



“网管员必读”系列推出之后又一经典力作

网络工程师必读

——网络安全系统设计

NETWORK ENGINEER

王 达 编著
飞思科技产品研发中心 监制

- ◆ **一本真正全局意义上的安全系统设计类图书**
真正以OSI/RM七层结构为主线的安全系统设计类图书，较全面、系统地介绍了OSI/RM七层结构中各层的主要安全技术及其应用。
- ◆ **专业的一手技术资料**
本书所介绍的网络安全技术均来自相关技术或者协议的原始资料和真实的应用实践总结，技术原理介绍深入、系统、全面，填补了国内图书在这方面的空白。
- ◆ **庞大的读者服务体系**
提供了庞大、完善的读者服务体系，方便读者交流。包括11个读者QQ群，两大主流媒体（51CTO和CSDN）的专家博客，两个读者交流技术圈，一个学生大本营。详情参见其中一个博客：winda.blog.51cto.com。



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

王 达
飞思科技产品研发中心

编著
监制

网络工程师必读

——网络安全系统设计

NETWORK ENGINEER



电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书从网络工程师的职业角度出发组织和安排内容,非常具有针对性。本书从网络安全系统设计全局出发,以 OSI/RM 的 7 层结构为主线,层层把关,全面、系统地介绍各层的主要安全技术和方案设计思路、方法。

本书从深层次分析了网络安全隐患存在的各个主要方面,然后从这几个方面出发,全面介绍企业局域网安全防护系统的设计方法。其中包括网络安全系统设计综述、物理层的网络安全保护方案、数据链路层的安全保护方案、网络层防火墙安全保护方案、网络层 Kerberos 身份认证方案、网络层证书身份认证、加密和签名方案、网络层 PKI 综合应用方案设计、网络层 IPSec 身份认证和加密方案、传输层 TLS/SSL 身份认证和加密方案、应用层 Web 服务器的综合安全系统设计与配置、WLAN 网络综合安全系统设计与配置,并通过实际可用的安全防护方法来实现网络安全隐患的排除或防护。这些不同方面的安全防护措施形成了一个系统的整体,使得企业网络从各个方面都得到足够的安全保证。以上这些都是网络工程师所必须掌握的基础知识和技能。

本书适合网络工程师参考学习,也可作为高等院校及相关培训机构的教材。

未经许可,不得以任何方式复制或抄袭本书的部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

网络工程师必读. 网络安全系统设计 / 王达编著. —北京: 电子工业出版社, 2009.8
ISBN 978-7-121-08336-5

I. 网… II. 王… III. 计算机网络—安全技术—系统设计 IV. TP393

中国版本图书馆 CIP 数据核字(2009)第 052921 号

责任编辑: 杨 鹂

印 刷: 北京天宇星印刷厂

装 订: 三河市皇庄路通装订厂

出版发行: 电子工业出版社

北京海淀区万寿路 173 信箱 邮编: 100036

开 本: 787×1092 1/16 印张: 48 字数: 1382.4 千字

印 次: 2009 年 8 月第 1 次印刷

印 数: 3 500 册 定价: 89.00 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 zlt@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。

朋友，你是否正有打算朝着网络安全工程方面发展，成为一名当前国内外最热门又最紧缺、最有发展前景的 IT 职业人士——网络安全工程师呢？你是否正为没有系统的网络安全系统设计方面的权威指南而发愁呢？本书或许是您很好的选择。

本书是目前国内 IT 图书市场中第一本真正从设计角度系统地介绍网络安全系统设计和综合方案的图书。本书最大的特点就是深入、系统地介绍了许多目前主流应用的网络安全技术体系架构和功能实现原理，如 Kerberos、证书和证书服务、IPSec、TLS/SSL 等。可能有许多读者对深奥的理论不感兴趣，在笔者所接触的网友中，的确有许多网友是这样的，只喜欢实操型的书籍。如果作为网络管理员，这可以理解，但是如果作为网络工程师，有这样的心态就非常不正确了。因为网络管理员的工作基本上都是操作型的，而网络工程师的工作则主要是进行各类系统的设计，是底层的。没有全面、深入、扎实的理论基础，不可能对相应技术有一个本质上的理解和运用，更谈不上利用这些技术来设计解决方案了。这就是网络管理员和网络工程师的一个本质区别。

