

## <<CCSP自学指南>>

### 图书基本信息

书名：<<CCSP自学指南>>

13位ISBN编号：9787115129857

10位ISBN编号：7115129851

出版时间：2005-2-1

出版时间：人民邮电出版社

作者：John F.Roland,张耀疆,陈克忠

页数：562

字数：1053000

译者：张耀疆,陈克忠

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>

## <<CCSP自学指南>>

### 内容概要

本书全面系统地介绍了在基于Cisco路由器的网络环境中，如何实施和管理网络安全。

全书共13章，从内容上可以分成5个部分。

第一部分包括第1章到第4章，详尽地介绍了网络安全的基本概念和相关Cisco路由器的基本的安全配置；第二部分包括第5章到第7章，介绍了3种Cisco IOS的增强功能——防火墙特征集；第三部分包括第8章到第10章，介绍了怎样利用Cisco路由器建立和管理VPN；第四部分包括第11章到13章，介绍了两种Cisco网络安全的管理工具——安全设备管理器(SDM)和路由器管理中心(MC)，以及一个全面地配置Cisco路由器的综合案例；附录部分给出了章节复习题答案、网络安全策略样例和访问控制列表参考

。

本书是Cisco Press出版的关于CCSP的官方教材，是CCSP应试者的必备书籍。

同时本书内容翔实，涉及知识面广，也适合广大网络管理人员和网络爱好者阅读与参考，更全面、更有效地保护自己的网络安全。

## <<CCSP自学指南>>

### 作者简介

John F.Roland , CCNA , CCDA , CCNP , CCDP , CSS-1 , MCSE , 是WesTek顾问公司的一名安全专家

。从IBM大型机上的COBOL编程到局域网/广域网设计和实施（美国军方网络），一直到最近开发CISCO及微软认证培训材料，JOHN已经在IT领域从业22年了。

目前，JOHN受托为一家大型的电缆通

# <<CCSP自学指南>>

## 书籍目录

第1章 网络安全简介	11.1 目标	21.1.1 一个封闭的网络	21.1.2 现代网络	31.1.3 威胁的能力——更危险更容易	41.1.4 安全角色的转变	41.1.5 电子商务的挑战	51.1.6 法律和政策的问题
51.2 Cisco SAFE Blueprint	61.2.1 路由器目标	71.2.2 交换机目标	71.2.3 主机目标	71.2.4 网络目标	71.2.5 应用目标	81.2.6 安全的管理和报告	81.3 网络攻击类型
91.3.1 网络安全威胁	91.3.2 网络攻击类型	101.4 网络安全策略	221.5 Cisco网络安全产品	231.6 Cisco管理软件	231.6.1 Cisco VPN设备管理器	231.6.2 Cisco PIX设备管理器	231.6.3 Cisco VPN方案中心
241.6.4 CiscoWorks VPN/安全管理方案	241.7 管理协议和功能	251.7.1 Telnet	251.7.2 简单网络管理协议	251.7.3 Syslog	261.7.4 简单文件传输协议	261.7.5 网络时间协议	261.8 NAT和NAT穿透
271.9 本章小结	281.10 本章复习题	29第2章 Cisco路由器安全基础	312.1 Cisco IOS防火墙特性	312.1.1 Cisco IOS防火墙价值	322.1.2 Cisco IOS防火墙特点	322.2 安全的Cisco路由器安装	332.2.1 对安装进行风险评估
332.2.2 Cisco路由器和交换机物理安装常见威胁	342.3 安全的Cisco路由器管理访问	362.3.1 连接路由器控制台端口	362.3.2 口令创建规则	372.3.3 初始化配置对话	372.3.4 配置最小口令长度	382.3.5 配置Enable Secret口令	382.3.6 配置控制台端口用户级口令
392.3.7 配置一个vty用户级口令	402.3.8 配置一个AUX用户级口令	412.3.9 用service password-encryption命令加密口令	412.3.10 增强用户名口令安全	422.3.11 用no service password-recovery保护ROMMON	432.3.12 记录认证失败率	442.3.13 设置路由器链路超时	442.3.14 设置特权级别
