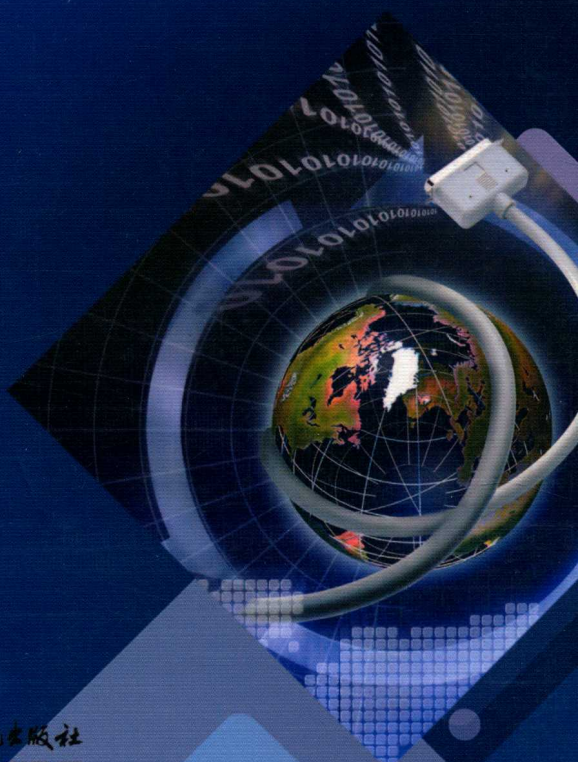
“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定）
高等职业教育精品示范教材 信息安全系列

网络安全产品调试与部署

主　编　路　亚　李贺华
副主编　柯宗贵　石龙兴　冯德万

本书特色：

- 以就业为导向，以能力为本位
- 项目案例引导，任务需求驱动
- 生活实例链接知识点，案例增加趣味性
- 通用教学内容与特殊教学内容协调配置



中国水利水电出版社
www.waterpub.com.cn

“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定）

高等职业教育精品示范教材（信息安全系列）

网络安全产品调试与部署

主　编　路　亚　李贺华

副主编　柯宗贵　石龙兴　冯德万

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书专注于网络安全产品的调试与部署，内容涵盖了防火墙、入侵检测、VPN、网络隔离、安全审计与上网行为管理、防病毒网关、网络存储、数据备份等常用的网络安全产品，详细介绍了其工作原理和配置方法，并结合工程案例进行应用部署。

本书共分 8 章，分别针对八类网络安全产品进行讲解，各章内容自成体系又相互关联，加强实践环节，以提高学习者的动手操作能力。

本书既可作为高职高专及应用型本科学校的信息安全技术专业学生的教材，也可作为企事业单位网络信息系统管理人员的技术参考手册、网络安全技术服务企业的培训教材。

本书配有电子教案，读者可以从中国水利水电出版社网站和万水书苑免费下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com。

图书在版编目（CIP）数据

网络安全产品调试与部署 / 路亚，李贺华主编. -- 北京 : 中国水利水电出版社，2014.9
“十二五”职业教育国家规划教材. 高等职业教育精品示范教材. 信息安全系列
ISBN 978-7-5170-2505-4

Ⅰ. ①网… Ⅱ. ①路… ②李… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2014)第215008号

策划编辑：祝智敏　责任编辑：张玉玲　加工编辑：孙　丹　封面设计：李　佳

书　名	“十二五”职业教育国家规划教材（经全国职业教育教材审定委员会审定） 高等职业教育精品示范教材（信息安全系列） **网络安全产品调试与部署**
作　者	主　编　路　亚　李贺华 副主编　柯宗贵　石龙兴　冯德万
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市铭浩彩色印装有限公司
规　格	184mm×240mm　16 开本　16.25 印张　356 千字
版　次	2014 年 9 月第 1 版　2014 年 9 月第 1 次印刷
印　数	0001—4000 册
定　价	35.00 元

高等职业教育精品示范教材（信息安全系列）

丛书编委会

序　言

随着信息技术和社会经济的快速发展，信息和信息系统成为现代社会极为重要的基础性资源。信息技术给人们的生产、生活带来巨大便利的同时，计算机病毒、黑客攻击等信息安全事故层出不穷，社会对于高素质技能型计算机网络技术和信息安全人才的需求日益旺盛。党的十八大明确指出“高度关注海洋、太空、网络空间安全”，信息安全被提到前所未有的高度。加快建设国家信息安全保障体系，确保我国的信息安全，已经上升为我国的国家战略。

