

微软院校认证课程系列教材

网络安全的实现和管理

——以 Windows Server 2003 和
ISA Server 2004 为例

微软公司 著



高等教育出版社

HIGHER EDUCATION PRESS

微软院校认证课程系列教材

网络基本架构的规划和维护

——以 Windows Server 2003 为例

活动目录的规划、实现和管理

——以 Windows Server 2003 为例

网络安全的实现和管理

——以 Windows Server 2003 和 ISA Server 2004 为例

企业级通信和协作的规划、实现和管理

——以 Exchange Server 2003 为例

数据库基础

实用软件工程方法

ISBN 7-04-018136-3



9 787040 181364 >

定价 114.00 元

此书为培训认证教学包的组成部分，不得单独销售

微软院校认证课程系列教材

网络安全的实现和管理

——以 Windows Server 2003 和
ISA Server 2004 为例

微软公司 著

高等教育出版社

本书的著作权归微软公司所有。未经微软公司书面许可, 本书的任何部分不得以任何形式或任何手段复制或传播。著作权人保留所有权利。

图书在版编目 (CIP) 数据

网络安全的实现和管理——以 Windows Server2003
和 ISA Server2004 为例 / 微软公司著. —北京: 高等
教育出版社, 2005.8

ISBN 7-04-018136-3

I. 网... II. 微... III. 计算机网络-安全技术-教
材 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2005) 第 085431 号

策划编辑	尹 洪	责任编辑	许 可	封面设计	张 楠	责任绘图	朱 静
版式设计	张 岚	责任校对	王 雨	责任印制	陈伟光		

出 版 高等教育出版社
社 址 北京市西城区德外大街 4 号
邮政编码 100011
总 机 010-58581000

购书热线 010-58581118
免费咨询 800-810-0598
网 址 <http://www.hep.edu.cn>
<http://www.hep.com.cn>

印 刷 北京外文印刷厂

开 本 787×1092 1/16
印 张 37.25
字 数 920 000

版 次 2005 年 8 月第 1 版
印 次 2005 年 8 月第 1 次印刷
定 价 114.00 元(含光盘)

版权所有 侵权必究

物料号 18136-00

编审委员	刘志鹏	朱之文	田本和	王军伟	郑祖宪	马肖风
	王 林	王建国	罗晓中			
组织策划	田本和	尹 洪	蒋 斌	周雨阳		
	蔡 锴	李朝晖	姬 琳			
技术编审	蒋 斌	蔡 锴	虞谷晔	卢丽娜	黄佩红	李朝晖
	喻艺丹	张广军				

Microsoft Official Curriculum 最终用户许可协议

重要须知——请认真阅读——您一旦打开“许可使用内容”包装的密封或以其他方式使用此处的“许可使用内容”，即表示您同意接受本《协议》各项条款的约束：本 Microsoft Official Curriculum 可能包含 Microsoft 或其供应商提供的软件或其他材料（总称“许可使用内容”），其使用应遵守以下各项 Microsoft 提示条款。每个软件程序都受一份最终用户许可协议（《协议》）的约束，而该《协议》是您（个人或单一实体）（“最终用户”）和 Microsoft Corporation（“Microsoft”）之间就允许使用软件及相关介质或印刷材料、“联机”或电子文档和基于 Internet 的服务达成的一份法律协议。本《协议》的修正条款或补充条款可能随软件一起提供。您一旦安装、复制或以其他方式使用“许可使用内容”，即表示您同意接受本《协议》各项条款的约束。如果您不同意，请（a）不要打开“许可使用内容”包装的密封；（b）不要使用软件、文档或其他材料，并且（c）退还“许可使用内容”。

“许可使用内容”随带软件的特别提示

许可证的授予。为与本“许可使用内容”一起使用而提供的任何软件（“软件”）都是 Microsoft Corporation 和（或）其供应商享有著作权的作品。“软件”只授予使用许可，而非出售。任何特定“软件”的使用都应遵守以下各《许可协议》中的一份《许可协议》：

（1）一般使用许可。Microsoft 授予最终用户一份有限的、非独家拥有的、免版权费的许可证，许可其在一台由一位单一用户随时使用或访问的单一计算机上安装和使用“软件”的一份副本，并且最终用户：（a）不得修改“软件”，但下文有明确规定时例外；（b）不得发行“软件”或其任何组成部分；（c）不得出借、出租、租赁、出售、分许可、转让“软件”或将“软件”随附的任何印刷材料用于提供商业运营服务；（d）不得在收费的公立或私立课程中使用“软件”；（e）不得对“软件”进行反向工程、反编译或反汇编；尽管有此项限制，但如果适用法律明确允许上述活动并且仅在适用法律明示允许上述活动的范围内，则例外；并且（f）不得转让“软件”的各项权利，除非本《协议》明确规定。

Microsoft 保留一切其他权利。Microsoft 及其供应商保留“软件”的一切产权和所有权，并且不转让或许可使用“软件”或其任何组成部分的任何权利，除非本《协议》具体说明。

