
Firewalls
The Complete Reference
HZ BOOKS
网络与信息安全技术丛书
设计、配置和维护当今最流行的防火墙
防火墙
技术大全
(美) Keith E. Strassberg
Richard J. Gondek
Gary Rollie
等著
李昂 刘芳萍 杨旭 程鹏 等译
Mc Graw Hill Education
机械工业出版社
China Machine Press

网络与信息安全技术丛书

防火墙技术大全

Keith E. Strassberg
（美） Richard J. Gondek 等著
Gary Rollie

李昂 刘芳萍 杨旭 程鹏 等译

机械工业出版社
China Machine Press

本书介绍了目前流行的七家防火墙产品系列的安装步骤、关键的配置选项及重要的维护工作等内容。还讲述了防火墙的网络基础、支持的网络布局设计、体系结构以及各种高级功能的实现原理。

本书内容具体包括：防火墙的网络基础、针对网络设计考虑、防火墙体系结构、高级功能以及对防火墙攻击的分析；本书重点提供Check Point Firewall-14.1和NG、Cisco PIX、Linux IP table、Microsoft ISA Server、NetScreen、SonicWall以及Symantec等七家不同厂商防火墙系列产品的背景介绍、功能描述、安装、配置和管理知识。

本书涉及的内容新颖全面，基础知识讲解清楚、描述清晰，与实际产品结合紧密、实用性极强。该书适合于网络安全管理员、工程师和技术人员，也适合于广大对防火墙感兴趣的读者作为参考。

本书版权登记号：图字：01-2002-4796

图书在版编目（CIP）数据

防火墙技术大全（美）斯特拉斯伯格（Strassberg, K. E.）等著；李昂等译. －北京：机械工业出版社，2003.3

（网络与信息安全技术丛书）

书名原文：Firewalls: The Complete Reference

ISBN 7-111-11524-4

Ⅰ.防… Ⅱ.①斯… ②李… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2003）第001669号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：谢晓竹 李 炎

北京瑞德印刷有限公司印刷·新华书店北京发行所发行

2003年3月第 1 版第 1 次印刷

787mm × 1092mm 1/16 · 36.5印张

印数：0 001- 4 000册

定价：59.00元

前　言

当网络涉及不同的信任级别时（例如Intranet、Internet或是网络划分），要保证安全必须安装安全控制设备。此类控制设备几乎总是某种形式的防火墙。

防火墙能够确保非授权的访问在经过企业的对外访问点时被阻止。防火墙技术已经出现十多年了。这项技术最初来自在路由器上实现简单的访问控制表。由于网络协议的复杂性，路由器的ACL被证明是不够的。例如文件传输协议FTP，会建立一个来自目标主机的反向通道。于是基于主机的防火墙诞生了。各种有竞争力的防火墙技术不断出现，不过到20世纪90年代末期，基于包的状态防火墙出现，并因为协议的灵活性和性能而成为最佳选择。

这几年出现的另一个现象是用专用网络设备代替通用计算机（Wintel，Sun）来实现防火墙。网络速度从10Mb增加到1G，一下提高了两个数量级。基于主机的防火墙并不是为这种高速网络环境设计的，从而加速了向专用平台的转移。采用专业网络设备的附带好处是因为操作系统的简化而相对较容易配置和管理。

在过去的五年中，防火墙供应商之间的差别已经缩小了。大多数供应商重组他们的产品，来包含状态包过滤和VPN。新的操作系统集成了一些防火墙的功能，例如Windows 2000/XP、Solaris 8以及Linux。大多数网络设备，包括防火墙，在管理和监控的可扩展性方面仍然比较薄弱。这对于大规模的防火墙设置是个重要问题，在这方面没有一家产品控制市场。

VPN比防火墙技术晚出现几年，它和企业的端点位置有关。如果VPN网关位于防火墙的后面，防火墙必须通过加密网络流。不只是目的端网络地址，隧道中的所有信息均加密。最好的解决方法就是在防火墙之前结束IP隧道。对大型企业来说，将防火墙和VPN功能集成在一个设备中还为时过早。将入侵检测加入到同一个平台也还太早。

