专业网管笔记 · 成就资深网管

网管员必备宝典系列丛书

网管员必备宝典

——网络安全

王文寿 王 珂 编著

清华大学出版社

网管员必备宝典系列丛书

网管员必备宝典——网络安全

王文寿　王　珂　编著

清华大学出版社
北　京

内 容 简 介

本书是一本基于企业安全需求角度编写的网络安全类图书，没有纯粹的深奥难懂的技术原理介绍，只有出于实际安全需求的经验总结和应用配置。本书共9章，第1章从全局角度分析了当前企业网络安全的形势和需求，介绍了网络安全基础知识。第2章到第9章分别介绍一个相对独立的安全技术应用，它们分别是：计算机病毒、木马和恶意软件的清除和防护，防火墙技术的应用，堡垒主机的配置，ISA Server 2004的应用配置，端口扫描和入侵检测应用，网络安全隔离，文件加密和数字签名，以及Windows Server 2003系统的主要安全功能配置。

本书的最大的特点就是实用性、可操作性和系统性非常强，而且基本上覆盖了Windows Server 2003域网络系统的主要网络安全配置。本书可供企业网络管理员参考，以及作为各类培训机构的网络安全和应用培训教程。

图书在版编目(CIP)数据

网管员必备宝典——网络安全/王文寿，王珂编著. —北京：清华大学出版社，2007.5
(网管员必备宝典系列丛书)
ISBN 978-7-302-14993-4

Ⅰ. 网… Ⅱ. ①王… ②王… 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(2007)第047159号

责任编辑：邹　杰　闫光龙
封面设计：付瑞学
版式设计：北京东方人华科技有限公司
责任校对：马素伟
责任印制：何　芊
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
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京市世界知识印刷厂
装 订 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：190×260　**印　张**：34　**字　数**：810千字
版　　次：2007年5月第1版　　**印　　次**：2007年5月第1次印刷
印　　数：1～5000
定　　价：49.00元

丛 书 序

关于本丛书

计算机网络技术经历了二十多年的发展，时至今日不仅其技术本身涉及面已非常广、包括的技术内容非常丰富，而且从职业方面来说也出现了许多专门的分支。网络管理员就是其中一个初级网络类职业，被国家正式以职业的形式认可。目前从就业形势来看，网络管理员的前景非常好，全国那么多企、事业单位，无论大小，至少有一名专业的网络管理员。再加上现在全国大大小小的网吧也是遍布大街小巷，而这些网吧都是初级网管员就业的好场所。

为了使全国千万个热爱网络管理工作的朋友迅速成为真正专业的网络管理员，由清华大学出版社和笔者一起联合推出了这套专门针对网络管理员这一职业技能训练的丛书——《网管员必备宝典》。本丛书是专门针对当前网络管理员这一职业而策划、编写的，主要读者对象是网络维护工程师、网络工程技术人员、信息系统管理人员，以及所有已经或正准备从事网络管理的网络爱好者。本丛书以实用为主要特点，从具体的企事业单位网络管理工作为出发点，全方位满足读者对网络基础知识、网络方案组建、网络应用配置、网络系统管理、网络安全管理、网站开发与维护等方面知识的需求。

本套丛书首批将有6本书推出，它们分别是《网管员必备宝典——网络基础》、《网管员必备宝典——网络组建》、《网管员必备宝典——网络应用》、《网管员必备宝典——Windows Server 2003 网络管理》、《网管员必备宝典——Red Hat Enterprise Linux 4.0 网络管理》和《网管员必备宝典——网络安全》，分别从不同侧面介绍了网络管理员必须掌握的专业知识和技能。

丛书特色

本丛书具有以下主要特色：

1. 系统性

以前许多同类图书，都是属于综合类图书，就是把所有与网络管理有关的知识和技能用一本，或者少数几本图书进行综合介绍。很显然这类书对于想系统地掌握网络管理知识和技能的朋友是不够的。本丛书首批推出的图书就从不同侧面，不同领域，用一本书的篇幅系统地介绍网络基础知识、网络组建、网络应用、网络管理、网络安全方面的专业知识和技能。而且每一本书中都有作者精心组织、内容非常丰富的专业知识，给了相应领域系统的介绍。

2. 针对性

本丛书是专门针对欲以网络管理员为职业的朋友而编写的自学或者培训的教材，所以本丛书中的内容都非常具有针对性，由于本丛书的作者有着多家大型跨国公司十多年大型网络管理经验，并且一直关注着国内外主流网络技术和应用，对当前及将来相当长一段时间内的主流网络技术和应用拥有专业的认识和掌握，所编写的每本书都是十分有针对性。

3. 专业性

图书的专业性不仅体现在图书的内容上，更体现在内容的组织上。好的图书，不仅内容非常专业、深入、不是泛泛而谈，而且在图书的内容组织上逻辑性非常强，符合读者阅读、学习的一般规律。有人说，图书的灵魂就在于内容的组织上，一点儿不错！图书是有思想的，而不是静态的资料汇编。好的图书要能给读者一个系统、全面、深入的解决方案，读者从书中可以得到相应领域和相应范围中全部的、专业的知识和技能，不应在中间出现知识链脱节、知识点跳跃的现象。本丛书的作者无论是在实际的网络管理方面，还是在图书的编写技巧方面，都有着非常丰富、非常成功的经验，这就是本套丛书专业性的根本保障。

