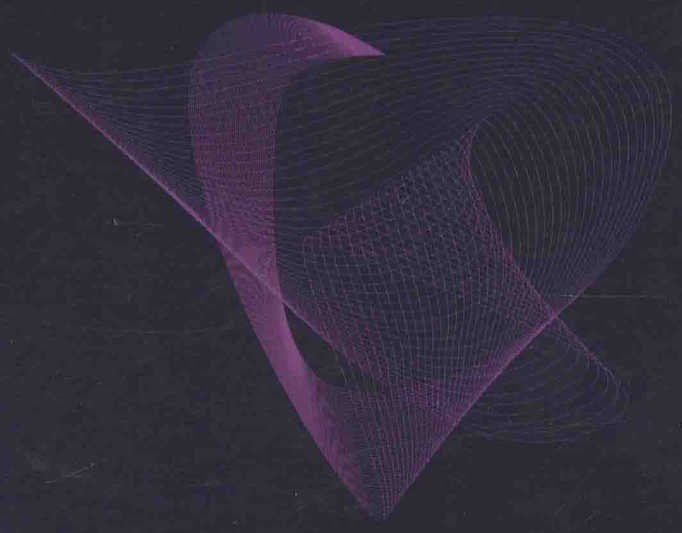
21世纪高等学校信息安全专业规划教材

防火墙技术及应用实践教程

毕 烨 吴秀梅 ◎ 编著

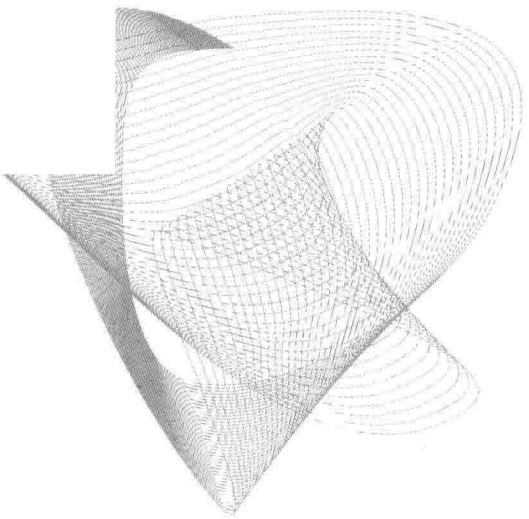


清華大學出版社

21世纪高等学校信息安全专业规划教材

防火墙技术及应用实践教程

毕 烨 吴秀梅 ◎ 编著



清華大學出版社
北京

内 容 简 介

本书共10章，第1章讲解防火墙的基础理论，内容包括防火墙概念、分类、功能及防火墙的相关知识等。第2章讲解防火墙的工作原理、具备的特性及常用的防火墙技术等。第3章讲解计算机操作系统如何配置系统自带的防火墙及如何应用防火墙等。第4章讲解常用著名防火墙设置和管理的基本操作。第5章讲解Red Hat Linux系统安全及Iptables防火墙配置。第6章讲解Windows Server 2003服务器防火墙和Windows 7防火墙的高级配置。第7章讲解Windows Server 2008 R2服务器的安全配置。第8章讲解ISA网络防火墙的应用操作。第9章介绍企业级防火墙TMG的部署。第10章讲解项目实践案例，虚拟企业的网络安全需求功能。

本教材适合学生自学参考，可作为本科、高职高专层次的教学实践用书，也可以给广大的网络安全入门的专业技术人员以及计算机爱好者提供参考。

图书在版编目(CIP)数据

防火墙技术及应用实践教程/毕烨，吴秀梅编著. —北京：清华大学出版社，2017
(21世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-46467-9

Ⅰ. ①防…　Ⅱ. ①毕… ②吴…　Ⅲ. ①防火墙技术－教材　Ⅳ. ①TP393.082

中国版本图书馆CIP数据核字(2017)第024660号

责任编辑：魏江江　薛　阳
封面设计：刘　键
责任校对：胡伟民
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：三河市春园印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：17　　**字　　数**：430千字
版　　次：2017年6月第1版　　**印　　次**：2017年6月第1次印刷
印　　数：1～2000
定　　价：39.00元

产品编号：062091-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

(5) 依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　言

网络安全问题随着互联网的发展与电子商务的盛行变得日益重要。随着企业和个人越来越频繁地使用互联网进行工作和生活，网络安全性成为一个重要的议题。数据在网络上传输，此时个人或公司传送的数据就有可能被拦截、修改或盗用。防火墙的目的就是保护网络不被未经授权的使用者经由外界网络不法侵入。

