

图书基本信息

书名：<<思科网络技术学院教程 CCNA安全>>

13位ISBN编号：9787115247629

10位ISBN编号：7115247625

出版时间：2011-4

出版时间：人民邮电

作者：思科网络技术学院

页数：302

译者：北京邮电大学

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

内容概要

本书所介绍的内容是针对思科网络技术学院最新的认证项目之一——CCNA安全课程，作为思科网络学院的指定教材，该书面向的读者群需要具备CCNA水平的知识。

本书共分9章，第1章介绍了现代网络安全威胁相关的知识，让大家了解网络安全发展的历史和现状，以及病毒、蠕虫和木马为典型代表的各种攻击的特点和防范。

随后的3章主要侧重于如何防止外部网络对内部网络的攻击，比如如何加强对路由器的保护、AAA认证以及防火墙技术和部署。

第5章介绍了如何对内部网络自身的保护，强调了网络入侵防御系统(IPS)的特点和在思科设备上的实现。

第6章是针对局域网的安全防护，主要侧重于对于交换网络的安全部署及配置。

第7章介绍了加密算法，普及了加密技术的基本知识。

第8章是本书的重要环节，介绍了使用路由器来实现虚拟专用网(VPN)技术，特别是IPsec技术的概念和配置。

第9章综合了前面的内容，介绍了如何设计和部署一个安全网络的全面解决方案，以及如何制定有效的安全策略等。

本书所介绍的内容涵盖了思科国际认证考试——CCNA安全(IINS 640-553)要求的全部知识，所以，读者也可以把本书作为该认证考试的考试指南。

作者简介

作者：（美国）思科网络技术学院 译者：北京邮电大学

书籍目录

第1章 现代网络安全威胁	1
1.1 一个安全网络的基本原则	1
1.1.1 网络安全的演进	1
1.1.2 网络安全的驱动者	3
1.1.3 网络安全组织	4
1.1.4 网络安全领域	6
1.1.5 网络安全策略	6
1.2 病毒、蠕虫和特洛伊木马	7
1.2.1 病毒	7
1.2.2 蠕虫	8
1.2.3 特洛伊木马	9
1.2.4 消除病毒、蠕虫和特洛伊木马	9
1.3 攻击方法	11
1.3.1 侦查攻击	11
1.3.2 接入攻击	12
1.3.3 拒绝服务攻击	13
1.3.4 消除网络攻击	15
第2章 保护网络设备	17
2.1 保护对设备的访问	17
2.1.1 保护边界路由器	17
2.1.2 配置安全的管理访问	20
2.1.3 为虚拟登录配置增强的安全性	22
2.1.4 配置SSH	23
2.2 分配管理角色	25
2.2.1 配置特权级别	25
2.2.2 配置基于角色的CLI访问	27
2.3 监控和管理设备	29
2.3.1 保证思科IOS和配置文件的安全	29
2.3.2 安全管理和报告	31
2.3.3 使用系统日志	33
2.3.4 使用SNMP实现网络安全	34
2.3.5 使用NTP	36
2.4 使用自动安全特性	37
2.4.1 执行安全审计	37
2.4.2 使用自动安全锁住路由器	39
2.4.3 用SDM锁定路由器	39
第3章 认证、授权和记账	42
3.1 使用AAA的目的	42
3.1.1 AAA概述	42
3.1.2 AAA的特点	43
3.2 本地AAA认证	44
3.2.1 使用CLI配置本地AAA认证	44
3.2.2 使用SDM配置本地AAA认证	46
3.2.3 本地AAA认证故障处理	47
3.3 基于服务器的AAA	47

