Windows Server 2008系统工程师 视频突击

Windows Server 2008 安全内幕

刘晓辉 李利军 编著

超值赠送 DVD 20小时的Windows Server 2008安全管理视频操作

清华大学出版社

Windows Server 2008 系统工程师视频突击

Windows Server 2008 安全内幕

刘晓辉　李利军　编　著

清华大学出版社
北　京

内 容 简 介

本书全面阐述 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 系统基本安全措施、增强型安全配置、用户账户安全、活动目录安全、组策略安全、文件系统安全、高级防火墙、系统事件和性能监视、数字证书、VPN 连接、NAP、网络应用服务安全等多个方面。通过阅读本书，读者可以快速掌握 Windows Server 2008 系统安全基本配置内容，迅速成长为拥有专业技术的系统安全工程师。

本书可作为大专院校计算机相关专业的教材，也适合具有一定基础的系统管理员和网络管理员阅读。

图书在版编目(CIP)数据

Windows Server 2008 安全内幕/刘晓辉，李利军编著. —北京：清华大学出版社，2009.11
(Windows Server 2008 系统工程师视频突击)
ISBN 978-7-302-21138-9

Ⅰ. W…　Ⅱ. ①刘…　②李…　Ⅲ. 服务器—操作系统(软件)，Windows Server 2003—安全技术　Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字(2009)第 175764 号

责任编辑：张　瑜
装帧设计：杨玉兰
责任校对：王　晖
责任印制：

出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：210×280　　**印　张：**36　　**字　数：**1027 千字
附 DVD 1 张
版　　次：2009 年 11 月第 1 版　　**印　次：**2009 年 11 月第 1 次印刷
印　　数：1~4000
定　　价：66.00 元

前　言

随着全球信息化程度的不断提高，计算机应用已经延伸到每个行业的各个领域，成为人们日常生活中不可或缺的一部分。根据某权威机构调查数据显示，截至 2008 年底，全球正在运行的计算机数量已经超过 10 亿台，中国占大半部分，在未来 5 年时间内，全球计算机数量将超过 20 亿台，并且中国增速会超过其他国家。中国不仅是计算机大国，而且是受病毒侵扰的大国，约有 20%的计算机被植入木马，并被恶意用户所劫持和控制。究其主要原因，大多是用户安全防范意识差所致。

许多人认为 Windows 操作系统是不安全的，其实并非如此。客观地讲，没有绝对安全的操作系统，任何操作系统的安全都是相对的。Linux 和 UNIX 也并非固若金汤，也同样会有系统漏洞，也同样会遭遇各种攻击。Windows Server 2008 已经度过了她一岁的生日，就现在的情况来看，无论安全性还是可靠性都得到了广大用户的认可。网络安全同样适用于 “木桶原理”，即网络安全涉及诸多方面，而最终导致问题出现的往往是安全性最差的那块“短板”。Windows 系统之所以往往充当“短板”角色，原因并不在于操作系统本身的安全架构和设计。即使操作系统本身已经很安全，但因为使用的人缺乏安全意识，也有可能导致操作系统在提高安全性方面所作的全部努力付之东流。

操作系统作为所有计算机资源的“统治者”，是一切应用程序的基础和核心。如果没有操作系统的安全，任何应用和管理都无从谈起。因此，操作系统的安全是整个计算机系统安全的基础。做事效率高当然是件好事，但是如果本末倒置，一切都将归零。不对初装的服务器系统进行安全设置就投入使用，无异于开发商没拿到批文就开工，司机没有取得驾驶证就开车上路，最终结局只有一个——自食恶果。其实，许多安全入侵事件都是由网络管理员或用户的疏忽或疏漏所导致，如果合理配置、全面扫描、完善各种审核机制，完全可以避免大多数的攻击。

相对于 Windows Server 2003，Windows Server 2008 的最大改进就是系统安全性的提升。在继承和发展了原有安全架构的基础上，新推出的 NAP(网络访问限制)技术极大地提高了网络客户接入的安全性，RFM(综合权限管理)可以有效地保护敏感数据的安全，只读域控制器提高了活动目录的安全性，增强型 VPN 连接则能确保用户远程访问的私密性。

