

ARM 平台下 Netfilter 日志管理技术研究

刘文¹, 赵晓东², 王伟², 徐磊², 肖松海¹

(1. 新疆机电职业技术学院 电气工程系, 新疆 乌鲁木齐 830011;

2. 新疆农业大学 科学技术学院, 新疆 乌鲁木齐 830091)

摘要:市面上中小型防火墙设备的日志管理功能极为有限。为了提高行为记录的效率及功能,设计防火墙软硬件平台,提出基于 ARM 平台下的 Netfilter 日志管理技术方案和通信日志收集、发送的流程逻辑思路;调用 Linux 内核 ipt_ULOG 模块获取 Netfilter 数据包处理日志并记录于嵌入式数据库;提出了日志管理的关键函数和嵌入式数据库的设计方法,利用脚本程序处理数据库日志信息并实现远程管理。测试表明:该方案能高效、全面地实现对互联网访问行为的管理;设计方案及研究结果为嵌入式防火墙的行为记录提供了依据。

关键词:嵌入式防火墙;Netfilter 日志;ipt_ULOG 模块;行为记录;ARM S3C2440

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2011)09-0250-04

Research on Log Management Technology of Netfilter Based on ARM Platform

LIU Wen¹, ZHAO Xiao-dong², WANG Wei², XU Lei², XIAO Song-hai¹

(1. Dept. of Electrical Engineering, Institute of Xinjiang Mechano-Electrical Vocational and Technical,
Urumqi 830011, China;

2. College of Science and Technology, Xinjiang Agricultural University, Urumqi 830091, China)

Abstract: Small and medium firewall device of the log management function was extremely limited. In order to improve the efficiency and function of behavior records, firewall hardware and software platform were designed. Proposed the logical process of Netfilter log management solution and communication log collecting and sending based on arm platform; Called the ipt_ULOG module of Linux kernel to get the log of Netfilter processing data packets and recorded in the embedded database, proposed the design method of the critical functions of the log management and the embedded database, handled database log information and achieved remote management by script. Tests show: the program could achieve the behavior management of internet access effective and comprehensive. And this results provide a basis for embedded firewall behavior management and the future.

Key words: embedded firewall; log of Netfilter; ipt_ULOG module; behavior management; ARM S3C2440

0 引言

在深入研究 ARM 技术原理和防火墙技术特点的基础上,搭建了以 ARM9 处理器为核心的防火墙硬件平台及其资源配置模块,针对 S3C2440 处理器研究了 Linux 内核裁减、移植和 Netfilter 调试方法,并在此基础上开发了相应的应用程序。建立的防火墙很好地满足了当前中小型网络环境的需求,在性能和功能方面有效地弥补了当前各类厂商中小型防火墙设备的不足之处,同时市面上中小型防火墙设备对数据包处理的日志管理功能极为有限^[1],尤其是缺乏对互联网访问

的行为记录功能。为此,文中在做了大量前期工作的基础上针对 ARM 平台下 Netfilter 日志管理技术做了深入研究,提出了 Netfilter 日志管理技术方案,并且通过了具体测试,取得了较好效果。

1 硬件平台设计

防火墙硬件平台的核心板主要包括:核心 CPU、Flash 存储器、SDRAM 存储器、IDE 接口、电源监控及复位电路、时钟驱动电路、网络接口、调试接口电路、系统供电电路、RS232 接口电路等。

系统上电后,电源监控及复位电路开始工作,产生复位信号。之后,核心板的 CPU 开始启动,此时 S3C2440 开始读取数据线上的值并初始化 CPU,主要包括存储器初始化、中断向量初始化、调试寄存器初始

收稿日期:2011-03-03;修回日期:2011-07-01

基金项目:新疆维吾尔自治区高校科研计划资助(XJEDU2010S48)

作者简介:刘文(1982~),男,四川广安人,讲师,硕士,主要研究领域为计算机应用技术(嵌入式系统)。

化等^[2]。当所有的硬件环境初始化完毕后,系统会将控制权交给存储在 Flash 中的 Linux 操作系统,通过操作系统管理系统中的所有硬件及任务。通过操作系统的调度来实现核心板管理以及实现硬件防火墙的路由、网关、内容过滤和日志管理等功能,而 Netfilter 对数据包处理的日志存储在 SD 卡和 IDE 存储设备中。

