第三篇　网络安全技术

第 3 章　防火墙技术

本章学习目标

- 防火墙的定义、发展简史、目的、功能、局限性
- 包过滤防火墙和代理防火墙的实现原理、技术特点以及实现方式
- 防火墙的常见体系结构
- 分布式防火墙的体系结构、特点

3.1　防火墙技术概述

防火墙（Firewall）是一种将内部网和公众网如 Internet 分开的方法。它能限制被保护的网络与 Internet 网络之间，或者与其他网络之间进行的信息存取、传递操作，可以作为不同网络或网络安全域之间信息的出入口，能根据企业的安全策略控制出入网络的信息流，且本身具有较强的抗攻击能力。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。

防火墙是提供信息安全服务，实现网络和信息安全的基础设施。在构建安全的网络环境的过程中，防火墙作为第一道安全防线，正受到越来越多用户的关注。通常一个单位在购买网络安全设备时，总是把防火墙放在首位。目前，防火墙已经成为世界上用得最多的网络安全产品之一。本章就是讲述防火墙是如何保证网络系统的安全的。

3.1.1　防火墙的定义

《辞海》上说“防火墙：用非燃烧材料砌筑的墙。设在建筑物的两端或在建筑物内将建筑物分割成区段，以防止火灾蔓延”。在 IT 这个变革一切、改造一切的世界里，人们借助了这个概念，“防火墙是设置在被保护网络和外部网络之间的一道屏障，以防止发生不可预测的、潜在破坏性的入侵。”如果说，只要用户使用了计算机，就应该使用杀毒软件；那么，只要用户联上了因特网，就应该构建防火墙。

简单地说，防火墙是位于内部网络与外部网络之间或两个信任程度不同的网络之间（如企业内部网络和 Internet 之间）的软件或硬件设备的组合，它对两个网络之间的通信进行控制，通过强制实施统一的安全策略，限制外界用户对内部网络的访问及管理内部用户访问外部网络的权限的系统，防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。

防火墙是设置在被保护网络和外部网络之间的一道屏障，是不同网络或网络安全域之间

信息的唯一出入口，能根据受保护的网络的安全政策控制（允许、拒绝、监测）出入网络的信息流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护，以防止发生不可预测的、潜在破坏性的侵入。防火墙本身具有较强的抗攻击能力，它是提供信息安全服务、实现网络和信息安全的基础设施。图 3.1 为防火墙示意图。

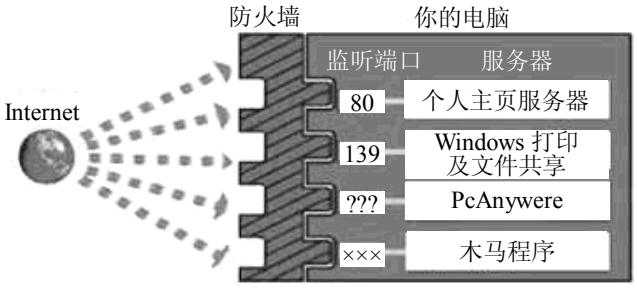

图 3.1 防火墙示意图

3.1.2 防火墙的发展简史

第一代防火墙：第一代防火墙技术几乎与路由器同时出现，采用了包过滤（Packet Filter）技术。

第二、三代防火墙：1989 年，贝尔实验室的 Dave. Presotto 和 Howard.Trickey 推出了第二代防火墙，即电路层防火墙，同时提出了第三代防火墙——应用层防火墙（代理防火墙）的初步结构。

第四代防火墙：1992 年，USC 信息科学院的 Bob.Braden 开发出了基于动态包过滤（Dynamic Packet Filter）技术的第四代防火墙，后来演变为目前所说的状态监视（State Fulinspection）技术。1994 年，以色列的 Check.Point 公司开发出了第一个基于这种技术的商业化的产品。

第五代防火墙：1998 年，NAI 公司推出了一种自适应代理（Adaptive Proxy）技术，并在其产品 Gauntlet Fire wall for NT 中得以实现，给代理类型的防火墙赋予了全新的意义，可以称之为第五代防火墙。

图 3.2 表示了防火墙技术的简单发展历史。

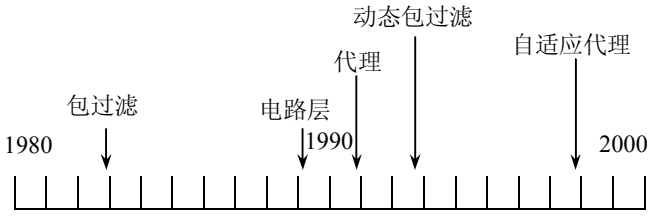

图 3.2 防火墙技术的简单发展历史

3.1.3 设置防火墙的目的与功能

通常应用防火墙的目的有以下几个方面：限制他人进入内部网络；过滤掉不安全的服务

和非法用户；防止入侵者接近用户的防御设施；限定人们访问特殊站点；为监视局域网安全提供方便。

无论何种类型防火墙，从总体上看，都应具有以下五大基本功能：过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止的业务；记录通过防火墙的信息内容和活动；对网络攻击的检测和告警。防火墙的主要功能就是控制对受保护网络的非法访问，它通过监视、限制、更改通过网络的数据流，一方面尽可能屏蔽内部网的拓扑结构，另一方面对内屏蔽外部危险站点，用以防范外对内、内对外的非法访问。其功能具体表现在以下四个方面：

（1）防火墙是网络安全的屏障。防火墙作为阻塞点、控制点，能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以内部网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护的网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

（2）防火墙可以强化网络安全策略。通过以防火墙为中心的安全方案配置，能将所有安全软件如口令、加密、身份认证、审计等配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。

（3）对网络存取和访问进行监控审计。如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当地报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的：其理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击、防火墙的控制是否充足，而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

（4）防止内部信息的外泄。通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节如 finger、DNS 等服务。finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用的 shell 类型等。但是 finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络中的 DNS 信息。这样，内部主机的域名和 IP 地址就不会被外界所了解。

除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布在全世界各地的 LAN 或专用子网，有机地连成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

总之，防火墙允许网络管理员定义一个中心点来防止非法用户进入内部网络；可以很方便地监视网络的安全性，并报警；可以作为部署 NAT（Network Address Translation，网络地址变换）的地点，利用 NAT 技术，将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来，用来缓解地址空间短缺的问题；防火墙还是审计和记录 Internet 使用费用的一个最佳地点，网络管理员可以在此向管理部门提供 Internet 连接的费用情况，查出潜在的带宽瓶颈位置，并能

够依据本机构的核算模式提供部门级的计费；防火墙可以连接到一个单独的网段上（从技术角度来讲，这就是所谓的停火区——DMZ），从物理上和内部网段隔开，并在此部署 WWW 服务器和 FTP 服务器，将其作为向外部发布内部信息的地点。

3.1.4 防火墙的局限性

防火墙技术是内部网络最重要的安全技术之一，但防火墙也有其明显的局限性。

1. 防火墙防外不防内

防火墙的安全控制只能作用于外对内或内对外，即对外可屏蔽内部网的拓扑结构，封锁外部网上的用户连接内部网上的重要站点或某些端口；对内可屏蔽外部危险站点，但它很难解决内部网控制内部人员的安全问题，即防外不防内。而据权威部门统计表明，网络上的安全攻击事件有 70%以上来自内部。

2. 网络应用受到结构性限制

传统的边界式防火墙依赖于物理上的拓扑结构，它从物理上将网络划分为内部网络和外部网络。而根据 VPN 的概念，它对内部网络和外部网络的划分是基于逻辑上的，逻辑上同处内部网络的主机可能在物理上分处内部和外部两个网络。传统的防火墙在此类网络环境的应用受到了结构性限制。

基于以上原因，传统防火墙不能在有两个内部网络之间通信需求的 VPN 网络中使用，否则 VPN 通信将被中断。虽然目前有一种 SSL VPN 技术可以绕过企业边界的防火墙进入内部网络 VPN 通信，但是应用更广泛的传统 IPSec VPN 通信中还是不能使用，除非是专门的 VPN 防火墙。

3. 防火墙难于管理和配置，易造成安全漏洞

防火墙的管理及配置相当复杂，要想成功维护防火墙，就要求防火墙管理员对网络安全攻击的手段及其与系统配置的关系有相当深刻的了解；防火墙的安全策略无法进行集中管理，一般来说，由多个系统（路由器、过滤器、代理服务器、网关、堡垒主机）组成的防火墙，管理上有所疏忽是在所难免的。

4. 效率较低、故障率高

由于防火墙把检查机制集中在网络边界处的单点上，产生了网络的瓶颈和单点故障隐患。从性能的角度来说，防火墙极易成为网络流量的瓶颈。

5. 很难为用户在防火墙内外提供一致的安全策略

许多防火墙对用户的安全控制主要是基于用户所用机器的 IP 地址而不是用户身份，这样就很难为同一用户在防火墙内外提供一致的安全控制策略，限制了网络的物理范围。

6. 防火墙只实现了粗粒度的访问控制

防火墙只实现了粗粒度的访问控制，且不能与网络内部使用的其他安全（如访问控制）集中使用。这样，就必须为网络内部的身份验证和访问控制管理维护单独的数据库。

3.1.5 防火墙技术发展动态和趋势

考虑到 Internet 发展的凶猛势头和防火墙产品的更新步伐，要全面展望防火墙技术的发展几乎是不可能的，但从产品及功能上，却又可以看出一些动向和趋势，防火墙产品正向以下趋势发展：

（1）优良的性能。新一代防火墙系统不仅应该能更好地保护防火墙后面内部网络的安全，而且应该具有更为优良的整体性能。数据通过率越高，防火墙性能越好。传统的代理型防火墙虽然可以提供较高级别的安全保护，但是同时它也成为限制网络带宽的瓶颈，这极大地制约了它在网络中的实际应用。现在大多数的防火墙产品都支持 NAT 功能，它可以让受防火墙保护一边的 IP 地址不至于暴露在没有保护的另一边，但启用 NAT 后，势必会对防火墙系统性能有所影响，如何尽量减少这种影响也成为了目前防火墙产品的卖点之一。另外防火墙系统中集成的 VPN 解决方案必须是真正的线速运行，否则将成为网络通信的瓶颈。特别是采用复杂的加密算法时，防火墙性能尤为重要。总之，未来的防火墙系统将会把高速的性能和最大限度的安全性有机结合在一起，有效地消除制约传统防火墙的性能瓶颈。

