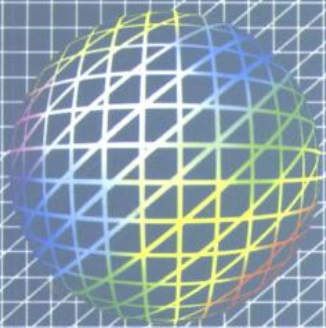


Firewalls 24 seven



网络管理技术丛书

高效构筑与 管理**防火墙**

[美] Matthew Strebe 著
Charles Perkins

吴焱黎 文董正卫 等译



每周7天,

每天24小时

保证网络全天候运转

使你成为

真正的网管专家

seven



电子工业出版社

Publishing House of Electronics Industry

URL: <http://www.phei.com.cn>



seven Firewalls

网络管理技术丛书

高效构筑与管理防火墙

M. 斯特雷
Matthew Strebe
〔美〕 C. 珀金斯
Charles Perkins 著

吴焱 黎文 董正卫 等译

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 提 要

本书全面、系统地介绍了因特网防火墙及其相关的网络知识。作者以必要的理论和技术细节为基础，结合其丰富的实践经验，以实用为目的，分别介绍了因特网安全基础知识、防火墙主要技术、操作系统与防火墙的结合、商业防火墙和其他安全性工具。

本书的读者对象为高级网络管理员和那些对防火墙和网络安全比较感兴趣的读者。



Copyright©1999 SYBEX Inc., 1151 Marina Village Parkway Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

本书英文版由美国SYBEX公司出版，SYBEX公司已将中文版独家版权授予中国电子工业出版社和北京美迪亚电子信息有限公司。未经许可，不得以任何形式和手段复制或抄袭本书内容。

图书在版编目 (CIP) 数据

高效构筑与管理防火墙/ (美) 斯特瑞伯 (Strebe, M.), (美) 伯金斯 (Perkins, C.) 著; 吴焱等译.
—北京: 电子工业出版社, 2000. 4

书名原文: Firewalls 24seven

ISBN 7-5053-4762-4

I. 高… II. ①斯… ②伯… ③吴… III. ①因特网—防火墙—基本知识 IV. TP393.4

中国版本图书馆CIP数据核字 (2000) 第08272号

书 名: 高效构筑与管理防火墙

著 作 者: [美] Matthew Strebe Charles Perkins

译 者: 吴焱 黎文 董正卫 等

责任编辑: 春丽 杨荟

印 刷 者: 北京天竺颖华印刷厂

装 订 者: 三河金马印装有限公司

出版发行: 电子工业出版社 URL: <http://www.phei.com.cn>

北京市海淀区万寿路173信箱 邮编: 100036 电话: 68279077

北京市海淀区翠微东里甲2号 邮编: 100036 电话: 68207419

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 19.375 字数: 490千字

版 次: 2000年4月第1版 2000年4月第1次印刷

书 号: ISBN 7-5053-4762-4
TP·2298

定 价: 33.00元

版权贸易合同登记号 图字: 01-1999-2985

凡购买电子工业出版社的图书, 如有缺页、倒页、脱页请向购买书店调换。

若书店售缺, 请与本社发行部联系调换。

译者序

随着因特网的迅猛发展，电子商务的日新月异，信息化社会的逐渐形成，网络安全变得越来越重要了。作为网络安全技术中保护内部网络不受公共网络攻击威胁的重要部分，防火墙越来越受到人们的重视。本书的作者从网络的基本框架结构入手，针对黑客攻击，以防火墙的基本安全功能为依托，考虑网络及网络用户的安全、使用和经济需要，从各个不同的角度对现代的防火墙技术做了十分详尽的分析和论证。

这本书可以分为理论和实践两个部分。理论部分包括介绍黑客的分类和他们使用的攻击方法，如死亡之Ping、服务拒绝攻击等；同时介绍了TCP/IP的结构以及因特网中的一些基本概念，如服务和套接字等；在加密的基础知识中介绍了公钥和私钥加密方法等；在介绍防火墙的基本功能时讲述了包过滤器、代理、网络地址翻译和虚拟专用网等。本书的实践部分包括不同操作系统上运行的防火墙如Windows NT和Linux上的防火墙功能等；还介绍了免费防火墙、商业防火墙及它们的主要功能，如WinGate、微软的代理服务器等。在每一章的结束部分，还有生动的案例分析介绍作者的一些实际工作经验。在本书的附录部分还可以查询到十分有用的关于网络安全的站点。