全书以系统安全配置为中心，配合大量的操作演示，从多个角度揭开 Windows Server 2008 系统安全的神秘面纱。本书共分为 15 章，主要内容涵盖 Windows Server 2008 系统基本安全措施、增强型安全配置、活动目录安全、防火墙、NAP 等多个方面。其中，重点的网络应用安全，如活动目录、文件服务器、NAP 的内容在本书的篇幅上也有所体现。

本书由刘晓辉、李利军编著，田俊乐、李海宁、赵卫东、刘淑梅、马倩、杨伏龙、李文俊、王同明、石长征、莫展宏、白华、郭腾、王淑江、王春海、陈志成、刘国增、王延杰及刘红等也参与了部分章节的编写工作。作者长期从事网络的搭建、配置和管理工作，具有丰富的网络管理实践经验，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一致好评。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

目　录

第 1 章　Windows Server 2008 初始安全

Windows Server 2008 是 Microsoft 公司的扛鼎之作，是目前功能最强大的网络服务器操作系统，不仅系统和网络功能有了一定的扩展，更重要的是安全性也有了很大提高。Windows Update、Windows 防火墙、安全配置向导、防间谍软件等功能，可以帮助用户做好基本的安全防护工作。若想完全利用这些功能，打造无懈可击的服务器操作系统，就必须详细了解这些功能，并根据需要进行相应的设置。

关键词

- Windows Server 2008 安装安全
- Windows Server 2008 基本安全
- Windows Server 2008 被动防御安全
- Windows Server 2008 系统安全

1.1 Windows Server 2008 安装安全

安装操作系统是一切应用和配置的基础。安装方式的正确与否将直接影响后续安全工作的开展，因此实施安装之前应详细了解 Windows Server 2008 安装注意事项。如果是升级安装方式，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。

1.1.1 系统安装安全指南

安装 Windows Server 2008 时应注意以下几点：

- 使用正版 Windows Server 2008 系统安装光盘，防止安装过程中被植入木马或间谍软件，影响系统安全性。另外，盗版系统安装光盘也可能影响计算机的兼容性，导致一些莫名其妙的问题。
- 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 RAID 5 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干净的系统分区中，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，安装之前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，可以为系统分区、数据分区和日志文件分区提供更高的安全性。NTFS 是真正的日志性文件系统，使用日志和检查点信息，即使在系统崩溃或者电源故障的时候也可以保证文件系统的一致性。只有使用 NTFS 格式的分区才能为文件提供访问权限控制，达到访问控制安全的目的。
- 没有进行任何安全配置的初装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 协议，避免其他网络协议给系统带来的漏洞。
- 通常情况下，不要将服务器加入到域，而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 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，微软公司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 安全补丁更新

安全补丁更新是 Windows 系统必不可少的安全配置。默认情况下，Windows Server 2008 安装完成后，自动更新功能是未配置的，管理员必须开启并指定选择相应的方式，为系统下载、安装补丁更新，以保护系统的安全。主要配置步骤如下。

① 为 Windows Server 2008 配置系统更新之前，每次启动计算机后都会在任务栏的右侧系统托盘中，显示如图 1-1 所示的提示信息。

② 单击此提示信息打开如图 1-2 所示的 Windows Update 对话框。除此之外，在“初始配置任务”

窗口的“更新此服务器”选项区域，以及在“服务器管理器”窗口的“安全信息”选项区域中，同样可以启动 Windows Update 配置向导。

图 1-1　“此时未自动安装更新”提示

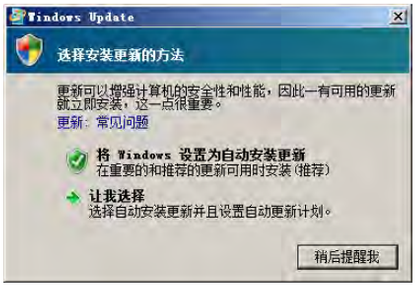

图 1-2　Windows Update 对话框

提示：只有第一次配置自动更新时才会显示该对话框，以后将不再显示。如果要让 Windows 系统自动下载并安装更新，可直接单击“将 Windows 设置为自动安装更新”，完成系统更新配置。

