21世纪 高等学校信息安全专业规划教材

网络安全教程与实践（第2版）

李启南 王铁君 编著

清华大学出版社

21世纪高等学校信息安全专业规划教材

网络安全教程与实践

（第2版）

李启南　王铁君　编著

清华大学出版社
北京

内 容 简 介

本书以培养注重实践、攻防兼备的高级网络安全人才为教学目标，系统阐述了防火墙、IPS、VPN、IPSec/SSL 网关、蜜罐五类常用网络安全设备的工作原理、配置方法，培养学生保障网络运行安全的实践能力，筑牢网络安全防御体系；探讨了 SQL 注入攻击、DDoS 攻击原理，培养学生在网络攻防对抗环境下使用网络安全漏洞扫描工具及时发现安全漏洞、准确处理网络攻击事件的实践能力；讲解了密码学原理在保证网络银行支付安全方面的具体应用，介绍了 SM2、SM3、SM4 国密算法，推广使用国产密码；研究了隐私保护、数字版权保护原理，为维护开发网络应用安全系统奠定理论基础；普及了《网络安全法》，帮助学生树立正确的网络安全观。

本书适合作为信息安全类专业入门教材和网络安全相关专业教材。

图书在版编目(CIP)数据

网络安全教程与实践/李启南，王铁君编著. —2 版. —北京：清华大学出版社，2018
(21 世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-49257-3

Ⅰ. ①网…　Ⅱ. ①李… ②王…　Ⅲ. ①计算机网络－安全技术－高等学校－教材
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 002484 号

责任编辑：郑寅堃　李　晔
封面设计：杨　兮
责任校对：梁　毅
责任印制：杨　艳

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 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：22　　**字　　数**：531 千字
版　　次：2012 年 9 月第 1 版　2018 年 7 月第 2 版　　**印　　次**：2018 年 7 月第1次印刷
印　　数：1～1500
定　　价：59.00 元

产品编号：076335-01

第 2 版前言

在本书第 1 版出版至今的 5 年多时间里，网络安全上升为国家安全的战略高度，《网络安全法》正式实施，网络安全一级学科正式设置并确定为新工科专业。这些重大举措推动了高校信息安全专业建设，促进了网络安全教学内容和方法的改革，迫切需要更新教学内容；另一方面，在教学实践中广大师生提出了很多中肯的建议，促使我们对教材相关章节的安排及内容取舍有了新的认识，也希望通过新版教材得以体现。

第 2 版继承了第 1 版的优点，体现精讲多练、教为主导、学为主体的原则，由浅入深、循序渐进地介绍网络安全基本原理、基本方法、基本技能，注重学生理论水平和实践技能的同步提高。既有严密、抽象的密码学原理讲解，也有具体、直观的网络安全设备(防火墙、VPN、IPS)配置操作、图像数字水印编程实现等实践内容，能够很好地满足网络安全课程理论教学和实践教学的需求。

网络安全教学的发展趋势是培养攻防兼备的人才，新工科教育要求教学更加强调工程实践能力和创新能力的培养，因此本书第 2 版新增了基于 IP 地址和端口的防火墙安全策略配置、VPN 单臂旁挂于防火墙配置、Zenamp 网络安全扫描、冰河木马攻击与防范、DES 算法和 RSA 算法性能测试、凯撒密码解密进阶、图像数字水印、基于同态加密的图像编辑 8 个实验教学内容，助力师生主动、积极开展实验教学，提倡自主创新拓展实验内容。