本书的第一、二部分由吴焱翻译，第三部分由董正卫翻译，第四、五部分和其他部分由黎文翻译。参加本书翻译工作的还有左林、尹春梅、袁德丽等。本书的翻译工作还得到了美迪亚公司工作人员的大力支持，在此一并表示感谢。

由于时间仓促及译者的水平有限，书中难免有不当之处，希望读者批评指教。谢谢！

译者

致 谢

我要感谢我的合作者，**Charles Perkins**，他给予了我极大的帮助。没有他的帮助，你可能要在两个多月之后才能读到这本书。

我还要感谢将这本书形成一个整体的**Sybex**的工作人员，尤其是**Malka Geffen**在比预期要多好几个月的时间里一直保持着对本书的极大热情；**Maureen Adams**将我的技术难题总结在一起；**Guy Hart-Davis**在搜集信息方面投入了很大精力，还有**Rodany Zake**对于我第一次写作技术书籍所给予的极大支持。还要感谢**Sybex**的其他工作人员：**Kristin O'Callaghan**，**Senoria Bilboo-Brown**，**Richard Ganis**，**Grey Magauran**，**Nila Nichols**和**Lisa Reardon**。也要感谢那些为这本书的基础提供实际工作经验的我的客户们。

——**Matthew Strebe**

在这里，我要感谢**Sybex**中的每一个人，他们在这本书中投入了辛勤努力，尤其是**Guy Hart-Davis**、**Maureen Adams**、**Malka Geffen**和**Lisa Reardon**。我也要感谢给我不懈支持我的家里人：**Charles & Georgia**、**Donna & Cliff**、**Cathy & Jeff**、**Becky & Mike**和**Joe**。

——**Charles Perkins**



前言

防火墙（Firewall）是因特网技术的最新发展之一。在20世纪80年代中期，诸如Compaq和IBM这样的大计算机销售商从不完善的安全系统中开发出了防火墙，这些大公司使用防火墙来保证他们自己网络的安全。这些网络卫士随着信息战争威胁的萌芽应运而生了。最令人们感兴趣和最新的发展，像网络地址翻译（Network Address Translation）和多层安全过滤，变化得如此之快，以致于刚出版两年的书就过时了——而我也希望这本书能有两年的生存期。

过去的安全问题可以使用简单的包过滤器或回拨调制解调器存储区解决。未来的安全问题将需要快速浏览并验证因特网信息中的每一个字节；需要在连接上网前加密站点真实的身份标识；还要加密最近互相传输的任何东西。幸运的是，技术和使用这些技术的团体反映了这些进展，使这些方法变得简单并不可见。由于销售商使操作系统更能抵抗攻击，对于那些可以在网上随意冲浪的人来说3W（World Wide Web）也悄悄地变得更安全了，只是偶尔地出现“这个站点没有授权”的警告或者出现了一个包含可疑内容的信息而受到阻碍。不过，网络本来就该这样。

现在的安全问题几乎都可以使用防火墙和虚拟专用网来解决。外围的安全工具如入侵检测器和安全扫描器尽其职责发出警报和警告，但是防火墙仍是因特网安全的基础，除非防火墙的功能性被植入到因特网使用的每个协议中，或者是每个连到因特网上的计算机都包含防火墙的等价物。即使以上的假设都实现了，因特网集中化的管理策略也将使公司网络长期使用防火墙。

关于这本书

写这本书是要完成这样一个目的：教授网络管理员要想明白因特网安全威胁，他们需要知道一些什么；使用什么样的技术去防范这些威胁；现在有什么样的产品可以帮助他们。当我无法在不同销售商之间找到一种共同语言将各种偏重于理论的防火墙书籍与在Web站点上的促销广告进行比较时，我希望有这样一本书；当我需要帮助我的某个特殊顾客找到某个满足其特殊需要的特殊防火墙产品时，我希望有这样一本书。

这本书将帮助你回答诸如这样的问题：

- 包过滤功能和状态检查之间有什么区别？为什么知道这个很重要？
- 使用网络地址翻译和使用代理服务器隐藏客户之间有什么不同？
- 购买一个防火墙产品需要做多少预算？
- 哪种防火墙更适合我的公司？

