第一图书网, tushu007.com

<<思科网络技术学院教程>>

图书基本信息

书名：<<思科网络技术学院教程>>

13位ISBN编号：9787115183002

10位ISBN编号：7115183007

出版时间：2008-10

出版时间：人民邮电出版社

作者：拉菲

页数：532

字数：1022000

译者：北京邮电大学思科网络技术学院

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

第一图书网, tushu007.com

前言

思科网络学院课程设计用来使你进入计算机网络领域，在这个领域工作或继续接受更多的教育和培训。
网络安全课程分为两个学期。
第一学期课程侧重于网络中的总体安全进程，并特别关注以下领域的实际操作技巧：安全策略设计和管理；安全技术、产品、解决方案；防火墙和安全路由器设计、安装、配置、维护；使用路由器和防火墙实现AAA；在OSI模型的第二层和第三层保护网络。

第一图书网, tushu007.com

<<思科网络技术学院教程>>

内容概要

思科网络技术学院项目（Cisco Networking Academy Program）是Cisco公司在全球范围推出的一个主要面向初级网络工程技术人员的培训项目。
作为它的课程之一，本书介绍了如何在Cisco的网络设备中实施IP网络的安全。
本书包括两个学期的课程内容。
第一学期课程内容侧重于网络中的总体安全进程，并特别关注以下领域的实际操作技巧：安全策略设计和管理，安全技术、产品、解决方案，防火墙和安全路由器设计、安装、配置、维护，使用路由器和防火墙实现AAA，在OSI模型的第二层和第三层保护网络等。
第二学期课程内容侧重于安全策略设计和管理，安全技术、产品、解决方案，防火墙和安全路由器设计、安装、配置、维护，使用路由器和防火墙实现入侵预防系统（IPS），使用路由器和防火墙实现虚拟专用网（VPN）等。
本书作为思科网络技术学院网络安全的指定教材，适合具备CCNA水平的读者学习。
另外，将要参加思科公司的CCSP认证考试的人员也可以把本书作为考试指南。

第一图书网, tushu007.com

作者简介

Antoon“ Tony ”W. Ruff目前在沃尔登大学攻读基于信息系统的应用商务管理和决策学博士。Tony毕业于马里兰大学，获得信息系统硕士学位，并获得南伊利诺斯大学工业技术学士学位。Tony目前是技术校园所有ECPI学院的计算机和信息科学（CIS）副院长，讲授Cisco学院CCNA、CCNP、网络

