第16章 防 火 墙

本章解释了什么是防火墙以及它为什么是基于 UNIX与Internet连接的网络分层防御策略的一个重要部分。它提供一些与防火墙、通用防火墙设计相关的策略以及对防火墙工具的概述。

简单地说，防火墙是在被保护的网络与 Internet之间限制访问的部件。它可以路由器或计算机等形式作为硬件来实现，也可以是在一个网关系统上运行的软件，或是它们的组合。

该术语最初来自于建筑业。防火墙通常用防火材料建成，位于相连接的公寓或建筑之间。有了防火墙，在墙一边发生的火灾不会蔓延到相邻的建筑。Steve Bellovin 1987年在给同事的一封电子邮件中第一次把该术语用于计算机安全[1]。像许多Internet术语一样，在物理防火墙和网络防火墙之间的寓意很丰富——很多时候，网络上总有火灾发生。几乎没有机构对感触热量有兴趣。

16.1 为什么要防火墙

Firewall FAQ[2]的作者Marcus J.Ranum和Matt Curtin很好地总结了使用防火墙的理由：

“ Internet像任何其他社会一样被各种各样的人所困扰，他们喜欢用画笔在别人的墙上写字、撕破别人的邮箱或只是坐在街上按喇叭来享受电子平等。有些人试图通过网络做一些真正的工作，其他人有一些保密或私人数据需要保护。一个防火墙的目标就是把那些无事生非的人挡在你的网络外，而使你仍能完成自己的工作 ”。

防火墙就像交通警察那样做两件事之一 ：让交通工具通过，或把它们挡住。像现实世界的警察一样，防火墙可以允许（在该范围内允许数据流通过）或偏执地拒绝除了特定的、事先认证的数据块以外的数据通过。用这种方式，它们体现了机构希望推行的安全策略。

像中世纪城堡的壁垒那样，良好的防火墙能够成为一个分层防御策略的重要部分。没有防火墙，一个LAN或子网对于外部攻击很脆弱，可能是因为 NIS的NFS这样的服务、薄弱的口令或系统的错误配置。整个网络的安全完全依赖每台主机上维护一致的、高水平的安全措施——在复杂的网络上很难维持这种状态。

防火墙能够：

- 控制到内部系统的访问，只有邮件和公众信息服务器可以从外部到达。
- 针对每台机器或每个用户来阻止对特定 Internet站点的访问。
- 通过过滤NFS这样不安全的服务来提高网络安全性。
- 让系统管理员致力于单独一个系统的安全而不是 LAN中每台主机，这样可以降低开销并提高效率。
- 通过阻止到finger和DNS这类服务的访问来加强保密，它们可能给攻击者泄漏信息。
- 监测一个内部网络和 Internet之间的通信以跟踪网络漏洞或内部人员的不法行为。
- 在两个远程位置建立一个加密连接（有时作为一个虚拟保密网络）。

16.2 策略考虑

在实现一个有效的防火墙之前需要建立两层网络安全策略。上层是服务访问策略，它指

明防火墙允许或限制哪些服务，这些服务怎样被使用，异常怎样处理。在保护网络安全和允许用户访问所需要的网络资源之间要进行实际的均衡。例如，一个服务访问策略也许说明只允许Internet访问邮件和信息服务器，或者也许放宽允许从 Internet上到特定主机的访问，但只能是经过认证的用户。

较低一层是防火墙设计策略，指明要实现什么限制机制。有两种基本但互斥的方案来指明防火墙策略：

- 缺省为允许 —— 缺省时允许所有服务通过，除了那些被服务访问策略明确禁止的服务。这符合一个“开放实验室”访问模型，能最大化功能。
- 缺省为拒绝 —— 缺省时拒绝所有的服务，除了那些被服务访问策略明确允许的服务。这符合用在信息安全许可领域中的经典访问模型。

