21世纪高等职业教育信息技术类规划教材
21 Shiji Gaodeng Zhiye Jiaoyu Xinxi Jishulei Guihua Jiaocai

计算机网络安全管理

JISUANJI WANGLUO ANQUAN GUANLI

王群 编著　余明辉 主审

- 基础知识与基本应用讲解浅显易懂
- 实训操作与基本原理介绍融会贯穿
- 教学内容与应用需求衔接有机结合

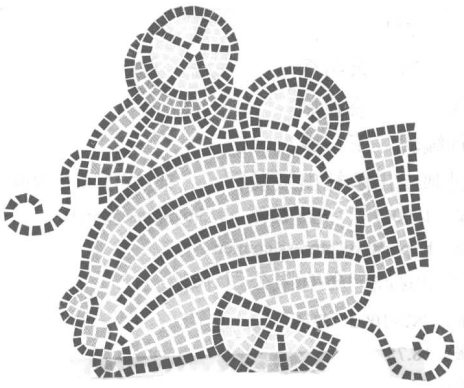
人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等职业教育信息技术类规划教材
21 Shiji Gaodeng Zhiye Jiaoyu Xinxi Jishulei Guihua Jiaocai

计算机网络安全管理

JISUANJI WANGLUO ANQUAN GUANLI

王群 编著　余明辉 主审



人民邮电出版社
北京

图书在版编目（CIP）数据

计算机网络安全管理 / 王群编著. -- 北京 : 人民邮电出版社, 2010.3
21世纪高等职业教育信息技术类规划教材
ISBN 978-7-115-21964-0

Ⅰ. ①计… Ⅱ. ①王… Ⅲ. ①计算机网络－安全技术－高等学校：技术学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2010)第010109号

内 容 提 要

本书从信息安全与网络安全的关系入手，在介绍了信息安全和网络安全的概念及联系、网络安全所面临的主要威胁和解决方法、网络安全的发展趋势等基础知识后，重点从物理安全、计算机病毒及防范、防火墙技术与应用、入侵检测与黑客攻击防范、数据加密技术及应用、VPN 技术与应用、无线网络安全、计算机网络管理等方面，系统介绍了相关技术的概念、简要工作原理、使用方法和应用特点。同时，为便于教学工作的开展，介绍了网络安全实验环境的组建方式，并结合一个具体的网络实例，分析了安全管理方案的设计和部署方法。

本书可作为高职高专计算机系“网络安全管理”及相关课程的教材，也可作为广大计算机应用工程技术人员、网络管理人员的参考书。

21 世纪高等职业教育信息技术类规划教材

计算机网络安全管理

◆ 编　　著　王　群
主　　审　余明辉
责任编辑　潘春燕
执行编辑　王　威

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：18.75
字数：477 千字　　2010 年 3 月第 1 版
印数：1－3 000 册　　2010 年 3 月河北第 1 次印刷

ISBN 978-7-115-21964-0

定价：32.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着计算机网络技术的快速发展及应用的逐渐普及，信息化已经成为推动社会发展的重要手段。实现信息化的基础设施是计算机网络，但是由于计算机网络具有连接形式的多样性、网络系统的开放性、终端接入的任意性、用户身份的弱认证性等特征，致使网络易受黑客、病毒和其他恶意程序的攻击，信息的安全和保密成为一个至关重要的问题。

“计算机网络安全管理”以计算机网络为基础和环境，以管理为手段，以安全为目标。网络安全与网络管理虽然在研究方法和研究内容上存在侧重点不同，但两者的实现目标是相同的，实现方法和过程是交叉的，安全离不开管理，管理的目标之一是安全。基于这一思想，本书将网络安全与网络管理两方面的内容从知识组织、实现方法、应用特点等方面进行了有机结合，实现了在安全中融入管理，在管理中实现安全。这一思想也符合目前计算机网络的应用现状和管理趋势。

