

**Windows Security
Strategy and Implementation
Handbook**

Windows安全

应用策略和 实施方案手册

程迎春 编著

- ✓ Windows 活动目录的安全设计和配置
- ✓ Windows 域和操作系统的安全管理
- ✓ Windows 网络安全管理和应用
- ✓ Windows CA 和证书的部署与应用
- ✓ IIS 5.0/IIS 6.0 的安全管理和应用
- ✓ ISA Server 2000 的管理和应用
- ✓ ISA Server 2004 新特性的应用
- ✓ SUS 2.0/SMS 2003 补丁管理
- ✓ 恶意软件防杀
- ✓ 安全审核与监测

书中给出了大量的
参考链接和下载地址，
包括微软官方提供的技术文档、
实用工具、补丁与更新等信息，
方便读者进行查阅和研究。

Windows Security
Strategy and Implementation
Handbook

Windows安全

应用策略和 实施方案手册

程迎春 编著



人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目 (CIP) 数据

Windows 安全应用策略和实施方案手册 / 程迎春编著. —北京: 人民邮电出版社, 2005.5

ISBN 7-115-13165-1

I. W... II. 程... III. 窗口软件, Windows—安全技术 IV. TP316.7

中国版本图书馆 CIP 数据核字 (2005) 第 042184 号

内 容 提 要

本书共分 10 章, 分别从活动目录安全管理、Windows 网络安全、公钥架构配置和应用、IIS 的安全使用、ISA Server 防火墙应用、补丁维护与病毒防护、安全审核与监测等方面全面系统地阐述了 Windows 安全问题, 对 Windows 安全所涉及的主要产品和组件进行了详细的剖析和安全应用管理指导。本书涉及的具体产品和组件包括 Windows 2000、Windows 2003、CA (PKI)、IIS 5.0、IIS 6.0、ISA Server 2000、ISA Server 2004、SUS 和 SMS Server 2003 等。

本书内容全面、系统且实用, 不仅介绍了 Windows 系统的安全管理技术, 还以实际应用为背景, 提供了大量的安全应用方案, 并详细介绍了相关的配置方法和技巧, 为用户掌握并实施 Windows 安全应用与管理提供了有力的支持。本书中的很多应用案例都是作者多年实际经验的总结, 具有相当的指导意义和参考价值。

Windows 安全应用策略和实施方案手册

- ◆ 编 著 程迎春
责任编辑 杜 洁
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67132692
北京密云春雷印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本: 787×1092 1/16
印张: 41.25
字数: 1006 千字
印数: 1—5 000 册
- 2005 年 5 月第 1 版
2005 年 5 月北京第 1 次印刷

ISBN 7-115-13165-1/TP · 4495

定价: 69.00 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

前言

写这本书的理由

现代办公已经离不开 IT 系统，一个不能保障安全的 IT 系统意味着机密泄漏、生产力破坏和经济损失。软件厂商和客户试图在软件设计、系统部署、系统管理与应用等各个环节中解决一系列安全问题，以实现全程护航。安全已经成为一个越来越热门的话题，人们无法承受安全风险之重，则要接受保护 IT 系统安全的挑战。

微软产品现已广泛地应用在各种规模的 IT 系统中，这使得微软产品的安全管理和应用受到格外的关注。特别是近年来，一些影响深远的病毒在微软产品中爆发，使得无论是微软公司还是产品用户都在不断地加强微软系统的安全性。

对于实际的复杂应用环境，Windows 安全已不再是孤立的 Windows 产品自身安全问题，它应该是一个涵盖 Windows 应用管理体系的多方位解决方案。但由于微软系统广泛而复杂，安全地配置和应用 Windows 以及相关系统确实是件煞费苦心的事情。

根据本人过去在微软产品技术支持部门和大规模 IT 管理部门的工作经验，很多用户都希望能够得到一些实用、具体的指导，真正将安全贯穿于系统设计、部署、维护 IT 系统的整个生命过程。虽然微软公司的支持网站和现在的图书市场中已经有很多关于安全主题的书籍，但却缺乏一本系统、全面、实用的图书，来逐步引导用户掌握并解决 Windows 系统的安全问题。