发展我国信息安全技术与产业，对确保我国信息安全有着极为重要的意义。信息安全领域的快速发展，亟需大量的高素质人才。但与之不相匹配的是，在高等职业教育层次信息安全技术专业的教学中，还更多地存在着沿用本科专业教学模式和教材的现象，对于学生的职业能力和职业素养缺乏有针对性的培养。因此，在现代职业教育体系的建立过程中，培养大量的技术技能型信息安全专业人才成为我国高等职业教育领域的重要任务。

信息安全是计算机、通信、数学、物理、法律、管理等学科的交叉学科，涉及计算机、通信、网络安全、电子商务、电子政务、金融等众多领域的知识和技能。因此，探索信息安全专业的培养模式、课程设置和教学内容就成为信息安全人才培养的首要问题。高等职业教育信息安全系列丛书编委会的众多专家、一线教师和企业技术人员，依据最新的专业教学目录和教学标准、结合就业实际需求，组织了以就业为导向的高等职业教育精品示范教材（信息安全系列）的编写工作。该系列教材由《网络安全产品调试与部署》、《网络安全系统集成》、《Web开发与安全防范》、《数字身份认证技术》、《计算机取证与司法鉴定》、《操作系统安全（Linux）》、《网络安全攻防技术实训》、《大型数据库应用与安全》、《信息安全工程与管理》、《信息安全法规与标准》、《信息安全等级保护与风险评估》等组成，在紧跟当代信息安全研究发展的同时，全面、系统、科学地培养信息安全类技术技能型人才。

本系列教材在组织规划的过程中，遵循以下几个基本原则：

（1）体现就业为导向、产学结合的发展道路。学科和专业同步加强，按企业需要、按岗位需求来对接培养内容。既能反映信息安全学科的发展趋势，又能结合信息安全专业教育的改革，且及时反映教学内容和教学体系的调整更新。

（2）采用项目驱动、案例引导的编写模式。打破传统的以学科体系设置课程体系、以知识点为核心的框架，更多地考虑学生所学知识与行业需求及相关岗位、岗位群的需求相一致，坚持“工作流程化”、“任务驱动式”，突出“走向职业化”的特点，努力培养学生的职业素养、职业能力，实现教学内容与实际工作的高仿真对接，真正以培养技术技能型人才为核心。

（3）专家和教师共建团队，优化编写队伍。由来自信息安全领域的行业专家、院校教师、企业技术人员组成编写队伍，跨区域、跨学校进行交叉研究、协调推进，把握行业发展和创新

教材发展方向，融入信息安全专业的课程设置与教材内容。

（4）开发课程教学资源，推进专业信息化建设。从充分关注人才培养目标、专业结构布局等入手，开发补充性、更新性和延伸性教辅资料，开发网络课程、虚拟仿真实训平台、工作过程模拟软件、通用主题素材库以及名师讲义等多种形式的数字化教学资源，建立动态、共享的课程教材信息化资源库，服务于系统培养技术技能型人才。

信息安全类教材建设是提高信息安全专业技术技能型人才培养质量的关键环节，是深化职业教育教学改革的有效途径。为了促进现代职业教育体系的建设，使教材建设全面对接教学改革、行业需求，更好地服务区域经济和社会发展，我们殷切希望各位职教专家和老师提出建议，并加入到我们的编写队伍中来，共同打造信息安全领域的系列精品教材！

丛书编委会

2014 年 6 月

前　言

近年来，我国互联网用户数量逐年增长，中国互联网络信息中心（CNNIC）发布的第33次《中国互联网络发展状况统计报告》显示，截至2013年12月，中国网民规模达6.18亿，互联网普及率为45.8%，全国企业使用计算机办公的比例为93.1%，使用互联网的比例为83.2%。网络的普及带来网络安全问题的日益严峻，2012年，CNCERT/CC抽样监测发现，境外约有7.3万个木马或僵尸网络控制服务器，进而控制我国境内1419.7万余台主机，同时拒绝服务攻击、网络钓鱼、网站被植入后门、篡改网站数据、病毒、蠕虫等形式的攻击也很频繁并呈增长态势。计算机网络用户在被迫提高防范意识，对网络安全产品提出了更高的需求。

