Cisco Networking Academy Program

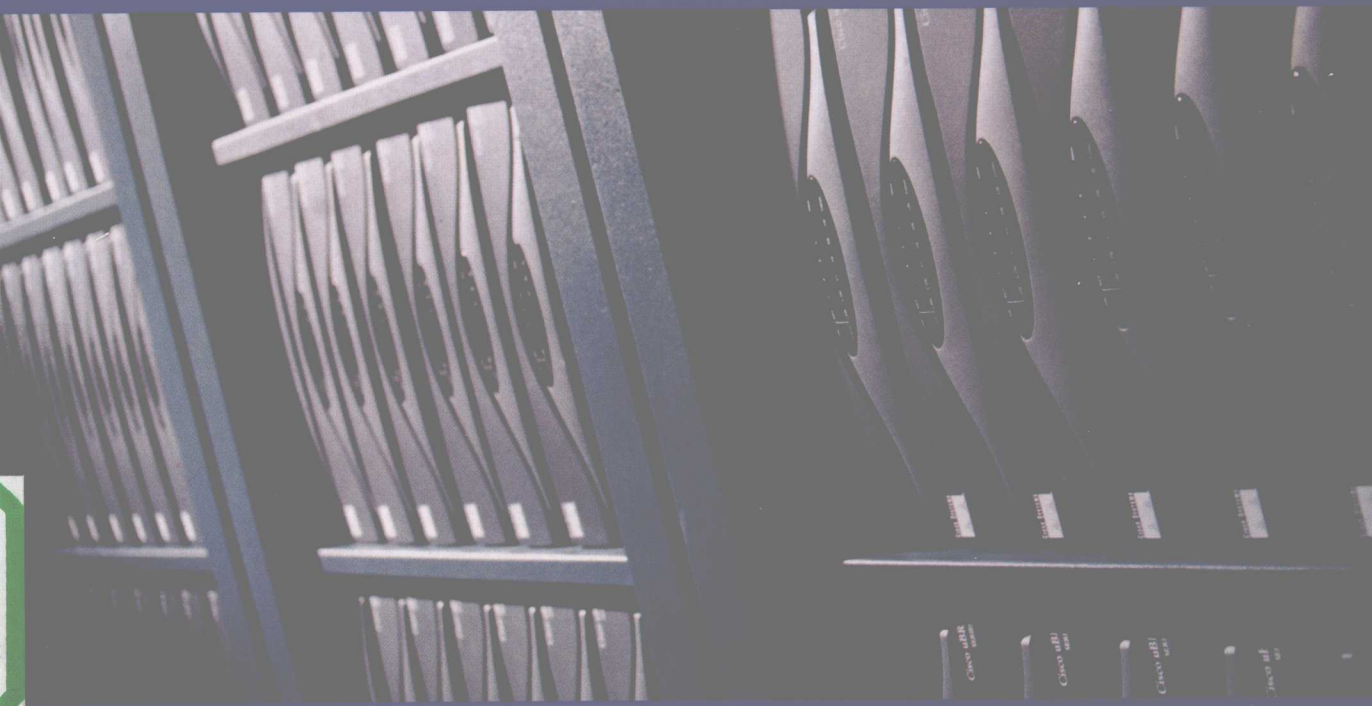
思科网络技术学院教程

网络安全（第一、二学期）

Network Security

1 and 2 Companion Guide

〔美〕Antoon W. Rufi 著
北京邮电大学 思科网络技术学院 译



The only authorized Companion Guide for the Cisco Networking Academy Program
思科网络技术学院唯一正规配套教材

人民邮电出版社
POSTS & TELECOM PRESS

Cisco Networking Academy Program

思科网络技术学院教程

网络安全（第一、二学期）

Network Security

1 and 2 Companion Guide

〔美〕Antoon W. Rufi 著

北京邮电大学 思科网络技术学院 译

人民邮电出版社

北京

图书在版编目（CIP）数据

思科网络技术学院教程．网络安全／（美）拉菲（Rufi, A.W.）著；北京邮电大学思科网络技术学院译．—北京：人民邮电出版社，2008.10
ISBN 978-7-115-18300-2

Ⅰ．思… Ⅱ．①拉…②北… Ⅲ．计算机网络—安全技术—教材 Ⅳ．TP393

中国版本图书馆 CIP 数据核字（2008）第 117086 号

版 权 声 明

思科网络技术学院教程 网络安全（第一、二学期）

◆ 著 [美] Antoon W. Rufi
译 北京邮电大学 思科网络技术学院
责任编辑 李 际

◆ 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 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京铭成印刷有限公司印刷

◆ 开本：787×1092 1/16
印张：34.5
字数：1 022 千字 2008 年 10 月第 1 版
印数：1－4 000 册 2008 年 10 月北京第 1 次印刷

著作权合同登记号 图字：01-2006-5642
ISBN 978-7-115-18300-2/TP

定价：75.00 元（附光盘）

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

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。

第二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入侵预防系统（Intrusion prevention system，IPS）；
- 使用路由器和防火墙实现虚拟专用网（Virtual private network，VPN）。

本书被设计作为一门课程材料的便捷桌面参考，可以随时随地使用。本书对课程中的内容进行强化，帮助你关注重点概念、为考试合理安排学习时间。

本书的目标

本书的目标是基于安全策略设计和管理教授全部安全过程。重点是安全技术、产品、解决方案，以及防火墙和安全路由器设计、安装、配置、维护。本书的第一学期课程内容介绍了使用路由器和防火墙实现认证、授权、计费（authentication, authorization, and accounting，AAA），以及在 OSI 模型的第二层和第三层进行网络保护。本书的第二学期课程内容介绍了使用路由器和防火墙实现入侵预防系统（intrusion prevention system，IPS），以及使用路由器和防火墙实现虚拟专用网（virtual private network，VPN）。本书设计用来与思科网络学院课程一起使用，也可以作为独立的参考书。