4. 实用性

“实用性”就是书中所介绍的内容不仅能在实际的工作中真正用得上，而且还要易学。事实上要真正写出实用性强的图书却并不是那么容易。究其原因，就是作者对相应领域没有一个深入的、全面的掌握，对当前主流的应用不是很了解，或者是因为作者在图书写作方面功力欠缺，不能很好地表达所写内容，读者当然也就无法从中获取所需的知识和技能了。

结束语

要真正使自己成为一个合格的职业网络管理员，就必须对与网络管理工作有关的每一个大的领域都有深入、系统、专业的学习。所以，我们就要针对每一个具体领域用一本书的篇幅系统、深入、专业地介绍各自领域的知识和技能。如本系列中的网络基础(包括网络技术和网络设备两个方面)、网络组建、网络应用、网络管理(分 Windows Server 2003 网络管理和 Linux 网络管理两本)和网络安全共 6 本。这 6 本书全面概括了网络管理员所需掌握的知识和技能，读者通过对这套书的学习就可以得到系统的知识和技能。

前　言

一谈到网络安全，许多朋友，甚至从事网络管理的朋友都认为就是诸如各种各样的黑客攻击，如盗取别人的密码、使某网站瘫痪等。把能黑掉某人的系统或QQ账号、网站等的能力作为自己网络安全方面能力高低的依据。其实这是非常错误的。作为企业网络管理员，要的是能有效部署网络安全系统策略的能力，而不是用几个命令或工具软件把人家的QQ或网站黑掉。即使真的有这方面的能力，就目前来说，我国绝大多数人也只是处于机械地使用一些命令或工具软件来进行所谓的攻击，并没有多少技术含量。

网络安全技术发展至今，网络安全已自成体系，不再是过去那种单一的计算机病毒、木马入侵威胁的时代，各种各样的黑客攻击令人防不胜防。我们需要掌握的是如何利用现有的条件，全面而又系统地堵住各种安全隐患出现的途径，这其中就包括各种诸如计算机病毒、木马、恶意软件等的防护工具，还有诸如防火墙系统的部署、网络安全隔离方法，文件加密与数字签名的应用，还有网络操作系统的底层协议配置、网络系统安全策略部署与配置等。一个完善的安全系统应该是一个封闭系统，系统中的各种措施都是环环相扣的，不能只片面地看到某些方面而忽视另一些方面，任何一环断链都将前功尽弃。如我们虽然有非常庞大、完善的计算机病毒、木马和恶意软件防护系统，可以确保整个网络都没有病毒、木马和恶意软件，但是如果防火墙策略没有部署好，有黑客成功地攻击到了网络系统，轻则可能盗取了某用户的账号和密码，重则使网络服务器瘫痪。这样的网络系统同样是不可靠的。又如，整个网络系统中的绝大多数安全系统都部署得非常完善，可是在用户访问控制方面非常混乱，权限分配不合理，导致一些用户的私有信息被泄露，用户权限被非法改动，一些用户该有的权限没有，而另一些用户不该有的权限却分配了。

本书是从企业网络安全需求的角度编写的，而不是像许多同类图书那样介绍一些在企业网络维护中并不实用的黑客攻击方法。全书共9章，第1章是从全局角度分析当前企业网络安全形势和需求，并介绍了笔者十多年来的一些经验总结。第2章到第9章分别介绍一个相对独立的安全技术应用，它们是：计算机病毒、木马和恶意软件的清除和防护，防火墙技术的应用，堡垒主机的配置，ISA Server 2004的应用配置，端口扫描和入侵检测应用，网络安全隔离，文件加密和数字签名，以及Windows Server 2003系统的主要安全功能配置。虽然不能说全面覆盖了企业网络安全的方方面面，但对于绝大多数企业网络来说，把这几个方面部署好就可以比较全面地满足需求了。

本书具有以下几个方面的显著特点：

- 自成封闭体系。在本书中所介绍的几个方面都是企业网络中最重要的，各安全子系统都是环环相扣，最终可以形成一个环封闭的安全系统的。这样就可以确保读者根据本书所介绍的配置方法配置出比较完善的企业网络安全系统。

- ❖ 可操作性强。本书所介绍的配置方案中，着重强调了各步配置细节。配置方案不仅包括了全面的技术细节，而且还结合丰富的配置图详细地介绍各配置步骤，这样一来，可操作性就比较强。读者根据书中介绍的步骤就可以顺利配置，而不是像一些同类图书那样仅是技术方面的介绍。
- ❖ 技术和方案主流。本书所介绍的各种网络安全技术和方案均是当前最主流甚至最新的，读者阅读本书后不仅可以为自己的企业网络配置完善的网络安全系统，还可以了解当前最主流、甚至最新的安全技术和产品。

