

<<网络安全管理实践>>

图书基本信息

书名：<<网络安全管理实践>>

13位ISBN编号：9787121077470

10位ISBN编号：7121077477

出版时间：2009-1

出版时间：电子工业出版社

作者：刘晓辉

页数：580

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>

## &lt;&lt;网络安全管理实践&gt;&gt;

## 前言

《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。

## <<网络安全管理实践>>

### 内容概要

本书全面深入地介绍了Windows服务器、交换机、路由器、无线网络和网络安全设备的安全设置，系统补丁服务器、网络防病毒服务器和NAP网络访问保护的构建，以及局域网的安全构建策略，提供了全面的局域网安全解决方案。

使读者能够全面掌握局域网络中的安全管理与设置技术，全面提升网络的安全水平，迅速成长为合格的网络管理员和安全规划师。

本书适用于中小型网络管理员和安全规划师，以及所有准备从事网络管理工作的网络爱好者，并可作为大专院校计算机专业的辅导教材。

## <<网络安全管理实践>>

### 书籍目录

第1章 网络安全综述 1.1 网络系统安全风险分析 1.2 安全需求与安全目标 1.3 网络安全规划 1.4 网络安全体系结构 1.5 安全管理第2章 Windows Server 2008初始安全 2.1 Windows Server 2008安装安全 2.2 Windows Server 2008基本安全 2.3 Windows Server 2008被动防御安全 2.4 Windows 系统安全 2.5 高级安全Windows防火墙第3章 系统漏洞安全 3.1 漏洞概述 3.2 漏洞扫描 3.3 系统更新第4章 活动目录安全 4.1 活动目录安全管理 4.2 活动目录数据库第5章 用户账户安全 5.1 系统管理员账户安全 5.2 用户账户安全 5.3 用户权限第6章 组策略安全 6.1 组策略模板 6.2 安全策略 6.3 软件限制策略 第7章 文件系统安全 7.1 NIFS权限 .....第8章 共享资源安全第9章 Internet信息服务安全第10章 事件日志、性能日志和警报第11章 系统补丁安全第12章 网络病毒安全第13章 交换机安全第14章 无线网络安全第15章 路由器安全第16章 网络安全设备管理

## &lt;&lt;网络安全管理实践&gt;&gt;

## 章节摘录

计算机网络安全方案，包括原有网络系统分析、安全需求分析、安全目标的确立、安全体系结构的设计等。

该解决方案的目标是在不影响当前业务的前提下，实现对局域网全面的安全管理。

借助对计算机网络的分析和设计，实现以下网络安全目的。

将安全策略、硬件及软件等方法结合起来，构成一个统一的防御系统，有效阻止非法用户进入网络，减少网络的安全风险。

建立统一的漏洞、补丁管理平台。

定期进行漏洞扫描、审计跟踪、分发补丁。

建立完善的漏洞、补丁评估体系，对于新的漏洞、补丁进行安全评测。

建立完善的备份机制，包括：数据库、操作系统、个人应用文件等。

通过入侵检测、入侵保护、流量检测等方式实现实时安全监控，提供快速响应故障的手段，同时具备很好的安全取证措施。

网络管理员能够很快重新组织被破坏了的文件或应用，使系统重新恢复到破坏前的状态，最大限度地减少损失。

在工作站、服务器上安装相应的防病毒、防间谍软件，由中央控制台统一控制和管理，完成带毒设备的阻隔和分离，实现全网统一部署。

培养、加强集团职员的安全意识。

建立完善的安全保护、预警、检查类的规章制度。

1.1 网络系统安全风险分析随着Internet网络急剧扩大和上网用户迅速增加，网络系统的风险变得更加严重和复杂。

原来由单台计算机安全事故引起的损害可能传播到整个系统，导致网络大范围的瘫痪和损失：加上用户缺乏安全控制机制和对Internet安全政策的认识不足，这些风险正日益加重。

针对企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险必须认真考虑，并且要针对面临的风险，采取相应的安全措施。

下述风险由多种因素引起，与网络结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。

网络安全可以从以下几个方面来理解：网络物理是否安全网络平台是否安全系统是否安全应用是否安全管理是否安全针对每一类安全风险，结合局域网的实际情况，下面将具体地分析网络的安全风险。

。

## <<网络安全管理实践>>

### 编辑推荐

《网管天下:网络安全管理实践(第2版)》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,能够全方位地解决网络建设与管理中的各种实际问题。局域网的安全构建策略,主要内容包括Windows服务器安全,网络交换机和路由器安全,无线局域网安全,Windows网络客户端安全。

<<网络安全管理实践>>

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>