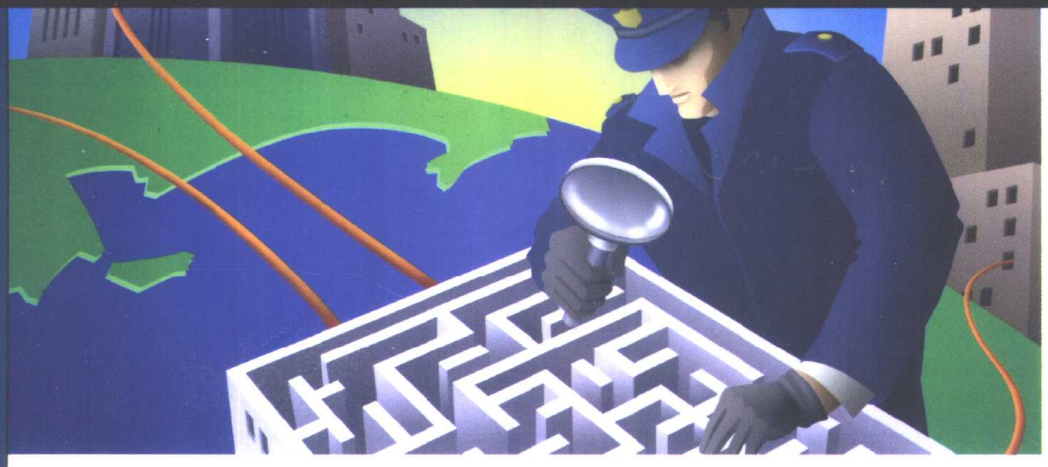
Cisco Systems
Cisco Press
Cisco职业认证培训系列
CISCO CAREER CERTIFICATIONS

CQS



Cisco 安全 PIX 防火墙

Cisco Secure PIX Firewalls

Reduce the threat of network attacks with the official CSPFA Coursebook

〔美〕David W. Chapman Jr.
Andy Fox 著
刘兴初 李逢天 译
李逢天 审校

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

Cisco 职业认证培训系列

Cisco 安全 PIX 防火墙

[美] David W. Chapman Jr. Andy Fox 著

刘兴初 李逢天 译

李逢天 审校

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

Cisco 安全 PIX 防火墙/（美）查普曼（Chapman, D. W.），（美）福克斯（Fox, J. A.）著；刘兴初，李逢天译. —北京：人民邮电出版社，2002.8

ISBN 7-115-10388-7

Ⅰ. C… Ⅱ. ①查…②福…③刘…④李… Ⅲ. 计算机网络—防火墙 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2002）第 043130 号

版权声明

Cisco 职业认证培训系列

Cisco 安全 PIX 防火墙

◆ 著 [美] David W. Chapman Jr. Andy Fox

译 刘兴初 李逢天

审 校 李逢天

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 315@ptpress.com.cn

网址 http://www.ptpress.com.cn

读者热线 010-67180876

北京汉魂图文设计有限公司制作

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：19

字数：454 千字 2002 年 8 月第 1 版

印数：1-4 000 册 2002 年 8 月北京第 1 次印刷

著作权合同登记 图字：01-2002-0395 号

ISBN 7-115-10388-7/TP・2939

定价：40.00 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

本书详细介绍了配置、验证并管理 PIX 防火墙产品系列的相关知识，内容包括黑客的常见攻击手段，网络内部和外部的安全威胁；不同型号 PIX 防火墙的特点，升级所需要完成的任务；基本的安装细节，以及如何启用更高级的特性和访问控制；采用 PIX 系统日志服务和 PIX AAA 子系统的管理和监测；配置 PIX 故障切换机制，PIX 上的 IPSec，以及 Cisco IOS 防火墙特性集。附录提供了一些很有帮助的参考，包括配置 PIX 入侵检测特性、SNMP 管理支持、DHCP 客户端和服务器、安全 Shell 协议（SSH）连接，以及许多与安全相关的资源。

本书适合那些准备参加 Cisco Security Specialist 1 认证考试的人员。本书还适合那些想理解并更有效地使用 PIX 防火墙的网络管理人员。

关于作者

David W. Chapman Jr.，CCSI，CCNP，CCDP，CSS-1，是 Global Knowledge 公司的 Cisco 安全讲师。David 是“Cisco 安全 PIX 防火墙”课程的主管，他负责保证课程的完整性和质量，并向刚接触这门课程的讲师提供指导。自从 1994 年，David 就开始在企业网络中使用 Cisco 公司的产品。在来到 Global Knowledge 公司之前，他在波特兰的一家 Cisco 金牌认证伙伴公司工作，去年他在那里帮助 Cisco 的 SmartStart Customers 计划建立原型、测试并建立安全的电子商务基础平台。最近，David 已经通过了 CCIE 安全资格考试，正准备参加实验室考试。