正是基于上述考虑，我萌发了要写一本书的念头，这本书将介绍 Windows 以及相关系统安全方面的应用，包括 Windows 系统本身、Windows 所创建的活动目录和域、Windows 网络技术、Windows 所包含的公钥架构安全、IIS 网站、系统监控，以及现在广受关注的微软防火墙 ISA Server 和 SUS/SMS 补丁管理技术。无独有偶，这些正是本人多年工作的主要技术领域，而本人在实际工作中所接触到的几千个实际用户案例又将为这本书提供了丰富的第一手应用素材。

本书面向的读者

本书适用于所有 Windows IT 管理员、IT 服务人员、方案提供商以及重视 Windows 安全的 IT 人员和对此感兴趣的人士，也可以用作 IT 安全人才培养机构的教材。

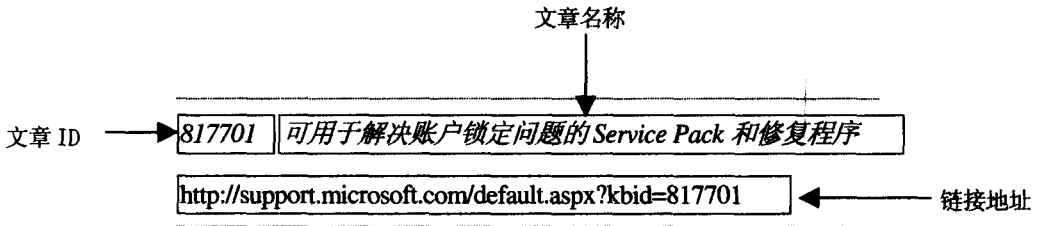
本书约定

1. 为了简便, 本书在不影响读者阅读的前提下采用了简称, 例如, “Windows Server 2003” 简称为 “Windows 2003”, “Windows 2000 Server” 简称为 “Windows 2000”, “鼠标右键单击” 简称为 “右击” 等。

2. 为了给读者提供更多的学习资源, 同时弥补本书篇幅有限的遗憾, 本书提供了大量的参考链接和下载地址, 许多本书无法详细介绍的问题都可以通过这些链接找到答案。因为这些参考链接和下载地址会因时间而有所变动或调整, 所以在此特别说明, 这些信息仅供参考, 本书无法保证所有的这些信息是长期有效的。

3. 本书所列出的插图可能会与读者实际环境中的操作界面有所差别, 这可能是由于软件版本的不同而引起的, 例如, 语言版本的不同会导致大小写的问题, 因此特别说明, 一切均以实际情况为准。

4. 本书提供了大量微软知识库文档的链接, 为了便于读者理解, 特做以下说明。



联系我们

“安全”是一个复杂而深邃的话题, 寥寥数百页不足以涉及所有的问题, 加上时间紧张, 书中难免会存在一些问题, 恳请各位读者批评与指正, 同时也希望和大家一起学习和交流。

关于本书的任何问题或意见, 欢迎和我 (alanacheng@gmail.com) 联系, 或者与本书的责任编辑 (dujie@ptpress.com.cn) 联系, 我们将尽快地回复你的邮件。

一点感想

在写书的 9 个月中, 我几乎利用了所有的休息时间, 完成了近 1000 页的初稿, 但在 “实用” 和 “质量” 的思想指导下, 最终缩减成现在的书稿, 无论怎样, 希望这本书对大家有一点帮助。

虽然写书的这段几乎无间断工作的日子, 曾让我身心憔悴, 我也与周围的朋友戏言 “多珍惜我的处女作, 它就是我的封笔作了”, 但看着眼前这厚厚的书稿, 心中依然无限欣慰。能够将自己多年积累的经验与人分享, 有助于他人, 就是我最大的乐趣和成就。

同时感谢程春苗、梅丽枝、费奔、黄荷、费新生等为本书所付出的心血和努力，他们在资料整理、环境搭建和试验测试方面给予我很大的帮助和支持。

如果这本书还能够盛起我的个人感情，我希望可以释放心中对父母淳朴厚重的养育之恩的不敢言谢之情，希望和他们一样平凡而又辛劳的人们能够早日走上小康道路，并希望我们国家能够更加繁荣富强。

