文章编号:1671-6833(2006)03-0085-04

Windows XP SP2 防火墙技术及应用

张玉凤,翟光群

(郑州大学信息工程学院,河南 郑州 450001)

摘 要:给出了Windows XP SP2防火墙的使用方法及应用实例.研究分析了Windows XP SP2防火墙(ICF)技术,在不同的联网环境下对个人防火墙和ICF分别进行了接入、安装、设置、应用实验.结果证明:Windows XP SP2的防火墙技术几乎拥有了其它个人防火墙技术的优点,且占用系统资源少,对于网络攻击具有较高的防范功能,增强了个人计算机的网络安全性.

关键词:Windows XP SP2防火墙;网络安全;攻击防范

中图分类号:TP 309.1 **文献标识码**:A

0 引言

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术,是网络安全的第一道屏障,也是保护计算机系统安全运行的一项关键技术.随着网络犯罪活动的日益猖獗,网络中的个人用户已成为其攻击的首要目标之一,使计算机面临数据丢失和机密泄露的危险,造成的损失难以估量.让人们了解使用Windows XP Service Pack 2 (SP2)系统自带的Internet连接防火墙(Internet Connection Firewall,以下简称ICF)技术,采取主动防御措施对防止系统资源浪费和保证网络安全有着重要意义.

1 Windows XP SP2的ICF分析

1.1 ICF功能

Windows XP SP2的ICF功能:①对允许在Internet与家庭网络之间进行通信的信息类型加以限制.②ICF为通过线缆调制解调器、DSL调制解调器或拨号调制解调器与Internet建立连接的独立计算机提供保护.③可以针对Internet上的大多数不良内容为计算机提供保护.④ICF采用状态防火墙技术,可监视通过其路径的所有通讯,并且检查所处理的每个消息的源和目标地址.⑤ICF是通过保存一个表格,记录所有自本机发出的目的IP地址、端口、服务以及其他一些数据来达到保护本机的目的.其原理是当一个IP数据包进入本机时,ICF会检查这个表格,判别这个IP数据包是不是本机所请求的,如果是就让它通过,如果在那个表格中没有找到相应的记录就抛弃这个IP数据包.⑥源自外部计算机的通讯(如Internet)将被防火墙阻止,除非在"服务"选项卡上设置允许该通讯通过.ICF不会向你发送活动通知,而是静态地阻止未经请求的通讯,例如不响应黑客的Ping命令,禁止外部黑客程序对本机进行端口扫描袭击,抛弃所有没有请求的IP包.所以,ICF可以在一定程度上能很好地保护我们的个人计算机.

1.2 ICF的特点

(1) ICF是Windows XP内建的功能,占用的系统资源相当少,最适应使用调制解调器(Modem)上网的用户,原因是用Modem上网的时间不会太长,一般在几小时上下(包月的除外).其次是每次建立连接后拨号服务器都会分配一个新的IP地址,长时间占用一个相同的IP的可能性应该很低.比起使用DSL和宽带的用户来讲,用Modem上网给黑客攻击增加了难度,所以,使用ICF既提供了一定的保护,而且又不太占用资源.

(2) 不应在没有连接Internet的计算机上启用ICF.如果在局域网内的计算机启用ICF,则它将干扰该计算机和网络上的其他计算机之间的某些通讯.如果局域网络已经具有防火墙或代理服务器,则不需要ICF.如果网络只有一个共享Internet连接,则应该启用ICF对其进行保护.

(3) 对于只使用浏览、电子邮件等系统自带

收稿日期:2006-01-20;**修订日期**:2006-04-08

基金项目:河南省重点科技攻关资助项目(0423020400)

作者简介:张玉凤(1951-),女,河南郑州人,郑州大学讲师,主要从事计算机网络应用技术,网络安全方面的研究.

的网络应用程序,ICF不会产生影响.也就是说,用IE、Outlook Express、office等微软系统自带的程序进行网络连接,ICF是默认不干预的.所以装上SP2后,即使打开其防火墙并且启用"不允许例外"选项,无需将IE加到"例外"就能上网,而ICF也不会询问是否要允许IE通过.

