职业教育计算机专业规划教材

网络安全技术

WANGLUO ANQUAN JISHU

○主编　孙振楠　许大宏

江苏教育出版社　凤凰职教

凤凰职教

职业教育计算机专业规划教材

网络安全技术

WANGLUO ANQUAN JISHU

○主编　孙振楠　许大宏

江苏教育出版社　凤凰职教

图书在版编目(CIP)数据

网络安全技术 / 孙振楠,许大宏主编. —南京：江苏教育出版社,2013.7(2023.8 重印)

ISBN 978-7-5499-2913-9

Ⅰ. ①网… Ⅱ. ①孙…②许… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2013)第 120384 号

职业教育计算机专业规划教材

书　　名　**网络安全技术**

主　　编　孙振楠　许大宏
责任编辑　王　颖
出版发行　江苏教育出版社
地　　址　南京市湖南路 1 号 A 楼,邮编：210009
出　　品　江苏凤凰职业教育图书有限公司
网　　址　http://www.fhmooc.com
印　　刷　河北铄柠印刷有限责任公司
厂　　址　河北省衡水市武邑县兴旺路以南
电　　话　0318-2212090
开　　本　787 毫米×1 092 毫米　1/16
印　　张　12.25
版次印次　2013 年 7 月第 1 版　2023 年 8 月第 17 次印刷
标准书号　ISBN 978-7-5499-2913-9
定　　价　32.00 元
批发电话　025-83677909
盗版举报　025-83658893

如发现质量问题,请联系我们。
【内容质量】电话:025-83658873　邮箱:sunyi@ppm.cn
【印装质量】电话:025-83677905

编 委 会

总序

这套系列教材无论在体例设计与逻辑架构上，还是在内容构成与呈现形式上，皆是务实与创造并重、规范与创新兼备，显示着编写者宽阔的视野和开阔的思路，予人耳目一新之感。在共建共享的合作机制下，编写人员克服“繁、难、散、旧”等传统教材编写过程中容易出现的通病，着力于“实”，尝试于“新”，指向于“活”。内容选择紧扣产业发展与企业用工需求，内容呈现方式也更加灵活。不仅给教师使用时提供了发挥与创造的空间，也让这套教材更具柔性，为教学活动提供了更为广阔自由的空间。同时，该系列教材还体现了专业与专业之间的叠加整合，甚至是异构融合。在系列化的整体架构下，相关专业之间可以顾盼呼应、相互支撑，从而在各自独立成书的基础上形成系列化、集成化、规模化的总体效应。

教材的设计编写要为提高教育教学质量服务。我们基于工作过程开发的以典型工作任务或案例为主体的项目化教材充分体现了“专业与产业对接、课程内容与职业标准对接、教学过程与生产对接”，教师要以开放的思维和姿态，充分利用教材中反映产业升级和技术进步的知识元素，调动学生内在的学习动力和发展潜力，引导学生在实践中学习，在学习中实践。此外，该系列教材中亦有许多与德育相关的教学资源。教师在教学中要引导学生树立正确的人生观、世界观、价值观，提高学生的道德水平和科学文化素养，让学校的课堂不仅是促进学生成才的平台，同样也是引领学生成人的园地。

我们相信，这套教材通过广大师生的创造性使用，一定会展现出自身的个性化魅力，有力促进示范校建设迈向更高的发展层次。同时，我们也真切地希望大家在使用中能及时反馈意见、提出建议，从而保证这套系列教材日臻完善。

编委会

前言

本丛书集中了全国各改革发展示范校建设单位本专业的骨干力量，在多年实际专业教学实践的基础上，经全国教育同行广泛交流合作编写而成。

目前，国内已经出版了众多版本的同类教材，各版本教材在编写体例、内容等方面风格各异。本丛书在全面培养学生的综合素质和职业能力方面、在提高职业院校学生就业和创业能力方面都有新的探索，并形成了“以就业和培养学生职业能力为导向”的课程体系和教材编写思想。与其他版本教材相比，本丛书具有以下两方面显著特点：