（2）替代使用许可。上述规定的一般使用许可将被任何具体“软件”随附或包括的《许可协议》（如果有）的各项条款取代或替代。除非最终用户首先同意《许可协议》的各项条款，否则将无法安装附带或包括该《许可协议》的“软件”。Microsoft 保留一切其他权利。Microsoft 及其供应商保留“软件”的一切产权和所有权，并且不转让或许可使用“软件”或其任何组成部分的任何权利，除非本《协议》明确说明。

（3）样本代码使用许可。如果将特定代码或一个样本应用程序作为“许可使用内容”中包括的实验室练习的部分提供（“样本代码”），则这类“样本代码”以“现有状况”被提供，并且没有任何类型的保证。Microsoft 授予您一份有限的、非独家拥有的、免版权费的许可证，

许可您为了个人使用的目的而安装、使用、修改和复制“样本代码”，条件是您不得：（a）发行“样本代码”或其任何组成部分；（b）出借、出租、租赁、出售、分许可或转让“样本代码”；（c）在收费的公立或私立课程中使用“样本代码”；并且（或者）（d）转让“样本代码”的任何权利。如果您修改“样本代码”，您应该根据 Microsoft 的请求，自付费用为因您或代表您对“样本代码”做出的任何修改而使 Microsoft 和 Microsoft 的分公司、关联公司、董事、高级主管、员工、代理商和独立供应商面临的任何索赔或诉讼提供辩护，并且您须赔偿 Microsoft 因这类索赔而招致的任何费用、损害赔偿和手续费方面的合理开支（其中包括但不限于律师费和其他专业人士收取的费用），并使其免受任何损害。Microsoft 应：（a）以书面形式就任何这类索赔或诉讼向您提供合理的及时提示，并且允许您通过 Microsoft 和您双方都接受的律师对这类索赔或诉讼进行答辩和辩护；（b）在您支付费用的情况下向您提供信息、协助和授权，以帮助您为这类索赔或诉讼进行辩护。您不对 Microsoft 在未经您书面允许的情况下做出的任何和解负责，但您不得以不合理的方式拒绝给予这样的允许。

其他许可限制。安装“软件”仅供最终用户根据适用的《许可协议》使用，并且除非以其他方式在另外一份协议中达成一致意见，否则得不到 Microsoft 或其供应商提供的技术或其他支持服务。法律明确规定：禁止在违反《许可协议》的情况下对“软件”进行任何复制或再发行。明确禁止为进一步复制或再发行软件而将“软件”复制到任何服务器或地点。

美国政府许可使用权利。根据 1995 年 12 月 1 日当天或之后签发的请求而提供给美国政府的所有软件，均根据本协议其他部分规定的商业许可使用权利和限制予以提供。根据 1995 年 12 月 1 日之前签发的请求而提供给美国政府的所有软件，视情况根据 FAR, 48 CFR 52.227-14 (1987 年 6 月) 或 DFAR, 48CFR252.227-7013 (1988 年 10 月) 中规定的“限制权利”予以提供。

免责条款。“软件”仅根据《许可协议》的各项条款对“软件”提供保证（如果提供保证的话）。除非在《许可协议》中提供保证，否则 Microsoft Corporation 和（或）其供应商就“软件”不提供任何的保证和条件，包括适销性、适用性、所有权和不侵权的所有默示保证和条件。

“许可使用内容”随带文档和（或）其他材料的具体说明

允许从“许可使用内容”（“文档”）中打印文档（如实验室说明等），条件是：（a）将这类文档用于您的个人培训，并且不得再出版或在任何网络计算机上张贴或以任何介质形式广播这类文档，并且（b）不得对任何文档做出任何修改。

明确禁止对任何介质上包含的作为“许可使用内容”组成部分的录像、录音、图形和（或）任何其他材料（“其它材料”）进行任何复制或再发行。

“许可使用内容”的各组成部分均受商业包装法律和其他法律的保护，并且不得全部或部分予以复制或模仿。除非 Microsoft 明示允许，否则不得复制或转发“许可使用内容”中的任何徽标、图形、声音或图像。

无保证。Microsoft 和（或）其供应商不对“许可使用内容”中不论为任何目的而可能包含的文档或其他材料中的信息、音像或任何其他内容是否合适提供任何保证，无论该类文档、信息、音像或任何其他内容是何目的。所有这类文档和其他材料均以“现有状况”提供，没有

任何类型的保证。Microsoft 和（或）其供应商特此就文档和其他材料不提供任何的保证和条件，包括适销性、适用性、所有权和不侵权的所有默示保证和条件。

有关第三方站点链接的说明

至第三方站点的链接。您可以使用“许可使用内容”链接至第三方站点。第三方站点不由 Microsoft 控制，并且 Microsoft 不对任何第三方站点的内容、第三方站点包含的任何链接或第三方站点的任何更改或更新负责。Microsoft 不对从任何第三方站点收到的网站广播或任何其他形式的传输负责。Microsoft 仅为了您的方便向您提供这些至第三方站点的链接，并且包括任何链接并不暗示 Microsoft 认可相应的第三方站点。