第 2 版将第 1 版的 13 章精简为 9 章，删除了第 1 版的第 2 章、第 9 章、第 10 章、第 11 章。具体修订内容如下：

第 1 章网络安全概论，按照 2015 年教育部“网络安全一级学科论证工作组”制定的知识体系重写了本章，新增《网络安全法》解读和 P2DR2 网络安全模型。

第 2 章密码学基础，新增椭圆曲线密码、国产密码、网络银行安全支付相关章节，对密码算法增加了例题讲解。

第 3 章网络攻防技术，由第 1 版的第 3 章、第 4 章、第 5 章内容合并而成。

第 4 章防火墙与入侵防御，新增防火墙入侵防御、内容过滤等网络安全配置实例介绍，培养学生配置网络安全设备，保证网络安全运行的实践能力。

第 5 章 IP 安全与 Web 安全，新增 SQL 注入攻击、VPN 安全性配置相关章节，在网络攻防对抗中应用所学理论知识保证网络安全。

第 6 章网络安全方案设计与评估、第 7 章计算机病毒与特洛伊木马未做内容修改。

第 8 章数字版权保护，新增章节，应用数字水印原理实现数字图像、数据库版权保

护,应用抗合谋数字指纹ECFF实现数字资源版权溯源追踪,为打击数字资源盗版提供技术支持。

第9章隐私保护,新增章节,介绍隐私保护及其度量方法;根据数据生命周期隐私保护模型具体讲解数据发布、数据存储、数据挖掘、数据应用4个阶段使用的隐私保护技术;应用同态加密解密技术实现密文图像编辑,保证云计算环境下用户数据的安全性。

本书第4章至第7章由王铁君编写,其余章节由李启南编写,并进行统稿。

兰州交通大学电子与信息工程学院吴辰文教授对本书进行了总体规划与设计,提出了再版方案,对内容的安排及实验与习题等方面给出了具体的指导建议,在此表示由衷的感谢。

清华大学出版社郑寅堃编辑认真、仔细地多次阅读了本书初稿,详细指出了存在的诸多错误之处,为本书顺利出版付出了巨大心血,在此表示衷心的感谢!

本书得到兰州交通大学实验教学改革项目(项目号:2018016)资助。

本书参考理论学时为32学时,实验学时为16学时;或者理论学时为24学时,讲授前6章后选择第7章、第8章、第9章中的一章讲授;实验学时为8学时,任意选做4个实验。

作为教学交流,我们整理了PPT课件以及习题的参考答案,请各位教师在清华大学出版社网站(http://www.tup.com.cn)免费下载参考。

由于作者水平有限,书中难免会有不当之处,敬请读者提出宝贵意见。

编 者

2018年1月

图书资源支持

感谢您一直以来对清华版图书的支持和爱护。为了配合本书的使用，本书提供配套的资源，有需求的读者请扫描下方的“书圈”微信公众号二维码，在图书专区下载，也可以拨打电话或发送电子邮件咨询。

如果您在使用本书的过程中遇到了什么问题，或者有相关图书出版计划，也请您发邮件告诉我们，以便我们更好地为您服务。

我们的联系方式：

地　　址：北京海淀区双清路学研大厦 A 座 707

邮　　编：100084

电　　话：010－62770175－4604

资源下载：http://www.tup.com.cn

电子邮件：weijj@tup.tsinghua.edu.cn

QQ：883604(请写明您的单位和姓名)

资源下载、样书申请

书圈

用微信扫一扫右边的二维码，即可关注清华大学出版社公众号“书圈”。

目　录

第 1 章　网络安全概论

本章学习要求

- 掌握网络安全定义、网络安全目标、网络安全教学内容；
- 掌握没有网络安全就没有国家安全的观点，认识网络安全的重要性；
- 掌握 DMZ 和个人隐私概念、常见的五类网络安全设备功能；
- 掌握 P2DR2 网络安全动态模型、网络安全评价标准；
- 掌握正确的网络安全观、《网络安全法》的主要内容。

1.1　网络安全定义

在信息革命的演进过程中，传统互联网、移动互联网、物联网快速发展起来，成为继陆、海、空、天之后的第五大空间，称之为网络空间(Cyberspace)。

网络空间是通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间，在信息时代是社会有机运行的指挥系统。在网络空间里不仅包括通过网络互联而成的各种计算系统(包括各种智能终端)、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他空间不同的特点是，网络空间没有明确的、固定的边界，也没有集中的控制权威。

在网络空间里，信息安全问题的内涵和外延也在不断放大，最终扩大到了整个网络空间。从此，信息安全的概念被网络安全所涵盖。

网络信息泄露关乎成千上万人的敏感信息和个人隐私，网络攻击和黑色产业威胁经济健康发展，网络舆论恶意炒作影响社会稳定，网络战争和网络间谍威胁国家安全。同时，由于网络核心技术、优势技术掌握在少数国家手里，网络安全问题极易被他人恶意传播、利用、控制和绑架，成为攻击、颠覆他国政权的手段、途径，网络安全已成为全世界关注的焦点和热点问题。

