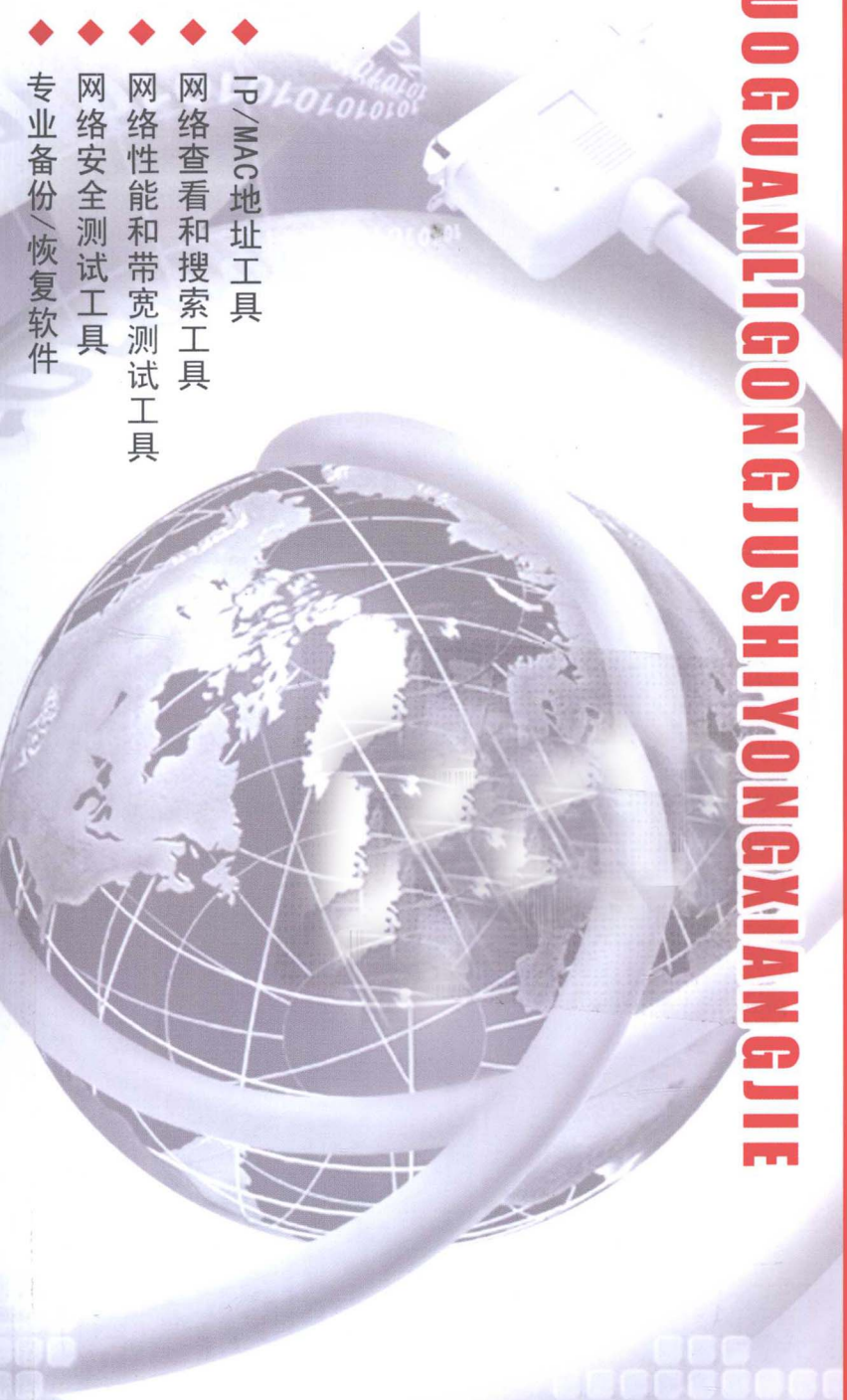
网管天下

# 网络管理工具实用详解（第3版）

WANGLUOGUANLIGONGJUSHIYONGXIANGJIE

张金荣　刘晓辉　编　著

- IP/MAC地址工具
- 网络查看和搜索工具