本书的读者

本书是为所有希望学习网络安全以及整体安全处理的读者编写的。主要目标读者是网络学院及四年制大学的学生。在教学环境中，本书可以作为在教室里使用的参考书。本书适合具有 CCNA 证书或具备同等知识的读者阅读。读者应掌握 TCP/IP 和基本的网络概念。

本书的第二类目标读者是专业培训机构的人员。为了使公司和学术机构能够使用有效的安全措施，必须对个人进行安全技术、产品以及解决方案的设计和实现方面培训。第三类目标读者是普通用户。本书适宜用户阅读，对那些不喜欢阅读传统技术手册的读者也很有吸引力。

本书的特点

本书的很多特点能够帮助读者全面理解书中的网络和路由知识。

- **目标**——每章开始列出了完成本章应达到的目标。它提供了对本章概念的参考。
- **图形、例子、表格、场景**——本书包含有助于解释理论、概念和命令的图形、例子以及表格。另外，特定的场景提供了能够使问题和解决方案具体化的真实生活情景。
- **每章总结**——每章最后是对本章关键概念的总结。它提供了本章的大纲，帮助学习。
- **关键术语**——大多数章列出了本章的关键术语，帮助学习。另外，关键术语对本章介绍的概念进行强化，帮助你在进入新概念之前理解本章内容。
- **“检查你的理解”问题**——每章最后是用于评估学习效果的复习题。这些问题对本章介绍的概念进行加强，并帮助你在进入其他章之前检查自己的理解情况。
- **技能培养**——本书中贯穿了实验室活动，这些实验使你能够将理论与实践联系起来。

本书是如何组织的

本书分为 18 章和 1 个附录。

第一学期

- **第 1 章**——互联网持续以指数级增长。随着个人、政府、商业应用在互联网上的普及，产生了很多直接的利益。然而，这些基于网络的应用和服务也对个人、公司或政府的信息资源造成安全风险。很多情况下，急于联网是以牺牲网络安全为代价的。信息是必须要被保护的财产。没有适当的网络安全，很多个人、公司、政府将要承担财产丢失的风险。网络安全是保护数字信息财产的过程。安全的目标是保护机密性、维持完整性、确保可用性。需要记住，如果一项业务要发挥它的最大潜力，必须保护所有网络不受威胁和攻击。典型情况下，由于弱点始终存在，这些威胁也是持续的，弱点的起源可能是软硬件配置错误、网络设计不当、继承的技术弱点或最终用户的粗心。本章对基本网络安全概念、常见弱点、威胁、攻击以及弱点分析进行了概览。
- **第 2 章**——安全风险不能被彻底消除或预防。但有效的风险管理和评估可以显著减小现存的安全风险。可以接受的风险级别取决于该业务能够消化多少风险。安全策略是决定如何管理风险时的一个重要组成部分。安全策略是对人们在获准使用某一组织的技术或访问某一组织的信息资产时，所必须遵守的规则的正式声明。安全策略可以是简单的网络资源使用政策，也可以非常复杂，长达上百页，对连接及相关政策的每一点都详细定义。路由器能够支持多种网络服务，使用户及主机进程连接到网络上。有些服务可以被限制或禁用，在不影响网络运行的前提下提高安全性。出于安全性考虑，网络设备通常只应该支持其所在网络需要的流量和协议。
- **第 3 章**——本章以网络防火墙的讨论开始。防火墙的存在增强了企业的安全性。通过在企业内部网络和外部网络之间提供必要的安全性，防火墙使在线商务成为可能。再加上访问控制，防火墙可成为网络安全管理的关键设备（焦点）。本章介绍 Cisco IOS 防火墙特性集、Cisco PIX 安全产品、Cisco 自适应安全产品和防火墙服务模块。这涵盖了各种不同的 PIX 产品、自适应安全产品模块及它们的功能和特性。虽然安全产品不是路由器，但它们却有一定的路由能力。同时，安全产品的基本配置命令也包含在本章中。再加上访问控制，防火墙可成为网络安全管理的关键设备（焦点）。

  本章还介绍了安全设备管理器（SDM）和自适应安全设备管理器（ASDM），它们通过图形化的用户界面提供更快速、更容易的配置方法。理解 TCP 和 UDP 如何用于安全产品的一个

重要方面是考察转换和连接。当流量从内部网络到外部网络或从外部到内部时，这些项目如何使用就变得非常重要。在考察转换和连接方面，本章将讲述网络地址转换（NAT）。

本章也包含端口地址转换（PAT）和 PIX 安全产品上的多接口配置。PAT 是一种类似于 NAT 的转换方法，它可使网管人员对外部用户隐藏内部网络地址结构并允许 IP 地址间的转换。然而，与 NAT 不同，它是以一对一为基础来租用 IP 地址的，它可更进一步，允许大量内部用户使用一个 IP 地址，此过程称为过载。

现在，你可以理解如何配置多个接口，该模块讨论了 PIX 安全产品如何支持额外的边界接口。

- **第 4 章**——本章全面介绍了验证、授权和记账（AAA）的体系结构，并且昭示了它们在网络安全中对于身份服务的重要性。AAA 安全是一个机构的全面网络安全策略的主要组成之一。AAA 是对网络的远程访问和网络设备的远程管理提供安全性的基本要素。在简要地讨论 AAA 之后，将要讨论一系列验证方法。

