



刘晓辉

编著

网络安全 设计、配置与管理 大全



随书含一张演示光盘，涵盖了书中所有重要的操作，
读者只需根据光盘中的示例操作，即可实现相应的功能。



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>



网络安全 设计、配置与管理 大全



刘晓辉 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书主要介绍计算机网络安全的设计、配置与实施,内容由网络操作系统安全、网络设备安全、网络访问安全和数据存储安全四部分组成,基本涵盖了当前主流的网络应用安全的方方面面。操作系统安全部分,主要以 Windows Server 2008 系统平台为例,穿插介绍 Windows Server 2003 系统中的特有安全功能,可以满足不同类型读者的安全需求。网络设备安全部分,主要介绍 Cisco 路由器、交换机、自适应安全设备和无线设备的安全配置和管理。网络访问安全部分主要介绍目前新型的网络访问控制技术,数据存储安全部分主要介绍网络存储技术。

本书主要面向初级网络管理员,尤其是系统安全和网络安全的爱好者。通读全书,即可解决网络管理工作中遇到的各种安全难题,在提高网络安全的同时,丰富自己的知识,迅速成长为专业的网络管理工程师。

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

网络安全设计、配置与管理大全 / 刘晓辉编著. —北京: 电子工业出版社, 2009.3

(网管宝典)

ISBN 978-7-121-07978-8

I. 网… II. 刘… 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 (2008) 第 196517 号

责任编辑: 顾慧芳

印 刷: 北京京科印刷有限公司

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: 850×1168 1/16 印张: 48.5 字数: 1140 千字

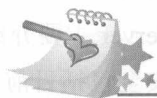
印 次: 2009 年 3 月第 1 次印刷

印 数: 3500 册 定价: 89.00 元 (含光盘 1 张)

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 zltz@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

中国互联网络信息中心（CNNIC）发布的报告显示，截至 2008 年 6 月底止，我国网民数量达到了 2.53 亿，首次大幅度超过美国，跃居世界第一位。近几年来，互联网技术发展迅速，由于用户水平参差不齐，网络安全事件频发，计算机病毒扩散、网络遭黑客攻击、计算机网络犯罪等违法事件的数量迅速增长，网络安全问题已成为人们普遍关注的问题。

随着计算机网络技术的不断发展，开放性、共享性和互联程度也越来越高，网络应用已经遍布社会的每个部门和行业，电子商务、数字货币、网络银行等业务的兴起以及各种专用网（如校园网）的建设，网络系统的安全与保密问题显得越来越重要。目前，全世界每年由于信息系统的脆弱性而导致的经济损失逐年上升，系统的安全问题日益严重。

网络攻击事件之所以频频发生，其根本的原因还在于操作系统、网络设备甚至网络协议本身存在着严重的安全漏洞。只要稍有疏忽或防范不及时，网络安全灾难便如影而至。但随着网络应用越加普及和深入，网络内存储的重要和敏感数据越多；那么核心业务对网络的依赖性越大，人们对网络安全的要求也就越高。由此不难看出，网络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。

在影响计算机网络安全因素的诸多因素中，用户无疑是最重要的因素之一。一方面，网络客户缺乏网络安全知识，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，所有的计算机基本上都在 Internet 这个危机四伏的海洋中裸泳，不断地中招、被劫持、做肉鸡、给其网络用户带来麻烦，甚至导致整个网络的瘫痪。另一方面，网络安全工程师人才匮乏，不能充分借助现有设备和技术构建安全防护屏障，打造固若金汤的局域网络，确保网络内部的用户和数据安全。

本书目的



因此，本书旨在帮助网络管理员，迅速成长为系统安全或网络安全工程师，打造出安全的服务器、安全的网络设备和安全的数据存储。同时，借助各种安全策略和手段，拒绝存在各种安全隐患的用户接入网络，从而有效督促普通用户采用安全措施。只有所有用户都安全了，网络安全才能够得到保障。

本书内容



本书由操作系统安全、网络设备安全、网络访问安全和数据存储安全四个部分共 24 章构成，内容涵盖网络安全的各种技术，从不同角度阐述实现网络安全的意义及实现方式，并配合相关实践操作，帮助用户快速掌握所学技能。操作系统安全包括 Windows Server 2008 和 Windows Server 2003 系统平台，以最新推出的 Windows Server 2008 为主，重点突出新功能的介绍和应用，如用户账户安全、Active Directory 安全、系统事件日志等。网络设备安全包括路由器、交换机、新一代防火墙和无线设备的安

全配置和管理等。网络访问安全包括 VPN 远程访问安全和 ISA Server。VPN 部分的内容可以帮助读者掌握当前主流的 VPN 技术，架设所需类型的远程安全传输。ISA Server 主要介绍 ISA Server 2006 的相关应用，包括安全访问代理、防火墙、服务器发布等。网络存储安全包括目前主流的网络存储、磁盘阵列、数据备份与恢复、磁盘配额等。

