从网管员到CTO

最全的网络专家实战经验

最实用的网管员进阶宝典

网络安全规划与管理实战详解

卓文华讯　刘晓辉　陈洪彬　编著

本书特色

- 对知识的讲述通俗易懂，深入浅出，融入了作者多年的心得
- 以任务为驱动，以需求为目标，将服务模块化，将技术条理化
- 案例独具匠心，具有高度的启发性和可扩展性
- 操作步骤详细，读者更容易上手

化学工业出版社

从网管员到CTO

网络安全规划与管理实战详解

卓文华讯　刘晓辉　陈洪彬　编著

化学工业出版社
·北京·

本书采用任务驱动式写作方式，以应用需求引出相关技术，针对不同网络管理任务给出不同的工具软件解决方案，实现网络监控、配置、诊断和管理模块化，使读者可以根据自己的网络管理任务选择相应的工具，并完成相应的网络安全规划与管理工作。

全书共分为15章，主要内容包括：Windows Server 2008初始安全、Windows系统漏洞安全、Windows端口安全、Windows活动目录安全、Windows组策略安全、Windows文件系统安全、Windows共享资源安全、Internet信息服务安全、Windows网络访问保护、Windows系统更新服务、Windows防病毒服务、Cisco交换机安全、Cisco路由器安全、Cisco无线网络安全及数据存储安全等。

本书采用全新的写作理念，以任务为驱动，以需求为目标，将服务模块化，将技术条理化，容纳了几乎所有重要的、常用的网络管理工具软件，涉及了各种典型的、复杂的应用场景，语言通俗易懂，内容丰富翔实，既可作为网络管理初学者的指导用书，又可作为资深网络管理员的参考用书。

图书在版编目（CIP）数据

网络安全规划与管理实战详解 / 刘晓辉，陈洪彬编著. —北京：化学工业出版社，2010.4
（从网管员到CTO）
ISBN 978-7-122-07746-2

Ⅰ.网… Ⅱ.①刘…②陈… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2010）第024208号

责任编辑：陈 静　　装帧设计：王晓宇
责任校对：郑 捷

出版发行：化学工业出版社（北京市东城区青年湖南街13号 邮政编码100011）
印　　装：北京市彩桥印刷有限责任公司
787mm×1092mm 1/16 印张29$^{3}/_{4}$ 字数724千字 2010年4月北京第1版第1次印刷

购书咨询：010-64518888（传真：010-64519686） 售后服务：010-64518899
网　　址：http://www.cip.com.cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　　价：55.00元

前　言

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等，发展到基于复杂的内部网、企业外部网和全球互联网的企业级计算机处理系统和世界范围内的信息共享。在计算机连接能力和连接范围大幅度提高的同时，基于网络连接的安全问题也日益突出。

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，不受偶然的或者恶意的原因而遭到破坏、更改和泄露，使系统连续、可靠、正常地运行，网络服务不中断。从用户的角度来说，希望涉及个人隐私或商业利益的信息在网络上传输时，其机密性、完整性和真实性受到保护，避免其他人或对手利用窃听、冒充、篡改或抵赖等手段侵犯用户的利益和隐私，因此网络安全成为了个人和机构，特别是企业必须解决的问题，而在企业中使用 Windows 操作系统和 Cisco 路由器的网络又是非常常见的。

为了帮助读者快速、扎实地掌握常见操作系统和网络设备的安全设置方法，本书以 Windows Server 2008 服务器操作系统及 Cisco 产品为例，介绍了若干增强网络安全性的措施和防堵网络漏洞的方法。全书的讲解以案例为导向，体现真实的企业需求，并以图文并茂的感性方式让读者获得第一手的安全经验。

本书特色

（1）讲述知识通俗易懂，深入浅出，融入了编者的多年心得。

编者具有专业的企业服务器安全管理的经历，具有多年的 Windows 操作系统及 Cisco 路由器使用经验，对企业环境中面临的安全问题以及解决措施有独特的见解，并能用通俗易懂的语言，深入浅出地表达出来。

（2）内容全面，重点突出，图文并茂。

编者曾多次受邀编写网络安全方面的教材，因此既对书中的重点内容有较好的把握，也对读者在学习中可能会碰到的疑点、难点有深刻的理解。书中采取了全程图解的方式，即使对于难以理解的操作，读者也能按图索骥，顺利掌握。