③　单击“让我选择”，打开如图 1-3 所示的“更改设置”对话框。在“选择 Windows 安装更新的方法”中，选择一种安装方法即可，各种安装方式的具体含义如下。

- 自动安装更新(推荐)：服务器连接到 Internet 后，系统将自动检测 Microsoft Update 服务器是否有所需更新，如果有则将自动下载并安装这些更新。选择该单选按钮后还需要指定系统自动安装更新的具体时间。
- 下载更新，但是让我选择是否安装更新：仅下载所需的系统更新，完成后通知用户在合适的时间手动安装。
- 检查更新，但是让我选择是否下载和安装更新：仅检测 Microsoft Update 服务器上提供的更新项目，并以列表方式提示系统管理员，管理员可以根据实际情况选择需要下载的系统更新。建议使用这种方式，可以减少不必要的服务器资源和网络带宽浪费。
- 从不检查更新(不推荐)：关闭系统更新功能，建议不要选择此项。

图 1-3　“更改设置”对话框

1.2 Windows Server 2008 基本安全

Windows Server 2008 基本安全配置包括 Internet 防火墙和安全配置向导。为确保 Windows Server 2008 服务器的安全，安装完成之后应立即启用并配置 Internet 防火墙，以便防止黑客或恶意软件通过网络或 Internet 访问计算机。安装网络服务之后，可以通过安全配置向导有针对性地部署网络访问安全策略。

1.2.1 Internet 连接防火墙

Internet 连接防火墙(Internet Connection Firewall，ICF)是 Windows 系统的内置防火墙，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恶意软件。默认情况下，ICF 是自动开启的。

1. 防火墙简介

Windows Server 2008 的 ICF 是一种典型的状态防火墙，不仅可以监视通过其路径的所有通信，并且检查所处理的每一条消息的源地址和目的地址，工作方式如图 1-4 所示。

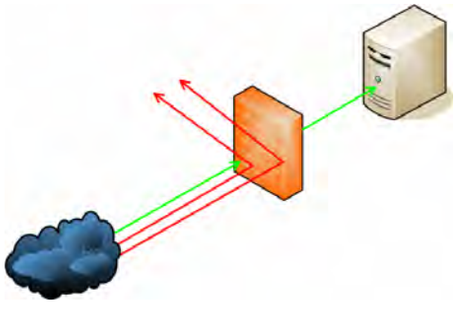

图 1-4 Internet 防火墙的工作方式

ICF 就像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，而阻碍那些没有请求的数据包，因此它是一个动态数据包过滤器。它可以对直接连接 Internet 或连接在运行 ICF 的“Internet 连接共享主机”后的计算机提供保护。启用后，ICF 会禁止所有来自 Internet 的未经允许的连接。为此，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。如果网络通信不是来自受保护的网络内部，或者没有创建任何端口映射，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 ping 通该主机(表示已经与该主机建立了一个通道)，然后对主机进行端口扫描，察看哪些端口是开放的，最后找出系统漏洞进行攻击。如果攻击个人电脑，通常是通过扫描一段 IP 地址开始来锁定目标，这种情况下，ping 不通的 IP 地址通常被认为没有使用而忽略过去。因此，ICF 的第一个功能就是不响应 ping 命令，而且，ICF 还禁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。如此一来，可以被黑客利用的系统漏洞就很少了。

ICF 是通过保存一个表格，记录所有自本机发出的目的 IP 地址、端口、服务以及其他一些数据来达到保护本机的目的。当一个 IP 数据包进入本机时，ICF 会检查这个表格，看到达的这个 IP 数据包是不是本机所请求的，如果是就让它通过，如果在这个表格中没有找到相应的记录就抛弃这个 IP 数据包。

