第一图书网, tushu007.com

<<Internet接入·网络安全>>

图书基本信息

书名：<<Internet接入·网络安全>>

13位ISBN编号：9787121118913

10位ISBN编号：7121118912

出版时间：2010-11

出版时间：电子工业

作者：袁浩//张金荣//刘晓辉

页数：526

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

前言

关于《网管天下》丛书《网管天下》丛书是一套由国内资深网络专家写给网络建设与管理人员的应用实践手册，其目的在于帮助初、中级网络管理员，全方位地解决网络建设与管理中的各种实际问题，包括综合布线设计、实施与测试，网络设计与设备选择、连接与配置，网络服务搭建、配置与监控，网络故障诊断、排除与预防，网络安全设计、配置与监视，网管工具选择、使用与技巧，网络设备、服务和客户管理的自动化等诸多方面；囊括了网络管理中几乎所有的内容，其目的在于将网络理论与实际应用相结合，提高读者分析和解决具体问题的能力，将所学变为所用，将书本知识变为操作技能。
《网管天下》第1版已经出版近两年的时间，取得了不错的销售业绩，在同类图书中名列前茅，受到了广大读者朋友的喜爱。
《网络管理工具实用详解》一书的版权还输出到了中国台湾，得到了中国台湾出版业同行的认可。
不过，在这两年时间里，新的网络设备不断推出、新的网络技术不断成熟、新的管理软件不断升级、新的网络应用也不断丰富，原来图书中的有些内容已经不能适应新设备、新技术、新软件和新应用的需求。
因此，在保留图书原有写作风格的基础上，对目录结构做了进一步优化，对过时的内容进行了大幅度的更新，隆重推出了《网管天下》第2版。
本丛书具有以下特点。
1. 授之以渔而不是授之于鱼。
紧贴网络实际情况，从真实的网络案例入手，为网络管理员提供全面的网络设计、网络组建、网络管理和网络维护等解决方案，以提高读者的分析能力、动手能力和解决实际问题的能力。
2. 实用才是硬道理。
为网络管理员提供彻底的、具有建设性的网络设计、网络组建和配置解决方案，真正解决网络建设和网络管理中的实际问题，突出实用性、针对性、技术性、经典性，举案说“法”、举一反三。
3. 理论新、技术新、设备新、案例新。
所有的应用案例都发生在最近两年，而且案例中只涉及最主流的、最成熟的设备和技术，以及最新版本的软件，不再讨论那些已被淘汰或面临淘汰的东西，从而力求反映网络的新技术和新潮流。
不仅让读者学了就能用，而且还可以拥有三年左右的“保鲜”期。
关于本书随着时代的发展和进步，Internet早已经不是新鲜事物。
随着信息化时代的加速到来，人们的日常生活、办公、消费、旅游、交往对计算机网络的依赖程度越来越高，信息安全已经成为与每个人、每个行业、每个领域都息息相关的问题。
2010年1月CNNIC发布的《第25次中国互联网络发展状况统计报告》显示，我国网民规模已达3.84亿，尽管总体增速有所放缓，但“异军突起”的商务类应用增幅却高达68%。
企业网络在企业中的地位已经从“可有可无”的辅助机构，转变为必不可少的关键部门。
有专家曾经预言，应用与安全将成为网络技术发展的两大方向。
近几年来，随着网络应用的加速发展，网络安全问题已经引起了许多国家的普遍关注，成为当今网络技术领域的一个重要研究课题。
对于企业网络而言，影响网络安全的因素很多，除Internet系统自身的开放性外，内部用户访问控制、用户身份识别、管理漏洞、安全意识不高等都可能给网络安全造成威胁。
网络安全与其他具体的网络应用有所不同，它是一个完整的体系，涉及日常管理、人为应用、周边环境、物理设备等多个方面，管理员只有充分应用现有设备和技术，准确把握安全管理的主线，才能打造固若金汤的企业网络，使企业在未来的发展中立于不败之地。
本书将整个企业网络的安全概括为内部网络安全、局域网接入安全、Internet接入安全、远程访问安全等几部分，内容涵盖了当今企业网络安全的方方面面，旨在帮助企业打造安全、可靠、高效、便捷的计算机网络。
全书共分14章，第1章网络安全规划，介绍企业网络安全的因素和解决方案。
第2章Windows系统安全，以Windows Server 2008系统为例介绍服务器系统安全的相关技术与配置。

第3章用户权限控制，介绍网络中不同用户账户访问权限的控制。
第4章系统安全策略，介绍与Windows系统安全相关的策略，以及如何通过组策略控制台部署安全策略。
第5章网络服务安全介绍Active Directory服务、文件服务、打印服务、WWW、FTP等常用服务的安全配置。
第6章系统漏洞扫描，介绍系统漏洞管理解决方案。
第7章入侵检测，介绍如何通过snort和sniffer监测网络运行状态。
第8章局域网接入安全，介绍如何通过ACS、交换机端口控制、802.1x等技术实现局域网接入安全。
第9章VPN安全接入，介绍企业网络中各种VPN接入方案的安全部署。
第10章网络访问保护，配合DHCP强制实例和VPN强制实例，介绍NAP系统的功能、组件和运行机制。
第11章Internet接入概述，介绍目前企业网络接入Internet常用的解决方案。
第12章Forefront TMG共享Internet接入，介绍Windows Server 2008用户如何通过TMG 2010实现局域网共享接入，以及相关的安全配置方案。
第13章路由器共享Internet接入，介绍路由器接入Internet方案中安全配置。
第14章网络防火墙共享Internet接入，介绍如何通过Cisco ASA实现共享Internet接入以及相关的安全配置。
本书由袁浩、张金荣、刘晓辉编著，马倩、白华、李海宁、田俊乐、陈志成、王延杰、刘红、赵卫东、刘淑梅、杨伏龙、李文俊、王同明、石长征、郭腾等也参与了部分章节的编写工作。
笔者长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，曾经出版过五十余部计算机类图书，均以易读、易学、实用的特点，受到众多读者的一致好评。
本书是笔者的又一呕心沥血之作，希望能对大家的系统维护和网络管理工作有所帮助。