  本章同时介绍了 Cisco 基于身份的网络服务（IBNS）和网络准入控制（NAC）。IBNS 是一个结合 Cisco 产品的完整解决方案，提供了对于网络连通性及资源进行验证、访问控制和用户策略等安全机制。NAC 是由工业界倡导，由 Cisco 公司发起的，使用网络架构在所有设备上执行安全策略，以寻求访问网络资源，从而能够限制病毒和蠕虫的攻击。
- **第 5 章**——Cisco 安全访问控制服务器（ACS）网络安全软件通过控制对一个 AAA 客户的访问，来帮助你验证用户。AAA 客户可以是任意一个网络上的设备，只要它配置了遵从网络用户到 AAA 服务器的验证和授权。Cisco 安全 ACS 的运行类似 Windows 的一项服务，它对访问网络的用户进行 AAA 控制。本章描述了 Cisco 安全 ACS 的特性、功能和体系结构，以及如何在 Cisco 路由器和交换机上配置 TACACS+和 RADIUS 与 Cisco 安全 ACS 共同工作。学完本章后，你将能够对基于 Windows 的 Cisco 安全 ACS 服务器进行安装、配置、运行和排错；你将能够描述基于 Windows 的 Cisco 安全 ACS 服务器的功能、特性和三元素的体系结构；你同样能够通过 Cisco 安全 ACS Windows 服务器来配置 TACACS+和 RADIUS。
- **第 6 章**——认证代理提供动态的、基于每个用户的认证和授权，根据工业标准 TACACS+及 RADIUS 认证协议对用户进行认证。对用户连接进行认证和授权为防止网络遭受攻击提供了更多的健壮性保护。在这章中，你将学习如何使用认证代理配置一台 Cisco 路由器进行认证。然后，本章将介绍如何在 PIX 安全产品上进行 AAA 的配置、监控和故障处理。
- **第 7 章**——Cisco 基于身份的网络服务（Identity Based Networking Services，IBNS）是一项集成解决方案，它结合了多项 Cisco 产品，这些产品提供的服务包括为保护网络连接和资源进行的认证、访问控制以及用户策略。Cisco IBNS 解决方案在带来更高安全性的同时，为组织的变化提供低成本管理。本章将介绍 Cisco IBNS，还将讨论 802.1x 和 EAP 与 IBNS 的关系。你还将学习到如何配置一台 Cisco 安全访问控制服务器 ACS（Secure Access Control Server）使用 EAP-MD5 和 RADIUS 进行认证。本章还讨论了使用 IEEE 802.1x 基于端口的认证来阻止未经授权的设备访问网络。随着局域网扩展到旅馆、机场、公司休息室，不安全的环境也相应产生。IEEE 802.1x 标准定义了一种基于客户端/服务器的访问控制和认证协议，限制未经授权的客户端通过公共可访问端口连接到局域网。认证中心在开放任何交换机或局域网提供的服务之前，将对每个连接到交换机端口的客户端进行认证。你可以在一台 Cisco Catalyst 交换机上学习配置 802.1x 基于端口的认证的必要步骤。
- **第 8 章**——本章详细讨论如何使用 Cisco IOS 防火墙特性集中的关键内容：基于上下文的访问控制（CBAC）实现网络安全。访问控制列表（ACL）用于过滤和保护网络流量。ACL 通过控制在接口上是转发还是阻塞被路由或被交换的数据包来过滤网络流量。每个数据包都按照在 ACL 中定义的规则被检查以确定如何处理。我们将详细讨论 ACL 的一种形式：CBAC。通过检查三层或更高层次的数据包内容，CBAC 可以提供更高级别的安全性。CBAC 收集的信息用来

建立防火墙 ACL 的临时开放通路。在本章中，你将学习到创建和建立 CBAC 所需的步骤。除了应用于 ACL，CBAC 还有其他用途。进入防火墙的数据包如果第一次通过了接口的入站 ACL 检查，才能被 CBAC 检查。如果数据包被 ACL 拒绝，则数据包被丢弃不被 CBAC 检查。

- **第 9 章**——本章包括访问控制列表（ACL）以及 PIX 安全器件如何处理 ACL。本章的第一部分关注于配置 ACL 以及了解在不同的网络环境中如何、何时使用 ACL。这部分还讨论 applet 过滤和 URL 过滤。你将了解到何时使用这项技术以及它的必要性。本章还介绍对象分组（object grouping）的概念，它将 ACL 放到对象以及嵌套对象分组中。为了简化创建和应用 ACL 的任务，管理员可以将网络对象（例如主机）分组，也可以将服务（例如 FTP 和 HTTP）分组。分组的 ACL 可以显著减少单条 ACL 的数目。模块化策略在配置网络策略时提供更细的粒度和更高的灵活性。模块化策略框架 Modular Policy Framework（MPF）提供了一种一致、灵活的方式来配置 PIX 安全器件特性。可以使用 MPF 的一种情况是为特定的 TCP 应用创建一个超时配置，而不是一个应用于所有 TCP 应用的配置。本章以对高级协议的处理和检查，以及你能如何调整它以适合 PIX 安全器件运行的讨论结束。本章继续讨论用于多媒体支持的高级协议，包括实时流协议，也包括支持 IP 电话所需要的协议。
- **第 10 章**——类似于路由器，二层和三层交换机都有自己的安全要求。然而，不像路由器有那么多讨论安全问题和防范风险的公共信息。本模块讨论二层攻击及如果利用 Cisco IOS 特性减少对网络威胁的方法。涉及二层攻击的几种类型和防范这些攻击的策略。完成本章的学习，你将掌握减少二层攻击威胁的方法，包括内容可寻址内存（CAM）表过载、VLAN 跳跃、生成树协议操纵、MAC 地址欺骗和 DHCP 耗尽。