没有策略是阻止一切的。缺省允许在某些情况下较为容易建立。其主要任务是识别并拒绝危险的协议。虽然缺省拒绝策略更接近机构的服务访问策略，提供更高层的安全，但它可能对用户造成不便。一个原因是许多服务（像 XWindow、FTP和RPC）很难被过滤。另一个原因是较新的服务，如RealAudio在可用后，用户将被阻止使用它们，直至防火墙管理员重新配置防火墙。

就像许多安全策略是一分为二的，这两种方式需要平衡并重复。有些情况下，请求的服务需要被拒绝，因为安全风险太大。有时，一个危险的服务对机构的任务可能是不可缺的，尽管危险也需要提供。

16.3 防火墙的危险

随着Internet上侵犯事件增加，有一种趋势就是购买一种“固定”防火墙产品。没有固定防火墙这样的事物 —— 像许多提高计算机安全的方法那样，一个防火墙要求就一个站点独特的需求和环境进行定制。如果用户要寻求一个标准方案，那么就走错路了。团体顾客要求供应商提供该能力的思潮导致错误配置防火墙，这是令人沮丧的。

Computer Security Institute与一群黑客召开一次“遭遇敌人”的电话会议[3]，当被问及商用防火墙软件包时，黑客提出了一些有趣的批评：

“首先，对任何打成包的大型商用防火墙，如果没有配置它的知识，那对你是毫无用处的。这就好像出去买了一辆汽车却不知如何开”。

一个商用防火墙软件包又自己创建了风险。就像一个黑客指出的：

“两千个人在他们的站点上安装了“ Super Firewall X”，然后你和我坐了一两个星期并闯进了“ Super Firewall X”—— 嘿，我们一下就可攻击两千个站点”。

另一个黑客对怎样对防火墙管理员进行基本培训提出了宝贵的建议：

“你不得不让某个人专心致力于网络的安全性。不能让三个人做这件事情。不得不让某个人知道它的内外整个情况，有人看出网络发生了某些问题，这不能是因为 Bob在上次值班时做了些古怪的事情”。

防火墙可能带来安全的错觉。有些站点似乎认为有了一个防火墙（任何防火墙），就可以使自己站点对于任何形式的攻击是安全的。在防火墙专家中有一句格言：总有一次跳跃可以越过前门到达后面的门。作为外围防御，防火墙只是难题的一部分 —— 许多战术中的一种，被用来为Internet站点提供层次防御。

一个防火墙不能阻止内部人员在防火墙之后进行攻击。有些公司通过在机构内安装内部防火墙来应付这种问题。一种错误的概念是认为可以把防火墙从非常安全的设置调节到中等安全的设置。就像 Bill Cheswick曾指出的：“ 攻击本质是二元的（ 0/1）。你被攻击或者没有，没有安全介于其间的防火墙 ”。[4]

内部防火墙可能降低使用性，并引诱职员找到方法来击败它（这也适用于其他安全措施一样）。Brent Chapman讲述了一个令人心寒的故事。一个计算机公司严格执行 “ 无 modem ” 策略，这是工程人员所痛恨的。安全部经理认为工程人员别无选择只能照办，但一种普通的攻击方法是 “ 到Frye去取一个V.32 modem，把它插入SPARC，在晚上拨掉最近一台传真机的线并插入modem。一个前任的工程人员一次又一次使用这种方式 ”。这不是一个教训吗？[5]

“ 1) 多数公司想雇用能解决问题的人员。如果防火墙是一个问题，他们也将去解决。

2) 管理人员没有认识到使用安全网络的困难。工程人员不认为他们的行为对安全有害。”