- 3.3.1 基于服务器AAA的特点 47
- 3.3.2 基于服务器AAA通信协议 47
- 3.3.3 Cisco安全ACS 48
- 3.3.4 配置Cisco安全ACS 50
- 3.3.5 配置Cisco安全ACS用户和组 53
- 3.4 基于服务器的AAA认证 54
 - 3.4.1 使用CLI配置基于服务器的AAA认证 54
 - 3.4.2 使用SDM配置基于服务器的AAA认证 55
 - 3.4.3 基于服务器的AAA认证故障处理 56
- 3.5 基于服务器的AAA授权和记账 57
 - 3.5.1 配置基于服务器的AAA授权 57
 - 3.5.2 配置基于服务器的AAA记账 58
- 第4章 实现防火墙技术 60
 - 4.1 访问控制列表 60
 - 4.1.1 用CLI配置标准和扩展IP ACL 60
 - 4.1.2 使用标准和扩展IP ACL 63
 - 4.1.3 访问控制列表的拓扑和流向 64
 - 4.1.4 用SDM配置标准和扩展ACL 64
 - 4.1.5 配置TCP的Established和自反ACL 66
 - 4.1.6 配置动态ACL 68
 - 4.1.7 配置基于时间的ACL 69
 - 4.1.8 复杂ACL实现的排错 71
 - 4.1.9 使用ACL减少攻击 71
 - 4.2 防火墙技术 72
 - 4.2.1 防火墙构建安全网络 72
 - 4.2.2 防火墙类型 73
 - 4.2.3 网络设计中的防火墙 75
 - 4.3 基于上下文的访问控制 76
 - 4.3.1 CBAC特性 76
 - 4.3.2 CBAC运行 77
 - 4.3.3 配置CBAC 79
 - 4.3.4 CBAC排错 82
 - 4.4 区域策略防火墙 84
 - 4.4.1 基于策略防火墙的特点 84
 - 4.4.2 基于区域策略的防火墙运行 85
 - 4.4.3 用CLI配置区域策略防火墙 86
 - 4.4.4 用SDM配置区域策略防火墙 88
 - 4.4.5 使用SDM向导配置基于区域的策略防火墙 90
 - 4.4.6 区域策略防火墙排错 91
- 第5章 执行入侵防御 93
 - 5.1 IPS技术 93
 - 5.1.1 IDS和IPS特性 93
 - 5.1.2 基于主机的IPS执行 95
 - 5.1.3 基于网络的IPS执行 96
 - 5.2 IPS特征文件 98
 - 5.2.1 IPS特征文件特性 98
 - 5.2.2 IPS特征警报 100

- 5.2.3 调整IPS特征报警 102
- 5.2.4 IPS特征行动 102
- 5.2.5 管理和监视IPS 104
- 5.3 执行IPS 106
 - 5.3.1 使用CLI配置Cisco IOS IPS 106
 - 5.3.2 使用SDM配置Cisco IOS IPS 108
 - 5.3.3 修改思科IPS特征 110
- 5.4 检验和监测IPS 111
 - 5.4.1 检验Cisco IOS IPS 111
 - 5.4.2 监测Cisco IOS IPS 111
- 第6章 保护局域网 113
 - 6.1 终端安全 113
 - 6.1.1 终端安全概述 113
 - 6.1.2 使用IronPort的终端安全 115
 - 6.1.3 使用网络准入控制的终端安全 116
 - 6.1.4 使用Cisco安全代理的终端安全 118
 - 6.2 第二层安全考虑 119
 - 6.2.1 第二层安全概述 119
 - 6.2.2 MAC地址欺骗攻击 120
 - 6.2.3 MAC地址表溢出攻击 120
 - 6.2.4 STP操纵攻击 121
 - 6.2.5 LAN风暴攻击 121
 - 6.2.6 VLAN攻击 121
 - 6.3 配置第二层安全 123
 - 6.3.1 配置端口安全 123
 - 6.3.2 检验端口安全 124
 - 6.3.3 配置BPDU保护和根保护 125
 - 6.3.4 配置风暴控制 126
 - 6.3.5 配置VLAN中继(Trunk)安全 127
 - 6.3.6 配置Cisco交换端口分析器 128
 - 6.3.7 配置Cisco远程交换端口分析器 128
 - 6.3.8 对于第二层建议的实践 129
 - 6.4 无线、VoIP和SAN安全 130
 - 6.4.1 企业高级技术安全考虑 130
 - 6.4.2 无线安全考虑 131
 - 6.4.3 无线安全解决方案 131
 - 6.4.4 VoIP安全考虑 132
 - 6.4.5 VoIP安全解决方案 134
 - 6.4.6 SAN安全考虑 136
 - 6.4.7 SAN安全解决方案 138
- 第7章 密码系统 140
 - 7.1 密码服务 140
 - 7.1.1 保护通信安全 140
 - 7.1.2 密码术 142
 - 7.1.3 密码分析 144
 - 7.1.4 密码学 145
 - 7.2 基本完整性和真实性 145