随着网络安全在实际工作中的重要性日益凸显，目前各高职高专院校也将网络安全管理课程作为网络专业的核心课程。

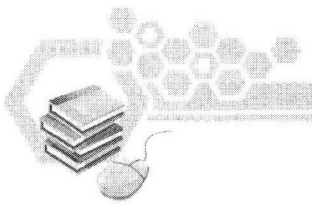
本书是作者在总结了多年网络课程的教学经验和网络管理工作的基础上编写的，在内容安排上本书强调了以下 3 点：一是从信息安全与网络安全的关系入手，介绍了信息安全和网络安全的概念及联系，分析了网络安全所面临的主要威胁，并提出了相应的解决方法。综合目前网络应用，提出了网络安全的发展趋势。通过这一部分内容的学习，使读者对网络安全的概念、现状及未来发展有一个总体宏观的认识。这部分内容全部安排在第 1 章；二是考虑到教学实际，立足安全管理技术的应用现状，从众多技术和方法中精练出了本书的主要内容（具体从第 3 章到第 10 章），其中包括物理安全、计算机病毒及防范、防火墙技术与应用、入侵检测与黑客攻击防范、数据加密技术及应用、VPN 技术与应用、无线网络安全、基于 SNMP 的网络管理技术及应用等；三是为了便于教学工作的开展，第 2 章专门介绍了网络安全实验环境的组建方式，其中包括 VMware 虚拟机的应用，Sniffer Pro 的配置和应用等。同时，第 11 章结合一个具体的网络实例，分析了安全管理方案的设计和实施方法，本章的内容也是对本书前面内容的综合应用。

在本书的编写过程中，作者参考了大量的国内外文献资料，其中部分文献的出处并未全部列出。对涉及的每一个实验操作都在实验室或真实网络环境中进行了测试，以保证实验操作步骤和内容的正确性。其中，部分实验和应用来自作者单位真实的网络环境。

在本书编写过程中得到了作者家人及同事的帮助，其中李馥娟、郭亚峰、刘庆航、聂明辉、陶慎亮等老师负责了部分实验的测试和文字的校对工作，番禺职院的余明辉老师审阅本书，借此机会向他们表示衷心的感谢！由于作者研究水平有限，书中难免存在一些缺点和错误，殷切希望广大教师和读者批评指正，作者的 E-mail 为 wqga@yeah.net。

编　者

2009 年 12 月于南京



目 录

第1章 计算机网络安全管理技术概述

以 Internet 为代表的互联网络能够取得今天的成功，在很大程度上取决于其**开放性、易扩展性和易用性**。与此同时，系统设计上的开放性、易扩展性和易用性却导致了应用上的不安全性。本章从信息安全的概念入手，逐步介绍网络安全管理的主要知识，为读者循序渐进地学习后续章节的内容提供一条清晰的思路和主线。

1.1 信息安全与网络安全

在介绍计算机网络安全的相关知识时，许多教材和专业图书将信息安全与网络安全混为一谈，认为信息安全就是网络安全，其实这种定义或认识是错误的，至少是不准确的。

1.1.1 信息安全

1. 信息的概念

信息的概念有广义和狭义之分：广义的信息概念是指事物的特征以及运动和变化状态，这些特征和状态给人们提供了有关认识这种事物的各种各样的信息；狭义的信息概念是指新闻、消息、情况、情报、报道、状态和一般知识等，如某件事的情节、各种资料、书报知识等。计算机网络中的信息一般具有以下特点。

- 具体化。这类信息专指在计算机网络环境中存在的信息。
- 数字化。这类信息被计算机通过编码处理后，以 0 和 1 组成的特殊组合形式存储在计算机及相关设备中。
- 网络化。这类信息主要通过计算机网络来传输。

2. 信息安全的概念

信息安全是对信息及信息系统的安全属性及功能、效率进行保障的过程，具体涉及人、技术和管理等综合因素，以保证信息内容、计算环境、边界与连接、网络基础设施的可用性、完整性、机密性、可控性、可审查性等安全属性，从而保障应用服务的效率和效益，以促进信息化的可持续发展。