16.4 防火墙的类型

在过去几年中出现了许多类型的防火墙。它们大概可分为网络级防火墙和应用程序级防火墙，尽管随着防火墙技术的混合和搭配，两者之间的区别越来越少了。

16.4.1 网络级防火墙

网络级防火墙的一个基本例子就是位于 Internet和内部网络之间的路由器，它根据数据包的来源、目的地址和端口来过滤。一个包过滤路由器（在防火墙语言中称为 “ 阻塞门 (choke) ”）能以不同的方式阻止来自指定主机或网络的连接，或者阻止到指定端口的连接。一个站点也许要阻止从一个敌对或不可信地址到来的连接，或者阻止所有来自外部地址的连接，除了与外部交换邮件的SMTP。

网络级防火墙速度快且对用户透明。它们相对比较容易建立而且便宜，因为许多机构已经拥有了与Internet相连的路由器。它们可以用直观的规则来编程，如 “ 阻止未启用服务的包 ” 或 “ 允许到信息服务器但阻止到其他主机的 TCP连接 ”。它们还很灵活，如子网 123.4.5.0的某人攻击用户的一个主机：用户可以配置一个网络级的防火墙来阻止来自该子网的所有访问。

包过滤路由器有一些潜在的弱点。老式路由器不支持扩充的日志 —— 表明用户可能被侵入的配置错误的第一个标志。包过滤规则叙述起来很复杂，过滤规则集可能太绕弯，使漏洞很难检测到。

16.4.2 应用程序网关

克服包过滤弱点的一个通用方法是使用一个应用程序级网关，一个运行 proxy服务的主机 —— 过滤Telnet和FTP这类服务连接的软件应用程序。运行 proxy服务的主机被称为 “ 应用程序网关 ” 或 “ 防御主机 ”。它可以和一个包过滤路由器组合起来提供更好的安全性和灵活性。

16.5 传统的防火墙配置

16.5.1 包过滤防火墙

这可能是最简单的防火墙，用户在 Internet网关安装一个包过滤路由器，然后配置路由器

的包过滤以便选择性地阻止或“过滤”协议和地址。根据制定的策略，内部系统也许能直接访问Internet，而从Internet到内部系统的所有或多数访问被阻止（见图 16-1）。

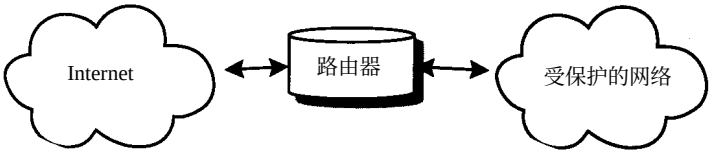

图16-1 一个包过滤防火墙

16.5.2 Dual-Homed主机

Dual-homed主机（也称为“dual-homed网关”）在很多方面比包过滤防火墙更优越，它是一种相对容易实现的简单配置，提供较好的安全性。许多早期 Internet防火墙建在一个称为“堡垒主机”的UNIX主机上，该主机是一个应用运送者、网络流量记录员和服务提供者。自然，一个堡垒主机要尽可能安全，因为它是网络攻击者关注的焦点。

一个dual-homed主机有两个网络接口， 一个连接到内部网络，另一个连接到 Internet。主机阻塞所有经过它的传输并运行 proxy服务。为了工作无误，计算机从不把包直接从一个接口送到另一个。这通过在许多UNIX系统中把内核变量ip_forwarding置为0（关闭）来实现。

这种防火墙（见图 16-2）比一个包过滤防火墙提供更大程度上的安全，因为它全部阻塞并遵从缺省拒绝策略。除非被指明允许，所有的服务都被拒绝，因为除了 proxy允许的服务外没有服务能通过。

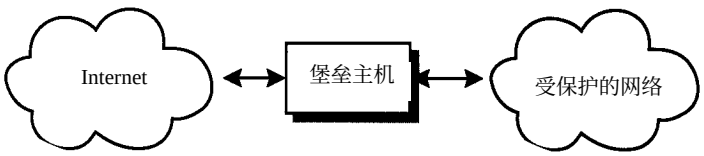

图16-2 一个Dual-homed主机防火墙

16.5.3 Screened主机

在Screened主机防火墙（见图16-3）中，对一个堡垒主机的访问由一个路由器控制，它有审查包的能力，在受保护的网络和Internet之间进行阻塞。它运行类似于dual-homed网关上运行的proxy软件，只允许到堡垒主机的传输。

