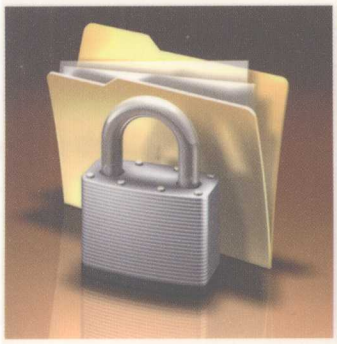
精通

本书为教育部立项课题“学分制下高校网络化教学实践与创新的研究”阶段性成果

Windows Server 2008 安全与访问保护

张晓莉　孙立威　王淑江　编著



本书内容：

服务器操作系统基本配置
用户账户安全配置
常用服务器安全配置
高级安全Windows防火墙和客户端安全配置

随书附赠
多媒体光盘

- 视频演示各项操作
- 提升内容理解层次
- 快速掌握操作方法

本书特点：

使用大量实践操作配合知识讲解
本书内容新颖，重点突出
每章配有小结、习题和实验

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

精通

Windows Server 2008 安全与访问保护

张晓莉　孙立威　王淑江　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书全面阐述了 Windows Server 2008 网络操作系统的安全配置和应用，主要内容包括 Windows Server 2008 操作系统安全概述、活动目录安全、用户账户安全、组策略安全、系统漏洞、端口和网络安全、Internet 信息服务安全、文件安全、Windows 防火墙、系统补丁维护、使用 SCCM 2007 分发客户端更新、证书服务与 SSL 安全协议、Windows 网络访问保护和数据库安全。本书语言流畅、通俗易懂、深入浅出、可操作性强，注重读者实战能力的培养和技术水平的提高，力求让读者通过学习本书，能够最大限度地确保系统能够安全、稳定、高效地运行。

本书适用于系统管理人员、安全管理人员和网络管理人员，以及对计算机系统维护和网络管理感兴趣的计算机爱好者，并可作为大专院校计算机专业的教材或课后辅导资料。

图书在版编目（CIP）数据

精通 Windows Server 2008 安全与访问保护/张晓莉，孙立威，王淑江编著. —北京：中国铁道出版社，2009.6
ISBN 978-7-113-10237-1

Ⅰ.精… Ⅱ.①张…②孙…③王… Ⅲ.服务器—操作系统（软件），Windows Server 2008—安全技术 Ⅳ.TP316.86

中国版本图书馆 CIP 数据核字（2009）第 109328 号

书　　名：精通 Windows Server 2008 安全与访问保护
作　　者：张晓莉　孙立威　王淑江　编著

责任编辑：苏　茜　　**编辑部电话：（010）63583215**
编辑助理：高　爽　　**封面设计：付　巍**
责任印制：李　佳　　**封面制作：白　雪**

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　邮政编码：100054）
印　　刷：北京新魏印刷厂
版　　次：2009 年 9 月第 1 版　　2009 年 9 月第 1 次印刷
开　　本：787mm×1092mm　1/16　印张：32.25　字数：703 千
印　　数：3 500 册
书　　号：ISBN 978-7-113-10237-1/TP・3403
定　　价：68.00 元（附赠光盘）

前言

Foreword

随着社会信息化程度的不断提高，计算机网络已经成为知识经济社会的必要条件和基础设施。但是，由于计算机网络系统自身的开放性以及各个环节不可避免的安全缺陷，安全风险和安全隐患无处不在。人们在享受 Internet 带来的便捷、经济和愉悦的同时，也面临着网络安全方面的巨大挑战。

网络攻击事件之所以频频发生，根本原因还在于操作系统、网络协议、用户等应用环节存在的安全漏洞。信息社会的飞速发展，迫使许多用户来不及经过必要的学习和认知阶段，就匆匆走上了计算机网络应用之路。缺乏网络安全知识，是这类人群的通病，他们平时很少采用系统补丁更新、病毒防火墙和网络防火墙等安全措施。而这些用户无异于高速公路上没有取得驾驶执照的司机，他们随时都可能成为整个网络的网络杀手。只要稍有疏忽或防范不及时，网络安全灾难便如影而至。由此不难看出，系统安全已经成为网络管理员在网络构建、网络升级和网络日常管理中的头等大事。

操作系统是所有计算机资源的管理者，是其他应用程序的基础和核心，一切应用程序都是建立在其之上的，如果没有操作系统的安全，计算机和网络系统安全就无从谈起，更谈不上其他应用软件的安全。因此，操作系统的安全是整个计算机系统安全的基础。随着操作系统版本的不断升级，应用功能越来越丰富，随之而来的安全漏洞也越来越多。其实，许多安全入侵事件都是由于管理员或用户的疏忽导致的，如果合理配置、全面扫描、完善各种审核机制，就可以避免大多数的攻击。