📖 本书主要内容

《网络工程师必读——网络安全系统设计》与笔者在本系列中写的另一部图书——《网络工程师必读——网络系统设计》一样，题目非常大（指其内涵），所涉及的技术、产品和方案非常广。就像我们在写一篇作文一样，题目越大，文章越难写。因为要写，或者可写的内容实在太多、太广，从主题选取，到各主题内容的选取都不是一件简单的事。毕竟就目前来说，网络安全已自成一个庞大的系统，所涉及的技术、产品和方案渗透到了网络领域的各个角落，而无论如何，一本书的篇幅都是非常有限的。所以，在笔者正式写这部书之前，仅写什么和怎么写这两个方面就考虑了非常长的时间。而且在编写这部书之前，总希望能借鉴一些已有的网络安全系统设计类图书的主题选取和写作方法，总希望用有限的篇幅尽可能系统地介绍一些主流的网络安全技术和方案设计思路。但非常遗憾，笔者在网络上查看了近 20 部网络安全类图书的目录，竟然没有一部是希望看到的。所以，笔者最终还是只能靠自己，从头设计本书的主体架构，包括整部图书的章节安排（也可以算是整部图书的体系架构）、各章的主题，以及各章内部的主要内容。综合起来是这样一个基本的写作思路：整部图书的主线是 OSI/RM 的 7 层结构，各章主要针对各主要层次的主要安全技术和方案进行展开，并在本书最后介绍了几个综合的网络安全系统设计和配置方案。

本书共 11 章，具体内容安排如下。

第 1 章 网络安全系统设计综述

本章主要对目前主要的网络隐患、所涉及的主要网络安全技术，以及网络安全系统的设计基本思路进行综合介绍。

第 2 章 物理层的网络安全保护方案

本章主要对基于 OSI/RM 物理层的主要网络安全保护技术和方案进行具体介绍。其中所涉及到的网络安全技术包括计算机网络通信物理介质、线路和设备的屏蔽、网络通信线路的物理隔离、网络通信线路的冗余、数据备份和容灾，以及典型网络物理层的安全保护工具的介绍等。

第 3 章 数据链路层的安全保护方案

本章主要介绍了各种主要的数据链路层可用的加密技术，以及 WLAN 网络中所用的各种数据链路加密、身份验证技术原理和配置方法，如 WEP、WPA、WPA2、IEEE 802.1x 和 IEEE 802.11i 等。还介绍了主流品牌网络设备 MAC 地址绑定和嗅探防护等。至于 VLAN 方面的详细配置在本系列的《网络工程师必读——网络设备配置与管理》（交换机分册）一书中介绍。

第 4 章 网络层防火墙安全保护方案

本章专门根据防火墙设备的主要应用，介绍了内、外围网络中防火墙安全保护系统的设计思路和方法。

第 5 章 网络层 Kerberos 身份认证方案

本章全面、深入地介绍了在 Windows 系统中默认采用的 Kerberos 身份认证技术体系架构、深层身份验证原理、主要应用及基本配置方法。这是目前国内图书市场和网站上极难得到的第一手专业文献。

第 6 章 网络层证书身份认证、加密和签名方案

本章主要以 Windows Server 2003 系统为例全面、深入地介绍了证书和证书服务技术体系架构、深层身份认证、数据加密和电子签名原理，以及证书服务系统的基本设计方法。这也是目前国内图书市场和网站上极难得到的第一手专业文献。

第 7 章 网络层 PKI 综合应用方案设计

本章介绍了各种规模的企业中 PKI 公钥基础结构中的 CA 层次结构设计、证书颁发和吊销、证书配置文件、规划密钥和数据恢复方案配置等几个重要方面内容。

第 8 章 网络层 IPSec 身份认证和加密方案

本章全面、深入地介绍了 IPSec 安全技术体系架构，AH 和 ESP 协议深层加密和身份认证原理，以及 IPSec 方案的设计思路、原则和基本应用配置方法。这也是目前国内图书市场和网站上极难得到的第一手专业文献。



在网络层的像 ACL、NAT、VPN 等其他一些安全保护方案，因为在本系列的丛书《网络工程师必读——网络设备配置与管理》（交换机分册）和《网络工程师必读——虚拟专用网》两书中已有详细介绍，所以不再在本书中介绍。

第 9 章 传输层 TLS/SSL 身份认证和加密方案

本章全面、深入地介绍了 TLS、SSL 技术体系架构、深层加密、数据完整性检查、身份

认证和数字签名原理，以及主流 TLS/SSL 应用方案的配置方法。

第 10 章 应用层 Web 服务器的综合安全系统设计与配置

本章以 IIS Web 服务器为主体，全面、细致地介绍了 Web 服务器网络安全系统设计的基本思路、检查表项和配置方法，着重介绍了各个方面的具体配置方法，可操作性和实用性极强。

第 11 章 WLAN 网络综合安全系统设计与配置

本章全面、细致地介绍了网络安全相对脆弱的 WLAN 无线网络的安全系统设计方法。其中不仅综合用到了本书第 3 章中介绍的各种基于当前主流 WLAN 安全技术(如 WEP、WPA、WPA2、802.1x)，还用到了有线网络中所用的一些主流网络安全技术和方案(如 IPSec、RADIUS、PKI 等)。本章还着重介绍了综合的 WLAN 网络安全方案设计思路和方法，并介绍了典型的配置示例，可操作性和实用性极强。