（3）案例独具匠心，具有高度的启发性和可扩展性。

编者选取了具有代表性的企业环境作为案例，详细讲解了解决和部署的方法，使读者带着目的去学习，并对相似的环境也能够举一反三，最终掌握应对各类企业网络安全环境的方法，成为拓展型的网络人才。

（4）格式醒目，便于阅读。

正文中既有大量图片，也有大段文字和命令等，其间穿插了表格、列表以及各种小提示等，从而让整体风格变得轻松活泼，更有利于读者阅读和理解。

本书内容

本书共 15 章，主要内容如下。

第 1 章介绍了 Windows Server 2008 的防火墙和系统安全等基本设置。

第 2 章介绍了扫描和修补 Windows Server 2008 系统漏洞的方法。

第 3 章介绍了查看和修补 Windows Server 2008 端口安全的方法。

第 4 章介绍了活动目录及其数据库的安全管理方法。

第 5 章介绍了组策略的配置方法。

第 6 章介绍了 Windows 文件系统安全的设置和漏洞防堵方法。

第 7 章介绍了 Windows 共享资源的管理和配置方法。

第 8 章介绍了 IIS 服务器安全相关的设置。

第 9 章介绍了 Windows 网络访问保护的部署和配置方法。

第 10 章介绍了使用 Windows 系统自动更新服务器来防堵系统漏洞的方法。

第 11 章介绍了使用 Symantec 杀毒软件来防治病毒的方法。

第 12 章介绍了 Cisco 交换机安全相关的设置方法。

第 13 章介绍了 Cisco 路由器安全相关的设置方法。

第 14 章介绍了 Cisco 无线网络安全相关的设置方法。

第 15 章介绍了利用各种数据存储方法来增强网络健壮性的方法。

本书适用于各类网络工程技术人员参考使用，也可作为高等院校计算机与信息技术及相关专业的教辅书。

本书由衡水学院刘晓辉和卓文华讯陈洪彬编著，李林、李勇、罗珍妮、向飞、胡芳、荣菁、向超、章静、杨辉等参与了文字整理、录入等工作。在本书的编写中，电子科技大学卢如海、吴君等老师提供了宝贵的建议，陈晓红、李春梅、李娇等做了多次细致的审校工作，在此一并表示感谢。

尽管我们在写作过程中投入了大量的时间和精力，但由于水平有限，疏漏和不足之处仍在所难免，敬请广大读者和同行斧正，可发送邮件（ben_uestc@163.com）与编者进行交流。

编者

2010 年 1 月

目 录

第 1 章

Windows Server 2008 初始安全

与 Windows Server 2003 相比，Windows Server 2008 的系统和网络功能都有了一定的扩展，安全性也有了很大提高。Windows 系统平台的安全保障无疑是构建服务器安全的基础，它涉及操作系统和应用程序的安装安全、系统服务安全、系统设置安全和用户账户安全等诸多方面。通常情况下，采用默认方式安装的 Windows Server 2008 为了便于系统管理，并未注重安全性的设置，因此必须对服务器系统进行必要的安全配置。

1.1 案例部署

微软推出的 Windows Server 系统，一向秉承简单、易用的风格，占领了中小企业的大部分市场，它是中小型网络应用服务器的首选。尤其是 Windows Server 2008 系统，不仅更加简单易用，而且无论功能还是性能，都有较大的提升。采取正确合理的系统安装方式，可以提高操作系统的安全性。如果采用的是升级安装方式，除了详细了解 Windows Server 2008 安装注意事项之外，还应及时下载补丁更新，以免导致升级安装的失败，或者升级完成后带来的安全隐患。

本案例是以一台安装了 Windows Server 2008 操作系统的计算机作为服务器的小型局域网，局域网中包含 18 台客户机。客户机的文件交换较为频繁，有一些员工经常使用移动设备存取数据，作为新就任的网络管理员，首先要做的就是对 Windows Server 2008 进行基本的安全配置，为了防御病毒和间谍程序的侵入，还需要配置 Windows Server 2008 的被动防御安全。此外在对客户机提供服务时，还要应对不安全客户端带来的挑战，需要对系统的应用程序安全、系统服务安全、注册表安全和审核策略进行配置，并详细建立防火墙规则。