有关全部“许可使用内容”的说明

“许可使用内容”中包括的“软件”、文档和其他材料可能包含不准确的技术内容或印刷错误。可能定期对内容进行修订。Microsoft 可随时在不提供通知的情况下对“许可使用内容”中规定的产品和（或）程序进行改进和（或）更改。

免责条款。除非另行说明，否则本《协议》提及的公司、产品、人物、特性和（或）数据均属虚构，并且无意以任何方式代表任何真实的个人、公司、产品或活动。

保留权利和所有权。Microsoft 保留未在本《协议》中明示授予您的一切权利。“许可使用内容”受著作权和其他知识产权法律及条约的保护。Microsoft 或其供应商拥有“许可使用内容”和其中组件的所有权、著作权和其他知识产权。

同意使用数据。您同意：Microsoft 及其关联公司可以收集和使用作为提供给您的产品支持服务的一部分而收集的与“许可使用内容”相关的技术信息（如果有）。Microsoft 可以将此信息仅用于改进我们的产品或为您提供定制的服务或技术，并且不会以能识别您身份的方式披露此信息。

额外软件/服务。除非我们随下列更新、增补、补充组件或基于 Internet 的服务组件一起提供其他应适用的条款，否则本《协议》适用于 Microsoft 在您获得“许可使用内容”的初始副本之日后可能提供给您的或为您准备的“许可使用内容”的更新、增补、补充组件或基于 Internet 的服务组件。就通过使用“许可使用内容”而提供给您的或为您准备的任何基于 Internet 的服务而言，Microsoft 保留停止这类服务的权利。

出口限制。您承认“软件”受美国出口法律管辖。您同意遵守所有适用于“软件”的国际法和国内法，其中包括美国出口管理条例以及由美国和其他国家（地区）政府颁发的最终用户、最终使用和目的地方面的限制。要了解详情，请访问 <http://www.microsoft.com/exporting/> 网站。

许可使用内容的转让。“许可使用内容”的原始最终用户可以将本《协议》和“许可使用内容”永久性地一次直接转让给另外一位最终用户，条件是该原始用户不得保留“许可使用内容”的任何副本，并且必须转让“许可使用内容”的所有部分（包括全部组件、介质及印刷材料、任何升级版本、各《许可协议》和（如果适用）正版标签）。这种转让不得为非直接转让，如以寄售方式转让。在转让之前，接收“许可使用内容”的最终用户必须同意遵守《协议》的

各项条款。如果“许可使用内容”是一个升级版本，任何转让都必须包括“许可使用内容”的所有先前版本。

终止。如果您未遵守本《协议》的各项条款和条件，在不损害其他权利的情况下，Microsoft 可终止本《协议》。如此类情况发生，您必须销毁“许可使用内容”的所有副本及其全部组成部分。

适用法律。本《协议》受中华人民共和国法律管辖。

责任限制。在适用法律所允许的最大范围内，无论损害赔偿是否在履行合约、出现疏忽或发生其他侵权行为时发生，Microsoft 和（或）其供应商绝不就因“许可使用内容”的任何组成部分或所有组成部分的使用或性能、因提供或未能提供服务、或因可从“许可使用内容”得到的信息而引起的或有关的任何特殊的、间接的、或特定的损害赔偿或任何损害赔偿（包括但不限于因营业中断，因使用、数据或利润的丧失，或因任何其他金钱上的损失而造成的损害赔偿）承担赔偿责任。在任何情况下，Microsoft 的全部责任以及您获得的惟一赔偿将限于为“许可使用内容”实际支付的款额或五美元（U.S.\$5.00）以两者中的较高款额为准；但是，如果您已经签订了一份 Microsoft 服务协议，Microsoft 对这类服务的全部责任将遵守该协议各项条款的规定。由于某些国家和地区不允许排除或限制责任，上述限制条款可能不适用于您。

全部协议；规定可分割性。本《协议》（包括随“许可使用内容”提供的本《协议》的任何补充条款或修正条款）是您与 Microsoft 之间就“许可使用内容”和支持服务（如果有）达成的全部协议，并且取代“许可使用内容”或本《协议》中所包含的任何其他标的之所有先前或同时存在的口头或书面的通信、建议和声明。如果任何 Microsoft 支持服务的政策或计划的条款与本《协议》的条款有冲突，以本《协议》的条款为准。如果本《协议》的任何条款被认定为作废、无效、不能执行或非法，其他条款应继续完全有效。

如果您对本《协议》有任何疑问，或者如果您由于某种原因希望与 Microsoft 联系，请使用“许可使用内容”中附带的地址信息与微软（中国）有限公司联系，或在<http://www.microsoft.com> 网站访问 Microsoft。

准则和定义

“许可使用内容”是一种专门设计的培训工具，供 Microsoft Certified Technical Education Center (Microsoft CTEC)、Microsoft Certified Partner (MCP)、Microsoft 认证培训讲师 (MCT)、IT Academy 计划成员和 Microsoft 可能随时以书面形式指定的其他机构使用。“许可使用内容”旨在使 Microsoft 的技术培训渠道能够向计算机专业人士提供系统、支持和开发培训课程。为了取得最佳成果，“许可使用内容”应该由 Microsoft 认证培训讲师 (MCT) 在课堂环境或在线学习环境中讲授。