本书主要特色

正如有以上整体规划，所以才使本书具有非常鲜明的特色，具体体现在以下几个方面。

● 真正的“设计”视角

在目前的图书市场中，尽管也有的书以“网络安全系统设计”命名，但极少是真正从设计角度进行章节和内容编排的，基本上都是在谈各方面的软件漏洞修补、黑客攻击原理、工具使用、加密算法等。笔者认为，这些对于完善的网络安全系统设计来说并不是最重要的，因为软件漏洞时刻在变化，而且每天都有一些软件退出历史舞台，也有大批新的软件发布上市，与之相对应的各种黑客攻击方法和工具也会不断变化。而每款软件都有它自身的 Bug，也就必然存在一些安全漏洞，尽管我们自己可以通过一些补丁程序来修补漏洞，但更多的还是要依赖开发相应软件的公司。如果我们的安全系统主要考虑这个方面，就太被动了，也本末倒置了，必然造成我们的安全系统需要不断地修改，紧跟这些软件漏洞进行修复。事实上，软件系统本身的漏洞完全可以通过我们网络安全系统中的一个极小部分(也就是及时更新软件补丁，有分离式的，也有集中式的，如部署 WUS 服务器)来全面解决，网络通信中要解决的真正的安全问题不是这些终端的安全问题，而是通信过程中的安全问题。

本书从网络安全系统设计全局出发，以 OSI/RM 的 7 层结构为主线，层层把关，较全面、系统地介绍各层的主要安全技术和方案设计思路、方法。

● 专业、深入

本书介绍了许多大型的网络安全技术和方案，主要包括物理层的各种介质，线路屏蔽技术和方案，数据链路层加密技术和方案，WLAN 无线网络安全系统方案，防火墙系统方案，Kerberos 身份验证技术和方案，证书的加密、签名、身份验证技术和方案，IPSec 加密、身份验证技术和方案，PKI 公钥基础结构系统设计，ACL、NAT、VPN 等技术，TLS/SSL 加密、身份验证技术和方案，WLAN 综合安全系统设计，Web 服务器安全系统设计等。

而且在介绍技术原理时，不再像同类书那样仅停留在表面上，而是深入挖掘了各技术的体系结构及各子技术的工作原理，使读者对相应技术有一个全面、深入的了解。其中像 Kerberos、证书和证书服务、TLS/SSL 等都是取材自 IETF、Netscape 和 Microsoft 英文官网上的第一手专业资料，在此非常感谢这些国外的公司为我们提供如此专业的技术参考文献。笔

者同时对内容进行了展开和具体化，使枯燥的原理也具有了灵气。

- 实用性和可读性强

即使在介绍技术时，本书也是结合实际的应用进行介绍的，所以读者在全面了解本书所介绍的技术后，就可以掌握相应技术的主要应用，应用于自己的设计方案中。另外，本书也从真正设计视角介绍了一些典型网络安全系统的设计方法，如 WLAN 无线网络的安全系统设计、PKI 公钥基础结构系统设计、Web 服务器安全系统设计等。所以，本书的实用性和可读性比较强，希望能使读者做到学以致用。

本书提供的服务

本书由王达主笔并统稿，参加编写、校验和排版的人员有：何艳辉、王珂、沈芝兰、马平、何江林、刘凤竹、卢京华、周志雄、洪武、高平复、周建辉、孔平、尚宝宏、姚学军、刘学、李翔、王娇、李敏、吴鹏飞等，在此一并表示由衷的感谢。由于编者水平有限，加之时间紧张，尽管我们花了大量时间和精力校验，但书中可能还存在一些错误，敬请各位读者批评指正，万分感谢！另提供了 7 个读者 QQ 群：73417650、17201450、21566766、32354930、5208368、13836245、4789821，2 个网上培训专用 QQ 群：17838740、57828783，以及 VIP 读者群：54435786。最新资讯请看我的博客：<http://winda.blog.51cto.com/>。

