Cisco Systems

CISCO NETWORKING ACADEMY PROGRAM

ciscopress.com

思科网络技术学院教程
网络安全基础

Cisco Networking Academy Program

Fundamentals of Network Security

Companion Guide

The only authorized textbook for the Cisco Networking Academy Program

内附光盘

[美] Cisco Systems 公司
Cisco Networking Academy Program 著
李涤非 欧岩亮 秦华 译

人民邮电出版社
POSTS & TELECOM PRESS

思科网络技术学院教程
网络安全基础

[美] Cisco Systems 公司
Cisco Networking Academy Program 著

李涤非 欧岩亮 秦 华 译

人民邮电出版社

图书在版编目（CIP）数据

网络安全基础/美国思科公司，思科网络技术学院著；李涤非，欧岩亮，秦华译.
—北京：人民邮电出版社，2005.4
思科网络技术学院教程

ISBN 7-115-13160-0

Ⅰ．网… Ⅱ．①美…②思…③李…④欧…⑤秦… Ⅲ．计算机网络—安全技术—高等学校—教材 Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2005）第 020940 号

思科网络技术学院教程

网络安全基础

◆ 著 [美] Cisco Systems 公司
Cisco Networking Academy Program
译 李涤非 欧岩亮 秦 华
责任编辑 陈 昇

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 ciscobooks@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67132705
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：38.5
字数：962 千字 2005 年 4 月第 1 版
印数：1－4 000 册 2005 年 4 月北京第 1 次印刷

著作权合同登记号 图字：01-2003-4801 号
ISBN 7-115-13160-0/TP・4490

定价：80.00 元（附光盘）

本书如有印装质量问题，请与本社联系 电话：（010）67129223

内容提要

本书是“思科网络技术学院教程 网络安全基础”课程的官方指定教材，是对该课程的课堂教学的补充。全书共分为15章，分别介绍了网络安全概览、基础路由器与交换机安全、路由器 ACL 和 CBAC、路由器 AAA 安全、路由器入侵检测、监测和管理、路由器端到端的 VPN、路由器远程访问 VPN、PIX 防火墙、PIX 防火墙的地址转换和连接、PIX 防火墙的访问控制列表（ ACL）、PIX 防火墙的 AAA、PIX 高级协议与入侵检测、PIX 故障切换与系统维护、PIX 防火墙 VPN、PIX 防火墙管理等内容。

本书适合参加思科网络技术学院网络安全基础课程的读者使用，对于参加 CCSP 和 CCIE 安全考试的读者也有较大的帮助。

前　言

*网络安全基础*连同*网络安全基础实验练习*，与相应的思科网络学院在线课程一同为您提供网络安全的全面介绍。

思科网络学院课程能帮您在计算机网络领域中获得职位，或者接受深层次的教育培训。网络安全基础课程重点关注基于安全策略的总体安全过程，主要强调安全边界、安全连接、安全管理、身份验证服务和入侵检测。本书也包括在 Cisco IOS 防火墙和 PIX Security Appliance 上安装、配置、监控和维护使用 Cisco 基于 CLI 和基于 Web 的设备管理器。

*网络安全基础*的设计目的是让用户可随时随地参考查阅。本书补充了课程中的材料，帮助您关注重要的概念并有助于安排好您的备考学习时间。

本书完全符合 Cisco 在课程中所使用的形式和格式。附带的光盘中包括了交叉引用的照片活动、电子实验活动，以及以生动的交互多媒体形式表现出的各种学习参考资料。

本书还介绍了 Cisco 公司 CCSP SECUR 和 CSPFA 考试的全部主题。

本书的目标

本书的目标使您学习基于安全策略的总体安全过程，主要强调的领域是安全边界、安全连接、安全管理、身份验证服务和入侵检测。本书设计与思科网络学院课程结合使用，也可单独作为参考资料。

本书的读者

本书面向任何要学习网络安全和总体安全过程的读者。主要的读者是社区学院和四年制的大学本科生。本书可用作课堂上的教科书，适合于具有 CCNA 证书或具有同等知识的读者使用。读者应该熟练掌握 TCP/ IP 和基本的网络概念。

其次面向的读者是企业的教育职员和全体教师。对于要想获得有效安全措施的公司和机构而言，必须在设计和实施安全技术、产品和解决方案方面对每个人进行培训。

最后面向的是一般用户。对于那些想要避开传统技术手册的用户来说，本书是他们的良师益友。

本书的特性

本书的很多特性可帮助读者加快对本书中所介绍的连网和路由选择技术的全面理解。

- **目标**——每章以一个目标列表开始，学习完本章后应掌握这些目标。目标提供了该章中所介绍概念的参考。

- **图、例、表和案例**——本书包含的图、例和表有助于解释各种理论、概念、命令和安装顺序，从而加深对概念的理解并有助于以直观的方式理解章中所介绍的内容。另外，特定的案例也提供了详细描述问题和解决方案的现实生活场景。
- **章节总结**——每章末尾是该章所涉及概念的总结，它提供了章节提要，可帮助学习。
- **关键术语**——多数章包括该章所涉及的关键术语。这些术语可帮助学习。另外，关键术语强化了章中所介绍的概念，并且在您学习新的概念前，有助于理解该章中的材料，在章中实际使用该术语的位置，您可以找到用黑体和斜体字突出显示的关键术语。
- **复习题和答案**——在每章结尾出现的复习题可作为对学习的评估。这些问题强化了每章中的概念，并且在学习其他章节之前，可测试您对本章内容的掌握情况。
- **技能提高活动**——本书中所引用的试验活动可在《思科网络技术学院教程　网络安全基础实验手册与练习册》一书中找到。这些试验可帮助您将理论与实践相结合。