从该定义可以看出，信息安全具有的3个基本要素为人、技术和管理。

- **人**。这里的人专指实现信息安全的整个过程中所涉及的人员，如单位信息安全制度的制定者与实施者，业务系统的设计者、开发者、维护者与管理者，业务系统的合法用户，可能存在的网络入侵者，信息安全事件的报告者、分析者、处理者，信息安全领域的法律工作者等。
- **技术**。这里的技术是指提供信息安全服务和实现信息安全保障过程中所采取的行之有效的技术措施和所采用的安全产品，具体包括信息安全体系结构和标准、信息安全策略、信息安全原则（如身份认证、PKI等）、信息安全产品（如防火墙、杀病毒软件、IDS、IPS等）、系统安全风险评估等。
- **管理**。这里的管理一般是指对实现信息安全的具体目标负有责任的有关人员所制定的管理职责，具体包括制定和实施符合实际需求的安全策略、安全管理、账号和密钥管理、数据和系统的备份与恢复等。

在人、技术和管理这三要素中，一方面三者相辅相成，缺一不可；另一方面，在将人的重要性放在第一位的同时，坚持“三分技术，七分管理”这一基本原则。

信息安全中定义的5个基本安全属性分别为可用性、完整性、机密性、可控性、可审查性。

- **机密性**。确保信息不暴露给未经授权的人或应用进程。
- **完整性**。只有得到允许的人或应用进程才能修改数据，并且能够判别出数据是否已被更改。
- **可用性**。只有得到授权的用户在需要时才可以访问数据，即使在网络被攻击时也不能阻碍授权用户对网络的使用。
- **可控性**。能够对授权范围内的信息流向和行为方式进行控制。
- **可审查性**。当网络出现安全问题时，能够提供调查的依据和手段。可审查性也称为“不可否认性”。

1.1.2 网络安全

1. 网络安全的概念

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性、机密性、可控性和可审查性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会被增加、修改、丢失和泄露等。

2. 网络安全的范畴

根据网络安全概念的定义，可将现代计算机网络安全的范畴分为**通信安全**和**计算机安全**两个

方面。其中，通信安全是对通信系统中所传输、处理和存储的信息的安全性进行保护，确保信息的可用性、完整性、机密性、可控性和可审查性；计算机安全则是对计算机系统中存储和正在处理的信息的安全性进行保护，又包括操作系统的安全和数据库的安全两个方面。

1.1.3　信息安全与网络安全之间的关系

从本质上来讲，网络安全就是通过采取相应的技术和管理制度，确保网络上信息的安全。从广义角度来看，凡是涉及网络上信息的可用性、完整性、机密性、可控性和可审查性的相关技术、理论和制度都是网络安全所要研究的领域。由此可以看出，信息安全和网络安全在宏观范畴内是相同的。但是，从狭义角度来看，信息安全与网络安全之间是有区别的，主要表现在以下几个方面。

- 涉及的对象不同。一是信息安全中的信息所涉及的内容非常广泛，既包括计算机网络中的信息，又包括非计算机网络中的信息。而网络安全所涉及的范围专指计算机网络，所涉及的对象很具体。
- 理解方式不同。从理解方式来看，信息安全较为抽象，而网络安全较为具体。
- 服务方式不同。在服务方式上，网络安全的实现目标就是确保网络中信息的安全，其中信息是服务的主体，而网络则是服务的载体。

由于在“计算机网络安全管理”这门课程中，不再考虑信息的获取和处理等技术细节，而是在网络环境中来讨论信息的安全性，为此，在没有特别说明的情况下，可以将信息安全等同于网络安全。

1.2　计算机网络安全威胁

无论从理论分析还是实际应用来看，目前以 Internet 和 Intranet 为代表的计算机网络存在的安全隐患和安全威胁越来越严重，计算机网络应用中的安全问题越来越被学术界和普通用户普遍关注，计算机网络的安全管理也越来越被重视。