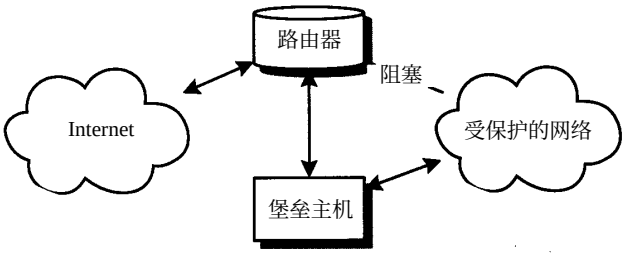

图16-3 一个Screened主机防火墙

Screened主机网关很灵活。它们给被认为可信的应用提供一个机会来通过审查路由器有选择地允许传输，或在相互依存的可信网络之间传输。这种配置的缺点

是要了解两种重要安全系统：堡垒主机和路由器。

16.5.4 Screened子网

在一个screened子网防火墙中，一个小型孤立网络放在内部网络和 Internet之间。用两个路由器来创建一个内部Screened子网——“ DMZ ”（Demilitarized Zone）。DMZ放置堡垒主机、信息服务器、 modem缓冲池以及其他访问受控制的系统。对 DMZ子网的访问由路由器中的审查规则保护，它限制传输，使子网中的主机只是那些能从内部网络和 Internet到达的系统。

Screened子网防火墙是dual-homed网关和screened主机防火墙的一种变型。 DMZ使一个外部人员要直接访问隐藏的内部网络十分困难。如果路由被阻塞，那么像 dual-home网关那样，所有传输必须通过堡垒主机上的一个应用程序（见图 16-4）。

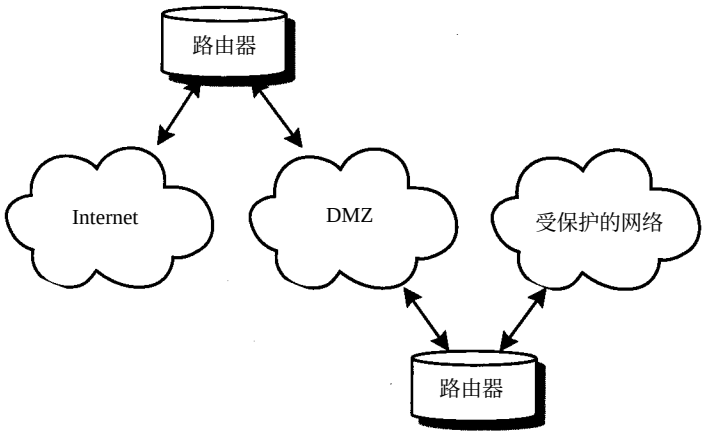

图16-4 一个Screened子网防火墙

16.6 防火墙规划

传统上，许多机构使用 UNIX主机和路由器建立了自己的防火墙。在过去几年中，防火墙功能被放入许多UNIX产品中，有许多免费和商业防火墙工具包也出现了。另外，一个机构也可以向外寻求防火墙服务：有许多 ISP和其他服务机构提供受监控的防火墙服务。

16.6.1 风险评估

所有的计算机安全规划都是从风险评估开始：我要保护什么？有哪些危险？不幸的是，当把一个私有网络连接到 Internet或任何不可信网络时，危险总是存在的。如果用户把系统连到Internet上，就需要探讨安全性，尽管用户认为“ 没有什么有价值的东西 ”可被偷走。许多小型家庭LAN操作者很奇怪地发现他们的 Linux在接收端被破坏：可以在 comp.security.unix新闻组发现他们求助的绝望呼叫。另一方面，大的商业公司把防火墙看作维持可信的联机客户的一个重要部分。