编 著 者

联系方式

咨询电话：(010) 88254160 88254161-67

电子邮件：support@fecit.com.cn

服务网址：<http://www.fecit.com.cn> <http://www.fecit.net>

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

CONTENTS

目 录

第 1 章 网络安全系统设计综述	1	1.5.3 评估现有网络安全策略	24
1.1 网络安全系统设计基础	2	1.5.4 设计细化的新网络安全策略初稿	25
1.1.1 网络安全的发展	2	1.5.5 第一次小范围的测试、评估和修改	31
1.1.2 网络安全威胁基础	4	1.5.6 第二次中、大范围的测试、评估和修改	32
1.1.3 企业网络的主要安全隐患	6	1.5.7 新网络安全策略文档终稿	32
1.1.4 网络安全系统的基本组成	7	1.5.8 新网络安全策略系统的正式应用	32
1.2 OSI/RM 各层的安全保护	9	第 2 章 物理层的网络安全保护方案	33
1.2.1 物理层的安全保护	9	2.1 物理层安全保护概述	34
1.2.2 数据链路层的安全保护	11	2.2 物理层的线路窃听技术分析	34
1.2.3 网络层的安全保护	12	2.3 计算机网络通信线路屏蔽	35
1.2.4 传输层的安全保护	13	2.3.1 选择屏蔽性能好的传输介质和适配器	36
1.2.5 会话层和表示层的安全保护	14	2.3.2 屏蔽机房和机柜的选择	38
1.2.6 应用层的安全保护	15	2.3.3 WLAN 无线网络的物理层安全保护	39
1.3 系统层的安全保护	16	2.4 物理线路隔离	40
1.4 网络安全系统设计	16	2.4.1 主要物理隔离产品	40
1.4.1 网络安全策略	16	2.4.2 物理隔离网闸的隔离原理	43
1.4.2 网络安全系统设计的基本原则	17	2.4.3 物理隔离网闸的典型应用	46
1.5 网络安全系统设计的思路	20	2.5 设备和线路冗余	46
1.5.1 安全隐患分析和基本系统结构信息的收集	20		
1.5.2 调查和分析当前网络的安全需求	23		

2.5.1	网络设备部件冗余	47	3.2.2	链路加密机.....	90
2.5.2	网络设备整机冗余	49	3.2.3	网卡集成式链路 加密原理	92
2.5.3	网络线路冗余	51	3.3	WLAN SSID 安全技术及 配置方法	94
2.6	机房和账户安全管理.....	51	3.3.1	SSID 概念及配置 方法	94
2.6.1	机房安全管理	51	3.3.2	BSSID 和 ESSID	95
2.6.2	账户安全管理	52	3.3.3	SSID 的安全问题	96
2.7	数据安全的管理	52	3.4	WLAN MAC 地址过滤	97
2.7.1	数据容灾概述	53	3.5	WLAN WEP 加密	98
2.7.2	容灾与存储、容错、 备份和远程复制的 关系	54	3.5.1	WEP 加密原理	98
2.7.3	数据容灾等级	56	3.5.2	WEP 解密原理	99
2.7.4	灾难恢复的关键 注意事项	60	3.5.3	WEP 加密的不足	99
2.8	物理层安全管理工具	61	3.5.4	WEP 加密的配置 方法	100
2.8.1	泛达综合布线实时 管理系统	61	3.6	WPA 加密	102
2.8.2	Molex 综合布线实时 管理系统	64	3.6.1	WPA 的 WLAN 链路加密	102
2.9	服务和账户安全规划	66	3.6.2	WPA 中的 IEEE 802.1x 身份认证系统	103
2.9.1	服务和账户安全 规划概述	66	3.6.3	EAPOL 消息的封装	105
2.9.2	服务的安全漏洞和 账户	67	3.6.4	IEEE 802.1x 的 认证过程	107
2.9.3	Windows Server 2003 中 服务的默认安全 设置更改	69	3.7	WPA2 加密	111
2.9.4	安全运行服务的原则	70	3.7.1	WPA2 简介	111
2.9.5	如何更安全地运行 服务	72	3.7.2	AES-CCMP 基础	112
3	数据链路层的安全保护方案	81	3.7.3	AES 算法的基本 原理	113
3.1	典型数据加密算法	82	3.7.4	WPA2 AES-CCMP 加/解密原理	115
3.1.1	基于“消息摘要”的 算法	82	3.8	无线 AP/路由器的 WPA 和 WPA2 设置	118
3.1.2	“对称/非对称密钥” 加密算法	85	3.8.1	个人用户无线 AP/路由器 的 WPA-PSK 或 WPA2-PSK 设置	119
3.2	数据加密	87	3.8.2	企业级无线 AP/路由器 的 WPA 或 WPA2 设置	120
3.2.1	数据加密技术	87			