Microsoft Official Curriculum (MOC)：由 Microsoft 开发的系列课程材料，用于提供 Microsoft 产品和技术的培训和解决方案。

Microsoft 认证培训讲师 (MCT)：具备必要的教学和技术能力并且由 Microsoft 认证为能够通过 Microsoft CTEC 讲授 Microsoft Official Curriculum 的个人。

Microsoft Certified Technical Education Center (Microsoft CTEC)：已经符合 Microsoft 对

指定其为下列场所的资格要求：（a）一处 Microsoft Certified Partner（MCP）营业点、和（b）一处提供 Microsoft CTEC 服务的任何场所。这些培训中心使用 MCT 向学生提供 MOC 课程培训。

Microsoft Certified Partner：已经符合被指定为 Microsoft Certified Partner 的资格要求的任何场所。

IT Academy 计划成员：已经符合被指定为 IT Academy 计划成员的资格要求的任何院校。

目 录

第 1 章 规划和配置授权和身份验证策略.....1	
1.1 Windows Server 2003 中的组和基本组策略.....2	
1.1.1 Windows Server 2003 中的组类型.....2	
1.1.2 组作用域.....3	
1.1.3 内置组.....3	
1.1.4 特殊组.....5	
1.1.5 管理安全组的工具.....6	
1.1.6 受限制的组策略.....6	
1.1.7 创建“受限制的组”策略的方法.....8	
1.1.8 实验 1-1: 创建组 and 指派权利.....8	
1.2 在 Windows Server 2003 中创建信任.....8	
1.2.1 Windows Server 2003 中的信任.....8	
1.2.2 在 Windows Server 2003 中信任使用的身份验证方法.....10	
1.2.3 与服务器操作系统相关的信任类型.....10	
1.2.4 使用 SID 筛选阻止 SID 电子欺骗.....11	
1.2.5 创建信任的方法.....12	
1.2.6 实验 1-2: 创建信任.....13	
1.3 使用组来规划、实现和维护授权策略.....13	
1.3.1 身份验证、授权和最小特权.....13	
1.3.2 用户/ACL 方法.....14	
1.3.3 账户组/ACL 授权方法.....15	
1.3.4 账户组/资源组授权方法.....15	
1.3.5 组命名规则.....16	
1.3.6 决定组何时作废的方法.....17	
1.3.7 实验 1-3: 创建组命名策略.....18	
1.4 身份验证模型的组件.....18	
1.4.1 Windows Server 2003 的身份验证功能.....18	
1.4.2 Windows Server 2003 中的身份验证协议.....18	
1.4.3 LM 身份验证.....19	
1.4.4 NTLM 身份验证的工作原理.....20	
1.4.5 Kerberos 身份验证的工作原理.....21	
1.4.6 Windows Server 2003 的机密存储.....23	
1.4.7 诊断身份验证问题的工具.....23	
1.5 规划和实现身份验证策略.....24	
1.5.1 评估环境的注意事项.....24	
1.5.2 控制对计算机授权的组策略设置.....25	
1.5.3 创建强密码策略的指导方针.....25	
1.5.4 账户锁定策略和登录限制的选项.....26	
1.5.5 创建 Kerberos 票证策略的选项.....27	
1.5.6 Windows Server 2003 对早期操作系统的身份验证方法.....27	
1.5.7 启用安全身份验证的方法.....28	
1.5.8 补充的身份验证的策略.....29	
1.5.9 Windows 徽标程序.....30	
1.5.10 实验 1-4: 配置安全的身份验证.....30	
1.6 实验 1-5: 规划和配置身份验证和授权策略.....31	
习题.....31	
第 2 章 安装、配置和管理证书颁发机构.....34	
2.1 PKI 和证书颁发机构简介.....34	
2.1.1 PKI.....34	
2.1.2 PKI 的组件.....35	
2.1.3 使用 PKI 的应用程序.....36	
2.1.4 使用支持 PKI 的应用程序的账户.....37	
2.1.5 PKI 工具.....38	
2.1.6 证书颁发机构.....40	
2.1.7 不同证书颁发机构类型之间的差异.....40	
2.1.8 证书颁发机构设计.....41	
2.1.9 CA 层次结构中的等级.....42	
2.2 安装证书颁发机构.....43	