1.2.1　安全威胁及相关概念

所谓**安全威胁**是指人、事、物对某一系统资源的可用性、机密性、完整性及对系统的合法使用所造成的危害。计算机网络中主要的安全威胁为攻击。安全威胁也可以分为故意威胁（如 DDoS 攻击）和偶然威胁（如将邮件发往错误的邮箱）两类。故意威胁又分为被动攻击和主动攻击两类，其中被动攻击只对信息进行监听（如搭线窃听），而不对信息进行任何篡改或破坏；主动攻击对信息进行故意篡改（如修改用户数据）和破坏（如删除重要数据文件）。安全威胁的组成如图 1-1 所示。

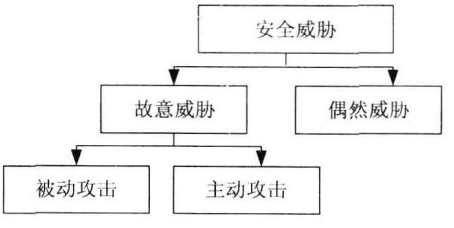


图 1-1　安全威胁的组成

与安全威胁有关的概念还包括脆弱性、风险、防护措施等。其中，**脆弱性**是系统中存在的漏洞，利用该漏洞可以危害系统的安全策略，导致信息的丢失、系统价

值和可用性的降低。需要说明的是，脆弱性的存在本身并不会引起危害，但却是攻击系统或者系统中某个实体的一个条件或条件的一部分。**风险**是对某个已知的、可能引发某种成功攻击的脆弱性的代价的评测。某一系统的脆弱性越高，意味着该系统被成功攻击的概率越大，风险也就越高。在计算机网络安全管理中，对系统安全风险的评估是一项非常有意义的工作。**防护措施**是指保护资源免受威胁所采取的一系列策略和过程。

1.2.2 典型安全威胁介绍

根据实现方式的不同，计算机网络的安全威胁可以分为物理威胁、系统漏洞威胁、身份鉴别威胁、线缆连接威胁和有害程序威胁几类，下面分别进行介绍。

1. 物理威胁

物理安全是一个非常简单的概念，即不允许其他人拿到或看到不属于自己的东西。目前，计算机和网络中所涉及的物理威胁主要有以下几个方面。

- **窃取**。窃取包括窃取设备、信息和服务等。
- **废物搜寻**。废物搜寻是指从已报废的设备（如废弃的硬盘、软盘、光盘、U 盘等介质）中搜寻可利用的信息。
- **间谍行为**。间谍行为是指采取不道德的手段来获取有价值的信息的行为。例如，直接打开别人的计算机复制所需要的数据，或利用间谍软件入侵他人的计算机来窃取信息等。
- **假冒**。假冒是指一个实体假扮成另一个实体后，在网络中从事非法操作的行为。这种行为对网络数据构成了巨大的威胁。

另外，像电磁辐射或线路干扰也属于物理威胁的范围。

2. 系统漏洞威胁

系统漏洞是指系统在方法、管理或技术中存在的缺点（通常称为 bug），而这个缺点可以使系统的安全性降低。目前，系统漏洞主要包括提供商造成的漏洞、开发者造成的漏洞、错误的配置、策略的违背所引发的漏洞等。因此漏洞是方法、管理、技术上存在缺陷所造成的。目前，由系统漏洞所造成的威胁主要表现在以下几个方面。

- **不安全服务**。不安全服务是指绕过设备的安全系统所提供的服务。由于这种服务不在系统的安全管理范围内，所以会对系统的安全造成威胁。其主要有网络蠕虫等。
- **配置和初始化错误**。配置和初始化错误是指在系统启动时，其安全策略没有正确初始化，从而留下了安全漏洞。例如，在木马程序修改了系统的安全配置文件时就会发生此威胁。

