基于 S3C2440 的嵌入式 IPv6 防火墙设计①

苏义鑫 王树佳 王 雁 (武汉理工大学 自动化学院 湖北 武汉 430070)

摘 要: 随着网络应用的不断发展，网络安全显得越来越重要。基于 X86 架构的边界防火墙成本较高，且难以遍布网络的每一个终端设备，无法构建全方位的安全防护网络。本文针对以上问题，设计了一种基于 S3C2440 嵌入式 IPv6 防火墙，并且提出了状态跟踪与智能包过滤相结合的动态包过滤方案。该方案通过智能访问控制技术优化包过滤规则集，从而提高了防火墙的吞吐量和安全性。

关键词: 防火墙; 嵌入式系统; IPv6; 智能访问控制技术; 动态包过滤; 网络安全

Design of Embedded IPv6 Firewall Based on S3C2440

SU Yi-Xin, WANG Shu-Jia, WANG Yan

(Institute of Automation, Wuhan University of Technology, Wuhan 430070, China)

Abstract: With the continuous development of network applications, network security becomes increasingly important. Boundary firewall based on x86 architecture is expensive and difficult to protect each terminal equipment .It can not build comprehensive security network. So this paper designs an embedded IPv6 firewall based on S3C2440 processor to solve the problems. This paper also gives a solution which combines SPI (Stateful Packet Inspection) and intelligent packet filtering into dynamic packet filtering mechanism. The solution optimizes packet filtering rule set by using intelligent access control technology. It also enhances the throughput of firewall and security.

Keywords: firewall; embedded system; IPv6; intelligent access control technology; dynamic packet filtering; network security

1 引言

在众多的网络安全设施中，防火墙是行之有效的重要网络安全设备，通过对网络通信进行筛选屏蔽以防未经授权的访问进出计算机网络[1]。防火墙是位于可信网络和不可信网络之间的一道安全屏障，其最核心的任务就是管理和控制进出网络的通信量，它可以截获中途传输的数据包并进行处理，然后与事先定义好的安全策略规则相比较，并最终决定转发或丢弃该数据包。传统的防火墙通常位于一段网络的边界，它可以很好的过滤外界用户对内部网络的访问，但对内部网络的攻击却无能为力。针对此问题近年来关于新型防火墙的研究有很多，如分布式防火墙系统[2]，嵌入式防火墙系统等。这些系统的目的是将防火墙的边界延伸，使其能够遍布网络的每一个终端设备，构建全方位的安全防护网络。

现有防火墙系统大多是针对于 IPv4 开发的，由于 IPv4 地址空间不足，且安全性较差，现有网络升级到 IPv6 是大势所趋。IPv6 作为下一代网络的基础以其海量的地址空间和较强的安全特性得到广泛的认可[3]，因此研究支持 IPv6 协议的防火墙是很有必要的。

以 Intel Xscale IXP425 为核心处理器设计的嵌入式 IPv6 防火墙[4]，较好的实现了对网络中的数据包进行动态过滤。但其成本较高，且 IXP425 强劲的网络处理性能在网络终端的应用中无法得以完全发挥。

① 基金项目:湖北省自然科学基金(2009CDB082)
收稿时间:2010-03-25;收到修改稿时间:2010-04-27

基于 U 盘的嵌入式防火墙[5]使用方便，设计新颖，但其需要依附于 x86 电脑硬件平台，且 U 盘的可靠性较差，不适于长期使用。

通用 ARM 处理器有较高的性价比和较多的软件支持，已广泛应用于生产生活的各个领域。本文通过对 IPv6 协议、IPv6 安全机制[6]和防火墙技术等方面的分析和研究，结合现有防火墙的特点，设计并实现了一个基于 S3C2440 的嵌入式 IPv6 防火墙系统。下面从硬件设计、软件设计和核心模块设计几个方面介绍该基于 S3C2440 的嵌入式 IPv6 防火墙。