Windows Server 2008 操作系统最突出的改进就是安全性的提升。本书共分为 14 章，主要内容包括 Windows Server 2008 操作系统安全概述、活动目录安全、用户账户安全、组策略安全、系统漏洞、端口和网络安全、Internet 信息服务安全、文件安全、Windows 防火墙、系统补丁维护、使用 SCCM 2007 分发客户端更新、证书服务与 SSL 安全协议、Windows 网络访问保护和数据库安全。本书从 Windows 操作系统安全的角度出发，配合大量实践操作，阐述了操作系统安全配置和管理在网络安全中起到的决定性作用；涉及的服务器和客户端操作系统，分别以目前最新的 Windows Server 2008 和 Windows Vista 为例，内容新颖，重点突出。每章最后配有小结、习题和实验，可以帮助读者巩固本章学过的知识。

本书主要面向具有一定基础的初级网络用户，尤其是热衷于系统安全和网络安全，喜欢探索尝试新技术的计算机爱好者。通过阅读本书，读者可以快速掌握最新的安全技术，最实用的管理技巧以及最常用的安全配置。

本书为教育部立项课题（编号 06JA880017）“学分制下高校网格化教学实践与创新的研究”的阶段性成果，由张晓莉、孙立威、王淑江编著，田俊乐、赵卫东、刘淑梅、马倩、杨伏龙、李文俊、王同明、郭腾、白华、莫展宏、李海宁、陈志成、刘国增、王延杰、刘红等参与了资料收集与调试工作。作者在河北经贸大学、烟台日报长年从事网络教学、实验和管理工作，具有较高的理论水平和丰富的实践经验，曾经出版过多部计算机类图书，均以易读、易学且实用的特点受到众多读者的好评。本书是作者的又一呕心沥血之作，希望对大家的操作系统安全配置与维护工作能有所帮助。

编　者

2009 年 6 月

目　录

第1章 Windows Server 2008 操作系统安全概述

Windows Server 2008 是微软公司继 Windows Vista 之后鼎力推出的新一代服务器操作系统，不仅网络功能强大，而且系统安全性也有了极大提高。使服务器系统安全工作涉及系统内核安全、应用程序安全、用户账户安全和端口安全等多个方面。Windows Server 2008 操作系统允许管理员根据服务器所处环境的不同，启用不同的安全防护策略。

本章导读

- ☑ Windows Server 2008 操作系统安装安全策略
- ☑ 系统服务的安全
- ☑ 用户账户安全
- ☑ 系统设置安全

1.1 Windows Server 2008 操作系统安全策略

Windows Server 2008 操作系统默认提供了多种安全功能，可以为系统程序、服务以及网络访问提供周密的安全防护。不过，在配置 Windows Server 2008 操作系统过程中用户必须注意安全性和易用性之间的矛盾，根据实际需求设置适当的安全级别即可。

1.1.1 操作系统安装注意事项

想要保护好系统安全就要步步为营，安装操作系统是第一步。安装 Windows Server 2008 时应注意以下几点：

- 使用通过正规渠道获得的 Windows Server 2008 操作系统光盘安装，防止安装过程中被植入木马或间谍软件，影响系统安全性和兼容性。
- 列出当前服务器所需的驱动程序、服务组件、杀毒软件、必备工具等，必要时可以事先进行汇总列表。
- 保证硬件设备的可靠性。建议为重要服务器使用磁盘阵列冗余技术，如 RAID0、RAID1 和 RAID5 等，确保服务器存储系统硬件的稳定性和安全性。

- 尽量使用全新方式安装系统，即将操作系统安装在一个全新主分区中，并提前做好合理规划，避免安装完成后重新修改系统配置带来的麻烦。例如，在安装之前应删除系统分区的所有文件，并重新格式化，确保磁盘完好无损。
- 使用 NTFS 文件系统格式化服务器所有磁盘分区，以便为系统分区、数据分区和日志文件分区提供更高的安全性。只有使用 NTFS 文件系统的分区，才能为文件配置 ACL（访问控制列表）访问权限控制，达到保护用户访问安全的目的。
- 没有进行任何安全配置的服务器，不要与任何公共设备或网络连接，必要时可以找一台可以确保安全性的服务器进行连接。
- 只为服务器安装必需的协议，如 TCP/IP，避免其他网络协议给系统带来漏洞。
- 通常情况下，不要将服务器加入到域，应安装成独立服务器模式。
- 为系统管理员设置一个安全性较高的密码。
- 不要在服务器上部署多操作系统，防止恶意用户通过其他系统控制权限获取重要信息，或对 Windows Server 2008 操作系统进行破坏。
- 如果条件允许，建议安装英文版 Windows Server 2008。通常情况下，Microsoft 总是最先发布英文版本的补丁，中文版本的补丁相对滞后一段时间。