防范网络攻击，或者在网络攻击发生时降低危害，需要构筑安全防御体系，这个体系主要包含防火墙、入侵检测、防病毒网关、VPN、网络隔离、数据备份、安全审计等网络安全产品。目前，这些网络安全产品已经成为政府、银行、学校、企业等实体实施办公自动化、电子商务、电子政务等信息化建设的基本安全保障，市场对网络安全产品的需求越来越大。相应地，安全设备生产厂商、信息系统集成商、信息系统运营商、安全服务提供商以及各单位的网络管理部门，对提供网络安全产品技术支持和技术服务的专业人员的需求也与日俱增。

网络安全产品的调试配置与应用部署能力，成为高职信息安全技术专业学生必备的专业技能。本书专注于网络安全产品的调试与部署，全书共8章，各章内容自成体系又相互关联，加强实践环节，期望能提高学习者的动手操作能力。

重庆电子工程职业学院信息安全技术专业是国家示范院校建设中，唯一一个信息安全类国家级重点建设专业，蓝盾信息安全技术股份有限公司是全国知名的信息安全产品生产商。本书是二者精诚合作的成果，将专业教师的教学经验和企业工程师的工程项目经验相结合，采用“真实项目引导，工作任务驱动”的形式组织教材内容，使其更适合高等职业教育需求。书中的实训部分使用了蓝盾的一些产品和Snort等开源软件，希望能够起到以点带面的示范作用，也希望读者能举一反三，提高对安全产品的调试、部署能力。

本书既可作为高职高专及应用型本科的信息安全技术专业学生的教材，也可以作为企事业单位网络信息系统管理人员的技术参考手册、网络安全技术服务企业的培训教材。

本书由重庆电子工程职业学院路亚和李贺华任主编，蓝盾信息安全技术股份有限公司柯宗贵、石龙兴和重庆安全技术职业学院冯德万任副主编，蓝盾信息安全技术股份有限公司梁琦、代雪玲、赖小卿及重庆电子工程职业学院梁雪梅也参与了编写。本书第1～3章由路亚编写，第4章由冯德万编写，第5章由李贺华编写，第6章由重庆安全技术职业学院张永宏编写，第7～8章由蓝盾信息安全技术股份有限公司技术人员编写。此外，蓝盾信息安全技术股份有限公司工程师颜星、龙志强、彭剑刚、何超提供了部分实训材料，并参与了部分编写工作，总工韦校春和重庆电子工程职业学院计算机学院武春岭副院长负责审稿工作。

本书在编写过程中得到了重庆电子工程职业学院领导和同事的支持，在此表示感谢。

由于编者水平有限，书中疏漏之处在所难免，敬请各位读者批评指正。

编者

2014年4月

目　录

1 防火墙产品调试与部署

知识目标

- 了解防火墙的定义和作用
- 掌握防火墙的工作原理及性能指标
- 掌握防火墙的架构和应用
- 理解防火墙的局限性

技能目标

- 能够根据项目进行方案设计
- 能够对防火墙进行部署、配置
- 能够对防火墙进行安全策略应用与测试

项目引导

项目背景

（某）教育局承担着国家的教育方针、政策的执行，研究并制定地方性教育方针、政策，规划、组织、实施教学设施的建设，以及指导实施全区教育信息化建设等任务，在该区的教育信息化建设中起着极为重要的枢纽作用。

各级学校作为教育局的下属单位，承担着人才培养的任务，在网络化、信息化浪潮中，

陆续连接上互联网。然而在使用网络的过程中，服务器经常受到各种攻击，严重威胁着校园网的安全。加上网络信息的良莠不齐，学生对网络内容的真假难辨，很容易让学生误入歧途。因此，学校的网络安全管理和上网行为管理成为了新的挑战。

该教育城域现有网络的整体结构遵循三级分层管理的体系结构。全区中学、小学和幼儿园将分批逐步接入该教育局网络信息中心，再通过统一出口上连到市教科网，共计 98 所学校通过光纤与教育局网络信息中心连接。该中心提供的服务主要包括 WWW 服务、FTP 服务、VOD 点播、数据库应用、防病毒服务等。城域网采用环型拓扑结构，ERRP 以太网的组网技术，实现信息中心与下属各学校单位间的互联互通；采用 VLAN 技术与 ACL 和启用 OSPF 协议对网络进行有效的分隔和提高效率。同时实现各单位拥有正式的 CERNET 地址，便于各单位进行信息发布。其现有网络拓扑图如图 1-1 所示。