- 网络性能和带宽测试工具
- 网络安全测试工具
- 专业备份/恢复软件



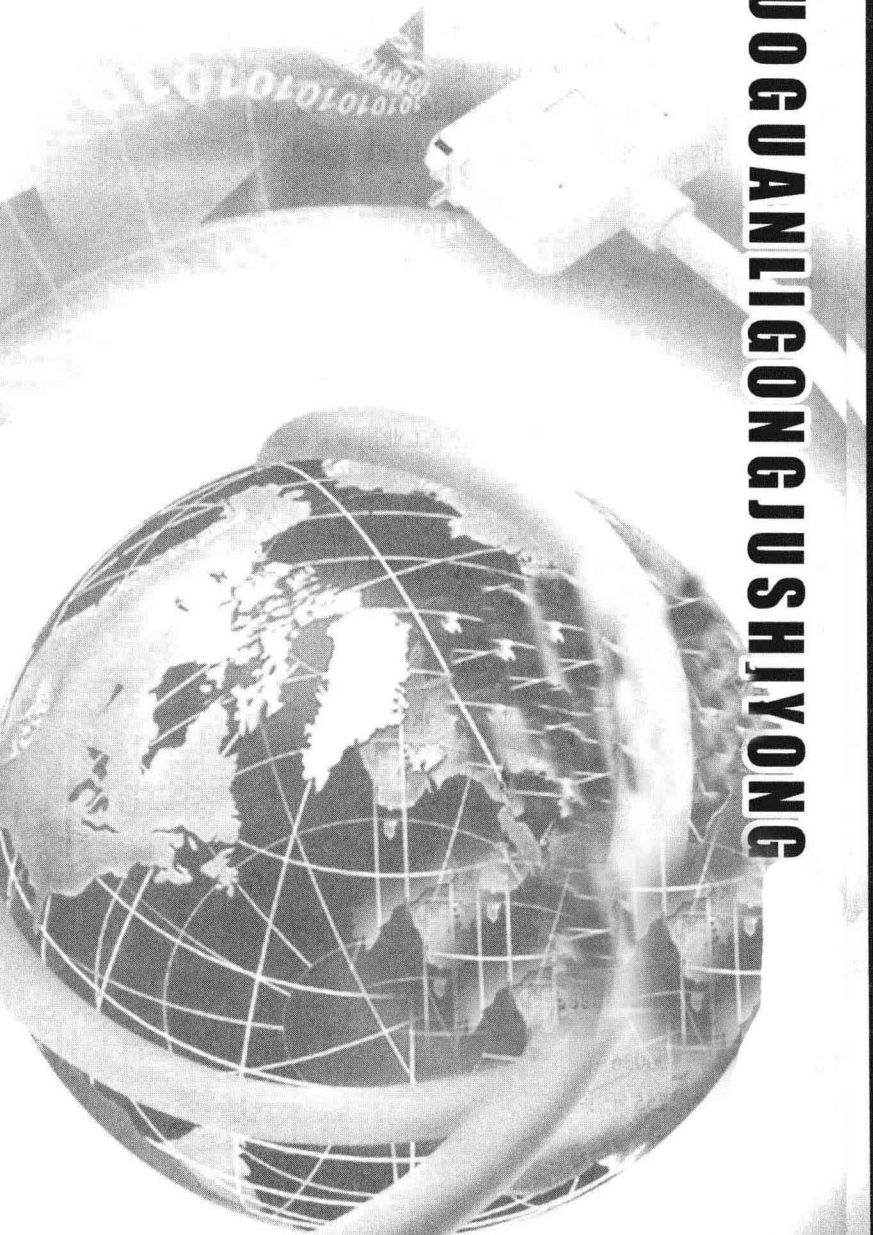
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网管天下