本书的组织方式

本书分为 15 章和 4 个附录。

- **第 1 章“网络安全概述”**——本章提供基本的网络安全概述，包括对攻击和威胁的介绍，其他的主题包括安全框架和策略，最后介绍了安全产品和解决方案。
- **第 2 章“基本的路由器和交换机安全”**——本章首先介绍了一般的路由器和交换机安全，说明了禁用不需要服务的重要性。本章还介绍了边界路由器的概念，并讨论了路由器管理。最后探讨了保护交换机和 LAN 访问安全的主题。
- **第 3 章“路由器 ACL 和 CBAC”**——本章介绍访问控制列表（ACL），包括 IP ACL 的类型。还介绍了基于上下文的访问控制（CBAC），包括：
  - 任务 1 和 2：配置 CBAC
  - 任务 3：使用端口到应用程序映射（PAM）
  - 任务 4：定义检查规则
  - 任务 5：应用检查规则和 ACL 到路由器接口
  - 任务 6：测试和检验 CBAC
- **第 4 章“路由器 AAA 安全”**——本章描述了验证、授权和记账（AAA）安全网络访问，包括网络访问服务器（NAS）AAA 验证过程和 Cisco 安全访问控制服务器的实现，本章还介绍了 AAA 服务器的概述和配置，最后介绍了 Cisco IOS 防火墙验证代理。
- **第 5 章“路由器入侵检测、监控和管理”**——本章介绍 IOS 防火墙入侵检测系统（IDS），说明了设置 IDS 并用日志记录和系统日志进行监控的过程。本章还讨论了简单网络管理协议（SNMP），介绍了管理路由器的方法，最后介绍了安全设备管理器（SDM）。
- **第 6 章“路由器配置站点到站点 VPN”**——本章介绍了虚拟专用网（VPN），然后讨论了 IOS 加密系统。文中解释了 IPSec，包括使用预共享密钥的站点到站点 IPSec VPN 的概念和数字证书。最后讨论了使用数字证书配置站点到站点 IPSec VPN 的方法。
- **第 7 章“路由器远程访问 VPN”**——本章介绍远程访问 VPN，还介绍了 Cisco Easy VPN 和 Cisco VPN 3.5 客户端。最后讨论了 VPN 企业管理。

- **第 8 章“PIX Security Appliance”**——本章介绍防火墙，并概述了各种 PIX Security Appliance 的型号、特点及其性能。本章所讨论的 PIX Security Appliance 主题包括启动、路由选择和多播配置，以及使用动态主机配置协议（DHCP）。
- **第 9 章“PIX Security Appliance 转换和连接”**——本章讨论了传输协议、网络地址转换和配置域名系统（DNS）的支持。介绍完转换后讨论的是连接。另外，本章还解释了如何在 PIX Security Appliance 上使用端口地址转换（PAT）。最后讨论了 PIX Security Appliance 上的多个接口。
- **第 10 章“PIX Security Appliance 访问控制列表”**——本章讨论了 ACL 和 PIX Security Appliance，举例说明如何使用 ACL。其他介绍的内容包括过滤、对象组和嵌套的对象组。
- **第 11 章“PIX 安全应用 AAA”**——本章介绍了如何在 PIX Security Appliance 上使用 AAA，包含验证配置、授权配置和记账配置。最后讨论了 PPPoE 和 PIX Security Appliance。
- **第 12 章“PIX 高级协议和入侵检测”**——本章介绍了使用 PIX Security Appliance 对高级协议的处理。还介绍了对多媒体的支持。另外，文中说明了 PIX Security Appliance 的配置，以提供攻击防护和入侵检测。本章定义了规避方法并提供了多个配置示例。也介绍了 PIX Security Appliance 的系统日志配置。最后讨论了 SNMP 和 PIX Security Appliance。
- **第 13 章“PIX 故障转移与系统维护”**——本章首先讨论了理解故障转移概念的内容，还讨论了串行电缆故障转移和基于 LAN 的故障转移。其他的主题包括通过远程访问进行系统维护和命令授权方法，最后介绍了密码恢复和 PIX Security Appliance 的升级。
- **第 14 章“PIX Security Appliance VPN”**——本章主要讨论 PIX Security Appliance 如何启用安全的虚拟专用网（VPN），还介绍了配置 VPN 的任务，包括：
  - 任务 1：有关 VPN 支持准备的配置
  - 任务 2：配置 IKE 参数
  - 任务 3：配置 IPSec 参数
  - 任务 4：测试和验证 VPN 配置