2 软件平台设计

系统的软件设计包括防火墙端系统、服务进程管理,日志的收集、发送,管理端配置系统及日志管理系统等模块。

防火墙端系统、服务进程管理模块:运行在防火墙 Linux 系统上的服务器端模块,接收客户端模块传来的控制和管理指令,然后针对 Netfilter 模块配置 Linux 系统的 iptables 规则和执行其他系统管理命令,比如重启防火墙,系统时间同步等^[3]。

日志的收集、发送模块:防火墙主机上运行日志收集、发送守护进程,将所有的系统日志通过 Netfilter 监视、行为记录模块 ipt_ULOG 发送到嵌入式数据库 SQLite。

管理端配置系统:通过 CGI 接口程序管理防火墙软硬件系统及嵌入式数据库内的日志,基于 B/S 结构设计,提供良好的图形用户界面,便于操作人员管理防火墙及监控系统运行情况。

日志管理系统模块:通过日志管理模块对系统安全日志及 Netfilter 行为日志查询和审计,管理日志收集发送和相关配置。

日志收集、发送及相关模块结构如图 1 所示。

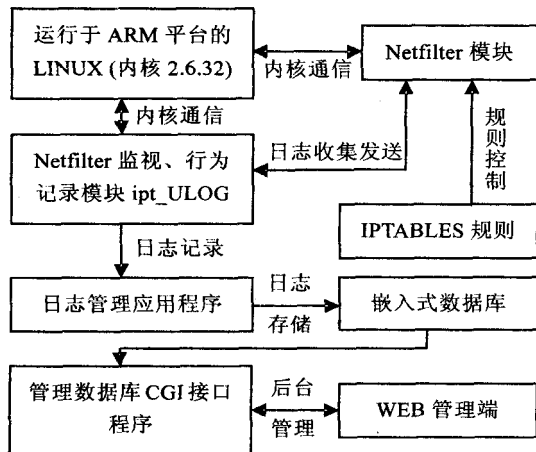


图 1 日志处理相关功能模块结构图

3 Netfilter 日志接收及发送流程逻辑设计与实现

3.1 Linux netlink 机制分析

Linux netlink 作为一种用户空间和内核空间通信

的机制,可以完成内核和用户通信以及以 IPC 机制完成进程间通信^[4]。netlink 定义了一个框架用来传递数据,而内核不解析策略只实现机制,所有策略由用户空间实现。与网络套接字一样,netlink 使用了 sk_buff 结构体,没有涉及 sk_buff 里面的标准字段,而仅用了一个扩展的 cb 字段,cb 在 sk_buff 的定义是 char cb [40],在 netlink 模块里的 NETLINK_CB 宏就是取自 cb 字段,所以可以用 netlink 向任何执行实体传输任何数据,不限于本机^[5]。

3.2 日志收集、发送的流程逻辑思路

日志管理进程运行后,系统自动解析用户设定的日志记录配置文件并与 ipt_ULOG 模块建立通信连接,随后创建接收 ipt_ULOG 模块数据的 netlink 套接字,然后初始化系统状态日志记录模块、初始化输出插件并判断其日志保存方式。使用无限循环来接收并处理内核传来的数据,如果系统收到终止信号,就结束日志管理进程^[6]。其工作流程设计如图 2 所示。

