CISCO SYSTEMS

CISCO NETWORKING ACADEMY PROGRAM

ciscopress.com

思科网络技术学院教程
网络安全基础
实验手册与练习册

Cisco Networking Academy Program

Fundamentals of Network Security

Lab Companion and Workbook

The only authorized Lab Companion and Workbook
for the Cisco Networking Academy Program

[美] Cisco Systems 公司
Cisco Networking Academy Program 著
韩东儒 包光磊 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 实验手册与练习册

[美] Cisco Systems 公司
Cisco Networking Academy Program 著

韩东儒 包光磊 译

人民邮电出版社

图书在版编目（CIP）数据

网络安全基础实验手册与练习册 / 美国思科公司，美国思科网络技术学院著；韩东儒，包光磊译. —北京：人民邮电出版社，2005.1
思科网络技术学院教程
ISBN 7-115-12729-8

Ⅰ. 网.... Ⅱ. ①美... ②美... ③韩... ④包... Ⅲ. 计算机网络—安全技术
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 121284 号

版 权 声 明

思科网络技术学院教程
网络安全基础 实验手册与练习册

◆ 著 [美] Cisco Systems 公司
Cisco Networking Academy Program
译 韩东儒 包光磊
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
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：23
字数：563 千字 2005 年 1 月第 1 版
印数：1-4 000 册 2005 年 1 月北京第 1 次印刷

著作权合同登记 图字：01 - 2003 - 4802 号
ISBN 7-115-12729-8/TP • 4281

定价：35.00 元

本书如有印装质量问题，请与本社联系 电话：（010）67129223

内 容 提 要

本书为《思科网络技术学院教程 网络安全基础》教程配套的实验手册，是对该课程的课堂教学和实验课程的补充。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 防火墙管理所设计的实验。

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 安全考试的读者也会有较大的帮助。

序

纵观世界，Internet 已给全球许许多多的人和他们的雇主带来了新的巨大商机。许多公司和组织在强化网络性能上的投资已经带来了生产力的大幅度提高。一些研究表明在整个经济体系中，生产力都有大幅度的提高。提高效率、增加利润和改善生活水平的愿望已经成为现实，而且还在不断发展之中。

这种生产力的提高不是简单地通过购买网络设备就可以实现的。它需要有专门的人才去规划、设计、安装、调度配置、操作、维护，并为网络排除故障。网络管理人员必须确保他们规划的网络是安全的并能持续稳定地工作。他们需要根据组织对设计功能的要求、组织对网络的依赖程度和组织的发展来部署新的网络功能。

为了满足互连网络社区的众多教育需求，Cisco Systems 公司创立了思科网络技术学院项目。思科网络技术学院是一个综合性的学习项目，它向学生提供了全球经济环境中所必需的关于 Internet 的基本技能。思科网络技术学院将面对面的教学、基于 Web 的课程内容、在线测试、学生成绩跟踪、动手实验、教师培训与支持，以及备考行业标准认证融为一体。

思科网络技术学院不断地增强教与学之间的融合。所有教师都是 CCAI（Cisco 认可的指导教师）基于 Internet 的评估和教师支持系统就是其中最大、最有效的部分，它包括每周 7 天、每天 24 小时的面向思科网络技术学院教师的服务系统。通过在线评估和反馈系统向学生提示尚需继续学习的内容，思科网络技术学院帮助学生以螺旋式的方式对课程进行学习。为网络技术学院设计的思科全球学习网络（Cisco Global Learning Network）基础设施向世界范围内的学生提供丰富的、交互式的、个性化的课程。Internet 的强大力量改变了人们工作、生活、娱乐和学习的方式，思科网络技术学院项目则是这场变革的先锋。

由 Cisco Press 出版的这本书是畅销的思科网络技术学院项目配套教程之一。这些书籍由思科全球教育事业部（Cisco Worldwide Education）和 Cisco Press 共同策划，它们为思科网络技术学院的在线学习内容提供了综合的支撑 。Cisco Press 出版的这些书籍是思科系统公司针对思科网络技术学院唯一的授权图本，包含纸介和光盘，它们确保思科网络技术学院的学生能获得最大的学习收益。