2　嵌入式IPv6防火墙的硬件设计

嵌入式 IPv6 防火墙的硬件设计如图 1 所示，其主控芯片采用三星公司的 32 位嵌入式处理器 S3C2440[7]。该处理器以 ARM920T RISC 为核心，标准工作频率为 400MHZ(最高工作频率：533MHZ)，运算能力为 450MIPS，有强劲的处理能力。

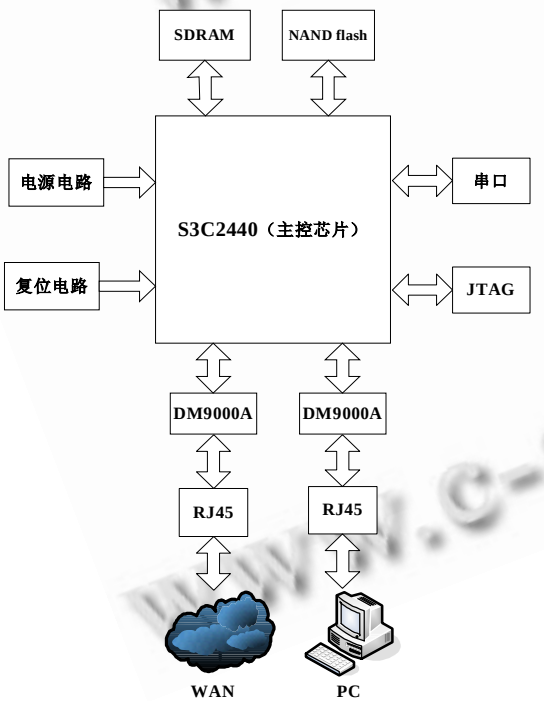

图 1　嵌入式 IPv6 防火墙硬件框图

S3C2440 处理器内部结构复杂，功能强大，片上集成了很多硬件资源。如：外部存储控制器，USB 接口，UART 接口，内部定时器，130 个通用 I/O 接口，24 通道外部中断源等。如此丰富的接口资源，可以很方便实现硬件电路的扩展。此外 S3C2440 支持 ARM920T 强大的指令集系统，具有独立的内存管理单元(MMU)，支持 NAND Flash 启动引导，可以方便的实现 Bootloader 和嵌入式操作系统的移植。

系统的存储单元主要包括 SDRAM 存储器和 Flash 存储器。SDRAM 为系统程序的运行提供内存空间，本系统采用两片 HY57V561620FTP-H(32M)并联，容量可达 64MB。Flash 用来存储程序，Flash 分为 NOR 型和 NAND 型 2 种。NOR 型 Flash 工艺复杂，成本较高，其优点是片内可执行应用程序，多用于存储系统的 Bootloader 引导程序。NAND 型 Flash 具有极高的存储密度和较快的写入和擦除速度且成本较低，适用于存储大容量数据和文件。考虑到 S3C2440 支持 NAND Flash 启动引导，故本系统选用 K9F1208U0M-YCB0(64MB)的 NAND 型 Flash 作为系统的 Flash 存储器。

系统的以太网接口单元采用 2 颗 10M/100M 自适应以太网控制器 DM9000A。DM9000A 芯片是 DEVICOM 公司研发的一款低功耗，高度集成，成本较低的单芯片快速以太网芯片，在嵌入式领域中使用非常广泛。它集成了物理层接口(PHY)、以太网媒体介质访问控制器(MAC)和外部处理器总线接口等。3.3V 的工作电压，降低了系统的功耗。DM9000A 的高度集成简化了系统以太网电路的硬件设计，特别适合作为嵌入式 IPv6 防火墙的网络接口。