(4) 如果有多台运行Windows XP的计算机要对所有具备Internet连接能力的计算机启用ICF.ICF是以连接为单位进行配置的.这就意味着如果通过多种方式从计算机上访问Internet(例如,在某些情况下使用调制解调器,而在其它情况下使用DSL),那么,就必须针对每种连接方式独立配置ICF.

(5) 如果拥有一台独立的计算机或通过拨号方式与Internet建立连接,那么,软件防火墙将是理想选择.此时,如果计算机是在企业网或校院网内,建议优先采用Windows XP SP2的防火墙ICF.

2 个人防火墙与ICF的区别

ICF和个人防火墙软件的区别在于,ICF是为提供基本入侵防御功能而设计的,其中并不包含个人防火墙应用程序所具备的高级功能特性.大多数个人防火墙产品能够使用户免受由那些侵犯个人隐私或允许网络黑客冒用他人计算机的软件所发起的攻击,而ICF则不具备此类特性.

个人防火墙对双向流量都进行审核,拥有更复杂的控制列表,ICF只阻截所有传入的未经请求的流量,对主动请求传出的流量不作理会.绝大多数商业个人防火墙都提供了应用程序过滤功能,可以阻止未通过认证的应用程序向外发送报文,这样就可以防止病毒或木马等恶意代码同外部建立未认证的连接,同时也可以防止用户的计算机被黑客用做分布式攻击的跳板.然而,Windows XP SP2所带的防火墙却只能对进入计算机的报文进行过滤,而不对计算机向外发出的报文进行过滤,它不对应用程序向外发送报文做任何限制.个人防火墙产品依据的防黑客原理通常是不一样的,例如Norton的Personal Firewall是基于应用程序的.基于应用程序的防火墙在使用上相当麻烦,因为必须要为每一个访问Internet的程序设置策略.而随着策略的增多,防火墙的效率也逐步下降,况且过多的策略也会相互矛盾、影响,给系统安全带来漏洞.另外,需要注意的是这些个人防火墙产品都非常占用系统资源.

当接入网络游戏联众世界的时候,本地计算机请求连接远程服务器,这时,个人防火墙立即提示是否允许此连接通过,而ICF对这个主动出站请求不做任何处理,如果入侵已经发生或间谍软件已经安装,并主动连接到外部网络,那么ICF不做任何提示;但这不表示Windows防火墙不安全,因为攻击多来自外部,而且如果间谍软件开放端口等待外部连接的时候,Windows防火墙将立即阻断连接,并且做出提示.

对来自外部请求连接ICF和个人防火墙在功能上区别不大.而且ICF防火墙有其独特的特性,包括:计算机的所有连接默认启用ICF、人性化的屏蔽模式,充分考虑到了计算机使用环境的变化和及时阻断攻击和恢复正常使用的情况、智能应用程序异常流量管理、内建支持IPv6等功能.

ICF和个人防火墙软件无法替代反病毒软件.个人用户当同时使用这两种类型的软件产品.

3 Windows XP SP2 ICF的安装设置

3.1 安装方法

(1) 命令法:单击"开始"→"运行",键入wscui.cpl,然后单击"确定",在"Windows安全中心"内单击"Windows防火墙"即可进行安装设置.

(2) 控制面版法:单击"开始"→"设置"→"控制面版",单击"Windows防火墙"即可进行安装设置.

(3) 连接设置:建立一个新的连接的时候,向导程序就会问你是否要激活ICF.在每一个连接的属性→高级选项中也可以选择激活或者取消ICF功能.在激活ICF之后,在高级选项的下部就会出现"设置"按钮,可以对ICF进行进一步的设置.ICF的设置主要有三项:①服务项,通过设定可以让ICF对某些服务不进行审核.TCP/IP的服务都是由端口来区分的,可以分别对TCP、UDP或者IP Protocol进行设置,在这一项中已经有了一些可选的缺省设置,也可以建立自己的设置.②日志项,ICF可以把它所抛弃的IP数据包以及获准通过的IP数据包都记录在案以便可以让你进行进一步的分析.③关于ICMP的,ICMP通常用于Ping、Tracert程序以及路由的动态实现,建议禁止所有的ICMP响应.