程迎春

2005. 3

程迎春，硕士，微软最有价值专家（MVP），具有多年的微软产品技术支持经验和大型跨国企业的IT管理经验，在信息安全方面有丰富的积累，处理过几千个技术和项目案例，精通微软系列产品技术，提供多种微软产品培训，为多家专业技术期刊和网站撰稿，曾参加微软总部举行的防火墙和安全技术讨论会。

目录

第 1 章 活动目录结构安全设计与配置	1
1.1 活动目录概述	1
1.2 设计目录林和域的安全边界	2
1.2.1 安全边界——目录林	2
1.2.2 目录林的安全规划	2
1.2.3 域的安全规划	3
1.3 目录林和域的功能级别选择和配置	4
1.3.1 Windows 2000 的域模式	4
1.3.2 查看 Windows 2000 域模式	6
1.3.3 升级 Windows 2000 域模式	7
1.3.4 Windows 2003 目录林和域的功能级别	8
1.3.5 Windows 2003 4 种域功能级别和功能比较	8
1.3.6 Windows 2003 三种目录林功能级别及功能比较	10
1.3.7 查看 Windows 2003 目录林和域的功能级别	11
1.3.8 Windows 2003 的目录林和域功能级别提升策略	11
1.3.9 提升域功能级别	13
1.3.10 提升目录林功能级别	14
1.4 域信任关系的管理和配置	14
1.4.1 域信任关系概述	15
1.4.2 6 种信任关系	18
1.4.3 Windows 2000/2003 目录林中的默认信任关系	19
1.4.4 外部信任关系	19
1.4.5 创建外部信任关系	20
1.4.6 配置和管理快捷信任关系	23
1.4.7 目录林信任关系介绍	24
1.4.8 配置目录林信任	24
1.4.9 保护目录林信任	27
1.4.10 选择性身份验证介绍	27
1.4.11 配置选择性身份验证	28
1.4.12 启用/禁用选择性身份验证	31
1.4.13 应用 SID 过滤	31

1.5 创建组织单元实现安全管理	33
1.5.1 组织单元功能介绍	33
1.5.2 创建组织单位	35
1.5.3 配置委派管理	35
第 2 章 Windows 和域的安全管理	39
2.1 Kerberos 的安全原理和应用	39
2.1.1 理解 Kerberos	39
2.1.2 实现 Kerberos 委派	43
2.1.3 Kerberos 在网络负载均衡中的应用和配置	43
2.1.4 Kerberos 在 Cluster 群集中的应用和配置	48
2.1.5 Kerberos 在 IPSec 网络中的使用	51
2.1.6 配置 Kerberos 策略	51
2.1.7 Kerberos 监控和排错	51
2.2 管理和保护活动目录中的账号和组	53
2.2.1 理解账号和组	54
2.2.2 需要关注的活动目录账号和组	57
2.2.3 保护活动目录管理组和账号	64
2.2.4 采用管理账号和组的最佳做法	74
2.2.5 账号的 SID 管理	77
2.2.6 计算机账号管理	78
2.3 委派身份验证	81
2.3.1 理解委派	81
2.3.2 理解和配置受限委派	82
2.3.3 如何在 Windows 2000 域中实现 Kerberos 委派	84
2.3.4 如何在 Windows 2003 域中实现 Kerberos 委派	86
2.4 管理和配置时间服务	89
2.4.1 时间服务对活动目录的重要性	90
2.4.2 时间服务是如何工作的	90
2.4.3 活动目录的时间同步	91
2.4.4 通过防火墙同步时间	92
2.4.5 监控时间服务	92
2.5 服务器安全保护	93
2.5.1 强化域控制器的安全配置	93
2.5.2 保护文件安全	97
2.5.3 服务器的物理安全保护	103
2.6 安全安装 Windows	104
2.6.1 安全安装 Windows 操作系统	104