第二学期

- **第 1 章**——本章介绍入侵防御和检测的基本概念。讨论了入侵检测系统（intrusion detection system，IDS）和入侵防御系统（intrusion prevention system，IPS）使用的检测引擎的基本类型。本章介绍了作为 Cisco 自防御网络解决方案中的组成部分的 IDS 和 IPS 设备。
- **第 2 章**——本章描述 Cisco IOS 入侵检测系统。并讨论在 PIX 安全产品上配置攻击卫士、入侵防护和避免的配置。
- **第 3 章**——这一章主要介绍 Cisco 支持 VPN 的设备上可用的虚拟私用网（virtual private network，VPN）协议。VPN 为远程用户在公网上提供与使用私用网络一样的网络连通性。然而，在允许用户访问网络之前，必须采取某种措施确认真实性、数据完整性和加密。在这一章中，介绍了两种基本的 VPN 类型：站点到站点 VPN 和远程访问 VPN。这里有对用于在 VPN 连接中确认真实性、数据完整性和机密性的协议和设备的深入讨论。
- **第 4 章**——本章包含 Cisco IOS 路由器和 PIX 安全器件的站点到站点 VPN（site-to-site VPN）配置。VPN 为远程用户在公网架构上提供与用户使用私有网络相同的网络连通性。然而，在允许用户访问网络之前，你必须采取一定的措施来保证真实性、数据完整性以及加密。本章讨论了如何为使用预共享密钥的站点到站点 VPN 标识和配置用于保证真实性、数据完整性、机密性的协议。
- **第 5 章**——本章将指导您在 Cisco 路由器上配置认证中心（certificate authorities，CA）的步骤。包括的内容有如何管理非易失性 RAM（nonvolatile RAM，NVRAM），如何在路由器上设置时间和日期，使用何种命令配置 RSA 密钥和 CA。本章的目标是使您能够在 Cisco IOS 路由器和 PIX 安全设备上完成使用数字证书认证来建立站点到站点 VPN。
- **第 6 章**——本章介绍了 Cisco Easy VPN 的两个组件：Cisco Easy VPN 服务器和 Cisco Easy VPN Remote。这两个组件协同工作，为用户提供安全、可靠、受保护的远程访问 VPN。本章包括 Easy VPN 如何工作，以及用户和管理员如何使用 Easy VPN 来简化安全 VPN（secure VPN）

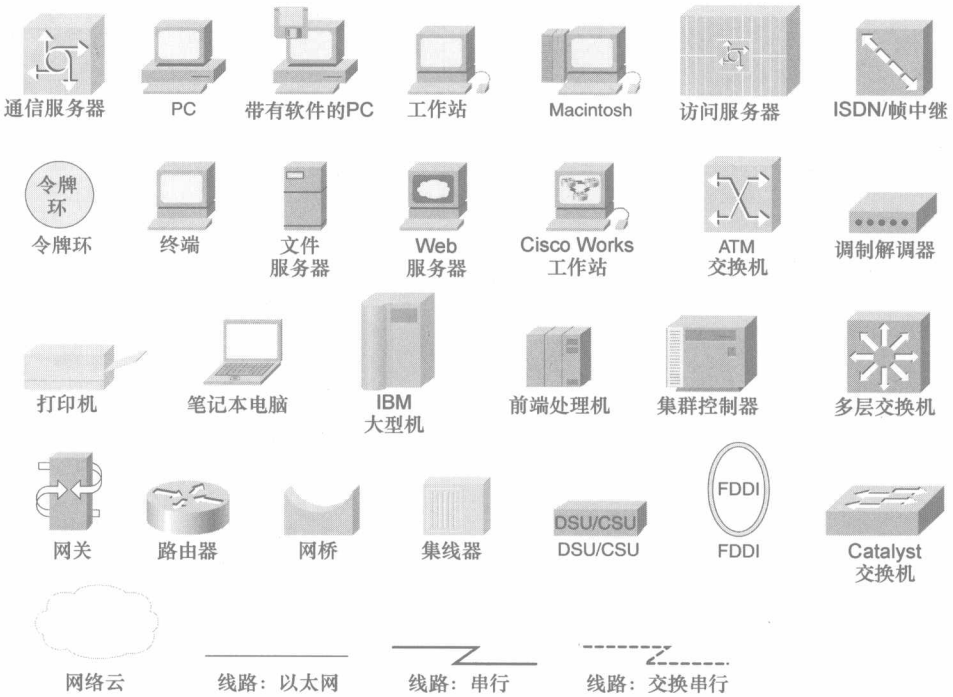
的创建。本章还包括将路由器和 PIX 安全器件配置为 Easy VPN 服务器。你也能学习到使用 Cisco VPN 客户端、Cisco 路由器、PIX 501 和 506/506E 配置 Easy VPN Remote。本章还解释了如何在一台适应性安全器件（Adaptive Security Appliance，ASA）上配置 WebVPN。