第一图书网, tushu007.com

<<思科网络技术学院教程>>

书籍目录

第一学期 第1章 弱点、威胁、攻击 1.1 关键术语 1.2 网络安全简介 1.2.1 网络安全需求 1.2.2 识别网络安全的潜在风险 1.2.3 开放的与封闭的安全模型 1.2.4 网络安全的发展趋势 1.2.5 信息安全组织 1.3 弱点、威胁和攻击介绍 1.3.1 弱点 1.3.2 威胁 1.3.3 攻击 1.4 攻击事例 1.4.1 侦查攻击 1.4.2 访问攻击 1.4.3 拒绝服务(DoS)攻击 1.4.4 假冒/IP欺骗攻击 1.4.5 分布式拒绝服务攻击 1.4.6 恶意代码 1.5 弱点分析 1.5.1 政策定位 1.5.2 网络分析 1.5.3 主机分析 1.5.4 分析工具 1.6 总结 1.7 检查你的理解 第2章 安全计划与策略 2.1 关键术语 2.2 关于网络安全及Cisco 2.2.1 安全轮(Security Wheel) 2.2.2 网络安全策略 2.3 端点保护和管理 2.3.1 基于主机和服务器的安全组件和技术 2.3.2 PC管理 2.4 网络保护和管理 2.4.1 基于网络的安全组件和技术 2.4.2 网络安全管理 2.5 安全体系 2.5.1 安全体系SAFE 2.5.2 Cisco自防卫网络 2.5.3 保护连通性(secure connectivity) 2.5.4 威胁防范(Threat Defense) 2.5.5 Cisco集成安全 2.5.6 计划、设计、实施、运行、优化模型(PDIOO、Plan、Design、Implement、Operate、Optimize) 2.6 基本的路由器安全 2.6.1 控制对网络设备的访问 2.6.2 使用SSH进行远程配置 2.6.3 路由器口令 2.6.4 路由器优先级和账户 2.6.5 Cisco IOS网络服务 2.6.6 路由、代理ARP、ICMP 2.6.7 路由协议认证和升级过滤 2.6.8 NTP、SNMP、路由器名、DNS 2.7 总结 2.8 检查你的理解 第3章 安全设备 3.1 可选设备 3.1.1 Cisco防火墙特性集 3.1.2 创建用户的防火墙 3.1.3 PIX安全设备 3.1.4 自适应安全设备 3.1.5 Finesse操作系统 3.1.6 自适应安全算法 3.1.7 防火墙服务模块 3.2 使用安全设备管理器 3.2.1 使用SDM启动向导 3.2.2 SDM用户界面 3.2.3 SDM向导 3.2.4 用SDM配置WAN 3.2.5 使用恢复出厂配置向导 3.2.6 监控模式 3.3 Cisco安全设备家族介绍 3.3.1 PIX501安全设备 3.3.2 PIX506E安全设备 3.3.3 PIX515E安全设备 3.3.4 PIX525安全设备 3.3.5 PIX535安全设备 3.3.6 自适应安全设备模块 3.3.7 PIX安全设备许可证 3.3.8 PIX VPN 加密许可 3.3.9 安全上下文 3.3.10 PIX安全设备上下文许可证 3.3.11 ASA安全设备许可证 3.3.12 扩展PIX515E特性 3.3.13 扩展PIX525特性 3.3.14 扩展PIX535特性 3.3.15 扩展自适应安全设备家族的特性 3.4 开始配置PIX安全设备 3.4.1 配置PIX 安全设备 3.4.2 帮助命令 3.4.3 安全级别 3.4.4 基本PIX安全设备的配置命令 3.4.5 其他PIX安全设备的配置命令 3.4.6 检查PIX安全设备的状态 3.4.7 时间设置和NTP支持 3.4.8 日志(syslog)配置 3.5 安全设备的转换和连接 3.5.1 传输协议 3.5.2 NAT 3.5.3 动态内部NAT 3.5.4 两个接口的NAT 3.5.5 个接口的NAT 3.5.6 PAT 3.5.7 增加PAT的全局地址池 3.5.8 static命令 3.5.9 nat 0命令 3.5.10 连接和转换 3.6 用自适应安全设备管理器管理PIX 3.6.1 ASDM运行需求 3.6.2 ASDM的准备 3.6.3 使用ASDM配置PIX安全设备 3.7 PIX安全设备的路由功能 3.7.1 虚拟LAN 3.7.2 静态和RIP路由 3.7.3 OSPF 3.7.4 多播路由 3.8 防火墙服务模块的运行 3.8.1 FWSM的运行要求 3.8.2 开始使用FWSM 3.8.3 校验FWSM的安装 3.8.4 配置FWSM的访问列表 3.8.5 在FWSM上使用PDM 3.8.6 重置和重启FWSM 3.9 总结 3.10 检查你的理解 第4章 信任和身份技术 4.1 关键术语 4.2 AAA 4.2.1 TACACS 4.2.2 RADIUS 4.2.3 TACACS+和RADIUS的比较 4.3 验证技术 4.3.1 静态口令 4.3.2 一次性口令 4.3.3 令牌卡 4.3.4 令牌卡和服务器方法 4.3.5 数字证书 4.3.6 生物测定学 4.4 基于身份网络服务(IBNS) 4.5 有线的和无线的执行 4.6 网络准入控制(NAC) 4.6.1 NAC组成 4.6.2 NAC阶段 4.6.3 NAC运行 4.6.4 NAC厂商的参与 4.7 总结 4.8 检查你的理解 第5章 Cisco安全访问控制服务器 5.1 关键术语 5.2 Cisco安全访问控制服务器产品概述 5.2.1 验证和用户数据库 5.2.2 Cisco安全ACS用户数据库 5.2.3 保持数据库稳定 5.2.4 基于Windows的Cisco安全ACS体系架构 5.2.5 Cisco安