防火墙(Firewall)是指设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流，且本身具有较强的抗攻击能力。

为实现企业内部所需求的各项任务，防火墙需按照各类部门用户的需求制订安全策略，主要解决企业内网管理问题，便于统一管理各个部门的工作需求，改善以往比较混乱的情况，对所有关于网络的管理进行整合。

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之一，一般安装在被保护区域的边界处，被保护区域与 Internet 之间的防火墙可以有效控制区域内部网络与外部网络之间的访问和数据传输，进而达到保护区域内部信息安全的目的，同时，通过防火墙的检查控制可以过滤掉很多非法信息。

本书介绍了防火墙的基本概念与实验操作、配置系统自带的防火墙、常用著名防火墙设置、Red Hat Linux 系统安全及 Iptables 防火墙配置、Windows Server 2003 服务器防火墙、Windows 7 防火墙的高级配置、Windows Server 2008 R2 服务器的安全配置、ISA 网络防火墙、企业级防火墙 TMG 的部署、虚拟企业的网络安全项目实践案例。

通常，计算机网络工程专业和其他相关计算机专业的学生需要学习网络安全方面的课程，防火墙技术课程是网络安全方面的重要环节，是教学和实践的必选课程。在教学和实践的过程中，我们感到选用的教材不太适合实际的教学和实践，有的教材太偏重理论知识，缺乏实验和操作，有的教材不合适学生使用。在这个情况下，我们多次研究和总结，编写了本教程，并在实际的教学和实践中得到了师生的较好反应，于是决定出版以方便同类学生使用。

本教材编写的原则：针对网络安全类专业的教学规划，介绍防火墙的基本概念，着重讲述防火墙技术的实验、项目设计，为本科及高职高专的网络安全类专业提供可行的、实用的教程。

本教材编写的特点：注重实践操作和项目案例，结合当前防火墙技术的开发与应用的知识点，着重介绍防火墙的实验案例，以便于读者进行实际操作和掌握，使读者较快掌握防火墙技术并在实际中解决问题，给广大从事网络安全的人员提供一些帮助。

本教材由上海第二工业大学毕烨负责编写，吴秀梅参编。通过收集大量资料，经过多个学期的教学、实践反复论证，并以防火墙的实验案例为主导思想，完成此教材的编写。感谢上海第二工业大学的学生苏东坡、马博、吴中宁，他们参与了本书的实验与论证。

本书适用于应用技术型本科院校、高职高专层次的学生掌握防火墙应用技术，为打造真实的工作环境，本教材在第 10 章编写了虚拟企业基于防火墙技术的网络安全的设计开发工作，使学生可以在校内学习到在企业工作中所需要的技术，实现学业到就业的无缝衔接。由于作者水平有限，书中难免存在疏漏与不妥之处，敬请读者予以指正。

目　录

第1章　防火墙概述

网络安全问题将随着 Internet 宽带发展与电子商务的事务需求变得日益重要。企业或个人利用互联网来进行交易越来越频繁，相对地网络安全性就成为一个重要的问题。个人会使用信用卡在网络上做交易、公司之间做信息交换，一些重要资料会在网络上相互流动，这时个人或公司传送的资料就有可能会被拦截、修改或盗用，而有些黑客有时会为了试试他的技术而入侵别人的计算机，严重的会致使公司的网站被破坏并毁掉顾客资料，以致影响到公司的利益或顾客的隐私及权利。为此防火墙的目的就是要保护网络不被未经授权的使用者经由外界网络（如 Internet）不法侵入，为维护企业及个人的利益建立一道安全屏障。

1.1　防火墙定义

防火墙是指隔离在本地网络与外界网络之间的一道防御系统，是这一类防范措施的总称。

防火墙的架构是一套独立的软、硬件配置，基本上是在一台服务器上，由操作系统（Operating System，OS）及网络防火墙应用软件而构成。它架构于互联网（Internet）与内部网络（Intranet）之间，被运用于两个网络之间，作为内部与外部沟通的桥梁，也是企业网络对外接触的第一道大门。