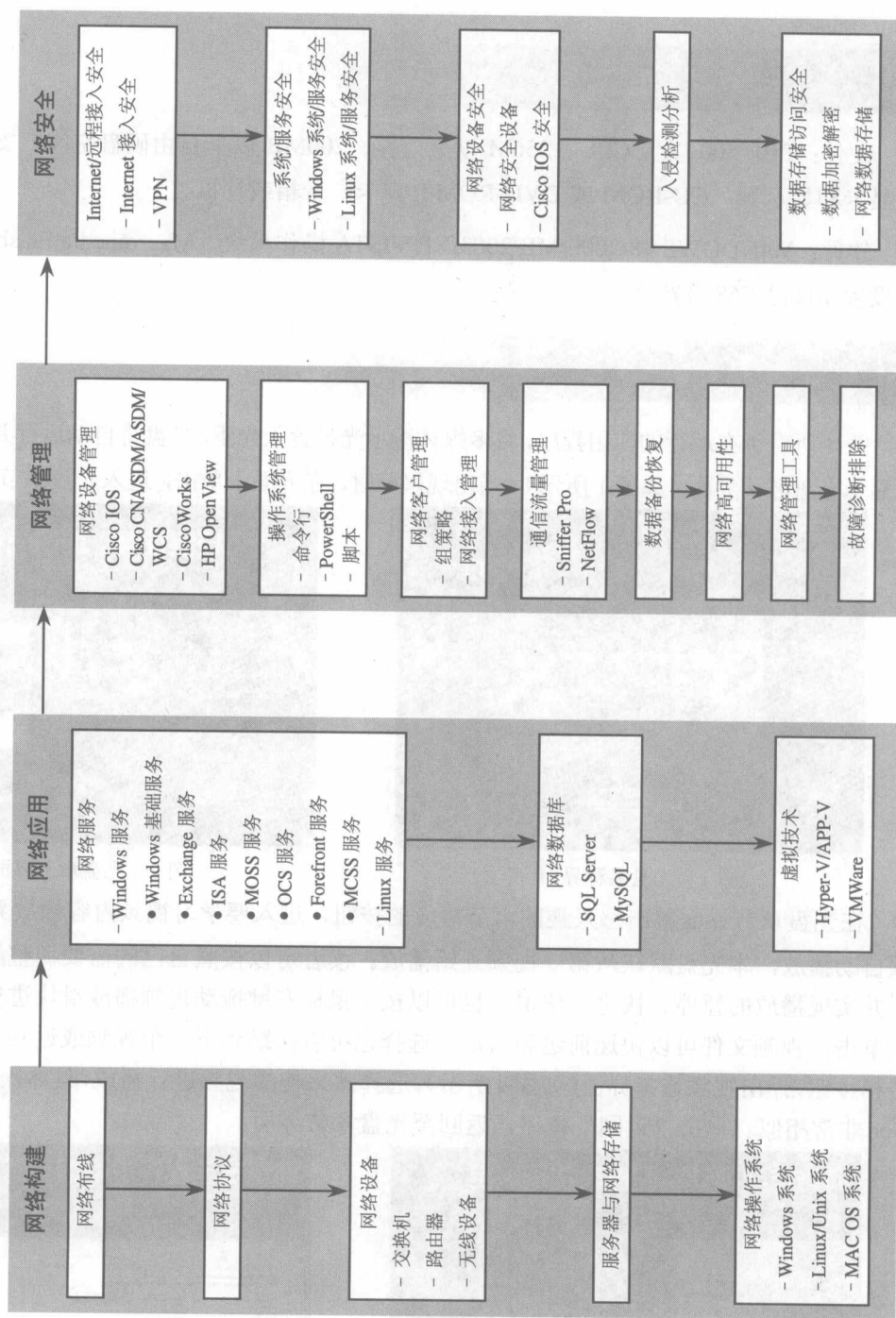
本书由刘晓辉编著，田俊乐、刘淑梅、赵卫东、杨伏龙、李文俊、王同明、石长征、郭腾、白华、李海宁、陈志成、李寅、刘国增、王延杰、刘红、王春海、王淑江等也参与了部分章节的编写工作。笔者长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，曾经出版过三十余部计算机类图书，均以易读、易学、实用的特点，受到众多读者的一致好评。本书是笔者的又一呕心沥血之作，希望对大家的系统维护和网络管理工作能有所帮助。

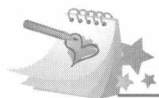
刘晓辉
2008.10



网管宝典学习路线图

笔者就自己对网络管理体系的理解，对网络管理学习者给出一个粗略线路图：





光盘说明

软硬件需要



硬件：PIII 500 以上 CPU、256M 以上内存、200MB 以上自由硬盘空间、支持 1024 X 768 分辨率的显卡和显示器、CD-ROM 或 DVD-ROM、声卡、音箱或耳机。