- **第 7 章**——本章以对二层安全最佳实践的讨论开始。介绍多个物理网络场景，然后逐个给出它们的弱点和解决技术。然后讨论安全设备管理器（Security Device Manager，SDM）安全审计特性。SDM 包含一个独特的安全审计向导（Security Audit Wizard），能够提供全面的路由器安全审计。SDM 使用来自 Cisco 技术支持中心（Cisco Technical Assistance Center，TAC）和因特网计算机安全联盟（International Computer Security Association，ICSA）的安全配置作为比较的基线和默认设置。本章还探讨了 VPN 的企业管理。管理是实现大型站点到站点（site-to-site）及远程访问 VPN 的最大挑战之一。VPN 路由器管理中心（Router MC）的主要任务是管理站点到站点 VPN。也讨论了理解 VPN 所需的关键主题。深入理解 Router MC 如何运作有助于更好地管理大型 VPN。最后，学习简单网络管理协议（Simple Network Management Protocol，SNMP）。
- **第 8 章**——本章提供了对安全上下文的概览和解释。一台单独的 PIX 安全器件可以被划分为多个虚拟防火墙，称为安全上下文。每个上下文都是一个独立的防火墙，有自己的安全策略、接口以及管理员。多个上下文类似于有多个独立防火墙。本章接下来讨论了安全上下文的配置和管理。

附录：

- **附录 A**——每章后面提供“检查你的理解”部分的问题的答案。
- **术语表**——列出了所有贯穿本书的关键术语。

本书中使用的图标



命令语法规则

本书中用于表示命令语法的规则同 IOS 命令手册一致。命令手册中的表示规则描述如下：

- 粗体字代表输入的是命令或关键字；在实际配置例子和输出（非常规的命令语法）中，粗体字代表用户手工输入的命令（如 **show** 命令）；
- 斜体字指用户实际输入的参数值；
- 竖线“|”用于分割可选的、互斥的选项；
- 方括号“[]”表示可选项；
- 花括号“{}”表示必选项；
- 方括号中的花括号“[{}]”表示必须在任选项中选择一个。

内容提要

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。

关于作者

Antoon "Tony"W. Rufi 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、网络安全以及IP电话课程。在成为ECPI讲师之前，他在美国空军工作近30年，从事大量电子及计算机程序和项目工作。Tony现在与妻子居住在佛吉尼亚州的普库森，他们已经在那里生活了33年。

关于技术审稿人

Dale Liu（CCAI、CCNA、CISSP、NSA IAM、NSA IEM）已经在计算机和网络领域工作了20年，具有编程、网络、信息安全等多方面经验。他目前讲授网络、路由以及安全课程，并在中小型公司的安全审计和架构设计领域工作。Dale目前居住在得克萨斯州的休斯顿。

Belle Woodward（CCNA、CCAI、CCNP）在位于伊利诺伊州卡本代尔的南伊利诺伊大学（SIU，Southern Illinois University）应用科学与艺术学院信息系统和应用技术学校担任助教。Belle有超过8年的网络和网络安全经验。她讲授网络安全、高级网络以及电信学。她对网络及网络安全大学课程进行重新设计后，她的学生在2006年美国中西部地区学院赛博对抗赛（CCDC，Collegiate Cyber Defense Competition）中获得第一名，并在美国全国CCDC中获得第四名。

献　　词

本书献给我的父母 Maxdonald 和 Ellen Rufi。我的父母带着美国梦于 1960 年移民到美国。没有他们的支持，这本书将不可能完成。

致　　谢

我要特别感谢 ECPI 技术学院院长 Mark Dreyfus 先生，以及主管学院事务的副院长 John Olson 先生。他们这些年来对 ECPI 的 Cisco 学院课程的鼓励和支持使我得以在不同的 Cisco 平台上吸收尽可能多的信息，并将这些信息传播给尽可能多的学生。

我还要感谢 Belle Woodward 为第二学期写作第 7 章。她是一位每个人都希望得到的好朋友，丝毫不吝于把她的经验灌注到这一章的内容中。

最后，但并非最不重要，我要感谢我的妻子Linda，她牺牲了我们在一起的时间，使我能够完成这一项目；还有我的岳父Dick Hamilton，尽管计算机并非他的本职，他仍为我提供了公正的意见，并对第一次的完成稿进行了一些重要编辑。

目　录

第一学期

第 1 章　弱点、威胁、攻击 ····· 2
1.1　关键术语 ····· 2
1.2　网络安全简介 ····· 3
1.2.1　网络安全需求 ····· 3
1.2.2　识别网络安全的潜在风险 ····· 5
1.2.3　开放的与封闭的安全模型 ····· 5
1.2.4　网络安全的发展趋势 ····· 9
1.2.5　信息安全组织 ····· 11
1.3　弱点、威胁和攻击介绍 ····· 12
1.3.1　弱点 ····· 13
1.3.2　威胁 ····· 14
1.3.3　攻击 ····· 15
1.4　攻击事例 ····· 16
1.4.1　侦查攻击 ····· 17
1.4.2　访问攻击 ····· 18
1.4.3　拒绝服务（DoS）攻击 ····· 21
1.4.4　假冒/IP 欺骗攻击 ····· 22
1.4.5　分布式拒绝服务攻击 ····· 23
1.4.6　恶意代码 ····· 25
1.5　弱点分析 ····· 27
1.5.1　政策定位 ····· 27
1.5.2　网络分析 ····· 27
1.5.3　主机分析 ····· 30
1.5.4　分析工具 ····· 31
1.6　总结 ····· 31
1.7　检查你的理解 ····· 32
第 2 章　安全计划与策略 ····· 34
2.1　关键术语 ····· 34
2.2　关于网络安全及 Cisco ····· 34
2.2.1　安全轮（Security Wheel）····· 35
2.2.2　网络安全策略 ····· 37
2.3　端点保护和管理 ····· 39
2.3.1　基于主机和服务器的安全组件和技术 ····· 39
2.3.2　PC 管理 ····· 41
2.4　网络保护和管理 ····· 42
2.4.1　基于网络的安全组件和技术 ····· 42
2.4.2　网络安全管理 ····· 47
2.5　安全体系 ····· 50
2.5.1　安全体系 SAFE ····· 50
2.5.2　Cisco 自防卫网络 ····· 51
2.5.3　保护连通性（secure connectivity）····· 51
2.5.4　威胁防范（Threat Defense）····· 52
2.5.5　Cisco 集成安全 ····· 54
2.5.6　计划、设计、实施、运行、优化模型（PDIOO、Plan、Design、Implement、Operate、Optimize）····· 55
2.6　基本的路由器安全 ····· 57
2.6.1　控制对网络设备的访问 ····· 57
2.6.2　使用 SSH 进行远程配置 ····· 59
2.6.3　路由器口令 ····· 60
2.6.4　路由器优先级和账户 ····· 62
2.6.5　Cisco IOS 网络服务 ····· 63
2.6.6　路由、代理 ARP、ICMP ····· 68
2.6.7　路由协议认证和升级过滤 ····· 70