2.6.2 安全升级域控制器	107
2.7 Windows 2000/2003 安全管理技巧	109
2.7.1 删除 OS/2 和 POSIX 子系统	109
2.7.2 限制空会话访问	110
2.7.3 从网络浏览列表中隐藏计算机	110
2.7.4 更改 DLL 搜索顺序	111
2.7.5 禁用媒体自动运行	112
2.7.6 关闭文件夹中的 Web 视图	112
2.7.7 使用 Syskey 提高安全性	113
2.7.8 提高 Windows 的抗 DoS 攻击能力	114
2.7.9 禁用不受信任网络中的 NetBIOS 和 SMB 协议	118

第 3 章 配置组策略实现安全管理 121

3.1 组策略基本概念	121
3.2 组策略处理和优先级	122
3.2.1 组策略的处理顺序	122
3.2.2 默认处理顺序的例外情况	122
3.2.3 组策略在启动和登录时的应用过程	124
3.3 组策略管理方法	125
3.3.1 组策略对象编辑器	125
3.3.2 编辑容器的组策略属性	127
3.3.3 GPMC	128
3.4 组策略的设计	132
3.5 GPO 权限管理	134
3.5.1 GPO 读取和应用权限管理	134
3.5.2 GPO 的创建权限管理	135
3.5.3 GPO 编辑权限管理	135
3.5.4 GPO 链接权限管理	136
3.5.5 组策略委派管理的推荐做法	137
3.6 组策略应用	137
3.7 组策略的安全管理功能	137
3.8 安全配置账号策略	138
3.8.1 安全配置密码策略	138
3.8.2 安全配置账号锁定策略	141
3.8.3 账号锁定排错	143
3.8.4 保护账号/密码安全性的其他方法	144
3.9 安全配置 Kerberos 策略	144
3.10 安全管理用户权利	145

3.11 配置计算机安全选项	149
3.11.1 编辑安全选项	152
3.11.2 保护 Administrator 账号	153
3.11.3 保护 Guest 账号	154
3.11.4 限制空白密码的本地账户只允许进行控制台登录	154
3.11.5 计算机账号密码管理	155
3.11.6 保护与域控制器间的 LDAP 数据流	155
3.11.7 保护 SMB 数据流	156
3.11.8 交互式登录：可被缓存的前次登录个数	157
3.11.9 交互式登录：要求域控制器身份验证以解锁工作站	157
3.11.10 Windows 2000 中的匿名访问限制	158
3.11.11 Windows 2003 中的匿名访问限制	159
3.11.12 限制空会话访问	160
3.11.13 加强密码存储的安全性	162
3.11.14 控制 Lan Manager 身份验证级别	163
3.11.15 确定基于 NTLM SSP 的会话安全	164
3.12 安全管理系统服务	165
3.13 通过组策略禁用 U 盘	166
3.14 软件限制策略	168
3.14.1 默认安全级别	168
3.14.2 附加规则	168
3.14.3 常规配置规则	169
3.14.4 配置软件限制策略	169
3.15 在组策略中使用安全模板	173
3.15.1 安全模板的概念	173
3.15.2 编辑安全模板	173
3.15.3 分析现有安全策略	174
3.16 Windows 2000/2003 默认安全策略	175
3.16.1 Windows 2000/2003 默认安全策略设置	176
3.16.2 恢复默认安全策略	176
3.17 Windows 2000/2003 安全模板推荐	185

第 4 章 Windows 网络安全部署 **187**

4.1 保护 DNS 服务器	187
4.1.1 使用组策略保护 DNS 服务	187
4.1.2 集成 DNS 服务到活动目录	187
4.1.3 启用安全的动态更新	189
4.1.4 控制区域复制	189

