基于 Intel XScale IXP425 处理器的嵌入式 IPv6 防火墙设计与实现

郑德政，陈金牛，曾文华
（厦门大学软件学院，智能信息技术福建省重点实验室 福建 厦门 361005）

【摘 要】：为解决防火墙对 IPv6 协议的兼容及对内部网络之间安全的保障问题，本文设计实现了基于 Intel XScale IXP425 处理器的嵌入式 IPv6 防火墙。该防火墙能通过 WEB 实现远程管理，对 IPv6 网络包和 IPv4 网络包均可进行良好的过滤。防火墙能够判断出网络包的协议类型，分别加以处理，实行动态包过滤，并可以解决 IPv6 分片攻击问题。通过实际设定过滤规则，对防火墙在 IPv6 和 IPv4 下的工作情况进行测试，验证了防火墙的准确性和高效性。

【关键词】：嵌入式防火墙；IPv6；WEB 管理；动态包过滤

1. 引言

随着计算机网络技术的突飞猛进，网络安全问题已经日益突出。防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域与安全区域的连接，同时不会妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信量，仅让安全、核准了的信息进入，同时又抵制对内部构成威胁的数据。防火墙的作用是防止不希望的、未授权的通信进出被保护的网络。一般的防火墙都具有过滤不安全服务和非法用户、控制对特殊站点的访问、提供监视 Internet 安全和预警的方便端点等功能。传统的边界防火墙只对网络的周边提供保护，在流量从外部的互联网进入内部局域网时对其进行过滤和审查。但是，并不能确保局域网内部的安全访问。最新一代的安全性解决方案将防火墙功能分布到网络的终端。分布于整个局域网内的嵌入式防火墙使用户可以方便地访问信息，而不会将网络的其他部分暴露在潜在非法入侵者面前[1]。凭借这种端到端的安全性能，用户无论通过内部网、外联网、虚拟专用网还是远程访问，实现与内部的互联不再有任何区别。

当前的防火墙多是基于 IPv4 协议。同多数嵌入式设备一样，如何实现嵌入式防火墙对 IPv6 的支持[2,3]，国内外尚处于研究阶段。世界上日本首先实现了对 IPv6 协议的硬件支持。中国在 IPv4 时代传统互联网中落后于国外，新一代互联网协议为中国在信息技术领域与世界同步提供了机遇。由于中国本身巨大的市场潜力，IPv6 的应用推广离不开中国。所以，开展对基于 IPV6 的嵌入式防火墙的应用研究，是一项很有实际价值的工作[4,7,8]。

本文在分析了 IPv6 的结构功能以及 IPv6 与网络安全的关系后，结合防火墙实现原理，设计提出了支持 WEB 管理、基于 Intel 网络处理器的嵌入式 IPv6 防火墙。给出了嵌入式 IPv6 防火墙的软、硬件体系结构，设计实现了 WEB 管理模块及防火墙功能模块，并给出了测试结果。

2. 嵌入式 IPv6 防火墙系统设计

2.1 硬件体系结构

本文设计的嵌入式 IPv6 防火墙的硬件体系结构如图 1 所示。其主体由以 Intel XScale IXP425 为核心的开发板组成，它主要由 IXP425 芯片和 DRAM、SRAM 存储设备以及两个物理网卡 LXT972 组成[5]。IXP425 芯片是防火墙的核心，主要由 XScale Core、UART、SRAM 控制器、DRAM 控制器组成。IXP425 的网口 1 与局域网内主机连接，网口 0 同外网连接。网络数据通过该硬件防火墙在内外网之间传输。同时可以通过网络访问防火墙并对其进行规则配置、日志查看等操作。

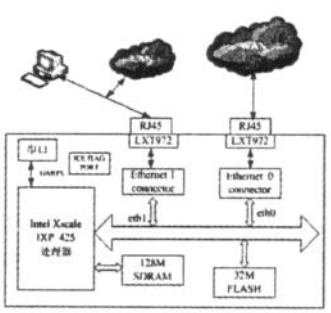

图 1 嵌入式 IPv6 防火墙硬件体系结构

2.2 软件体系结构

嵌入式 IPv6 防火墙软件体系结构的设计思路是：通过 WEB 管理系统设置管理规则，防火墙根据这些规则来过滤控制数据包。本防火墙软件结构主要由两个部分组成：WEB 管理模块和防火墙功能模块。WEB 管理模块通过 CGI 编程，运行在开发板的 Boa 服务器上；防火墙功能模块加载到开发板的嵌入式 Linux 内核中。如图 2 所示。