16.6.2 策略

用户必须选择高层策略来勾画出防火墙支持的服务，并指明选择缺省拒绝还是缺省允许。

还应把防火墙策略集成到站点的整个安全策略中。

16.6.3 人员

除了最小的安装之外，都要求防火墙管理员是一个全职工作。没有什么能代替一个训练有素的全职系统管理员，如果他能监测性能、升级系统、使用 bug补丁程序并确保系统对于侵入是安全的。一个维护差劲的防火墙可能比没有防火墙还糟，因为它可能已放入了一个侵入者而还认为站点是安全的。一个站点的安全策略应该清楚地反映出强大防火墙管理的重要性。

防火墙不是一个对系统管理减少关注的借口。事实上相反：如果一个防火墙被穿透，一个管理差劲的站点可能对侵入敞开大门并最终造成损失。一个防火墙不能降低对高水平系统管理的需要。

16.6.4 预算

在高端，在整个公司内安装并配置防火墙可能花费数十万美元。在低端，一个运行 Linux 的老式PC可以免费做到这点。一定要考虑维护上的开销：甚至免费的防火墙也需要持续的监测和升级。

16.6.5 最低限度的需求

一旦建立了策略，分析完风险，说明了开销，就要准备为防火墙系统开发一组设计需求。下面列出了从NIST刊物《Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls》中摘录的可能出现的需求。[6]

- 防火墙应能支持“拒绝所有服务，除了明确许可的服务”这种设计策略，甚至在该策略不被使用的情况下。
- 防火墙应能支持用户的安全策略，而不是强加上去。
- 防火墙应该比较灵活，它应该在原有安全策略被改变时适应新的服务和需求。
- 防火墙应该包含先进的认证措施，或为安装先进的认证措施保留“挂钩”。
- 防火墙应使用过滤技术来根据需要许可或拒绝到指定主机的服务。
- IP过滤语言应该灵活，对程序友好，并应能过滤尽可能多的属性，包括源和目的 IP地址、协议类型、源和目的TCP/UDP端口以及往内和往外的接口。
- 防火墙应为FTP和Telnet这样的服务使用proxy服务器，使防火墙可以集中使用先进的认证方式。如果需要NNTP、X、http或gopher这类服务，防火墙应包含相应的proxy服务。
- 防火墙应具有集中 SMTP访问的能力，以减少站点和远程系统之间的直接 SMTP连接数目。
- 防火墙应适应到站点的公开访问，这样公众信息服务器可以被防火墙保护，但与不需要公众访问的系统相隔离。
- 防火墙应具有集结和过滤拨入访问的能力。
- 防火墙应具有记录传输和可疑活动的机制，还要有日志缩减机制使日志可读和可理解。
- UNIX的安全版本应是防火墙的一部分，要有其他安全工具来保证防火墙主机的完整性，操作系统应安装所有的补丁程序。
- 防火墙应以可验证强壮性和正确性的方式开发。它应该设计简单，能被理解和维护。

• 防火墙和任何相应的操作系统应及时用补丁程序和 bug修复程序进行升级。

16.7 防火墙工具评述

包过滤和其他防火墙功能被加入到许多现代 UNIX系统中，包括Linux和*BSD系统。另外，有许多防火墙工具可以使用，从公开领域的代码到昂贵的商业产品。许多工具集成在“ 工具包 ”中，另外一些则是单独的。

提示 由Catherine Fulmer维护的一个商业防火墙产品列表可以在下面地址找到：

http://www.waterw.com/~manowar/vendor.html

下面是网络上的免费工具。注意这种程序中的许多个都有执照限制。

1. Freestone

SOS Crop.开发了Brimstone防火墙的这个免费版本。 Freestone是一个可移植的全功能防火墙产品，它支持像FTP和Telnet proxies这些可以用一个访问控制列表机制扩展的服务。其安装和配置很复杂，需要很多步。下面内容摘录于其 README文件：“ Freestone应被看成是为得到一个安全的防火墙提供许多工具，而不是一个完全承包的解决方案 ”。