3. 身份鉴别威胁

所谓身份鉴别是指对网络访问者的身份（主要有用户名和对应的密码等）真伪进行鉴别。目前，身份鉴别威胁主要包括以下几个方面。

- **口令圈套**。常用的口令圈套是通过一个编译代码模块实现的。该模块是专门针对某一些系统的登录界面和过程而设计的，运行后与系统的真正的登录界面完全相同。该模块一般会插入到正常的登录界面之前，所以用户先后会看到两个完全相同的登录界面。一般情况下，

当用户进行第一次登录时系统会提示登录失败，然后要求重新登录。其实，第一次登录的用户名和密码并未出错（除非真的输入有误），而是一个圈套，它会将正确的登录数据写入到数据文件中。

- **口令破解**。这是最常用的一种通过非法手段获得合法用户名和密码的方法。
- **算法考虑不周**。密码输入过程必须在满足一定的条件下才能正常工作，这个过程通过某些算法来实现。在一些攻击入侵方法中，入侵者采用超长的字符串来破坏密码算法，从而成功地进入系统。
- **编辑口令**。编辑口令需要依靠操作系统的漏洞，如为部门内部的人员建立一个虚设的账户，或修改一个隐含账户的密码，这样任何知道这个账户（指用户名和对应的密码）的人员便可以访问该系统。

4. 线缆连接威胁

线缆连接威胁主要指借助网络传输介质（线缆）对系统造成的威胁，主要包括以下几个方面。

- **窃听**。窃听是指使用专用的工具或设备，直接或间接截获网络上的特定数据包并进行分析，进而获取所需的信息的过程。窃听一般要将窃听设备连接到通信线缆上，通过检测从线缆上发射出来的电磁波来获得所需要的信号。解决该数据被窃听的有效手段是对数据进行加密。
- **拨号进入**。拨号进入是指利用调制解调器等设备，通过拨号方式远程登录并访问网络。当攻击者已经拥有目标网络的用户账户时，就会对网络造成很大的威胁。
- **冒名顶替**。冒名顶替是指通过使用别人的用户账户和密码获得对网络及其数据程序的使用能力。由于别人的用户账户和密码不易获得，所以这种方法实现起来并不容易。

5. 有害程序威胁

计算机和网络中的有害程序是有相对性的，例如有害程序不是出于恶意目的，但却被恶意利用。有害程序造成的威胁主要包括以下几个方面。

- **病毒**。计算机病毒是一个程序，是一段可执行的代码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件在不同的计算机或存储设备之间被复制时，它们就随同文件一起蔓延开来。
- **逻辑炸弹**。逻辑炸弹是嵌入在某个合法程序里面的一段代码，被设置成当满足某个特定条件时就会发作。逻辑炸弹具有病毒的潜伏性。一旦条件成熟导致逻辑炸弹爆发，就会改变或删除数据或文件，引起机器关机或完成某种特定的破坏性操作。
- **特洛伊木马**。特洛伊木马是一个包含在一个合法程序中的非法的程序。该非法程序被用户在不知情的情况下执行。一般的木马都有客户端和服务器端两个执行程序，其中客户端程序是攻击者进行远程控制的程序，而服务器端程序即是木马程序。攻击者如果要通过木马攻击某个系统，其先决条件是要把木马的服务器端程序植入到要控制的计算机中。
- **间谍软件**。间谍软件是一种新的安全威胁，它可能在浏览网页或者安装软件时，在不知情的情况下被安装到计算机上。间谍软件一旦安装就会监视计算机的运行，窃取计算机上的重要信息或者记录计算机的软件、硬件设置，严重危害到计算机中的数据和个人隐私。