第一，本系列教材根据职业教育教学特点，以应用为主线，辅以理论知识的介绍，着力培养学生的职业能力，这是本丛书最大的特点。

本系列教材是将完整的课程体系按照工作过程导向，分解为若干实践项目，辅助以相应的理论知识形成的项目化教材。

本系列教材设有对应的“任务驱动”或“工学结合”，很好地贯彻了工学结合的理念，结构和体例形式体现了职业教育教学的实际需求。

第二，本系列教材结构框架的形成，是校企深度合作的产物。

本系列教材由编写团队与国内知名 IT 企业专家共同根据课程对应的企业实际工作流程、工作岗位进行职业能力分析，在此基础上形成完整的项目化教材结构框架，而每一个教学项目内又分解为若干个工作（学习）任务。

《网络安全技术》由孙振楠和许大宏担任主编，严圣华、吴建华、胡娟、眭春辉、周娟、耿永利、孙惠芬、王修喜、吕国庆、高欣、孙振华、王艳萍参编，全书框架结构由孙振楠和许大宏共同拟定。在此，衷心感谢提供各类资料、项目素材及教材格式建议的各位同事。

鉴于本专业知识更新快，涉及面广，加上编写者水平有限，时间仓促，教材中难免存在疏漏与不妥之处，敬请广大读者与专家批评指正。

编　者

目录

项目一　认识计算机网络安全产品市场环境

项目描述

中职实习生小丁，来易阳网络安全公司面试实习岗位，经理给他的第一个任务就是让他先通过公司的产品资料和市场宣传资料了解公司的背景，查找并了解安全行业的软、硬件市场情况，学习信息安全基础、安全行业法律法规知识，然后再进一步熟悉公司所处行业的情况，在此过程中可以通过与其他各相关部门技术人员沟通，索要行业技术资料，也可以通过互联网查找自己需要的信息，但最终需要通过入职测试才能继续在公司实习。

能力目标

1. 了解网络安全行业的背景。
2. 了解网络安全行业市场的发展动向。
3. 掌握信息安全基础知识。
4. 了解网络安全行业基本法律法规。

职业素养

1. 培养主动学习的意识。
2. 学会获取资料的多种方式。
3. 增强面试过程中的应试能力。
4. 积极关注网络安全行业的发展动态。

任务一　网络安全硬件

任务描述

网络已渗透到人们生活的方方面面，极大地丰富了人们的沟通和生活方式，但也存在层出不穷的网路安全威胁问题。在此大背景下，网络安全产品由最初的防火墙、IDS/IPS、VPN 产品，逐步出现了内容过滤、上网行为管理等越来越“智能”的产品，但也因此带来了网络安全产品市场的混乱。想要成为网络安全行业中的一员，首先应该了解该行业中硬件市场的现状及发展趋势，掌握一些主流网络安全硬件的使用方法。

任务目标

1. 了解网络安全的概念。
2. 了解网络安全硬件市场的现状。
3. 熟识主流的网络安全硬件。

知识储备

一、网络安全简介

1. 概念

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，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全本质上是网络上信息的安全。广义上，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

2. 主要特性

（1）保密性

指信息不泄露给非授权用户、实体或过程，或供其利用的特性。

（2）完整性

指数据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、不被破坏或丢失的特性。

(3) 可用性

指可被授权实体访问并按需求使用的特性,即当需要时能存取所需的信息。如网络环境下拒绝服务、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。

(4) 可控性

指对信息的传播及内容具有控制能力。

(5) 可审查性

指出现安全问题时能够提供依据与手段。

想一想

什么是网络安全,网络安全有哪些特征?

二、思科网络安全认证

1. CCNA 安全

CCNA 安全认证是为了考核负责网络安全的 IT 专业人员的一项认证,它表示通过认证的专业人士拥有相应的专业技能,能够胜任网络安全专家、网络安全管理员和网络安全支持工程师等职位。该认证所验证的技能包括:在保持数据和设备的完整性、保密性和可用性的条件下安装、故障排除和监控网络设备,以及使用思科在安全架构中所采用的技术进行开发的能力。IT 人员在完成了思科培训后,将会掌握关于核心安全技术、开发安全策略、抵御风险的知识。聘请获得 CCNA 安全认证的专业人士,IT 企业或机构将会拥有能够开发安全基础设施、识别网络安全威胁和漏洞和抵御安全威胁的 IT 员工。