3.8.3	WLAN 客户端第三方软件的 WPA 和 WPA2 设置	121	3.14	H3C S5600 交换机基于端口的 MAC 地址绑定	141
3.8.4	Windows XP 无线客户端 WPA/WPA2 配置	125	3.14.1	S5100 系列交换机的 Security MAC 地址配置	141
3.9	最新的 WLAN 安全标准——IEEE 802.11i	126	3.14.2	S5600 系列交换机的 Security MAC 地址配置	142
3.9.1	IEEE 802.11i 概述	127	3.15	H3C SR8800 系列业务路由器 MAC 和 IP 地址绑定	144
3.9.2	WRAP 加密机制	127	3.15.1	MAC 和 IP 地址绑定配置	144
3.10	MAC 地址欺骗防护	129	3.15.2	MAC 和 IP 地址绑定典型配置示例	146
3.10.1	ARP 和 RARP 协议工作原理	130	3.16	H3C SecPath 系列防火墙上的 MAC 和 IP 地址绑定	147
3.10.2	ARP 协议帧格式	131	3.16.1	MAC 和 IP 地址绑定配置	148
3.10.3	MAC 地址欺骗原理	132	3.16.2	MAC 和 IP 地址绑定典型配置示例	149
3.10.4	MAC 地址欺骗预防	133	3.17	网络嗅探的防护	149
3.11	Cisco 设备上基于端口的 MAC 地址绑定	136	3.17.1	网络嗅探原理	149
3.11.1	基于端口的单一 MAC 地址绑定基本配置步骤	136	3.17.2	网络嗅探的防范	151
3.11.2	基于端口的单一 MAC 地址绑定配置示例	138	第 4 章	网络层防火墙安全保护方案	153
3.12	Cisco 基于端口的多 MAC 地址绑定	138	4.1	防火墙的分类和技术	154
3.12.1	基于端口的多 MAC 地址绑定配置思路	138	4.1.1	包过滤防火墙简介	154
3.12.2	基于端口的多 MAC 地址绑定配置示例	139	4.1.2	包过滤技术的发展	155
3.13	Cisco 设备上基于 IP 的 MAC 地址绑定	139	4.1.3	包过滤原理	155
3.13.1	一对一的 MAC 地址与 IP 地址绑定	139	4.1.4	包过滤技术的主要优、缺点	156
3.13.2	一对多，或者多对多的 MAC 地址与 IP 地址绑定示例	140	4.1.5	代理防火墙	157
			4.2	防火墙系统的设计	158
			4.2.1	内、外部防火墙系统	158
			4.2.2	防火墙在企业网络体系结构中的位置	159
			4.2.3	典型防火墙系统设计	161

4.3	防火墙在网络安全防护中的 主要应用	164	5.2.3	Kerberos V5 协议 标准	188
4.3.1	控制来自互联网对 内部网络的访问	164	5.2.4	Kerberos V5 身份认证 所用端口	190
4.3.2	控制来自第三方局域网 对内部网络的访问	166	5.3	Kerberos SSP 认证	190
4.3.3	控制局域网内部不同 部门之间的访问	167	5.4	Kerberos 物理结构	192
4.3.4	控制对服务器中心的 网络访问	168	5.4.1	Kerberos 中的 密钥	192
4.4	内部防火墙系统设计	169	5.4.2	Kerberos 票证	195
4.4.1	内部防火墙系统 概述	170	5.4.3	认证符	199
4.4.2	内部防火墙规则	170	5.4.4	凭证缓存	200
4.4.3	内部防火墙的 可用性需求	171	5.4.5	密钥分发中心 (KDC)	200
4.4.4	内部容错防火墙集 配置	174	5.5	Kerberos V5 交换和消息 摘要	204
4.4.5	内部防火墙系统设计 的其他因素要求	175	5.5.1	Kerberos V5 身份认证 的 3 个子协议	204
4.5	外围防火墙系统设计	177	5.5.2	身份认证服务 (AS) 交换	205
4.5.1	外围防火墙系统 概述	178	5.5.3	票证许可服务 (TGS) 交换	206
4.5.2	外围防火墙规则	178	5.5.4	客户端/服务器 (CS) 交换	207
4.5.3	外围防火墙系统的 可用性要求	179	5.6	Kerberos 交换消息详解	207
第 5 章	网络层 Kerberos 身份认证 方案	181	5.6.1	身份认证服务交换 消息详解	208
5.1	身份认证概述	182	5.6.2	票证许可服务交换 消息详解	211
5.1.1	单点登录身份认证 执行方式	182	5.6.3	客户端/服务器身份认证 交换消息详解	214
5.1.2	主要的身份认证 类型	183	5.7	Kerberos 身份认证应用 示例	216
5.2	Kerberos 身份认证基础	183	5.7.1	本地登录示例	216
5.2.1	Kerberos V5 身份 认证机制	184	5.7.2	域登录示例	217
5.2.2	Kerberos V5 身份 认证的优点与缺点	187	5.7.3	域用户的工作站 登录	217
			5.7.4	单域身份认证示例	223
			5.7.5	用户到用户的 身份认证	226