这本书主要是为那些积极的网络管理员写的，这里假设他们理解如何使用和配置TCP/IP协议，并且他们熟悉Windows NT, Novell NetWare，或者是UNIX操作系统（尽管书中没出现多少关于操作系统细节的知识）。

如果你不是一个网络管理员，但知道需要一个防火墙，这本书也可以帮助你找到现有许多即插即用的防火墙设备，并且这些设备不但安全而且容易使用和配置。如果你属于后面

这一类，可能会发现在书中前面部分一些关于技术的讨论比较难懂。你可以随意跳过任何不懂的部分，而在其后需要时再返回来读。

这本书是如何组织的

这本书分为五个部分和一个附录，五个部分中包含十九章。第一部分和第二部分应从头至尾按顺序看，其余部分随意。

第一部分：因特网（Internet）

第1章至第5章覆盖了在我们钻研防火墙技术之前应该理解的一些知识，如因特网，防火墙的基本功能，黑客，加密和TCP/IP内部工作的详细解释。

第二部分：防火墙技术

第6章至第10章包含了大多数防火墙都基于的四个主要技术：包过滤功能（packet filtering），网络地址翻译（Network Address Translation），身份认证（authentication）和通道技术（tunneling）。这部分也详细介绍了为保证任何防火墙能被安全地配置应采取的措施。

第三部分：操作系统与防火墙功能

第11章和第12章讨论了可以对操作系统采取何措施来保证所提供服务的。这点对公共服务器尤其重要。

第四部分：商业防火墙

第13章至第16章是本书最有特点的一部分——它对大部分商用的防火墙解决方案进行了介绍。你可以使用这些章节来对比不同的防火墙并为你的组织找到最合适的。

第五部分：其他安全性资源

第17章至第19章包括了基于防火墙之上的可用来保证网络安全的工具，也描述了黑客用来攻击防火墙的不同方法。

获得更多

安全性并不是一个静态的东西，它是一个不断演化的过程。不可能只是加入一个防火墙就希望它能永远地解决安全性问题。随着攻击方法的改变，相应的解决方案也就过时了，随之防火墙也就失效了。要想获得真正的安全，就必须保持警惕。我发现这样做最容易的办法就是成为附录A中所列站点的邮件清单上的一员并访问这些站点。

本书的相关站点为www.24sevenbook.com，在该站点上我将有规律地贴出一些到重要安全信息的链接。就认为它是到安全世界的一个入口吧。

目 录

第一部分 因特网 (Internet)

第1章	理解防火墙	1
	防火墙构件	2
	有效的边界安全	9
第2章	黑客	19
	黑客的种类	19
	攻击载体	23
	黑客使用的技术	24
第3章	从安全的观点看TCP/IP	36
	你必须熟悉TCP/IP	36
	TCP/IP规则	36
	传统的网络结构	38
第4章	从安全的观点看套接字和服务	59
	利用基于套接字的服务	59
	因特网名	62
	协议	66
第5章	加密	75
	如何保守秘密	75
	网络中的加密	79
	密码分析人员的协同工作	82

第二部分 防火墙技术

第6章	包过滤功能	91
	无状态包过滤器是如何工作的	92
	状态检查包过滤器是如何工作的	96
	通过包过滤器进行的黑客行为	98
	包过滤功能的最好实现	99
第7章	网络地址翻译	101
	解释NAT	101
	NAT的问题	108
	通过NAT进行攻击	109
第8章	应用级代理	112
	代理如何进行工作	112
	代理的最好实现	119

第9章 虚拟专用网	123
解释虚拟专用网	123
VPN的特点	126
VPN的类型	128
保证远程访问的安全	130
VPN的最好实现	131
第10章 理想的防火墙	135
定义你的安全需求	135
配置规则	139

第三部分 操作系统与防火墙功能

第11章 作为防火墙的NT	151
性能	152
局限	158
Windows 2000	159
第12章 免费防火墙	164
Linux与IPChains	164
可信信息系统防火墙工具箱	168
FreeBSD和Drawbridge	171
用DOS和IPROUTE进行包过滤	176

