的 ftp 支持模块
touch/ var/ lock/ subsys/ local
```

②在/ etc/ rc. d 中建立了 3 个控制脚本,限制内部网络用户对外部地址的访问。

a. student. sh: : 地址范围从 192. 168. 8. 0 到 192. 168. 15. 255 的 IP 地址,规划为学生宿舍使用网段,目前暂时只限防问该校园网。

(下转第 90 页)

续表

电路形式及调整难易	线性	带宽	低端死区	测点误差	适应电压摆幅及传输距离	成本比较	典型电源配置	
							隔离前	隔离后
V/F—F/V 外围器件稍多调整较易	一般	缓变信号	不存在死区	低端误差较大,最大达20.8%,输出不稳定	0～10V 可远距离传输	中档	±15V	±15V
隔离模块电路最简单 不须调整	最好	5kHz	不存在死区	误差基本上在1%以下,最大也不超过2%	0～5V 只能隔离	高	无	+15V
A/D—D/A 外围电路多调整较难	好	5kHz	基本不存在	多数测试点误差都小于1%,低端误差偏大	0～4.095V 可远距离传输	较高	+5V	+5V

[参考文献]

[1] 杨振江,蔡德芳. 新型集成电路使用指南与典型应用[M]. 西安:西安电子科技大学出版社,1998.

[2] CD-ROM 2002 Maxim Integrated Products, Inc.

[3] Agilent Technologies Inc:High-Linearity Optocouplers Technicl Data.

(上接第69页)

b. teacher.sh:地址范围从192.168.0.0到192.168.7.255的IP地址,规划为部分需要访问限制的教学、办公网络,规定可以访问Cernet所定义的免费IP地址。

c. reloadfirewall.sh:为控制重新启动NAT模块,当改变IP地址范围时,执行这个脚本使得配置立即生效。

这里只是netfiler配置防火墙的一个较为基本、简单的应用,有关netfiler的更复杂的应用,有待读者进一步去实践。

结束语 用Linux新的内核netfiler来实现内部局域网和Internet之间的防火墙,无疑是一种简单、快捷,而且经济高效的方法。只要掌握Linux的netfiler和其它相关技术,完全可以配置出一台功能强大、安全的防火墙。

[参考文献]

[1] http://www.gnumonks.org/[EB].

[2] http://netfilter.kernelnotes.org/[EB].

[3] http://chinaunix.net[EB].

[4] 刘成勇,等. Chris Hare. Internet防火墙与网络安全[M]. 北京:机械工业出版社,1998.

[5] 谢希仁,刘成勇,等. 计算机网络(第2版)[M]. 北京:电子工业出版社,1999.