本书由王文寿、王珂主笔编写，参加编写和校对的还有张玉龙、陈玉新、孙志辉、张新同、催丹丹、刘力、徐亚军、高莉莎、王新宝、王磊、李梅、李军等，在此一并表示由衷的感谢！限于作者自身水平和时间紧等因素，尽管笔者尽了最大努力，但书中仍可能存在一些错误，敬请读者批评指正，万分感谢！

编　者

目　录

第1章

企业网络安全概述

随着局域网与广域网应用的进一步融合，原来一直被认为是安全地带的企业局域网，现在也不能独善其身了，各种各样的安全威胁同样使得它无处可躲。当然“躲”是“躲”不过的，除非完全隔绝与外界网络的联系，但这在当前信息化时代中是不可能的。况且即使完全不与外网连接，网络安全威胁同样存在，因为安全威胁的来源不仅仅是“网络”，如磁盘(如现在 U 盘、MP3、移动硬盘等)、光盘的使用，线路侦听等同样可以使得企业局域网感染各种病毒、木马或其他恶意程序，也可能使得公司机密数据泄露。面对这一现实，作为企业网络管理员的我们，理应积极地站出来，为公司领导分忧，制定出符合自己公司实际需求并在财力承受范围内的网络安全策略。本书就是从这样的角度出发，全面介绍与企业网络有关的安全策略技术和方案。

本章先从总体上了解当前企业网络所面临的主要网络安全威胁的类型和来源，只有清楚了这些，才能有目的地部署本书后续章节将要介绍的安全策略系统。

本章重点

- 主要网络安全威胁的特点和主要防御方法；
- 常见网络攻击的特征及防御方法；
- 主要企业网络安全认识误区；
- 网络安全策略设计的基本原则；
- 典型的企业网络安全策略；
- 网络安全策略实施的基本步骤。

1.1 企业网络安全概述

随着计算机网络的普及和发展，以及政府和企业信息化建设步伐的加快，现有企业的网络体系结构越来越复杂。复杂的网络结构暴露了众多安全隐患，对网络安全的需求以前所未有的速度迅猛增长。如何使网络安全满足业务的高速推进，成为越来越热门的话题。

安全的网络系统对于现代企业来说是日常办公和业务应用的支撑体系。很多企业曾饱尝网络系统遭受攻击的痛苦，意识到了网络安全的重要性，实施了简单的基于防火墙技术的安全解决策略，但绝大多数企业还处于观望阶段，或者处于一种调研阶段。

尽管企业网络与个人网络所存在的主要安全隐患一样，都是计算机病毒感染、木马和恶意程序的入侵和黑客攻击，但企业网络安全与个人计算机的网络安全相比，安全防护的重要性要高许多。一旦存在这些安全隐患，企业网络的损失可能是无法估计的。毕竟个人用户最多只是个人的计算机系统损坏，或者数据丢失，而对于企业网络远没有这么简单。企业网络一旦受到威胁，就可能使整个网络无法正常工作，服务器系统瘫痪，甚至所有网络数据毁坏或丢失，其损失可能是灾难性的。作为网络管理员，应当根据当前安全形势认清企业网络中主要需要防范的安全隐患，而不要以个人计算机网络安全来概括企业网络安全。

正是基于企业网络安全的重要性，企业网络安全防护成本要远比个人网络高。在个人计算机的网络安全防护中通常只是安装个人版病毒防护程序和软件防火墙，而在企业网络中，仅靠这些是远远不够的。企业网络中通常部署的是硬件防火墙、网络版病毒防护程序和其他诸如入侵检测系统、网络隔离设备等。同时，部署企业网络的容灾系统也是非常必要的，因为它是一切安全防护措施的最后的防线。

在近十年来，网络安全产品从简单的防火墙到具备报警、预警、分析、审计、监测等功能的网络安全系统，在技术上已经实现了巨大进步，也为政府和企业在构建网络安全体系方面提供了更加多样化的选择。但是，网络面临的威胁却并未随着技术的进步而有所抑制，反而使矛盾更加突出，从层出不穷的网络犯罪到日益猖獗的黑客攻击，似乎网络世界正面临着前所未有的挑战。本章先宏观地介绍一下企业网络安全威胁的类型和来源，具体的防御措施将在本书后面各章中进行介绍。

1.2 网络安全威胁的分类与基本对策

“网络威胁”简单地说就是指对网络中软、硬件的正常使用、数据的完整无损，以及网络通信正常工作等造成的威胁。当然这种威胁可大可小，大的可以使整个网络中的 PC 机和服务器处于瘫痪状态，网络数据被无情销毁，可能会使一个公司因此而被迫停产、关闭；小的可能只是网络中某个用户计算机上发现了病毒，造成系统性能下降。

那么，具体有哪些网络威胁呢？其实很简单，如病毒、木马、网络监听、黑客攻击以及包括诸如流氓软件在内的恶意软件等都属于网络威胁的范畴。

这些网络威胁总体来说可分为两大类：一类是主动攻击型威胁，如网络监听和黑客攻击。这些威胁都是对方人为通过网络通信连接进行的。另一类就是被动型威胁(这里仅反映多数情况