软件：WINDOWS 98/2000/ME/2003/XP/VISTA 操作系统，Macromedia Flash Player6.0 以上播放器、设置 1024 X 768 分辨率。

操作指南



关闭所有正在运行的应用程序，将多媒体演示光盘置入光驱，光盘将自动运行并播放宣传片头动画，然后显示光盘名称界面（如图 1 所示），当出现鼠标时，在界面上单击，进入光盘章节界面（如图 2 所示）。

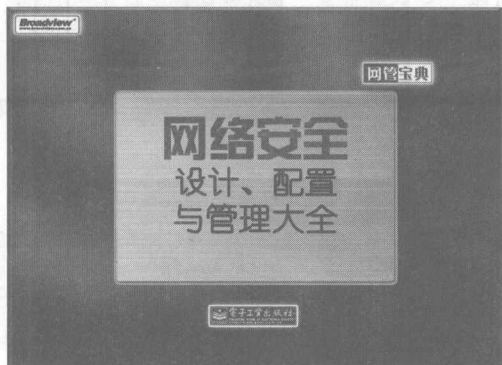


图 1 光盘名称界面



图 2 光盘章节界面



在光盘章节界面单击感兴趣的章节对应的按钮，进入要学习视频内容播放界面（如图 3 所示），视频自动播放，本光盘默认从第一视频开始播放。读者可以按照自己的需要调整解说和背景音乐的音量，并实现播放的暂停、快进、快退，也可以按下鼠标左键拖动视频播放滑块进行快速浏览，在播放条上单击，视频文件可以快速前进和后退。选择也可直接跳到下一个视频或返回上一个视频。点击视频选择按钮，弹出视频选择界面（如图 4 所示），选择感兴趣的视频进行播放，具体操作与 Windows Media Player 非常相似。单击“返回”按钮，返回至光盘章节界面。