4.1.5 启用或禁用 DNS 服务器的 IP 地址	190
4.1.6 调整事件日志和 DNS 服务日志的大小	190
4.1.7 使用防火墙屏蔽 DNS 攻击	191
4.2 保护 DHCP 服务器	191
4.2.1 防止 DHCP 拒绝服务攻击	192
4.2.2 配置 DHCP 日志	192
4.2.3 使用 IPSec 筛选器禁用端口	193
4.3 应用 IPSec 提高网络安全	193
4.3.1 IPSec 简介	193
4.3.2 配置 IPSec 协议免除	199
4.3.3 IPSec 使用方案推荐	200
4.3.4 配置传输模式的 IPSec	201
4.3.5 配置隧道模式的 IPSec	221
4.3.6 IPSec 监控和排错	224
4.3.7 IPSec 与 NAT 设备的兼容性	228
4.3.8 IPSec 与防火墙的集成使用	229
4.4 安装和配置 IAS 服务器	229
4.4.1 安装 IAS 服务	229
4.4.2 配置 RADIUS 客户端	229
4.4.3 为 IAS 服务器申请证书	230
4.4.4 配置远程访问策略	230
4.5 安全配置 VPN 应用	232
4.5.1 VPN 技术的类型	232
4.5.2 VPN 的应用场合和实例模型介绍	233
4.5.3 规划 VPN 远程访问应用	234
4.5.4 配置 VPN 远程访问服务器	240
4.5.5 配置 L2TP/VPN 远程访问服务器	251
4.5.6 在 VPN 远程访问应用中使用 EAP 验证方法	254
4.5.7 规划网关至网关的 VPN 应用	258
4.5.8 配置网关至网关的 VPN 应用	262
4.5.9 在网关至网关的 VPN 应用中使用 EAP 验证	267
4.6 安全的无线网络应用	270
4.6.1 制定安全的无线网络策略	270
4.6.2 配置 EAP_TLS 验证+WEP 加密的无线网络	273
4.6.3 配置 EAP-MSCHAP v2 +WEP 的无线网络	280

第 5 章 公钥架构的部署与应用 285

5.1 公钥架构的工作原理	285
---------------	-----

5.1.1 公钥架构的组成部分	285
5.1.2 非对称密钥	286
5.1.3 证书介绍	286
5.1.4 证书颁发机构	289
5.1.5 证书应用	292
5.1.6 证书身份验证	293
5.2 公钥架构设计	294
5.2.1 证书需求	294
5.2.2 CA 层次结构设计	296
5.2.3 CA 架构设计方案举例	301
5.2.4 CA 的硬件和软件要求	302
5.2.5 CA 配置规划	303
5.3 安装 CA 系统	304
5.3.1 CA 安装准备	304
5.3.2 安装独立根 CA	306
5.3.3 安装企业根 CA	309
5.3.4 安装子 CA	309
5.4 实现 CA 的安全管理	313
5.4.1 检查 CA 证书	314
5.4.2 CRL 分发点的管理	314
5.4.3 配置 CRL 有效期	315
5.4.4 AIA 分发点的管理	316
5.4.5 修改策略模块	316
5.4.6 CA 安全控制	317
5.4.7 证书模板的管理方法	319
5.4.8 续订 CA 证书	327
5.4.9 修改 CA 证书的有效期	328
5.4.10 根 CA 信任	329
5.4.11 CA 工具 Certutil	338
5.4.12 备份和还原 CA	340
5.5 证书的安全管理	341
5.5.1 证书管理工具	342
5.5.2 查看证书内容	344
5.5.3 导出证书	347
5.5.4 导入证书	349
5.5.5 将证书映射到用户账号	350
5.5.6 证书有效期管理	350
5.5.7 证书的申请	351
5.5.8 Web 证书申请方法	352

5.5.9 证书管理单元申请方法	358
5.5.10 配置证书的自动颁发	359
5.5.11 证书续订	365
5.5.12 证书的吊销	367
5.6 智能卡部署	367
5.6.1 智能卡硬件准备	368
5.6.2 颁发智能卡证书	368
5.6.3 智能卡证书续订	375
5.6.4 智能卡应用	376
5.7 文件加密	377
5.7.1 加密文件系统概述	378
5.7.2 EFS 的实施过程	379
5.7.3 为故障恢复代理生成文件恢复证书	380
5.7.4 备份文件恢复证书密钥	381
5.7.5 创建基于域的故障恢复代理	381
5.7.6 创建本地恢复代理	382
5.7.7 启用 EFS	382
5.7.8 启用 EFS 文件共享	384
5.7.9 备份 EFS 证书和密钥	385
5.7.10 EFS 数据恢复	385
5.7.11 EFS 最佳做法	385
 第 6 章 IIS 5.0/IIS 6.0 的安全使用	 387
6.1 IIS 的安装和配置	388
6.2 Web 权限管理	390
6.2.1 Web 的安全控制方法	390
6.2.2 Web 站点验证方法的比较与应用	395
6.3 IIS 5.0 Web 安全管理	400
6.3.1 IIS 中的安全组件	400
6.3.2 IIS 5.0 工作方式的揭密	404
6.3.3 IIS 5.0 的主要安全隐患	404
6.3.4 强化 IIS 5.0 的安全设置	406
6.4 IIS 6.0 Web 安全管理	413
6.4.1 Windows 2003 默认不安装 IIS 6.0	414
6.4.2 应用程序模型	414
6.4.3 利用 Windows 2003 的安全改善功能	417
6.4.4 安全的网站设置	418
6.5 以 Web 方式修改密码	421