1. 网络安全定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络能够提供不中断服务。

网络安全的具体含义因观察角度的不同而不同：

(1) 从用户(个人、企业等)的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性方面的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。

(2) 从网络运行管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

(3) 对安全保密部门来说,他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵,避免机要信息泄露,避免对社会产生危害,对国家造成巨大损失。

(4) 从社会教育和意识形态角度来讲,网络上不健康的内容会对社会的稳定和人类的发展造成阻碍,必须对其进行控制。

因此我们认为网络安全既要保证构成网络系统的软件、硬件资源具有可用性(网络运行安全),也要保护网络系统存储、使用的信息具有机密性、完整性、可用性、真实性和可控性(网络信息安全),是网络信息安全和网络运行安全的有机结合,网络运行安全是网络信息安全的前提和基础,网络信息安全是网络运行安全的具体表现和目的。

理解网络安全的关键是必须认识到现实网络中存在各种各样的敌手(攻击者),他们通过多种技术手段或者破坏网络设施,阻止网络运行安全,危害国家安全;或者非法获取网络信息,追求个人利益最大化,损害全社会的网络信息安全。

网络安全的内涵和外延是与时俱进的。在计算机网络产生之前,网络安全主要是指通信安全,重点关注的是信息加密(信息的保密性)。计算机网络产生后,网络安全中的网络主要是指计算机网络,网络安全是指保护计算机网络不因偶然或恶意因素的影响而遭到破坏、更改、泄露,系统连续、可靠、正常地运行,网络服务不中断。

随着"三网融合"的发展,网络安全领域也从计算机网络延伸到物联网和有线电视网络。近几年来,网络安全进一步向物理世界和虚拟世界延伸,包括与国家基础设施密切相关的工业控制网络或系统(如电力网络、交通控制网络、城市供水网络、石油天然气网络和核电控制系统等)、虚拟的社交网络等,网络安全上升到了网络空间安全。

网络空间安全(Cyberspace Security,简称 Cyber Security)研究网络空间中的安全威胁和防护问题,即在有敌手(adversary)的对抗环境下,研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施以及网络和系统本身的威胁和防护机制。

网络空间安全不仅仅包括传统信息安全所研究的信息的保密性、完整性和可用性,同时还包括构成网络空间基础设施的安全和可信。

这里,进一步明确一下信息安全、网络安全、网络空间安全概念之异同,三者均属于非传统安全,均聚焦于信息安全问题。信息安全使用范围比较广,可以指线下和线上的信息安全,既可以指传统的信息系统安全,也可以指网络安全或网络空间安全,但无法完全替代网络安全与网络空间安全的内涵;网络安全、网络空间安全的核心都是信息安全问题,只是出发点和侧重点有所区别。网络安全可以指信息安全或网络空间安全,但侧重点是线上安全和网络社会安全;网络空间安全可以指信息安全或网络空间安全,但侧重点是与陆、海、空、太空并列的空间概念。

网络安全、网络空间安全、信息安全三者相比较,前两者反映的信息安全更立体、更宽域,有更多层次,也更多样,更能体现网络和空间的特征,并与其他安全领域有更多的渗透与融合。