以上所介绍的各种典型安全威胁及所包含的内容如图 1-2 所示。

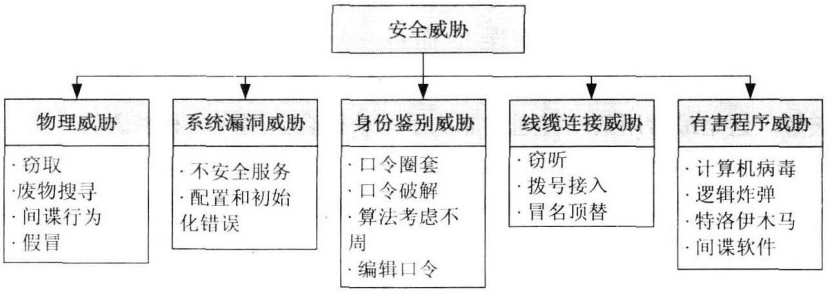


图 1-2　典型安全威胁及内容

1.3 计算机网络安全管理需求分析

安全管理的对象是计算机网络中存在的各类安全威胁，安全威胁的出现必将会导致安全管理技术的产生及安全防范制度的完善。本节综合考虑信息安全三要素中人、管理和技术的特点，分别介绍和分析计算机网络安全管理的主要技术、方法和措施。

1.3.1 物理安全

物理安全是保护计算机网络设备、设施以及其他介质免遭地震、水灾、火灾等环境事故以及人为操作失误及各种计算机犯罪行为导致破坏的过程，它主要包括环境安全、设备安全和介质安全 3 个方面。

保证物理安全可用的技术手段很多，这方面有许多可以依据的标准。例如，GB50173-1993《电子计算机机房设计规范》、GB2887-1989《计算站场地技术条件》、GB9361-1988《计算站场地安全要求》以及其他诸如防辐射防电磁干扰的众多标准等。当然，要保证物理安全，人员素质管理也非常重要。一方面需要制定切实可行的安全管理制度，另一方面需要加强对人员安全意识的教育和培养。

1.3.2 安全隔离

随着新型网络攻击手段的不断出现和一些企事业单位对网络安全要求的不断提高，一个全新的概念——“安全隔离技术”应运而生。在计算机网络安全管理中，隔离是最有效的一种管理方法。**安全隔离**是指在确保把有害攻击隔离在可信网络之外，并保证可信网络内部信息不外泄的前提下，完成不同网络之间信息的安全交换和共享。到目前为止，安全隔离技术已经过了以下几个发展阶段。

1. 完全隔离

采用完全独立的设备、存储和线路来访问不同的网络，做到了完全的物理隔离，但需要多套网络和系统，建设和维护成本较高，一般仅适用于一些专用网络。目前，像公安系统的公安专网、军队系统的军网等专用网络便是采用安全隔离方式来实现的。

2. 硬件卡隔离

通过硬件卡控制独立存储和分时共享设备与线路来实现对不同网络的访问。该技术在 20 世纪 90 年代中期应用较为广泛，许多政府机关和企事业单位为了保护计算机上的数据，多采用硬件卡进行隔离。因为在此期间，多数计算机仍以单机操作为主，当需要上网时，则通过硬件卡切换到另一系统，以加强对系统数据资源的保护。目前，该技术仍然在一定范围内使用，但存在使用不便、可用性差等问题，有些还存在设计上的安全隐患。

3. 数据转播隔离

该技术利用转播系统分时复制文件的途径来实现隔离。该方法切换时间较长，甚至需要手工完成，不仅大大降低了访问速度，更不支持常见的网络应用，只能完成特定的基于文件的数据交换。

4. 空气开关隔离

该技术是通过使用单刀双掷开关，通过内外部网络分时访问临时缓存器来完成数据交换的。该方法支持的网络应用较少，传输速度慢，硬件故障率较高，容易成为网络的瓶颈。

5. 安全通道隔离

该技术通过专用通信硬件和专有交换协议等安全机制，来实现网络间的隔离和数据交换，不仅解决了以往隔离技术存在的问题，并且在网络隔离的同时实现高效的内外网数据的安全交换，它透明地支持多种网络应用，成为当前隔离技术的发展方向。