第四部分 商业防火墙

第13章 Windows NT的防火墙	183
Firewall-1	184
NetGuard的Guardian NCC	188
NAI的Gauntlet	192
Axent的Raptor	197
Microsoft的Proxy Server	201
第14章 UNIX防火墙	206
AltaVista Firewall 98	206
Unicenter TNG Network Security Optioon	209
SecurIT Firewall	211
WatchGuard FireBox II	213
NetWall	216
SunScreen EFS	218
第15章 其他防火墙	222
BorderManager	223
Elron Firewall	226
GNAT Box	229
AS/400使用的IBM Firewall	232

第16章 专用防火墙	236
PIX Firewall	236
Lucent Managed Firewall	239
SonicWALL	241
NetScreen 10 & 100.....	244

第五部分 其它安全性资源

第17章 安全性实用工具	249
你已拥有的软件	250
安全性分析工具	258
协议分析器	260
轻型代理	261
虚拟专用网 (VPN)	262
加密工具	263
口令强度检查器	264
第18章 攻击概览	267
服务拒绝攻击	267
利用型攻击	272
信息收集型攻击	274
假消息攻击	277
第19章 入侵检测	280
不寻常的入侵问题	280
侵入工具与技术	281
入侵检测系统	283
已有的IDS系统	285
附录A 在线资源	293



第一部分 因特网 (Internet)

主要内容:

- 因特网是如何工作的
- 防火墙是如何工作的
- 谁盗用数据
- 黑客的动机
- TCP/IP基础
- TCP/IP高层协议
- 黑客如何寻找TCP/IP的薄弱环节
- 加密是如何进行的
- 加密如何在因特网上提供安全
- 加密如何提供证实用户身份的机制

第1章 理解防火墙

不能控制国界的国家不能保证其公民的安全，也不能制止海盗和小偷。不能控制访问的网络不能保证存储数据的安全和保密，也不能防止黑客盗用网络资源。

因特网提供的通信效率使直接连接到因特网的私人网络大量增加。直接因特网连接很容易使黑客盗用私人网络资源。在Internet出现以前，黑客可以广泛使用的是从家里连接到私人网络的办法，这只有用调制解调器直接拨号和使用公共电话网来实现。那时，远程访问只是相当小的问题。

当将私人网络连接到因特网时，实际上是将你的网络直接连接到每个直接连在因特网的网络上。在那里没有固定的中央安全控制点。

防火墙 (Firewall) 被用来在私人网络的边界上建立的安全检查点。通过在因特网和私人网络之间提供路由功能，防火墙检查所有在这两个网络间的通信，防火墙根据这些通信是否匹配已编好的策略规则来决定通过或是断开通信。如果防火墙正确配置了并且没有严重的可被利用的错误，你的网络将会远离风险。

现在，可选择的防火墙产品有几百个，不同专家对如何使用防火墙保证网络安全也有不同的理论。这章将详细讨论一个普通防火墙的操作，论述在防火墙中所需的重要功能的轮廓，并讨论防火墙如何在不同大小的网络中部署。第一部分的其他部分更详细介绍由这章引出的概念。第二部分详细介绍了高级的防火墙概念。本书的第三部分对比了流行的防火墙产品，其中包括这些产品的安装和配置。

防火墙构件

防火墙通过检测在内部网与外部网（如因特网）之间的请求，然后允许或是拒绝每个连接请求，使因特网连接尽量安全。功能强大的防火墙是在所有软件层上——从数据链路层到应用层——保护网络。

防火墙位于网络的边界，也就是说在那些提供访问其他网络的网关上。因此，防火墙被认为是边界安全。边界安全的概念是非常重要的——没有它，网络中的每个主机都将不得不自己执行防火墙的功能；有了这个概念，就没有必要花费宝贵的计算资源，没必要增加连接、身份认证所需的时间，没必要在本地的高速网中加密数据。防火墙使你可以集中化管理那些为上述任务而优化并专门从事上述任务的机器上的所有外部安全服务。

也由于防火墙的本质，防火墙在内部网和外部网之间造成了瓶颈，因为所有外部网和内部网之间的通信都要必须通过单一的一个控制点。这只是为安全付出的很小代价。由于外部租用线的连接速度比现代的计算机速度相对要慢，所以由防火墙引起的等待时间就相当明显了。

防火墙的主要功能都使用下列的三个基本方法：

包过滤功能（Packet Filtering） 拒绝接受从未授权的主机发送的TCP/IP包，并拒绝接受使用未授权服务的连接请求。

网络地址翻译（Network Address Translation, NAT） 翻译内部主机的IP地址而使外部监视器无法探测到它们。NAT也称为IP伪装（IP masquerading）。