3.2 Windows防火墙设置中几个重要选项

(1) 当单击选中"不允许例外"选项时,Windows防火墙将阻止所有连接到个人计算机的请求,即使请求来自"例外"选项卡上列出的程序或服务也是如此.该选项十分有用,可以阻止所有连

接到个人计算机的尝试,因而当使用 Windows 防火墙并启用了"不允许例外"选项时,仍然可以查看网页,收发电子邮件或使用即时消息传递程序.有助于保护个人计算机.

(2) 当单击选中"例外"选项时,该选项卡可以添加程序和端口例外,可以允许特定类型的传入通信.可以为每个例外设置范围.对于家庭和小型办公室网络,建议可能的条件下,将范围设定为仅限局域网内部.这样配置可以使同一个子网上的计算机可以与此计算机上的程序连接,但拒绝源自远程网络的通信.

如果开放了某个端口,那么对这个端口的访问将被允许通过.端口或者服务可以在"例外"选项中设置或者通过指定应用程序的方法设置,如QQ等,如果开放端口的服务不是一个应用程序如IIS服务,可以直接设置开放的协议和端口号.对于只使用网络浏览、电子邮件、共享文件夹、进行普通处理的客户端和服务器应用程序的用户,Windows 防火墙不会产生影响.

3.3 ICF 的特别功能

3.3.1 ICF 的连接设置

ICF 可以精确的设置是对某台计算机或者某些子网允许连接;如果没有开启服务,则所有连接都将被拒绝.设置方法:安全中心→防火墙设置→例外→编辑(某个服务)→更改范围→自定义列表.在自定义列表中,如果对某个 IP 提供服务,设置子网掩码为全 1,例如 192.168.0.3/255.255.255.255;如果针对某个子网提供服务,设置正确的子网掩码,如 192.168.0.1/255.255.255.128,多个项目之间用","号隔离.使用 IPSec 规则可以提供对计算机向外发出的报文进行过滤的功能.

3.3.2 文件及打印共享、网上邻居设置

在"例外"选项上"程序和服务"列表中选择"文件及打印机共享"即可.这样可能带来新问题,如果企业网络同时连接外部网络,比如 Internet,对外开放这些端口是不安全的,此时在"编辑服务"选项中点击"更改范围",在弹出的对话框中选择"仅我的网络(子网)",这样设置后,文件和打印共享服务只对内部提供,而对外而言服务是不可见的,这样就安全多了.

3.3.3 ICF 配置、检查

当 ICF 安装、配置、启动使用后,运行"Netsh firewall show state";"Netsh firewall show config"命令可以检查显示防火墙状态和配置信息,以便达到最佳效果.

4 ICF 应用分析

定期分析日志可以发现潜在的安全问题,ICF 的日志分为两部分:一部分是 ICF 审核通过的 IP 数据包,而另一部分就是 ICF 抛弃的 IP 数据包.日志一般存于 Windows 目录之下,文件名是 pfirewall.log.其文件格式符合 W3C 扩展日志文件格式,分为两部分,分别是文件头和文件主体.文件头主要是关于 pfirewall.log 这个文件的说明,需要注意的主要是文件主体部分.文件主体部分记录有每一个成功通过 ICF 审核或者被 ICF 所抛弃的 IP 数据包的信息,包括源地址、目的地址、端口、时间、协议以及其他一些信息.

在实际的使用中应尽量避免在局域网中使用 ICF,它可能会给一些网络应用带来影响.在个人计算机中使用也可能会对一些程序的运行带来影响.例如,OICQ 的"语音世界"功能就是建立在双方交互的基础上的,而 ICF 会影响这些交互过程从而使得连接无法建立.解决这个问题就是找到 OICQ 使用哪个端口来实现语音功能,在前面介绍的属性→高级→设置→服务中来添加一项自定义设置从而使 ICF 忽略这个端口的检测.这样,OICQ 的语音功能就可以正常使用了.