第一图书网, tushu007.com

全ACS如何验证用户 5.2.6 用户可更改的口令 5.3 使用Cisco安全ACS配置TACACS+和RADIUS 5.3.1 安装步骤 5.3.2 管理基于Windows的Cisco安全ACS 5.3.3 排错 5.3.4 启用TACACS+ 5.4 检验TACACS+ 5.4.1 失败 5.4.2 通过 5.5 配置RADIUS 5.6 总结 5.7 检查你的理解 第6章 在三层配置信任和身份 6.1 关键术语 6.2 Cisco IOS防火墙认证代理 6.2.1 认证代理的运行 6.2.2 支持的AAA服务器 6.2.3 AAA服务器配置 6.2.4 AAA配置 6.2.5 允许AAA流量到路由器 6.2.6 认证代理配置 6.2.7 测试和验证认证代理 6.3 介绍PIX安全器件AAA特性 6.3.1 PIX安全器件认证 6.3.2 PIX安全器件授权 6.3.3 PIX安全器件计费 6.3.4 AAA服务器支持 6.4 在PIX安全器件上配置AAA 6.4.1 PIX安全器件访问认证 6.4.2 交互式用户认证 6.4.3 本地用户数据库 6.4.4 认证提示和超时 6.4.5 直通代理认证 6.4.6 认证非Telnet、FTP、HTTP或HTTPS流量 6.4.7 隧道用户认证 6.4.8 授权配置 6.4.9 可下载的ACL 6.4.10 计费配置 6.4.11 控制台会话计费 6.4.12 命令计费 6.4.13 AAA配置故障处理 6.5 总结 6.6 检查你的理解 第7章 在二层配置信任和身份 7.1 关键术语 7.2 基于身份的网络服务(IBNS) 7.2.1 特点及好处 7.2.2 IEEE 802.1x 7.2.3 选择正确的EAP 7.2.4 Cisco LEAP 7.2.5 IBNS和Cisco安全ACS 7.2.6 部署ACS的考虑 7.2.7 Cisco安全ACS RADIUS配置 7.3 配置802.1x基于端口的认证 7.3.1 使能802.1x认证 7.3.2 配置交换机到RADIUS服务器的通信 7.3.3 使能周期性重认证 7.3.4 手工重认证连接到端口的客户 7.3.5 使能多主机 7.3.6 将802.1x配置重设为默认值 7.3.7 查看802.1x统计信息和状态 7.4 总结 7.5 检查你的理解 第8章 在路由器上配置过滤 8.1 关键术语 8.2 过滤和访问列表 8.2.1 数据包过滤 8.2.2 状态过滤 8.2.3 URL过滤 8.3 Cisco IOS防火墙基于上下文的访问控制 8.3.1 CBAC数据包 8.3.2 Cisco IOS ACL 8.3.3 CBAC如何运行 8.3.4 CBAC所支持的协议 8.4 配置Cisco IOS防火墙基于上下文的访问控制 8.4.1 CBAC配置任务 8.4.2 准备CBAC 8.4.3 设置审计跟踪和警告 8.4.4 设置全局超时时间 8.4.5 设置全局阈值 8.4.6 主机限制的半开连接 8.4.7 系统定义的端口与应用映射 8.4.8 用户定义的PAM 8.4.9 设定应用的检测规则 8.4.10 为IP分片定义检测规则 8.4.11 定义ICMP检测规则 8.4.12 将检测规则和ACL应用于接口 8.5 测试与校验CBAC 用SDM配置Cisco IOS防火墙 8.6 总结 8.7 检查你的理解 第9章 在PIX安全器件上配置过滤 9.1 关键术语 9.2 配置ACL和内容过滤 9.2.1 PIX安全器件ACL 9.2.2 配置ACL 9.2.3 ACL行号 9.2.4 icmp命令 9.2.5 nat 0 ACL 9.2.6 Turbo ACL 9.2.7 使用ACL 9.2.8 恶意代码过滤 9.2.9 URL过滤 9.3 对象分组 9.3.1 开始使用对象分组 9.3.2 配置对象分组 9.3.3 嵌套对象分组 9.3.4 管理对象分组 9.4 配置安全器件模块策略 9.4.1 配置一个类映射 9.4.2 配置一个策略映射 9.4.3 配置一个服务策略 9.5 配置高级协议检查 9.5.1 默认流量检查和端口号 9.5.2 FTP检查 9.5.3 FTP深度报文检查 9.5.4 HTTP检查 9.5.5 协议应用程序检查 9.5.6 多媒体支持 9.5.7 实时流协议(Real-Time Streaming Protocol，RSTP) 9.5.8 支持IP电话所需要的协议 9.5.9 DNS检查 9.6 总结 9.7 检查你的理解 第10章 在交换机上配置过滤 10.1 关键术语 10.2 二层攻击简介 10.3 MAC地址、ARP和DHCP攻击 10.3.1 减少CAM表过载攻击 10.3.2 MAC欺骗：中间人攻击 10.3.3 ARP欺骗 10.4 DHCP侦听(DHCP Snooping) 10.4.1 动态ARP检测 10.4.2 DHCP耗尽攻击(DHCP Starvation Attacks) 10.5 VLAN攻击 10.5.1 VLAN跳跃攻击 10.5.2 私用VLAN攻击 10.5.3 私用VLAN防御 10.6 生成树协议攻击 10.7 总结 10.8 检查你的理解 第二学期 第1章 入侵检测和防御技术 1.1 关键术语 1.2 入侵检测和防御介绍 1.2.1 基于网络与基于主机 1.2.2 警报的类型 1.3 检测引擎 1.3.1 基于签名的探测 1.3.2 签名的类型 1.3.3 基于异常状态检测 1.4 Cisco的IDS和IPS设备 1.4.1 Cisco集成的解决方案 1.4.2 Cisco IPS 4200系列探测器 1.5 总结 1.6 检查你的理解 第2章 配置网络入侵检测和入侵防护 2.1 关键术语 2.2 Cisco IOS入侵防护系统(IPS) 2.2.1 Cisco IOS入侵防护系统的起源 2.2.2 路由器的性能 2.2.3