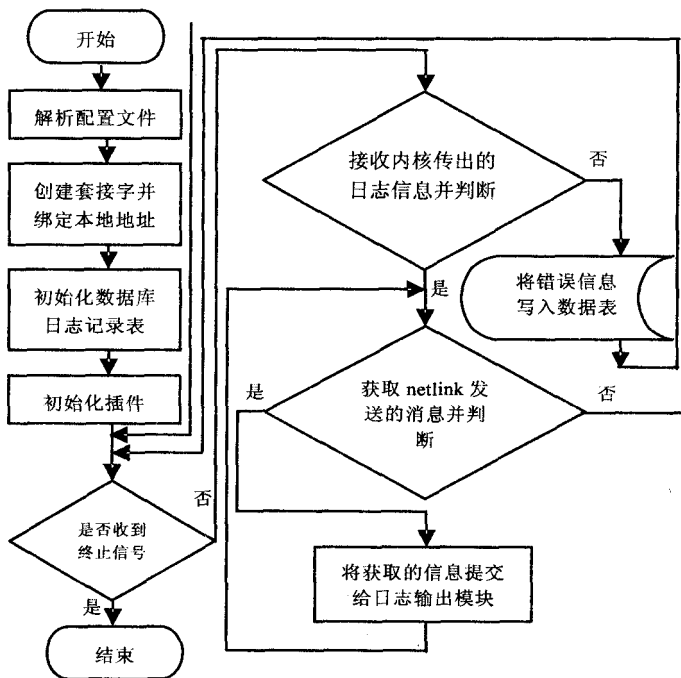


图 2 日志收集、发送流程图

3.3 Netfilter 日志接收及发送代码实现

针对日志收集、发送的流程图实现具体代码。初始化全局变量,创建 netlink 套接字,注册 netlink target 部分代码如下:

```
static int __init init(void)
{
    int i;
    DEBUGP("ipt_ULOG: init module\n");
    if (nlbufsiz >= 64 * 1024) {
        printk("Netlink buffer has to be <= 64kB\n");
        return -EINVAL;
    }
    for (i = 0; i < DATA_MAXNLGROUPS; i++) {
```

```

init_timer(&DATA_buffers[i].timer);
data_buffers[i].timer.function = data_timer;
data_buffers[i].timer.data = i; }
nflognl = netlink_kernel_create(NETLINK_NFLOG,
NULL);
if (!nflognl)
return -ENOMEM;
if (ipt_register_target(&ipt_data_reg) != 0) {
sock_release(nflognl->sk_socket);
return -EINVAL; }
if (nflog)
nf_log_register(PF_INET, &ipt_logfn);
return 0; }

```

netlink 通过调用 API netlink_broadcast 函数实现发送数据包,同时删除定时器、清除标志变量、修改部分起控制作用的成员的值等,其部分代码如下:

```

static void data_send(unsigned int nlgroupnum)
{
data_buff_t *ub = &data_buffers[nlgroupnum];
if (timer_pending(&ub->timer)) {
DEBUGP("ipt_ULOG: data_send: timer was pending, deleting\n");
del_timer(&ub->timer); }
if (ub->qlen > 1)
ub->lastnlh->nmsg_type = NLMSG_DONE;
NETLINK_CB(ub->skb).dst_groups = (1 << nlgroupnum);
ub->qlen, nlgroupnum);
netlink_broadcast(nflognl, ub->skb, 0, (1 << nlgroupnum), GFP_ATOMIC);
ub->qlen = 0; ub->skb = NULL; ub->lastnlh = NULL;
};

```

4 日志管理功能模块设计

4.1 关键函数与 ipt_ULOG 模块通信的实现

日志管理程序按照图 1 描述的流程设计,包含了与 ipt_ULOG 模块通信的函数与参数、日志存储方式、排错处理等;进程启动时,读取配置文件中的函数值决定程序的输出方式以及日志记录的等级和方式等。部分的函数、参数功能描述及取值情况见表 1。

程序段举例:ub->datalen 是当前 netlink group 编号下已经收聚的队列的长度,指定的 queuethreshold 是需要收集的阈值,当达到这个值时,将其发送至用户空间。

```

if (ub->datalen >= loginfo->queuethreshold) {
if (loginfo->queuethreshold > 1)
nlh->nmsg_type = NLMSG_DONE;
data_send(Group_no);
}

```

表 1 日志管理的关键函数、参数功能描述

关键函数、参数	功能描述及取值范围
Group_no()、Groupnu	应用程序绑定 netlink 的组播号,取值范围 1~32
Log_file	读取程序状态信息,包括程序启动、关闭、出错及连接数据库的运行信息
Log_level	通信日志等级,debug(1)、info(3)、notice(5)、error(7)、fatal(8),设置默认记录等级为 3
Re_mem()、Memsize	Netlink 接口接收数据函数及可接收数据缓存值,最小及最大值参照内核 buffer 和 rmem_max 值
Pulgin	插件选项,控制信息的输出方式;包括对 SQLite3 数据库的操作方式,基于 ipv4 协议的协议头、AH 和 ESP 协议头信息,对本地日志文件的支持等 ^[7]
Data_sync()、sync	刷新缓冲区数据函数及默认值