最好的安全方案是提供多层的访问控制，其中防火墙是重要的一层。以后的几年中，随着安全体系组件的商品化，防火墙的功能还会增加。防火墙将不断发展以满足应用层安全控制日益增加的需求。

——Christopher M. King，CISSP
信息安全业务主管
Greenwich技术联盟

注：参与本书翻译工作的人员还有尚红、刘东卫、吴珍珍、王乐欣、徐洪芳、张飞扬、胡飞志、黄中辛、李欣济等。

目 录

第1章 简 介

Internet确实已经成为了人类所构建的最丰富多彩的虚拟世界。其绝对用户的数目正成百上千地在世界各地增长，而且这种增长将一直持续下去。Internet这个虚拟世界欢迎每一个人前来做生意、相互沟通、研究信息或仅仅是享受网上冲浪的乐趣，其庞大的规模连同其使用者的互异性一起创建出了一个绝无仅有的融合体。此外，它也存在被误用、滥用和用来实施犯罪的可能性，而这种会导致危害的可能性使得用来保护Internet资源的安全措施和设备变得不可或缺。

几乎与Internet一样众所周知的，还有那些费尽心机闯入他人计算机系统的“黑客”（hacker）及其不怀好意的同党“破解者”（cracker）。不幸的是现如今闯入一个系统已不再需要什么高深的计算机技巧，现在词汇表里有一个新词儿叫“脚本玩家（script kiddie）”，“脚本玩家”其实没有什么神奇的计算机魔力，而只是拥有一段专为发现和闯入别人系统而编写的程序。“脚本玩家”并不了解那段程序是如何进行攻击闯入的，他仅仅知道如何去使用。甚至那些“脚本玩家”也逐渐在整个攻击过程中丧失了作用，因为程序已经变得非常智能化，不用人参与就能完成对系统的扫描和破坏。这种情况使得近几年来攻击的频率、密度和实施攻击的资源发生了显著的增长。

Internet用户必须认识到这些地下活动是Internet的一个部分，而且这些地下活动最终会发现你们的系统。Internet遍布于全球，而法律实施机构却没有办法把哪怕只是一小撮网络罪犯绳之以法。但好在事态没有完全失控，我们可以使用很多工具来保护系统安全。其中防火墙是威力最大和效果最好的武器，它使得那些邪恶势力只能在信息高速公路上到处游荡而不能得逞。

本书可以作为设计、构建和维护当今最流行防火墙的参考指南。这本指南不特定局限于哪个供货商，因而既可用于指导新防火墙的实施，也可作为对正在使用的防火墙进行管理的案头参考。它涵盖了适合所有类型用户的有用信息，这些用户既包括大公司的防火墙管理员，也包括小办公室的网管、个人用户及普通的爱好者。

1.1 防火墙的定义

防火墙的基本功能是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。防火墙可以有不同的结构和规模，通常防火墙是由几台计算机构成的。在本书中，防火墙指的是位于可信网络（例如，内部网）和不可信网络（例如，Internet）之间并对经过其间的网络流量进行检查的一台或多台计算机。防火墙有如下特性：

- 所有的通信都经过防火墙。
- 防火墙只放行经过授权的网络流量。
- 防火墙能经受得起对其本身的攻击。

简而言之，防火墙就是在可信网络和不可信网络之间的一个缓冲。“防火墙”这个词实际是从建筑上一种技术派生而来的，这种技术通过用一堵由防火材料建成的墙体来阻止或减缓火势的蔓延。它实质上是一种障碍物。在网络中，防火墙是一个防范从其他网络发起的攻击的屏障。

防火墙既可以是一台路由器、一台个人电脑或一台主机，也可以是由多台主机构成的体系，它们被配置

为专门保护一个私有网络，使其免受那些被处于可信网络之外的主机滥用的某些协议和服务的影响。一套防火墙系统通常位于一段网络的边界，例如某站点与Internet的连接处。然而，防火墙也能够而且应该被置于网络边界之内，因为这样可为一小批特定主机提供额外的、特殊的保护。