总之,不同名称的内涵和外延是不同的,侧重点也不同。我们既要看到不同名称间的差异,在不同场合使用不同名称;也应该看到其核心内容是相同的,关注共同内容的学习。

2. 网络安全教学内容

教育部"网络安全一级学科论证工作组"提出的教学内容包括网络空间安全基础理论、密码学基础知识、系统安全理论与技术、网络安全理论与技术、应用安全技术知识5个部分,

如图 1-1 所示。

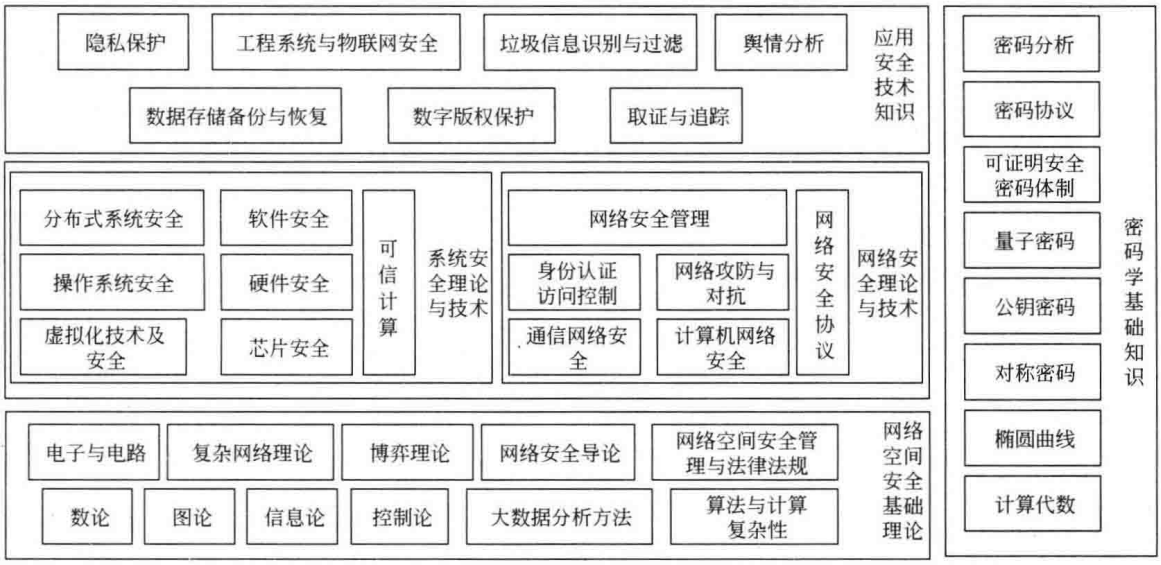

图 1-1　网络安全教学内容

(1) 网络空间安全基础理论是支撑整个学科的基础，为其他方向的研究提供理论、架构和方法学指导。

(2) 密码学基础主要研究在有敌手的环境下，如何实现计算、通信和网络的信息编码和分析，为网络、系统及应用安全提供密码机制。

(3) 系统安全理论与技术主要研究网络环境下计算单元(端系统)的安全，是网络空间安全的基础单元。

(4) 网络安全理论与技术保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全。

(5) 应用安全技术是指网络空间中建立在因特网之上的应用和服务系统，如国家重要行业应用、社交网络等。应用安全研究各种安全机制在一个复杂系统中的综合应用，保证网络空间中大型应用系统的安全，也是安全机制在互联网应用或服务领域中的综合应用。

本书第 2 章讲解密码学基础知识，第 3 章～第 6 章讲解网络安全理论与技术，第 7 章讲解系统安全理论与技术，第 8 章、第 9 章分别讲解应用安全技术中的数字版权保护、隐私保护。

1.1.1　网络信息安全

网络信息安全是对信息保密性、完整性、可用性的保护，具体指在有敌手的对抗环境下，研究信息在产生、传输、存储、处理各个环节中所面临的威胁和防御措施。

机密性、完整性、可用性(Confidentiality，Integrity，Availability，CIA)称为信息安全的三要素。

机密性：通过各种加密技术，保证信息不泄露给非授权用户、实体或过程或被其利用的特性。目的是防止对信息进行未授权的“读”。

完整性：保证信息未经授权不能进行改变的特性。即信息在存储或传输过程中保持不

被修改、不被破坏和丢失的特性,保证接收到的信息和发出的信息是相同的。目的是防止或至少是检测出未授权的"写"(对数据的改变)。

可用性:可被授权实体访问并按需求使用的特性。即当需要时保证合法用户对信息或资源的使用不会受到影响或被不正当地拒绝。例如网络环境下拒绝服务(DoS)、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

理想状态下,网络系统抽象为如图1-2所示的AB模型,Alice和Bob相互通信。本书约定Alice是网上银行Bank的合法客户。如何保证网上银行支付安全是网络安全应用的范例,也是本书学习的重点。