张金荣　刘晓辉　编　著

# 网络安全管理实践（第3版）

WANGLUOGUANLIGONGJUSHIJIYONG



電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

## 内 容 简 介

本书全面深入地介绍了局域网中最常用的安全管理技术及不同类型网络安全方案的规划与设计，主要内容包括服务器系统安全、用户账户安全、共享资源安全、局域网接入安全、局域网传输安全、Internet 接入安全、网络设备安全以及网络数据安全等，基本涵盖了当前主流局域网安全管理涉及的方方面面，可以满足不同领域用户快速打造安全网络的需求。

本书主要面向具有一定基础的中高级用户，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，读者能够全面掌握局域网安全管理的方案设计与实施，提升网络安全技术水平，迅速成长为出色的网络安全管理员和网络安全工程师。

本书为“网管天下”系列《网络安全管理实践》的第 3 版，结合读者反馈意见和建议以及当前网络安全技术发展趋势，在原有基础上补充了大量的新内容、新技术和新案例。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

**图书在版编目(CIP)数据**

网络安全管理实践 / 张栋，刘晓辉编著. —3 版. —北京：电子工业出版社，2012.1
（网管天下）
ISBN 978-7-121-14806-4

Ⅰ. ①网… Ⅱ. ①张… ②刘… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 207906 号

策划编辑：郭鹏飞
责任编辑：鄂卫华
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：31　字数：794 千字
印　　次：2012 年 1 月第 1 次印刷
定　　价：59.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前　言

## 关于《网管天下》丛书

《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》前两版，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，得到了中国台湾出版业同行的认可，在中国台湾也取得了不错的销售业绩。随着网络技术的不断进步，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 3 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，以及最新版本的软件，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。

## 关于本书

网络在方便日常生活，提高工作效率、提升生活质量的同时，也有其危险的一面，轻则

使自己正常的工作、生活和学习受到影响，重则可能会危及财产和生命。由于网络安全事件，致使企业蒙受巨大经济损失的案例屡见不鲜，并且在最近几年正在朝着频率高、数额大的方向发展。相关专家曾经预言，应用与安全将成为网络技术发展的两大方向，网络安全问题已经引起了世界各国的普遍关注，我国正在逐步加大高等教育以及相关技术培训中有关网络安全技术知识的渗透与应用，从最初的专业化向普及化推广发展。

从技术上讲，网络安全是一门涉及计算机科学、网络技术、通信技术、信息加密、网络管理等多个领域的综合性学科。网络安全管理员的基本要求是能够根据既定网络架构给出相应的安全解决方案，随时掌握网络运行情况，能够熟练运用各种安全防护措施确保目标网络的稳定运行。在实际应用中，影响网络安全的因素有很多，除了网络自身的不安全性意外，病毒、人为因素、误操作等各种行为都可能导致漏洞的产生，如果恶意用户趁虚而入将直接威胁网络的安全运行，甚至造成数据丢失和网络瘫痪。

本书由张栋、刘晓辉编著，李海宁、陈志成、田俊乐、王淑江、王春海、赵卫东、刘淑梅、马倩、杨伏龙、李文俊、石长征、王同明、郭腾、白华、刘媛、莫展宏、由磊等也参与了部分章节的编写工作。笔者长期从事网络教学、实验和管理工作，规划、设计、论证、实施并验收过多个大中型网络建设项目，具有较高的理论水平和丰富的实践经验。曾经出版过近百部计算机类图书，均以易读、易学且实用的特点受到众多读者的一致好评。本书是笔者的又一呕心沥血之作，希望能对读者的网络搭建及管理工作有所帮助。

如果您在配置网络和管理网络时遇到了疑问或问题，或者对本书有什么看法，欢迎发送E-mail至hslxh@163.com，进行讨论或寻求支持。由于笔者水平有限，书中难免有疏漏之处，敬请专家和读者不吝赐教。