更多信息参见：

http://www.soscorp.com/products/Freestone.html

要下载，参见：

```
ftp://ftp.soscorp.com/pub/sos/freestone/

ftp://ftp.cs.columbia.edu/pub/sos/freestone/
```

2. IP Filter

IP Filter是一个用在防火墙环境中的 TCP/IP包过滤器。它能被配置成一个可载入的内核模块或纳入到一个 UNIX内核中。它提供脚本来进行安装并可根据需要修补文件。 IP Filter可以显式地拒绝/许可任何包通过，区别不同接口，根据 IP网络或主机过滤，或者有选择地过滤任何IP协议。它还提供日志和测试。 IP Filter被包含在几个免费 UNIX产品中，包括 FreeBSD、OpenBSD和NetBSD。

更多信息参见：

http://cheops.anu.edu.au/~avalon/ip-filter.html

要下载，参见：

ftp://coombs.anu.edu.au/pub/net/ip-filter/

3. Juniper防火墙工具包

Juniper是一个建立安全有效 Internet防火墙的工具包。它用在 dual-homed堡垒主机上，使包不直接在接口之间传递。 Juniper实现了透明的proxy设备，允许内部机器、未路由的网络透明地访问Internet，就好像它们直接连接上去一样。 Juniper于1998年成为一个公开源程序产品。它能运行在BSD/OS、FreeBSD、NetBSD和Linux上。

更多信息参见：

http://www.obtuse.com/juniper/

要下载，参见：

ftp://ftp.obtuse.com/pub/juniper/

4. Mediator One

Mediator One是一个完全免费的防火墙软件包，运行在单独一个系统上。它提供一组稳固

的proxy以及网络连接的认证和审计功能。可以用一个基于浏览器的接口来配置、控制和查询防火墙。

更多信息参见：
http://www.comnet.com.au/htmls/mediator1.html
要下载，参见：
http://www.comnet.com.au/htmls/mediator-registration.html

5. SOCKS

SOCKS是一个网络代理协议，它使一个 SOCKS服务器一端的主机能获得对另一端主机的完全访问而不要求直接 IP可达。SOCKS包括两个基本部分： SOCKS服务器和SOCKS客户库。服务器认证并授权连接请求，建立代理连接并转发数据。客户库位于客户的应用程序和传输层之间。由于其简单性， SOCKS广泛应用在线路级防火墙：一个 SOCKS服务器后的主机可以获得到Internet的完全访问，而客户端对它们访问的 Internet主机仍是隐藏的。有两种版本的SOCKS可以使用。 SOCKS V4执行三个功能：连接请求、代理线路建立和应用数据转发。SOCKS V5增加了认证。

更多信息参见：
http://www.socks.nec.com/
http://www.socks.nec.com/rfc/rfc1928.txt
要下载，参见：
http://www.socks.nec.com/cgi-bin/download.pl
ftp://ftp.nec.com/pub/socks/

6. Tcpr

Tcpr是一组通过防火墙向前传送 FTP和Telnet命令的Perl脚本。向前传送发生在应用程序级，所以它很容易控制。未重编译的 C代码是所需要的。Tcpr由一个解释命令的inetd类型服务器、一个转发程序和一个向服务器交流的客户程序组成。客户端要求服务器向一个指定 TCP端口号的远程主机转发连接，服务器调用转发程序并向客户端返回一个 proxy端口号。客户端然后调用telnet或ftp，告诉它们连接到转发主机的 proxy端口号。转发程序然后在客户机和远程主机之间传输数据。Tcpr是为SunOS和Perl 4写的。