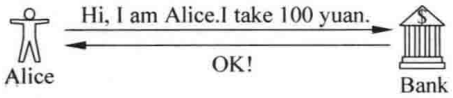

图1-2 AB模型

由于信息在一个开放的网络(大气、通信网络、计算机网络、物联网)中传输,通过网络获取信息是简单可行的,通信具有公开性,所以真实的通信系统中是存在敌手(攻击者)的。有敌手的AB系统如图1-3所示,攻击者Trudy可以侦听、截取通信信息,读懂通信内容(被动攻击),也可以删除、增加报文、重放报文、篡改报文(主动攻击)。例如Trudy可以篡改交易金额,可以在Alice关机后重放通信内容。

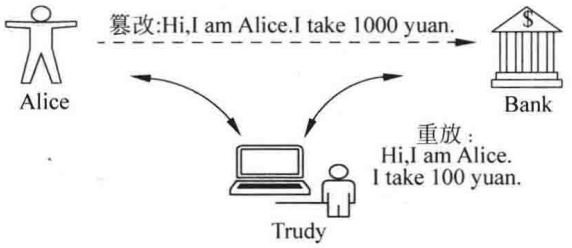

图1-3 有敌手的AB模型

对图1-3而言,信息的机密性表现为Alice不想让Trudy知道她存款账户有多少钱;完整性表现为Bank需要防止Trudy擅自增加自己账户的余额,或者改变Alice账户里的余额。

机密性和完整性不是同一个概念。在图1-4中,Trudy不能读懂通信的内容(机密性),但可以修改这些不可读的数据(破坏完整性)。

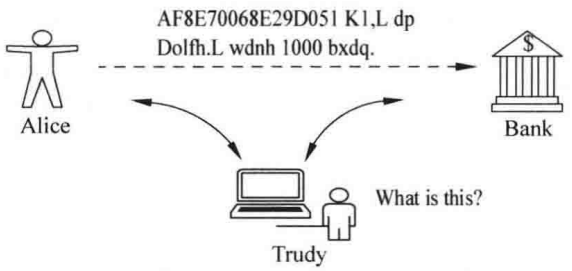

图1-4 加密AB模型

此外，Trudy 对 Bank 发动 DoS 攻击，会导致 Alice 无法获得服务，转而从其他银行获得服务，从而破坏 Bank 的可用性。

显然，Trudy 通过延时重放就可假冒 Alice，Bank 如何知道这个登录的“Alice”是真实的 Alice，而不是 Trudy 假冒的？这是身份认证需要解决的问题。

有敌手的对抗环境，我们需要解决以下问题：

(1) 如何防止 Trudy 窃听信息？使用信息加密技术解决。

(2) 信息在传输中有没有改变？使用数据摘要技术解决。

(3) Alice is Alice? Bank 如何确认 Alice 不是 Trudy 假冒的？使用身份认证技术解决。

(4) 如何防止重放？使用时间戳技术解决。

1.1.2　网络运行安全

网络运行安全是指网络系统的硬件、软件不因偶然的或者恶意的原因而遭受到破坏、更改，系统连续可靠正常地运行，网络服务不中断。

Internet 的开放性使得我们不可能保证整个 Internet 的安全性，因此需要将网络划分为安全区(Trust)、不安全区(Untrust)、隔离区(DeMilitarized Zone，DMZ)3 个不同等级的安全区域。

通常使用防火墙(Firewall)将网络划分为安全区和不安全区两个区域，如图 1-5 所示，安全区也称内网，多为局域网或 Intranet；不安全区特指 Internet。