（2）可扩展的结构和功能。选择哪种防火墙，除了应考虑它基本性能外，毫无疑问，还应考虑用户的实际需求与未来网络的升级。因此，防火墙除了具有保护网络安全的基本功能外，还提供对 VPN 的支持，同时还应该具有可扩展的内驻应用层代理。除了支持常见的网络服务以外，还应该能够按照用户的需求提供相应的代理服务，例如，如果用户需要 NNTP、X-Window、HTTP 和 Gopher 等服务，防火墙就应该包含相应的代理服务程序。未来的防火墙系统应是一个可随意伸缩的模块化解决方案，从最基本的包过滤到带加密功能的 VPN 型包过滤，直至一个独立的应用网关，使用户有充分的余地构建自己所需要的防火墙体系。

（3）简化的安装与管理。防火墙产品配置和管理的难易程度是防火墙能否达到目的的主要考虑因素之一。若防火墙的配置和管理过于困难，则可能会造成设定上的错误，反而不能达到其功能。未来的防火墙将具有非常易于进行配置的图形用户界面，NT 防火墙市场的发展证明了这种趋势。

（4）主动过滤。许多防火墙都包括对过滤产品的支持，并可以与第三方过滤服务连接，这些服务提供了不受欢迎的 Internet 站点的分类清单。防火墙还在它们的 Web 代理中包括时间限制功能，允许非工作时间的冲浪和登录，并提供冲浪活动的报告。

（5）防病毒与防黑客。许多防火墙具有内置防病毒与防黑客的功能。

下面各点可能是防火墙技术下一步的走向和选择：

1）防火墙将从目前对子网或内部网络管理的方式向远程上网集中管理的方式发展。

2）过滤深度不断加强，从目前的地址、服务过滤，发展到 URL（页面）过滤，关键字过滤和对 ActiveX、Java 等的过滤，并逐渐有病毒扫除功能。

3）利用防火墙建立虚拟专用网（VPN）是较长一段时间的主流，IP 的加密需求越来越强，安全协议的开发是一大热点。

4）对网络攻击的检测和告警将成为防火墙的重要功能。

5）安全管理工具不断完善，特别是可疑活动的日志分析工具等将成为防火墙产品中的一部分。

综上所述，未来防火墙技术会全面考虑网络的安全、操作系统的安全、应用程序的安全、用户的安全、数据的安全等五个方面。此外，防火墙产品还将把网络前沿技术，如 Web 页面超高速缓存、虚拟网络和带宽管理等与其自身结合起来。

3.2 防火墙技术

3.2.1 防火墙技术的分类

尽管防火墙的发展经过了几代，根据防范的方式和侧重点的不同，防火墙技术可分为很多种类型，但是按照防火墙对内外来往数据的处理方法，大致可以将防火墙分为两大体系：包过滤防火墙和代理防火墙。前者以以色列的 Checkpoint 防火墙和 Cisco 公司的 PIX 防火墙为代表，后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

1. 包过滤防火墙

数据包过滤（Packet Filtering）技术是防火墙为系统提供安全保障的主要技术，它通过设备对进出网络的数据流进行有选择地控制与操作。包过滤操作一般都是在选择路由的同时在网络层对数据包进行选择或过滤（通常是对从 Internet 进入到内部网络的包进行过滤）。选择的依据是系统内设置的过滤逻辑，被称为访问控制表（Access Control Table）或规则表。规则表指定允许哪些类型的数据包可以流入或流出内部网络，例如：只接收来自某些指定的 IP 地址的数据包或者内部网络的数据包可以流向某些指定的端口等;哪些类型的数据包的传输应该被拦截。防火墙的 IP 包过滤规则以 IP 包信息为基础，对 IP 包源地址、目标地址、传输方向、分包、IP 包封装协议（TCP/UDP/ICMP/IP Tunnel）、TCP/UDP 目标端口号等进行筛选、过滤。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合来确定是否允许该数据包通过。包过滤处理如图 3.3 所示。

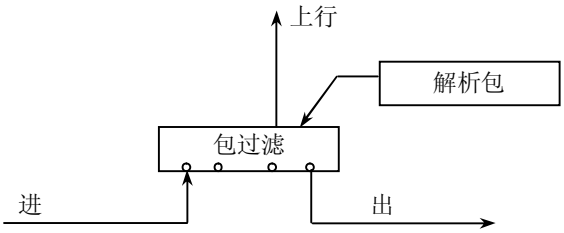

图 3.3 包过滤处理

包过滤操作可以在路由器上进行，也可以在网桥，甚至在一个单独的主机上进行。

数据包过滤是一个网络安全保护机制，它用来控制流出和流入网络的数据。不符合网络安全的那些服务将被严格限制。基于包中的协议类型和协议字段值，过滤路由器能够区分网络流量；基于协议特定的标准，路由器在其端口能够区分包和限制包的能力叫包过滤（Packet Filtering）。正因如此，过滤路由器也可以称作包过滤路由器（Packet Filter Router）。

（1）数据包过滤技术的发展。包过滤类型的防火墙遵循的一条最基本原则是“最小特权原则”，即明确允许那些管理员希望通过的数据包通过，而禁止其他的数据包通过。有两种数据包过滤技术，分别为静态包过滤和动态包过滤技术。

1）静态包过滤。一般防火墙的包过滤的过滤规则是在启动时配置好的，只有系统管理员才可以修改，是静态存在的，称为静态规则。利用静态包过滤规则建立的防火墙就叫静态包过滤防火墙，如图 3.4 所示。这种类型的防火墙根据定义好的过滤规则审查每个数据包，即与规

则表进行比较，以便确定其是否与某一条包过滤规则匹配。

图 3.4　静态包过滤防火墙

2）动态包过滤。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。即采用了基于连接状态的检查和动态设置包过滤规则的方法，将属于同一连接的所有包作为一个整体的数据流看待，通过规则表与连接状态表的共同配合进行检查。动态过滤规则技术避免了静态包过滤所具有的问题，使防火墙弥补了许多不安全的隐患，在最大程度上降低了黑客攻击的成功率，从而大大提高了系统的性能和安全性。如图 3.5 所示。

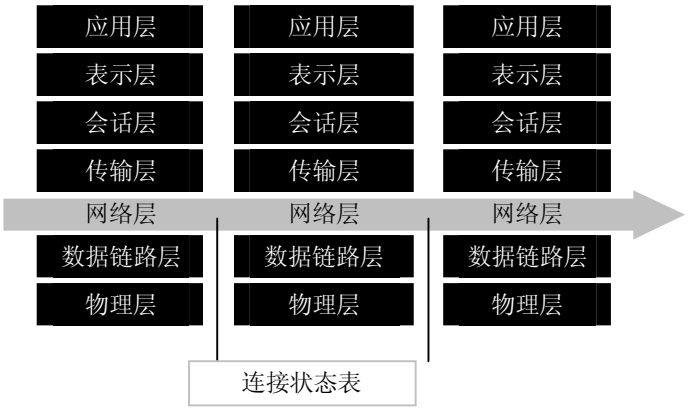

图 3.5　动态包过滤防火墙

（2）包过滤的优点。数据包过滤防火墙逻辑简单、价格便宜，易于安装和使用，网络性能和透明性好，它通常安装在路由器上，而路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。包过滤防火墙的优点具体体现在下面几点：

1）不用改动应用程序。包过滤不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。

2）一个过滤路由器能协助保护整个网络。数据包过滤的主要优点之一是一个单个的、恰当放置的包过滤路由器有助于保护整个网络。如果仅有一个路由器连接内部与外部网络，不论内部网络的大小、内部拓扑结构如何，通过那个路由器进行数据包过滤，在网络安全保护上就

能取得较好的效果。

3）数据包过滤对用户透明。数据包过滤是在 IP 层实现的，Internet 根本感觉不到它的存在；包过滤不要求任何自定义软件或者客户机配置；它也不要求用户任何特殊的训练或者操作，使用起来很方便。较强的“透明度”是包过滤的一大优势。

4）过滤路由器速度快、效率高。较 Proxy 而言，过滤路由器只检查报头相应的字段，一般不查看数据包的内容，而且某些核心部分是由专用硬件实现的，故其转发速度快、效率较高。

总之，包过滤技术是一种通用、廉价、有效的安全手段。之所以通用，是因为它不针对各个具体的网络服务采取特殊的处理方式；之所以廉价，是因为大多数路由器都提供分组过滤功能；之所以有效，是因为它能很大程度地满足企业的安全要求。

（3）包过滤的缺点。

1）不能彻底防止地址欺骗。大多数包过滤路由器都是基于源 IP 地址、目的 IP 地址而进行过滤的。而数据包的源地址、目的地址以及 IP 的端口号都在数据包的头部，很有可能被窃听或假冒（IP 地址的伪造是很容易、很普遍的），如果攻击者把自己主机的 IP 地址设成一个合法主机的 IP 地址，就可以很轻易地通过报文过滤器。所以，包过滤最主要的弱点是不能在用户级别上进行过滤，即不能识别不同的用户和防止 IP 地址的盗用。

过滤路由器在这点上大都无能为力。即使按 MAC 地址进行绑定，也是不可信的。对于一些安全性要求较高的网络，过滤路由器是不能胜任的。

2）一些应用协议不适合于数据包过滤。如 RPC、X-Window 和 FTP。

3）正常的数据包过滤路由器无法执行某些安全策略。数据包过滤路由器上的信息不能完全满足用户对安全策略的需求。例如，数据包的报头信息只能说明数据包来自什么主机，而不知是什么用户；只知数据包发送到什么端口，而不知发到什么应用程序。这就存在着很大的安全隐患和管理控制漏洞。