2.6.8 NTP、SNMP、路由器名、DNS …… 72
2.7 总结 …… 74
2.8 检查你的理解 …… 74
第 3 章 安全设备 …… 76
3.1 可选设备 …… 76
3.1.1 Cisco 防火墙特性集 …… 77
3.1.2 创建用户的防火墙 …… 78
3.1.3 PIX 安全设备 …… 78
3.1.4 自适应安全设备 …… 79
3.1.5 Finesse 操作系统 …… 81
3.1.6 自适应安全算法 …… 81
3.1.7 防火墙服务模块 …… 81
3.2 使用安全设备管理器 …… 82
3.2.1 使用 SDM 启动向导 …… 83
3.2.2 SDM 用户界面 …… 84
3.2.3 SDM 向导 …… 85
3.2.4 用 SDM 配置 WAN …… 85
3.2.5 使用恢复出厂配置向导 …… 86
3.2.6 监控模式 …… 86
3.3 Cisco 安全设备家族介绍 …… 88
3.3.1 PIX501 安全设备 …… 88
3.3.2 PIX506E 安全设备 …… 88
3.3.3 PIX515E 安全设备 …… 88
3.3.4 PIX525 安全设备 …… 88
3.3.5 PIX535 安全设备 …… 89
3.3.6 自适应安全设备模块 …… 89
3.3.7 PIX 安全设备许可证 …… 91
3.3.8 PIX VPN 加密许可 …… 91
3.3.9 安全上下文 …… 92
3.3.10 PIX 安全设备上下文许可证 …… 92
3.3.11 ASA 安全设备许可证 …… 92
3.3.12 扩展 PIX515E 特性 …… 93
3.3.13 扩展 PIX525 特性 …… 93
3.3.14 扩展 PIX535 特性 …… 93
3.3.15 扩展自适应安全设备家族的特性 …… 94
3.4 开始配置 PIX 安全设备 …… 94
3.4.1 配置 PIX 安全设备 …… 95
3.4.2 帮助命令 …… 96
3.4.3 安全级别 …… 96
3.4.4 基本 PIX 安全设备的配置命令 …… 97
3.4.5 其他 PIX 安全设备的配置命令 …… 100
3.4.6 检查 PIX 安全设备的状态 …… 105
3.4.7 时间设置和 NTP 支持 …… 108
3.4.8 日志（syslog）配置 …… 109
3.5 安全设备的转换和连接 …… 111
3.5.1 传输协议 …… 111
3.5.2 NAT …… 112
3.5.3 动态内部 NAT …… 114
3.5.4 两个接口的 NAT …… 114
3.5.5 3 个接口的 NAT …… 115
3.5.6 PAT …… 116
3.5.7 增加 PAT 的全局地址池 …… 118
3.5.8 static 命令 …… 118
3.5.9 nat 0 命令 …… 120
3.5.10 连接和转换 …… 121
3.6 用自适应安全设备管理器管理 PIX …… 127
3.6.1 ASDM 运行需求 …… 127
3.6.2 ASDM 的准备 …… 129
3.6.3 使用 ASDM 配置 PIX 安全设备 …… 130
3.7 PIX 安全设备的路由功能 …… 131
3.7.1 虚拟 LAN …… 131
3.7.2 静态和 RIP 路由 …… 135
3.7.3 OSPF …… 137
3.7.4 多播路由 …… 140
3.8 防火墙服务模块的运行 …… 143
3.8.1 FWSM 的运行要求 …… 144
3.8.2 开始使用 FWSM …… 144
3.8.3 校验 FWSM 的安装 …… 145
3.8.4 配置 FWSM 的访问列表 …… 146
3.8.5 在 FWSM 上使用 PDM …… 147
3.8.6 重置和重启 FWSM …… 147
3.9 总结 …… 148
3.10 检查你的理解 …… 148
第 4 章 信任和身份技术 …… 150
4.1 关键术语 …… 150
4.2 AAA …… 150
4.2.1 TACACS …… 151
4.2.2 RADIUS …… 151
4.2.3 TACACS+和 RADIUS 的比较 …… 153
4.3 验证技术 …… 154