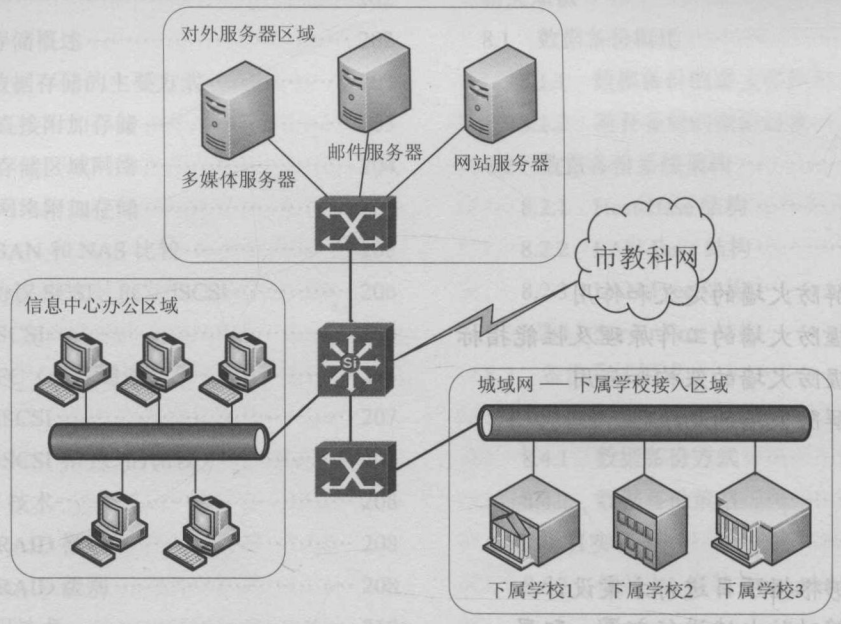


图 1-1　整改前网络拓扑图

需求分析

分析现有网络环境，对网络现状进行评估，结合各学校网络环境，有效计划、设计、优化网络安全体系，以保护网络，防止系统被入侵和攻击，并提供专业的安全服务，建立信息系统安全运行维护体系，保障教育局城域网的安全运行。

企业网络安全工程师针对此项目的用户背景和需求，通过多次交流和沟通，结合单位的网络架构，分别从技术和管理的安全角度进行了风险分析，整体评估了网络中存在的安全隐患，目前网络存在的安全隐患主要有以下几个方面。

（1）缺乏对已知病毒的查杀能力。

目前，网络的接入学校尚未部署网络防病毒软件，无法提供对已知病毒的实时检测和查杀。

（2）无法防范来自教科网的网络攻击。

网络接入的学校尚未部署相应的防攻击安全产品，而学校内部可访问互联网及教育科研网的信息点较多，师生上网经常有来一些无意的黑客攻击和网络木马，导致校园网网络堵塞。

（3）网络资源滥用严重。

学生滥用教育网络资源现象较严重，比如 QQ 聊天、联网游戏、电影下载、网页浏览、BT 下载、IM 实时通信、P2P 文件共享等行为。不当的资源利用及学生非法上网行为带来了间谍软件、恶意程序和计算机病毒，导致了教育系统网络资源耗尽、内网病毒泛滥等一系列安全问题。

（4）缺乏学生上网行为监控手段。

学生到底在网上干什么？出了问题该找谁？这两大问题是每个教育管理者最关心的问题。但教育系统网络拥有最庞大的联网信息点，技术管理难度大，缺乏系统的学生网上行为监控手段。

通过以上分析，网络安全工程师认为目前亟需完成以下安全建设。

（1）建立一套完善的安全组织、管理机构。

目前，尚未建立一套完善的安全组织机构，没有相应的安全管理岗位设置、人员配备等措施。这是亟待解决的问题，需要该教育局信息中心健全机构、完善人员配备。

（2）建立一套完善的安全管理制度。

应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；应建立日常管理活动中常用的安全管理制度，以规范安全管理活动，约束人员的行为。