Andy Fox，CCSI，CCNA，CCDA，CSS-1，是 Global Knowledge 公司的一名 CCSI(认证 Cisco 认证的讲师)。Andy 已经讲授了 5 年多的 Cisco 认证课程，目前是“管理 Cisco 网络安全（MCNS）”课程的主管。Andy 在 1980 年从 Purdue 大学毕业后，从事了计算机科学方面的职业，在空军担任计算机操作员。Andy 在他的 5 年军旅生涯中从事过不同的工作。其中一个工作是在德国的 Ramstein 空军基地的 BBN C70 MINET 主机的系统管理员。那份工作帮助他得到了下一份工作：在 Massachusetts Cambridge 的 Bolt Beranck 和 Newman 的网络运行控制员。在网络运行中心工作期间，Andy 帮助维护许多广域网络，包括 ARPANET、MILNET 和 MINET。他随后的工作是在 New York City 的 TYMNET（英国电信）的系统工程师和在 Pennsylvania Collegeville 的 RPR 药厂的系统工程师，在这些工作之后，他于 1996 年成为了一名讲师。

关于技术审稿人

Randy Ivener 是 Cisco 公司的高级工程服务组的安全和 VPN 专家。他是一名 CCNP、Cisco 安全专家-1（CSS-1）和 ASQ 认证的软件质量工程师。作为一名网络安全顾问，他用了几年的时间，帮助公司理解并保护他们的网络安全。他熟悉许多安全产品和技术，包括防火墙、VPN、入侵检测和认证系统。在从事安全工作之前，他将很多时间用于软件开发并担任培训讲师。Randy 毕业于美国海军学院，拥有 MBA 学位。

Doug McKillip，P.E.，CCIE #1851，是一名独立顾问，从事与 Global Knowledge 公司相关的 Cisco 认证培训方面的咨询。他在计算机网络方面超过 13 年的工作经验，在过去的 9 年中，他主要从事安全和防火墙工作。在最初采用 MCNS 第一版培训课程的时候，Doug 提供了许多指导性的和技术性的帮助，他一直是 Global Knowledge 公司（Cisco 公司的培训伙伴）的首席讲师和课程主管。Doug 拥有 MIT 的化学工程学士与硕士学位，Delaware 大学的计算机科学硕士学位。他现在居住在 Delaware Wilmington。

David Ofsevit 是 Cisco 公司的技术市场工程师。现在，他在 Cisco 的企业解决方案工程组工作，侧重于网络设计的安全部分。这个工作得益于他先前从事的销售技术支持的工作经验，当时他也是从事网络安全工作。他是 Cisco 安全领域解决方案设计组的成员，也是安全与 VPN 顾问组的成员。

在 1996 年，Cisco 公司收购了 TGV 软件公司，David 自从那时起就加入了 Cisco 公司。在 TGV 公司工作之前，David 工作过的公司有 DEC 公司、Mitre Corporation 公司和美国运输部。他拥有 MIT 的电子工程 S.B-S.M 组合学位。

Gilles Piche，CCSI，是一名安全顾问，在过去 5 年中，他在加拿大一直工作于网络安全领域。在此之前，他供职于

加拿大政府，从事网络工程工作。Gilles 也是一名 Cisco 认证的安全讲师，在最近的一年半时间里，他为 Global Knowledge Network（加拿大）公司讲授 Cisco 安全课程。

前　言

本书的目的是为了帮助网络工程师深刻理解 PIX 防火墙，以及如何使用防火墙来减轻对他们网络的巨大威胁。读者需要具备基本的 IP 操作和安全概念，这样才能更好地利用本书的内容。对于刚刚接触网络安全和 PIX 防火墙的读者，我们建议先阅读《管理 Cisco 网络安全（MCNS）》（Michael Wenstrom 著，中文版由人民邮电出版社出版）。就像 MCNS 课程是“Cisco 安全 PIX 防火墙”课程的前期必要课程一样，MCNS 一书提供了本书所需的许多基本知识。

不仅网络工程师将从本书中受益，网络设计者也将发现书中的案例学习对于设计安全网络基础结构是非常有价值的。而且，信息系统审计员也将获得所需的知识，以正确评估复杂的配置，判断是否符合保密要求。本书所提供的案例学习将用来对常用的配置进行讨论。

本书的创作动机

本书面向的读者是那些想要更新他们的基本 PIX 操作知识并想钻研高级配置的网络工程师。我们发现在书店里目前还没有其他的书讲述 PIX 的高级特性。

本书目标

本书的目标是将那些具备基本 PIX 知识的读者引领到一个更高的水平，使他们掌握高级 PIX 防火墙技能。通过向读者提供通用的实际案例学习，本书帮助读者在设计并实施他们自己的 PIX 安全方案时，理解各种配置方案的优点和不足。