5 结束语

ICF 是 Windows XP SP2 提供的一项新的功能,它并不是用来取代现有的个人防火墙产品,但是 ICF 提供了一个强大的保护层,可以阻止恶意用户和程序依靠未经请求的传入流量攻击计算机.实用证明 ICF 几乎具备了其它个人防火墙的优点,对于黑客的网络攻击拥有较高的防范性能,增强了个人计算机的网路安全性.

参考文献:

[1] 胡道元,闵京华.网络安全技术[M].北京:清华大学出版社.2004.

[2] 胡建伟,汤建龙,杨绍全.网络对抗原理[M].西安:电子科技大学出版社.2004.

[3] 翟光群,张玉凤.网络蠕虫病毒分析与防范研究[J].河南科学,2005,23(6):935~937.

[4] 冯运波.防火墙技术的演变[J].计算机安全,2005,(5):102~105.

[5] Microsoft. Understanding Windows Firewall . http://www.microsoft.com/windowsxp/using/security/internet/sp2-wfintro.mspx, 2006-02.

Windows XP SP2 Firewall Technology and Its Application

Zhang Yu - feng, Zhai Guang - qun

(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: This paper provides the operation method of Windows XP SP2 firewall and application embodiment. It studies Windows XP SP2 firewall (ICF) technology, through inserting, installing, setting up personal firewall and ICF respectively under different networkings. The result proves: The firewall of Windows XP SP2 almost has all the merits of other kinds of personal firewalls, and it takes up less systematic resources, is less likely to be attacked, and has better network security.

Key words: Windows XP SP2 firewall; Network security; The attack guards against

(上接第84页)

的CPU系统时间已经到达98%,这表明CPU已经满荷工作,此时通过计费网关原型的网络带宽和它所处理的响应数应能反映计费网关原型的实际处理性能.测试结果表明:以每秒处理3 300个HTTP请求/响应对,带宽达到47MByte/s的处理能力,基于x86硬件和Linux的计费网关是完全可以满足一个大中型服务提供商的业务需求的.

参考文献:

[1] 张 宏.移动业务管理平台CMX[EB/OL].http://www.cisco.com/CN/network_telecom/2005_06_18.shtml, 2005.6.18.

[2] 李 涛. 无线综合业务网关[EB/OL]. http://www.huawei.com/ProductView_06_02_03.shtml,2006.2.3.

[3] 张 海,李彭军,李 宸. 基于Netfilter框架的计费网关[J]. 计算机应用,2002, 58(12):23~26.

[4] 林子惠. Linux平台下电信级计费网关的研究与实现[D]. 西安:西北工业大学, 2005. 35~48.

[5] 郑 芸. 基于Linux平台下的Email监控系统[J]. 西安交通大学学报, 2002,67(3)45~48.

[6] 杨润华. 高性能IP宽带计费网关的设计与实现[J]. 计算机应用研究,2003, 54(5):23~26.

[7] 尹远洪,张建中. 计费网关中的规则处理模块的设计和实现[J]. 福建电脑, 2004,26(6):89~92.

Research on the Carrier Grade Accounting Router Using Linux

ZHU Si - feng[1,2], LI Hui - min[3]

(1. Department of Mathematical and Information Science, Zhoukou Normal University, Zhoukou 466000, China; 2. Department of Computer Science, Northwestern Polytechnical University, Xi'an 710065, China; 3. Department of Computer, Zhengzhou Science and Technology College, Zhengzhou 450064, China)

Abstract: This paper researches into the actuality the carrier grade accounting router using linux, designs a model of accounting router based on linux kernel, and implements a prototype of accounting router based on linux kernel running in the x86 hardware. The main research contents are as follows: (1) Using the Netfilter framework, dada pack recombine in network level and the application protocol analysis were implemented. (2) Kernel module use Netlink socket to communicate with the user application while the Netfilter to do the application protocol analysis and filtering. (3) Finally, it tested the prototype of the accounting router system with carrier grade x86 server, and proved the availability with the performance data.

Key words: Linux; Netfilter; Linux kernel; accounting router