（3）基层学校安全管理人员技术水平有待提高。

各学校的网络管理员的技术水平参差不齐，有的学校甚至根本没有专职的网络管理员，对自身网络设备的维护技术力量不足，要求他们来维护网络安全的难度比较大。

（4）需建立安全事故应急预案机制。

应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程及事后教育和培训等内容。

方案设计

网络安全系统是整体的、动态的，要真正实现一个系统的安全，就需要建立一个从保护、检测、响应到恢复的一套全方位的安全保障体系，它集防火墙、入侵检测、安全扫描系统、内网安全保密及审计系统、基于等级保护的综合安全管理与预警平台、网络防病毒系统等于一体，在技术上将多种网络安全技术和优秀网络安全产品有机集成，实现安全产品之间的互通与联动，将是一个统一的、可扩展的安全体系平台。要实现这个完备的安全体系，需要在信息中心和各下属学校的关键网络节点部署包含防火墙、入侵检测、漏洞扫描、防病毒、安全审计等在内的各类安全产品，并实行统一管理、联动防护。

完备的安全防范体系要从防火墙做起，因为该网络首要防范的目标是来自外网的攻击，只有

先阻断了来自外网的攻击，才能从容布置其他安全设备。如图 1-2 所示，在服务器区域、内网区域、市教科网区域边界，部署 1 台万兆高性能防火墙，分别连接服务器区域、办公区域和市教科网区域，实现其各区域的逻辑上的隔离，同时分担整个教育城域网的进出流量和访问控制。

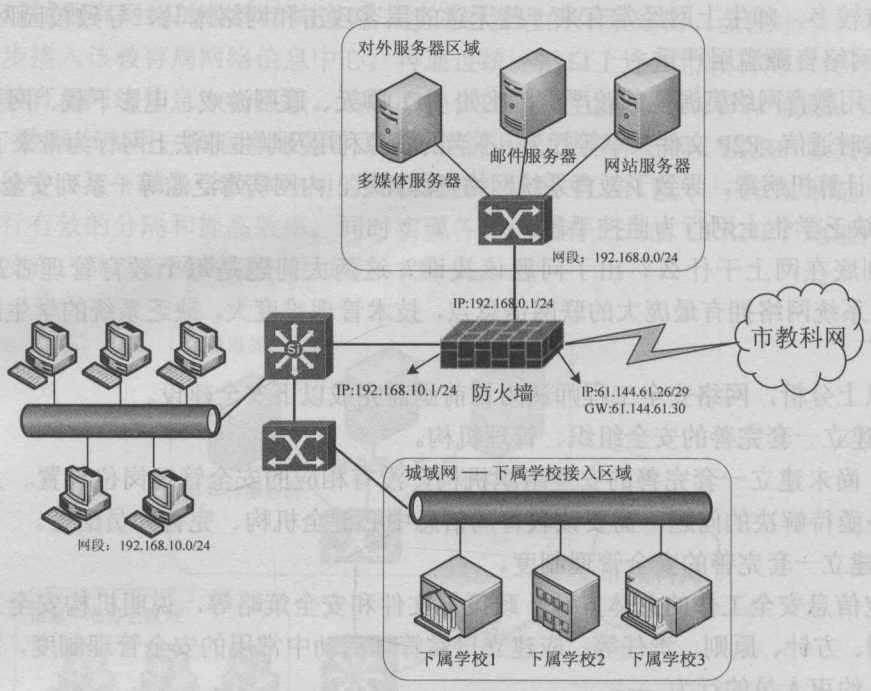


图 1-2　网络安全拓扑图

部署的蓝盾万兆高性能防火墙是新一代高速状态检测防火墙，不仅支持丰富的协议（如 HTTP、FTP、SMTP、H.323、IPSec 等），还支持有害命令和不法协议的检测功能。提供高速的策略过滤、基于高速硬件过滤检测的防攻击、针对具体协议应用的状态检测、静态和动态黑名单过滤、不同策略业务的流控等特性。万兆高性能防火墙提供的丰富统计分析功能和分级分类的详细日志输出，为用户进一步跟踪非法事件提供了必要的保障。此外，该防火墙还能够和专业的 NIDS 设备联合组网，充分发挥 IDS 设备高效、全面的安全保障能力，为后续网络加固打下基础。

相关知识

1.1　防火墙概述

1.1.1　防火墙的概念

防火墙（Firewall）是一种位于内部网络与外部网络之间、专用网与公用网之间的网络安

全系统，是设置在被保护网络和另外网络之间的一道屏障，实现网络的安全保护，以防止发生不可预测的、潜在破坏性的入侵，通常是由软件和硬件设备组合而成。图 1-3 为防火墙作用的示意图。