代理服务（Proxy Service） 代表内部主机进行高层应用连接，完全中断内部主机与外部主机的网络层连接。

大多数防火墙也执行下面两个重要的安全服务：

加密的身份认证（Encrypted Authentication） 允许公共网络上的用户从外部网络为获得对专用网络的访问权证实他们的身份。

加密通道（Encrypted Tunnels） 通过公共媒介（如因特网）为两个专用网络之间建立一个安全的连接。这将使两个物理上分离的网络使用因特网连接而不是租用线连接进行通讯。通道技术也称为虚拟专用网技术（Virtual Private Networking, VPN）。

几乎所有的防火墙都使用上述这些基本功能提供安全服务。现在市场上有几百种防火墙产品进行着激烈的市场竞争。大多数产品都功能强大，只是在一些表面的细节上有所不同。这章的剩余部分将介绍大多数防火墙都支持的这五大基本功能。

也可以使用只执行上述功能之一的设备或是服务；例如，使用一个路由器执行包过滤功能，然后让另外一台机器做代理服务器。在这种情况下，或者是包过滤器必须将通信内容送至代理服务器，或者是代理服务器必须在没有包过滤保护的情况下置于网络之外。这两种情况都没有使用在一个地方执行所有这些功能的一个防火墙产品安全。

包过滤器（Packet Filter）

第一个因特网防火墙就是包过滤器。包过滤器将网络协议（如IP）和传输协议包（如TCP）与一个规则数据库进行比较，只有在这些包符合规则数据库中的细则的情况下才转发这些包。包过滤器可以在路由器中实现或在TCP/IP服务器栈中实现（见图1.1）。

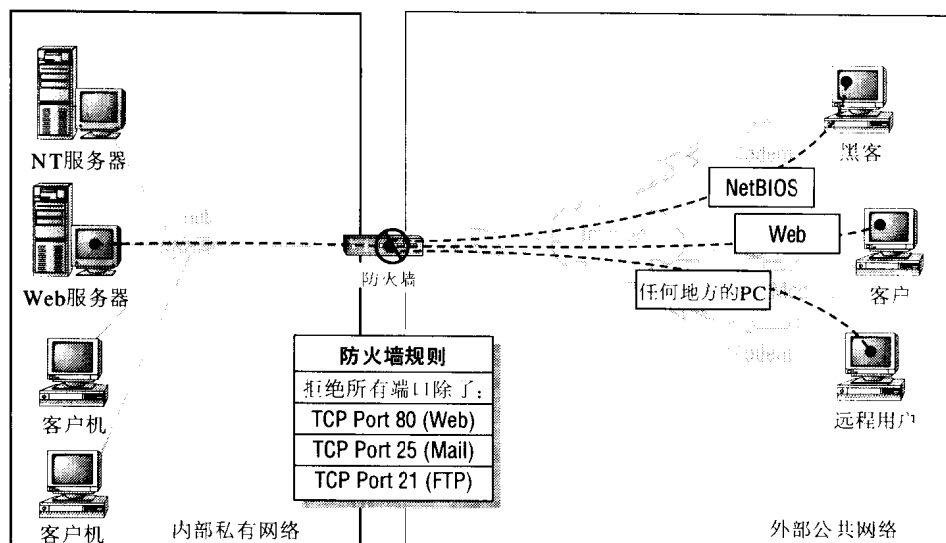


图1.1 过滤因特网连接阻断不想接受的通信

在路由器内实现的包过滤器防止可疑的通信到达目标网络；而服务器中的TCP/IP包过滤器模块只是防止某个机器响应可疑的通信，通信仍能到达网络并锁定网络上的计算机。路由过滤器保护目标网络上的所有机器不接受可疑的数据传输。正是由于这个原因，服务器的TCP/IP栈中的过滤功能（如NT中提供的）只能在过滤路由功能之外实现，而并不能代替它。过滤器通常遵循下面的规则：

- 放弃入站的连接请求但允许出站的连接请求通过。
- 去除绑定在那些不允许连接到因特网的端口（如NetBIOS对话口）上的TCP包，但允许那些应连接到因特网的端口（如SMTP，简单邮件传输协议）上的包通过。大多数过滤器能明确指定哪个服务器的哪种通信允许通过——例如，在端口号25上的SMTP传输只允许到达某个邮件服务器的IP地址上。
- 限制对某个IP地址范围的人站访问。