452.3.15 配置旗标消息	462.3.16 安全的SNMP访问	472.4 Cisco路由器AAA介绍	572.4.1 AAA模型：网络安全结构	572.4.2 实施AAA	582.4.3 用本地服务实施AAA	592.4.4 用外部服务实施AAA	592.4.5 TACACS+和RADIUS AAA协议
602.4.6 认证方法和易用性	612.5 为Cisco边界路由器配置AAA	652.5.1 认证边界路由器访问	652.5.2 边界路由器AAA配置过程	662.5.3 对特权EXEC和配置模式进行安全访问	662.5.4 用aaa new-model命令启用AAA	672.5.5 aaa authentication命令	672.5.6 aaa authorization命令
702.5.7 aaa accounting命令	722.6 AAA排障	732.6.1 debug aaa authentication命令	732.6.2 debug aaa authorization命令	742.6.3 debug aaa accounting命令	752.7 本章小结	762.8 Cisco IOS命令回顾	762.9 本章复习题
762.10 案例研究	762.10.1 未来公司	772.10.2 安全策略符合性	782.10.3 解决方案	79第3章 Cisco路由器网络高级AAA安全	833.1 Cisco Secure ACS介绍	833.1.1 Cisco Secure ACS for Windows	843.1.2 Cisco Secure ACS for UNIX(Solaris)
943.2 安装Cisco Secure ACS 3.0 for Windows 2000/NT服务器	953.2.1 配置服务器	963.2.2 校验Windows服务器和其他网络设备间的连接	963.2.3 在服务器上安装Cisco Secure ACS for Windows	963.2.4 用Web浏览器配置Cisco Secure ACS for Windows	963.2.5 为AAA配置其余设备	973.2.6 校验正确安装和操作	973.3 Cisco Secure ACS for Windows管理和排障
973.3.1 认证失败	993.3.2 授权失败	1003.3.3 记帐失败	1003.3.4 拨入PC问题排障	1003.3.5 使用Cisco IOS命令排障	1013.4 TACACS+概述	1013.4.1 一般特性	1013.4.2 配置TACACS+
1023.4.3 校验TACACS+	1053.5 RADIUS概述	1073.5.1 客户端/服务器模型	1083.5.2 网络安全	1083.5.3 灵活的认证机制	1083.5.4 配置RADIUS	1083.5.5 RADIUS增强属性	1103.6 Kerberos概述
1113.7 本章小结	1123.8 Cisco IOS命令回顾	1123.9 本章复习题	1123.10 案例研究	1133.10.1 场景	1143.10.2 解决方案	114第4章 Cisco路由器威胁对策	1174.1 用路由器来保护网络
1174.1.1 单个边界路由器	1174.1.2 边界路由器和防火墙	1184.1.3 集成防火墙的边界路由器	1184.1.4 边界路由器、防火墙和内部路由器	1194.2 加强路由器服务和接口的安全性	1194.2.1 关闭BOOTP服务器	1204.2.2 关闭CDP服务	1204.2.3 关闭配置自动加载服务
1214.2.4 限制DNS服务	1224.2.5 关闭FTP服务器	1224.2.6 关闭Finger服务	1234.2.7 关闭无根据ARP	1244.2.8 关闭HTTP服务	1254.2.9 关闭IP无类别路由选择服务	1254.2.10 关闭IP定向广播	1264.2.11 关闭IP鉴别
1264.2.12 关闭ICMP掩码应答	1274.2.13 关闭ICMP重定向	1274.2.14 关闭IP源路由选择	1284.2.15 关闭ICMP不可达消息	1284.2.16 关闭MOP服务	1294.2.17 关闭NTP服务	1294.2.18 关闭PAD服务	1304.2.19 关闭代理ARP
1314.2.20 关闭SNMP服务	1324.2.21 关闭小型服务器	1334.2.22 启用TCP Keepalive	1344.2.23 关闭TFTP服务器	1354.3			