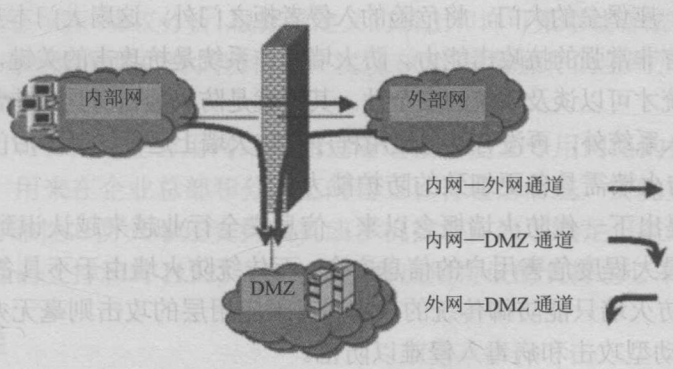


图 1-3 防火墙作用示意图

安装在主机上的防火墙就是一个位于计算机及其所连接的网络之间的软件或硬件。该计算机流入/流出的所有网络通信和数据包均要经过此防火墙。

而在网络中的防火墙，是一个将内部网和公众访问网（如 Internet）分开的系统或设备，允许得到授权的人和数据进入网络，同时将未经授权的人和数据拒之门外，最大限度地阻止网络中的黑客来访问内部网络。

防火墙有两种工作姿态：默认拒绝和默认允许。

默认拒绝就是只允许明确允许的，拒绝没有特别允许的任何事情。这种姿态假定防火墙应该阻塞所有的信息。默认允许就是只拒绝明确拒绝的，允许没有特别拒绝的任何事情。这种姿态假定防火墙应该转发所有的信息。显然，前者更安全，但可能会将正常的数据拒绝掉；后者较危险，因为会有没有明确禁止但是危险的数据进入网络。

防火墙作为第一道网络安全屏障，具有如下基本特性：

（1）防火墙必须部署在网络关键节点（阻塞点、控制点）。

内部网络和外部网络之间的所有网络数据流都必须经过防火墙，这样防火墙才能起到防护作用，防火墙不能防范绕过防火墙的攻击。只有当防火墙是内、外部网络之间通信的唯一通道时，才可以全面、有效地保护企业网内部网络不受侵害。

根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界，即是采用不同安全策略的两个网络连接处，比如用户网络和互联网之间连接、与其他业务往来单位的网络连接、用户内部网络不同部门之间的连接等。防火墙的目的就是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

（2）只有符合安全策略的数据流才能通过防火墙。

防火墙最基本的功能是确保网络流量的合法性，并在此前提下将网络的流量快速地从一

条链路转发到另外的链路上去。无论是包过滤防火墙还是应用代理网关，都是对经过的数据流进行检测，将不符合安全策略的进行阻断，只允许符合安全策略的数据流通过。

（3）防火墙自身不能被攻破。

防火墙就好像一座堡垒的大门，将危险的入侵者拒之门外，这扇大门本身必须非常坚固，所以防火墙自身应具有非常强的抗攻击能力。防火墙操作系统是抗攻击的关键，只有自身具有完整信任关系的操作系统才可以谈及系统的安全性。其次就是防火墙自身具有非常低的服务功能，除了专门的防火墙嵌入系统外，再没有其他应用程序在防火墙上运行，减少后门的可能性。

（4）应用层防火墙需具备更细致的防护能力。

自从 Gartner 提出下一代防火墙概念以来，信息安全行业越来越认识到应用层攻击成为当下取代传统攻击，最大程度危害用户的信息安全，而传统防火墙由于不具备区分端口和应用的能力，以至于传统防火墙只能防御传统的攻击，对于应用层的攻击则毫无办法。具体来讲，就是防火墙对数据驱动型攻击和病毒入侵难以防范。

1.1.2 防火墙的功能

防火墙对网络的保护包括以下工作：拒绝未经授权的用户访问，阻止未经授权的用户存取敏感数据，同时允许合法用户不受妨碍地访问网络资源。一个防火墙（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来降低风险。具体来讲，防火墙的功能主要包含以下几个方面。

（1）执行访问控制，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。例如，在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙上。

（2）进行日志记录，管理和监控网络访问。

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，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。收集一个网络的使用和误用情况也是非常重要的，可以清楚地看出防火墙是否能够抵挡攻击者的探测和攻击，同时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，并能够结合入侵检测系统，实现安全联动。

（3）进行路由交换和 NAT 网络地址转换，缓解地址空间短缺的问题，同时隐藏内部网络结构的细节。

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露内部细节（如 Finger、DNS 等）服务。利用防火墙对内部网络进行划分，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