第一图书网, tushu007.com

Cisco IOS入侵防护系统特征库 2.2.4 配置Cisco IOS入侵防护系统的过程 2.3 在PIX安全设备上启用攻击防护功能(attack guards) 2.3.1 Mail Guard 2.3.2 DNS Guard 2.3.3 FragGuard和虚拟重组(Virtual Reassembly) 2.3.4 AAA泛洪防护 2.3.5 SYN泛洪保护 2.3.6 TCP intercept 2.3.7 SYN Cookies 2.3.8 连接限制 2.4 在PIX安全设备上配置入侵防护 2.4.1 入侵检测和PIX安全设备 2.4.2 配置入侵防护 2.4.3 配置IDS策略 2.5 在PIX安全设备上配置阻断(shunning) 2.6 总结 2.7 检查你的理解 第3章 加密与VPN技术 3.1 关键术语 3.2 加密的基本方法 3.2.1 对称加密 3.2.2 不对称加密 3.2.3 Diffie-Hellman 3.3 完整性要素 3.3.1 散列 3.3.2 散列方法认证码HMAC 3.3.3 数字签名和证书 3.4 实现数字证书 3.4.1 认证中心支持 3.4.2 简单证书注册协议SCEP 3.4.3 CA服务器 3.4.4 使用CA注册一台设备 3.5 VPN拓扑 3.5.1 站点到站点VPN 3.5.2 远程访问VPN 3.6 VPN技术 3.6.1 WebVPN 3.6.2 隧道协议 3.6.3 隧道接口 3.6.4 IPSec 3.6.5 认证头AH 3.6.6 封装安全载荷ESP 3.6.7 隧道和传输模式 3.6.8 安全关联 3.6.9 IPSec的5个步骤 3.6.10 因特网密钥交换IKE 3.6.11 IKE和IPSec 3.6.12 Cisco VPN解决方案 3.7 总结 3.8 检查你的理解 第4章 使用预共享密钥配置站点到站点VPN 4.1 关键术语 4.2 使用预共享密钥的IPSec加密 4.2.1 规划IKE和IPSec策略 4.2.2 步骤1：确定ISAKMP(IKE阶段1)策略 4.2.3 步骤2：定义IPSec(IKE阶段2)策略 4.2.4 步骤3：检查当前配置 4.2.5 步骤4：确保网络在没有加密时也能工作 4.2.6 步骤5：确认ACL允许IPSec 4.3 使用预共享密钥在路由器上配置IKE 4.3.1 步骤1：启用或禁止IKE 4.3.2 步骤2：创建IKE策略 4.3.3 步骤3：配置预共享密钥 4.3.4 步骤4：验证IKE配置 4.4 使用预共享密钥为路由器配置IPSec 4.4.1 步骤1：配置变换集 4.4.2 步骤2：确定IPSec(IKE阶段2)策略 4.4.3 步骤3：创建加密ACL 4.4.4 步骤4：创建加密图 4.4.5 步骤5：将加密图应用到接口 4.5 测试和验证路由器的IPSec配置 4.5.1 查看配置的ISAKMP策略 4.5.2 显示配置的变换集 4.5.3 