嵌入式 IPv6 防火墙的工作流程是：防火墙模块开始运行时，读取防火墙过滤规则配置文件，建立访问控制列表（ACL）；在运行过程中，可以通过 WEB 界面管理 ACL，查看访问日志以及网络工作状态。网络数据包从外部网络进来后，首先对其进行包头预处理，判断数据包类型，然后进入防火墙模块，对其进行静态包过滤操作和碎片检查，如果没有问题则进入后续操作，分别是 NAT 转换、建立状态跟踪列表、进行动态包过滤。被接受的数据包进入等待队列，准备发往内部网络；从内部网络发出来的包首先生成网络数据包，然后在对数据包进行校对（主要是包头），然后发往发送队列，传送给外部网络。

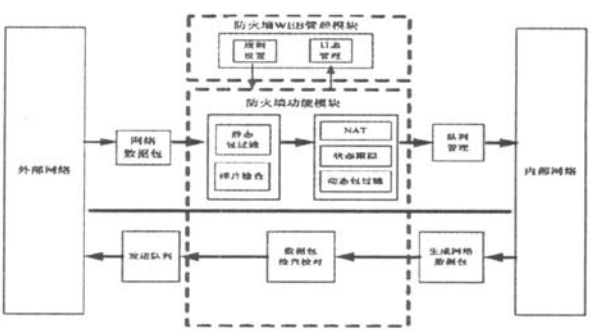

图 2 嵌入式 IPv6 防火墙软件体系结构

3. 嵌入式 IPv6 防火墙 WEB 管理设计与实现

在嵌入式 Linux 系统中，比较常用的 WEB 服务器有 Boa、Httpd、mini- Httpd 和 Thttpd 等几种，其中 Httpd 最小，只要几千字节的空间就可以，功能也最为简单；而 Thttpd 所需空间相对较大，但功能强大；Boa 使用比较广泛，其运行空间约 140KB 左右，功能适中[6]。最常用的是 Boa 和 Thttpd。本文设计的嵌入式 IPv6 防火墙的界面管理服务器采用 Boa，管理软件通过 C 语言编写的 CGI 程序实现。

WEB 管理模块包括以下 3 个部分，分别是防火墙管理模

基金项目："985 工程"智能化国防信息安全技术科技创新平台项目（0000- X07204）

块，系统状态模块，系统工具模块。

(1).防火墙管理模块：用来设置规则，包括添加、删除规则，查看规则表，生成规则文件供防火墙调用。

(2).系统状态模块：用来显示当前网络状态和查看日志。

(3).系统工具模块：设置防火墙的一般属性，如 IP 路由地址、重启等功能。

4. 嵌入式 IPv6 防火墙功能模块设计与实现

本文设计的嵌入式 IPv6 防火墙的核心功能模块由 4 个部分组成：目的地址转换 DNAT 模块，状态跟踪模块，源地址转换 SNAT 模块，包过滤模块。

(1).DNAT(Destination Network Address Translation)模块：完成目的地址 NAT 转换，其作用是把经过防火墙到内部网络的数据包根据用户预先设定好的规则进行转化，重写包的目的 IP 地址，让外部网络到内部网络的数据包能够正确的到达内部主机。这部分由运行在 XScale 内核中的操作系统完成。

(2).状态跟踪模块：协助包过滤模块进行连接状态的记录，是实现带状态的包过滤(动态包过滤)的关键模块。

(3).SNAT(Source Network Address Translation)模块：完成源地址 NAT 转换，其作用是把从内部网络经防火墙发到外部网络的 IP 数据包根据已有规则进行转化、重写包的源 IP 地址，让内部网络到外部网络的数据包能够正确的到达外部主机。这部分由运行在 XScale 内核中的操作系统完成。

(4).包过滤模块：根据访问控制表(ACL)完成网络数据包网络层传输层的包过滤处理，是防火墙最主要的功能模块之一。配合前面状态跟踪模块所记录的当前包的状态实现带状态的包过滤(动态包过滤)。

由于本防火墙开始是在 IPv4 下开发，最后移植到 IPv6 环境下，同时目前的网络环境也要求防火墙必须 IPv6 与 IPv4 兼容，所以上述模块都有 IPv6 和 IPv4 两个部分。流程原理类似，这里以 IPv6 为例介绍功能模块控制流程，如图 3 所示。