4）安全性较差。过滤判别的只有网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC 类的协议；非法访问一旦突破防火墙，即可对主机上的软件和配置漏洞进行攻击；大多数过滤器中缺少审计和报警机制，通常它没有用户的使用记录，这样，管理员就不能从访问记录中发现黑客的攻击记录。而攻击一个单纯的包过滤式的防火墙对黑客来说是比较容易的，他们在这一方面已经积累了大量的经验。

5）数据包工具存在很多局限性。如数据包过滤规则难以配置，管理方式和用户界面较差；对安全管理人员素质要求高；建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。

从以上分析可以看出，包过滤防火墙技术虽然能确保一定的安全保护，也有许多优点，但是包过滤毕竟是第一代防火墙技术，本身存在较多缺陷，不能提供较高的安全性。因此，在实际应用中，很少把包过滤技术当作单独的安全解决方案，通常是把它与应用网关配合使用或与其他防火墙技术揉合在一起使用，共同组成防火墙系统。

2. 代理防火墙

代理防火墙（Proxy）是一种较新型的防火墙技术，它分为应用层网关和电路层网关。

（1）代理防火墙的原理。所谓代理服务器，是指代表客户处理在服务器连接请求的程序。

当代理服务器得到一个客户的连接意图时，它将核实客户请求，并用特定的安全化的 Proxy 应用程序来处理连接请求，将处理后的请求传递到真实的服务器上，然后接受服务器应答，并做进一步处理后，将答复交给发出请求的最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接和隔离内、外部网络的作用，所以又叫代理防火墙。代理防火墙工作于应用层，且针对特定的应用层协议。代理防火墙通过编程来弄清用户应用层的流量，并能在用户层和应用协议层间提供访问控制；而且，还可用来保持一个所有应用程序使用的记录。记录和控制所有进出流量的能力是应用层网关的主要优点之一。代理防火墙的工作原理如图3.6所示。

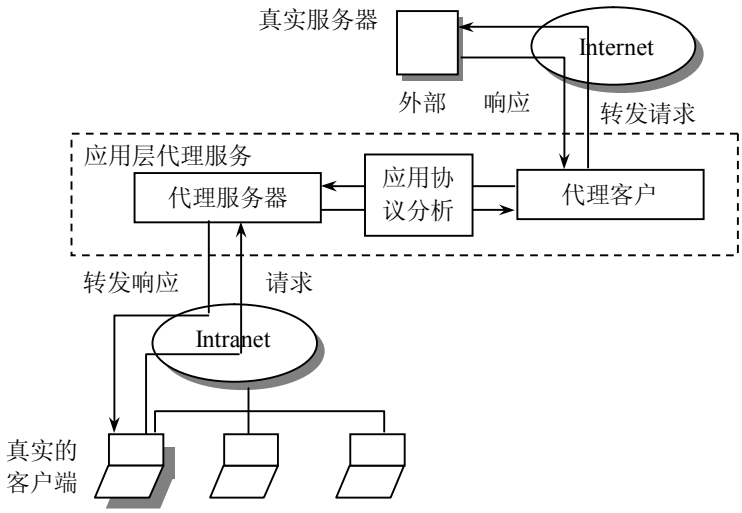

图 3.6　代理的工作方式

从图 3.6 中可以看出，代理服务器（Proxy Server）作为内部网络客户端的服务器，拦截住所有要求，也向客户端转发响应。代理客户（Proxy Client）负责代表内部客户端向外部服务器发出请求，当然也向代理服务器转发响应。

（2）应用层网关型防火墙。

1）原理。应用层网关（Application Level Gateways）防火墙是传统代理型防火墙，它的核心技术就是代理服务器技术，它是基于软件的，通常安装在专用工作站系统上。这种防火墙通过代理技术参与到一个 TCP 连接的全过程，并在网络应用层上建立协议过滤和转发功能，所以叫做应用层网关。当某用户（不管是远程的还是本地的）想与一个运行代理的网络建立联系时，此代理（应用层网关）会阻塞这个连接，然后在过滤的同时，对数据包进行必要的分析、登记和统计，形成检查报告。如果此连接请求符合预定的安全策略或规则，代理防火墙便会在用户和服务器之间建立一个“桥”，从而保证其通信。对不符合预定的安全规则的，则阻塞或抛弃。换句话说，“桥”上设置了很多控制。

同时，应用层网关将内部用户的请求确认后送到外部服务器，再将外部服务器的响应回送给用户。这种技术对 ISP 很常见，被用于在 Web 服务器上高速缓存信息，并且扮演 Web 客户和 Web 服务器之间的中介角色。它主要保存 Internet 上那些最常用和最近访问过的内容：在 Web 上，代理首先试图在本地寻找数据，如果没有，再到远程服务器上去查找。为用户提供了更快的访问速度，并且提高了网络安全性。应用层网关的工作原理如图 3.7 所示。

图 3.7　应用层网关防火墙

2）优点。应用层网关防火墙最突出的优点就是安全，这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。由于每一个内外网络之间的连接都要通过 Proxy 的介入和转换，通过专门为特定的服务如 HTTP 编写的安全化的应用程序进行处理，然后由防火墙本身提交请求和应答，没有给内外网络的计算机以任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网络。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。包过滤类型的防火墙是很难彻底避免这一漏洞的。

应用层网关防火墙同时也是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用，它工作在 OSI 模型的最高层，掌握着应用系统中可用作安全决策的全部信息。

3）缺点。代理防火墙的最大缺点就是速度相对比较慢，当用户对内外网络网关的吞吐量要求比较高时，（比如要求达到 75M～100Mbps 时）代理防火墙就会成为内外网络之间的瓶颈。所幸的是，目前用户接入 Internet 的速度一般都远低于这个数字。在现实环境中，要考虑使用包过滤类型防火墙来满足速度要求的情况，大部分是高速网（ATM 或千兆位 Intranet 等）之间的防火墙。

（3）电路层网关防火墙。另一种类型的代理技术称为电路层网关（Circuit Level Gateway）或 TCP 通道（TCP Tunnels）。在电路层网关中，包被提交用户应用层处理。电路层网关用来在两个通信的终点之间转换包，如图 3.8 所示。

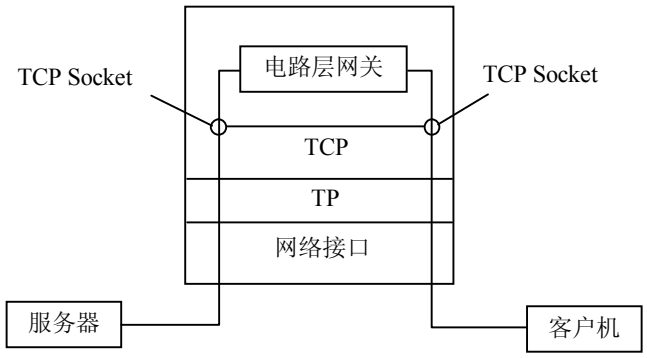

图 3.8　电路层网关

电路层网关是建立应用层网关的一个更加灵活方法。它是针对数据包过滤和应用网关技

术存在的缺点而引入的防火墙技术，一般采用自适应代理技术，也称为自适应代理防火墙。在电路层网关中，需要安装特殊的客户机软件。组成这种类型防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器（Dynamic Packet Filter）。在自适应代理与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应 Proxy 的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求或是从网络层转发数据包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。所以，它结合了应用层网关型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。电路层网关防火墙的工作原理如图 3.9 所示。

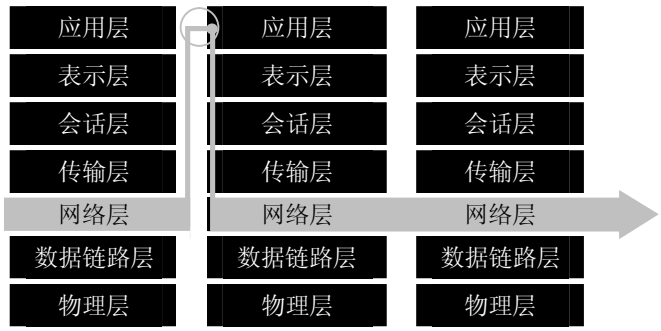

图 3.9　电路层网关防火墙

电路层网关防火墙的特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”，由两个终止代理服务器上的“链接”来实现，外部计算机的网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。此外，代理服务也对过往的数据包进行分析、注册登记，形成报告，同时当发现被攻击迹象时会向网络管理员发出警报，并保留攻击痕迹。

（4）代理技术的优点。

1）代理易于配置。代理因为是一个软件，所以它较过滤路由器更易配置，配置界面十分友好。如果代理实现得好，可以对配置协议要求较低，从而避免了配置错误。

2）代理能生成各项记录。因代理工作在应用层，它检查各项数据，所以可以按一定准则，让代理生成各项日志、记录。这些日志、记录对于流量分析、安全检验是十分重要和宝贵的。当然，也可以用于记费等应用。

3）代理能灵活、完全地控制进出流量、内容。通过采取一定的措施，按照一定的规则，用户可以借助代理实现一整套的安全策略，比如说可以控制“谁”和“什么”，还有“时间”和“地点”。

4）代理能过滤数据内容。用户可以把一些过滤规则应用于代理，让它在高层实现过滤功能，例如文本过滤、图像过滤（目前还未实现，但这是一个热点研究领域），预防病毒或扫描病毒等。

5）代理能为用户提供透明的加密机制。用户是通过代理控制数据的输入/输出，从而可以让代理完成对数据加/解密的功能，方便了用户，确保了数据的机密性。这点在虚拟专用网中

特别重要。代理可以广泛地用于企业外部网中，提供较高安全性的数据通信。

6）代理可以方便地与其他安全手段集成。目前的安全问题解决方案很多，如认证（Authentication）、授权（Authorization）、账号（Accouting）、数据加密、安全协议（SSL）等。如果把代理与这些手段联合使用，将大大增加网络安全性。这也是近期网络安全的发展方向。

（5）代理技术的缺点。

1）代理速度较路由器慢。路由器只是简单察看 TCP/IP 报头，检查特定的几个域，不作详细分析、记录。而代理工作于应用层，要检查数据包的内容，按特定的应用协议（如 HTTP）进行审查、扫描数据包内容，并进行代理（转发请求或响应），故其速度较慢。

