文章编号:1004-1478(2011)06-0005-04

基于SPI的个人Windows防火墙设计与实现

蔡增玉[1], 陈志豪[2], 刘书如[1], 甘勇[1]

(1.郑州轻工业学院 计算机与通信工程学院, 河南 郑州 450002;
2.河南天海电器有限公司, 河南 鹤壁 458030)

摘要:针对目前基于Windows平台的个人防火墙不能较好地根据应用程序进行控制且缺少与商用防火墙对比等问题,提出了一种基于SPI的Windows个人防火墙.该防火墙采用Winsock2 SPI编程技术,系统模块间使用动态链接库、全局变量接口和函数接口,从而较好地实现了数据监视、日志管理、管理规则和系统监视等功能.实验结果表明,该防火墙具有良好的性能,实现了个人防火墙的基本技术指标,能够保护个人计算机的网络安全.

关键词:网络安全;个人防火墙;服务提供者接口
中图分类号:TP393.09 **文献标志码**:A

Design and implementation of personal Windows firewall based on SPI

CAI Zeng-yu[1], CHEN Zhi-hao[2], LIU Shu-ru[1], GAN Yong[1]

(1. *College of Comp. and Com. Eng., Zhengzhou Univ. of Light Ind., Zhengzhou* 450002, *China*;
2. *He'nan THB Electr. Co., Ltd., Hebi* 458030, *China*)

Abstract: In view of the problem that the current platform based on the Windows personal firewall can not control according to the application program and lack of business firewall contrast, one kind personal Windows firewall based on the SPI was proposed. The firewall uses Winsock2 SPI programming technology, the system module adopts the dynamic link library, global variable interface and interface functions, and realizes data monitoring, log management, management rules and system monitoring and other functions. The experimental results showed that the firewall had good performance and achieved the basic function of the personal firewall. It can guarantee the network safety of personal computer.

Key words: network security; personal firewall; service provider interface(SPI)

0 引言

防火墙可以对要通过的数据包进行监测、限制、更改,从而有效地对外屏蔽被保护网络的信息[1].随着Internet的广泛普及,网络安全问题日益严重,对基于Windows平台的个人防火墙具有极大需求.基于Windows平台的个人防火墙系统的实现需要理解Windows网络编程的一些独特底层接口和网络协议底层,难度很大[2],研究人员对此开展了研究并取得了一些成果[3-6].但是,这些成果主要集中在根据IP报头进行网络封包截获,而根据应用程序进行控制的比较少,也没有进行性能测试,更缺

收稿日期:2011-04-26
基金项目:"十一五"国家科技支撑计划(2006BAK01A38);河南省基础与前沿技术研究计划项目(082300410280)
作者简介:蔡增玉(1979—),男,河南省鹤壁市人,郑州轻工业学院讲师,硕士,主要研究方向为智能规划与网络安全.

少与商用个人防火墙的对比.本文拟运用SPI(service provider interface)报文截获技术,设计与实现Windows个人简易防火墙,并且与瑞星个人防火墙进行比较,以期达到个人防火墙的基本技术指标.

1 基于SPI的个人Windows防火墙设计

1.1 功能设计

基于SPI的个人Windows防火墙的功能设计是:根据用户的设定对进出系统的数据包进行处理,建立完整的网络访问日志系统,同时为用户设置防火墙提供接口.其主要功能模块有数据监视、日志管理、管理规则设置和系统设置.

1)数据监视.数据监视的主要作用是将系统中当前网络访问信息显示在防火墙的用户界面,将可视的数据信息提供给用户,包括网络连接的应用程序路径、防火墙的管制动作、使用的协议类型等信息.用户可以通过防火墙界面上的停止/启动按钮进行控制.

2)日志管理.包括记录日志和查询日志.当连接网络时,网络连接信息将被防火墙写入日志文件,用户对过滤规则和系统设置进行修改也要写入日志系统.当用户需要查询日志时,可以在指定的时间段进行.