在互联网上防火墙是一种非常有效的网络安全系统，通过它可以隔离风险区域（即 Internet 或有一定风险的网络）与安全区域（局域网）的连接，同时不会妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信量，从而完成看似不可能的任务；仅让安全、核准了的信息进入，同时又抵制有威胁的数据。随着安全性问题上的失误和缺陷越来越普遍，对网络的入侵不仅来自高超的攻击手段，也有可能来自配置上的低级错误或不合适的口令选择。因此，防火墙的作用是防止不希望的、未授权的通信进出被保护的网络，强化了网络安全政策。

一般的防火墙都可以达到以下目的：一是可以限制他人进入内部网络，过滤掉不安全服务和非法用户；二是防止入侵者接近防御设施；三是限定用户访问特殊站点；四是为监视 Internet 安全提供方便。由于防火墙假设了网络边界和服务，因此更适合于相对独立的网络，例如 Intranet 等种类相对集中的网络。防火墙正在成为控制对网络系统访问的非常流行的方法。目前，在 Internet 上的 Web 网站中，超过三分之一的 Web 网站都是由某种形式的防火墙加以保护，这是对黑客防范最严，安全性较强的一种方式，任何关键性的服务器，都建议放在防火墙之后。

防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成。

在互联网上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域（即 Internet 或有一定风险的网络）与安全区域（局域网）的连接。所谓“防火墙”，是指一种将内

部网和公众访问网(如 Internet)分开的方法,它实际上是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度,它能允许"同意"的人和数据进入网络,同时将"不同意"的人和数据拒之门外,最大限度地阻止网络中的黑客访问网络。换句话说,如果不通过防火墙,公司内部的人就无法访问 Internet,Internet 上的人也无法和公司内部的人进行通信。

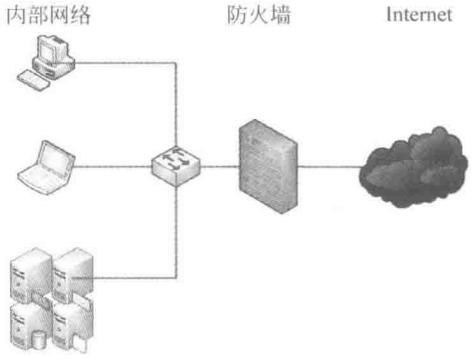


图 1-1 防火墙逻辑位置示意图

防火墙是设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合,如图 1-1 所示。它是不同网络或网络安全域之间信息的唯一出入口,能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流,且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。

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。防火墙可以是硬件型的,所有数据都首先通过硬件芯片监测,也可以是软件类型,软件在计算机上运行并监控。其实硬件型也就是芯片里固化了的软件,但是它不占用计算机 CPU 处理时间,功能非常强大,处理速度很快,但对于个人用户来说软件型更加方便实用。

防火墙技术从诞生开始,就在时刻不停地发展着,各种不同结构不同功能的防火墙,构筑成网络上的一道道防御大堤。

1.2 防火墙的分类与技术

1.2.1 防火墙的分类

防火墙分类的方法很多,除了从形式上把它分为软件防火墙和硬件防火墙以外,还可以从技术上分为包过滤型、应用代理型和状态监视三类;从结构上又分为单一主机防火墙、路由集成式防火墙和分布式防火墙三种;按工作位置分为边界防火墙、个人防火墙和混合防火墙;按防火墙性能分为百兆级防火墙和千兆级防火墙两类;等等。虽然看似种类繁多,但这只是因为业界分类方法不同罢了,例如,一台硬件防火墙就可能由于结构、数据吞吐量和工作位置而规划为"百兆级状态监视型边界防火墙",因此这里主要介绍的是技术方面的分类,即包过滤型、应用代理型和状态监视型防火墙技术。

为了更有效率地对付网络上各种不同的攻击手段,防火墙也划分出几种防御架构。根据物理特性,防火墙分为两大类,硬件防火墙和软件防火墙。软件防火墙是一种安装在负责内外网络转换的网关服务器或者独立的个人计算机上的特殊程序,它是以逻辑形式存在的,防火墙程序跟随系统启动,通过运行在 Ring0 级别的特殊驱动模块把防御机制插入系统关于网络的处理部分和网络接口设备驱动之间,形成一种逻辑上的防御体系。