1.2 Windows Server 2008 基本安全配置

为确保 Windows Server 2008 服务器的安全，安装完成之后应立即配置 Internet 防火墙等基本安全配置，防止黑客或恶意软件通过 Internet 访问计算机。另外，还可以在安装网络服务之后，通过安全配置向导部署针对性的网络访问安全策略。

1.2.1 配置 Internet 防火墙

Internet 防火墙（Internet Connection Firewall，ICF）是 Windows Server 2008 系统内置的简单防火墙。ICF 不仅可以阻止来自外部网络的恶意访问或攻击，还可以阻止当前服务器向其他计算机发送的恶意软件。默认情况下，ICF 是自动开启的。

Windows Server 2008 系统的 ICF 在默认情况下已经启动，管理员可以根据需要进行配置。如果服务器已经连接到网络，则网络访问策略的设置可能会阻止管理员对 Windows 防火墙的配置。此时应暂时退出网络，或请求管理员赋予相应的操作权限完成此项工作，具体的操作步骤如下。

STEP 01 在 Windows Server 2008 的“控制面板”窗口中，双击“Windows 防火墙”图标，显示如图 1-1 所示的“Windows 防火墙”窗口。此时，显示 Windows 防火墙已启用。

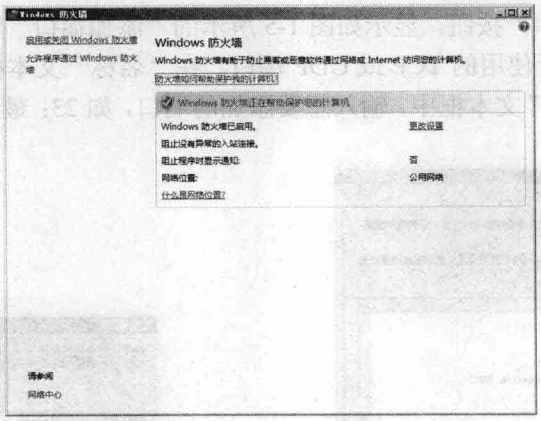

图 1-1 “Windows 防火墙”窗口

注 意

“网络位置”的设置将直接影响 Internet 防火墙的安全级别。Windows Server 2008 提供了 3 个网络位置可供选择，分别是家庭、办公室和公共场所。在网络和共享中心可修改相应设置，如图 1-2 所示，如果点选“专用”（与家庭或办公室对应）单选按钮，则防火墙将自动信任网络上的人和设备；如果点选“公用”（与公共场所对应）单选按钮，则 Windows 防火墙将自动阻止所有来自网络的访问和请求，并且使当前计算机对周围计算机不可见。

STEP 02 单击“启用或关闭 Windows 防火墙”链接，显示如图 1-3 所示的“Windows 防火墙设置”窗口，系统默认点选的是“启用”单选按钮。如果同时勾选“阻止所有传入连接”复选框，防火墙将阻止所有主动连接当前服务器的尝试。当需要为该服务器提供最大限度的保护时，才使用该设置，启用该设置后将忽略“例外”选项卡中的所有设置。通常情况下，不推荐勾选该复选框。

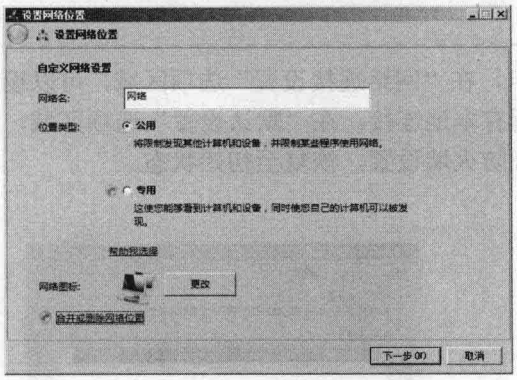

图 1-2 “设置网络位置”窗口

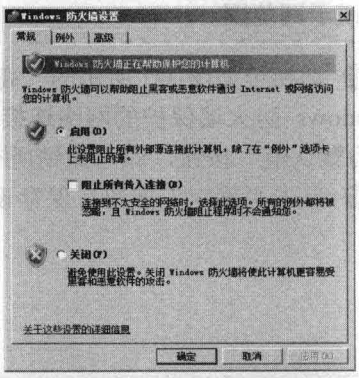

图 1-3 “Windows 防火墙设置”窗口

STEP 03 切换至如图 1-4 所示的“例外”选项卡，或者在“Windows 防火墙”窗口中，单击“允许程序通过 Windows 防火墙”链接。在“程序或端口”列表框选中该服务器欲提供的网络服务即可。