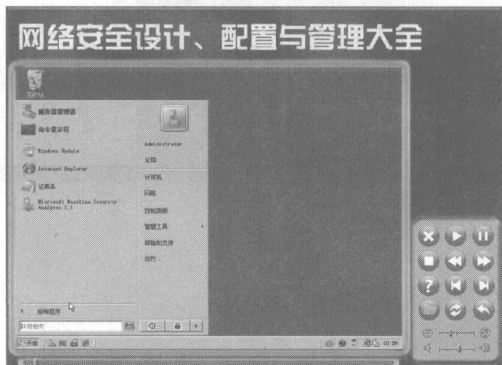


图 3 视频内容播放界面

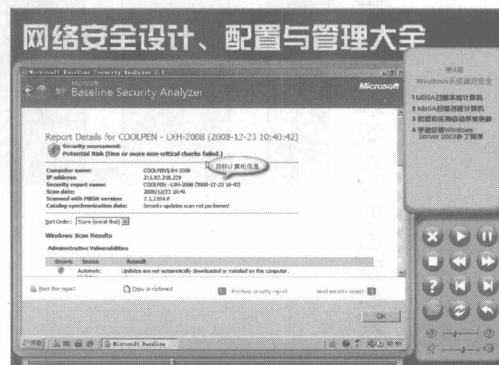


图 4 视频选择界面

 在光盘章节界面和播放界面中，单击“光盘帮助”按钮，显示光盘使用帮助文件（如图 5 所示）。单击返回按钮，返回章节界面。

 单击“退出光盘”按钮，显示光盘的制作团队信息（如图 6 所示），在退出界面上点击鼠标左键将自动结束光盘播放。



图 5 光盘帮助



图 6 退出界面

目 录

第 1 部分 操作系统安全

第 1 章 网络安全概述2

1.1 网络安全基础2

1.1.1 网络安全的含义2

1.1.2 网络安全的属性2

1.1.3 网络信息安全因素4

1.1.4 网络信息安全机制5

1.2 网络系统安全风险分析6

1.2.1 物理安全风险分析6

1.2.2 网络平台的安全风险分析7

1.2.3 系统的安全风险分析7

1.2.4 应用的安全风险分析7

1.2.5 管理的安全风险分析7

1.2.6 其他安全风险8

1.3 安全需求与安全目标9

1.3.1 安全需求9

1.3.2 网络安全策略10

1.3.3 系统安全目标10

1.4 网络安全体系结构10

1.4.1 物理安全11

1.4.2 网络结构规划11

1.4.3 系统安全13

1.4.4 信息安全13

1.4.5 应用安全14

1.5 安全管理14

1.5.1 安全管理规范14

1.5.2 安全管理的功能15

1.6 网络安全技术16

1.6.1 防病毒技术16

1.6.2 防火墙技术17

1.6.3 入侵检测技术18

1.6.4 访问控制技术18

1.6.5 安全扫描技术19

1.6.6 网络安全应急响应体系19

1.7 网络安全的规划与设计20

1.7.1 网络安全规划原则20

1.7.2 划分 VLAN 和 PVLAN21

1.7.3 客户端安全21

第 2 章 Windows Server 2008 初始安全22

2.1 Windows Server 2008 安装安全22

2.1.1 Windows 安装安全指南22

2.1.2 安全补丁更新22

2.2 Windows Server 2008 基本安全配置24

2.2.1 Internet 防火墙24

2.2.2 安全配置向导26

2.3 Windows Server 2008 被动防御安全35

2.3.1 配置防病毒系统35

2.3.2 配置防间谍系统38

2.4 Windows Server 2008 系统安全39

2.4.1 应用程序安全39

2.4.2 系统服务安全39

2.4.3 注册表安全41

2.4.4 审核策略44

2.5 高级安全 Windows 防火墙47

2.5.1 工作原理47

2.5.2 配置防火墙规则47

2.5.3 使用组策略配置高级防火墙49

2.5.4 新建 IPSec 连接安全规则51

第 3 章 Windows 系统漏洞安全55

3.1 漏洞概述55

3.1.1 系统漏洞的特性55

3.1.2 漏洞生命周期56

3.1.3 漏洞管理流程57

3.1.4 漏洞修补策略58

3.2 漏洞扫描58

3.2.1 漏洞扫描概述59

3.2.2 漏洞扫描工具 MBSA59

3.2.3 MBSA 漏洞扫描67

3.3 系统更新72

3.3.1 系统补丁部署原则73

3.3.2	系统更新的实施	73	6.2.2	重设用户密码	164
第4章	Windows 端口安全	80	6.2.3	禁用用户账户	168
4.1	端口概述	80	6.2.4	设置域用户账户登录选项	169
4.1.1	端口分类	80	6.2.5	域用户组安全	171
4.1.2	应用程序和服务端口	81	第7章	Windows 组策略安全	174
4.1.3	端口攻击	82	7.1	组策略模板概述	174
4.1.4	查看使用端口	89	7.1.1	Windows Server 2008 中的 策略模板	174
4.2	配置端口	94	7.1.2	ADMX 模板的特点	174
4.2.1	启动/关闭服务法	94	7.1.3	ADMX 文件编辑方式	175
4.2.2	IP 安全策略法	95	7.2	安全策略	175
4.2.3	禁用 NetBIOS 端口	106	7.2.1	账户策略	176
第5章	Windows 活动目录安全	108	7.2.2	审核策略	181
5.1	活动目录安全管理	108	7.2.3	用户权限分配	185
5.1.1	全局编录	108	7.3	软件限制策略	189
5.1.2	操作主机	110	7.3.1	软件限制策略概述	189
5.1.3	功能级别	117	7.3.2	安全级别设置	190
5.1.4	信任关系	119	7.3.3	默认规则	195
5.1.5	权限委派	127	7.4	IE 安全策略	197
5.1.6	只读域控制器	132	7.4.1	阻止恶意程序入侵	197
5.2	活动目录数据库	135	7.4.2	禁止改变本地安全访问级别	198
5.2.1	设置目录数据库访问权限	136	第8章	Windows 文件系统安全	200
5.2.2	活动目录数据库的备份	136	8.1	NTFS 权限	200
5.2.3	活动目录数据库的恢复	140	8.1.1	NTFS 文件夹权限和 NTFS 文件权限	200
5.2.4	恢复任意时间活动目录 数据库备份	142	8.1.2	访问控制列表	202
5.2.5	使用授权还原模式恢复个别 对象	143	8.1.3	多重 NTFS 权限	203
5.2.6	整理活动目录数据库	145	8.1.4	NTFS 权限的继承性	204
5.2.7	重定向活动目录数据库	147	8.2	设置 NTFS 权限	205
5.2.8	活动目录服务器故障	148	8.2.1	设置 NTFS 权限基本策略 和规则	205
第6章	Windows 用户账户安全	155	8.2.2	取消“Everyone”所有权限	206
6.1	管理员账户安全	155	8.3	高级权限设置	207
6.1.1	更改 Administrator 账户名	155	8.3.1	指定高级访问权限	207
6.1.2	禁用 Administrator 账户	157	8.3.2	复制和移动文件夹对权限 的影响	209
6.1.3	减少管理员组成员	157	8.4	文件审核	209
6.1.4	系统管理员口令设置	158	8.4.1	审核策略	210
6.1.5	加密系统账户数据库	160	8.4.2	设置审核对象	210
6.1.6	删除 Windows Server 2003 系统中 的备份账号数据库	161	8.4.3	NTFS 权限审核	210
6.2	用户账户安全	162	8.4.4	选择审核项的应用位置	212
6.2.1	创建安全用户账户	162	8.5	文件屏蔽	213

8.5.1	创建限制文件组	213
8.5.2	创建屏蔽模板	215
8.5.3	部署文件屏蔽策略	216
8.5.4	文件屏蔽测试	217
8.6	文件压缩和加密	218
8.6.1	NTFS 压缩	218
8.6.2	加密文件系统	220
8.7	删除不安全文件	225
8.7.1	取消系统的文件保护功能	225
8.7.2	注册表安全设置的项目	226
8.7.3	审核部分设置的项目	226
8.7.4	删除不必要的可执行文件	226
8.7.5	删除不必要的可执行程序	226
8.8	NTFS 权限应用实例	226
8.8.1	屏蔽 FlashGet 广告	226
8.8.2	NTFS 权限复制	228