2.2.1 CAPolicy.inf 文件	43	3.2.4 使用 Certreq.exe 执行的任务	68
2.2.2 安装企业从属 CA 的方法	45	3.2.5 启用自动证书注册的方法	69
2.2.3 在从属 CA 上安装证书的方法	46	3.2.6 吊销证书的方法	69
2.3 管理证书颁发机构	46	3.2.7 实验 3-2: 吊销证书	70
2.3.1 应用程序检查证书状态的方法	47	3.3 管理证书	70
2.3.2 证书验证测试	47	3.3.1 密钥恢复概述	70
2.3.3 吊销证书的原因码	48	3.3.2 导出密钥和证书使用的文件格式	71
2.3.4 证书服务发布 CRL 的方式	49	3.3.3 导出密钥的工具	71
2.3.5 CRL 发布间隔的规划标准	50	3.3.4 导出密钥的方法	72
2.3.6 CRL 发布点的位置	51	3.3.5 实验 3-3: 导出私钥	73
2.3.7 修改发布位置的方法	52	3.3.6 密钥存档和恢复的要求	73
2.3.8 实验 2-1: 决定颁发机构信息访问 和 CRL 可用性	53	3.3.7 配置 CA 进行密钥存档的方法	73
2.4 备份和还原证书颁发机构	53	3.3.8 密钥恢复过程	75
2.4.1 备份 CA 的方法	54	3.3.9 降低密钥恢复相关安全风险的指 导方针	77
2.4.2 备份证书服务的方法	54	3.4 实验 3-4: 部署和管理证书	77
2.4.3 还原证书服务的方法	55	习题	77
2.4.4 备份证书服务的最佳实践	56	第 4 章 智能卡证书的规划、实现和 故障诊断	80
2.5 实验 2-2: 安装和配置证书颁发机构	56	4.1 多因素身份验证简介	80
习题	57	4.1.1 多因素身份验证	81
第 3 章 配置、部署和管理证书	59	4.1.2 多因素身份验证的场景	82
3.1 配置证书模板	59	4.1.3 多因素身份验证设备	83
3.1.1 数字证书	59	4.1.4 使用智能卡进行多因素身份验证 的好处	84
3.1.2 数字证书的生命周期	60	4.1.5 使用智能卡的应用程序	85
3.1.3 证书模板	60	4.1.6 智能卡基本架构组件	86
3.1.4 证书模板的类型	62	4.2 规划和实现智能卡基本架构	87
3.1.5 证书模板分类	63	4.2.1 确定组织中应该使用智能卡的场合	88
3.1.6 证书模板权限	64	4.2.2 选择智能卡和阅读器的指导方针	89
3.1.7 更新证书模板的方法	64	4.2.3 证书颁发机构要求	90
3.1.8 修改和取代现有证书模板的指 导方针	64	4.2.4 智能卡证书模板	91
3.1.9 修改和取代证书模板的方法	65	4.2.5 启用智能卡证书模板	91
3.1.10 实验 3-1: 取代证书模板	66	4.2.6 证书注册方法	91
3.2 部署与吊销用户和计算机证书	66	4.2.7 配置注册代理	92
3.2.1 证书注册方法	67	4.2.8 注册用户的智能卡证书	93
3.2.2 使用基于 Web 界面注册证书的 方法	67	4.2.9 实验 4-1: 规划智能卡部署	94
3.2.3 使用证书申请向导申请证书的方法	68	4.3 智能卡基本架构的管理和故障诊断	94

4.3.1 用户培训计划应包含的内容.....94	5.4.2 在多个用户之间共享加密文件的 方法..... 114
4.3.2 管理智能卡基本架构的组策略设置.....95	5.4.3 远程服务器上的文件共享..... 115
4.3.3 配置智能卡组策略.....96	5.4.4 在不同位置之间移动或复制加密 文件的影响..... 116
4.3.4 诊断常见智能卡错误的指导方针.....97	5.4.5 WebDAV 服务器..... 117
4.4 实验 4-2: 实施智能卡.....98	5.4.6 实验 5-3: 启用 EFS 文件共享..... 118
习题.....98	5.5 EFS 故障排除..... 118
第 5 章 加密文件系统的规划、实现 和故障排除.....100	5.5.1 管理远程加密文件的指导方针..... 118
5.1 EFS 简介.....100	5.5.2 解决 EFS 常见问题的指导方针..... 118
5.1.1 EFS.....100	5.6 实验 5-4: 加密文件系统的规划、部署 和故障排除..... 120
5.1.2 EFS 的工作原理.....101	习题..... 120
5.2 在独立的 Windows XP 环境中实现 EFS.....102	第 6 章 规划、配置和部署安全的成 员服务器基线..... 123
5.2.1 在独立环境中实现 EFS 的最佳 实践.....102	6.1 成员服务器基线概述..... 123
5.2.2 自签名的证书.....103	6.1.1 受信计算基..... 123
5.2.3 使用 Windows 资源管理器加密 和解密文件的方法.....104	6.1.2 维护受信计算基的要求..... 124
5.2.4 创建数据恢复代理的方法.....104	6.1.3 安全基线元素..... 124
5.2.5 管理明文数据的指导方针.....105	6.1.4 建立安全基线的指导方针..... 124
5.2.6 创建密码重设磁盘的方法.....106	6.2 规划安全的成员服务器基线..... 124
5.2.7 在独立计算机上禁用 EFS.....107	6.2.1 为服务器规划安全基线的指导 方针..... 125
5.2.8 实验 5-1: 在独立的 Windows XP 环境中实现 EFS.....108	6.2.2 预定义的安全模板..... 126
5.3 在使用 PKI 的域环境中规划和实现 EFS.....108	6.2.3 Windows Server 2003 中的安全 性环境..... 128
5.3.1 在使用 PKI 的域环境中规划 EFS 的指导方针.....109	6.2.4 其他安全模板..... 129
5.3.2 确定计算机上是否在使用 EFS 的方法.....110	6.2.5 保存安全模板的最佳实践..... 129
5.3.3 更改域的恢复策略的方法.....110	6.2.6 其他安全设置..... 130
5.3.4 迁移到新证书的方法.....111	6.2.7 管理组设计的最佳实践..... 131
5.3.5 在 Windows XP 中启用 3DES 算法的方法.....112	6.2.8 实验 6-1: 规划安全的成员服务 器基线..... 132
5.3.6 在关机时清除页面文件的方法.....112	6.3 配置其他安全设置..... 132
5.3.7 实验 5-2: 在使用 PKI 的域环境 中规划 EFS.....113	6.3.1 将安全组手工添加到“用户权 限分配”..... 132
5.4 实现 EFS 文件共享.....113	6.3.2 重命名域中服务器上的 Administrator 和 Guest 账户..... 133
5.4.1 EFS 文件共享.....114	6.3.3 时间同步过程..... 133