编著者

2011年7月



此为试读，需要完整PDF请访问：www.ertongbook.com

# 目录

CONTENTS

此为试读,需要完整PDF请访问: www.ertongbook.com

# 第 1 章　网络安全规划与设计

网络安全已经成为企业管理者倍加重视的问题，其重要性是不言而喻的，尤其是知名企业更是如此。许多黑客甚至以攻破某企业网络为荣，尽管这种行为有时只是一场恶作剧，但是大多数网络入侵都意味着企业数据的丢失或网络瘫痪，对企业生产、声誉产生不利影响。计算机网络的安全体系，覆盖网络应用的每个细枝末节，是一套完整的综合应用系统，通常涉及安全风险分析、用户需求评估、安全技术规划和部署以及网络安全管理等方面。

## 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，风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统，引起大范围的瘫痪和损失。另外加上缺乏安全控制机制和对 Internet 安全政策的认识不足，这些风险正日益严重。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，下述安全风险必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。这些安全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。

计算机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，结合局域网络的实际情况，将具体的分析网络的安全风险。

### 1.1.1　物理安全风险分析

物理安全是涉及实现和维护计算机网络物理设备安全的措施，这意味着对管理人员、硬件以及控制信息，在所有状态下的支持系统元素和资源的物理保护，如果攻击者获得被控制设备的物理访问权，就可以绕过对此设备的大多数基于安全技术的控制。

计算机网络物理安全主要是指自然灾害事故、电源故障、人为操作失误或错误、设备被破坏或丢失、电磁干扰、线路截获等方面。除此之外，机房的物理环境及附属设施以及管理人员，也应归于网络物理安全风险范围。

物理安全是整个网络系统安全的前提，在局域网络内，由于网络的物理跨度不大，只要制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险是完全可以避免的。

### 1.1.2 网络平台的安全风险分析

网络应用已经遍布我们生活的每一个角落，网络在给我们的生活带来便利的同时，也暴露其自身的弱点。众多网络功能的实现都是借助网络服务器实现的，而若想使每一个人都能享用这项服务，就必须将服务器放在公开的 Internet 上，每时每刻都可能遭受来自不同用户的攻击和入侵。

对于网络供应商而言，局域网络公开服务器区、特殊服务节点是与外界联系的枢纽，一旦不能运行或受到攻击，将影响集团的业务。同时公开服务器本身要为外界服务，必须开放相应的服务。因此，规模比较大网络的管理人员对 Internet 安全事故做出有效反应变得十分重要。有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

### 1.1.3 系统的安全风险分析

所谓系统的安全，是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任，安全只是一个相对的概念，绝对的安全是不存在的。

在日常应用中，用户可以通过对现有的操作平台进行安全配置、对操作和访问权限进行严格控制，从而提高系统的安全性。首先，不但要选用尽可能可靠的操作系统和硬件平台，而且必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次，应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

### 1.1.4 应用的安全风险分析

应用系统的安全跟具体应用有关，涉及很多方面。应用系统的安全是动态的、不断变化的。应用的安全性也涉及到信息的安全性，同样包括很多方面。

#### 1. 应用系统安全是动态的、不断变化的

应用的安全涉及面很广，以目前 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案就有几十种，但其系统内部的编码甚至编译器导致的 BUG 是很少有人能够发现的，因此一套详尽的测试软件是必须的。但是应用系统是不断发展且应用类型是不断增加的，其结果是安全漏洞也是不断增加且隐藏越来越深。

#### 2. 应用的安全性涉及到信息、数据的安全性

信息的安全性涉及机密信息泄露。未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。由于局域网络跨度不大，绝大部分重要信息都在内部传递，因此信息的机密性和完整性是可以保证的。对于有些特别重要的信息需要对内部进行保密的（比如领导子网、财务系统传递的重要信息）可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。