我希望你们能成功，Cisco Systems 公司和 Internet 将伴随着你们的学习历程。我同时希望在完成思科网络技术学院的课程后，你们会选择继续不断的学习。除了出版思科网络技术学院的书籍外，Cisco Press 还出版了大量的网络技术和认证书籍，它们提供了丰富的资源。思科系统公司还建立一个由多家专业培训公司构成的网络——思科培训合作伙伴（ Cisco Learning Partners）——他们提供了全套的思科培训课程。他们提供了多种培训方式，包括电子学习、自主学习及教师指导学习。他们的教师是思科认证的，教材也是由思科公司提供的。当你准备学习时，请访问思科网站（Cisco.com ）的“Learning&Event”部分，以了解思科公司及其培训合作伙伴的全部教育支持。

感谢您选择了这本书，同时也感谢您选择思科网络技术学院项目！

Kevin Warner
Cisco Systems 公司
全球教育事业部高级总监

前　言

本书是对思科网络技术学院项目课堂教学和实验课程的补充，掌握这些内容可以帮助你在计算机网络领域从容应聘或接受更高级的教育和培训。

如果你在你已经使用了思科网络技术学院项目的在线学习资料，并且学习了一些与 Cisco IOS 网络安全（SECUR）和 Cisco 安全高级 PIX 防火墙（CSFPA）认证考试相关的主题，本书可以帮助使你得到进一步的培训。以上两门考试是思科认证安全专家（CCSP）认证中的一部分。本书遵循了思科系统公司应用在教程中的样式和风格。

本书包含那些基于目前思科网络技术学院项目的实验，还有一些附加资料。大部分的实验是动手练习，需要访问到一个有 Cisco 路由器的实验或模拟器。附加的纸上实验被包含来作为在线教程的补充，它们是对于复杂主题的实践练习。

本书的读者

本书是为任何想学习网络安全和综合安全过程的读者所写的。本书主要的目标读者是高级中学、大专和大学的学生。特别需要指出的是，在教学环境里，本书既可以用在教室里作为一本教科书手册，也可以用在计算机实验室里作为一本实验手册。

本书是如何组织的

表 I-1 概述了本书中所有的实验，包含在线课程中的目标指示器（TI），难度级别（1 到 3，这里 3 是最难的），还有用来完成这次实验所需的时间。

表 I-1　　主要的实验概览

实验号 (TI)	标　题	难　度 （1-3，这里 3 是最难的）	估计时间 （分钟）
1.1.5	面向学生的实验	1	15
1.2.8	缺陷和漏洞攻击	1	20
1.3.3	设计一个安全计划	2	30
2.1.6	配置常规路由器安全	1	15
2.2.1	控制 TCP/IP 服务	1	15
2.3.2	配置 NAT/PAT	2	15
2.4.2	配置日志记录	1	15
2.4.3	设置时间和网络时间协议	2	15