防火墙保护可信网络的办法在于它本身及其使用的策略/规则。下面是现今四类主要的防火墙技术：

- 包过滤器
- 应用级网关
- 电路级网关
- 状态包检查引擎

同所有的技术解决方案一样，防火墙技术也面临着其他产品和技术所面对的技术进步和生命周期的问题。第4章和第5章提供了更多关于不同防火墙类型和技术的详细信息。

1.2　为什么使用防火墙

人们要提的第一个问题可能是为什么要使用防火墙？把每个单独的系统配置好能经受住攻击不就行了吗？对此问题最简单的回答是：防火墙只专注于一件事——在已授权和未授权通信之间作出决断，这就避免了在安全性、可用性和功能上进行权衡和妥协。

如果没有防火墙，系统就只能依靠他们自己的安全设备和配置。这些系统可能正在运行升级功能或方便管理的服务，但这些服务可能并不十分安全，或不可信任，或者仅应从一个特定的位置才能被访问。防火墙可用于这种层次的访问控制。

如果周围没有防火墙，安全就完全仰仗主机自身了。而整个系统的安全将由系统中安全性最差的主机所决定。网络越大，把网络内所有主机维护至同样高的安全水平就越复杂。若一时粗心（例如只给15台Web服务器的14台打了关系安全的补丁），则因为简单的配置错误或未能修补所有漏洞就会导致闯入的发生。

防火墙成为了与不可信网络进行联络的惟一纽带，于是管理员就不用再确保多台机器要尽可能的安全了，他只要集中关注防火墙就行了。但这并不是说躲在防火墙里面的系统就不再需要严格的安全措施了，防火墙只是提供了一层避免错误的额外保护而已。

防火墙是一个优秀的审计员。因为所有的网络流量都经过它，那些包含在其日志中的信息可以用来重新构建新的事件以防安全出现缺口。

总之，防火墙减轻了系统被用于非法和恶意目的的风险（例如，被非法攻击者黑掉）。那么这些系统面临的被防火墙所防范的风险又是什么呢？企业的系统和数据有以下三个主要方面受到防火墙保护：

- **机密性的风险**　包括某方未经授权就访问敏感数据或数据的过早泄漏。一个商业公司很容易仅仅是因为泄漏了他们的商业计划、公司交易秘密或财务状况就损失数百万元。
- **数据完整性的风险**　包括未经授权就对数据进行修改，例如财务信息、产品特性或某网站上商品的价格。商业公司的成长和兴旺依赖于其信息系统提供信息的准确性，如果系统信息是不可靠的，那又怎能作出最好的决策（比如销售水平如何？哪一个可用账户是准确的）？
- **可用性的风险**　系统可用性保证系统可以适时地为用户服务（就是说用户需要用它的时候）。那些不可用的系统导致公司损失了大量的财政收入和雇员的生产效率，同时也无形中挫伤了消费者对公司的信心并损坏了公司的公众形象。

1.3　常见攻击类型

前面的几节介绍了为什么个人和团体要使用防火墙。现在的问题是，到底那些攻击是怎样未经授权就获

取了系统访问权？关于攻击的动机不胜枚举，从“看看是否能行得通”到使用一个已被侵害的系统进攻另一个系统，再到协作刺探，甚至仅仅是想把系统搞垮和破坏掉这样简单的恶意动机。

见诸文字的有几十种不同的方法可以使闯入者获取系统的访问权。第6章提供了一些补充的关于对防火墙进行攻击的常见方法的信息。本章在这里只是简要列出了最常见的攻击方法：

- **社交工程** 攻击者哄骗系统管理员或其他授权用户，让他们透露出其登录信息或系统操作的细节。
- **软件错误** 攻击者钻研出了程序的漏洞并能使一个应用程序或服务未经授权就强制运行，他还可以强制运行一些恶意命令。这种攻击在程序运行时带有其他权限或管理权限的情况下尤为危险。这种漏洞通常是指“缓冲区溢出攻击”或“格式化字符串攻击”。

注意 想了解更多关于“缓冲区溢出攻击”或“格式化字符串攻击”的信息，请参考以下网址：

http://www.insecure.org/stf/smashstack.txt

http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html

http://julianor.tripod.com/teso-fs1-1.pdf

- **病毒和特洛伊木马** 攻击者诱骗一个合法用户执行某个攻击程序。最常用的做法是把攻击程序伪装成一个看起来没什么问题的电子邮件或藏在某个病毒里面。一旦被执行，攻击程序就会执行一系列恶意操作，包括安装后门程序、盗取文件和机密甚至删除文件。
- **脆弱的系统配置** 攻击者能够通过其可获得的服务和账户研究出系统的错误。通常这些错误包括没有改变默认账户的密码（既有系统级的也有应用级的）、未限制对应用管理程序的访问或是没有禁止多余的和未用的服务。