显示IPSec SA的当前状态 4.5.4 显示配置的加密图 4.5.5 打开IPSec事件的调试输出 4.5.6 打开ISAKMP事件的调试输出 4.5.7 使用SDM配置一个VPN 4.6 使用预共享密钥配置一个PIX安全器件站点到站点VPN 4.6.1 任务1：准备配置VPN支持 4.6.2 任务2：配置IKE参数 4.6.3 任务3：配置IPSec参数 4.6.4 任务4：测试和验证IPSec配置 4.7 总结 4.8 检查你的理解 第5章 使用数字证书配置站点到站点VPN 5.1 关键术语 5.2 在路由器上配置CA支持 5.2.1 步骤1：管理NVRAM 5.2.2 步骤2：设置路由器的时间和日期 5.2.3 步骤3：在路由器主机表中加入CA服务器条目 5.2.4 步骤4：生成RSA密钥对 5.2.5 步骤5：声明一个CA 5.2.6 步骤6：认证CA 5.2.7 步骤7：为路由器申请一个证书 5.2.8 步骤8：保存配置 5.2.9 步骤9：监视和维护CA互操作性 5.2.10 步骤10：验证CA支持配置 5.3 使用数字证书配置Cisco IOS路由器站点到站点VPN 5.3.1 任务1：准备IKE和IPSec 5.3.2 任务2：配置CA支持 5.3.3 任务3：配置IKE 5.3.4 任务4：配置IPSec 5.3.5 任务5：测试和验证IPSec 5.4 使用数字证书配置PIX安全设备站点到站点VPN 5.5 总结 5.6 检查你的理解 第6章 配置远程访问VPN 6.1 关键术语 6.2 Cisco Easy VPN介绍 6.2.1 Easy VPN服务器概览 6.2.2 Cisco Easy VPN Remote概览 6.2.3 Cisco Easy VPN如何工作 6.3 Cisco Easy VPN服务器配置任务 6.3.1 任务1：创建一个IP地址池 6.3.2 任务2：配置组策略查找 6.3.3 任务3：为远程VPN客户访问创建ISAKMP策略 6.3.4 任务4：为模式配置推送定义一个组策略 6.3.5 任务5：创建一个变换集 6.3.6 任务6：创建一个带RRI的加密图 6.3.7 任务7：将模式配置应用到动态加密图 6.3.8 任务8：将动态加密图应用到路由器接口上 6.3.9 任务9：使能IKE失效对等体检测 6.3.10 任务10：(可选)配置XAUTH 6.3.11 任务11：(可选)启用XAUTH保存口令特性 6.4 Cisco Easy VPN客户端4.x配置任务 6.4.1 任务1：在远程用户的PC上安装Cisco VPN客户端4.x 6.4.2 任务2：创建一个新的客户端连接条目 6.4.3 任务3：选择一个认证方法 6.4.4 任务4：配置透明隧道 6.4.5 任务5：启用并增加备份服务器 6.4.6 任务6：通过拨号网络配置一条到因特网的连接 6.5 为接入路由器配置Cisco Easy VPN Remote 6.5.1 Easy VPN Remote操作模式