3)管理规则设置.用户可以手动添加应用程序到控制管理规则文件,系统也可以根据防火墙的模式自动将拦截的网络通信应用程序添加到此控制管理规则文件中.当用户添加控制管理规则时,可以设置各个管理规则的子项.这些子项包括目的网络IP地址、访问网络的时间段设置、协议类型、端口信息等.在控制管理规则的设置中还可以设置防火墙的3种工作模式,即允许所有、询问所有和拒绝所有.用户可以根据需要进行设置,这些设置同规则设置一样都被写入控制管理规则的文件.

4)系统设置.防火墙系统设置包括是否记录日志文件、日志文件的大小、开机自动启动系统、发生数据包拦截时是否报警或者闪烁系统光标.系统设置信息会全部写入防火墙的规则设置文件.

1.2 系统体系设计

目前Windows下个人防火墙软件常见的网络数据包的拦截技术有利用Winsock2 SPI的拦截技术、基于IP过滤钩子的拦截技术、基于传输驱动接口的拦截技术和基于中间驱动的拦截技术[2-3].本文采用Winsock2 SPI编程技术实现个人防火墙系统.该方法有以下优点:工作在应用层,以DLL的形式存在,编程、调试方便;跨Windows平台,可以直接在Windows 98/NT/2000/XP上应用;封包没有按照底层协议进行切片,比较完整,很容易做内容过滤.

SPI处于系统Winsock2 API接口和计算机网络接口之间,主要是为Winsock2 API提供一个可以编程的接口.当Winsock2网络应用程序尝试连接网络时,首先会使用Winosck2 API接口,在经过合适的选择之后将会调用下一层的接口,也就是SPI接口.应用程序会通过这个接口来连接网络.简易防火墙实现的关键技术就是要在API和SPI接口间插入自己设计的一个接口,当发生网络调用时,自定义的接口会被首先调用,在调用中本系统可以对此次网络连接进行一系列的操作.

1.3 接口设计

系统接口就是软件系统各个不同的组成部分衔接的约定.在本文简易防火墙的设计中,系统模块间使用的接口有动态链接库接口、全局变量接口和Windows消息接口.

1)动态链接库接口.本文中动态库与防火墙主界面的数据通信使用了这种接口.为了程序的安全性,本系统并没有把所有的函数都变为接口.在动态库中只设置了2个函数作为接口,一个是让访问网络的应用程序调用的接口,另一个接口提供防火墙系统与动态库的数据交换和一些信息的设置.通过动态链接库接口,用户将设置的管理规则加载到动态库中,在需要调用这些规则时直接在自己的缓存中就可以找到,不必再次加载.

2)全局变量接口.防火墙的主界面就是1个对话框类全局变量,我们可以在程序的任何地方使用它.本系统的动态库有1个进程间共享的变量,通过这些全局变量,防火墙系统可以保存应用程序调用时的数据信息.虽然使用全局变量容易使程序出现问题,降低变量的可控性,但在本系统中很多地方都使用了全局变量.例如,在动态库中使用一个全局变量的函数指针来保存操作系统的基础服务提供,当防火墙放行应用程序时,直接使用这个变量可以轻松地得到操作系统的服务提供者.本系统尽量使这些变量赋值的地方单一,减少错误的发生.在可控性方面,本系统通过设置临界区来使这些变量只在特定的时刻进行赋值.

3)Windows消息接口.当动态库有信息要通知

用户界面时，通过Windows消息接口将一些数据发送给用户界面；当动态库中的封包数据将要显示在系统的用户界面时，也通过消息接口通知系统从指定的缓冲区中取出数据.

2 基于SPI的个人Windows防火墙的实现

2.1 关键技术

笔者在Windows XP(SP2)操作系统下，以VC++6.0为开发工具，成功开发出了一个基于SPI的Windows个人防火墙系统. 基于SPI的Windows防火墙的主要工作过程：防火墙拦截一个网络连接后，首先提取连接中有用的数据，如源和目的地址、端口、打开连接的应用程序及其路径等信息；接着把这些信息发送到实时监控程序，监控程序让防火墙去匹配用户设置的管理规则，当用户没有设置规则时，防火墙自动提醒用户，让用户自己做出合理的选择. 其关键技术有应用层协议解析、SPI服务函数的认证和过滤规则匹配.