4.2 日志存储流程实现

为了保证整个系统的安全性、可靠性以及数据更新的实时性,将引导程序、嵌入式 Linux、busybox 等烧写在 Nand Flash 芯片第一、第二、第三分区上,文件系统采用 cramfs;将嵌入式数据库 SQLite 移植到 Nand Flash 第四分区上,文件系统采用 Yaffs2;数据表、日志数据及 CGI 接口程序等存储在容量较大的 IDE 设备之上,文件系统采用 Reiserfs。

日志管理程序在解析配置文件时加载数据库应用模块 output_SQLITE3.so,根据 SQLite 数据库连接信息(包括数据库主机地址、用户名、密码、权限等)连接数据库^[8]。建立连接后,获取指定的数据表中的字段名,根据这些字段名,将日志信息输出为特定的格式,并将这个指定格式的信息写入 SQLite 数据库服务器中对应的字段,日志存储流程见图 3。

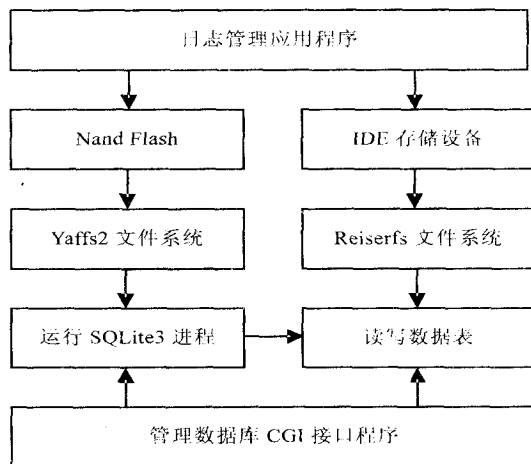


图 3 日志存储流程

SQLite 数据表关键字段及功能描述见表 2。

4.3 管理端设计

在 ARM 平台上,移植嵌入式 WEB 服务端程序 BOA、PHP 运行环境和嵌入式数据库 SQLite,完成 BOA、PHP 和 SQLite 的整合^[9];在防火墙端解析 CGI 接口程序和处理数据表信息(Netfilter 日志数据);动

态管理程序利用 PHP 语言开发,主要功能是处理数据表各字段记录、解释客户端请求等,利用标准输出把处理结果发送到 BOA 服务器,最后将日志信息传递到客户端浏览器上;采用 HTTP 验证的方式登陆防火墙日志管理系统,有效地增强了系统的安全性^[10]。

表 2 数据表关键字段及功能描述

字段名称	数据类型	功能描述
Client_mac	VARCHAR(80)	记录连接防火墙主机的 mac 地址
oob_time_sec oob_time_usec	INT UNSIGNED	统计传输层协议使用带外数据发送数据的时间
ip_srcaddr ip_dstaddr	INT UNSIGNED	记录源、目标 IP 地址
ip_protocol	TINYINT UNSIGNED	记录 IP 协议
ip_totlen	SMALLINT UNSIGNED	记录 IP 头长度
tcp_sreport tcp_dstport	SMALLINT UNSIGNED	记录 tcp 源及目标端口
udp_sreport udp_dstport	SMALLINT UNSIGNED	记录 udp 源及目标端口
icmp_type	TINYINT UNSIGNED	记录 icmp 相关信息

5 日志管理功能测试

测试方法:设置防火墙 IP 地址为:192.168.1.8,在管理端编写记录访问本机 SSHD、WEB 服务的 Netfilter 规则代码,客户机(地址为:192.168.1.191)访问防火墙 22、80 端口,日志管理端主要记录客户机访问防火墙数据包大小、访问时间、源地址、目标地址、源端口及目标端口等^[11]。测试规则部分代码如下:

```
iptables -N syn-flood
iptables -A INPUT -i $ { FIREWALL_DEVICE } -p tcp --syn -j syn-flood
iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
iptables -A syn-flood -j DROP
iptables -N LOG_SSHD_WEB
iptables -A INPUT -s $ { CLIENT_DEVICE } -p tcp --dport 22 -j LOG_SSHD_WEB[12]
iptables -A INPUT -s $ { CLIENT_DEVICE } -p tcp --dport 80 -j LOG_SSHD_WEB
.....
iptables -A LOG_SSHD_WEB -j DROP
```