2. 配置 Internet 防火墙

Windows Server 2008 系统的 ICF 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。

① 在 Windows Server 2008 的“控制面板”窗口中，双击“Windows 防火墙”图标，显示如图 1-5 所示的窗口。本例中的 Windows 防火墙已启用。

图 1-5　“Windows 防火墙”窗口

② 单击“启用或关闭 Windows 防火墙”链接，打开如图 1-6 所示的“Windows 防火墙设置”对话框，系统默认选择“启用”单选按钮。如果同时选中“阻止所有传入连接”复选框，则防火墙将阻止所有主动连接当前服务器的尝试，除非需要为该服务器提供最大程度的保护时，才使用该设置，启用该设置后将忽略“例外”列表中的所有设置。通常情况下，不推荐选择该复选框。

③ 单击“例外”或者在“Windows 防火墙”窗口中单击“允许程序通过 Windows 防火墙”链接，则显示如图 1-7 所示的“例外”选项卡，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。

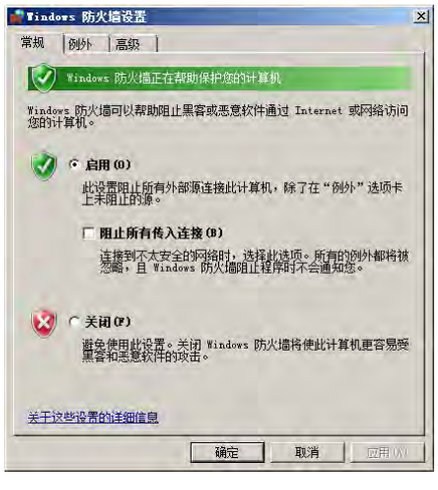

图 1-6　“Windows 防火墙设置”对话框

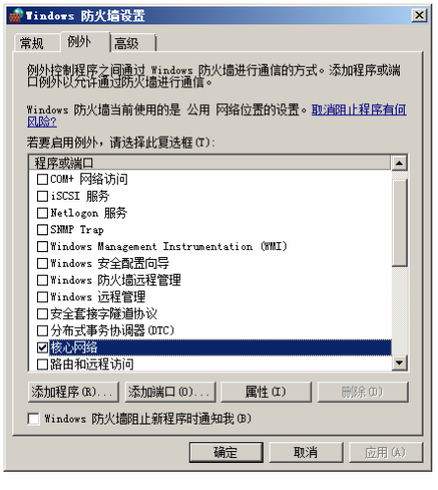

图 1-7　“例外”选项卡

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。

④ 单击“添加端口”按钮，打开如图 1-8 所示的“添加端口”对话框，即可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；根据需要选择 TCP 或 UDP 端口类型。

⑤ 单击“更改范围”按钮，打开如图 1-9 所示的“更改范围”对话框。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)。

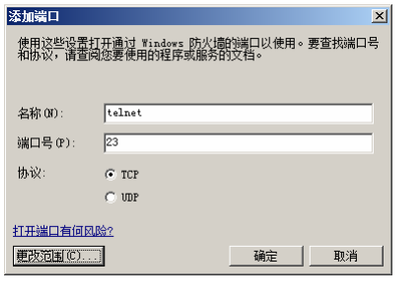

图 1-8 “添加端口”对话框

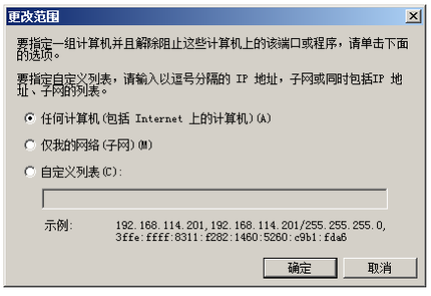

图 1-9 “更改范围”对话框

提示：选择“仅我的网络”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。选择“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。

⑥ 单击“高级”标签，切换至如图 1-10 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。需要注意的是，必须是本地计算机上 Administrators 组的成员，或者是被委派了适当的权限的用户，才可以还原 Windows 防火墙默认设置。如果计算机已经加入到某个域中，则 DomainAdmins 组的成员可以执行该过程。