1)应用层协议解析. 由于SPI是在应用层截获数据封包的，因此可以对基于应用层的网络协议进行解析. 在本系统中，将截获的封包数据分离处理并保存到一个Session字段中，然后通过各种协议的各个字段对其进行协议的解析处理. 例如HTTP协议中的“host”字段表示本次连接的域名，在提取这个域名时，首先把缓存区中的数据进行字符标准化处理，然后遍历查找主机标识“host”，查到并取出标识后到回车符前一行数据，从而得到主机信息. 其他协议提取方式与此相同.

2)SPI服务函数的认证. 通过挂接技术实现对SPI函数的截获后，要进行相应的认证(过滤)操作才能完成整个通信过程. 认证主要是通过调用一组对访问权限控制的函数来实现. 当网络应用程序发生不同的网络行为时，都会对其动作行为进行一次认证，从而充分保证连接的安全性.

3)过滤规则匹配. 过滤规则的匹配是防火墙的核心部分，决定着防火墙的处理速度，但是该过程也比较复杂. 在此以截获本机发送数据包为例进行说明. 发生封包截获时，首先检查封包的目的地址是否为本地地址，如果是，防火墙会放行；若不是，就继续通过防火墙系统当前的工作模式去确定处理动作. 当工作模式为询问时，规则匹配会进入管理规则匹配阶段. 在此阶段，首先从管理规则文件中查找是否有关于本次连接规则的信息，如果有，则按规则设定确定处理动作；若没有相关规则并且是第一次查找，那么防火墙会直接询问用户，让用户对本次连接采取管制动作，若不是第一次查找，那么防火墙会根据上次的管制动作来决定本次的管制动作. 具体流程如图1所示.

2.2 系统测试

测试环境：安装Windows XP(SP2)系统的联网个人计算机2台，分别为测试机和辅助测试机，其硬件配置相同，都为512 M的DDR内存，40 G容量7 200转硬盘. 这2台计算机通过百兆交换机连接在一起.

使用测试软件NetIQChariot对防火墙进行性能测试. 从测试机发送1 000个数据包到辅助测试机，同时开启HTTPtext, HTTPgif, FTPput, FTPget 4对PAIR，得到分别在不使用防火墙、使用瑞星防火墙(版本号23.00.19.33)和使用本文防火墙情况下的平均吞吐量、转发速率、响应时间等数据(运行100次计算机平均值)，如表1所示. 结果表明，本文设计实现的防火墙对个人计算机常用的HTTP和FTP协议的吞吐能力、转发速率和响应时间产生了一定的影响，但影响非常小，可以通过规则匹配算法的改进进一步改善包过滤的时间. 与瑞星防火墙相比，本文设计的防火墙在平均吞吐量和响应时间上具有优势，但转发速率稍低.

功能测试方面，参照瑞星、天网等个人防火墙的功能，对本文设计的防火墙进行测试，其功能测试结果见表2. 测试结果表明，基于SPI的Windows防火墙具备了个人防火墙的常用功能，能够比较便捷地实现对个人PC的上网保护，很好地实现了系统功能设计.

3 结论

本文采用Winsock2 SPI编程技术，在系统模块间使用动态链接库、全局变量接口和函数接口实现了Windows个人防火墙设计. 该系统具有系统实现方便、跨Windows平台、CPU占用低等特点. 实验结果表明，该系统能够较为方便地实现Windows个人防火墙的功能，具有一定的应用前景，也为下一步的研究奠定了基础. 下一步的主要工作是对此系统进行如下的改进和完善：1)优化过滤规则数据结构和匹配算法，提高处理数据速度；2)使用内核数据包拦截技术对核心层的数据包进行更彻底的过滤，