### 1.1.5 管理的安全风险分析

管理是网络中安全最为重要的部分。责权不明、管理混乱、安全管理制度不健全及缺乏可操作性等都可能会引起管理安全的风险。责权不明、管理混乱，使得一些员工或管理员随便让一些非本地员工甚至外来人员进入机房重地，或者员工有意无意泄露所知道的一些重要信息，而管理上却没有相应制度来约束。

当网络出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

### 1.1.6 其他安全风险

#### 1. 黑客攻击

在计算机网络飞速发展的同时，黑客技术也日益高超。目前黑客能运用的攻击软件已有1000 多种。黑客自己开发或利用已有的工具寻找计算机系统和网络的缺陷和漏洞，并对这些缺陷实施攻击，如软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷和人为的失误等。

发现并实现黑客技术通常要求这个人对计算机和网络非常精通，发现并证实一个计算机系统漏洞可能需要做大量测试、分析大量代码和长时间的程序编写。大部分黑客是利用已有的软件，这并不需要多么高超的技术。如今，Internet 上的黑客站点随处可见，黑客工具可任意下载，从而对网络的安全构成了极大的威胁。

#### 2. 通用网关接口漏洞

黑客可以通用网关接口（CGI）脚本自身的漏洞，执行一些非法任务，通常情况下，这些CGI 脚本所在 WWW 服务器中寻找。要防止这类问题发生，应将这些 CGI 脚本设置为较低级用户特权。提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

#### 3. 恶意代码

恶意代码主要利用本地主机上一些特殊的 Native API 函数和内核系统函数，进行感染、传播和隐藏，从而达到对系统进程、文件、注册表、系统服务和网络服务等进行控制的目的。新形式的恶意代码攻击，大量使用多重加密壳、驱动关联壳、变形壳等代码保护机制和多态和变形等新的技术，传统的恶意代码查杀技术遭到了严重的挑战。

从技术上进行分类，恶意代码使用的技术手段可以分为：

- 用户模式系统调用劫持。
- 核心模式系统调用劫持。

- 核心模式数据篡改。
- 核心模式中断处理程序劫持。

### 4. 病毒

计算机病毒一直是计算机安全的主要威胁。随着计算机技术的不断进步，计算机病毒的发展速度也是非常惊人的，每天网络上都会出现成千上万种新的病毒。大多数病毒都有一定的破坏性，严重的可能导致重要数据丢失、系统瘫痪，甚至硬件损毁。例如，被誉为“2006年十大计算机病毒之首”的“熊猫烧香”，可以在极短的时间内感染本地计算机中所有的可执行文件。

### 5. 不满的内部员工

不满的内部员工（计算机人员、其他工作人员）熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员工能造成更大的损失，例如，可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据等。

### 6. 针对网络的其他手段

一般认为，目前对网络的攻击手段主要表现在如下几方面：

#### ■ 非授权访问

没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。非授权访问主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

#### ■ 信息泄露或丢失

信息泄露或丢失指敏感数据在有意或无意中被泄露出去或丢失，通常包括，信息在传输中丢失或泄露（如“黑客”们利用电磁泄露或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账户等重要信息。），信息在存储介质中丢失或泄露，通过建立隐蔽隧道等窃取敏感信息等。

#### ■ 破坏数据完整性

破坏数据完整性以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

#### ■ 拒绝服务攻击

拒绝服务攻击不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被拒绝而无法进入计算机网络系统或不能得到相应的服务。

#### ■ 利用网络传播病毒

网络是当今计算机病毒的主要传播途径之一，不仅后果严重，而且难于防范。这种传播

方式主要特点是：被病毒感染的计算机会自动扫描所在网络的其他计算机，如果这些计算机也存在这种漏洞，便会被入侵，这些被入侵的计算机会继续扫描攻击……此类病毒传播速度快，在很短时间内感染数台计算机。而且这种病毒会使得多台计算机同时扫描，占用网络的大量带宽，甚至阻塞整个网络的通信。要从根本上杜绝这种安全隐患，首先要在全网计算机中部署杀毒软件，并及时升级，同时必须配合在全网计算机中检查系统漏洞，及时做好系统补丁更新。