在进入 IPv6 处理流程以后，第一步所做的就是头部有效性检查，如果有效则立刻进入 IPv6 DNAT 模块。IPv6 DNAT 用于对 IPv6 的包进行目的地址转换，并负责 NAT 的动态表的维护工作。在内核操作系统中有一个和 IPv6 DNAT 模块对应的控制模块，它处理那些需要解析到应用层的数据包。

第二个主要处理模块是 IPv6 状态跟踪，这个模块是为了辅助包过滤的一个重要模块，用于记录连接的状态。

第三个主要处理模块是本文设计的防火墙的重头模块--动态包过滤模块，该模块将当前包与 ACL(访问控制表)的规则进行匹配，匹配结果通过参数传递出去。

第四个主要处理模块是 IPv6 SNAT 模块，这个模块对 IPv6 包进行源地址转换。在内核操作系统中有一个和 IPv6 SNAT 模块对应的控制模块，它处理那些需要解析到应用层的数据包。

当外网的包进入内网，会流经前三个模块直到 IPv6 路由查询，然后被发送出去进入内网。外网向内网发送的包在 IPv6 部分中，首先对目的地址转换(DNAT)，这样把目的地址(在开启 NAT 时一般是防火墙的公共 IP)转换成内网的可用实际 IP，这样才形成真正可用于建立连接的数据包；第二步 IPv6 的状态跟踪模块记录下当前数据包所在的连接状态；第三步开始动态包过滤，此时有了第二步记录的连接状态能进行有状态的包过滤操作；最后对数据包进行路由查询和发送。

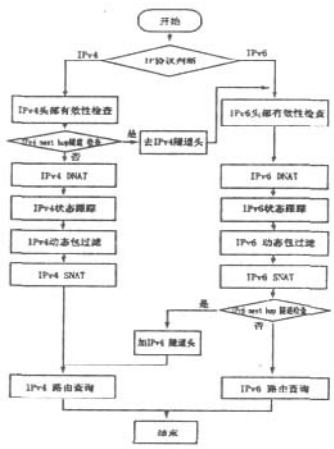

图 3 嵌入式 IPv6 防火墙功能模块控制流程

当内网的包向外网发送的时候，会流经后三个模块，然后进行 IPv6 路由查询之后被发送去外网。内网发出的包经过 IPv6 状态跟踪记录或更新连接状态，进行动态包过滤，在发出之前做 SNAT(源地址转换)处理，将源 IP(通常是内部 IP，对外网无效)转换成防火墙的对外公共 IP。

IPv4 部分的流程和 IPv6 部分完全一样，不再叙述。通过图 3 所示的流程控制，防火墙能支持纯 IPv4、IPv6 网络和 IPv6 in IPv4 的隧道包。

5. 测试结果

在对本文设计的嵌入式 IPv6 防火墙的测试中，使用两台 IPv6 主机访问防火墙保护下的内网主机的方式，对防火墙进行测试。外网主机的环境一台为 Windows XP，另一台是 Linux。通过对外网主机访问记录的验证来检测防火墙的性能。

分别对 IPv4 数据包和 IPv6 数据包设置规则。

(1).对 IPv4 进行测试设置

对于源地址为 59.77.6.10 到 59.77.6.110 之前的主机，不允许其对主机 59.77.6.118 的端口号在 21 到 80 之间的访问，即 118 主机的 ftp 和 http 服务不对上述网段的主机开放。

(2).对 IPv6 进行测试设置

对于地址为 2001:da8:e800:3060:5834:fe1:7ec:28b4 的主机(操作系统为 Windows XP)，防火墙内主机的访问规则设置为：对于源端口为 23，目的端口大于 1024，ack 置 1 的包允许通过，ack 为 0 的则拒绝；源端口为 80，目的端口大于 1024，ack 置 1 的包允许通过，ack 为 0 的则拒绝。设置完成后查看规则表，如图 4 所示。

图 4 防火墙规则表内容

规则生效后查看日志，如图 5 所示。从日志中可以看出，无论是上述设定中的 IPv4 地址段还是 IPv6 地址，系统都能按照规则对数据包进行处理，实现了 IPv6 防火墙功能。