除了试图进行未授权系统访问之外，一些恶意的人可能只是想把系统搞垮。对于那些重要的而又被广泛关注的系统应用，由此造成的商业损失将会非常惨重。这些攻击被称为拒绝服务（denial of service, DoS）攻击，它是指某个用户、网络或组织被剥夺了他们通常享有的资源和服务。而某些服务的丧失通常也意味着有关个体网络服务的失效，例如电子邮件和Web服务，有时还会造成网络连接的暂时丢失。

1.4 防火墙的部署

尽管第3章还将对网络设计和防火墙部署有一个更深入地探讨，在这里我们先引出几个话题。防火墙可以并应该安装于两个有不同安全要求的网络互联之处，最常见的是被置于于本地网和Internet相连的地方。而其他常见的防火墙应用还包括保护与第三方的连接，比如与市场数据提供商的连接，以及保护网络内部的与敏感数据的连接。

在讨论网络的时候，本书使用了“网络边界”（network perimeter）这个概念，这个概念是指一个本地网络的整个边界。本地网络通过输入点和输出点与其他网络（例如Internet）相连，这些连接点几乎都装有防火墙。

表面看起来“网络边界”的定义是很简单的，但是随着虚拟专用网络（Virtual Private Network，VPN）的出现，原来很确切的边界变得模糊了。虚拟专用网络技术允许一个远端用户通过防火墙连入一个网络就好像他在网络内部一样。这已经成为一种公司网络的扩展，但是那些外面的主机无法再受到公司防火墙的保护了。那些恶意的攻击者可以先攻破那些外面的用户并通过这种渠道穿过公司的防火墙。管理员应该考虑为那些外面的系统安装个人防火墙以期达到获得一致安全水平的目的。

1.5 防火墙的优势和弱点

防火墙仅仅是整体安全构架的一个部分。然而作为一个比较独立的部分，防火墙的设计应该满足整体设

计中的至关重要的安全需求。和其他事物一样，防火墙也有它的优势和弱点。

1.5.1 优势

一般防火墙有以下优势：

- 防火墙可以出色地完成执行公司整体安全策略的任务。经过适当配置，防火墙应能把通信约束在管理决策所能接受的范围之内。
- 防火墙可用于限制对某些特殊服务的访问。举例来说，防火墙可以允许公众访问Web服务器但禁止他们访问Telnet端口和其他非公开的域。大多数防火墙可以提供在授权机制下的有选择性访问服务。
- 防火墙功能专一。因此，不必在安全性和可用性之间进行什么权衡妥协。
- 防火墙有出色的审计功能。若有足够的磁盘空间或远程记录功能，防火墙能够存录所有经过的网络流量。
- 防火墙可以向相关人员发出警告信息。

1.5.2 弱点

一般来说防火墙有如下弱点：

- 防火墙不能防范经过授权的东西。你可能会奇怪这是什么意思，这就是说防火墙允许其所保护的系统应用的正常通信流量通过防火墙——否则就不对了。如果一个应用程序自身就有错误，那么防火墙也不会阻止由此引起的攻击，因为对于防火墙来说，这是经过授权的。
- 防火墙只是按对其配置的规则进行有效的工作。一个过于随意的规则配置可能会减弱防火墙的功效。
- 防火墙对于社交工程类型的攻击或一个授权用户利用合法访问进行的恶意攻击不起作用。
- 防火墙不能修复脆弱的管理措施或设计有问题的安全策略。
- 防火墙不能阻止那些不经过它的攻击。

1.6 完善的安全措施

虽然关于如何最有效地配置和管理防火墙的完整讨论已经超出本书范围（关于这个话题可以找到很多书），但对一些能够提高防火墙整体安全性能的重要概念作些介绍还是很有益处的。这些概念既可用于防火墙也可用于被防火墙保护的系统。同时请注意，以下介绍的概念和措施相互间并非是排斥的，如果能适当地综合应用，将会获得更高的安全保障水平。