5.8	Kerberos V5 身份认证的 启用与策略配置.....	228	6.7	证书服务物理结构.....	266
第 6 章	网络层证书身份认证、加密 和签名方案.....	231	6.7.1	证书数据库和 CA 日志文件.....	267
6.1	证书和证书服务基础.....	232	6.7.2	注册表.....	267
6.1.1	证书概述.....	232	6.7.3	活动目录.....	267
6.1.2	证书的主要功能.....	233	6.7.4	文件系统.....	269
6.1.3	证书的主要应用.....	235	6.8	证书服务进程和交互.....	270
6.1.4	证书客户端角色.....	239	6.8.1	证书是如何创建的.....	270
6.1.5	证书服务概述.....	240	6.8.2	证书的自动注册.....	272
6.2	CA 证书.....	241	6.8.3	证书的手动注册.....	277
6.2.1	CA 证书简介.....	241	6.8.4	自定义证书注册和 更新应用.....	279
6.2.2	CA 证书应用的 情形.....	242	6.8.5	使用可选组件注册 和续订.....	281
6.3	证书结构.....	243	6.8.6	证书是如何吊销的.....	283
6.3.1	证书体系架构.....	243	6.9	证书模板属性选项和设计.....	287
6.3.2	证书模板.....	245	6.9.1	证书模板属性选项.....	287
6.3.3	证书的物理和 逻辑存储.....	250	6.9.2	证书模板设计方面 的考虑.....	294
6.3.4	证书存储区.....	253	6.9.3	证书模板规划 注意事项.....	296
6.4	CA 证书进程和交互.....	255	6.9.4	证书模板的部署.....	299
6.4.1	根 CA 证书是如何 被创建的.....	256	第 7 章	网络层 PKI 综合应用 方案设计.....	303
6.4.2	根 CA 证书是如何 被更新的.....	257	7.1	本章概述.....	304
6.4.3	从属 CA 证书是如何 被创建的.....	258	7.1.1	部署 PKI 的必要性和 本章所使用的技术.....	304
6.4.4	合格的从属策略是 如何被应用的.....	259	7.1.2	规划和部署 PKI 的 基本流程.....	306
6.5	证书服务体系架构.....	260	7.2	定义证书需求.....	307
6.5.1	证书服务引擎.....	261	7.2.1	确定安全应用需求.....	308
6.5.2	策略模块.....	262	7.2.2	确定证书需求.....	312
6.5.3	客户端策略模块.....	263	7.2.3	文档化证书策略和 证书实施声明.....	314
6.5.4	退出模块.....	263	7.2.4	定义证书应用需求 示例.....	315
6.5.5	证书数据库.....	264	7.3	设计证书颁发机构层次 结构.....	316
6.5.6	CryptoAPI 接口.....	264			
6.5.7	证书服务协议.....	264			
6.6	证书服务接口.....	265			

7.3.1	规划核心 CA 选项 ——设计根 CA	317
7.3.2	规划核心 CA 选项 ——选择内部与 第三方 CA	318
7.3.3	规划核心 CA 选项 ——评估 CA 容量、 性能和可扩展需求	320
7.3.4	规划核心 CA 选项 ——PKI 管理模式	322
7.3.5	规划核心 CA 选项 ——CA 类型和角色	323
7.3.6	规划核心 CA 选项 ——整体活动目录 结构	327
7.3.7	规划核心 CA 选项 ——CA 安全性	329
7.3.8	规划核心 CA 选项 ——确定 CA 数量	333
7.3.9	选择信任模式	334
7.3.10	在信任层次结构中 定义 CA 角色	338
7.3.11	建立命名协定	338
7.3.12	选择 CA 数据库 位置	338
7.3.13	CA 结构设计示例	339
7.4	扩展证书颁发机构结构	341
7.4.1	评估影响扩展信任 的因素	341
7.4.2	选择扩展 CA 结构 配置	344
7.4.3	限制计划外的信任	346
7.5	定义证书配置文件	348
7.5.1	选择证书模板	349
7.5.2	选择证书安全选项	350
7.5.3	使用合格的从属来 限制证书	354
7.5.4	配置证书示例	359
7.6	创建证书管理规划	360

7.6.1	选择注册和续订 方法	361
7.6.2	将证书映射到身份	363
7.6.3	创建证书吊销策略	368
7.6.4	规划密钥和数据 恢复	372
7.6.5	创建证书管理规划 示例	375

第 8 章 网络层 IPsec 身份认证和

	加密方案	377
8.1	IPsec 基础	378
8.1.1	什么是 IPsec	378
8.1.2	IPsec 的设计初衷	379
8.1.3	IPsec 的优势	381
8.2	IPsec 提供的安全服务	382
8.2.1	IPsec 提供的安全 属性	382
8.2.2	Kerberos V5 身份 认证协议	383
8.2.3	基于公钥证书的 身份认证	383
8.2.4	预共享密钥验证	384
8.2.5	采用哈希函数的 数据完整性验证	384
8.2.6	具有加密功能的 数据保密性	385
8.2.7	密钥管理	386
8.2.8	密钥保护	386
8.3	IPsec 的使用模式	388
8.3.1	传输模式	388
8.3.2	隧道模式	389
8.4	IPsec 协议类型	389
8.4.1	IPsec AH 协议	390
8.4.2	IPsec ESP 协议	394
8.5	Windows Server 2003 中 的 IPsec	397
8.5.1	IPsec 逻辑体系 架构	398