第 9 章 Windows 共享资源安全 230

9.1	共享文件夹权限	230
9.1.1	资源共享方式	230
9.1.2	共享文件夹的权限	231
9.1.3	共享文件夹权限与 NTFS 权限	233
9.1.4	Windows Server 2008 共享和发现	234
9.2	默认共享安全	235
9.2.1	查看默认共享	235
9.2.2	停止默认共享	236
9.2.3	IPC\$	239
9.2.4	设置隐藏的共享	242

第 10 章 Internet 信息服务安全 243

10.1	IIS 安全机制	243
10.1.1	IIS 安装安全	243
10.1.2	IIS 自身安全性	243
10.2	Web 安全	244
10.2.1	用户身份验证	244
10.2.2	授权规则	247
10.2.3	IPv4 地址和域限制	248
10.2.4	端口安全	250
10.2.5	SSL 安全	251
10.2.6	审核 IIS 日志记录	256
10.2.7	设置内容过期	257
10.2.8	.NET 信任级别	258
10.3	FTP 安全	259

10.3.1	NTFS 访问安全	260
10.3.2	设置 TCP 端口	263
10.3.3	连接数量限制	264
10.3.4	用户访问安全	264
10.3.5	文件访问安全	266

10.4 Windows Server 2008/2003

差异化设置	267
10.4.1 内容分级设置	267
10.4.2 获取用于 SSL 加密的服务器证书	267

第 11 章 Windows 事件日志、性能

日志和警报	273
-------	-----

11.1 事件查看器 273

11.1.1 事件基本信息	273
11.1.2 事件的类型	274
11.1.3 事件查看器的使用	274

11.2 安全性日志 287

11.2.1 启用审核策略	288
11.2.2 审核事件 ID	289
11.2.3 日志分析	298

11.3 可靠性和性能 299

11.3.1 监视工具	299
11.3.2 数据收集器集	305
11.3.3 报告	311

11.4 Windows Server 2008/2003

异化设置	312
11.4.1 使用“警报”监控磁盘空间	313
11.4.2 使用“警报”监控密码破解	315
11.4.3 使用“性能日志”监视文件授权访问	315

第 12 章 Windows 客户端安全 318

12.1 Windows Vista 安全 318

12.1.1 客户端安全概述	318
12.1.2 锁定计算机	318
12.1.3 用户账户安全	321
12.1.4 加密文件系统	326
12.1.5 Windows 防火墙	326
12.1.6 系统更新设置	327
12.1.7 Internet Explorer 设置	330
12.1.8 Windows Defender	334
12.1.9 BitLocker 驱动器加密	338

12.2 Windows XP 安全 343

12.2.1	锁定计算机	343	15.1.2	安装 Symantec Endpoint Protection Manager	405
12.2.2	以普通用户运行计算机	344	15.2	部署 Symantec Endpoint Protection 客户端	414
12.2.3	Windows 防火墙	346	15.2.1	安装受管理客户端	414
12.2.4	系统更新设置	348	15.2.2	部署非受管客户端	419
12.2.5	Windows Defender	349	15.3	升级病毒库	421
12.3.1	安装 LiveUpdate 管理工具	421	15.3.1	配置更新	423
12.3.2	配置更新	423	15.3.2	配置 LiveUpdate 策略	430
12.3.3	配置 LiveUpdate 策略	430			
第 13 章	Windows 网络访问保护	351	第 2 部分	网络设备安全	
13.1	NAP 概述	351	第 16 章	网络设备 IOS 安全	434
13.1.1	NAP 系统工作机制	351	16.1	登录密码安全	434
13.1.2	NPS 的功能	352	16.1.1	配置 Enable 密码	434
13.2	部署和配置 NAP 服务	353	16.1.2	配置 Telnet 密码	435
13.2.1	安装 NPS	353	16.1.3	配置管理用户	436
13.2.2	修改 DHCP 相关选项	355	16.2	配置命令级别安全	437
13.2.3	配置 NPS 策略	357	16.2.1	配置多个用户级别	437
13.3	部署 NAP 客户端	363	16.2.2	登录和离开授权级别	438
13.3.1	配置 NAP 客户端	363	16.3	终端访问限制安全	438
13.3.2	测试 NAP 客户端	365	16.3.1	控制虚拟终端访问	438
第 14 章	Windows 系统更新服务	367	16.3.2	控制会话超时	439
14.1	WSUS 概述	367	16.4	SNMP 安全	439
14.1.1	WSUS 3.0 功能和特点	367	16.4.1	配置 SNMP 字符串	440
14.1.2	部署 WSUS 服务器的重要性	368	16.4.2	配置 SNMP 组和用户	440
14.1.3	WSUS 的体系结构	368	16.4.3	SNMP 配置实例	441
14.2	WSUS 服务端部署	369	16.5	HTTP 服务安全	442
14.2.1	WSUS 服务器需求	369	16.5.1	关闭 HTTP 服务	442
14.2.2	准备工作	370	16.5.2	配置安全 HTTP 服务	443
14.2.3	WSUS 服务器端的安装和配置	372	16.5.3	配置安全 HTTP 客户端	444
14.2.4	WSUS 服务器的常规选项设置	379	16.6	系统安全日志	444
14.3	WSUS 客户端配置	383	16.6.1	日志信息概述	444
14.3.1	安装 WSUS 客户端	383	16.6.2	启用系统日志信息	447
14.3.2	通过本地策略配置客户端	385	16.6.3	设置日志信息存储设备	447
14.3.3	客户端获取并安装更新	386	16.6.4	配置日志消息的时间戳	448
14.4	WSUS 服务应用和管理	386	16.6.5	配置日志序列号	449
14.4.1	执行服务器同步操作	387	16.6.6	定义消息严重等级	449
14.4.2	计算机及分组管理	388	16.6.7	限制日志发送到历史表和 SNMP	450
14.4.3	更新的管理	391	16.6.8	配置 UNIX 系统日志服务器	450
14.4.4	监视 WSUS 服务器和客户端状况	398	16.7	IOS 系统版本升级	451
14.4.5	设置特殊文件发布	400			
第 15 章	Windows 防病毒服务	402			
15.1	Symantec Endpoint Protection 企业版的安装	402			
15.1.1	Symantec 产品简介	402			