6.6 证书在 Web 中的应用	421
6.6.1 SSL 网站的工作原理	421
6.6.2 SSL 网站配置	421
6.6.3 配置客户端证书验证	427
6.6.4 实现证书与账号映射	430
6.6.5 配置 IIS 证书应用中的 CRL 检查	434
6.6.6 网站证书应用中的常见问题	435
6.7 安全配置 FTP 站点	438
6.7.1 FTP 站点的配置	438
6.7.2 创建用户隔离的 FTP 站点	440
6.7.3 FTP 的安全控制	443
6.7.4 FTP 的端口和访问模式	446
6.7.5 多种方法提高 FTP 站点安全性	447
 第 7 章 ISA Server 2000 的应用与管理	 449
7.1 ISA Server 2000 介绍	449
7.1.1 ISA Server 2000 服务器	449
7.1.2 ISA Server 的客户端	451
7.2 ISA Server 2000 的应用设计	455
7.2.1 缓存代理服务器	455
7.2.2 防火墙或者集成模式 ISA Server	456
7.2.3 容量规划建议	458
7.3 安装 ISA Server	459
7.3.1 安装前的准备	459
7.3.2 安装独立的 ISA Server	459
7.3.3 安装更新	461
7.4 安全访问控制	462
7.4.1 对外访问控制原理	462
7.4.2 ISA Server 基准访问控制协议	468
7.4.3 代理内部客户端访问外部 Web 网站	470
7.4.4 代理内部客户端访问外部 FTP 网站	473
7.4.5 代理内部客户端访问外部 TCP/UDP 应用程序	473
7.4.6 代理内部客户端收发外网邮件服务器的邮件	474
7.4.7 内部客户端通过 ISA Server 使用 QQ	475
7.4.8 内部客户端通过 ISA Server 访问流媒体文件	476
7.4.9 内部客户端通过 ISA Server 使用 MSN Messenger	477
7.4.10 内部客户端通过 ISA Server 访问外部文件共享	480
7.4.11 控制内部客户端访问非 TCP/UDP 应用程序	481

7.4.12 代理内部客户端 Ping 连外网计算机	482
7.4.13 代理内部客户端访问外部 VPN 服务器	483
7.5 服务安全发布	483
7.5.1 服务安全发布原理	483
7.5.2 Web 发布 HTTP 网站	485
7.5.3 发布内部非标准端口 HTTP 网站	490
7.5.4 将 HTTP 网站发布在非标准端口上	490
7.5.5 发布内部的主机头网站	491
7.5.6 发布 HTTPS 网站	492
7.5.7 发布 FTP 网站	494
7.5.8 服务器发布	495
7.5.9 安全发布企业 Exchange 服务器	498
7.6 配置 SMTP 过滤器保护邮件安全	507
7.7 发布 ISA Server 本机的服务	508
7.8 ISA Server 本机安全配置	509
7.9 ISA Server 与 VPN 应用	512
7.9.1 外网用户直接 VPN 连接 ISA Server	512
7.9.2 外网用户通过 NAT 设备 VPN 连接 ISA Server	514
7.9.3 配置网关至网关的 VPN/ISA Server 应用	515