在没有软件防火墙之前，系统和网络接口设备之间的通道是直接的，网络接口设备通过网络驱动程序接口(Network Driver Interface Specification，NDIS)把网络上传来的各种报文都忠实地交给系统处理，例如，一台计算机接收到请求列出机器上所有共享资源的数据报文，NDIS 直接把这个报文提交给系统，系统在处理后就会返回相应数据，在某些情况下就会造成信息泄漏。而使用软件防火墙后，尽管 NDIS 接收到的仍然是原封不动的数据报文，但是在提交到系统的通道上时多了一层防御机制，所有数据报文都要经过这层机制根据一定的规则判断处理，只有它认为安全的数据才能到达系统，其他数据则被丢弃。因为有规则提到“列出共享资源的行为是危险的”，因此在防火墙的判断下，这个报文会被丢弃，这样一来，系统接收不到报文，则认为什么事情也没发生过，也就不会把信息泄漏出去了。

软件防火墙工作于系统接口与 NDIS 之间，用于检查过滤由 NDIS 发送过来的数据，在无须改动硬件的前提下便能实现一定强度的安全保障，但是由于软件防火墙自身属于运行于系统上的程序，不可避免地需要占用一部分 CPU 资源维持工作，而且由于数据判断处理需要一定的时间，在一些数据流量大的网络里，软件防火墙会使整个系统工作效率和数据吞吐速度下降，甚至有些软件防火墙会存在漏洞，导致有害数据可以绕过它的防御体系，给数据安全带来损失，因此，许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施，而是使用看得见摸得着的硬件防火墙。

硬件防火墙是一种以物理形式存在的专用设备，通常架设于两个网络的驳接处，直接从网络设备上检查过滤有害的数据报文，位于防火墙设备后端的网络或者服务器接收到的是经过防火墙处理的相对安全的数据，不必另外分出 CPU 资源去进行基于软件架构的 NDIS 数据检测，可以大大提高工作效率。

硬件防火墙一般是通过网线连接于外部网络接口与内部服务器或企业网络之间的设备，这里又另外划分出两种结构，一种是普通硬件级别防火墙，它拥有标准计算机的硬件平台和一些功能经过简化处理的 UNIX 系列操作系统和防火墙软件，这种防火墙措施相当于专门拿出一台计算机安装了软件防火墙，除了不需要处理其他事务以外，它毕竟还是一般的操作系统，因此有可能会存在漏洞和不稳定因素，安全性并不能做到最好；另一种是所谓的“芯片”级硬件防火墙，它采用专门设计的硬件平台，在上面搭建的软件也是专门开发的，并非流行的操作系统，因而可以达到较好的安全性能保障。

所谓的边界防火墙、单一主机防火墙又是什么概念呢？所谓边界，就是指两个网络之间的接口处，工作于此的防火墙就被称为“边界防火墙”；与之相对的有“个人防火墙”，它们通常是基于软件的防火墙，只处理一台计算机的数据而不是整个网络的数据，现在一般家庭用户使用的软件防火墙就是属于这一类。而单一主机防火墙，就是最常见的一台台硬件防火墙了；一些厂商为了节约成本，直接把防火墙功能嵌进路由设备里，就形成了路由集成式防火墙。

下面介绍防火墙的基本类型。

1. 包过滤防火墙

第一代防火墙和最基本形式的防火墙检查每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则。这称为包过滤防火墙。本质上，包过滤防火墙是多址的，表明它有两个或两个以上网络适配器或接口。例如，作为防火墙的设备可能有两块网卡(NIC)，一块连到内部网络，一块连到公共的 Internet。防火墙的任务，就是作为“通信警察”，指引包

和截住那些有危害的包。

包过滤防火墙检查每一个传入包，查看包中可用的基本信息（源地址和目的地址、端口号、协议等）。然后，将这些信息与设立的规则相比较。如果已经设立了阻断 Telnet 连接，而包的目的端口是 23 的话，那么该包就会被丢弃。如果允许传入 Web 连接，而目的端口为 80，则包就会被放行。

多个复杂规则的组合也是可行的。如果允许 Web 连接，但只针对特定的服务器，目的端口和目的地址二者必须与规则相匹配，才可以让该包通过。

最后，可以确定当一个包到达时，如果有理由让该包通过，就要建立规则来处理它。

建立一个包过滤防火墙规则的例子如下。

对来自专用网络的包，只允许来自内部地址的包通过，因为其他包包含不正确的包头部信息。这条规则可以防止网络内部的任何人通过欺骗性的源地址发起攻击。而且，如果黑客对专用网络内部的机器具有了不知从何得来的访问权，这种过滤方式可以阻止黑客从网络内部发起攻击。