续表

实验号 (TI)	标　题	难　度 （1-3，这里 3 是最难的）	估计时间 （分钟）
2.4.5	配置 SSH	2	20
3.2.4	标准的、扩展的、命名的和注释的访问控制列表	3	30
3.2.5	Lock-and-Key 访问控制列表	3	30
3.2.7	基于时间的访问控制列表	2	20
3.8.3	在 Cisco 路由器上配置 Cisco IOS 防火墙 CBAC	3	35
4.2.3	在 Cisco 路由器上配置 AAA	2	20
4.3.1	安装和配置 Windows 版本 的 CSACS 3.0	2	30
4.5.2	配置验证代理	2	30
5.2.5	配置 IOS 防火墙 IDS	2	15
5.3.8	配置 Syslog	3	30
5.4.5	配置 SNMP	2	15
6.4.5	使用预共享密钥配置 Cisco IOS IPSec	2	30
6.6.6	使用数字证书配置 IPSec	2	30
7.3.6	使用 Cisco Easy VPN 配置远程访问	2	20
8.3.3	配置 PIX 防火墙	2	25
8.5.3	配置 PIX 防火墙作为一台 DHCP 服务器	1	15
9.6.3.1	配置穿透 PIX 安全防火墙的访问	2	25
9.6.3.2	配置多重接口	3	25
10.1.2	在 PIX 防火墙上配置 ACL	3	40
10.4.4	配置对象群组	2	35
11.3.5	使用 Windows 2000 CSACS 配置在 PIX 安全防火墙上的 AAA	3	40
12.1.7	在 Cisco PIX 防火墙上配置并测试高级协议处理	2	20
12.4.3	配置入侵检测	2	30
13.3.3	配置基于局域网的故障切换（可选）	2	30
13.5.3	配置 SSH、命令授权和本地用户身份验证	2	25
13.6.2	执行密码恢复	2	20
14.6.6	在两台 Cisco 安全 PIX 安全防火墙间使用 IPSec 配置一个安全的 VPN 网关	3	45
14.7.5	在 PIX 和 VPN 客户端之间使用 IPSec 配置一个安全的 VPN	2	30
14.8.2	在两台 PIX 防火墙间配置具有 CA 支持的 IPSec	2	30
15.6.3	通过 PDM 配置 PIX 防火墙	3	45

本书的特点

许多本书中的特色有助于更容易全面地理解书中包含的网络和路由选择知识。

- **词汇练习**——本书每一章开始的部分。在此部分中，学生将复习一些本章所涉及的技术相关术语，并提供它们的定义。
- **实验**——在手册中的每个实验都提供实验目标或实验目的。实验列举出所需的设备，

并提供一个可以使你将实验与现实情况相联系的场景。每个实验同时也提供一些辅助资源（基于 Web 和与文本印刷的）给学生参考，以加强他们对实验概念的理解。另外，每个实验还提供在实验中使用的关键命令列表。

- **复习问题与测验**——为了检验对所涉及概念的理解情况，每一章以需要简单回答的复习问题和抽选出特定知识点的多项选择题作为结束部分。这些问题有助于验证你对章节中所实现技术的理解程度。

本书中采用的命令语法表示习惯与 Cisco IOS 命令参考中的习惯相同：

- 命令和关键字用粗体字表示。在配置实例中（不是一般的命令语法），**粗体字**表示命令需要用户手工输入（例如 show 命令）。
- *斜体字*表示用户需要提供具体值的参数。
- 大括号（{ }）表示一个必需的组成元素。
- 中括号（[ ]）表示一个可选的组成元素。
- 竖号（|）用于分开互斥的选项。
- 在中括号内的大括号和竖号（例如[x { y | z }]）表示在一个可选组成元素之内的必需元素。你不一定要输入中括号中的内容，但是如果你输入了，你必须输入大括号中的必需选项。

目　录

第1章　网络安全概览

随着在不同操作系统中越来越多的安全缺陷被发现和攻击，管理员保护网络就势在必行了。掌握了最新的系统缺陷同时了解网络的弱点，系统管理员将在保护网络和公司资产方面处于一个更为有利的位置。针对管理员的一些相当好的在线资源包括：思科公司网站的安全目录（http://www.cisco.com/security/）和 CERT 的协调中心网站（http://www.cert.org）。

因为对于多数读者来说，网络安全是一个全新的概念，因此本章将向你介绍一些新的概念和术语，并讨论网络安全的需求，同时还将讨论保护网络的目标和关键元素。

你将学习现有不同的缺陷和威胁，还有做什么能够保护你的网络。使用一些攻击者同样使用的工具，你能确定存在什么样的弱点，然后去纠正这些弱点。通过了解所需寻找的内容，你能确定哪些需要修复以及如何修复。