# <<CCSP自学指南>>

关闭不用的路由器接口 1364.4 实施Cisco访问控制列表 1374.4.1 识别访问控制列表 1374.4.2 IP  
 访问控制列表类型 1384.4.3 注释IP ACL条款 1434.4.4 开发ACL规则 1434.4.5 ACL定向过滤  
 1434.4.6 将ACL应用到接口 1444.4.7 显示ACL 1444.4.8 启用Turbo ACL 1454.4.9 增强ACL  
 1464.5 用ACL来应对安全威胁 1474.5.1 流量过滤 1484.5.2 理论网络 1494.6 过滤路由器服  
 务流量 1504.6.1 Telnet服务 1504.6.2 SNMP服务 1504.6.3 路由选择协议 1514.7 过滤网络流  
 量 1514.7.1 IP地址欺骗对策 1524.7.2 DoS TCP SYN攻击对策 1534.7.3 DoS Smurf攻击对策  
 1534.7.4 过滤ICMP消息 1544.8 DDoS对策 1554.8.1 TRIN00 1554.8.2 Stacheldraht 1564.8.3  
 Trinity V3 1564.8.4 Subseven 1564.9 路由器配置示例 1574.10 实施Syslog日志 1584.10.1  
 Syslog系统 1594.10.2 Cisco日志安全级别 1594.10.3 日志消息格式 1604.10.4 Syslog路由器命令  
 1614.11 为企业网络设计安全的管理和报告系统 1624.11.1 SAFE结构通览 1634.11.2 信息路径  
 1644.11.3 带外管理一般指南 1654.11.4 日志和报告 1664.11.5 配置SSH服务器 1674.11.6 安  
 全的SNMP访问 1684.12 用AutoSecure加强Cisco路由器安全 1724.12.1 起点 1724.12.2 接口选择  
 1734.12.3 安全的Management层面服务 1734.12.4 创建安全旗标 1744.12.5 配置口令、AAA  
 、SSH 服务器和域名 1754.12.6 配置特定接口服务 1754.12.7 配置Cisco Express Forwarding和入口  
 过滤 1764.12.8 配置入口过滤和CBAC 1764.12.9 检查配置并应用于运行配置中 1774.12.10 例子  
 :使用AutoSecure之前典型的路由器配置 1844.12.11 例子:使用AutoSecure之后典型的路由器配置  
 1854.13 本章小结 1904.14 Cisco IOS命令回顾 1904.15 本章复习题 1904.16 案例研究  
 1914.16.1 场景 1924.16.2 解决方案 192第5章 Cisco IOS防火墙基于上下文访问控制的配置  
 1975.1 Cisco IOS防火墙介绍 1975.1.1 Cisco IOS防火墙特征集 1985.1.2 理解CBAC 1985.1.3  
 理解认证代理 1995.1.4 理解入侵检测 1995.2 用CBAC保护用户免受攻击 2005.2.1 Cisco IOS访  
 问控制列表 2005.2.2 CBAC是如何工作的 2005.2.3 支持的协议 2025.2.4 告警和审计跟踪  
 2025.3 配置CBAC 2035.3.1 打开审计跟踪和告警 2035.3.2 全局超时值和阈值 2035.3.3 端口  
 到应用的映射(Port-To-Application Mapping) 2065.3.4 定义应用协议审查规则 2085.3.5 路由器接口  