2）代理对用户不透明。许多代理要求客户端作相应改动或安装定制客户端软件，这给用户增加了不透明度。由于硬件平台和操作系统都存在差异，要为庞大的互异网络的每一台内部主机安装和配置特定的应用程序既耗费时间，又容易出错。

3）对于每项服务代理可能要求不同的服务器。可能需要为每项协议设置一个不同的代理服务器，因为代理服务器不得不理解协议以便判断什么是允许的和不允许的，并且还装扮一个对真实服务器来说是客户、对代理客户来说是服务器的角色。挑选、安装和配置所有这些不同的服务器工作量可能很大。

4）代理服务不能保证免受所有协议弱点的限制。作为一个安全问题的解决方法，代理取决于对协议中哪些是安全操作的判断能力。每个应用层协议，都或多或少存在一些安全问题，对于一个代理服务器来说，要彻底避免这些安全隐患几乎是不可能的，除非关掉这些服务。

代理取决于在客户端和真实服务器之间插入代理服务器的能力，这要求两者之间交流的相对直接性。而且有些服务的代理是相当复杂的。

5）代理不能改进底层协议的安全性。因为代理工作于 TCP/IP 之上，属于应用层，所以它就不能改善底层通信协议的能力。如 IP 欺骗，伪造 ICMP 消息和一些拒绝服务的攻击。而这些方面，对于一个网络的健壮性是相当重要的。

3. 两种防火墙技术的对比

两种防火墙技术的对比如表 3.1 所示。

表 3.1 两种防火墙技术

	包过滤防火墙	代理防火墙
优点	价格较低	内置了专门为了提高安全性而编制的 Proxy 应用程序，能够透彻地理解相关服务的命令，对来往的数据包进行安全化处理
	性能开销小，处理速度较快	安全，不允许数据包通过防火墙，避免了数据驱动式攻击的发生
缺点	定义复杂，容易出现因配置不当带来的问题	速度较慢，不太适用于高速网（ATM 或千兆位 Intranet 等）之间的应用
	允许数据包直接通过，容易造成数据驱动式攻击的潜在危险	
	不能理解特定服务的上下文环境，相应控制只能在高层由代理服务和应用层网关来完成	

3.2.2　防火墙的主要技术及实现方式

防火墙的安全技术包括包过滤技术、代理、网络地址转换（NAT）等多种技术。实现防火墙的方式也多种多样。先进的防火墙产品功能越来越强大，正逐渐将网关与安全系统合二为一。

1. 双端口或三端口的结构

新一代防火墙产品具有两个或三个独立的网卡，内外两个网卡可不作 IP 转化而串接于内部网与外部网之间，另一个网卡可专用于对服务器的安全保护。

2. 透明的访问方式

以前的防火墙在访问方式上要么要求用户作系统登录，要么需要通过 SOCKS 等库路径修改客户机的应用。新一代防火墙利用了透明的代理系统技术，从而降低了系统登录固有的安全风险和出错概率。

3. 灵活的代理系统

代理系统是一种将信息从防火墙的一侧传送到另一侧的软件模块。新一代防火墙采用了两种代理机制，一种用于代理从内部网络到外部网络的连接；另一种用于代理从外部网络到内部网络的连接。前者采用网络地址转换（NAT）技术来解决；后者采用非保密的用户定制代理或保密的代理系统技术来解决。

4. 多级的过滤技术

为保证系统的安全性和防护水平，新一代防火墙采用了三级过滤措施，并辅以鉴别手段。在分组过滤一级，能过滤掉所有的源路由分组和假冒的 IP 源地址；在应用级网关一级，能利用 FTP、SMTP 等各种网关，控制和监测 Internet 提供的所用通用服务；在电路网关一级，实现内部主机与外部站点的透明连接，并对服务的通行实行严格控制。

5. 网络地址转换技术（NAT）

网络地址转换（NAT，Network Address Translate）是一种用于把内部 IP 地址转换成临时的、外部的 IP 地址的技术。在内部网络通过安全网卡访问外部网络时，将产生一个映射记录。系统将外出的源地址和源端口映射为一个伪装的地址和端口，让这个伪装的地址和端口通过非安全网卡与外部网络连接，这样对外就隐藏了真实的内部网络地址，同时还意味着用户不需要为其网络中每台机器取得注册的 IP 地址。在外部网络通过非安全网卡访问内部网络时，它并不知道内部网络的连接情况，而只是通过一个开放的 IP 地址和端口来请求访问，防火墙则根据预先定义好的映射规则来判断这个访问是否安全及是否接受这个访问请求。网络地址转换的过程对于用户来说是透明的，不需要用户进行设置，用户只要进行常规操作即可。NAT 的工作过程如图 3.10 所示。

有些防火墙提供了“内部网到外部网”，“外部网到内部网”的双向 NAT 功能。同时支持两种方式的网络地址转换，一种为静态地址映射，即外部地址和内部地址一对一的映射，使内部地址的主机既可以访问外部网络，也可以接受外部网络提供的服务。另一种是更灵活的方式，可以支持多对一的映射，即内部的多个机器可以通过一个外部有效地址访问外部网络。让多个内部 IP 地址共享一个外部 IP 地址，就必须转换端口地址，这样内部不同 IP 地址的数据包就能转换为同一个 IP 地址而端口地址不同，通过这些端口对外部提供服务，这就意味着用户不需要为其网络中每台机器取得注册的 IP 地址。利用 NAT 转换功能不仅可以更有效地利用 IP 地址资源，解决 IP 地址短缺的问题；而且可使系统管理员自行设置内部的地址而不必对外公

开，隐藏了内部网络的真实地址，从而使外来的黑客无法探知内部网络的结构；同时使用 NAT 的网络，与外部网络的连接只能由内部网络发起，极大地提高了内部网络的安全性。

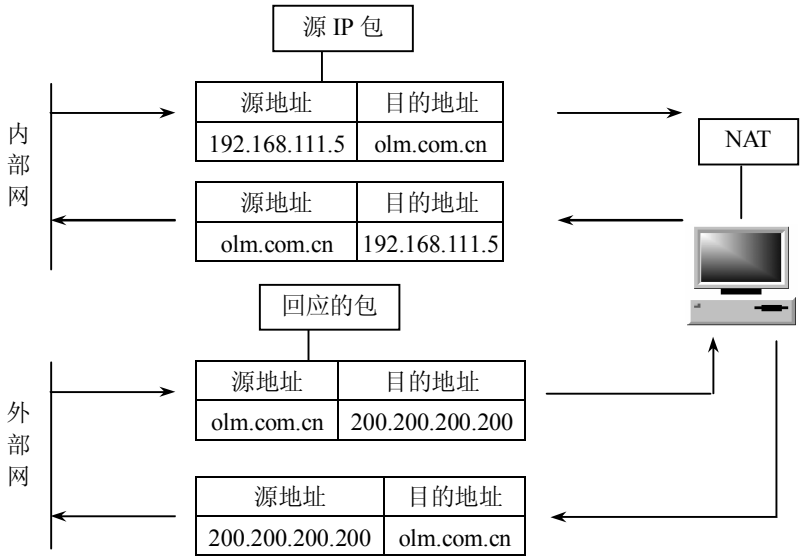

图 3.10　NAT 的工作过程

6. 网络状态监视器

由于现在广泛使用的 Intranet 均采用共享信道的方法，即把发给指定主机的信息广播到整个网络上。尽管在普通方式下，某台主机只能收到发给它的信息，然而只要这台主机将网络接口的方式设成“杂乱”模式的话，就可以接收到整个网络上的信息包。利用 Intranet 这个特性，将监视器接在用户网络环境某个特定的位置，如 Intranet 与 Internet 连接出口处，则监视器可以接收整个网络上的信息包。

状态监视器作为防火墙技术其安全特性最佳，它采用了一个在网关上执行网络安全策略的软件引擎，称之为检测模块。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施监测，抽取部分数据，即状态信息，并动态地保存起来作为以后制定安全决策的参考。检测模块支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充。

与其他安全方案不同，当用户访问到达网关的操作系统前，状态监视器要抽取有关数据进行分析，结合网络配置和安全规定做出接纳、拒绝、鉴定或给该通信加密等决定。一旦某个访问违反安全规定，安全报警器就会拒绝该访问，记录并向系统管理器报告网络状态。状态监视器还可以监测 Remote Procedure Call 类的端口信息。状态监视器的主要缺点是配置非常复杂，而且会降低网络的速度。

（1）网络状态监视器的基本功能。

1）可以按照指定的 IP 地址、特定域名或特定用户截取 Internet 上指定出口处流出的信息，或者截取全部数据包。

2）把截获的数据包重组，还原成用户传递的文件和明文（电子邮件、FTP 文件或 HTTP

文件等）。

3）分析、处理截获的信息。

4）用户可查询监控的最终结果，也可实时监视。

5）具有系统操作数据访问安全控制的能力，并且有自动转储的备份机制和智能卡存取访问控制。

（2）网络状态监视器的作用。担当了网络安全审计员：有利于事后分析、追查网络的攻击、破坏、涉密等犯罪行为，便于检查网络运行状态和安全状况；同时可作为网络安全报警器和保密检查员。

7. Internet 网关技术

由于是直接串连在网络之中，新一代防火墙必须支持用户在 Internet 互联的所有服务，同时还要防止与 Internet 服务有关的安全漏洞。故它要能以多种安全的应用服务器（包括 FTP、Finger、Mail、Telnet、News、WWW 等）来实现网关功能。为确保服务器的安全性，对所有的文件和命令均要利用“改变根系统调用（chroot）”作物理上的隔离。

在域名服务方面，新一代防火墙采用两种独立的域名服务器，一种是内部 DNS 服务器，主要处理内部网络的 DNS 信息；另一种是外部 DNS 服务器，专门用于处理机构内部向 Internet 提供的部份 DNS 信息。