通过设计一个符合公司需要的安全构架，然后将该策略应用到网络，你就有可能消除对网络的大部分攻击。

单词练习

机密性（confidentiality）

完整性（integrity）

身份验证（authentication）

可用性（availability）

侦察（reconnaissance）

包嗅探器（packet sniffer）

拒绝服务（DoS）

分布式拒绝服务（DDoS）

死亡之 Ping（Ping of death）

smurf 攻击（smurf attack）

安全策略（security policy）

防火墙（firewall）

入侵检测（intrusion detection）

入侵检测系统（IDS）

实验 1.1.5：面向学生的实验

估计时间：15 分钟

小组成员的数目：两个小组，每组 4 名学生

目标

在本次实验中，学生将实现下列目标：

- 审核实验的捆绑设备。
- 理解安全的 Pod 拓扑。
- 理解 Pod 命名与寻址方案。
- 加载 IOS 防火墙映像。
- 加载默认的实验配置。
- 用线缆连接标准的实验拓扑。
- 测试连通性。

概览

本章描述了为本课程而用线缆连接和配置标准实验拓扑的基础。学生会熟悉贯穿整个课程使用的物理的和逻辑拓扑。为了避免实验练习的问题，在配置安全以前，正确的实验设置和连接是必要的。在真实世界的场景中，在进行更高级的配置以前检查网络是否正常工作是很重要的。