警告： 那些带有需要为返回的通道打开1023以上端口包过滤功能的简单包过滤器或是路由器，对于安全来讲都不是十分有效的设备。这些包过滤器并不能阻止内部用户或是特洛伊木马在客户机的1024端口以上建立一个欺骗性的服务，而仅仅是侦听从外部来的连接请求。防火墙（这里指的是检查所有状态的过滤器和安全协议）只为那些在安全范围内被要求返回一个连接请求的服务器打开通道——选择这些服务器而不选择那些不能保持连接状态简单包过滤器。

复杂的过滤器使用专用的算法检查所有通过它们的那些连接的状态，并寻找黑客攻击的证据，如资源路由，ICMP（Internet Control Messages Protocol，网间控制报文协议）重定向，IP地址假冒等。表现出这些特征的连接都将被中断。

一般都允许因特网客户建立与外部主机的连接，而外部主机通常不允许启动连接请求。当内部主机决定启动一个TCP连接时，这个主机就发送一个报文到那个公共服务器的IP地址和端口号（例如，www.microsoft.com:80连接到微软的Web（万维）站点）。在这个连接启

动报文中，它告诉远程服务器它的IP地址是什么和哪个端口侦听响应信号（例如，localhost:2050）。

警告：早期的FTP客户机和服务器只在这样的情况下才能正确地工作，即远程服务器被允许在TCP端口20上建立数据通道，而这样将破坏一般的规则，此规则使所有入站请求都将被截断。近期的FTP产品支持被动连接，这将允许客户建立命令通道（21）和数据通道（20）。现在的状态检查防火墙允许客户机建立它自己的返回通道。通常不值得为支持早期的ftp软件而降低安全性。

外部服务器通过将数据传送到由内部客户提供的端口的方法来返回数据。由于防火墙检查所有在内部主机和外部主机之间的数据交换，防火墙也就知道连接是由带有其内部接口的内部主机启动的，外部主机的IP地址是什么，和内部主机希望从哪个端口接受返回的数据。那么防火墙就记住允许在连接报文中指定的主机把数据返回到仅在这个端口指定的内部主机IP地址。

如果连接中的那个主机关闭了TCP连接，防火墙就在它的状态表中删除这个条目（它的连接内存），而这样也允许远程主机将传输的数据返回到内部主机。

过滤功能并不能完全解决因特网的安全问题。首先，在内部过滤器中的计算机IP地址将在出站数据传输中体现出来，这样就很容易被人侦察到过滤器内部因特网主机的类型和数量，也很容易针对这些地址进行攻击。过滤功能并不隐藏过滤器内部主机的标识。

过滤器不能完全检查基于高层协议的IP报文中的所有片段，如TCP报文头，因为这个报文头只在第一个片段中出现。接下来的片段没有报头信息并仅能与IP层的规则来比较，这样就放过了一些不应该进行的数据传输通过过滤器。这将使网络上目标计算机IP栈中的程序错误和恶意攻击程序有了可乘之机，这也会使与内部网络中的特洛伊木马的通信得以进行。

操作系统的过滤功能

在大多数UNIX和Windows NT的版本中都在TCP/IP协议接口中包括包过滤功能。既可在一个功能强大的防火墙的基础上再加上这个过滤功能来控制对某些服务器的访问，也可以在内部组织中不设防火墙而仅把这个包过滤功能做为衡量内部安全的附加标准。正像过滤功能不能完全保证整个网络的安全一样，操作系统的过滤功能对于建立一个完全安全的环境也是不够的。

不要只依赖操作系统中内置过滤功能来保护整个网络。用户可以在网络内部使用操作系统的过滤功能建立一个过滤器来使那些确实希望使用的协议通过。这样可以使软件不会在不希望的方式下工作，也可以使特洛伊木马失效，即使它们要设法安装到你的系统中的话。

基本的操作系统过滤功能允许用户为自己网络中的每个适配器定义接受准则，这些准则是针对基于下面的入站连接的：

- IP协议号
- TCP端口号
- UDP端口号

这个过滤功能通常并不用在出站连接中（这些连接是从你的服务器中发出的），并在系统中为每个适配器分别定义。

注意: Windows 2000支持出站过滤功能; Windows NT 4不支持。

一个典型的服务器设置服务来监听下面的端口。这些端口要想正常提供服务就必须通过过滤器打开这些端口。

简单TCP/IP服务通常侦听下面端口:

端口	TCP/IP服务
7	Echo (回应)
9	Discard (放弃)
13	Daytime (时间)
17	Quote of the Day (对日期的引用)
19	Character Generator (字符生成器)

因特网服务器侦听下面端口:

端口	服务器
21	File Transfer Protocol (FTP, 文件传输协议)
23	Telnet (远程登录)
70	Gopher (一种基于文本的分布式菜单查询系统)
80	World Wide Web (HTTP, 超文本传输协议)
119	Net News (NNTP, 网络新闻传输协议)

文件服务器通常侦听下面的端口:

端口	服务
53	Domain Name Service (DNS服务, 域名服务, 如果安装了的话)
135	RPC Locator Service (远程过程调用定位器服务, 只在Windows NT中使用)
137	NetBIOS Name Service (NetBIOS名字服务, 只在WINS服务器中使用)
139	NetBIOS Session Service (NetBIOS对话服务, 只在Windows网络和SMB/CIFS服务器中使用)
515	由TCP/IP打印服务使用的LPR, 如果安装了的话
530	Remote Procedure Call (远程过程调用, 由Windows NT的WinLogon服务和许多其他高层网络应用程序使用的RPC)

邮件服务器通常被配置为侦听下面的端口:

端口	邮件服务器
25	Simple Mail Transfer Protocol (简单邮件传输协议, SMTP, 邮件服务器对服务器的邮件交换)
110	Post Office Protocol version 3 (邮局协议版本3, 服务器对客户机的邮件交换)
143	Internet Mail Access Protocol (因特网邮件访问协议, 客户访问邮件服务器)

如果你安装了其他服务软件，就必须确定服务器的过滤器被设置为侦听服务需要的那些端口——否则，服务就不会工作。在软件制造商那里找到这些服务都需要哪些端口。这些并不应用在边界防火墙中，如果希望为公众提供这些服务，只需配置边界防火墙允许这些服务通过。

缺省情况下禁用所有协议和地址，然后明确指定希望支持的服务和主机。禁止所有到内部网络主机的连接请求。如果许可了任何人站连接请求，也就允许黑客建立到特洛伊木马的连接和利用恶意攻击程序。过滤掉并且不同应ICMP重定向和回送（ping）报文。截断所有TCP源发送的包。TCP源路由包很少用在合法的目的上。截断所有发向内部路由器上的外部发送协议（RIP，OSPF）的更新。网络以外的任何人都不应传输RIP更新信息。考虑禁用片段号在零以上的片段传输，因为这些功能大多过时并经常被滥用。将公共服务主机如Web服务器和SMTP服务器放在包过滤器之外，而不是在包过滤器上开一个洞。不要相信单独一个包过滤器就可以保护你的网络。

使用IP伪装

网络地址翻译（NAT，Network Address Translation），也就是所说的IP伪装（IP masquerade），解决了隐藏内部主机地址的问题。NAT实际上是一个基本的代理：某个主机名代表所有内部主机提出请求，这样就使这些主机的身份不为公网所知。Windows NT不提供这个功能——如果需要使用IP伪装就必须使用第三方的防火墙产品。Linux和许多UNIX操作系统提供了这个功能，作为推销操作系统的一部分。

注意：Windows 2000支持网络地址翻译；Windows NT 4不支持。

通过将所有内部主机地址转化为防火墙地址，NAT就隐藏了内部IP地址。然后防火墙就重新传送因特网主机的数据，防火墙使用自己的地址重传数据，并使用TCP端口号来跟踪公共网上哪个连接与专用网的哪个主机相对应。对于因特网，所有在内部网络中对外的传输好像都是从一台相当忙碌的计算机中发出的。

NAT有效地隐藏了所有有关内部主机在TCP/IP层次的信息，避免了它们被因特网上的窃贼发现。地址翻译也允许在内部网络中使用任何你想使用的IP地址范围，即使这些地址已经在因特网中的其他地方已经使用了。这就意味着你不必在InterNIC那里注册一个地址块了，或者不必在连接到因特网之前从那些得到的简单地址中重新分配网络地址了。