1.3.3 访问控制

访问是使信息在不同设备之间流动的一种交互方式。访问控制决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源。适当的访问控制能够阻止未经允许的用户有意或无意地获取数据。访问控制的手段包括用户识别代码、口令、登录控制、资源授权（例如用户配置文件、资源配置文件和控制列表）、授权核查、日志和审计。

访问控制主要是通过防火墙、交换机或路由器的使用来实现的。防火墙是实现网络安全最基本、最经济、最有效的安全措施之一，通过制定严格的安全策略，防火墙可以对内外网络或内部网络不同信任域之间进行隔离，使所有经过防火墙的网络通信接受设定的访问控制。此外，通过防火墙提供的 NAT 功能，也可以起到网段隔离的作用（主要是局域网与广域网之间）。

另外，随着微电子技术的发展，交换机和路由器的数据处理和存储能力得到了提高。为此，目前许多设备已集成了原来多个设备所提供的功能。例如，现在的绝大多数防火墙已提供了原来路由器才具有的 ACL（Access Control List，访问控制列表）、NAT（Network Address Translation，网络地址转换）等功能。同时，在一些路由器上也提供了原本由防火墙才具有的访问控制功能。

1.3.4 加密通道

加密通道是利用数据加密技术，对网络信道（通道）中传输的各类信息进行加密处理，以确

保信息的安全性。给网络通信提供加密通道，也是普遍使用的一项安全技术。随着技术的发展，目前加密通道可以建立在数据链路层、网络层、传输层甚至是应用层。

1. 数据链路层加密

数据链路层加密可以使用专用的链路加密设备，其加密机制是点对点的加、解密。在通信链路两端，都应该配置链路加密设备，通过位于两端加密设备的协商配合来实现传输数据的加密和解密过程。

近年来，VPN（Virtual Private Network，虚拟专用网）技术得到了快速发展，并得到了广泛应用。其中，位于数据链路层的 VPN 可以实现链路层加密。目前这样的 VPN 技术主要有 3 种：L2F（Layer 2 Forwarding，第二层转发）、PPTP（Point-to-Point Protocol，点到点隧道协议）、L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）。在进行网络通信时，链路层 VPN 首先会将各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中，这种双层封装形成的数据包依靠链路层协议来传输，最终起到点对点加密通信的效果。

2. 网络层加密

网络层加密通过网络层 VPN 技术来实现，最典型的就是 IPSec（Internet Protocol Security）。现在许多提供 VPN 功能的防火墙设备中都支持 IPSec。

网络层 VPN 也需要对原始数据包进行多层封装，但最终形成的数据包是依靠第三层协议（一般是 IP 分组）进行传输的，本质上是端到端的数据通信。

3. 传输层加密

传输层加密通道可以采用 SSL（Secure Socket Layer，安全套接层）和 TLS（Transport Layer Security，传输层安全）技术。SSL 是应用比较广泛的一种传输层安全协议，它介于应用层协议和 TCP/IP 之间，为传输层提供安全性保证。

TLS 是 IETF（The Internet Engineering Task Force，互联网工程任务组）的标准，它建立在 SSL 3.0 基础之上，只是所支持的加密算法不同，这两种加密协议不能互通。

此外，还有一些其他的传输层安全技术，例如 SSH、SOCKS 等。

4. 应用层加密

应用层加密与具体的应用类型结合紧密，典型的有 SHTTP、SMIME 等。（SHTTP）安全超文本传输协议是面向消息的安全通信协议，可以为单个 Web 主页定义加密安全措施。而 SMIME（Secure Multipurpose Internet Mail Extensions，加密多用途 Internet 邮件扩展）则是一种电子邮件加密和数字签名技术。应用层加密还包括利用各种加密算法开发的加密程序。

1.3.5 入侵检测

入侵检测（Intrusion Detection）技术是近年来发展迅速的一种安全技术。我们知道，防火墙是最早被采用的访问控制措施，但防火墙“防外不防内”的先天弱点，加上防火墙对实时入侵行为识别及反应能力的限制，使得入侵检测技术成为整体安全解决方案中必不可少的一部分。