内容概要

本书以实际应用为主，从服务器安全、常用网络服务安全、安全设备部署、网络设备安全配置、常用Internet接入方式、局域网接入安全、网络访问保护、Internet接入安全、远程访问VPN安全等多个角度，全面介绍了企业计算机网络安全解决方案。
本孖统观全局，对企业网络安全中常用的技术进行深入浅出的讲解，可以帮助读者快速掌握最基本的计算机网络安全技术，打造安全、可靠的企业网络环境。
　　本书语言通俗易懂，图文并茂，配合大量操作实例，介绍了企业网络中每个环节的安全解决方案。
本书可作为中小企业网络管理员、网络技术爱好者、网络维护与服务人员、在校大专院校学生提高网络实战能力的必备学习用书，也可作为高职高专、培训机构的教材或教学参考书。

书籍目录

第1章 网络安全规划 1.1 网络安全体系结构 1.1.1 物理安全 1.1.2 网络结构规划 1.1.3 系统安全 1.1.4 信息安全 1.1.5 应用安全 1.2 网络安全系统的设计与管理原则 1.2.1 网络安全系统的设计原则 1.2.2 网络安全系统的管理 1.3 网络安全规划实例 1.3.1 服务器安全 1.3.2 网络设备安全 1.3.3 网络防火墙部署规划 1.3.4 IDS部署规划 1.3.5 IPS部署规划 1.3.6 局域网接入安全 1.3.7 Internet接入安全 1.3.8 远程接入安全规划 第2章 Windows系统安全 2.1 操作系统安装与更新 2.1.1 系统安装注意事项 2.1.2 补丁安装注意事项 2.1.3 配置Windows Update 2.1.4 补丁安装 2.2 系统管理员账户 2.2.1 默认组权限 2.2.2 更改Administrator账户名称 2.2.3 系统管理员密码设置 2.2.4 创建陷阱账户 2.3 磁盘访问权限 2.3.1 权限范围 2.3.2 设置磁盘访问权限 2.3.3 查看磁盘权限 2.4 系统账号数据库 2.4.1 启用加密 2.4.2 删除系统账号数据库 2.4.3 备份和恢复账户信息 2.5 Internet连接防火墙 2.5.1 Internet防火墙简介 2.5.2 启用Internet防火墙 2.6 安全配置向导 2.6.1 配置安全服务 2.6.2 应用安全配置策略 2.7 默认共享 2.7.1 查看默认共享 2.7.2 停止默认共享 2.8 关闭端口 2.8.1 服务端口 2.8.2 端口威胁 2.8.3 查看端口 2.8.4 启动/关闭服务法 2.9 系统服务安全 2.9.1 系统服务配置注意事项 2.9.2 服务账户 第3章 用户权限控制 第4章 系统安全策略 第5章 网络服务安全 第6章 系统漏洞扫描 第7章 入侵检测 第8章 局域网安全接入 第9章 VPN安全接入 第10章 网络访问保护 第11章 Internet接入概述 第12章 Forefront TMG共享Internet接入 第13章 路由器共享Internet接入 第14章 网络防火墙共享Internet接入

章节摘录

插图：服务器是企业网络的重要基础，其安全性将直接影响企业网站以及网络应用的安全，甚至会影响企业的生存与发展。
服务器的大部分应用都是基于网络操作系统等软件实现的，因此，无论是应用程序出错，还是硬件故障都可能导致服务器瘫痪。
若想做好服务器安全防护工作，必须从多方面入手。
服务器硬件安全服务器硬件设备的维护主要包括增加和卸载设备、更换设备、工作环境维护等。
因为服务器的运行是不间断的，因此这些维护工作必须存确保服务器正常运行的状杰下讲行。
增加内存和硬盘容量。
服务器的内存和硬盘都是支持热插拔的，建议增加与原设备同厂商、同型号、同容量的内存或硬盘，避免由于兼容性问题而导致服务器宕机。
定期为服务器除尘。
很多服务器故障都是由于内部灰尘导致的，因此建议管理员每个月定期的拆机打扫一次。
控制机房温度和湿度。
虽然服务器对工作环境的要求比较宽泛，但是当服务器周边环境比较恶劣时同样会降低其处理速度和稳定性。
2.操作系统安全服务器操作系统的安全是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。
对于操作系统的安全防范可以采取如下策略。
对操作系统进行安全配置，提高系统的安全性。
系统内部调用不对Internet公开，关键性信息不直接公开，尽可能采用安全性高的操作系统。
应用系统在开发时，采用规范化的开发过程，尽可能地减少应用系统的漏洞。
网络上的服务器和网络设备尽可能不采取同一家的产品。
通过专业的安全工具（安全检测系统）定期对网络进行安全评估。

编辑推荐

《Internet接入·网络安全》：网络安全整体规划、服务器及常用网络服务安全设、置、网络设备部署及安全配置、常用Internet接入方式及接入安全、远程访问VPN安全。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com