在匿名 FTP 方面，服务器只提供对有限的受保护的部份目录的只读访问。在 WWW 服务器中，只支持静态的网页，而不允许图形或 CGI 代码等在防火墙内运行，在 Finger 服务器中，对外部访问，防火墙只提供可由内部用户配置的基本的文本信息，而不提供任何与攻击有关的系统信息。SMTP 与 POP 邮件服务器要对所有进、出防火墙的邮件进行处理，并利用邮件映射与标头剥除的方法隐除内部的邮件环境，Ident 服务器对用户连接的识别进行专门处理，网络新闻服务则为接收来自 ISP 的新闻开设了专门的磁盘空间。

8. 安全服务器网络（SSN）

为适应越来越多的用户向 Internet 上提供服务时对服务器保护的需要，新一代防火墙采用分别保护的策略对用户上网的对外服务器实施保护，它利用一张网卡将对外服务器作为一个独立网络处理，对外服务器既是内部网的一部分，又与内部网关完全隔离。这就是安全服务器网络（SSN）技术，对 SSN 上的主机既可单独管理，也可设置成通过 FTP、Telnet 等方式从内部网上管理。

SSN 的方法提供的安全性要比传统的隔离区（DMZ）方法好得多，因为 SSN 与外部网之间有防火墙保护，SSN 与内部网之间也有防火墙的保护，而 DMZ 只是一种在内、外部网络网关之间存在的一种防火墙方式。换言之，一旦 SSN 受破坏，内部网络仍会处于防火墙的保护之下，而一旦 DMZ 受到破坏，内部网络便暴露于攻击之下。

9. 用户鉴别与加密

为了降低防火墙产品在 Telnet、FTP 等服务和远程管理上的安全风险，鉴别功能必不可少，新一代防火墙采用一次性使用的口令字系统来作为用户的鉴别手段，并实现了对邮件的加密。

10. 用户定制服务

为满足特定用户的特定需求，新一代防火墙在提供众多服务的同时，还为用户定制提供支持，这类选项有：通用 TCP，出站 UDP、FTP、SMTP 等类，如果某一用户需要建立一个数据库的代理，便可利用这些支持，方便设置。

11. 审计和告警

新一代防火墙产品的审计和告警功能十分健全，日志文件包括一般信息、内核信息、核心信息、接收邮件、邮件路径、发送邮件、已收消息、已发消息、连接需求、已鉴别的访问、告警条件、管理日志、进站代理、FTP 代理、出站代理、邮件服务器、名服务器等。告警功能会守住每一个 TCP 或 UDP 探寻，并能以发出邮件、声响等多种方式报警。此外，新一代防火墙还在网络诊断、数据备份与保全等方面具有特色。

下面分别介绍几种应用防火墙的设计实现方式。

（1）应用网关代理。这种防火墙在网络应用层提供授权检查及代理服务。当外部某台主机试图访问（如 Telnet）受保护网时，它必须先在防火墙上经过身份认证。通过身份认证后，防火墙运行一个专门为 Telnet 设计的程序，把外部主机与内部主机连接。在这个过程中，防火墙可以限制用户访问的主机、访问的时间及访问的方式。同样，受保护网络内部用户访问外部网时也需先登录到防火墙上，通过验证后才可使用 Telnet 或 FTP 等有效命令。

应用网关代理（Application Gateway Proxy）的优点是既可以隐藏内部 IP 地址，也可以给单个用户授权，即使攻击者盗用了一个合法的 IP 地址，也通不过严格的身份认证。其缺点是这种认证使得应用网关不透明，用户每次连接都要受到“盘问”，这给用户带来许多不便；而且这种代理技术需要为每个应用网关写专门的程序。

（2）回路级代理服务器。回路级代理服务器也称一般代理服务器，它适用于多个协议，但无法解释应用协议，需要通过其他方式来获得信息。所以，回路级代理服务器通常要求修改过的用户程序。其中，套接字服务器（Sockets Server）就是回路级代理服务器。套接字（Sockets）是一种网络应用层的国际标准。当受保护网络客户机需要与外部网交互信息时，在防火墙上的套接字服务器检查客户的 UserID、IP 源地址和 IP 目的地址，经过确认后，套服务器才与外部的段服务器建立连接。对用户来说，受保护网与外部网的信息交换是透明的，感觉不到防火墙的存在，那是因为因特网络用户不需要登录到防火墙上。但是客户端的应用软件必须支持“Socket API”，受保护网络用户访问公共网络所使用的 IP 地址也都是防火墙的 IP 地址。

（3）代管服务器。顾名思义，代管服务器技术是把不安全的服务（如 FTP、Telnet 等）放到防火墙上，使它同时充当服务器，对外部的请示做出回答。与应用层代理实现相比，代管服务器技术不必为每种服务专门写程序。

而且，受保护网内部用户想对外部网访问时，也需先登录到防火墙上，再向外提出请求，这样从外部网向内就只能看到防火墙，从而隐藏了内部地址，提高了安全性。

（4）IP 通道（IP Tunnels）。经常会出现这种情况，一个大公司的两个子公司相隔较远，需通过 Internet 通信。这种情况下，可以采用 IP Tunnels 来防止 Internet 上的黑客截取信息。从而在 Internet 上形成一个虚构的企业网。

假如子网 A 中一主机（IP 地址为 X.X.X.X）欲向子网 B 中某主机（IP 地址为 Y.Y.Y.Y）发送报文，该报文经过本网防火墙 FW1（IP 地处 N.N.N.1）时，防火墙判断该报文是否发往子网 B，若是，则再增加一报头，变成从此防火墙到子网 B 防火墙 FW2（N.N.N.2）的 IP 报文，而原 IP 地址封装在数据区内，同原数据一起加密后经 Internet 发往 FW2。FW2 接收到报文后，若发现源 IP 地址是 FW1 的，则去掉附加报头，解密，在本网上传送。从 Internet 上看，就只是两个防火墙的通信。即使黑客伪装了从 FW1 发往 FW2 的报文，由于 FW2 在去掉报头

后不能解密，会抛弃报文。

（5）隔离域名服务器（Split Domain Name Sever）。这种技术是通过防火墙将受保护网络的域名服务器与外部网络的城名服务器隔离，使外部网络的域名服务器只能看到防火墙的 IP 地址，无法了解受保护网络的具体情况，这样可以保证受保护网络的 IP 地址不被外部网络知悉。

（6）邮件转发技术（Mail Forwarding）。当防火墙采用上面所提到的几种技术使得外部网络只知道防火墙的 IP 地址和域名时，从外部网络发来的邮件就只能送到防火墙上，这时防火墙对邮件进行检查，只有当发送邮件的源主机是被允许通过的，防火墙才对邮件的目的地址进行转换，送到内部的邮件服务器，由其进行转发。

3.2.3　防火墙的常见体系结构

一个防火墙系统通常由屏蔽路由器和代理服务器组成。屏蔽路由器是一个多端口的 IP 路由器，它通过对每一个到来的 IP 包依据一组规则进行检查来判断是否对之进行转发。屏蔽路由器从包头取得信息，例如协议号、收发报文的 IP 地址和端口号、连接标志及另外一些 IP 选项，对 IP 包进行过滤。屏蔽路由器的优点是简单和低（硬件）成本。其缺点在于正确建立包过滤规则比较困难，屏蔽路由器的管理成本高，缺乏用户级身份认证等。

屏蔽路由器（Screening Router）又叫包过滤路由器，是最简单、最常见的防火墙，屏蔽路由器作为内外连接的唯一通道，要求所有的报文都必须在此通过检查。除具有路由功能外，再装上包过滤软件，利用包过滤规则完成基本的防火墙功能，如图 3.11 所示。屏蔽路由器可以由厂家专门生产的路由器实现，也可以用主机来实现。这种配置的缺点有以下几点：

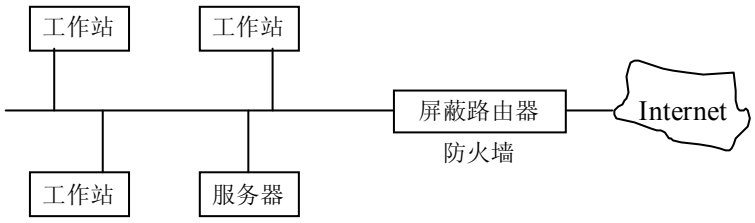

图 3.11　屏蔽路由器示意图

（1）没有或有很少的日志记录能力，因此网络管理员很难确定系统是否正在被入侵或已经被入侵了。

（2）规则表随着应用的深化会很快变得很大而且复杂。

（3）这种防火墙的最大弱点是依靠一个单一的部件来保护系统，一旦部件出现问题会使网络的大门敞开，而用户可能还不知道。

代理服务器是防火墙系统中的一个服务器进程，它能够代替网络用户完成特定的 TCP/IP 功能。一个代理服务器本质上是一个应用层的网关，一个为特定网络应用而连接两个网络的网关。

由于对更高安全性的要求，屏蔽路由器和代理服务器通常组合在一起构成混合系统，形成复合型防火墙产品。其中屏蔽路由器主要用来防止 IP 欺骗攻击。目前最广泛采用的配置是双宿主机网关防火墙、屏蔽主机型防火墙，以及被屏蔽子网型防火墙。

1. 双宿主机网关

这种配置是用一台装有两块网卡（NIC）的计算机作堡垒主机，两块网卡各自与受保护网络和外部网络相连，每一块网卡都有一个 IP 地址。堡垒主机上运行着防火墙软件——代理服务器软件（应用层网关），可以转发应用程序、提供服务等。所以叫做双宿主机网关（Dual Homed Gateway）防火墙，如图 3.12 所示。

图 3.12　双宿主机网关示意图

应该指出的是，在建立双宿主机时，应该关闭操作系统的路由能力，否则从一块网卡到另一块网卡的通信会绕过代理服务器软件，而使双宿主机网关失去防火墙的作用。

双宿主机网关优于屏蔽路由器的地方是：堡垒主机的系统软件可用于维护系统日志、硬件复制日志或远程日志。这对于日后的检查很有用，但这不能帮助网络管理者确认内部网中哪些主机可能已被黑客入侵。