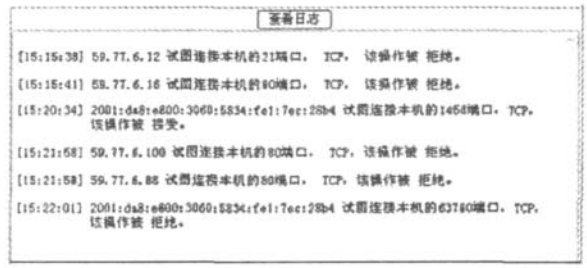

图 5 防火墙日志测试结果

6. 结束语

本文设计了基于 Intel XScale IXP425 处理器的嵌入式 IPv6 防火墙，包括硬件体系结构、软件体系结构和 WEB 管理系统结构等，涉及动态包过滤、NAT 地址转换等多种网络安全技术和 WEB 服务技术。嵌入式 IPv6 防火墙在 IXP425 处理器硬件基础上实现了对 IPv4、IPv6 协议的同时支持，并对网络中的数据包进行动态包过滤，过滤规则可以通过 WEB 界面远程对其控制修改。相对于一般 IPv4 防火墙，嵌入式 IPv6 防火墙既兼容了 IPv6 协议，又支持 WEB 访问，方便了防火墙的管理。随着 IPv6 协议的不断推广使用，包括防火墙在内的网络设备对 IPv6 协议的支持已成为必然的趋势。基于网络处理器的嵌入式 IPv6 防火墙的发展也会越来越成熟。

进一步的工作将围绕以下几个方面进行：

(1).增加防火墙功能，对数据进行加密解密处理，充分发挥 IXP425 的功能特性；优化规则匹配查找时的算法，提高包过滤效率。

(下转第 13 页)

置项。该信息格式如下:

```
[USERDB]
DBNUM = 1
;DBNUM =DBTYPE $DBNAME $SERVERNAME $USERNAME $PASSWORD $NODE$COUNT$STATE$STANDBY$ACTIVE $
;DBTYPE,数据库类型,如 0 表示 MSSQLSERVER,1 表示 ORACLE
;NODE,节点号
;COUNT,当前用户数
;STATE,运行状态
;STANDBY,备用库信息
;ACTIVE,是否激活
0 = 1$RCYW_DB$ RCYW_DB $RCYW$RCYW$170$0$0$0$0$
……
```

这些信息中包括了要导出或导入数据的数据库信息，导出导入工具读入配置信息,根据数据库配置采用相应的接口,通过多线程连接多个数据库，然后由导出导入模块进行导出或导入操作。

转换配置库是导入操作最重要的操作之一。首先它由开发人员在软件测试阶段根据用户数据库结构生成简化模板，在系统运行阶段,结合原数据库和新数据库数据字典,可以通过手工或界面化操作增加用户字段，用户可以通过不同版本的配置库,以方便不同系统软件之间不同版本之间数据的导出导入。其格式如下:

```
[CONFIGINFO]
; DESC=是对本配置文件的描述
DESC=xxxxx
; IGNORELINES=忽略文件的前 XXX 行,取值范围 0~255,缺省为 0
IGNORELINES=2;
; FLDNAMEEXIS=文件中是否有参数名称行,1:有,0:没有
FILPARAEXIST=1;
[SYSTEMTYPE]
[TABLEINFO]
;这里主要配置需要入库的数据库表名称
TABLENUM=8
TABLE1=表 1
TABLE2=表 2
……
;如果需要转换,给出相应的转换规则
……
```

3.2 界面的构造及功能实现

整个界面包括:获取系统配置、查看修改系统配置、获取转换配置库、导出界面和导入界面。界面中尽量使用 Windows 标准控件,如下拉表框和列表框等,预先写入相关信息供用户选择,减少用户的输入,用户在输入相应的入口参数后,程序自动把数据字典和配置文件的信息动态地写入各个控件项中。在获取系统配置文件和转换配置库界面中用户可以根据系统的实际情况修改配置文件和转换字段信息。如果后台数据库管理系统功能中包括了用户数据字典的维护,可以屏蔽这部分功能,降低组件封装的实现难度。

在导出导入功能实现过程中，用户可以选择导出数据为中间格式的文件或者通过内存库直接导入新数据库。内存数据库通过使用 STL 技术生成,利用 STL 提供的功能减少了内存库操作功能的实现,提高了开发的效率。导出功能根据系统配置文件获取数据库信息，通过封装的数据库接口完成数据库的读写操作,通过转换配置库可以由用户选择哪些表或字段不需要导出,直接通过转换配置库界面过滤该表或字段信息即可。为了提高导出的性能,可以利用多线程使多个数据库同时导出。导入操作和导出操作类似,不再赘述。