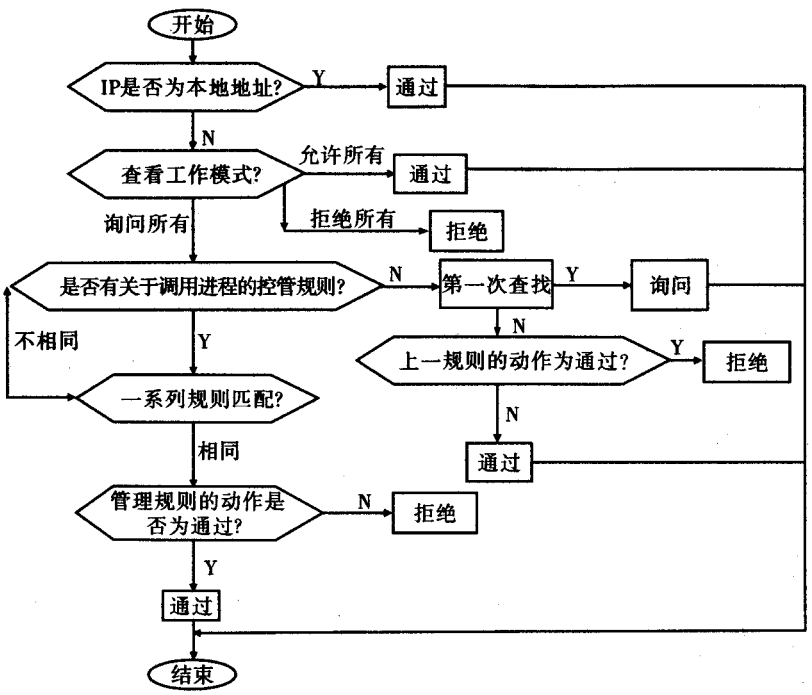

图1 发送数据包规则匹配流程

表1 防火墙性能测试结果

测试脚本	平均吞吐量/(Mb·s^{-1})			转发速率/(次·s^{-1})			响应时间/s		
	不使用防火墙	本文防火墙	瑞星防火墙	不使用防火墙	本文防火墙	瑞星防火墙	不使用防火墙	本文防火墙	瑞星防火墙
HTTPtext	14.139	13.054	13.770	171.585	158.428	167.112	0.006	0.006	0.006
HTTPgif	13.161	12.920	13.195	159.722	156.800	160.136	0.006	0.006	0.006
FTPput	39.977	36.007	37.016	4.996	4.500	4.626	0.200	0.222	0.216
FTPget	50.357	51.389	47.726	6.294	6.423	5.965	0.159	0.156	0.168
Totals	113.646	110.956	105.808	342.598	326.151	337.840	0.093	0.098	0.099

表2 本文设计的防火墙功能测试结果

功能	测试结果
恶意软件保护	支持,能够防范绝大多数的木马
日志功能	支持,事实写入日志文件
报警	支持,通过图标闪烁提醒
协议支持	多协议(UDP,TCP,SMTP,FTP,HTTP等)支持
端口过滤和IP地址过滤	支持
应用程序控制	支持放行、阻塞、询问、中止
用户选择记忆	支持

实现应用层和核心层的双重过滤;3)将防火墙与入侵检测技术等网络安全技术相结合,构建纵深安全防护体系.

参考文献:

[1] 张婷,赵锦东,王永强. 基于Visual C++的个人防火墙的设计与实现[J]. 唐山学院学报,2009,22(6):58.

[2] 刘鹏远. Windows下个人防火墙实现技术路线分析[J]. 计算机工程与设计,2008,29(21):5461.

[3] 刘鹏远. SPI截获Windows个人防火墙系统技术要点分析[J]. 湖南工程学院学报:自然科学版,2008,18(2):56.

[4] 孙江宏,吴少华,周安民,等. 基于包过滤防火墙的防御系统的设计与实现[J]. 微机算信息,2006,22(3):37.

[5] 陈永辉,向科峰,吕琳. 基于Winsock 2 SPI网络封包截获[J]. 兵工自动化,2006,25(3):55.

[6] 胡滨,贺超凯,左明. Windows下使用SPI过滤网络数据包[J]. 华中科技大学学报:自然科学版,2003,10(S1):169.