6.3.4 配置时间同步.....	134	7.2.7 实验 7-1: 配置 DNS 更新凭据.....	158
6.3.5 实验 6-2: 配置时间服务.....	134	7.3 规划和配置基本架构服务器的	
6.4 部署安全模板.....	135	安全基线.....	158
6.4.1 部署安全模板的方式.....	135	7.3.1 针对基本架构服务器的安全威胁.....	159
6.4.2 使用组策略在域环境中部署安全		7.3.2 基本架构服务器基线策略.....	159
模板.....	135	7.3.3 配置其他 DHCP 设置的方法.....	159
6.4.3 在独立的计算机上部署安全模板.....	136	7.3.4 增加 DHCP 服务器容错能力的	
6.4.4 使用脚本部署安全模板.....	136	方法.....	160
6.4.5 部署安全模板的最佳实践.....	137	7.3.5 保护 WINS 服务器的指导方针.....	160
6.5 安全模板故障诊断.....	137	7.3.6 创建静态 WINS 条目.....	161
6.5.1 解决与应用组策略有关的问题.....	137	7.3.7 实验 7-2: 创建 GPO 以限制对	
6.5.2 解决不期望的安全设置问题.....	143	基本架构服务器的访问.....	162
6.5.3 解决系统策略问题.....	146	7.4 规划文件和打印服务器的安全基线.....	162
6.6 实验 6-3: 规划、配置和部署成员		7.4.1 针对文件和打印服务器的安全	
服务器基线.....	147	威胁.....	162
习题.....	148	7.4.2 文件服务器和打印服务器基线	
第 7 章 为服务器角色规划、配置和		策略.....	162
部署安全基线.....	150	7.4.3 保护文件服务器的指导方针.....	163
7.1 规划和配置域控制器的安全基线.....	150	7.4.4 保护打印服务器的指导方针.....	163
7.1.1 针对域控制器的安全威胁.....	150	7.4.5 实验 7-3: 创建组合式文件和	
7.1.2 域控制器基线策略.....	151	打印服务器基线策略.....	163
7.1.3 Active Directory 数据库和日志		7.5 规划和配置 IIS 服务器的安全基线.....	163
文件.....	151	7.5.1 针对 IIS 服务器的安全威胁.....	164
7.1.4 Ntdsutil.exe.....	152	7.5.2 IIS 服务器基线策略.....	164
7.1.5 移动 Active Directory 数据库和		7.5.3 安装 IIS 的方式.....	165
日志文件的方式.....	152	7.5.4 为 IIS 服务器设置用户权限分配	
7.1.6 调整 Active Directory 事件日志		的指导方针.....	165
文件的大小.....	153	7.5.5 配置 IIS 日志记录的指导方针.....	166
7.1.7 SYSKEY.....	153	7.5.6 在 IIS 中配置额外设置的指导方针.....	166
7.2 规划和配置 DNS 服务器的安全基线.....	154	7.6 Internet 验证服务基线策略.....	166
7.2.1 针对 DNS 服务器的安全威胁.....	154	7.6.1 配置 IAS.....	167
7.2.2 保护 Microsoft DNS 服务器的		7.6.2 RADIUS 消息验证程序.....	167
指导方针.....	155	7.6.3 账户锁定.....	168
7.2.3 配置 DNS 动态更新凭据.....	155	7.6.4 隔离控制.....	168
7.2.4 限制 DNS 区域传输的方式.....	157	7.6.5 日志记录注意事项.....	169
7.2.5 限制从外部访问 DNS 服务器的		7.6.6 用防火墙保护 IAS.....	169
指导方针.....	157	7.7 Exchange Server 服务器基线策略.....	169
7.2.6 防止 DNS 高速缓存污染的方式.....	158	7.7.1 网络加密.....	169