日志信息最终通过 WEB 服务器传递到客户端浏览器上,图 4 展示了日志管理的部分功能,包括 TCP 数据包的连接信息、不同时间段的数据包流量、数据包的大小等细节内容。

6 结束语

提出了基于 ARM9 平台的防火墙硬件构架,软件平台基于 Linux,采用嵌入式操作系统和动态数据分类

存储的机制,将互联网访问行为日志记录在大容量存储介质上,数据可长时间保存。提出了 Netfilter 日志接收及发送流程逻辑,并编写了程序;对日志管理方案做了深入分析,提出思路并做了具体的实现;移植嵌入式数据库、WEB 服务器、PHP 执行环境等,编写了相应的日志记录规则并开发了应用程序,最终实现了对 Netfilter 日志的有效管理,通过了具体测试。

TCP 数据包 :				(0 , 9)		平均数据包流量	
22	139	22/11/10 01:20:54	23/11/10 00:38:27			1 min :	0.2834 pkt/s
80	95	22/11/10 01:21:34	22/11/10 01:24:28			5 min :	0.8764 pkt/s
						15 min :	2.5543 pkt/s

数据大小	源地址	目标地址	协议	动态端口	目标端口	访问日期
345	192.168.1.191	192.168.1.8	tcp	4035	http	22/11/10 01:24:23
342	192.168.1.191	192.168.1.8	tcp	4035	http	22/11/10 01:24:18
341	192.168.1.191	192.168.1.8	tcp	4035	http	22/11/10 01:24:18
414	192.168.1.191	192.168.1.8	tcp	2581	ssh	23/11/10 00:38:26
413	192.168.1.191	192.168.1.8	tcp	2581	ssh	23/11/10 00:38:26
412	192.168.1.191	192.168.1.8	tcp	2581	ssh	23/11/10 00:38:26

图 4 效果展示

参考文献 :

- [1] 刘 文,阎晓菲,王卫平,等.基于嵌入式 uClinux 路由器的防火墙设计[J].新疆农业大学学报,2009(5):84-87.
- [2] 尹家生,周 健,辜丽川.基于 Linux 的高速网络流量采集与分析模型研究[J].计算机工程与应用,2006(10):118-120.
- [3] 周功业,吴 彬.基于 NAT 扩展的 PnP 网络[J].计算机工程与科学,2005,27(7):13-15.
- [4] 曹利峰,陈性元,杜学绘.基于 Netfilter 框架的 VPN 网关的一体化设计[J].计算机工程与应用,2006,42(2):130-131.
- [5] 马 博,袁 丁.基于 Linux 驱动级内核访问监控技术研究及实现[J].计算机应用,2009,29(9):237-239.
- [6] Babbin J,Biles S,Orebaug A D.Hsnort Cookbook[M].[s.l.]:O,Reilly,2005:12-22.
- [7] Karagiannis T,Broido A,Faloutsosm,et al.Transport layer identification of P2P Traffic[C]//Proc of Internet easurement conference.[s.l.]:[s.n.],2004.
- [8] 刘 雷,赛 英,王 帅.NAT-PT 转换网关在 netfilter 框架中的实现[J].计算机工程与设计,2007(2):73-76.
- [9] 聂朝恩,高荣芳.一种 Linux 平台上基于包过滤的网络流量采集系统[J].计算机应用,2007,27(8):185-188.
- [10] 陈海军,李仁发,杨 磊.基于 Linux 内核扩展模块的 P2P 流量控制[J].计算机工程,2007(1):176-178.
- [11] 刘 文.Netfilter 数据转发性能测试与研究[J].计算机工程与应用,2011(3):61-62.
- [12] 刘 文,赵晓东,肖松海,等.基于 ARM 平台的引导程序分析与移植研究[J].软件导刊,2011(2):26-28.