在公共网络，只允许目的地址为 80 端口的包通过。这条规则只允许传入的连接为 Web 连接。这条规则也允许与 Web 连接使用相同端口的连接，所以它并不是十分安全。

丢弃从公共网络传入的包，而这些包都有网络内的源地址，从而减少 IP 欺骗性的攻击。

丢弃包含源路由信息的包，以减少源路由攻击。要记住，在源路由攻击中，传入的包包含路由信息，它覆盖了包通过网络应采取的正常路由，可能会绕过已有的安全程序。通过忽略源路由信息，防火墙可以减少这种方式的攻击。

2. 状态/动态检测防火墙

状态/动态检测防火墙，试图跟踪通过防火墙的网络连接和包，这样防火墙就可以使用一组附加的标准，以确定是否允许和拒绝通信。它是在使用了基本包过滤防火墙的通信上应用一些技术来做到这点的。

当包过滤防火墙见到一个网络包，包是孤立存在的。它没有防火墙所关心的历史或未来。允许和拒绝包的决定完全取决于包自身所包含的信息，如源地址、目的地址、端口号等。包中没有包含任何描述它在信息流中的位置的信息，则该包被认为是无状态的，它仅是存在而已。

检查一个有状态包防火墙跟踪的不仅是包中包含的信息。为了跟踪包的状态，防火墙还记录有用的信息以帮助识别包，例如已有的网络连接、数据的传出请求等。

如果传入的包包含视频数据流，防火墙可能已经记录了有关信息，是关于位于特定 IP 地址的应用程序最近向发出包的源地址请求视频信号的信息。如果传入的包是要传给发出请求的相同系统，防火墙进行匹配，包就可以被允许通过。

一个状态/动态检测防火墙可截断所有传入的通信，而允许所有传出的通信。因为防火墙跟踪内部出去的请求，所有按要求传入的数据被允许通过，直到连接被关闭为止。只有未被请求的传入通信被截断。

如果在防火墙内正运行一台服务器，配置就会变得稍微复杂一些，但状态包检查是很有力度和适应性的技术。例如，可以将防火墙配置成只允许从特定端口进入的通信，只可传到特定服务器。如果正在运行 Web 服务器，防火墙只将 80 端口传入的通信发到指定的 Web 服务器。

另外，状态/动态检测防火墙可提供的其他一些额外的服务如下。

(1) 将某些类型的连接重定向到审核服务中去。例如，到专用 Web 服务器的连接，在 Web 服务器连接被允许之前，可能被发到 SecutID 服务器(用一次性口令来使用)。

(2) 拒绝携带某些数据的网络通信，例如，带有附加可执行程序的传入电子消息，或包含 ActiveX 程序的 Web 页面。

跟踪连接状态的方式取决于包通过防火墙的类型。

(1) TCP 包。当建立起一个 TCP 连接时，通过的第一个包被标有包的 SYN 标志。一般情况下，防火墙会丢弃所有外部的连接企图，除非已经建立起某条特定规则来处理它们。对内部的连接试图连到外部主机，防火墙会注明连接包，允许响应及随后再连接两个系统之间的包，直到连接结束为止。在这种方式下，传入的包只有在它是响应一个已建立的连接时，才会被允许通过。

(2) UDP 包。UDP 包比 TCP 包简单，因为它们不包含任何连接或序列信息。它们只包含源地址、目的地址、校验和携带的数据。信息的缺乏使得防火墙确定包的合法性很困难，因为没有打开的连接可以测试传入的包是否应被允许通过。可是，防火墙跟踪连接状态的方式可以确定。对传入的包，若它所使用的地址和 UDP 包携带的协议与传出的连接请求匹配，该包就被允许通过。和 TCP 包一样，UDP 包会被允许通过，是响应传出的请求或已经建立了指定的规则来处理它。

对其他种类的包，情况和 UDP 包类似。防火墙仔细地跟踪传出的请求，记录下所使用的地址、协议和包的类型，然后对照保存过的信息核对传入的包，以确保这些包是被请求的。

3. 应用程序代理防火墙

应用程序代理防火墙实际上并不允许在它连接的网络之间直接通信。它是接收来自内部网络特定用户应用程序的通信，再建立单独的公共网络服务器连接。网络内部的用户不直接与外部的服务器通信，所以服务器不能直接访问内部网的任何一部分。