7.7.2 日志记录注意事项.....	170	8.3.3 软件限制策略选项.....	185
7.7.3 使用防火墙保护 Exchange Server	170	8.3.4 规划和实现软件限制策略的 最佳实践	186
7.8 SQL Server 服务器基线策略.....	171	8.3.5 创建规则的方法.....	186
7.8.1 身份验证.....	171	8.4 为移动客户端实现安全.....	187
7.8.2 授权.....	172	8.4.1 对移动客户端的威胁.....	187
7.8.3 日志记录注意事项.....	172	8.4.2 在移动客户端上保护硬件的 最佳实践	188
7.8.4 使用防火墙保护 SQL Server.....	173	8.4.3 在移动客户端上保护操作系统 安全的最佳实践	188
7.9 实验 7-4: 规划、配置和实现服务器 角色的安全基线	174	8.4.4 为移动客户端更改启动密码的 方法	189
习题.....	174	8.4.5 在移动客户端上保护数据安全的 最佳实践	190
第 8 章 规划、配置、实现和部署 安全客户端计算机基线.....	176	8.5 实验 8-3: 规划、实现、配置和部署 安全客户端计算机基线	190
8.1 规划和实现安全客户端计算机基线.....	176	习题.....	190
8.1.1 客户端计算机基线.....	176	第 9 章 规划和实现软件更新服务.....	192
8.1.2 为保护客户端安全预定义的 安全模板	177	9.1 软件更新服务和更新管理介绍.....	192
8.1.3 Microsoft Windows XP 安全 指南模板	177	9.1.1 更新管理的优点.....	192
8.1.4 管理模板.....	178	9.1.2 更新管理基本架构的基本要素.....	193
8.1.5 管理模板和安全模板的区别.....	179	9.1.3 操作系统的更新管理工具.....	193
8.1.6 添加和删除管理模板.....	179	9.1.4 应用程序的更新管理工具.....	195
8.1.7 Microsoft Office 模板.....	180	9.1.5 SUS 组件.....	196
8.1.8 规划客户端计算机基线的指导 方针	181	9.1.6 更新管理中使用的文件.....	196
8.1.9 实验 8-1: 安装 Office Resource Kit 模板	181	9.2 规划更新管理战略.....	197
8.2 配置和部署客户端计算机基线.....	181	9.2.1 更新管理生命周期.....	198
8.2.1 组策略环回处理模式.....	182	9.2.2 分析更新状态的网络环境的方法.....	199
8.2.2 启用环回处理的方式.....	182	9.2.3 使用 MBSA 分析网络环境的方法.....	200
8.2.3 重命名客户端计算机上的 Administrator 和 Guest 账户的方式	182	9.2.4 实验 9-1: 安装和运行 MBSA.....	201
8.2.4 配置和部署客户端计算机基线 的指导方针	183	9.2.5 MSRC 漏洞严重程度系统.....	201
8.2.5 实验 8-2: 为环回模式配置管 理模板	183	9.2.6 测试更新阶段.....	202
8.3 规划和实现软件限制策略.....	183	9.2.7 部署更新的场景.....	203
8.3.1 软件限制策略的用途.....	184	9.2.8 规划 SUS 基本架构的指导方针.....	204
8.3.2 标识软件的规则.....	184	9.3 实现 SUS 基本架构.....	205
		9.3.1 安装 SUS1.0 SP1 的方法.....	205
		9.3.2 安装后的任务.....	206
		9.3.3 Automatic Updates 客户端.....	207