4.3.1 静态口令 …… 154
4.3.2 一次性口令 …… 154
4.3.3 令牌卡 …… 155
4.3.4 令牌卡和服务器方法 …… 155
4.3.5 数字证书 …… 156
4.3.6 生物测定学 …… 157
4.4 基于身份网络服务（IBNS） …… 158
4.5 有线的和无线的执行 …… 160
4.6 网络准入控制（NAC） …… 161
4.6.1 NAC 组成 …… 161
4.6.2 NAC 阶段 …… 162
4.6.3 NAC 运行 …… 163
4.6.4 NAC 厂商的参与 …… 164
4.7 总结 …… 165
4.8 检查你的理解 …… 165
第 5 章 Cisco 安全访问控制服务器 …… 167
5.1 关键术语 …… 167
5.2 Cisco 安全访问控制服务器产品概述 …… 167
5.2.1 验证和用户数据库 …… 169
5.2.2 Cisco 安全 ACS 用户数据库 …… 169
5.2.3 保持数据库稳定 …… 170
5.2.4 基于 Windows 的 Cisco 安全 ACS 体系架构 …… 171
5.2.5 Cisco 安全 ACS 如何验证用户 …… 172
5.2.6 用户可更改的口令 …… 174
5.3 使用 Cisco 安全 ACS 配置 TACACS+和 RADIUS …… 175
5.3.1 安装步骤 …… 175
5.3.2 管理基于 Windows 的 Cisco 安全 ACS …… 176
5.3.3 排错 …… 177
5.3.4 启用 TACACS+ …… 178
5.4 检验 TACACS+ …… 180
5.4.1 失败 …… 180
5.4.2 通过 …… 181
5.5 配置 RADIUS …… 183
5.6 总结 …… 183
5.7 检查你的理解 …… 184
第 6 章 在三层配置信任和身份 …… 186
6.1 关键术语 …… 186
6.2 Cisco IOS 防火墙认证代理 …… 186
6.2.1 认证代理的运行 …… 186
6.2.2 支持的 AAA 服务器 …… 187
6.2.3 AAA 服务器配置 …… 188
6.2.4 AAA 配置 …… 188
6.2.5 允许 AAA 流量到路由器 …… 190
6.2.6 认证代理配置 …… 191
6.2.7 测试和验证认证代理 …… 192
6.3 介绍 PIX 安全器件 AAA 特性 …… 193
6.3.1 PIX 安全器件认证 …… 193
6.3.2 PIX 安全器件授权 …… 194
6.3.3 PIX 安全器件计费 …… 195
6.3.4 AAA 服务器支持 …… 195
6.4 在 PIX 安全器件上配置 AAA …… 196
6.4.1 PIX 安全器件访问认证 …… 196
6.4.2 交互式用户认证 …… 196
6.4.3 本地用户数据库 …… 198
6.4.4 认证提示和超时 …… 199
6.4.5 直通代理认证 …… 200
6.4.6 认证非 Telnet、FTP、HTTP 或 HTTPS 流量 …… 201
6.4.7 隧道用户认证 …… 203
6.4.8 授权配置 …… 204
6.4.9 可下载的 ACL …… 205
6.4.10 计费配置 …… 207
6.4.11 控制台会话计费 …… 208
6.4.12 命令计费 …… 209
6.4.13 AAA 配置故障处理 …… 209
6.5 总结 …… 212
6.6 检查你的理解 …… 212
第 7 章 在二层配置信任和身份 …… 214
7.1 关键术语 …… 214
7.2 基于身份的网络服务（IBNS） …… 214
7.2.1 特点及好处 …… 214
7.2.2 IEEE 802.1x …… 215
7.2.3 选择正确的 EAP …… 219
7.2.4 Cisco LEAP …… 220
7.2.5 IBNS 和 Cisco 安全 ACS …… 221
7.2.6 部署 ACS 的考虑 …… 223
7.2.7 Cisco 安全 ACS RADIUS 配置 …… 224
7.3 配置 802.1x 基于端口的认证 …… 225
7.3.1 使能 802.1x 认证 …… 227

7.3.2 配置交换机到 RADIUS 服务器的通信 …… 227
7.3.3 使能周期性重认证 …… 228
7.3.4 手工重认证连接到端口的客户 …… 229
7.3.5 使能多主机 …… 229
7.3.6 将 802.1x 配置重设为默认值 …… 229
7.3.7 查看 802.1x 统计信息和状态 …… 229
7.4 总结 …… 230
7.5 检查你的理解 …… 230
第 8 章 在路由器上配置过滤 …… 232
8.1 关键术语 …… 232
8.2 过滤和访问列表 …… 232
8.2.1 数据包过滤 …… 233
8.2.2 状态过滤 …… 233
8.2.3 URL 过滤 …… 235
8.3 Cisco IOS 防火墙基于上下文的访问控制 …… 235
8.3.1 CBAC 数据包 …… 236
8.3.2 Cisco IOS ACL …… 236
8.3.3 CBAC 如何运行 …… 236
8.3.4 CBAC 所支持的协议 …… 238
8.4 配置 Cisco IOS 防火墙基于上下文的访问控制 …… 239
8.4.1 CBAC 配置任务 …… 239
8.4.2 准备 CBAC …… 239
8.4.3 设置审计跟踪和警告 …… 240
8.4.4 设置全局超时时间 …… 241
8.4.5 设置全局阈值 …… 242
8.4.6 主机限制的半开连接 …… 243
8.4.7 系统定义的端口与应用映射 …… 243
8.4.8 用户定义的 PAM …… 244
8.4.9 设定应用的检测规则 …… 245
8.4.10 为 IP 分片定义检测规则 … 246
8.4.11 定义 ICMP 检测规则 …… 247
8.4.12 将检测规则和 ACL 应用于接口 …… 248
8.5 测试与校验 CBAC …… 251
用 SDM 配置 Cisco IOS 防火墙 …… 252
8.6 总结 …… 253
8.7 检查你的理解 …… 253
第 9 章 在 PIX 安全器件上配置过滤 …… 256
9.1 关键术语 …… 256
9.2 配置 ACL 和内容过滤 …… 256
9.2.1 PIX 安全器件 ACL …… 257
9.2.2 配置 ACL …… 258
9.2.3 ACL 行号 …… 259
9.2.4 icmp 命令 …… 259
9.2.5 nat 0 ACL …… 260
9.2.6 Turbo ACL …… 262
9.2.7 使用 ACL …… 262
9.2.8 恶意代码过滤 …… 265
9.2.9 URL 过滤 …… 266
9.3 对象分组 …… 268
9.3.1 开始使用对象分组 …… 269
9.3.2 配置对象分组 …… 269
9.3.3 嵌套对象分组 …… 271
9.3.4 管理对象分组 …… 274
9.4 配置安全器件模块策略 …… 275
9.4.1 配置一个类映射 …… 277
9.4.2 配置一个策略映射 …… 277
9.4.3 配置一个服务策略 …… 279
9.5 配置高级协议检查 …… 280
9.5.1 默认流量检查和端口号 …… 280
9.5.2 FTP 检查 …… 283
9.5.3 FTP 深度报文检查 …… 285
9.5.4 HTTP 检查 …… 286
9.5.5 协议应用程序检查 …… 287
9.5.6 多媒体支持 …… 291
9.5.7 实时流协议（Real-Time Streaming Protocol，RSTP） …… 291
9.5.8 支持 IP 电话所需要的协议 …… 293
9.5.9 DNS 检查 …… 295
9.6 总结 …… 296
9.7 检查你的理解 …… 297
第 10 章 在交换机上配置过滤 …… 299
10.1 关键术语 …… 299
10.2 二层攻击简介 …… 299
10.3 MAC 地址、ARP 和 DHCP 攻击 …… 300
10.3.1 减少 CAM 表过载攻击 …… 301
10.3.2 MAC 欺骗：中间人攻击 …… 302