 审查规则和ACL 2115.3.6 测试和验证CBAC 2155.4 本章小结 2165.5 Cisco IOS命令回顾  
 2175.6 本章复习题 2175.7 案例研究 2185.7.1 场景 2195.7.2 解决方案 219第6章 Cisco  
 IOS防火墙认证代理 2236.1 介绍Cisco IOS防火墙认证代理 2236.1.1 定义认证代理 2236.1.2 支  
 持AAA协议和服务 2246.1.3 发起一个会话 2246.1.4 认证代理过程 2256.1.5 应用认证代理  
 2276.1.6 配置认证代理 2276.2 配置AAA服务器 2286.2.1 在Cisco安全访问控制服务器(CSACS)  
 上配置认证代理服务 2286.2.2 在Cisco安全访问控制服务器上建立用户授权配置文件 2296.2.3 在  
 建立用户授权配置文件时使用proxyacl#n属性 2306.3 用AAA服务器配置Cisco IOS 防火墙  
 2306.3.1 打开AAA 2316.3.2 指定认证协议 2316.3.3 指定授权协议 2316.3.4 定义TACACS+  
 服务器和它的密钥 2316.3.5 定义RADIUS服务器和它的密钥 2326.3.6 允许到路由器的AAA流量  
 2326.3.7 打开路由器的HTTP服务器 2336.4 配置认证代理 2346.4.1 设置默认空闲时间  
 2346.4.2 定义可选的认证代理标志 2346.4.3 定义和应用认证代理规则 2356.4.4 将认证代理规  
 则关联到ACL 2366.5 测试和验证配置 2366.5.1 show命令 2366.5.2 debug命令 2366.5.3 清除  
 认证代理缓存 2376.6 本章小结 2376.7 Cisco IOS命令回顾 2386.8 本章复习题 2386.9 案例研  
 究 2386.9.1 场景 2396.9.2 解决方案 239第7章 Cisco IOS防火墙入侵检测系统 2437.1 Cisco  
 IOS IDS介绍 2437.1.1 网络能见度 2457.1.2 支持的路由器平台 2457.1.3 实施问题 2477.1.4 签  
 名应用 2477.1.5 响应选项 2487.2 配置Cisco IOS IDS 2487.2.1 步骤1——初始化Cisco IOS路  
 由器 2497.2.2 步骤2——配置保护、关闭和排除签名 2507.2.3 步骤3——建立和应用审查规则  
 2517.2.4 步骤4——验证配置 2537.2.5 步骤5——将Cisco IOS IDS路由器加到CiscoWorks安全监控  
 中心 2547.3 本章小结 2567.4 Cisco IOS IDS使用的签名 2567.5 Cisco IOS命令回顾 2597.6 本  
 章复习题 2597.7 案例研究 2607.7.1 场景 2617.7.2 解决方案 261第8章 用Cisco路由器和预共  
 享密钥建立IPSec VPN 2658.1 在Cisco路由器打开安全VPN 2658.1.1 定义VPN 2658.1.2 Cisco  
 VPN路由器产品线 2678.2 什么是IPSec 2688.2.1 机密性(加密) 2698.2.2 数据完整性 2738.2.3  
 起源认证 2748.2.4 反重放保护 2778.3 IPSec协议框架 2788.3.1 IPSec协议 2788.3.2 使用模式  
 :比较隧道模式和传输模式 2808.3.3 在IPSec隧道中的DF位覆盖功能性 2818.3.4 IPSec框架