双宿主机网关的一个致命弱点是：一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网上用户均可以随便访问内部网。

2. 屏蔽主机网关

屏蔽主机网关（Screened Gateway）由屏蔽路由器和应用网关组成，屏蔽路由器的作用是包过滤，应用网关的作用是代理服务，即在内部网络和外部网络之间建立了两道安全屏障，既实现了网络层安全（包过滤），又实现了应用层安全（代理服务）。屏蔽主机网关很容易实现：在内部网络与因特网的交汇点，安装一台屏蔽路由器，同时在内部网络上安装一个堡垒主机（应用层网关）即可，如图 3.13 所示。

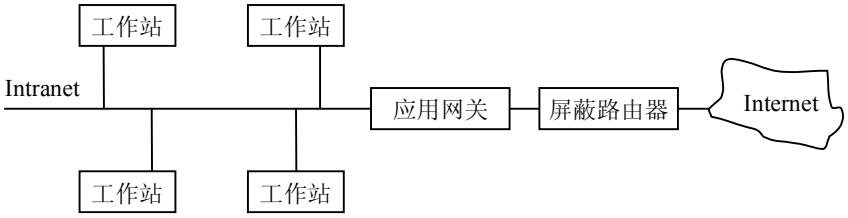

图 3.13　屏蔽主机网关示意图

注意：应用网关只有一块网卡，因此它不是双宿主机网关。

屏蔽主机网关防火墙具有双重保护，它比双宿主机网关防火墙更灵活，安全性更高。但由于要求对两个部件配置以便能协同工作，所以防火墙的配置工作很复杂。

3. 被屏蔽子网

被屏蔽子网（Screened Subnet）防火墙是在屏蔽主机网关防火墙的基础上再加一个路由

器，两个屏蔽路由器放在子网的两端，形成一个被称为非军事区（灰色阴影区域）的子网，即在内部网络和外部网络之间建立一个被隔离的子网，如图 3.14 所示。内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信，像 WWW 和 FTP 服务器可放在 DNZ 中。有的屏蔽子网中还设有一堡垒主机作为唯一可访问点，支持终端交互或作为应用网关代理。这种配置的危险带仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。外部屏蔽路由器和应用网关与在屏蔽主机网关防火墙中的功能相同。内部屏蔽路由器在应用网关与受保护网络之间提供附加保护，从而形成三道防线。因此，一个入侵者要进入受保护的网络比主机过滤防火墙更加困难。但是，它要求的设备和软件模块最多，其配置最贵且相当复杂。

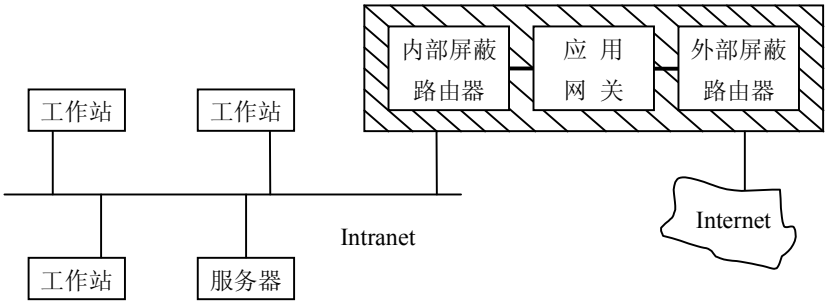

图 3.14　被屏蔽子网防火墙示意图

3.3　防火墙的主要性能指标

防火墙的主要性能指标包括如下九个方面。

1. 支持的局域网接口类型、数量及服务器平台

支持的 LAN 接口类型：防火墙所能保护的网络类型，如以太网、快速以太网、千兆以太网、ATM、令牌环及 FDDI 等。

支持的最大 LAN 接口数：指防火墙所支持的局域网络接口数目，也是其能够保护的不同内网数目。

服务器平台：防火墙所运行的操作系统平台（如 Linux、UNIX、Windows NT、专用安全操作系统等）。

2. 支持的协议

支持的非 IP 协议：除支持 IP 协议之外，还支持 AppleTalk、DECnet、IPX 及 NETBEUI 等协议。

建立 VPN 通道的协议：构建 VPN 通道所使用的协议，如密钥分配等，主要分为 IPSec、PPTP、专用协议等。

可以在 VPN 中使用的协议：在 VPN 中使用的协议，一般是指 TCP/IP 协议。

3. 对加密技术的支持

支持的 VPN 加密标准：VPN 中支持的加密算法，如数据加密标准 DES、3DES、RC4 以

及国内专用的加密算法。

提供基于硬件的加密：是否提供硬件加密方法，硬件加密可以提供更快的加密速度和更高的加密强度。

4. 对认证技术的支持

支持的认证类型：是指防火墙支持的身份认证协议，一般情况下具有一个或多个认证方案，如 RADIUS、Kerberos、TACACS/TACACS+、口令方式、数字证书等。防火墙能够为本地或远程用户提供经过认证与授权的对网络资源的访问，防火墙管理员必须决定客户以何种方式通过认证。

支持的认证标准和 CA 互操作性：厂商可以选择自己的认证方案，但应符合相应的国际标准，该项指所支持的标准认证协议，以及实现的认证协议是否与其他 CA 产品兼容互通。

支持数字证书。

5. 对访问控制技术的支持

通过防火墙的 IP 数据包的过滤规则应易于理解，易于编辑修改；同时应具备一致性检测机制，防止冲突。应用层协议过滤要求主要包括 FTP 过滤、基于 RPC 的应用服务过滤、基于 UDP 的应用服务过滤要求以及动态包过滤技术等。

在应用层提供代理支持，如 HTTP、FTP、TELNET、SNMP 等。

在传输层提供代理支持。

支持 FTP 文件类型过滤。

用户操作的代理类型：应用层高级代理功能，如 HTTP、POP3。

支持网络地址转换（NAT）。

支持硬件口令、智能卡等，这是一种比较安全的身份认证技术。

6. 对各种防御功能的支持

支持病毒扫描，提供内容过滤，能防御拒绝服务攻击（DoS），能阻止 ActiveX、Java、Cookies、JavaScript 入侵。能够过滤用户上载的 CGI、ASP 等程序，当发现危险代码时，向服务器报警。

7. 对安全特性的支持

支持转发和跟踪网间控制报文协议（ICMP 协议/ICMP 代理）。

提供入侵实时警告：提供实时入侵告警功能，当发生危险事件时，是否能够及时报警，报警的方式可能通过邮件、呼机、手机等。

提供实时入侵防范：提供实时入侵响应功能，当发生入侵事件时，防火墙能够动态响应，调整安全策略，阻挡恶意报文。

识别/记录/防止企图进行 IP 地址欺骗：IP 地址欺骗指使用伪装的 IP 地址作为 IP 包的源地址对受保护网络进行攻击，防火墙应该能够禁止来自外部网络而源地址是内部 IP 地址的数据包通过。

8. 管理功能

通过集成策略集中管理多个防火墙：是否支持集中管理，防火墙管理是指对防火墙具有管理权限的管理员行为和防火墙运行状态的管理。管理员的行为主要包括：通过防火墙的身份鉴别、编写防火墙的安全规则、配置防火墙的安全参数、查看防火墙的日志等。防火墙的管理一般分为本地管理、远程管理和集中管理等。

提供基于时间的访问控制：是否提供基于时间的访问控制。

支持 SNMP 监视和配置：SNMP 是简单网络管理协议的缩写。

本地管理：是指管理员通过防火墙的 Console 口或防火墙提供的键盘和显示器对防火墙进行配置管理。

远程管理：是指管理员通过以太网或防火墙提供的广域网接口对防火墙进行管理，管理的通信协议可以基于 FTP、TELNET、HTTP 等。

支持带宽管理：防火墙能够根据当前的流量动态调整某些客户端占用的带宽。

负载均衡特性：负载均衡可以看成动态的端口映射，它将一个外部地址的某一 TCP 或 UDP 端口映射到一组内部地址的某一端口，负载均衡主要用于将某项服务（如 HTTP）分摊到一组内部服务器上以平衡负载。

故障转移特性（failover）：指支持容错技术，如双机热备份、故障恢复，双电源备份等。

9. 记录和报表功能

防火墙处理完整日志的方法：防火墙规定了对于符合条件的报文做日志，应该提供日志信息管理和存储方法。

提供自动日志扫描：指防火墙是否具有日志的自动分析和扫描功能，这可以获得更详细的统计结果，达到事后分析、亡羊补牢的目的。

提供自动报表、日志报告书写器：防火墙实现的一种输出方式，提供自动报表和日志报告功能。

警告通知机制：防火墙应提供告警机制，在检测到入侵网络以及设备运转异常情况时，通过警告来通知管理员采取必要的措施，包括 E-mail、呼机、手机等。

提供简要报表（按照用户 ID 或 IP 地址）：防火墙实现的一种输出方式，按要求提供报表分类打印。

提供实时统计：防火墙实现的一种输出方式，日志分析后所获得的智能统计结果，一般是图表显示。

列出获得的国内有关部门许可证类别及号码：这是防火墙合格与销售的关键要素之一，包括公安部的销售许可证、国家信息安全测评中心的认证证书、总参的国防通信入网证和国家保密局的推荐证明等。

3.4　分布式防火墙

因为传统的防火墙设置在网络边界，在内部企业网和外部互联网之间构成一个屏障，进行网络存取控制，所以称为“边界式防火墙”（Perimeter Firewall）。随着计算机网络安全技术的发展和用户对防火墙功能要求的不断提高，在目前传统的边界式防火墙基础上开发出了一种新型防火墙，那就是“分布式防火墙”（Distributed Firewall）。它要负责对网络边界、各子网和网络内部各节点之间的安全防护，所以分布式防火墙是一个完整的系统，而不是单一的产品。

3.4.1　分布式防火墙的体系结构

分布式防火墙的体系结构包含网络防火墙、主机防火墙、中心管理三个部分：

1. 网络防火墙

网络防火墙（Network Firewall）功能上与传统的边界式防火墙类似，用于内部网与外部

网之间，以及内部网各子网之间的防护。与传统边界式防火墙相比，它多了一种用于对内部子网之间的安全防护层，这样整个网络的安全防护体系就显得更加全面、可靠。这一部分可采用纯软件方式实现，也可以提供相应的硬件支持。