CCNA 主要测验考生在保护思科路由器、交换机以及相关网络安全方面的知识,通过它可验证的技能包括:在保持数据和设备的完整性、保密性和可用性的条件下安装、故障排除和监控网络设备,以及使用思科在安全架构中所采用的技术进行技术开发。准备该考试的考生需要学习“实施思科 IOS 网络安全(IINS)”课程。

2. CCSP 认证

CCSP 认证(思科认证资深安全工程师)表示 IT 人员精通或者熟知思科网络的安全知识。获得 CCSP 认证资格的网络人士能够保护和管理网络基础设施,以提高生产率和降低成本。CCSP 认证的内容侧重于安全 VPN 管理、思科自适应安全设备管理器(ASDM)、PIX 防火墙、自适应安全设备(ASA)、入侵防御系统(IPS)、思科安全代理(CSA)以及怎样将上述技术集成到一个统一的集成化网络安全解决方案之中等主题。

CCSP 的考试内容有:SECUR(SecuringCiscoIOSNetworks,CiscoIOS 网络安全)、CSPFA(CiscoSecurePIXFirewallAdvanced,Cisco 安全高级 PIX 防火墙)、CSIDS(CiscoSecureIntrusionDetectionSystem,Cisco 安全入侵检测系统)、CSVPN(CiscoSecureVPN,Cisco 安全 VPN)、CSI(CiscoSAFEImplementation,CiscoSAFE 实现)。

3. CCIE 安全

随着网络安全性的持续增长,它在 IT 行业的影响也日益扩大。CCIE 安全认证是最高级的网络安全认证挑战,它引领 IT 人员进入管理及创建终端到终端的安全网络的职业生涯。安全领域的 CCIE 认证表示网络人士在 IP 和 IP 路由以及特定的安全协议和组件方面拥有专家级知识。

CCIE 安全认证的步骤如下：

（1）CCIE 安全笔试 v3.0

即通过两小时的资格笔试，以获取参加实践考试的资格，笔试内容涵盖了网络的相关概念和一些设备命令的知识。

（2）CCIE 安全实验考试

CCIE 安全实验考试总长 8 小时，用于测试在限时的测试情况下，网络人士运行安全网络的能力。它要求必须在通过 CCIE 安全笔试后的 3 年内通过实验考试，以获取 CCIE 安全认证资格证书，且第一次尝试实验考试的时间必须在 18 个月内。

案例分析

小丁想了解思科网络安全认证的相关知识，并想在毕业前通过 CCNA 安全认证，请您帮助小丁到网站上搜集思科网络安全认证的相关资料，分别列出 CCNA 安全认证、CCSP 安全认证和 CCIE 安全认证所需要学习的内容。

三、安全沙盒

1. 简介

安全沙盒，简称 DCSS（全称为 Digital China Secure SandBox），DCSS－3008 是神州数码网络公司专为网络安全攻防实验室研发的安全沙盒，是进行网络安全攻击和防御的模拟平台，用以锻炼学生动态网络安全维护的能力。安全沙盒 DCSS－3008 具有 10 个千兆电口，其中 2 个用于管理，8 个用于学生实验，可以满足 8 人同时实验。安全沙盒的名字取材于军事术语“沙盘”，它可以模拟实战演练战术和技术。图 1－1－1 为 DCSS－3008R2 模型图。