第一图书网, tushu007.com

6.5.2 接入路由器的Cisco Easy VPN Remote配置任务 6.6 配置PIX安全器件作为Easy VPN服务器 6.6.1 任务1：为远程VPN客户端访问创建一个ISAKMP策略 6.6.2 任务2：创建一个IP地址池 6.6.3 任务3：为模式配置推送定义一个组策略 6.6.4 任务4：创建一个变换集 6.6.5 任务5至任务7：动态加密图 6.6.6 任务8：配置XAUTH 6.6.7 任务9：配置NAT和NAT 0 6.6.8 任务10：启用IKE DPD 6.7 配置PIX 501或506E作为Easy VPN客户端 6.7.1 PIX安全器件Easy VPN Remote特性概览 6.7.2 Easy VPN Remote配置 6.7.3 Easy VPN客户端模式以及启用Easy VPN Remote客户端 6.7.4 Easy VPN Remote认证 6.8 配置适应性安全器件支持WebVPN 6.8.1 WebVPN最终用户接口 6.8.2 配置WebVPN常用参数 6.8.3 配置WebVPN服务器和URL 6.8.4 配置WebVPN端口转发 6.8.5 配置WebVPN E-mail代理 6.8.6 配置WebVPN内容过滤器和ACL 6.9 总结 6.10 检查你的理解 第7章 安全网络体系和管理 7.1 关键术语 7.2 影响二层消除技术的因素 7.2.1 单安全区域、单用户组、单物理交换机 7.2.2 单安全区域、单用户组、多物理交换机 7.2.3 单安全区域、多用户组、单物理交换机 7.2.4 单安全区域、多用户组、多物理交换机 7.2.5 多安全区域、单用户组、单物理交换机 7.2.6 多安全区域、单用户组、多物理交换机 7.2.7 多安全区域、多用户组、单物理交换机 7.2.8 多安全区域、多用户组、多物理交换机 7.2.9 二层安全最佳实践 7.3 SDM安全审计 7.4 路由器管理中心 7.4.1 Hub-and-Spoke拓扑 7.4.2 VPN设置和策略 7.4.3 设备层级和继承 7.4.4 活动 7.4.5 工作 7.4.6 构建块 7.4.7 支持的隧道技术 7.4.8 安装Router MC 7.4.9 开始使用Router MC 7.4.10 Router MC界面 7.4.11 Router MC标签 7.4.12 基本工作流和任务 7.5 简单网络管理协议SNMP 7.5.1 SNMP介绍 7.5.2 SNMP安全 7.5.3 SNMP版本3(SNMPv3) 7.5.4 SNMP管理应用程序 7.5.5 在Cisco IOS路由器上配置SNMP支持 7.5.6 在PIX安全器件上配置SNMP支持 7.6 总结 7.7 检查你的理解 第8章 PIX安全器件上下文、故障倒换和管理 8.1 关键术语 8.2 配置PIX安全器件在多上下文模式中运行 8.2.1 启用多上下文模式 8.2.2 配置安全上下文 8.2.3 管理安全上下文 8.3 配置PIX安全器件故障倒换 8.3.1 理解故障倒换 8.3.2 故障倒换的要求 8.3.3 基于串行电缆的故障倒换配置 8.3.4 基于LAN的活跃/备用故障倒换配置 8.3.5 活跃/活跃故障倒换 8.3.6 配置透明防火墙模式 8.3.7 透明防火墙模式概览 8.3.8 启用透明防火墙模式 8.3.9 监控和维护透明防火墙 8.4 PIX安全器件管理 8.4.1 管理Telnet访问 8.4.2 管理SSH访问 8.4.3 命令授权 8.4.4 PIX安全器件口令恢复 8.4.5 适应性安全器件口令恢复 8.4.6 文件管理 8.4.7 映像升级和认证密钥 8.5 总结 8.6 检查你的理解 附录A “检查你的理解”部分的答案 术语表

第一图书网, tushu007.com

章节摘录

插图：第一学期第1章 弱点、威胁、攻击1.5 弱点分析在为现有网络增加新的安全解决方案时，要先对网络状态有一个认识，了解当前的需求。
只有经过这些分析才可能对系统的某个部分的重新设计、重建进行改进并满足需要。
分析可以分解为以下几步：1.政策定位；2.网络分析；3.主机分析。
本章余下的部分将深入探讨每个步骤及分析工具。
1.5.1 政策定位如果已经存在安全策略，设计者要分析它并确定安全需求，这将影响方案的设计。
开始时，设计者应检查两项基本的安全策略。
？
确定需要保护的资源。
这将帮助设计者对网络中敏感的计算机资源提供正确的保护级别并确认敏感的数据流。
一确认可能的攻击者。
这将帮助设计者为内部及外部用户分配信任等级，并更细致地划分用户，如合作伙伴、消费者、IT外购合作者。
设计者也应利用风险评估过程估算安全策略是否是可发展的。
例如，安全策略中是否包含了所有可能的风险，是否忽视了一些重要的威胁。
设计者还应评估安全策略的防御过程以确定是否可防御所有威胁，这将确保安全策略是通用的、完整的。
对于需要高安全级别保护的组织还需要更深入地防护以避免单点故障。
设计者也需要确定相对于被保护资源，安全设备的投资是可接受的。
策略分析的结果如下：策略评估的正确性及完整性；确定在安全策略实施阶段之前，应做的改进。

第一图书网, tushu007.com

编辑推荐

《思科网络技术学院教程网络安全(第1、2学期)》作为思科网络技术学院网络安全的指定教材，适合具备CCNA水平的读者学习。
另外，将要参加思科公司的CCSP认证考试的人员也可以把《思科网络技术学院教程网络安全(第1、2学期)》作为考试指南。

第一图书网, tushu007.com

<<思科网络技术学院教程>>

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