16.7.1	备份系统软件映像	451	17.6.5	修改安静周期	500
16.7.2	恢复或升级系统软件映像	452	17.7	配置 SPAN 和 RSPAN	500
第 17 章	Cisco 交换机安全	455	17.7.1	SPAN 和 RSPAN 简介	501
17.1	访问列表安全	455	17.7.2	SPAN 和 RSPAN 默认配置	502
17.1.1	访问列表概述	455	17.7.3	SPAN 会话中的流量监视限制	502
17.1.2	IP 访问列表	457	17.7.4	配置本地 SPAN	503
17.1.3	时间访问列表	461	17.7.5	配置 RSPAN	506
17.1.4	MAC 访问列表	463	17.7.6	显示 SPAN 和 RSPAN 状态	509
17.1.5	创建并应用 VLAN 访问列表	464	17.8	配置 RMON	509
17.2	基于端口的传输控制	465	17.8.1	默认的 RMON 配置	509
17.2.1	风暴控制	465	17.8.2	配置 RMON 警报和事件	510
17.2.2	流控制	467	17.8.3	创建历史表组项	511
17.2.3	保护端口	468	17.8.4	创建 RMON 统计组表项	511
17.2.4	端口阻塞	469	17.8.5	显示 RMON 的状态	512
17.2.5	安全端口	469	17.9	使用 Cisco CNA 配置安全	512
17.2.6	传输速率限制	473	17.9.1	CNA 可管理的设备简介	512
17.2.7	MAC 地址更新通知	476	17.9.2	Cisco CNA 安全导向	513
17.2.8	绑定 IP 和 MAC 地址	479	17.9.3	配置端口安全	516
17.3	动态 ARP 检测	479	17.9.4	配置 ACL	518
17.3.1	默认动态 ARP 检测配置	479	第 18 章	Cisco 路由器安全	520
17.3.2	动态 ARP 检测的配置方针	480	18.1	路由器 ACL 安全	520
17.3.3	在 DHCP 环境下配置动态 ARP 检测	480	18.1.1	Cisco 路由器 ACL 配置	520
17.3.4	在无 DHCP 环境下配置 ARP ACL	481	18.1.2	配置路由器 ACL 蠕虫病毒 限制	520
17.3.5	限制 ARP 数据包的速率	482	18.1.3	配置路由器 ACL 限制 P2P 下载	521
17.3.6	运行有效检测	482	18.2	网络地址转换	522
17.3.7	配置日志缓冲	483	18.2.1	NAT 概述	522
17.3.8	显示动态 ARP 检测信息	483	18.2.2	静态地址转换的实现	523
17.4	VLAN 安全	484	18.2.3	动态地址转换的实现	524
17.4.1	VLAN 概述	484	18.2.4	端口复用地址转换	525
17.4.2	划分 VLAN	485	18.3	路由器物理访问安全	526
17.4.3	设置 VLAN Trunk 过滤	488	18.3.1	管理人员控制	527
17.5	私有 VLAN 安全	489	18.3.2	控制 CON 端口	527
17.5.1	PVLAN 概述	490	18.3.3	禁用 AUX 端口	528
17.5.2	配置 PVLAN	491	18.3.4	权限分级策略	528
17.6	基于端口的认证安全	495	18.4	网络服务和路由协议安全	528
17.6.1	IEEE 802.1x 认证简介	495	18.4.1	路由器网络服务安全	528
17.6.2	配置 IEEE 802.1x 认证	498	18.4.2	路由器路由协议安全	530
17.6.3	配置交换机到 RADIUS 服务器的通信	499	18.5	网络加密协议	532
17.6.4	配置重新认证周期	499	18.5.1	使用 IKE 建立安全联盟配置	532
			18.5.2	使用手工方式建立安全联盟	533
			18.6	网络攻击安全防范	534