在本次课程中会用到 4 个基本的实验拓扑。

图 1-1 描述了使用 IOS 防火墙路由器的实验网络环境，对应第 1 章到第 6 章。

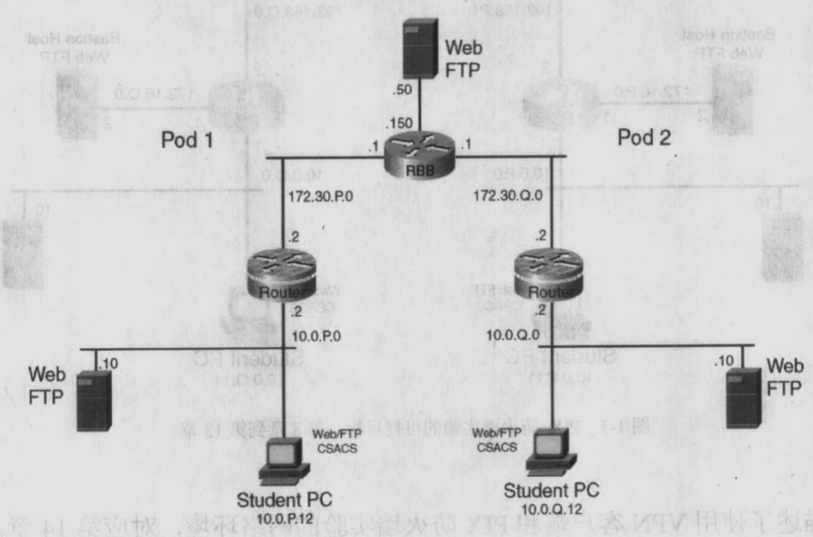

图 1-1　IOS 防火墙实验的可视目标：第 1 章到第 6 章

图 1-2 描述了使用 VPN 客户端和 IOS 防火墙的实验网络环境，对应第 7 章。

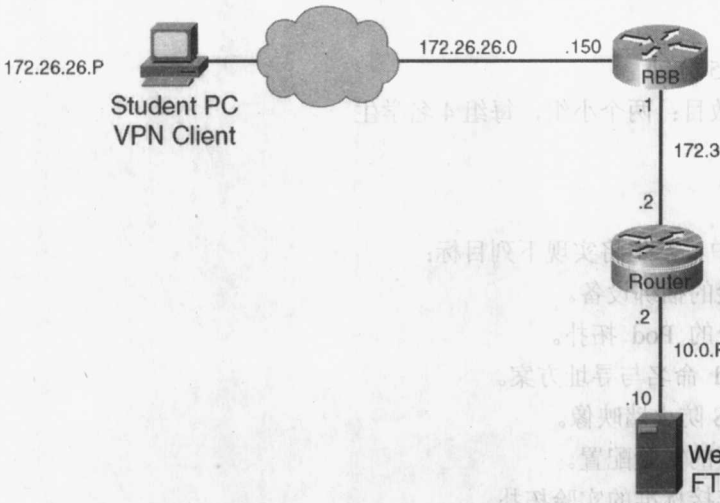

图 1-2 VPN 客户端到 IOS 防火墙实验的可视目标：第 7 章

图 1-3 描述了使用 PIX 防火墙的实验网络环境，对应第 8 章到第 13 章。

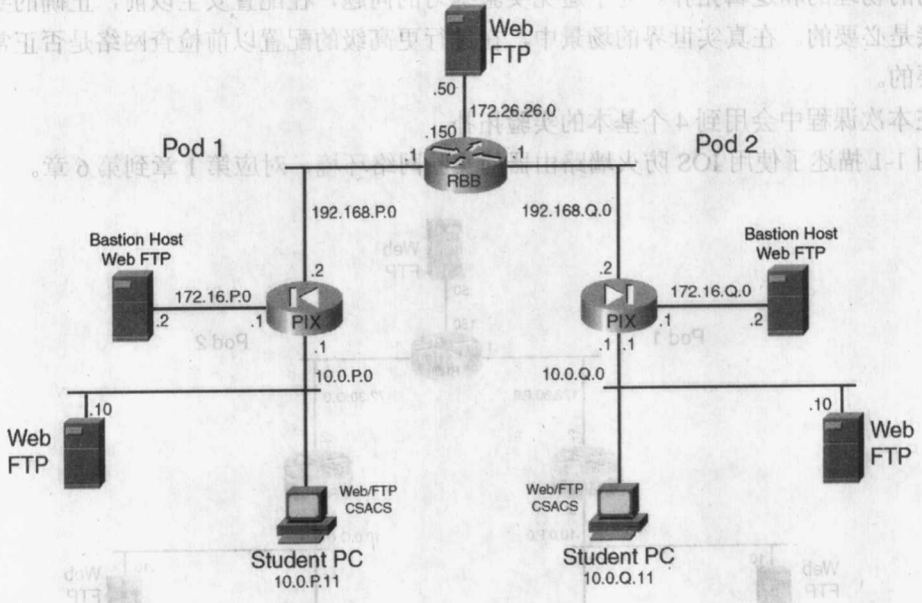

图 1-3 PIX 防火墙实验的可视目标：第 8 章到第 13 章

图 1-4 描述了使用 VPN 客户端和 PIX 防火墙实验的网络环境，对应第 14 章。

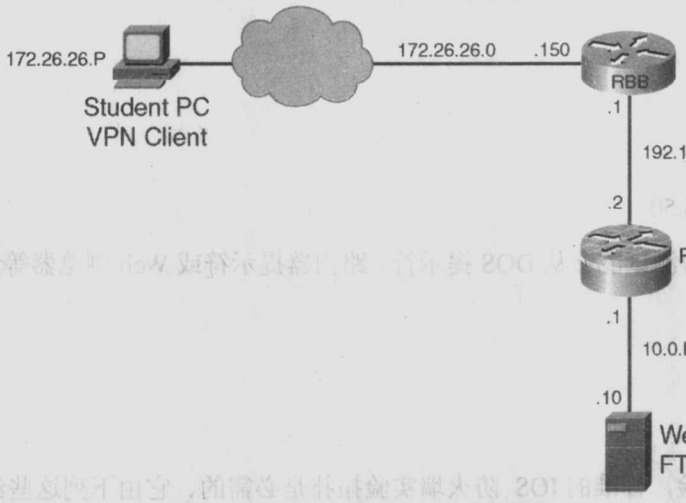

图 1-4　VPN 客户端到 PIX 防火墙实验的可视目标：第 14 章

如表 1-1 所列的，每个拓扑都存在 3 个基本设置。

表 1–1　　实验拓扑设置

名字	信任级别	共同点	网络	物理端口
内部	信任	私有	LAN	Ethernet/FE/GE
外部	不信任	公共	WAN（Internet）	Ethernet/Serial
非军事区	受保护	伙伴网	LAN	Ethernet/FE/GE