3.3 组件的实现[4,5,6]

上述通用数据导出导入的原理和设计思想及实现步骤只是一种方案，并不局限于某种开发工具，用户可以使用 VB、VC、Delphi、C++ Builder 等编程语言来实现。本文作者采用了 VC++ 6.0 在 Windows 平台下来实现通用数据导出导入功能，并封装 ODBC 生成动态连接库，作为连接各种平台下不同数据库的驱动程序接口，鉴于该组件封装的功能能够用到不同的编程语言环境下,利用 VC 的灵活性及 MFC 开发 ActiveX 的相关技术,集成通用数据导出导入所有的功能和接口，使用通用数据导出导入以 ActiveX 空间的形式应用到多种开发语言中。ActiveX 是 Microsoft 提出的一种标准，可以使用不同语言的开发的软件构件在 Windows 平台下相互集成，它是以组件对象模型为基础的开放技术的集合[2,3]。由于其独立于开发语言,使不同的开发语言应用该导入导出组件就变得相当容易。

4. 在实际系统中的应用

在开发本校学生教务管理系统中充分显示了使用该组件的优越性，两个系统后台数据库采用当前比较流行的 Oracle9i 和 MSsqlserver2000 及 Sysbase，数据库管理系统采用 PB8.0 开发。导出导入工具可以作为独立的工具运行在该系统和现有的信息管理系统中,在导出导入过程中,使用界面化操作获取系统配置文件和转换配置库,并进行修改满足操作需求,用户只需根据界面操作即可完成数据库之间的数据转换及相关操作。该组件主程序不再改变，用户通过修改转换配置库来完成各种数据库及不同数据库结构之间的转换,大大提高了开发的效率。

5. 结束语

本文分析了在管理信息系统中通用数据导出导入功能的原理和实现方法，主要介绍了一种基于配置文件和转换配置库的通用数据导出导入工具的设计和实现方法，利用系统配置文件和转换配置库使导出导入功能完全和系统分离开来，友好的操作界面能够满足用户操作的需求,并使用组件技术进行封装,不仅提供操作接口的灵活性和可扩展性，而且提高了系统的开发效率,该组件可以运用到每一个信息管理系统中,具有较高的通用性和可扩充性,但对转换配置库的维护完全由用户来维护,所以用户需要提前熟悉配置库的功能,增加了用户的工作量。

参考文献:

1. 何珍文,吴冲龙,张夏林,往新庆。数据库应用程序中通用动态查询实现方法研究[J].计算机工程,2002.(11):92~94.
2. Corry C, Cadman J.COM/DCOM primer plus[M]. Indianapolis: Sams Publishing, 1999.
3. Pan Aimin.COM principles and applications[M].Beijing: Tsinghua University press, 1999.
4. 金正淑,葛华.组件技术的研究与探讨[J].东北电力学院学报,2003,(3): 51~54.
5. Adam Denning. ActiveX Controls Inside Out [M]. Microsoft Press, 1997.
6. 李磊,李一凡,郝明国。基于用户数据字典的通用动态查询组件的研究与实现[J]. 微电子学与计算机,2005,(3):17~19

(上接第 3 页)

(2).深入对 IPv6 协议的分析,增强对 IPv6 的处理能力。

(3).完善防火墙 WEB 管理功能,增加其功能。

参考文献:

1. 钱炜,罗军舟.基于嵌入式 Linux 的硬件防火墙系统设计[J].微机发展,2004 年 6 期(14),124- 127.
2. 蒋亮,郭健.下一代网络移动 IPv6 技术[M].北京:机械工业出版社,2005.
3. 互联网工程任务组 http://www.ietf.org.
4. 刘玉莎,张晔,张志浩.嵌入式防火墙系统的实现[J].计算机系统应用,1999 年 9 期.
5. Intel Company.Xscale425 处理器手册[Z], March 2005.
6. 王则林. 基于 WEB 的嵌入式 Linux 防火墙服务管理系统的研究与实现[D],苏州大学硕士学位论文,2005.
7. 吴广霖,白瑞林.基于平台的嵌入式 WEB 服务器的设计与实现[J].计算机工程,2005,18 期(31),216- 218.
8. 赵轩.基于状态检测的硬件防火墙实现技术研究[D],2004 年 11 月,国防科技大学硕士学位论文.