3　嵌入式IPv6防火墙的软件设计

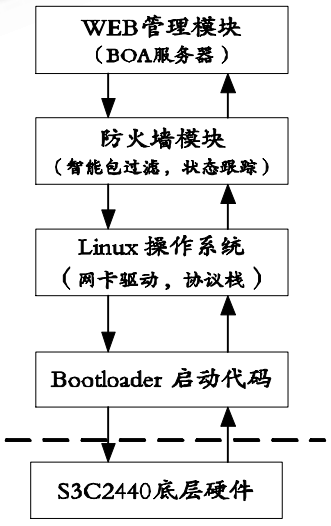

图 2　嵌入式 IPv6 防火墙软件层次结构图

嵌入式 IPv6 防火墙系统的软件编写采用了模块化程序设计的方法。模块化编程有利于程序设计任务的划分，使程序易于编写和调试，便于检验和维护。本系统将启动代码(Bootloader)，Linux 操作系统(网卡驱动、协议栈)，防火墙模块(智能包过滤，状态跟踪等)和 WEB 管理模块(Boa 服务器)都编写成独立模块。系统软件层次结构如图 2 所示。

第一层：启动代码(Bootloader)。它是芯片复位后进入操作系统之前执行的一段代码，主要是为操作系统的启动提供基本的运行环境，如初始化 CPU、初始化存储器系统等。本系统选用 U-Boot 作为系统的 Bootloader。

第二层：Linux 操作系统，屏蔽了对底层硬件的具体操作，为上层应用提供了丰富的支持，包括底层设备驱动，网卡驱动和网络协议栈等。在 Linux 操作系统下，开发者只需关注于应用软件编程，大大节省了系统的开发时间。

第三层：防火墙模块(智能包过滤[8]，状态跟踪[9]等)，该模块是嵌入式防火墙系统的核心，其包括动态 NAT 模块：负责对进出防火墙的数据包进行地址翻译；状态跟踪模块：维护网络的会话连接信息，协助智能包过滤模块进行连接状态的跟踪，是实现状态检测包过滤(动态包过滤)的关键模块；智能包过滤模块：根据访问控制表(ACL)对进出网络的数据包进行过滤，并对过滤规则进行统计，记忆和决策，动态优化过滤规则优先级列表，实现高速高效的包过滤处理功能。

第四层：WEB 管理模块，以 CGI 语言为基础，构建 Boa 服务器平台。通过该模块用户可以方便地查看防火墙日志，添加或修改过滤规则，调整过滤规则的优先级，监控防火墙网络状态等。