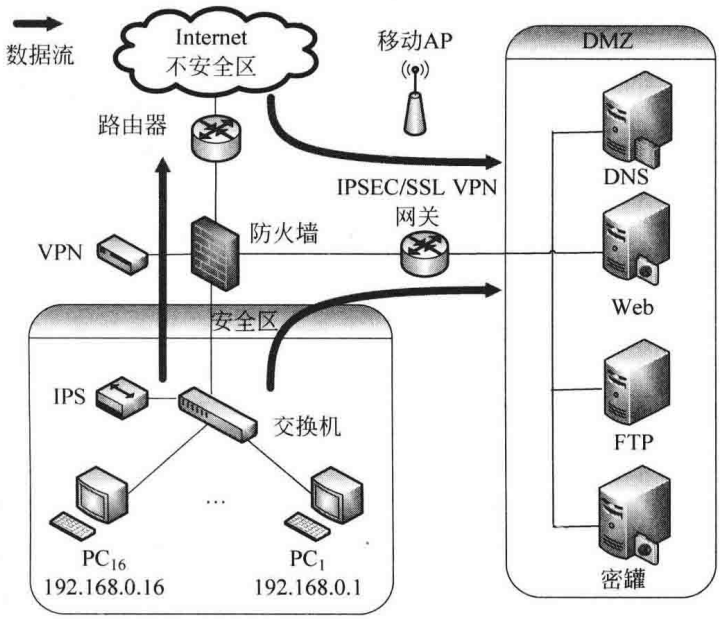

图 1-5　网络安全设备应用示意图

防火墙是由计算机软件、硬件设备组合而成，在一个安全区和不安全区之间执行访问控制策略的一个或一组系统。个人计算机使用软件防火墙，但为了满足网络实时通信的要求，网络都使用硬件防火墙，可以理解为是一个专门执行访问策略的专用计算机。

硬件防火墙通常具有多个端口分别连接多个不同网络，如图 1-5 中防火墙具有 3 个端

口。不同网络的数据包流入防火墙后,防火墙根据网络管理员设定的过滤规则对流经的每个数据包分析包头,判断其是否匹配过滤规则,匹配则放行,否则丢弃该数据包。过滤规则示例见表1-1。

表1-1 防火墙过滤规则

规则序号	包的方向	源地址	目的地址	处理方法
1	出	192.168.1.1/8	61.135.169.121	运行通过
2	入	61.135.169.121	192.168.1.1/8	拒绝通过

防火墙默认情况下设置为阻止外网对内网进行访问,例如为图1-5中的防火墙设置表1-1的过滤规则后,位于外网的百度服务器(IP地址为61.135.169.121)就不能向内网发送信息(访问内网),但内网用户(IP地址为192.168.1.1/8)仍然能访问百度服务器。

如果我们把服务器放在内网就会导致外网无法访问该服务器,所以需要定义出一个DMZ区域:Trust和Untrust都可以访问DMZ区域,该区域既不是绝对的安全,也不是绝对的不安全,这就是设计DMZ区域的核心思想。

一个划分有DMZ的网络必须遵守6条访问控制策略,明确各个网络之间的访问关系。

(1) 内网可以访问外网。

(2) 内网可以访问DMZ。

(3) 外网不能访问内网。

(4) 外网可以访问DMZ。

(5) DMZ不能访问内网。

(6) DMZ不能访问外网。

DMZ是为了解决安装防火墙后外部网络(Untrust)不能访问内部网络(Trust)服务器的问题而设立在非安全区与安全区之间的一个缓冲区,这个缓冲区位于内部网络和外部网络之间的小网络区域内,在这个小网络区域内可以放置一些必须公开的服务器设施,如企业Web服务器、FTP服务器和论坛等。另一方面,通过这样一个DMZ区域,更加有效地保护了内部网络,因为这种网络部署,比起一般的防火墙方案,对攻击者来说又多了一道关卡。

第一代网络运行安全技术,以保护为目的,划分明确的网络边界,利用各种保护和隔离手段,如用户鉴别和授权、访问和控制、多级安全、权限管理和信息加解密等,试图在网络边界上阻止非法入侵,从而达到确保信息安全的目的。这些技术解决了许多安全问题,但并不是在所有情况下都能清楚地划分并控制边界,保护措施也并不是在所有情况下都有效。因此,第一代网络运行安全技术并不能全面保护网络运行安全,于是出现了第二代网络运行安全技术。

第二代网络运行安全技术,以保障为目的,以检测技术为核心,以恢复技术为后盾,融合了保护、检测、响应和恢复4大类技术,使用如图1-5所示的防火墙(Firewall)、入侵检测系统(Intrusion Protect System,IPS)、虚拟专用网(Virtual Private Network,VPN)等常用网络安全设备实现,它们的功能如表1-2所示。

第二代网络运行安全技术也称为信息保障技术,目前已经得到了广泛应用。信息保障技术的基本假设是:如果挡不住敌人,至少要能发现敌人或敌人的破坏。例如,能够发现系