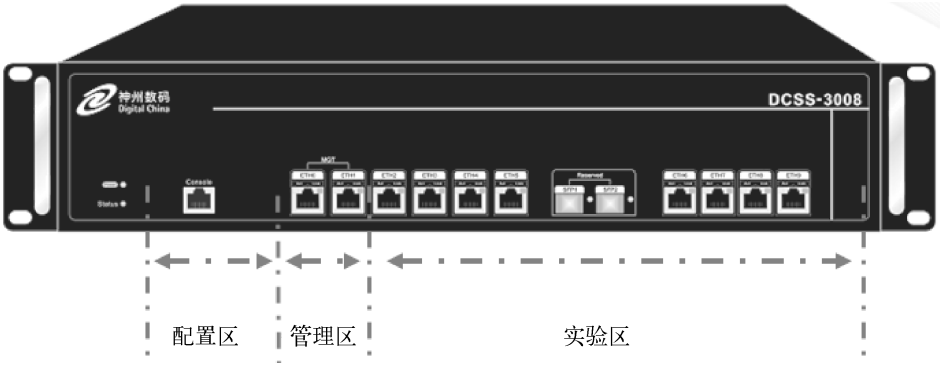

图 1－1－1　DCSS－3008R2 模型图

（1）配置区

沙盒设备初始配置 COM 接口，能够对沙盒设备进行基本属性的信息配置管理。

（2）管理区

包含沙盒与管理服务器连接接口与网络配置管理接口，能够进行沙盒设备管理、维护。

（3）实验区

沙盒设备提供实验操作网络接口，图中的设备能够为 10 个实验者提供独立的虚拟实验环境平台。

2. 安全沙盒的部署

安全沙盒的典型部署示意图如图 1－1－2 所示。

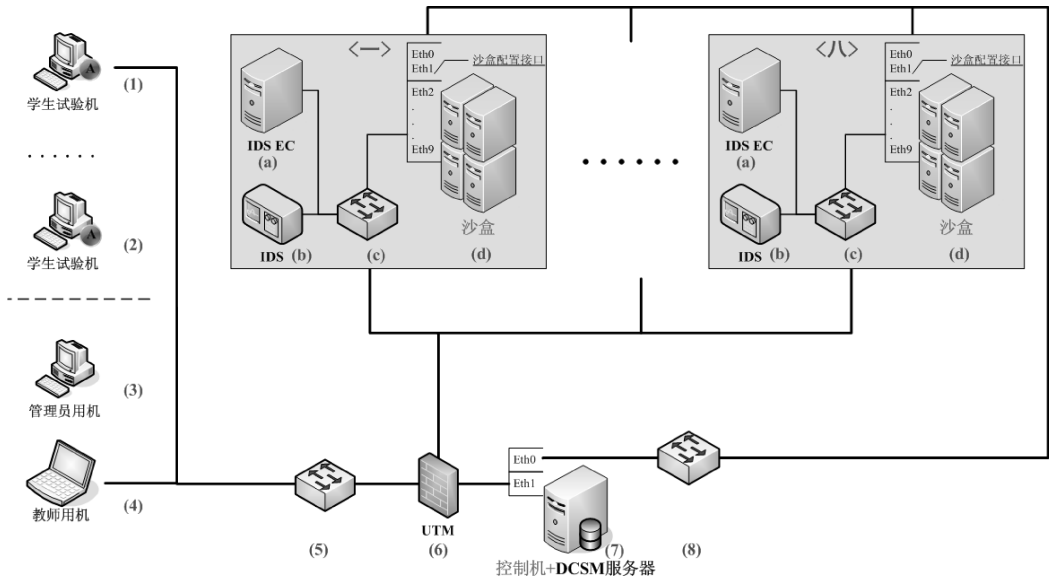

图 1－1－2 SandBox 部署示意图

视频实验室的实际部署如图 1－1－3 所示。

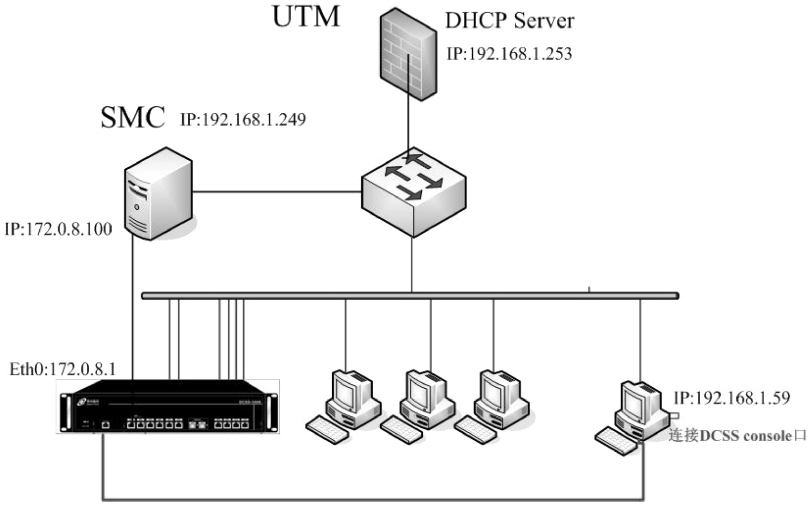

图 1－1－3 视频实验室实际部署图

3. 安全沙盒系统的特点

（1）提供多系统平台的教学

安全沙盒系统为计算机及网络安全教育提供多系统平台的教学课件，在教学、培训过程

中，根据需要可以启动基于不同操作系统平台的教学课件，满足所有教学环境的需求。

（2）多种模式的攻防课件

安全沙盒系统为计算机及网络安全教育提供多模式的安全攻防实验课件，能够进行各种安全威胁的攻防操作，针对不同的攻击防御模式提供多种实验课件选择。

（3）全程自主操作的攻防演练

安全沙盒系统的全部课件均是将安全理论与实际环境和动手操作相结合的实验课程，在所有的学习过程中，都需要通过实际动手进行实验操作，完成课件要求的安全威胁攻击以及针对该攻击采取安全防御措施。它采用不同的实验课程让学员亲身体验计算机及网络安全的攻防全过程，让学生从枯燥的理论学习中解脱出来，可以极大地提升学生学习网络安全知识的积极性，并帮助学生在未来的就业和职业发展中奠定扎实、实用的技术基础。

（4）真实的攻防环境

在安全沙盒系统中，目标主机、操作系统、漏洞均是真实存在的，入侵、防护过程完全真实，并非像一些实验系统只能模拟输出既定的结果，它更贴近实际。

（5）模块化、可独立部署或融合部署