18.6.1	IP 欺骗防范	534
18.6.2	SYN 淹没防范	535
18.6.3	Ping 攻击防范	536
18.6.4	DoS 和 DDoS 攻击防范	537
18.7	使用 SDM 配置路由器安全	537
18.7.1	Cisco SDM 简介	537
18.7.2	配置路由器安全	539
第 19 章	Cisco 无线网络安全	540
19.1	无线网络设备安全	540
19.1.1	无线接入点安全	540
19.1.2	无线路由器安全	549
19.2	IEEE 802.1x 身份认证	555
19.2.1	部署 IEEE 802.1x 认证	555
19.2.2	无线访问认证配置步骤	555
19.2.3	配置 Cisco 无线 AP	556
19.3	无线网络客户端安全	556
19.3.1	对等网络无线安全	556
19.3.2	接入点无线客户安全	563
19.4	使用 WCS 配置无线网络安全	567
19.4.1	WCS 系统需求	567
19.4.2	WCS 应用	568
第 20 章	Cisco 安全设备	572
20.1	网络安全设备概述	572
20.1.1	网络防火墙	572
20.1.2	入侵检测系统	575
20.1.3	入侵防御系统	576
20.1.4	漏洞扫描	581
20.2	网络安全设计	582
20.2.1	防火墙设计	582
20.2.2	入侵检测设计	585
20.2.3	入侵防御设计	587
20.2.4	综合安全设计	589
20.3	Cisco ASDM 配置	589
20.3.1	Cisco ASDM 简介	589
20.3.2	Cisco ASDM 初始化	592
20.3.3	配置 DMZ	593
20.3.4	管理安全设备	599
20.4	网络访问控制	602
20.4.1	ACL 使用规则	602
20.4.2	将 Conduit 转换成 ACL	603
20.4.3	ICMP 命令使用	604
20.4.4	ACL 配置实例	604

第 3 部分 网络访问安全

第 21 章	VPN 远程访问安全	608
21.1	VPN 概述	608
21.1.1	VPN 简介	608
21.1.2	VPN 的特点与应用	608
21.1.3	VPN 的类型与适用	610
21.2	借助路由器实现 VPN	613
21.2.1	路由器硬件和软件限制	613
21.2.2	路由器 VPN 设置	613
21.3	借助网络防火墙实现 VPN	615
21.3.1	借助 Cisco PIX 实现 VPN	615
21.3.2	借助 Cisco ASA 5510 实现 VPN	622
21.4	借助 Windows Server 实现 VPN	631
21.4.1	搭建 VPN 服务器	631
21.4.2	VPN 服务器端的设置	636
21.4.3	VPN 客户端的配置	644
第 22 章	Internet 访问安全	646
22.1	ISA Server 2006 概述	646
22.1.1	ISA Server 2006 简介	646
22.1.2	理论知识准备	648
22.1.3	ISA Server 的部署与应用	650
22.2	Internet 连接配置	656
22.2.1	允许内网计算机使用主机的 DHCP 服务器	657
22.2.2	允许内网使用 ping 命令	659
22.2.3	允许内网计算机访问外部 Web 站点	660
22.2.4	允许内网访问外部 FTP 服务器	661
22.2.5	允许本地主机访问外网	662
22.2.6	允许内网计算机使用 QQ、UC 等 聊天软件	663
22.2.7	禁止访问某些网络	666
22.2.8	禁止使用第三方的代理服务器	668
22.2.9	修改访问规则	669
22.2.10	阻止 BT 类软件	671
22.2.11	阻止某些文件	672
22.3	发布服务器	673
22.3.1	发布 Web 服务器	673
22.3.2	发布 FTP 服务器	677
22.3.3	发布邮件服务器	679
22.3.4	发布 Exchange 的 OWA 服务	680
22.3.5	发布 SQL Server 服务器	682

22.3.6	发布终端服务器	683
22.3.7	发布安全 Web 服务器	683
22.3.8	为 Internet 用户提供代理服务	684
22.4	实现安全 VPN 访问服务	685
22.4.1	在 ISA Server 中启用 VPN	
22.4.1	服务器	685
22.4.2	检查与配置 VPN 服务器	688
22.4.3	用户管理与设置	688
22.5	高效访问 Internet	689
22.5.1	启用缓存	689
22.5.2	创建正向缓存	690
22.5.3	禁止反向缓存	692
22.5.4	禁止对某些站点缓存	693
22.6	ISA Server 2006 的备份与恢复	693
22.6.1	备份防火墙策略	694
22.6.2	备份 ISA Server 2006 的 所有配置	695
22.6.3	恢复 ISA Server 2006 的配置	696