第 8 章 ISA Server 2004 新特性的应用 521

8.1 多重网络支持功能应用	521
8.1.1 ISA Server 2000 的网络设计局限	521
8.1.2 ISA Server 2004 的多重网络支持功能	522
8.2 防火墙策略新特性应用	527
8.2.1 ISA Server 2000 访问策略设计的局限	527
8.2.2 ISA Server 2004 集成防火墙策略	527
8.2.3 防火墙策略是有序的	528
8.2.4 默认拒绝策略	528
8.2.5 系统策略	529
8.2.6 策略存储	530
8.2.7 配置防火墙策略	530
8.3 访问策略	531
8.3.1 配置其他网络访问 ISA Server 本机	531
8.3.2 远程管理 ISA Server	534
8.3.3 ISA Server 本机访问其他网络	535
8.3.4 配置内部及 VPN 客户端访问外部网络	536
8.4 协议筛选	538

8.4.1 HTTP 协议筛选	538
8.4.2 FTP 只读配置	541
8.4.3 SMTP 协议筛选	541
8.5 服务器发布	542
8.5.1 发布标准端口的 Web 服务器	542
8.5.2 发布非标准端口的 Web 服务器	546
8.5.3 使用 Web 发布规则发布 FTP 站点	546
8.5.4 发布内网服务器	547
8.5.5 发布非标准端口的 FTP 服务器	550
8.6 利用增强的 VPN 功能	551
8.6.1 发布 VPN 服务器	552
8.6.2 在 ISA Server 上启用 VPN 客户端访问	553
8.7 利用增强的监视功能	555
8.7.1 仪表板	555
8.7.2 在日志查看器中进行实时监视	556
8.7.3 内置日志查询	556
8.7.4 会话的实时监视和筛选	557
8.7.5 连接性验证程序	558
8.7.6 将日志存储到 MSDE 数据库	558
8.7.7 发布报告	559
8.8 导出、导入、备份、还原功能	560
8.8.1 备份还原 ISA Server	560
8.8.2 导出导入配置信息	561
8.9 内核模式的安全锁定	562
8.10 与硬件集成	563

第 9 章 补丁管理与恶意软件防杀 565

9.1 介绍 Windows 更新与补丁	565
9.2 Windows 更新网站	568
9.3 自动更新客户端	568
9.4 SUS 补丁管理部署	569
9.4.1 SUS 应用场景推荐	569
9.4.2 下载必要的软件	570
9.4.3 安装 SUS 服务软件和 MSBA	571
9.4.4 配置客户端计算机的自动更新组件	573
9.4.5 SUS 补丁管理流程	577
9.4.6 使用 MSBA 评估客户端的补丁安装情况	578
9.4.7 配置 SUS 服务器选项	580

9.4.8 服务器补丁更新管理	582
9.4.9 在测试环境中安装补丁	584
9.4.10 将补丁分发到客户机	584
9.4.11 补丁卸载	585
9.4.12 SUS 补丁更新监控	585
9.5 SMS 补丁管理部署	585
9.5.1 安装 SMS 2003 安全管理扫描工具	586
9.5.2 设置补丁包的自动更新分发点	588
9.5.3 分发扫描工具	588
9.5.4 搭建测试实验室	589
9.5.5 使用向导分发补丁	589
9.5.6 使用 SMS 评估网络计算机的补丁安装情况	595
9.6 恶意软件的防杀	596
9.6.1 恶意软件的常见传播方式	596
9.6.2 恶意软件的破坏力	597
9.6.3 恶意软件分析	598
9.6.4 恶意软件防护方法	602
9.6.5 清除恶意软件	608
 第 10 章 安全审核与监测	 611
10.1 安全评估方法	611
10.1.1 MBSA 安全评估	612
10.1.2 其他入侵监测评估方法	616
10.2 审核管理	616
10.2.1 审核配置	617
10.2.2 系统无法记录安全事件时是否关闭系统	618
10.2.3 审核登录事件	618
10.2.4 审核账户登录事件	620
10.2.5 审核账户管理	621
10.2.6 审核对象访问	622
10.2.7 审核目录服务访问	625
10.2.8 审核特权使用	625
10.2.9 审核进程跟踪	626
10.2.10 审核系统事件	626
10.2.11 审核策略更改	628
10.3 Windows 日志管理	628
10.3.1 保护事件日志	628
10.3.2 配置组策略保护事件日志	629