另外，本章还介绍了 Cisco VPN 客户端到 PIX Security Appliance VPN 和扩展 PIX Security Appliance VPN 的方法。

- **第 15 章“PIX Security Appliance 管理”**——本章介绍 PIX Security Appliance 管理工具，包括 Cisco PIX 设备管理器（PDM），讲述了如何准备 PDM、如何使用 PDM 配置 PIX Security Appliance，以及如何用它来创建站点到站点和远程访问 VPN。最后讨论了企业 PIX 管理。
- **附录 A“关键术语”**——该术语表包含本书中使用的所有关键术语。
- **附录 B“复习题的答案”**——本附录包含了每章末的习题答案。
- **附录 C“物理层安全”**——本附录讨论了从最基本到最复杂级别的第 1 层安全。指出了用户和网络所面对的一些威胁。本附录还讨论了在基础级别上管理网络安全的企业所能获得的好处。
- **附录 D“操作系统安全”**——本附录讨论了操作系统安全许多复杂的细节问题，附录的第一部分讨论了 Linux 操作系统的安全，第二部分讨论了 Windows 操作系统的安全。

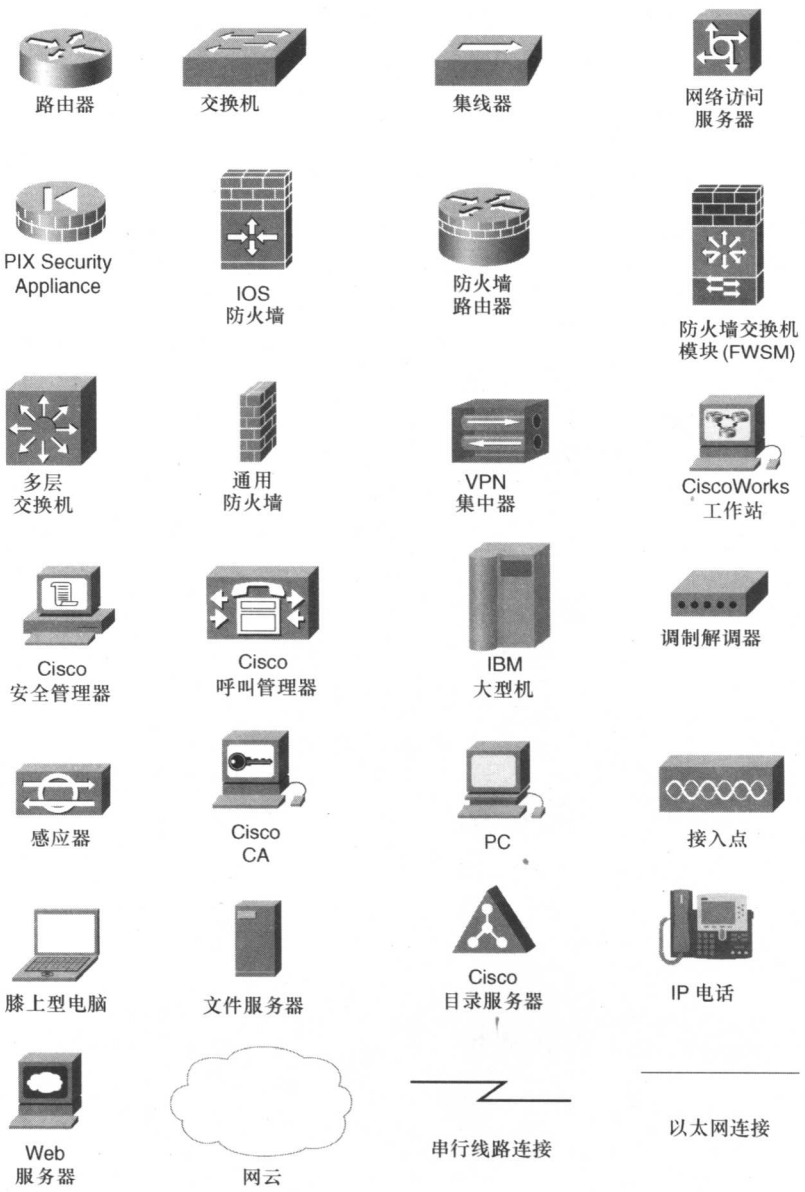
命令语法约定

本书中使用的命令语法约定与 Cisco IOS 软件命令参考中所用的约定相同。命令参考中描述的约定如下：

- 竖线(|)用来分开可选的互斥参数。
- 方括号([ ])括出可选的参数。
- 花括号（{}）表示必需的选项。
- 方括号套尖括号([{ }])表示可选的命令中必要的参数。
- **黑体字**指出指令和关键字。
- *斜体字*表示要提供的参数值。

Cisco 系统网络图标说明

Cisco 公司使用了标准化的图标集来表示网络拓扑结构说明中的各种设备，下面的图标说明中显示了最常见的图标，全书中会经常出现这些图标。



目　录

第一部分

第三部分