第 4 部分 数据存储安全

第 23 章	网络数据存储安全	700
23.1	网络存储	700
23.1.1	DAS	700
23.1.2	NAS	701
23.1.3	SAN	704
23.1.4	虚拟存储	706

23.1.5	磁盘阵列	707
23.2	RAID 的实现	712
23.2.1	RAID 卡管理	713
23.2.2	Windows Server 2008 RAID 5 的设置	714
23.3	数据备份和恢复	716
23.3.1	备份数据	716
23.3.2	恢复数据	721
23.4	磁盘配额	723
23.4.1	磁盘配额的功能	723
23.4.2	磁盘配额管理	724
23.4.3	监控每个用户的磁盘配额 使用情况	726

第 24 章 数据流量监控与分析 727

24.1	网络流量监控利器—— Sniffer Pro	727
24.1.1	Sniffer Pro 安装与配置	727
24.1.2	Sniffer Pro 的监控模式	730
24.1.3	创建过滤器	737
24.1.4	Sniffer 的使用	740
24.1.5	应用实例	746
24.2	网络流量分析利器——MRTG	751
24.2.1	MRTG 简介	751
24.2.2	网络设备和服务器的准备	752
24.2.3	监控计算机上的 MRTG 配置	755
24.2.4	监控服务器设置	757

第 1 部分 操作系统安全

- 第 1 章 网络安全概述
- 第 2 章 Windows Server 2008 初始安全
- 第 3 章 Windows 系统漏洞安全
- 第 4 章 Windows 端口安全
- 第 5 章 Windows 活动目录安全
- 第 6 章 Windows 用户账户安全
- 第 7 章 Windows 组策略安全
- 第 8 章 Windows 文件系统安全
- 第 9 章 Windows 共享资源安全
- 第 10 章 Internet 信息服务安全
- 第 11 章 Windows 事件日志、性能日志和警报
- 第 12 章 Windows 客户端安全
- 第 13 章 Windows 网络访问保护
- 第 14 章 Windows 系统更新服务
- 第 15 章 Windows 防病毒服务

第1章 网络安全概述

通常情况下,“安全”是指抵抗风险的能力和状态,意味着受到保护,免受那些有意或其他方式产生危害的攻击。网络安全系统是指保障计算机网络通信免受来自各方面的入侵或攻击的整体系统,通常包括系统安全、访问安全、接入安全、存储安全、设备安全等方面。随着网络应用的不断扩展,人们对网络安全的要求也不断提高,甚至许多国家的政府部门都不惜投入大量的人力、物力和财力,来提高计算机网络系统的安全性。

1.1 网络安全基础

计算机网络是地理上分散的多台计算机互联的集合,借助相关的通信协议和网络链路实现资源共享和网络通信。计算机网络的脆弱性是伴随计算机网络一同产生的,换言之,安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中,网络特性决定了不可能无条件、无限制地提高其安全性能。

1.1.1 网络安全的含义

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,不受任何破坏、更改和泄露,确保系统能连续可靠正常运行,确保网络服务不中断。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。为了保证计算机网络的安全性,通常需要从计算机安全、链路传输安全、网络应用和服务安全等多方面入手。

计算机网络安全之所以如此重要,其主要原因在于:

- 存储和处理重要信息的政府部门的计算机,往往直接关系到国家政治稳定、经济兴衰、军事国防等领域,而这些重要机密信息往往成为不法分子、敌对势力热衷的攻击目标。
- 随着计算机系统功能的不断扩展,系统组成越来越复杂、系统规模越来越大,特别是 Internet 的迅猛发展,存取控制、逻辑连接数量不断增加,软件规模空前膨胀,任何隐含的漏洞都可能造成巨大的损失。
- 人们对计算机系统的依赖性越来越强,甚至在有些领域这种依赖已经无法替代。
- 计算机应用人员技术水平有限,教育和培训却往往跟不上知识更新的需要,操作人员、编程人员和系统分析人员的失误和缺乏经验,都会造成系统的安全功能不足。
- 计算机网络安全问题涉及许多学科领域,如自然科学、社会科学、密码学等。就计算机系统的应用而言,安全技术涉及计算机技术、通信技术、存取控制技术、检验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄漏技术等。因此,它是一个非常复杂的综合问题,并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。
- 对网络安全问题重视程度不够,广泛存在着重应用轻安全、质量法律意识淡薄、计算机素养不高的问题。计算机系统的安全是相对不安全而言的,许多危险、隐患和攻击都是隐藏的、潜在的、难以明确却又是广泛存在的。

1.1.2 网络安全的属性

从本质上来讲,计算机网络安全就是网络上的信息安全。凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全具有以下几个基本属性。