可单独接入终端机器进行安全实验，更可配合神州数码 DCFW 防火墙、UTM 统一威胁管理系统、IDS 入侵检测系统、DCSM 内网安全管理系统、神州数码交换机、路由器、接入认证系统等基础安全及网络实验室模块，并将其组合成真实攻防的全局环境。

（6）特色技术

① 虚拟化技术：在主操作系统上虚拟出不同的虚拟服务器，每个应用层的实验程序运行在独立的软件环境中，可同时启动多项安全实验，最大限度发挥系统资源的使用率，提高“安全沙盒”的性价比。

② 实验包技术：把一个攻防实验所需要的所有组件，包括运行环境、主服务程序、非公有工具、技术帮助文档等通过加密技术组成一个完整的实验包，可以方便地进行管理和加载。通过利用实验包快照技术，教师可以方便对学生的实验情况进行评分。

③ 虚拟系统动态迁移技术：攻防平台和课件平台分离，教师通过控制台可以为学生开启各种计算机及网络安全教学课程的实验环境，学生可以在实验环境中进行各种计算机及网络安全的攻防实验。独立隔离的实验环境不会对其他网络造成危害，并且可以最大限度地利用系统资源，提供尽可能多的服务。

④ 虚拟环境“一键恢复”技术：通过便捷地将安全沙盒系统恢复到初始状态，等待开展下一批实验，把教师的管理工作量降低到最低，从而有利于教师把主要精力放在攻防实验教学本身。

四、安全网关

DCFW－1800E－10G 多核安全网关是面向网络服务运营商、大型企业网、大型校园网等大型骨干网络设计开发的新一代多功能安全网关产品，它采用了领先的 64 位多核 MIPS 体系架构和 Crossbar 高速交换总线技术，使其不但在防火墙性能上实现了全面的跨越，而且在防病毒、IPS、VPN、QoS 及应用层管控等方面的处理能力方面也得到了前所未有的提升。配合 64 位并行安全操作系统在多线程并行处理能力上的优势，DCFW－1800E－10G 即使在同时处理多任务时也全无性能瓶颈之虞。DCFW－1800E－10G 安全网关提供 1 个

GE 接口、12 个 SPF 插槽和 2 个 XFP 万兆插槽，可充分满足大型网络对于不同接口类型及高接口密度的需求，图 1－1－4 所示为 DCFW－1800E－10G 的前面板模型，图 1－1－5 所示为其组网示意图。