10.3.3 ARP 欺骗 …… 303
10.4 DHCP 侦听（DHCP Snooping）· 303
10.4.1 动态 ARP 检测 …… 305
10.4.2 DHCP 耗尽攻击（DHCP Starvation Attacks） …… 305
10.5 VLAN 攻击 …… 306
10.5.1 VLAN 跳跃攻击 …… 306
10.5.2 私用 VLAN 攻击 …… 308
10.5.3 私用 VLAN 防御 …… 308
10.6 生成树协议攻击 …… 309
10.7 总结 …… 310
10.8 检查你的理解 …… 310

第 二 学 期

第 1 章 入侵检测和防御技术 …… 314
1.1 关键术语 …… 314
1.2 入侵检测和防御介绍 …… 314
1.2.1 基于网络与基于主机 …… 315
1.2.2 警报的类型 …… 315
1.3 检测引擎 …… 317
1.3.1 基于签名的探测 …… 317
1.3.2 签名的类型 …… 317
1.3.3 基于异常状态检测 …… 318
1.4 Cisco 的 IDS 和 IPS 设备 …… 319
1.4.1 Cisco 集成的解决方案 …… 319
1.4.2 Cisco IPS 4200 系列探测器 …… 320
1.5 总结 …… 320
1.6 检查你的理解 …… 321
第 2 章 配置网络入侵检测和入侵防护 …… 322
2.1 关键术语 …… 322
2.2 Cisco IOS 入侵防护系统（IPS） … 322
2.2.1 Cisco IOS 入侵防护系统的起源 …… 324
2.2.2 路由器的性能 …… 324
2.2.3 Cisco IOS 入侵防护系统特征库 …… 324
2.2.4 配置 Cisco IOS 入侵防护系统的过程 …… 325
2.3 在 PIX 安全设备上启用攻击防护功能（attack guards） …… 329
2.3.1 Mail Guard …… 329
2.3.2 DNS Guard …… 329
2.3.3 FragGuard 和虚拟重组（Virtual Reassembly） …… 330
2.3.4 AAA 泛洪防护 …… 331
2.3.5 SYN 泛洪保护 …… 332
2.3.6 TCP intercept …… 332
2.3.7 SYN Cookies …… 333
2.3.8 连接限制 …… 333
2.4 在 PIX 安全设备上配置入侵防护 … 334
2.4.1 入侵检测和 PIX 安全设备 … 334
2.4.2 配置入侵防护 …… 335
2.4.3 配置 IDS 策略 …… 336
2.5 在 PIX 安全设备上配置阻断（shunning） …… 337
2.6 总结 …… 338
2.7 检查你的理解 …… 339
第 3 章 加密与 VPN 技术 …… 341
3.1 关键术语 …… 341
3.2 加密的基本方法 …… 341
3.2.1 对称加密 …… 341
3.2.2 不对称加密 …… 342
3.2.3 Diffie-Hellman …… 343
3.3 完整性要素 …… 344
3.3.1 散列 …… 345
3.3.2 散列方法认证码 HMAC … 345
3.3.3 数字签名和证书 …… 346
3.4 实现数字证书 …… 348
3.4.1 认证中心支持 …… 348
3.4.2 简单证书注册协议 SCEP … 349
3.4.3 CA 服务器 …… 349
3.4.4 使用 CA 注册一台设备 …… 352
3.5 VPN 拓扑 …… 352
3.5.1 站点到站点 VPN …… 353
3.5.2 远程访问 VPN …… 353
3.6 VPN 技术 …… 354
3.6.1 WebVPN …… 355
3.6.2 隧道协议 …… 356
3.6.3 隧道接口 …… 358
3.6.4 IPSec …… 358
3.6.5 认证头 AH …… 359