# <<CCSP自学指南>>

2828.4 IPsec的5个步骤 2828.4.1 IPsec步骤1：感兴趣的流量 2838.4.2 IPsec步骤2：IKE阶段1  
 2838.4.3 IPsec步骤3：IKE阶段2 2858.4.4 IPsec步骤4：数据传输 2868.4.5 IPsec步骤5：隧道终  
 止 2878.5 IPsec和动态虚拟专用网 2878.6 使用IKE预共享密钥配置IPsec 2948.6.1 任务1配  
 置IPsec加密：为IKE和IPsec准备 2948.6.2 任务2配置IPsec加密：配置IKE 3008.6.3 任务3配  
 置IPsec加密：配置IPsec 3038.6.4 任务4配置IPsec加密：测试和验证IPsec和ISAKMP 3118.7 手动  
 配置IPsec 3158.8 使用RSA加密Nonces配置IPsec 3168.9 和IPsec一起使用NAT 3188.9.1 IKE阶  
 段1和阶段2协商 3188.9.2 NAT穿透包封装 3198.9.3 配置IPsec和NAT一起工作 3198.10 本章小  
 结 3208.11 Cisco IOS命令回顾 3208.12 本章复习题 3208.13 案例研究 3218.13.1 场景  
 3218.13.2 解决方案 322第9章 用Cisco路由器和CA建立高级IPsec VPN 3279.1 证书权威  
 3279.1.1 Cisco IOS CA支持标准 3289.1.2 简单证书登记协议 3299.1.3 CA服务器和Cisco路由  
 器的协同性 3299.1.4 用CA登记一台设备 3319.1.5 多个RSA密钥对支持 3319.2 配置CA支持任务  
 3329.2.1 配置CA支持之任务1：为IKE和IPsec作准备 3329.2.2 配置CA支持之任务2：配置CA支持  
 3359.2.3 配置CA支持之任务3：为IPsec配置IKE 3459.2.4 配置CA支持之任务4：配置IPsec  
 3469.2.5 配置CA支持之任务5：测试和验证IPsec 3469.3 本章小结 3479.4 Cisco IOS命令回顾  
 3479.5 本章复习题 3479.6 案例研究 3479.6.1 场景 3489.6.2 解决方案 349第10章 用Cisco  
 Easy VPN 配置IOS 远程接入 35310.1 介绍Cisco Easy VPN 35310.1.1 Cisco Easy VPN Server  
 35310.1.2 Cisco Easy VPN Remote 35410.2 Cisco Easy VPN Server概述 35410.2.1 12.2(8)T和Cisco  
 Easy VPN的新特征 35510.2.2 支持的IPsec属性 35610.2.3 不支持的IPsec属性 35610.3 Cisco Easy  
 VPN Remote概述 35710.3.1 支持的Cisco Easy VPN远程客户端 35710.3.2 Cisco Easy VPN Remote  
 阶段II 36010.3.3 Cisco VPN Client 3.5概述 36310.3.4 Cisco Easy VPN功能 36510.4 配  
 置Cisco Easy VPN Server支持XAUTH 36810.4.1 任务1：配置XAUTH 36910.4.2 任务2：建立IP地址  
 池 37010.4.3 任务3：配置组策略搜寻 37010.4.4 任务4：为远程VPN客户接入建立ISAKMP策略  
 37110.4.5 任务5：为MC“推”定义组策略 37110.4.6 任务6：建立变换集 37310.4.7 任务7：  