9.3.4 Automatic Updates 客户端配置选项	207	10.4.3 启用 LDAP 签名的方法	232
9.3.5 管理 SUS 服务器的方法	208	10.4.4 在 Web 服务器上启用 SSL 的 方法	232
9.3.6 保护 SUS 服务器安全的最佳实践	209	10.4.5 部署 IPSec 策略的方法	234
9.3.7 备份 SUS 服务器的方法	210	10.4.6 实验 10-3: 安装 SSL 证书	234
9.3.8 更新管理的最佳实践	210	10.5 IPSec 通信故障排除	234
9.3.9 实验 9-2: 配置 SUS 服务器	211	10.5.1 IPSec 故障排除工具	235
9.4 实验 9-3: 安装、配置和维护更新 管理基本架构	211	10.5.2 事件查看器	235
习题	211	10.5.3 在安全性日志中禁用 IKE 事件 审核的方法	236
第 10 章 数据传输安全性的规划、部 署和故障排除	213	10.5.4 验证策略已应用的工具	236
10.1 安全数据传输方法	213	10.5.5 IP 安全监视器控制台	237
10.1.1 安全数据传输面临的威胁	213	10.6 实验 10-4: 数据传输安全性的规划、 部署和故障排除	238
10.1.2 SSL 和 TLS	214	习题	239
10.1.3 SSL/TLS 保护数据安全的方法	215	第 11 章 部署配置和管理 SSL	241
10.1.4 PPTP	217	11.1 安全套接字层 (SSL) 概述	241
10.1.5 PPTP 保护数据安全的方法	217	11.1.1 SSL 工作原理	241
10.1.6 SMB 签名	218	11.1.2 SSL 与 IPSec 比较	242
10.1.7 LDAP 签名	219	11.1.3 获取 SSL 证书	242
10.1.8 WEP 确保数据保密性的方法	219	11.1.4 续订 SSL 证书	243
10.1.9 WPA 确保数据保密性的方法	220	11.1.5 配置防火墙	243
10.1.10 实验 10-1: 确定协议以及功能	221	11.2 其他 SSL 应用程序	244
10.2 IPSec 简介	221	11.2.1 在 Active Directory 域控制器上 启用 SSL	244
10.2.1 IPSec 的功能和特点	222	11.2.2 在运行 SQL Server 的计算机上 启用 SSL	245
10.2.2 用于加密功能的 IPSec 模式	223	11.2.3 在邮件服务器上启用 SSL	247
10.2.3 使用 IPSec 进行身份验证的方法	224	习题	249
10.2.4 IPSec 策略	225	第 12 章 规划和实施无线网络的安 全措施	250
10.3 规划数据传输安全性	226	12.1 保护无线网络安全简介	250
10.3.1 确定数据传输安全要求的指导 方针	226	12.1.1 无线网络的好处	250
10.3.2 需要安全数据传输的计算机	227	12.1.2 对无线安全的常见威胁	251
10.3.3 网络通信图	227	12.1.3 无线网络标准	252
10.3.4 创建网络通信图的注意事项	228	12.1.4 使用安全措施降低无线网络 风险的指导方针	252
10.3.5 实验 10-2: 创建网络通信图	229	12.1.5 无线网络架构	253
10.4 实现安全数据传输方法	229		
10.4.1 使用 IPSec 创建自定义安全 策略的方法	229		
10.4.2 启用 SMB 签名的方法	232		

12.2 实现 802.1x 身份验证	253
12.2.1 802.1x 身份验证类型	254
12.2.2 802.1x-EAP-TLS 身份验证 解决方案的用途和组件	254
12.2.3 802.1x-EAP-TLS 身份验证 工作原理	255
12.2.4 实现 802.1x 的客户端、服务 器和硬件要求	256
12.2.5 实现 802.1x 身份验证的最佳 实践	257
12.3 规划安全的 WLAN 策略	257
12.3.1 规划 PKI 的方法	258
12.3.2 创建证书模板的注意事项	258
12.3.3 规划 IAS 基本架构的指导方针	260
12.3.4 使用 RADIUS 日志的指导方针	261
12.3.5 规划无线接入点位置和设置 的方法	262
12.3.6 远程访问连接策略	263
12.3.7 实验 12-1: 规划无线接入点 位置	264
12.4 实现安全 WLAN	264
12.4.1 IAS 配置步骤	265
12.4.2 IAS 的安装方法	266
12.4.3 将 WAP 配置为 RADIUS 客户 端的方法	266
12.4.4 备份和导出 IAS 配置的方法	267
12.4.5 IAS 远程访问策略	267
12.4.6 创建无线网络策略的方法	269
12.4.7 无线网络策略设置	269
12.4.8 无线接入点设置	271
12.4.9 实验 12-2: 安装 IAS	271
12.5 无线网络故障排除	271
12.5.1 故障排除工具	271
12.5.2 排除 IAS 错误的工具	272
12.5.3 IAS 身份验证的故障排除步骤	274
12.6 实验 12-3: 规划和实施无线网络的 安全措施	275
习题	275

第 13 章 保护远程访问安全	277
13.1 远程访问技术和漏洞简介	277
13.1.1 远程访问方法	277
13.1.2 远程访问的威胁	278
13.1.3 选择隧道协议的考虑事项	280
13.1.4 选择远程访问身份验证协议的 考虑事项	281
13.1.5 解决远程访问部署难题的指导 方针	283
13.1.6 连接管理器	283
13.1.7 网络隔离区服务	284
13.1.8 网络访问隔离区控制组件	285
13.1.9 网络访问隔离区控制的工作原理	286
13.2 规划远程访问战略	286
13.2.1 确定远程访问硬件要求的指导 方针	287
13.2.2 ISP 提供的组件和功能	288
13.2.3 部署远程访问服务器的指导方针	288
13.2.4 VPN 服务器放置	289
13.2.5 远程访问的数据加密	290
13.2.6 在 VPN 客户端上创建路由项 的技术	291
13.2.7 远程访问连接条件的属性	292
13.2.8 创建高度可用的远程访问解决 方案的指导方针	293
13.2.9 实验 13-1: 启用安全远程访问 协议	293
13.3 实现 VPN 服务器	293
13.3.1 配置 VPN 服务器的方法	294
13.3.2 配置 RAS 锁定的方法	294
13.3.3 配置名称解析的方法	295
13.4 部署网络访问隔离区控制组件	295
13.4.1 隔离区资源	296
13.4.2 校验客户端配置的脚本	297
13.4.3 在远程访问服务器上安装 Rqs.exe 的方法	297
13.4.4 为 VPN 客户端配置安装和配置 CMAC 的方法	298