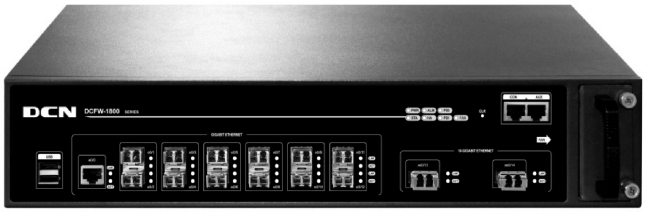

图 1－1－4　DCFW－1800E－10G 前面板模型

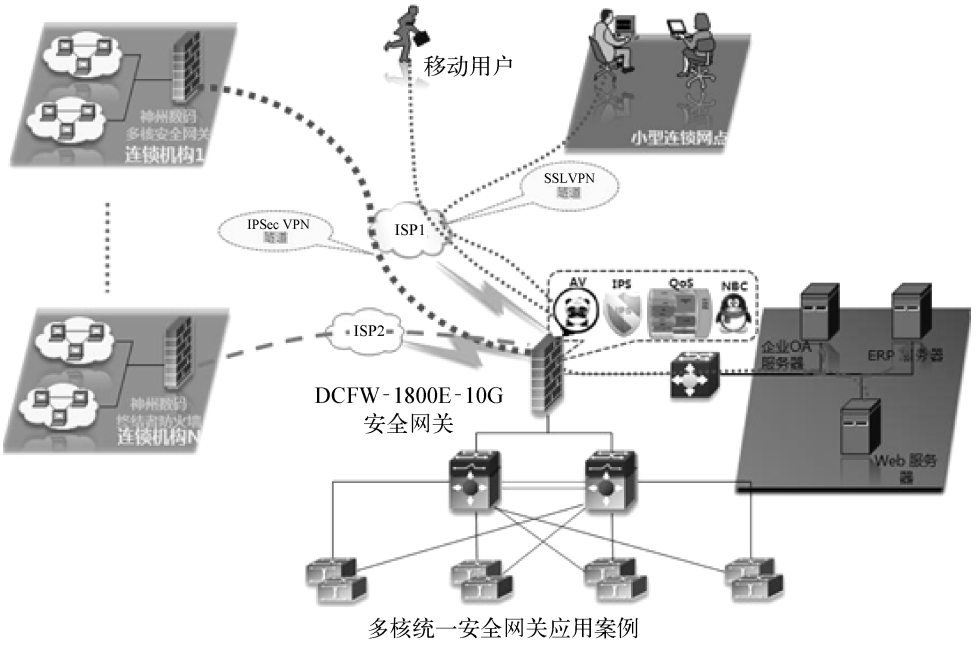

图 1－1－5　DCFW－1800E－10G 组网示意图

五、入侵检测系统

DCNIDS－1800－M3 入侵检测系统是基于网络的动态入侵检测系统，它采用旁路方式全面侦听网上信息流，动态监视网络上流过的所有数据包，通过检测和实时分析，及时甚至提前发现非法或异常行为，并进行响应，通过采取告警、阻断和在线帮助等事件响应方式，以最快的速度阻止入侵事件的发生。它采用专门定制的硬件平台，能够在高负载的网络上提供高水平的性能；同时使用专用的操作系统，从而提供了最大可能的自身安全。

DCNIDS－1800－M3 采用先进的多层分布式体系结构，包括控制台、事件收集器、传感器，这种结构能够更好地保证整个系统的可扩展性和可靠性，也更具备灵活性和可伸缩性，能够满足各种规模的企业级网络的安全和管理需要。它具有入侵检测、实施监控响应、协议还原、流量统计分析等各种功能，适合企业级网络对网络的监测。

部署 DCNIDS－1800－M3 入侵检测系统，可以为用户的网络安全提供可靠的保障。它可以使用户及时发现各类入侵行为（如黑客入侵、拒绝服务、蠕虫泛滥、内部的可疑行为等），发现系统的脆弱性问题（如系统漏洞、弱口令等），并且加强内部网络运行状况的管理（如对通信内容管理、流量监测、访问控制监测、数据回放取证等）。入侵检测设备部署如图 1－1－6 所示。