## 1.2 安全需求与安全目标

通过对网络结构、网络安全风险分析，再加上黑客、病毒等安全威胁日益严重。解决网络安全问题解决势在必行。针对不同安全风险，必须采用相应的安全措施来解决，从而使网络安全达到一定的安全目标。

### 1.2.1 安全需求

通过前面对局域网络结构、应用及安全威胁分析，可以看出其安全问题主要集中在对服务器的安全保护、防黑客和病毒、重要网段的保护以及管理安全上。因此，必须采取相应的安全措施杜绝安全隐患，应该做到以下几点：

- 公开服务器的安全保护。
- 防止黑客从外部攻击。
- 入侵检测与监控。
- 信息审计与记录。
- 病毒防护。
- 数据安全保护。
- 数据备份与恢复。
- 网络的安全管理。

针对局域网络系统的实际情况，在系统考虑如何解决上述安全问题的设计时应满足如下要求。

- 大幅度地提高系统的安全性（重点是可用性和可控性）。
- 保持网络原有的能特点，即对网络的协议和传输具有很好的透明性，能透明接入，无需更改网络设置。
- 易于操作、维护，并便于自动化管理，而不增加或少增加附加操作。
- 尽量不影响原网络拓扑结构，同时便于系统及系统功能的扩展。
- 安全保密系统具有较好的性能价格比，一次性投资，可以长期使用。
- 安全产品具有合法性，及经过国家有关管理部门的认可或认证。
- 分布实施。

### 1.2.2 网络安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则，该安全策略模型包括了建立安全环境的 3 个重要组成部分。

- 法律规章。安全的基石是社会法律、法规、规章、制度与相应的制裁手段，这部分用于建立一套安全管理标准和方法。即通过建立与信息安全相关的法律、法规和单位的规章制度，使不法分子慑于法律，不敢轻举妄动。
- 先进技术。先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。
- 严格管理。各网络使用机构、企业和单位应建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

### 1.2.3 系统安全目标

局域网络系统安全应该实现以下目标：

- 建立一套完整可行的网络安全与网络管理策略。
- 将内部网络、公开服务器网络和外网进行有效隔离，避免与外部网络的直接通信。
- 建立网站各主机和服务器的安全保护措施，保证系统安全。
- 对网络服务请求内容进行控制，使非法访问在到达主机前被拒绝。
- 加强合法用户的访问认证，同时将用户的访问权限控制在最低限度。
- 全面监视对公开服务器的访问，及时发现和拒绝不安全的操作和黑客攻击行为。
- 加强对各种访问的审计工作，详细记录对网络、公开服务器的访问行为，形成完整的系统日志。
- 备份与灾难恢复，强化系统备份，实现系统快速恢复。
- 加强网络安全管理，提高系统全体人员的网络安全意识和防范技术。

一个合格的网络系统应实现以下安全目标：

- 保护网络系统的可用性。
- 保护网络系统服务的连续性。
- 防范网络资源的非法访问及非授权访问。
- 防范入侵者的恶意攻击与破坏。
- 保护企业信息通过网上传输过程中的机密性、完整性。
- 防范病毒的侵害。
- 实现网络的安全管理。

## 1.3 网络安全规划

不同类型的计算机网络用户，对信息安全要求的级别也是有所不同的。网络安全性的提升是要以巨大的资金投入为基础的，因此，部署计算机网络安全之前，必须了解网络用户的需求，根据其实际情况确定安全系统的主体目标，只有这样才可以制定出一套可靠实用的网络安全系统。

### 1.3.1 网络安全规划原则

在对局域网络系统安全方案设计、规划时，应遵循以下原则。



此为试读，需要完整PDF请访问：www.ertongbook.com