提示：在“高级安全 Windows 防火墙”工具中，也可以查看 Windows 防火墙的“例外”设置。

STEP 04 单击“添加端口”按钮，显示如图 1-5 所示的“添加端口”窗口。在此窗口可以向列表中增加新的网络服务所使用的 TCP 或 UDP 端口。在“名称”文本框中，输入便于识别的名称，如 telnet；在“端口号”文本框中，输入想要添加的端口，如 23；最后，根据需要选择“TCP”或“UDP”端口类型。

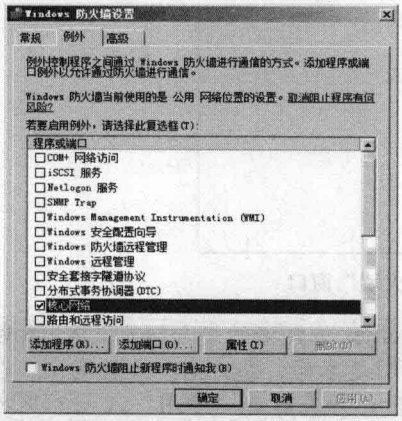

图 1-4 “例外”选项卡

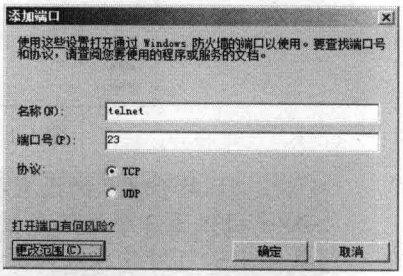

图 1-5 “添加端口”窗口

STEP 05 单击“更改范围”按钮，显示如图 1-6 所示的“更改范围”窗口，指定详细的限定范围可以提高防火墙策略的安全性。默认情况下，开放的防火墙端口适用于任何计算机（包括 Internet 上的计算机）。

提示：点选“仅我的网络（子网）”单选按钮，则开放端口仅适用于本地计算机所在子网，对其他用户仍然关闭；点选“自定义列表”单选按钮，则可以根据需要指定详细的 IP 地址或子网范围。

STEP 06 切换至如图 1-7 所示的“高级”选项卡，在“网络连接设置”选项区域，可以设置接受 Windows 防火墙保护的网络连接，默认为所有本地连接。在“默认设置”选项区域，单击“还原为默认值”按钮，即可撤销所有 Windows 防火墙设置，恢复至初始状态。

STEP 07 单击“确定”按钮，保存设置即可。

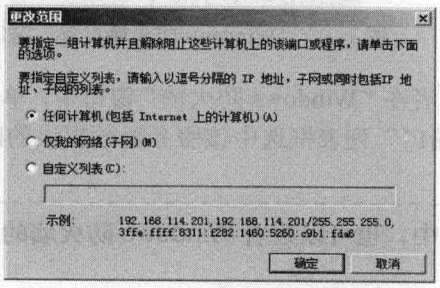

图 1-6 “更改范围”窗口

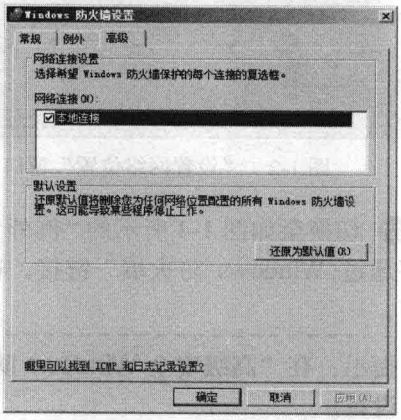

图 1-7 “高级”选项卡