 用RRI建立动态加密映射 37310.4.8 任务8：将MC应用到动态加密映射 37410.4.9 任务9：将动态  
 加密映射应用到路由器的外部接口 37510.4.10 任务10：打开IKE DPD(可选) 37510.5 为组配置文  
 件配置RADIUS认证 37610.6 Cisco VPN Client 3.5安装和配置任务 37710.6.1 任务1：安装Cisco  
 VPN Client 3.x 37710.6.2 任务2：建立新的连接条目 37810.6.3 任务3(可选)：修改Cisco VPN Client  
 选项 37810.6.4 任务4：配置Cisco VPN Client基本属性 37910.6.5 任务5：配置Cisco VPN Client认  
 证属性 38010.6.6 任务6：配置Cisco VPN Client连接属性 38110.7 和Cisco VPN Client 3.5一起工作  
 38210.7.1 程序菜单 38210.7.2 日志查看器 38310.7.3 设置MTU大小 38310.7.4 客户端连接状  
 态：基本标签 38410.7.5 客户端连接状态：统计标签 38510.8 即将来临的Cisco VPN Client更新  
 38610.8.1 虚拟适配器 38610.8.2 对Windows和Mac统一了VPN客户端 38610.8.3 删除警告(包括  
 原因) 38710.8.4 单一IPsec-SA 38710.8.5 个人防火墙增强 38710.8.6 第三方VPN厂商兼容  
 38710.8.7 RADIUS SDI XAUTH请求管理 38710.8.8 ISO标准格式日志文件名 38810.8.9 GINA增  
 强 38810.9 本章小结 38810.10 Cisco IOS命令回顾 38810.11 本章复习题 38810.12 案例研究  
 38910.12.1 场景 39010.12.2 解决方案 390第11章 使用安全设备管理器保护Cisco路由器  
 39511.1 理解安全设备管理器 39511.1.1 SDM特征 39611.1.2 智能安全配置 39611.1.3 SDM用  
 户类型 39711.1.4 SDM特征的详细资料 39711.2 理解SDM软件 39711.2.1 支持的Cisco IOS版本  
 和设备 39811.2.2 获取SDM 39811.2.3 在已有的路由器上安装SDM 39811.2.4 显示路由器的闪存  
 空间 39911.2.5 SDM软件需求 39911.2.6 SDM路由器通信 40011.3 使用SDM启动向导  
 40011.3.1 第一次SDM访问 40111.3.2 诊断SDM故障 40711.4 介绍SDM用户界面 40711.4.1  
 SDM主窗口特征 40711.4.2 SDM菜单栏 40811.4.3 SDM工具栏 40811.4.4 SDM向导模式选项  
 40911.5 使用WAN向导配置WAN 41011.5.1 建立新WAN连接 41011.5.2 运行串口向导  
 41111.5.3 配置封装和IP地址 41111.5.4 配置LMI和DLCI 41111.5.5 配置高级选项 41211.5.6  
 完成WAN接口配置 41211.5.7 查看和编辑已有的WAN连接 41211.5.8 使用高级模式验证接口状态  
 41311.6 使用SDM配置防火墙 41311.6.1 建立基本防火墙 41411.6.2 建立高级防火墙 41511.7  
 使用SDM配置VPN 41811.7.1 使用预共享密钥建立站到站的VPN 41911.7.2 查看或改变VPN设