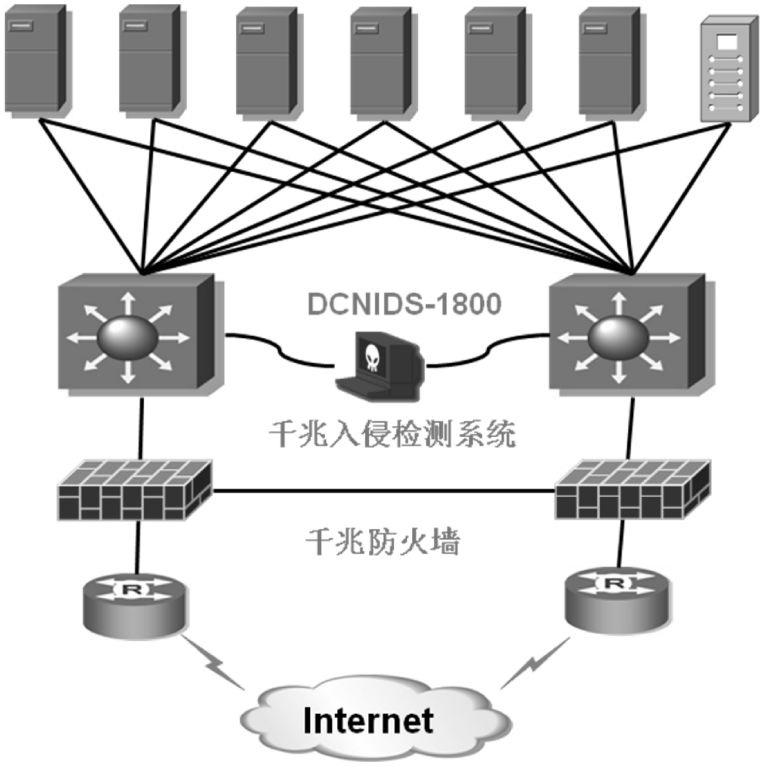

图 1－1－6　入侵检测设备部署图

想一想

请总结网络安全硬件行业发展的现状。

知识拓展　网络安全设备识别

随着网络规模的扩大，网络安全问题也日益凸显。每个企业网络中都会部署相关网络安全设备，网络管理员要能够在现有网络拓扑中找出哪些是安全设备，明白这些设备的作用是什么，还应能够在现有网络中扩充安全设备。

训练内容

图 1－1－7 是经典的网络安全拓扑图，请指出网络中的安全设备及网络所划分的区域，并描述设备和各区域的功能。

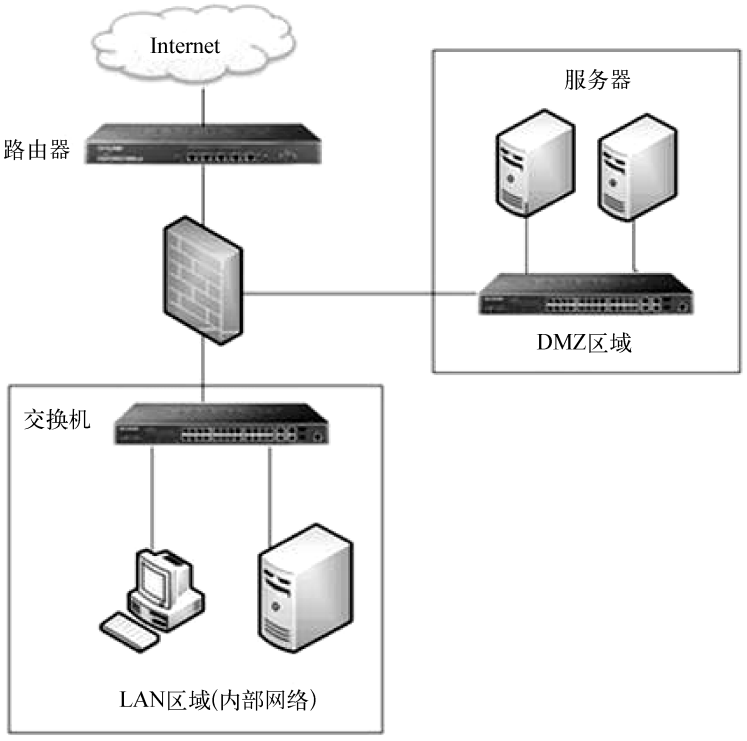

图 1－1－7　网络安全拓扑图