2. 主机防火墙

主机防火墙（Host Firewall）用于对网络中的服务器和桌面机进行防护。这也是传统边界式防火墙所不具有的，也算是对传统边界式防火墙在安全体系方面的一个完善。它是作用在同一内部子网之间的工作站与服务器之间，以确保内部网络服务器的安全。这样防火墙的作用不仅是用于内部与外部网之间的防护，还可应用于内部网各子网之间、同一内部子网工作站与服务器之间。可以说达到了应用层的安全防护，比起网络层更加彻底。这一部分同样也有纯软件和硬件两种产品。

3. 中心管理

中心管理（Central Management）：这是一个服务器软件，负责总体安全策略的策划、管理、分发及日志的汇总，防火墙可以进行智能管理，提高了防火墙的安全防护灵活性。这是一种新的防火墙管理功能，也是传统的边界式防火墙所不具有的。

分布式防火墙由中心管理定义策略，但由各个分布在网络中的端点实施这些制定的策略。首先由制定防火墙接入控制策略的中心管理通过编译器将策略语言诉描述转换成内部格式，形成策略文件；然后中心管理采用系统管理工具把策略文件分发给各台“内部”主机；“内部”主机将从两方面来判定是否接受收到的包，一方面是根据 IP 安全协议，另一方面是根据服务器端的策略文件。

3.4.2 分布式防火墙的特点

综合起来，分布式防火墙具有以下几个主要特点：

1. 主机驻留

这种分布式防火墙的最主要特点就是采用主机驻留方式，所以也可称之为“主机防火墙”，它的重要特征是驻留在被保护的主机（关键服务器、数据及工作站）上，该主机以外的网络不管是处在网络内部还是网络外部都认为是不可信任的，因此可以针对该主机上运行的具体应用和对外提供的服务设定针对性很强的安全策略。对于 Web 服务器来说，分布式防火墙进行配置后能够阻止一些非必要的协议如 HTTP 和 HTTPS 之外的协议通过，从而阻止了非法入侵的发生，同时还具有入侵检测及防护功能。

这一特点对分布式防火墙体系结构的突出贡献是，使安全策略不仅仅停留在网络与网络之间，甚至把安全策略推广延伸到每个网络末端。

2. 嵌入操作系统内核

这主要是针对目前的纯软件的分布式防火墙来说的。众所周知，操作系统自身存在许多安全漏洞，运行在其上的应用软件无一不受到威胁。为了彻底堵住操作系统的漏洞，分布式防火墙的安全监测核心引擎要以嵌入操作系统内核的形态运行，直接接管网卡，对所有的信息流进行过滤与限制，无论是来自 Internet，还是来自内部网络，在把所有 IP 数据包进行检查后再提交操作系统。为实现这样的运行机制，除防火墙厂商自身的开发技术外，与操作系统厂商的技术合作也是必要的条件，因为这需要一些操作系统不公开的内部技术接口。不能实现这种运行模式的分布式防火墙由于受到操作系统安全性的制约，存在着明显的安全隐患。

3. 类似于个人防火墙

分布式防火墙针对桌面应用的主机防火墙与个人防火墙有相似之处，如它们都对应个人系统，但其差别又是本质性的。首先它们管理方式迥然不同，个人防火墙的安全策略由系统使用者自己设置，目标是防外部攻击，而针对桌面应用的主机防火墙的安全策略由整个系统的管理员统一安排和设置，除了对该桌面机起到保护作用外，也可以对该桌面机的对外访问加以控制，并且这种安全机制是桌面机的使用者不可见和不可改动的。其次，个人防火墙面向用户个人，针对桌面应用的主机防火墙是面向企业级客户的，它与分布式防火墙其他产品共同构成一个企业级应用方案，形成一个安全策略中心统一管理，安全检查机制分散布置的分布式防火墙体系结构。

4. 适用于服务器托管

互联网和电子商务的发展促进了互联网数据中心（DC）的迅速崛起，其主要业务之一就是服务器托管服务。对服务器托管用户而言，该服务器逻辑上是其企业网的一部分，只不过物理上不在企业内部，对于这种应用，边界防火墙解决方案就显得比较牵强附会，而分布式防火墙解决方案则是一个典型应用。对于纯软件式的分布式防火墙则用户只需在该服务器上安装上主机防火墙软件，并根据该服务器的应用设置安全策略即可，并可以利用中心管理软件对该服务器进行远程监控，不需任何额外租用新的空间放置边界防火墙。对于硬件式的分布式防火墙因其通常采用 PCI 卡式的，通常兼顾网卡作用，所以可以直接插在服务器机箱里面，也就无需单独的空间托管费了，对于企业来说更加实惠。

在新的安全体系结构下，分布式防火墙代表新一代防火墙技术的潮流，它可以在网络的任何交界和节点处设置屏障，从而形成了一个多层次、多协议，内外皆防的全方位安全体系。分布式防火墙的优势主要体现在如下几个方面：

（1）增强系统的安全性。增加了针对主机的入侵检测和防护功能，加强了对内部攻击的防范，可以实施全方位的安全策略。

在传统边界式防火墙应用中，内部网络非常容易受到有目的的攻击，一旦攻击者入侵了企业局域网的某台计算机，并获得这台计算机的控制权，便可以利用这台计算机作为入侵其他系统的跳板。而分布式防火墙将防火墙功能分布到网络的各个子网、桌面系统、笔记本计算机以及服务器上。凭借这种端到端的安全性能，分布式防火墙可以使企业避免发生由于某一台端点系统的入侵而导致向整个网络蔓延的情况发生，同时也使通过公共账号登录网络的用户无法进入那些限制访问的计算机系统。另外，由于分布式防火墙使用了 IP 安全协议使各主机之间的通信得到了很好的保护。所以分布式防火墙有能力防止各种类型的被动和主动攻击。特别在当用户使用 IP 安全协议中的密码凭证来标志内部主机时，基于这些标志的策略对主机来说无疑更具可信性。

（2）提高了系统性能。消除了结构性瓶颈问题，提高了系统性能。

传统防火墙由于拥有单一的接入控制点，无论对网络的性能还是对网络的可靠性都有不利的影响。分布式防火墙不但从根本上去除了单一的接入点，还可以针对各个服务器及终端计算机的不同需要，对防火墙进行最佳配置，配置时能够充分考虑到这些主机上运行的应用，可在保障网络安全的前提下大大提高网络运转效率。

（3）系统的扩展性。分布式防火墙随系统扩充提供了安全防护无限扩充的能力。

（4）实施主机策略。对网络中的各节点可以起到更安全的防护。

（5）应用更为广泛，支持 VPN 通信。

分布式防火墙最重要的优势在于，它能够保护物理拓扑上不属于内部网络，但位于逻辑上的“内部”网络的那些主机，这种需求随着 VPN 的发展越来越多。对这个问题的传统处理方法是将远程“内部”主机和外部主机的通信依然通过防火墙隔离来控制接入，而远程“内部”主机和防火墙之间采用“隧道”技术保证安全性，这种方法使原本可以直接通信的双方必须绕经防火墙，不仅效率低而且增加了防火墙过滤规则设置的难度。与之相反，分布式防火墙的建立本身就是基本逻辑网络的概念，因此对它而言，远程“内部”主机与物理上的内部主机没有任何区别，它从根本上防止了这种情况的发生。

3.5 Windows 2000 环境下防火墙及 NAT 的实现

由于种种原因，用 Microsoft Proxy Server 作为访问 Internet 的代理服务器，常常受到外部各种黑客搜索软件的探测和攻击。由于拥有专线的用户，也常常使用 Microsoft Proxy Server 为内部访问 Internet 提供方便，因此对疏于安全防范的用户来说，遭受的损失将不仅仅是金钱上的，而且可能给黑客留下攻击的后门，那情况就更糟了。但是不一定非要放弃使用 Proxy Server，而改用昂贵的硬件或软件防火墙。在下面的案例中提供了一种通过结合 Windows 2000 Server 的网络地址转换功能和 Microsoft Proxy Server 的动态包过滤功能，达到内部端口信息的隐藏和保护。

1. 实现方法

通过网络地址转换把内部地址转换成统一的外部地址，避免了使用代理服务所引起的账号安全问题和代理服务端口被利用的危险。同时为了避免各种代理服务端口探测和其他各种常用服务端口的探测，如 Web 代理端口 80、8080；21（FTP）；80（WWW）；25（SMTP）；110（POP3）；53（DNS），可以启用 Microsoft Proxy Server 的动态包过滤功能和 IP 分段过滤，达到端口隐形的效果。为了访问 Internet 和向外提供服务，还需要在 Proxy Server 的过滤列表中加入许可。

2. 案例环境

已知内部网络 10.1.0.0，子网掩码：255.255.255.0。假定 ISP 供应商提供的 IP 地址段为：192.168.0.9～192.168.0.14，子网掩码：255.255.255.248。假定有一台 Web 服务器（WWW），地址为 10.1.0.20，其完整域名为：www.target.com，对应解析的 IP 地址为 192.168.0.10，由 ISP 负责其域名解析。另有一台运行 Windows 2000 Server 及 MS Proxy Server 的服务器（Firewall），在其上装有两块网卡，命名为本地连接 1 和本地连接 2，它们的 IP 地址分别为：10.1.0.1 和 192.168.0.9。

注意：在这两块网卡的 IP 地址分配上，内部接口的 IP 地址应配置为内部网段的第一个 IP 地址，即 10.1.0.1；同理，外部接口的 IP 地址也应为有效地址段的第一个，即 192.168.0.9。路由器（192.168.0.14）专线接入 Internet。

3. MS Windows 2000 NAT 网络地址转换的实现

（1）路由和远程访问服务。集成在 Windows 2000 Server 的路由和远程访问服务（RRAS）提供了各种访问和连接 Internet 的能力，如连接远程访问用户、连接远程网络和接入 Internet。为了使局域网更安全的访问 Internet，RRAS 还提供了网络地址转换的功能，即把内部地址转