# <<CCSP自学指南>>

置 42011.8 使用SDM执行安全审查 42011.8.1 执行安全审查 42011.8.2 一步加固 42211.9 使用出厂复位向导 42411.10 使用SDM高级模式 42411.10.1 高级模式——概要 42411.10.2 高级模式——接口和连接 42611.10.3 高级模式——规则 42711.10.4 高级模式——路由选择 42711.10.5 高级模式——NAT 42811.10.6 高级模式——系统属性 42911.10.7 高级模式——VPN 43111.11 理解监控模式 43111.12 本章小结 43211.13 Cisco IOS命令回顾 43211.14 本章复习题 43211.15 案例研究 43311.15.1 场景 43411.15.2 解决方案 434第12章 管理企业VPN路由器 43712.1 路由器MC 1.2.1简介 43712.1.1 理解路由器MC概念 43812.1.2 路由器MC组件 43912.1.3 路由器MC 1.2.1支持的设备 44012.1.4 路由器MC通信 44012.1.5 支持的隧道技术 44112.2 安装路由器MC 44112.2.1 安装需求 44112.2.2 客户端访问需求 44212.2.3 安装过程 44312.2.4 配置路由器支持SSH 44312.3 使用路由器MC 44312.3.1 CiscoWorks登录 44412.3.2 CiscoWorks用户授权角色 44412.3.3 在CiscoWorks中添加用户 44612.3.4 启动路由器MC 44612.3.5 使用路由器MC主窗口 44712.3.6 使用路由器MC界面 44712.3.7 使用设备标签 44812.3.8 使用配置标签 44912.3.9 使用部署标签 45012.3.10 使用报告标签 45012.3.11 使用管理标签 45012.4 建立工作流程和活动 45112.4.1 工作流程任务 45112.4.2 任务1：建立活动 45212.4.3 任务2：建立设备组 45412.4.4 任务3：导入设备 45512.4.5 任务4：定义VPN设置 45912.4.6 任务5：定义VPN策略 46412.4.7 任务6：批准活动 47112.4.8 任务7：建立和部署作业 47112.5 配置基本的Cisco IOS防火墙设置 47412.5.1 分片规则 47512.5.2 超时值和性能 47512.5.3 半打开连接限制 47612.5.4 日志 47612.5.5 ACL范围 47712.6 建立访问规则 47712.7 使用建构块 47812.7.1 网络组 47812.7.2 变换集 47912.7.3 服务组 47912.8 网络地址转换规则 48012.8.1 地址池 48012.8.2 流量过滤 48012.9 管理配置 48112.9.1 上传 48112.9.2 查看配置 48212.9.3 路由器MC部署选项 48312.10 管理 48512.10.1 部署报告 48512.10.2 活动报告 48612.10.3 审计跟踪报告 48612.10.4 管理 48612.11 本章小结 48712.12 本章复习题 48712.13 案例研究 48712.13.1 场景 48812.13.2 解决方案 488第13章 案例研究 49113.1 简介 49113.2 需求 49113.3 解决方案 49413.3.1 开始路由器配置 49413.3.2 解决方案的配置步骤 49513.3.3 结束路由器配置 500附录A 各章复习题答案 505第1章 505第2章 506第3章 507第4章 508第5章 510第6章 511第7章 512第8章 513第9章 514第10章 515第11章 516第12章 518附录B 网络安全策略实例 521B.1 授权和范围的说明 521B.1.1 适用对象 521B.1.2 网络安全策略的范围 522B.1.3 网络安全策略负责人 522B.1.4 系统管理员责任 522B.1.5 网络安全策略维护流程 523B.1.6 实施过程 523B.1.7 用户培训 523B.2 漏洞审计策略 523B.2.1 可接受的使用 523B.2.2 频率 523B.2.3 审计目标 523B.2.4 报告 524B.3 网络使用策略 524B.3.1 可接收的网络使用 524B.3.2 不可接收的网络使用 524B.3.3 服从要求 524B.4 身份鉴别和认证策略 524B.4.1 可接受的使用 525B.4.2 密码管理 525B.4.3 认证管理 525B.5 Internet访问策略 525B.5.1 可接受的使用 525B.5.2 防火墙使用 525B.5.3 公共服务使用 525B.6 园区访问策略 526B.6.1 可接受的使用 526B.6.2 信任关系 526B.6.3 网络设备安全 526B.7 远程访问策略 526B.7.1 可以接受的使用 527B.7.2 移动计算 527B.7.3 从家中访问 527B.7.4 远距离工作协议 527B.7.5 分支机构访问 527B.7.6 商务合作者(外联网)访问 527B.7.7 加密 527B.8 事件处理策略 528B.8.1 入侵检测需求 528B.8.2 事件响应过程 528B.8.3 联络点 529附录C 配置标准和扩展访问列表 531C.1 IP编址和通用访问列表概念 532C.1.1 IP地址 532C.1.2 通配符掩码 535C.1.3 一般访问列表配置任务 536C.1.4 访问列表配置原则 536C.2 配置标准IP访问列表 537C.2.1 标准IP访问列表处理 537C.2.2 标准IP访问列表命令 538C.2.3 标准访问列表的定位 539C.2.4 标准IP访问列表中的一般错误 540C.2.5 标准IP访问列表举例 541C.3 配置扩展IP访问列表 541C.3.1 扩展IP访问列表处理 542C.3.2 扩展IP访问列表命令 543C.3.3 ICMP命令语法 544C.3.4 TCP语法 546C.3.5 UDP语法 547C.3.6 扩展IP访问列表的定位 548C.3.7 扩展IP访问列表举例1 548C.3.8 扩展IP访问列表举例2 549C.4 验证访问列表配置 549C.5 命名的IP访问列表 550C.6 总结 552C.7 参考文献 552C.7.1 配置IP访问列表 552C.7.2 IP协议和编址信息 553术语表 555





## <<CCSP自学指南>>

### 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>