1.1.2 配置 Internet 防火墙系统

Internet 防火墙是一道屹立于主机和 Internet 之间的安全屏障，用于防止来自 Internet 或所在局域网的非法访问。防火墙的基本工作原理是，对多种类型的网络通信内容进行过滤。

最常用的基于操作系统的防火墙系统就是 Windows 系统防火墙，此外用户还可以选择其他第三方专业防火墙软件，如天网、瑞星等。建议用户使用系统默认的 Internet 防火墙。

1. Windows 防火墙简介

Windows Server 2008 内置的 Internet 防火墙是一种典型的状态防火墙，不仅可以监视通过它的所有通信，还可以检查所处理的每一条消息的源地址和目的地址。其工作机制如图 1-1 所示。

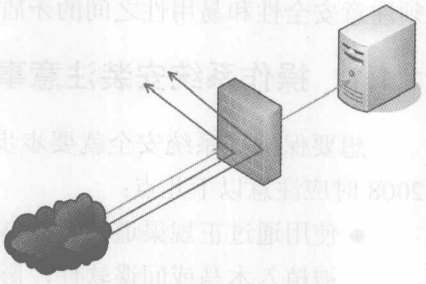


图 1-1 Internet 防火墙

Windows 防火墙就像是一个在计算机和外部 Internet 之间建立的“盾牌”，可以允许请求的数据包通过，而阻止没有请求的数据包进入。启用系统防火墙后，会禁止所有来自 Internet 的未经允许的连接。防火墙使用“网络地址转换器（NAT）”逻辑来验证访问网络或本地主机的入站请求。因此，如果网络通信不是来自受保护的网络内，或者没有创建任何端口映射，则入站数据就被丢弃。

通常情况下，黑客入侵的第一步就是找到所要攻击主机的 IP 地址，再使用 ping 命令建立到该主机的通道，然后对主机进行端口扫描，确定攻击入口。在这种情况下，ping 不

通的 IP 地址，黑客通常认为其没有被使用而忽略过去。因此，Windows 系统防火墙的一个实用功能就是禁止响应 ping 命令，而且还能阻止外部程序对本机进行端口扫描，抛弃所有没有请求的 IP 数据包。

2. 配置 Internet 防火墙

默认情况下，Windows Server 2008 操作系统的防火墙已经启动，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，则默认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。

> **提示：**有关 Windows 防火墙的具体配置，读者可参考本书“第 9 章 Windows 防火墙”中的详细介绍。

3. ICMP 配置

ICMP 主要用于网络控制和诊断，如 ping 命令就是利用该协议中的回显请求功能实现的。ICMP 是一种无连接的协议，即只要发送端完成 ICMP 报文的封装并传递给路由器，该报文即可自动寻找目的地址。因此，ICMP 的一个致命缺点就是易伪造，入侵者通常会使用 ping 命令建立到攻击目标的连接。通过配置 Windows Server 2008 高级防火墙中的相关规则，即可禁止本地主机响应 ping 命令。

01 依次选择“开始”→“管理工具”→“高级安全 Windows 防火墙”命令，打开图 1-2 所示的“高级安全 Windows 防火墙”窗口。

02 单击“入站规则”选项，在“入站规则”窗格中双击“核心网络 – Internet 组管理协议（ICMP-In）”选项，打开图 1-3 所示的“核心网络 – Internet 组管理协议（ICMP-In）属性”对话框。

图 1-2 “高级安全 Windows 防火墙”窗口

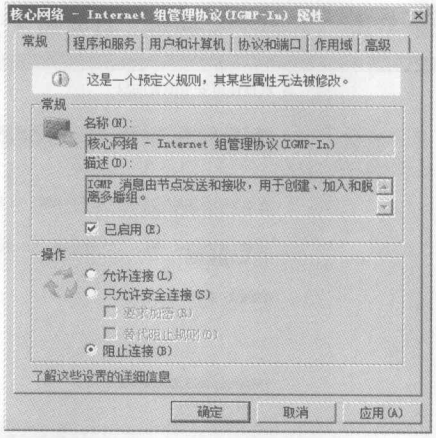


图 1-3　属性对话框

03 在“操作”选项区域中选中“阻止连接”单选按钮。这样就可以阻止本地计算机响应 ping 请求，确保系统安全。

04 单击“确定”按钮，保存设置。