警告：尽管你可能在带有NAT的防火墙之后使用任何IP地址块，但是要注意，在访问因特网上具有与内部网络中的某个计算机相同IP地址的机器是会遇到问题的。由于这个原因，为避免这种情况的发生，最好在防火墙内使用保留的10.0.0.0网段（或其他保留的网段）。

最后，NAT允许在整个网络上复用一个IP地址。许多小的公司依靠一个上游因特网服务供应商的服务，而这些上游服务提供者并不愿提供大的地址块，因为他们自己的地址范围也是很有限的。你可能希望在不告诉ISP的情况下共享一个拨号或电缆调制解调器。如果使用IP伪装这些操作都是可能实现的。

另一个不好的方面是NAT只在TCP/IP上实现。再一次强调，这意味着隐藏在TCP/IP有效数据中的信息可能被传输到一个高层的服务中，并被利用来发现高层传输中弱点或用来传输特洛伊木马。所以还必须使用一个高层的服务如一个代理来避免高层服务的安全问题。

代理 (Proxy)

NAT解决了许多与直接连接到因特网上相关的问题，但是它仍不能完全约束通过防火墙的数据报流。对于那些使用网络监视器的人来说，观察从防火墙出来的数据传输并确定这个防火墙是否正在为其他机器做地址翻译是可能的。接下来，黑客截下TCP连接或假冒返回的连接通过防火墙也是可能的。

应用程序级的代理避免了上述问题的发生。应用程序级代理允许完全断开通过防火墙的网络级协议数据流并将网络通信仅限于高级协议如HTTP，FTP和SMTP。

代理允许对服务器的出站连接请求，然后代表客户向实际的目标服务器发出请求。当服务器返回数据时，再把数据传输给客户。代理基本上是执行了一个良性的中间人攻击，并且代理是一个很好的例子，它表明你和另外一个终端用户之间的任何路由器如何在没有你的许可下可以秘密地执行任何处理过程。

应用程序代理（如微软代理服务器）与网络地址翻译和过滤器不一样，因为因特网客户机应用程序被设置为与代理对话（通常是这样的）。例如，你告诉IE（Internet Explorer，微软公司的网络浏览器）你Web代理的地址，IE将所有的Web请求发送给代理服务器而不是解析IP地址并直接建立一个连接。

注意：如果没有过滤器或是IP伪装，通过简单地使在Web浏览器中代理的设置失效，就无法阻止用户绕过应用级代理。

应用程序代理不一定非要在防火墙上运行；无论是在网络内还是在网络外任何服务器都可以执行代理服务器的功能。没有防火墙，你仍是没有任何真正的安全，所以你既需要代理也需要防火墙。至少必须放置某些类型的包过滤器保护代理服务器不受网络层的服务拒绝攻击（例如著名的“死亡之ping”）。并且，如果代理不在防火墙上运行，你就必须以某种方式在防火墙上打开一个通道。理想情况下，防火墙将执行代理服务器的功能。这会使从公网方面来的包不能通过防火墙。

有一些防火墙代理要比其他的复杂的多。因为它们具有IP包过滤功能和IP伪装功能，它们能简单地阻断连接到远程主机的出站请求（如HTTP的80端口）而不是配置客户软件具体地寻址代理服务。然后防火墙代理连接到远程服务器并请求代表着锁定的客户的数据。通过使用防火墙的NAT功能检索到的数据返回到请求的客户，看上去防火墙代理就像远程服务器一样。代理的这种操作方式被称为是透明的。

安全代理甚至具有为指定内容执行应用程序级过滤功能的能力。例如，一些防火墙HTTP代理寻找HTML页中的标签，这些标签要引用嵌套了Java或ActiveX的小程序，然后剔除指定的部分。这将防止小程序在客户机上执行，并消除用户意外地下载特洛伊木马的危险。这种类型的过滤功能相当重要，因为如果你的用户受到诱惑下载了嵌套在ActiveX中的特洛伊木马，过滤功能、代理功能和IP伪装功能并不能防止网络受到攻击。

你可能已经注意到了，当网络的层次越向上时，安全服务也就变得越专门化了。例如，过滤功能就在IP，TCP和UDP中变得越来越专门化了。与IP共同使用其他协议的应用程序如Banyan Vines就必须使用价格特别高的或者说功能非常强大的防火墙。

代理更是极其专门化，因为它们只能为某个指定的应用程序工作。例如，你必须要有