在大部分实验中，物理接口没有明确规定为 Ethernet0、Fa0/0、E0/0 等等。取而代之，一个实验会指导学生去配置外部接口、内部接口或 DMZ 接口。学生必须根据路由器模块和接口特征去配置接口。

注意两个拓扑图都指出一种特殊的编号方式、命名和寻址方案。基本的实验拓扑包括两个 Pod。每个 Pod 包含一台路由器、一个防火墙、一台学生用 PC 和一个内部服务器。在寻址与命名方案中的 **P** 值参照那个分配给包含 1～4 名学生小组的 Pod 路由器。

在命名与寻址方案中的 **Q** 值会在测试安全或者与对端小组的连通性时使用。例如，假定要求使用 Pod 1 路由器的小组 ping 邻接路由器 172.30.**Q**.2，在这种情况下，**Q** 值被代替为 2。

在大多数实验里的基本任务如下：

- 在 Pod 设备上配置安全，例如一个路由器或防火墙。
- 在 Pod 设备上测试安全。
- 在对端小组的设备上测试安全性。
- 测试穿过 Pod 设备和穿过对端设备的 LAN 和 WAN 服务。

当测试连通性和安全配置时，请注意观察提示符。一些可能的提示符如下：

- C:\
- Router>
- http://10.0.P.12
- ftp://172.26.26.50

这是重要的，因为测试能够从 DOS 提示符、路由器提示符或 Web 浏览器等地方被执行。

工具和资源

为了完成本次实验，标准的 IOS 防火墙实验拓扑是必需的、它由下列这些组成：

- 两个 Pod 路由器。
- 两个 Pod 防火墙。
- 两台学生用 PC。
- 一台带有 Intel Pro Server 的服务器和一块支持 VLAN 的网卡。
- 骨干交换机和路由器。
- 两根 console 线和超级终端（HyperTerminal）。
- 匹配 Cat5 的接插线。
- （可选）带有标识的主机。

命令列表

本次实验使用表 1-2 中列出的命令。

表 1-2　　实验 1-1 的命令

命令	描述
copy run start	保存当前 RAM 里的配置到 NVRAM 中
copy tftp flash	从 TFTP 服务器下载一个新的映像到 Flash 存储器
copy tftp start	从 TFTP 服务器下载一个配置到 NVRAM 中
enable	打开特权命令
show interface	显示配置路由器上所有接口的统计信息

续表

命令	描述
show ip interface	显示与一个接口有关的状态和全局参数
show ip route	显示 IP 路由选择表的内容
show running-config	显示 RAM 中的当前配置
show startup-config	显示已保存的配置，也就是 NVRAM 的内容
show version	显示系统硬件的配置、软件版本、配置文件的名称和来源、以及引导映像

任务 1：检查设备

步骤 1. 从物理方面检查每个设备。注意在 IOS 路由器和 PIX 防火墙上可用接口的有效性。

步骤 2. 注意有些设备被一个粘性标记所标注。表 1-3 提供了需要被标注的设备的列表。

表 1-3　　标注的设备

路由器	PIX 防火墙	学生 PC	骨干设备
Router1	pix1	PC1	RBB（骨干路由器）
Router2	pix2	PC2	SW0（骨干交换机）
			SS（超级服务器）

这些设备创建了两个标准的 Pod。每个 Pod 可适用于包含 1～4 名学生的小组。

任务 2：检验 Pod 路由器上的 IOS 防火墙映像

步骤 1. 打开电源，测试路由器。如果 IOS 映像需要升级，可从 Cisco.com 下载 IOS 软件。下载仅对注册用户有效。

平台	版本	软件特征
2610XM-2611XM	12.2.8T5	IP/FW/IDS Plus IPSec 56（or 3DES）