- 7.2.1 密码散列 145
- 7.2.2 MD5和SHA-1的完整性 146
- 7.2.3 HMAC的真实性 147
- 7.2.4 密钥管理 148
- 7.3 机密性 150
 - 7.3.1 加密 150
 - 7.3.2 数据加密标准 152
 - 7.3.3 3DES 153
 - 7.3.4 高级加密标准 153
 - 7.3.5 替代加密算法 154
 - 7.3.6 Diffie-Hellman密钥交换 155
- 7.4 公钥密码术 156
 - 7.4.1 对称加密与非对称加密 156
 - 7.4.2 数字签名 157
 - 7.4.3 Rivest、Shamir和Alderman 159
 - 7.4.4 公共密钥基础架构 159
 - 7.4.5 PKI标准 161
 - 7.4.6 认证授权 162
 - 7.4.7 数字证书和CA 163
- 第8章 实现虚拟专用网络 165
 - 8.1 VPN 165
 - 8.1.1 VPN概述 165
 - 8.1.2 VPN拓扑 166
 - 8.1.3 VPN解决方案 168
 - 8.2 GRE VPN 170
 - 8.3 IPsec VPN组件和操作 171
 - 8.3.1 IPsec介绍 171
 - 8.3.2 IPsec安全协议 173
 - 8.3.3 因特网密钥交换 175
 - 8.4 使用CLI实现站点到站点的IPsec VPN 177
 - 8.4.1 配置一个站点到站点的IPsec VPN 177
 - 8.4.2 任务1——配置兼容ACL 178
 - 8.4.3 任务2——配置IKE 178
 - 8.4.4 任务3——配置变换集 179
 - 8.4.5 任务4——配置加密ACL 180
 - 8.4.6 任务5——应用加密映射 181
 - 8.4.7 验证IPsec配置和故障排除 182
 - 8.5 使用SDM实现站点到站点的IPsec VPN 182
 - 8.5.1 使用SDM配置IPsec 182
 - 8.5.2 VPN向导——快速安装 183
 - 8.5.3 VPN向导——逐步安装 184
 - 8.5.4 验证、监控VPN和VPN故障排除 185
 - 8.6 实现远程访问VPN 185
 - 8.6.1 变化的公司版图 185
 - 8.6.2 远程访问VPN介绍 186
 - 8.6.3 SSL VPN 187
 - 8.6.4 Cisco Easy VPN 189

8.6.5	使用SDM配置一台VPN服务器	190
8.6.6	连接VPN客户端	191
第9章	管理一个安全的网络	192
9.1	安全网络设计的原则	193
9.1.1	确保网络是安全的	193
9.1.2	威胁识别和风险分析	194
9.1.3	风险管理和风险避免	197
9.2	Cisco自防御网络	197
9.2.1	Cisco自防御网络介绍	197
9.2.2	Cisco SDN解决方案	199
9.2.3	Cisco集成安全组合	201
9.3	运行安全	201
9.3.1	运行安全介绍	201
9.3.2	运行安全的原则	202
9.4	网络安全测试	204
9.4.1	网络安全测试介绍	204
9.4.2	网络安全测试工具	205
9.5	业务连续性规划和灾难恢复	206
9.5.1	连续性规划	206
9.5.2	中断和备份	206
9.6	系统开发生命周期	207
9.6.1	SDLC介绍	207
9.6.2	SDLC的各阶段	207
9.7	开发一个全面的安全策略	209
9.7.1	安全策略概述	209
9.7.2	安全策略的结构	210
9.7.3	标准、指南、规程	211
9.7.4	角色和职责	212
9.7.5	安全意识和培训	212
9.7.6	法律与道德	214
9.7.7	对安全违规的响应	215
	术语表	217

章节摘录

版权页：SANS是在1989年作为合作性的研究和教育组织而建立的。

SANS关注信息安全培训和鉴定。

SANS开发关于信息安全各个方面的研究文档。

从审计员、网络管理员到首席信息安全官，人们分享应对不同挑战的经验教训和解决方案。

SANS的核心是全球从公司到大学各组织的安全从业人员，齐心协力帮助整个信息安全社团。

SANS资源大部分是可以免费申请到的。

包括流行的互联网早期警告系统——互联网风暴中心（Internet Storm Center），每周新闻摘要News Bites，每周漏洞摘要@RISK，快速安全报警以及超过1 200篇备受赞誉的原创性研究论文。

SANS开发了安全课程，可用于准备参加审计、管理、运营、法律问题、安全管理及软件安全的全球信息安全认证（Global Information Assurance Certification，GIAC）。

GIAC对安全职业人员的技能进行认证，范围从入门级的信息安全到高级领域，例如审计、入侵检测、事故处理、防火墙和边界保护、数据取证、黑客技能、Windows和UNIX操作系统安全以及安全的软件和应用编码。

编辑推荐

《思科网络技术学院教程·CCNA安全》：无论是上网还是在实际环境中，《思科网络技术学院教程·CCNA安全》都是方便阅读、重点突出、便于复习的学习资源。

书中文字都提取自在线教程，可使读者抓住重点。

每节的标题可为课堂讨论和考试提供相关在线课程的快速参考。

《思科网络技术学院教程·CCNA安全》是帮助你成功完成思科网络技术学院CCNA安全课程的唯一官方指定教材。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>