1.6.1 完善系统本身

除了在一些非常罕见的场合，一般系统和其应用程序并非是按最安全的要求安装的。往往会有一些对你系统的功能而言额外的服务被安装上并默认为激活状态，一种好的习惯是只开放系统所提供的服务和最必须的账户。很多闯入的发生都是由于那些对系统而言多余的服务和账户被攻破。这种禁止多余服务和为提高安全性而进行重新配置的措施经常被称作“主机加固”（host hardening）。下面是进行主机加固时可用的一个较小的检查列表：

- 禁止所有的不需要的或不必须的服务。
- 删除不需要的账户和组。更改默认的应用程序和系统账户的密码或干脆禁止它们。禁止那些不需要交互式登录的账户。
- 重新配置剩余的服务以提高安全性。
- 保证所有的管理功能的安全。

• 使用强健的密码。强健的密码是指由多于7个字符并有大写字母、小写字母、数字和其他字符混合构成的密码。

注意 SANS（系统管理监测与网络安全研究所，www.sans.org）出版了一些关于操作系统最佳安全措施的指南。

1.6.2 补丁

如今连绵不绝出现的各种补丁可能会使人们感到不安而且经常会被遗忘。新的攻击很快就会被发现，一个一分钟前还算安全的系统转眼就会变得无比脆弱。若想让系统总是处于最安全状态，就应订阅多份错误提醒邮件列表和软件供货商的邮件列表。比较流行的漏洞提醒服务由以下组织进行维护：

• 由ISS（Internet Security Systems）维护的xforce数据库及邮件列表。

其网址为http://www.iss.net/xforce。

• 由SecurityFocus维护的Bugtraq（一个黑客组织的邮件组）存档的拷贝及邮件列表。

其网址为http://www.securityfocus.com。

• CERT（Computer Incident Emergency Response Team，计算机事故紧急响应小组）的网址为http://www. cert.org。

• CVE（Common Vulnerabilities and Exposures，常见弱点曝光）数据库的网址为http://www.cve.mitre.org。

注意 打了补丁之后，应该确认系统安全性没有被削弱。例如Sun就曾经因为他们发布的Solaris操作系统的补丁把已经禁止的服务重新启用而坏了他们的名声。

1.6.3 硬件与操作系统

早些时候防火墙都是运行于通用操作系统如Windows NT和Unix之上的软件，它们通过修改系统的内核和TCP/IP协议栈来监测流量。所以防火墙的性能就与其所运行的操作系统所存在的问题休戚相关。要想获得较高的安全性，就必须对操作系统进行加固、修补和维护（如前几节所述）。如果没有足够的专业人士或时间来维护一个操作系统的功能，那么这些工作将是既费时又困难的。然而，现在已经有很多防火墙供货商把他们的产品作成硬件了。

硬件防火墙集成了操作系统和防火墙软件的功能，形成了一个整体牢固、功能专一的设备。在集成的过程中，那些对于筛选屏蔽数据包不必要的功能被删除掉了。此外，这种产品提供了功能完善的管理接口，使得防火墙的配置和维护得到了进一步的简化。硬件防火墙在使用时不需要作很多主机加固的工作（当然改变默认密码还是必要的）。管理员不用再费心于重新配置和修补通用操作系统，而是可以集中注意力构思防火墙规则，同原来基于操作系统的软件防火墙相比，硬件防火墙显著地减少了操作和维护的费用。本书将探讨很多硬件防火墙，其中包括Cisco PIX、Netscreen、SonicWall以及运行于Nokia IPSO平台上的CheckPoint FireWall-1。

1.6.4 层次防御

虽然防火墙本身是一个出色的安全工具，但我们并不能完全依靠它。前面曾经提到，防火墙不能防范那些拥有授权的通信。当一个入侵者绕过防火墙又会怎样呢？可以设想如下情况：一个入侵者通过HTTP访问Web服务器并获取了系统shell访问权限。由于通过HTTP访问Web服务器是合法的所以防火墙允许这种访问通过，攻击者可以利用这一点并通过这个渠道去攻击网络上其他的服务器和系统，而这时已没有了防火墙