更多信息参见：
ftp://coast.cs.purdue.edu/pub/tools/unix/tcpr/

7. TIS 防火墙工具包

TIS Internet防火墙工具包是一个免费可用的程序集，对于在 UNIX系统上建立网络防火墙是“ 可实际配置 ”的。工具包组件可以单独使用或与其他防火墙组件混合搭配使用。工具包以“ 没有明确许可就是拒绝 ”的方式来支持防火墙的实现。它支持建立 dual-homed网关、screened主机网关和screened子网网关。TIS在1998年与Network Associates合并，现在出售一个商业防火墙软件包：Gauntlet Internet Firewall。

更多信息参见：
http://www.tis.com/prodserv/fwtk/index.html
要下载（需要电子邮件确认），参见：
http://www.tis.com/prodserv/fwtk/readme.html

ftp://ftp.tis.com/pub/firewalls/toolkit/

8. udprelay

由Tom Fitzgerald开发的udprelay实现了一个在防火墙主机上运行的守护进程，它由一个配置文件指引在网络中传递UDP数据包。

要下载，参见：
ftp://coast.cs.purdue.edu/pub/tools/unix/udprelay-0.2.tar.gz

9. xforward

由Win Treese开发的xforward通过网络防火墙转发X Window系统连接。

要下载，参见：
ftp://crl.dec.com/pub/DEC/xforward.tar.Z

10. Xp-BETA

Xp-BETA是一个为X11协议开发的应用程序网关，它使用Socks和/或CERN WWW Proxy。

要下载，参见：
ftp://ftp.mri.co.jp/pub/Xp-BETA

16.8 一个使用ipchains的Linux防火墙

提供内核级防火墙功能是Linux的众多优点之一。防火墙工具ipfwadm（基于BSD ipfw）为在Linux上集成防火墙功能提供很多系统管理选项。 1998年，许多Linux开发者对以前的Linux IPv4防火墙代码进行了重要的改写并起名为“ ipchains ”。

提示 ipchains工具对Linux内核2.1.102及以上版本的IP包过滤是需要的。运行2.0内核系列的系统可以下载一个内核补丁程序。要检查自己的系统是否有ipchains，可查找文件/proc/net/ip-fwchains。

设置过滤器的ipchains工具可以用来确定怎样处理包。过滤器由三个防火墙链（或规则）来控制，分别是input、forward和output。当一个包到达时，内核使用input链来确定它是生存还是死亡。如果它存活下来，则对其进行路由。如果包被另一台机器预定，则内核查询 forward链。最后，内核在送它上路之前查询output链。

提示 要得到ipchains的更多信息，可参见http://www.rustcorp.com/linux/ipchains/HOWTO.html上Paul Russell的Linux IPCHAINS-HOWTO和官方的IPCHAINS主页http://www.rustcorp.com/linux/ipchains/

像ipchains这样的创新表明建立防火墙的艺术在继续发展。系统和应用安全最终可能发展到像防火墙这样的外围防御被尽力实施。这个变化如果到来，那它将由复杂的连接需求和扩展的Internet商务所驱动。同时， Internet连接站点继续应用防火墙；供应商将提高本身的技术；系统管理将在配置和维护中抗争。读者可以通过订购 Firewall Wizards List来与防火墙领域的发展保持同步 —— 参见http://www.nfr.net/forum/firewall-wizards.html来得到更多信息。

注释：

[1] Bellovin和Cheswick一起写了一本书《Firewalls and Internet Security: Repelling the Wily Hacker》(Addison-Wesley, 1994)。

[2] 参见http://www.clark.net/pub/mjr/pubs/fwfaq/index.htm。

[3] 参见http://www.gocsi.com/hacker.htm。他们中的一些人可能更准确的应称为“破坏者（cracker）”，但我按照原文档来称呼。
[4] 摘自http://www.cs.purdue.edu/coast/firewalls/firewalls_bof_95.txt。
[5] 同上。
[6] John P. Wack and Lisa J. Carnahan, NIST Special Publication 800-10。参见http://csrc.nist.gov/nistpubs/800-10/。