另外，如果不为特定的应用程序安装代理程序代码，这种服务是不会被支持的，不能建立任何连接。这种建立方式拒绝任何没有明确配置的连接，从而提供了额外的安全性和控制性。

例如，一个用户的 Web 浏览器可能在 80 端口，但也经常可能是在 1080 端口，连接到了内部网络的 HTTP 代理防火墙。防火墙会接收这个连接请求，并把它转到所请求的 Web 服务器。这种连接和转移对该用户来说是透明的，因为它完全是由代理防火墙自动处理的。代理防火墙通常支持的一些常见的应用程序有 HTTP、HTTPS/SSL、SMTP、POP3、IMAP、NNTP、Telnet、FTP 和 IRC。

应用程序代理防火墙可以配置成允许来自内部网络的任何连接，它也可以配置成要求用户认证后才建立连接。要求认证的方式有只为已知的用户建立连接的限制，为安全性提供了额外的保证。如果网络受到危害，这个特征使得从内部发动攻击的可能性大大减少。

4. NAT

讨论到防火墙的主题，就一定要提到有一种路由器，尽管从技术上讲它根本不是防火墙。网络地址转换(NAT)协议将内部网络的多个 IP 地址转换到一个公共地址发到 Internet 上。

NAT 经常用于小型办公室、家庭等网络，多个用户分享单一的 IP 地址，并为 Internet 连接提供一些安全机制。

当内部用户与一个公共主机通信时，NAT 追踪是哪一个用户发起的请求，修改传出的包，这样包就像是来自单一的公共 IP 地址，然后再打开连接。一旦建立了连接，在内部计算机和 Web 站点之间来回流动的通信就都是透明的了。

当从公共网络传来一个未经请求的传入连接时，NAT 有一套规则来决定如何处理它。如果没有事先定义好的规则，NAT 只是简单地丢弃所有未经请求的传入连接，就像包过滤防火墙所做的那样。

可是，就像对包过滤防火墙一样，可以将 NAT 配置为接受某些特定端口传来的传入连接，并将它们送到一个特定的主机地址。

1.2.2 防火墙的技术

传统意义上的防火墙技术分为三大类：包过滤（Packet Filtering）、应用代理（Application Proxy）和状态监视（Stateful Inspection）。无论一个防火墙的实现过程多么复杂，归根结底都是在这三种技术的基础上进行功能扩展的。

1. 包过滤技术

包过滤是最早使用的一种防火墙技术，它的第一代模型是静态包过滤（Static Packet Filtering）。使用包过滤技术的防火墙通常工作在 OSI 模型中的网络层（Network Layer）上，后来发展更新的动态包过滤（Dynamic Packet Filtering）增加了传输层（Transport Layer）。简而言之，包过滤技术工作的地方就是各种基于 TCP/IP 协议的数据报文进出的通道，它把这两层作为数据监控的对象，对每个数据包的头部、协议、地址、端口、类型等信息进行分析，并与预先设定好的防火墙过滤规则（Filtering Rule）进行核对，一旦发现某个包的某个或多个部分与过滤规则匹配并且条件为“阻止”的时候，这个包就会被丢弃。适当地设置过滤规则可以让防火墙工作得更安全有效，但是这种技术只能根据预设的过滤规则进行判断，一旦出现一个没有在设计人员意料之中的有害数据包请求，整个防火墙就形同虚设了。

读者也许会想，自行添加不行吗？但是别忘了，为普通计算机用户考虑，并不是所有人都了解网络协议的，如果防火墙工具出现了过滤遗漏问题，他们只能等着被入侵了。一些公司采用定期从网络升级过滤规则的方法，这个创意固然可以方便一部分家庭用户，但是对相对比较专业的用户而言，却不见得就是好事，因为他们可能会有根据自己的机器环境设定和改动的规则，如果这个规则刚好和升级到的规则发生冲突，用户就该郁闷了，而且如果两条规则冲突了，防火墙会不会当场崩溃？也许就因为考虑到这些因素，至今没见过有多少个产品会提供过滤规则更新功能的，这并不能和杀毒软件的病毒特征库升级原理相提并论。