8.5.2	IPSec 身份认证和 组件	401	8.9.3	IPSec 策略设计与规划 的最佳操作	442
8.5.3	策略代理体系架构	402	8.9.4	建立 IPSec 安全 计划	445
8.5.4	IKE 模块体系架构	405	8.9.5	策略配置	446
8.5.5	IPSec 驱动体系架构	407	8.9.6	默认筛选器列表	446
8.5.6	IPSec 策略数据结构	407	8.9.7	默认响应规则	448
8.5.7	IPSec 分配的网络端口 和协议	410	8.9.8	IPSec 策略的 应用方法	450
8.5.8	IPSec 策略规则	411	8.10	IPSec 应用方案设计	453
8.6	IPSec 密钥安全关联和密钥 交换原理	415	8.10.1	IPSec 安全通信方案 的主要应用	454
8.6.1	安全关联基本原理 和类型	415	8.10.2	不推荐的 IPSec 方案	458
8.6.2	主模式协商 SA	417	8.10.3	管理使用仅在 Windows Server 2003 家族中 可用的新增功能的 策略	458
8.6.3	快速模式协商 SA	424	8.10.4	IP 筛选器配置的 考虑	459
8.6.4	密钥交换原理	426	8.10.5	筛选器操作的 配置考虑	461
8.6.5	SA 生存期	427	8.11	IPSec 策略的应用方案 配置	462
8.7	IPSec 驱动工作原理	427	8.11.1	IPSec 方案配置前 的准备	462
8.7.1	IPSec 驱动的职责	427	8.11.2	IPSec 安全方案配置 的基本步骤	463
8.7.2	IPSec 驱动通信	428	8.11.3	IPSec 在 Web 服务器 访问限制中的应用 示例	464
8.7.3	IPSec 驱动程序模式	428	8.11.4	IPSec 在数据库服务器 访问限制中的应用 示例	475
8.7.4	IPSec 驱动的包处理	430	8.11.5	IPSec 在阻止 NetBIOS 攻击中的应用示例	476
8.8	IPSec 策略及策略筛选器	431	8.11.6	IPSec 在保护远程访问 通信中的应用示例	478
8.8.1	IPSec 策略	431			
8.8.2	IPSec 策略规则	433			
8.8.3	默认响应规则	434			
8.8.4	IPSec 策略筛选器	435			
8.8.5	IPSec 筛选器的 应用顺序	437			
8.8.6	IPSec 筛选中的默认 排除	438			
8.8.7	IPSec 筛选器的设计 考虑	440			
8.9	Windows Server 2003 IPSec 系统的部署	441			
8.9.1	Windows Server 2003 IPSec 部署的简易性	441			
8.9.2	部署 Windows Server 2003 IPSec 前所需的确认	442			

第 9 章 传输层 TLS/SSL 身份认证和加密方案	481
9.1 TLS/SSL 基础.....	482
9.1.1 TLS/SSL 简介	482
9.1.2 TLS/SSL 标准的 历史	483
9.1.3 TLS 与 SSL 的区别	483
9.1.4 TLS/SSL 所带来的 好处	484
9.1.5 TLS/SSL 的局限性	485
9.1.6 常见的 TLS/SSL 应用	485
9.1.7 安全通道技术	487
9.1.8 TLS 和 SSL 的依从	487
9.2 TLS/SSL 体系架构.....	488
9.2.1 安全通道 SSPI 体系 架构	488
9.2.2 TLS/SSL 体系架构	490
9.2.3 TLS/SSL 握手协议	491
9.2.4 记录层	495
9.3 TLS/SSL 工作原理.....	495
9.3.1 TLS/SSL 进程和 交互机制.....	495
9.3.2 TLS 的完整握手 过程	497
9.3.3 客户端 Hello 消息	498
9.3.4 服务器 Hello 消息	501
9.3.5 客户端响应 Hello 消息	503
9.3.6 计算主密钥和子系列 密钥	504
9.3.7 完成消息	505
9.3.8 应用数据流	506
9.3.9 恢复安全会话	507
9.3.10 重新协商方法	507
9.3.11 安全通道的证书 映射	509
9.3.12 TLS/SSL 所使用的 网络端口	510

9.4 WTLS	511
9.4.1 WAP 的主要特点和 体系架构	511
9.4.2 WAP 架构与 WWW 架构的比较	514
9.4.3 WAP 安全机制	516
9.4.4 WTLS 体系架构.....	518
9.4.5 WTLS 的安全功能.....	519
9.4.6 WTLS 与 TLS 的 区别	520
9.5 SSL 在 IIS Web 服务器中 的应用	522
9.5.1 安装 CA	522
9.5.2 生成证书申请.....	524
9.5.3 提交证书申请.....	527
9.5.4 证书的颁发和导出.....	530
9.5.5 在 Web 服务器上 安装证书	532
9.5.6 在 Web 服务器上 启用 SSL	534
9.6 SSL VPN.....	535
9.6.1 SSL VPN 网络结构 和主要应用	536
9.6.2 SSL VPN 的主要优势 和不足	537

