<<VPN虚拟专用网安全实践教程>>

图书基本信息

书名：<<VPN虚拟专用网安全实践教程>>

13位ISBN编号：9787302212348

10位ISBN编号：7302212341

出版时间：2010-1

出版时间：清华大学

作者：金汉均//仲红//汪双顶

页数：213

前言

21世纪，随着人类步入信息社会，信息产业正成为全球经济发展的主导产业。
计算机科学与技术在信息产业中占据了重要的地位，随着互联网技术的普及和推广，网络技术更是信息社会发展的推动力，人们日常学习、生活和工作都越来越依赖于网络，因此信息技术、信息安全技术和网络安全技术正发展成为越来越重要的学科。
互联网技术的发展改变了人们的生活，今天信息安全内涵已发生了根本变化。
安全已从一般性的安全防卫，变成了一种非常普通的安全防范；从一种研究型的安全学科，变成了无处不在，与人们学习、生活和工作息息相关的安全技术。
技术的普及也推动了社会对人才的需求，因此建立起一套完整的网络安全课程教学体系，提供体系化的安全专业人才培养计划，培养一批精通安全技术的专业人才队伍，对目前高校计算机网络安全方向专业人才的培养，显得尤为重要。
1. 关于教材开发背景结合国家“十一五”本科计算机专业课程规划体系，以及深人领会教育部计算机科学与技术教学指导委员会编制的“计算机科学与技术专业规范的知识体系和课程大纲”文件精神，为及时反映目前网络安全专业学科发展动态，创新网络教材编辑委员会组织编写了本书。
希望编撰的网络安全知识，既重视理论、方法和标准的介绍，又兼顾技术、系统和应用分析，在内容结构和知识点布局上还有所创新。
此外随着互联网技术的普及和推广，日常学习和工作依赖于网络的比重增加，计算机网络安全的实施和防范技术，成为目前最为瞩目的学习内容。
根据上述思路，创新网络教材编辑委员会选择网络安全技术在生活中具体应用，作为教材开发主线，规划出面向实际工程案例，可操作、可应用、可实施的网络安全技术教程。
更希望规划的安全技术直观、形象、具体、可落实，选编和规划的安全知识具有专业化、体系化、全面化特征，能体现和代表当前最新的网络安全技术发展方向。

<<VPN虚拟专用网安全实践教程>>

内容概要

本书主要介绍使用VPN技术组建安全网络实践教程，全书分为两个知识模块，分别为组建虚拟专用网安全基础知识，和使用虚拟专用网安全产品组建虚拟专用网实践教程。
知识点包括：构建站点到站点IPSec，站点到站点IPSec VPN（数字签名），IPSec VPN，远程访问IPSec VPN（用户口令），远程访问IPSec VPN (USB-Key数字证书），远程访问IPSec VPN的授权控制，使用桥接模式构建IPSec VPN，使用路由器构建GRE VPN，使用路由器构建GRE over IPSec VPN，在地址重叠环境中部署IPSec VPN，远程访问IPSec VPN准入控制，构建SSL VPN，构建SSL VPN单臂通信实验等。
全书在每个章节中，对所使用到相关安全产品的基本配置、基本界面、功能配置，都进行详细的讲解，以帮助读者熟悉产品的使用，并进一步诠释了其在工程项目中的实施方法。
本书可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生，学习和研究网络安全产品及技术的实验教材。
此外本书还可作为网络安全专业认证的培训教材以及网络设计师、网络工程师、系统集成工程师以及其他专业技术人员技术参考书。

作者简介

金汉均，博士，华中师范大学计算机科学系教授，长期在教学一线从事网络工程技术的教学和科研工作，主要研究方向是“网上虚拟现实中的关键技术和最优化算法应用”等。
近年来，他在网络安全领域的研究也有突出成就，有十五篇论文被世界SCI、EI、ISTP三大检索企业收录。

<<VPN虚拟专用网安全实践教程>>

书籍目录

章节摘录

插图：由于需要在Internet上传输公司内部的私有信息，VPN用户对数据的安全性都比较关心，安全问题是VPN的核心问题。
目前VPN主要采用四项技术来保证安全，这四项技术分别是隧道技术（Tunneling）、加解密技术（Encryption 8L Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication）。
通过这四项安全技术来保证企业远程办公员工安全访问公司内部网络。
其中隧道技术是VPN的基本技术，类似于点对点连接技术，它在公用网建立一条专用数据通道（隧道），让数据包通过这条隧道传输。
隧道由隧道协议形成，分为第二、三层隧道协议。
第二层隧道协议是先把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，双层封装形成的数据包通过第二层协议进行传输。
常见的第二层隧道协议有L2F、PPTP、L2TP等。
其中L2TP协议由PPTP与L2F融合而形成。
第三层隧道协议是把各种网络协议，直接装入隧道协议中，形成的数据包依靠第三层协议进行传输，其中第三层隧道协议有VTP、IPSec等。
IPSec（IP Seeurity）是最常见第三层隧道协议，由一组RFC文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在IP层提供安全保障。
Internet Protocol Seeurity（IPSec）是由Internet Engineering Task Force（IETF）组织定义的安全标准框架，是保护IP协议安全通信的标准。
它主要对IP协议分组进行加密和认证，用以提供公用和专用网络的端对端加密和验证服务。
IPSec具有互操作性、高质量、基于加密特征，适用于IPv4和IPv6的协议规范。
IPSec能够对数据的存取控制、机密性、完整性和可用性提供保证，并能够防止重放攻击。
IPSec可应用在IP层对IP包进行封装，或在IP层与数据链路层之间提供安全保障。

编辑推荐

《VPN虚拟专用网安全实践教程》：教育部高等学校信息安全类安全专业教学指导委员会、中国计算机学会教育专业委员会共同指导《VPN虚拟专用网安全实践教程》注重实际工作中遇到的安全问题的解决能力。
全书以安全技术应用为主线，以培养学学生安全问题解决能力为目标，以加强实际安全技能锻炼为根本，满足学校安全类课程实践教学需要。
因此全书在编写过程中、强化实践教学能力的培养，着重讲授生活中的网络安全问题，诠释对应的安全策略配置，最后依据学校提供的安全实践教学平台，直观、形象地诠释安全技术，帮助学生理解抽象的网络安全专业理论。

<<VPN虚拟专用网安全实践教程>>

版权说明