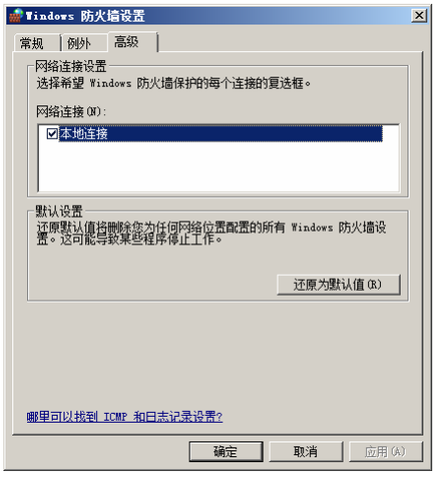

图 1-10 “高级”选项卡

提示：与 Windows Server 2003 的 Internet 防火墙不同的是，“高级”选项卡中的“ICMP”相关设置已被转移到“高级安全 Windows 防火墙”中。

⑦　单击“确定”按钮，保存设置即可。

1.2.2　安全配置向导

安全配置向导(SCW)可以帮助管理员快速完成创建、编辑、应用和回滚安全策略操作。用户可以根据需要创建针对某个服务器角色的安全策略，并且可以将其应用到其他服务器上。配置和应用 SCW 时应注意以下几点：

- SCW 禁用不需要的服务并提供对具有高级安全性的 Windows 防火墙的支持。
- 使用 SCW 创建的安全策略与安全模板不同，其中前者扩展名为.xml，而后者扩展名为.inf。用户创建的安全策略源于安全模板，安全模板包含的安全设置可以应用于所有的服务器角色。
- 部署 SCW 安全策略后并不会影响服务器提供服务时所需的组件，并且应用之后，管理员仍可以通过服务器管理器安装所需的组件。
- 应用 SCW 安全策略之后，SCW 将自动选择所有从属角色。
- 创建和应用 SCW 安全策略时，应确保服务器的 IP 协议及端口配置完全正确。

1. 创建安全策略

①　依次单击“开始”→“管理工具”→“安全配置向导”命令，打开如图 1-11 所示的“欢迎使用安全配置向导”界面。也可以在“开始”菜单的“开始搜索”文本框中输入 SCW 命令，单击“确定”按钮来启动安全配置向导。

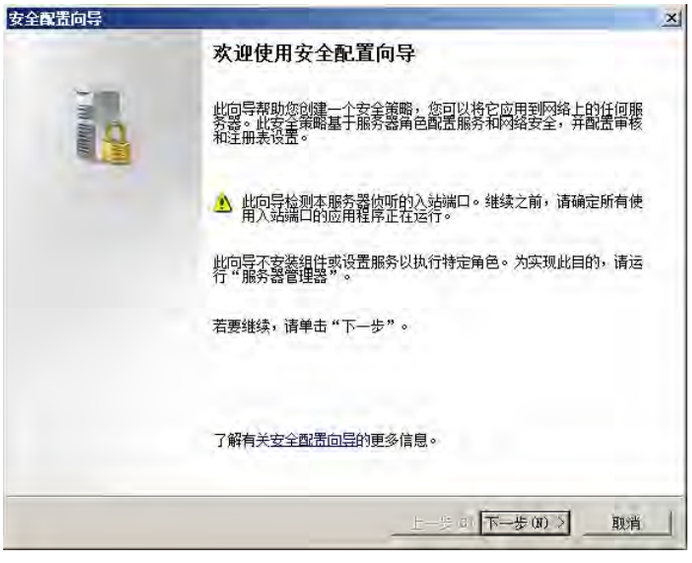

图 1-11　“欢迎使用安全配置向导”界面

②　单击“下一步”按钮，显示如图 1-12 所示的“配置操作”界面。

安全配置向导提供了 4 种配置操作。

- 新建安全策略：可以创建用于配置服务、Windows 防火墙、Internet 协议安全(IPSec)设置、审核