4 防火墙核心模块设计

一个防火墙能否起到较好的过滤效果关键在于防火墙的核心过滤模块设计。本防火墙的核心过滤模块整体工作流程如图 3 所示。

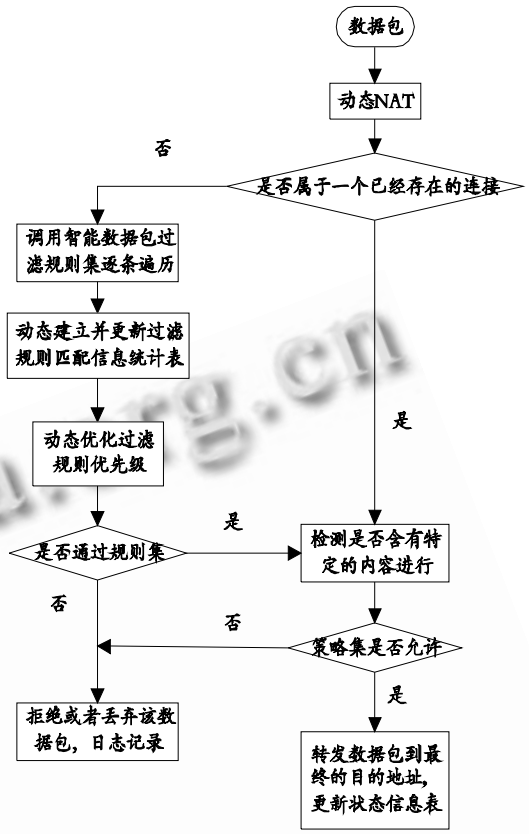

图 3 嵌入式 IPv6 防火墙工作流程图

嵌入式 IPv6 防火墙的工作流程：

(1) 当 IPv6 数据包通过网络接口进入防火墙之后，首先将经过动态 NAT 模块进行网络地址翻译，其目的是将外部公网 IP 与内部私网 IP 相互映射。

(2) 在完成动态 NAT 之后，防火墙会遍历连接状态跟踪信息表判断该数据包是否属于一个已经存在连接。此连接状态跟踪信息表记录着已存在连接的源 IP 地址、目的 IP 地址、传输层的源端口号、目的端口和 TCP 序列号等，通过这些信息防火墙可以高效快速的识别出该数据包是否属于一个已经存在的连接。

(3) 如果该数据包不属于一个已经存在的连接，系统会调用智能数据包过滤规则集，并逐条遍历整个规则集。与此同时防火墙会动态地建立并更新过滤规则匹配信息表，根据该信息表，系统采用统计、记忆、概率和决策的智能方法对数据进行识别，动态地优化过滤规则优先级。智能的数据识别方法，消除了匹配检查所需要的海量计算，高效发

现网络行为的特征值，直接进行访问控制，由于这些方法多是人工智能学科采用的方法，因此又称为智能访问控制技术。

(4) 如果该数据包通过了过滤规则集的审查，或者该数据包属于一个已经存在的连接，防火墙会对数据包是否含有特定内容进行检测，此时防火墙仅仅对数据包的关键信息进行检测，因此大大加快了检测的效率和速度。

(5) 如果该数据包未能通过状态跟踪安全策略，或者未能通过智能包过滤规则集，防火墙会拒绝或者丢弃该数据包，并进行日志记录。

(6) 在数据包通过了上述的过滤和审查后，防火墙就会将该数据包转发到最终的目的地址，并且防火墙会在其连接状态跟踪信息表中为此次会话创建或者更新一个连接信息。防火墙将会使用这个连接项对返回的数据包进行过滤。

5 结束语

本文对防火墙技术做了深入研究，设计了基于 S3C2440 处理器的嵌入式 IPv6 防火墙。该防火墙实现了支持 IPv6 协议的状态跟踪与智能包过滤相结合的动态包过滤。并成功搭建了远程 WEB 管理平台，方便地管理过滤规则、防火墙日志和网络状态等。随着 IPv6 网络的逐渐推广，包括防火墙在内的网络设备对 IPv6 网络的支持将成为必然趋势。因此基于 ARM 的嵌入式 IPv6 防火墙的应用前景也会越来越广阔。

参考文献

1 阎慧,王伟,宁宇鹏著. 防火墙原理与技术.北京:机械工业出版社, 2000:1－4.

2 张森.基于嵌入技术的分布式防火墙研究[硕士学位论文].南京:南京航空航天大学, 2004.

3 王常杰,秦浩,王育民. 基于 IPv6 的防火墙设计.计算机学报, 2001,(2):219－223.

4 郑德政,陈金牛,曾文华. 基于 Intel XScale IXP425 处理器的嵌入式 IPv6 防火墙设计与实现.福建电脑, 2008,(2):2－3.

5 张锦祥. 基于 U 盘的嵌入式防火墙系统的设计与实现.武汉大学学报:理学版, 2005,51(3):333－336.

6 吴军利,陈作人. 一种基于IPv6与防火墙结合的安全机制研究.微电子学与计算机, 2000,(3):6－10.

7 Samsung Electronics Co, Ltd. S3C2440X USER MANUAL.

8 邓国清. 智能防火墙技术研究[硕士学位论文].长春:吉林大学, 2007.

9 赵轩. 基于状态检测的硬件防火墙实现技术研究[硕士学位论文].长沙:国防科技大学, 2004.