第 10 章 应用层 Web 服务器的综合 安全系统设计与配置	541
10.1 我国网站安全现状	542
10.2 Web 服务器的身份验证 技术选择	543
10.2.1 NTLM 身份验证机制 选择和配置方法	543
10.2.2 Kerberos 身份验证机制 选择和配置方法	547
10.2.3 摘要式身份验证机制 选择和配置方法	548
10.2.4 公钥加密身份认证 机制选择	553

10.2.5	证书身份认证机制 选择和配置方法.....	555
10.3	Web 服务器传输层安全技术 选择.....	558
10.4	Web 服务器的安全威胁 与对策.....	559
10.4.1	主机枚举.....	560
10.4.2	拒绝服务.....	562
10.4.3	未经授权的访问.....	562
10.4.4	随意代码执行.....	563
10.4.5	特权提升.....	563
10.4.6	病毒、蠕虫和 特洛伊木马.....	564
10.5	安全 Web 服务器检查表.....	564
10.6	Windows Server 2003 Web 服务器安全策略设计.....	580
10.6.1	Web 服务器的匿名 访问和 SSLF 设置.....	581
10.6.2	Web 服务器审核 策略设置.....	582
10.6.3	Web 服务器用户权限 分配策略设置.....	591
10.6.4	Web 服务器的安全 选项策略设置.....	600
10.6.5	Web 服务器的事件 日志策略设置.....	617
10.6.6	Web 服务器的其他 安全策略设置.....	619
第 11 章	WLAN 网络综合安全系统 设计与配置.....	629
11.1	选择 WLAN 的安全 策略.....	630
11.1.1	WLAN 面临的主要 安全问题.....	630
11.1.2	WLAN 安全策略的 决策.....	631
11.1.3	如何真正确保 WLAN 的安全.....	633
11.1.4	WLAN 的身份验证 和授权.....	634
11.1.5	WLAN 的数据保护.....	635
11.1.6	使用 WLAN 数据 保护的 IEEE 802.1x 的优点.....	637
11.2	WLAN 安全方案选择.....	637
11.2.1	不部署 WLAN 技术.....	638
11.2.2	使用基于 802.11 静态 WEP 的基本安全.....	638
11.2.3	使用 EAP 和动态加密 密钥的 IEEE 802.1x.....	639
11.2.4	使用 EAP-TLS 的 IEEE 802.1x.....	640
11.2.5	使用 PEAP 的 IEEE 802.1x.....	640
11.2.6	使用 VPN 技术保护 WLAN 网络.....	641
11.2.7	使用 IPSec 保护 WLAN.....	643
11.2.8	主要 WLAN 安全 方案比较.....	644
11.3	使用 IEEE 802.1x 设计 WLAN 安全系统.....	645
11.3.1	IEEE 802.1x WLAN 安全方案设计 基本思路.....	645
11.3.2	使用 IEEE 802.1x 和 加密确保 WLAN 安全.....	646
11.3.3	使用证书或密码.....	646
11.3.4	解决方案的先决 条件.....	647
11.3.5	WLAN 安全选项 考虑.....	648
11.3.6	确定 IEEE 802.1x WLAN 所需的软件设置.....	654
11.3.7	其他注意事项.....	658

11.4	使用 IEEE 802.1x 实现 WLAN 安全性.....	659
11.4.1	方案实现基本思路	659
11.4.2	IEEE 802.1x WLAN 计划工作表.....	660
11.4.3	准备安全 WLAN 的环境.....	661
11.4.4	配置和部署 WLAN 身份验证证书.....	662
11.4.5	配置 WLAN 访问基础结构.....	671
11.4.6	让用户和计算机能够访问安全 WLAN.....	675
11.4.7	配置 IEEE 802.1x 网络的无线接入点.....	680
11.4.8	测试和验证	681
11.5	IEEE 802.1x EAP-TLS WLAN 安全方案网络结构设计.....	681
11.5.1	IEEE 802.1x EAP-TLS 身份验证解决方案概述.....	681
11.5.2	IEEE 802.1x EAP-TLS WLAN 网络安全结构方案设计标准.....	684
11.5.3	IEEE 802.1x EAP-TLS 方案网络结构逻辑设计与评估.....	686

11.6	使用 PEAP 和密码确保无线 LAN 的安全.....	692
11.6.1	解决方案的基本思路.....	692
11.6.2	PEAP 解决方案的优势和工作原理	693
11.6.3	组织结构和 IT 环境计划	696
11.6.4	方案设计标准计划	697
11.6.5	WLAN 体系结构部署计划	698
11.6.6	针对大型组织的扩展计划	710
11.6.7	解决方案体系结构的变化计划	712
11.6.8	准备安全 WLAN 网络环境	715
11.6.9	方案网络证书颁发机构构建	725
11.6.10	WLAN 安全的基础结构构建	728
11.6.11	WLAN 客户端配置	741
后 记	747