为了解决这种鱼与熊掌难以兼得的问题，人们对包过滤技术进行了改进，这种改进后的技术称为动态包过滤技术（市场上存在一种基于状态的包过滤防火墙技术，即 Stateful-based Packet Filtering，它们其实是同一类型）。与它的前辈相比，动态包过滤功能在保持原有静态包过滤技术和过滤规则的基础上，会对已经成功与计算机连接的报文传输进行跟踪，并且判断该连接发送的数据包是否会对系统构成威胁，一旦触发其判断机制，防火墙就会自动产生新的临时过滤规则或者对已经存在的过滤规则进行修改，从而阻止该有害数据的继续传输。但是由于动态包过滤需要消耗额外的资源和时间来提取数据包内容进行判断处

理，所以与静态包过滤相比，它会降低运行效率，但是静态包过滤已经几乎退出市场了，能选择的，大部分也只有动态包过滤防火墙了。

2. 应用代理技术

由于包过滤技术无法提供完善的数据保护措施，而且一些特殊的报文攻击仅使用过滤的方法并不能消除危害（如 SYN 攻击、ICMP 洪水等），因此人们需要一种更全面的防火墙保护技术，在这样的需求背景下，采用应用代理（Application Proxy）技术的防火墙诞生了。代理服务器作为一个为用户保密或者突破访问限制的数据转发通道，在网络上应用广泛。一个完整的代理设备包含一个服务端和客户端，服务端接收来自用户的请求，调用自身的客户端模拟一个基于用户请求的连接到目标服务器，再把目标服务器返回的数据转发给用户，完成一次代理工作过程。“应用代理”防火墙，实际上就是一台小型的带有数据检测过滤功能的透明代理服务器（Transparent Proxy），但是它并不是单纯地在一个代理设备中嵌入包过滤技术，而是一种被称为应用协议分析（Application Protocol Analysis）的新技术。

“应用协议分析”技术工作在 OSI 模型的最高层——应用层上，在这一层里能接触到的所有数据都是最终形式，也就是说，防火墙“看到”的数据和我们看到的是一样的，而不是一个个带着地址端口协议等原始内容的数据包，因而它可以实现更高级的数据检测过程。整个代理防火墙把自身映射为一条透明线路，在用户方面和外界线路看来，它们之间的连接并没有任何阻碍，但是这个连接的数据收发实际上是经过了代理防火墙转向的，当外界数据进入代理防火墙的客户端时，“应用协议分析”模块便根据应用层协议处理这个数据，通过预置的处理规则查询这个数据是否带有危害，由于这一层面对的已经不再是组合有限的报文协议，所以防火墙不仅能根据数据层提供的信息判断数据，更能像管理员分析服务器日志那样“看”内容辨危害。而且由于工作在应用层，防火墙还可以实现双向限制，在过滤外部网络有害数据的同时也监控着内部网络的信息，管理员可以配置防火墙实现一个身份验证和连接时限的功能，进一步防止内部网络信息泄漏的隐患。

最后，由于代理防火墙采取代理机制进行工作，内外部网络之间的通信都需先经过代理服务器审核，通过后再由代理服务器连接，根本没有给分隔在内外部网络两边的计算机直接会话的机会，可以避免入侵者使用“数据驱动”攻击方式（一种能通过包过滤技术防火墙规则的数据报文，但是当它进入计算机处理后，却变成能够修改系统设置和用户数据的恶意代码）渗透内部网络，可以说，应用代理是比包过滤技术更完善的防火墙技术。

但是，似乎任何东西都不可能逃避墨菲定律的规则，代理型防火墙的结构特征偏偏正是它最大的缺点，由于它是基于代理技术的，通过防火墙的每个连接都必须建立在为之创建的代理程序进程上，而代理进程自身是要消耗一定时间的，更何况代理进程里还有一套复杂的协议分析机制在同时工作，于是数据在通过代理防火墙时就不可避免地发生数据迟滞现象。换个形象的说法，每个数据连接在经过代理防火墙时都会先被请进保安室喝杯茶、搜搜身，再继续赶路，而保安的工作速度并不能很快。代理防火墙是以牺牲速度为代价换取了比包过滤防火墙更高的安全性能的，在网络吞吐量不是很大的情况下，也许用户不会察觉到什么，然而到了数据交换频繁的时刻，代理防火墙就成了整个网络的瓶颈，而且一旦防火墙的硬件配置支撑不住高强度的数据流量而发生罢工，整个网络可能就会因此瘫痪了。所以，代理防火墙的普及范围还远远不及包过滤型防火墙，所以就目前整个庞大的软件防火墙市场来说，代理防火墙很难有立足之地。