换成 ISP 分配的有效 IP 地址，很好地隐藏了内部网络信息和利于访问 Internet。对于需要向外提供服务的内部主机，也能通过地址的转换，接入 Internet。既能保证服务的正常运行，又能结合代理服务器的防火墙特性过滤非正常的访问。

在运行 Windows 2000 Server 及 MS Proxy Server 的服务器上，为了保证完全的通过地址转换访问 Internet，应通过 Internet 服务管理器，停止 Web Proxy、Winsock Proxy、Socks Proxy 的运行。请注意，此时 Proxy Server 的 IP 过滤功能仍然运行，因为相关的后台服务并未停止。

启动 RRAS 服务的过程为：依次单击“开始”→“程序”→“管理工具”→“路由和远程访问”命令，在弹出的对话框中右击“服务器”，在此例中为“Firewall（local）”，然后从菜单中选择“配置并启用路由和访问服务”。出现“RRAS 配置向导”对话框。单击“下一步”按钮，选择“Internet 连接服务器”，然后单击“下一步”按钮，选择“设置有网络地址转换（NAT）路由协议的路由器”。单击“下一步”按钮，选择“使用选择的 Internet 连接”，单击“连接入 Internet 的本地连接 2”，单击“下一步”按钮。然后再单击“下一步”按钮，完成服务的启动。

（2）网络地址转换的实现。

1）静态路由。启动 RRAS 之后，进入路由和远程访问管理界面，在“IP 路由选择”→“静态路由”中建立如下路由信息：

0.0.0.0 0.0.0.0　192.168.0.14（路由器地址）interface 本地连接 2 1

2）网络地址转换。为了让内部网络访问 Internet，接下来要完成的任务是使用 RRAS 提供 DHCP 服务，自动为内部主机分配 IP 地址。如果已经安装了 DHCP 服务可以不用此项设置。内部主机的默认网关均设为服务器防火墙的内部接口地址，此例中为本地连接 10.1.0.1，DNS 服务器地址设为 ISP 的 DNS 服务器地址即可。同时还需要设置 DHCP 分配的排除地址，这些地址是为向外提供服务的主机保留，因为这些主机需要静态的 IP 地址。

设置过程为：启动 RRAS 之后，进入路由和远程访问管理界面，在“IP 路由选择”→“网络地址转换”中右击，从弹出的快捷菜单中选择“属性”选项，单击地址分配一栏，设置地址范围为：10.1.0.0，子网掩码为：255.255.255.0，排除地址为：10.1.0.20，10.1.0.1。

3）地址和特殊端口。最后要使外部网络能够访问内部提供服务的主机和使内部访问 Internet，还须配置下列信息：配置 IP 地址的范围，建立保留 IP 地址条目，配置服务端口的重定向，如表 3.2 所示。

表 3.2　地址和特殊端口配置

配置 IP 地址池的范围	192.168.0.9	255.255.255.252	192.168.0.10
建立保留 IP 地址条目	192.168.0.10	10.1.0.20	允许传入会话
配置服务端口的重定向	192.168.0.10	公用端口号 80	10.1.0.20

在这里，地址转换只使用了有效 IP 地址段中的 192.168.0.9，192.168.0.10 两个地址。设置过程为：启动 RRAS 后，进入路由和远程访问管理界面，在“IP 路由选择”→“网络地址转换”的右边栏目中，选中本地连接 2 右击，从弹出的快捷菜单中选择“属性”选项，分别在地址和特殊端口进行配置。

4）IP 地址欺骗过滤。为防止外部和内部网络的 IP 地址欺骗，需要对此接口进行过滤，同样是在 RRAS 中完成配置。

内部地址欺骗过滤：建立外部接口，对谎称为内部地址的 IP 包进行过滤。

进入“IP 路由选择”→“常规”一栏，在右边栏目中选取本地连接 2 右击，从弹出的快捷菜单中选择“属性”选项，进入输入过滤器，配置接口过滤掉来自外部的内部地址访问，如表 3.3 所示。

表 3.3　内部地址欺骗过滤配置

源地址	源掩码	目标地址	目标掩码	协议	源端口	目标端口
10.1.0.0	255.255.0.0	任何	任何	任何	任何	任何

外部地址欺骗过滤：建立内部接口，对谎称为外部有效地址的 IP 包过滤。

同上，只不过选择的是内部接口——本地连接，如表 3.4 所示。

表 3.4　外部地址欺骗过滤配置

源地址	源掩码	目标地址	目标掩码	协议	源端口	目标端口
192.168.0.0	255.255.255.248	任何	任何	任何	任何	任何

4. MS Proxy Server 动态包过滤和反向代理

Proxy Server 功能的配置界面如图 3.15 所示。

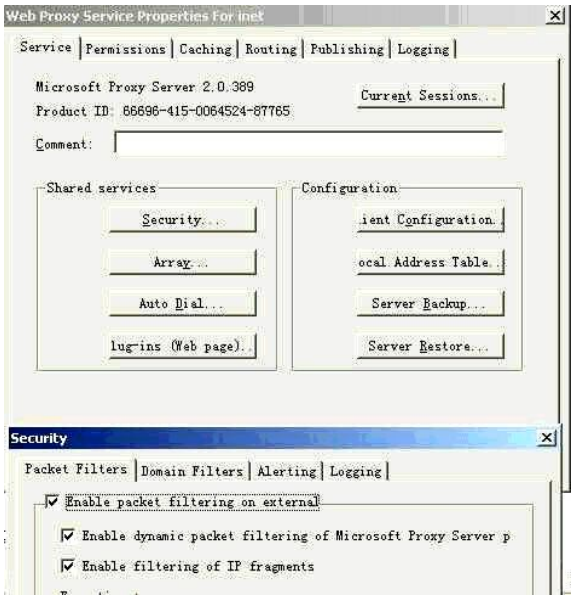

图 3.15　Proxy Server 功能的配置界面

下面对由包过滤产生的记录文件和此例所使用的过滤规则作列表说明。

（1）MS Proxy Server 动态过滤记录文件的详细说明。分析 MS Proxy Server 动态过滤产生的记录文件有助于发现新的问题和及时补漏，此类文件默认在 Winnt\system32\msplogs 目录下，文件名一般为 Pfyymmdd 形式。

2001-2-7，14:55:45，202.112.139.116，202.96.215.61，Tcp，1819，8080，SYN，0，202.96.215.51，-，-，

下面是对文件中一条记录条目的说明，如表 3.5 所示。

表 3.5　一条记录条目的说明

日期	时间	源地址	目标地址	协议	远端口	目标端口	Tcp 标志
2001-2-7	14:55:45	202.112.139.116	202.96.215.61	Tcp	1819	8080	SYN
过滤	接口	保留字段（Tcp Flags）					
0	202.96.215.51	-，-					

共分为以下几个部分：

- 通用信息记录部分。包括记录的时间和日期，即 IP 包被接受的日期和时间。
- 远程地址信息记录。包括源地址、源端口、访问协议。
- 局部地址信息记录。包括目标地址、目标端口。
- 过滤信息记录。包括过滤规则（0 或 1，分别表示拦截和通过）或地址接口。
- 包信息区域。Tcp Flags 连接标志。

（2）MS Proxy Server 动态包过滤的实现。在 MS Proxy Server 的过滤列表中建立此例中的过滤规则（许可通行的访问和连接），如表 3.6 所示。

表 3.6　动态包过滤规则

Number（序号）	Direction（进出方向）	Protocol（协议）	Local port（本地端口）	Remote port（远程端口）	Local address（本地地址）	Remote address（远端地址）
1	In	ICMP	PING	RESPONSE	Default	Any
2	In	ICMP	TIMEOUT	Any	Default	Any
3	In	ICMP	UNREACHABLE	Any	Default	Any
4	Out	ICMP	Any	Any	Default	Any
5	Both	TCP	HTTP SERVER	Any	192.168.0.10	Any
6	In	TCP	Dynamic	HTTP SERVER	192.168.0.10	Any
7	In	TCP	Dynamic	HTTP SERVER	Default	Any
8	Out	TCP	Dynamic	HTTP SERVER	192.168.0.10	Any
9	Out	TCP	Dynamic	HTTP SERVER	Default	Any
10	Both	UDP	Any	DNS	Default	Any

在此例中，因为地址转换只是用了有效 IP 地址段中的 192.168.0.9 和 192.168.0.10，其中 192.168.0.10 用于 Web 的访问，所以所有访问 Internet 的内部地址都转换成了 192.168.0.9（本地接口 2），从而在过滤表中就建立了允许通过 Default 外部接口访问 Internet Web 服务的规则（表中 7，9 行）；对外的访问还允许了 DNS 域名查询（第 10 行）；第 5 行允许外部访问内部 Web 主机，这里，首先访问到的是地址 192.168.0.10，然后通过地址转换把访问指向 10.1.0.20；第 6 行和第 8 行需配置，否则可能地址转换无法成功；第 1、2、3、4 行允许了内部对外部地

址的探测，同时又禁止向内的 ICMP 响应探测；未在列表中的所有访问均被拦截，这样由 SMB 共享产生的 139 端口连接探测、代理端口 8080 或 80 的探测均被阻截。

习题三

3-1 简要回答防火墙的定义和发展简史。
3-2 设置防火墙目的是什么？防火墙的功能和局限性各有哪些？
3-3 简述防火墙的发展动态和趋势。
3-4 试述包过滤防火墙的原理及特点。静态包过滤和动态包过滤有什么区别？
3-5 试述代理防火墙的原理及特点。应用层网关和电路层网关有什么区别？
3-6 防火墙的主要技术及实现方式有哪些？
3-7 防火墙的常见体系结构有哪几种？
3-8 屏蔽路由器防火墙和屏蔽主机网关防火墙各是如何实现的？
3-9 简述分布式防火墙的体系结构、主要特点。
3-10 分布式防火墙的优势主要体现在哪几个方面？
3-11 上机练习：配置一个双宿主机网关防火墙。