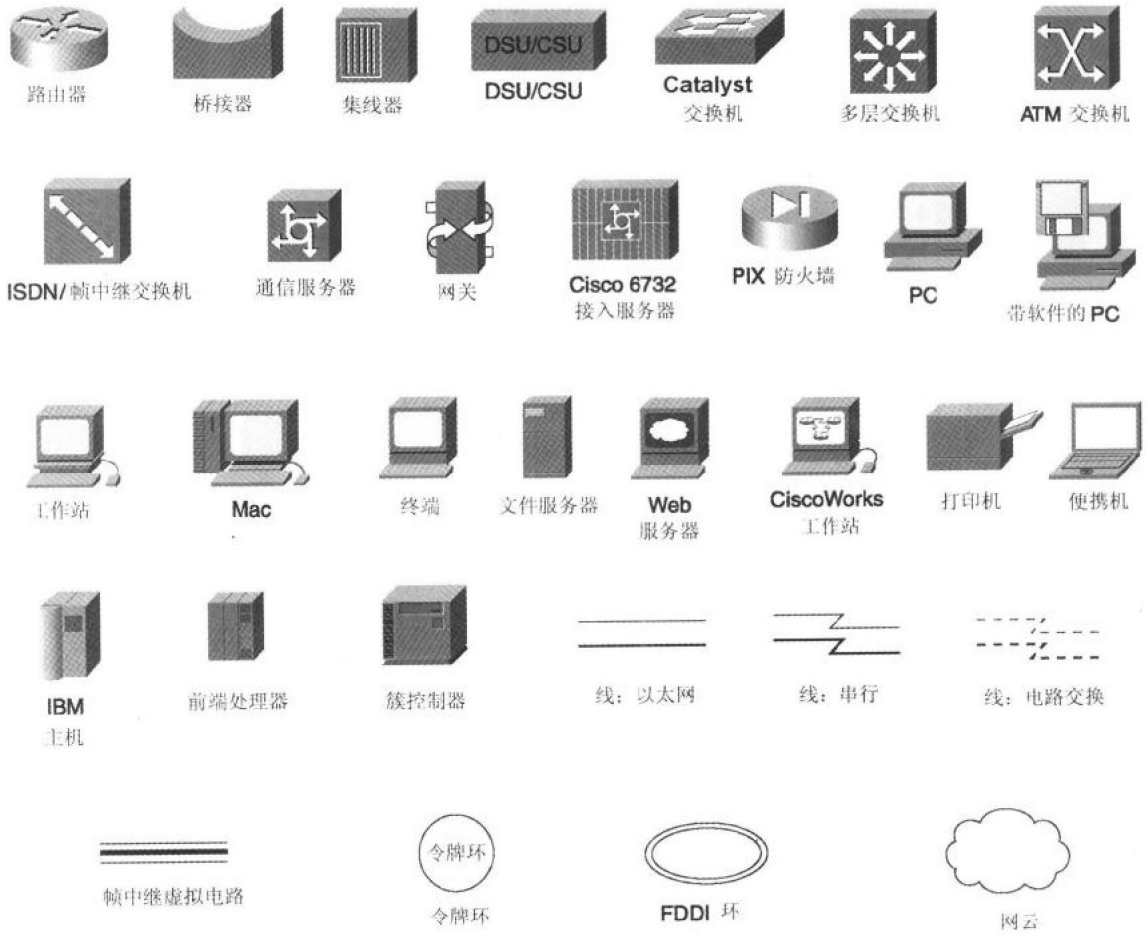
本书所用的表示习惯

本书中采用的命令语法的表示习惯与 Cisco IOS 软件命令参考中的习惯相同。命令参考的表示习惯如下：

- 竖条(|)用于分开互斥的选项。
- 方括号[ ]表示任选的关键字或参数。
- 大括号{ }表示必选项。

- 大括号位于方括号内[{ }]表示任选项中的必选项。
- 命令和关键字用粗体字表示。在配置实例和输出显示中（不是指一般的命令语法），粗体字表示命令需要用户手工输入（例如 **show** 命令）。
- 斜体字表示用户应输入具体值的参数。

本书所用的图标



序

2001 年 1 月，Cisco Systems 公司宣布了一套新的职业认证系列，称为 Cisco 认证专家（Cisco Qualified Specialist，CQS）。最先发布的 CQS 是 Cisco 安全专家 1（Cisco Security Specialist 1，CSS-1）。CSS1 是设计用于认证技术人员的通用网络安全技能和知识，它侧重于入侵检测系统、防火墙和虚拟专用网络。最近，对于合格的网络安全专业人员的需求量越来越大。每天，企业都在进行着一场永无终止的战争：保证他们网络的安全，使他们的网络免受那些蓄意破坏系统或企图获取非授权访问权限的黑客的威胁。对于那些负责确保访问安全并控制网络内部活动的网络安全专业人员来讲，控制防火墙被认为是一项很关键的技能。

《Cisco 安全 PIX 防火墙》采用书本的形式，所讲授的知识与有导师辅导的实验室课程和远程教学的同名课程是一样的。尽管以书本的形式来推广这些知识与参加由 Cisco 教学伙伴提供的 Cisco 认证培训中获得的动手经验不能相提并论，但它是满足全球对 Cisco 培训需求的一个极具价值的构成部分。本书使读者能够描述、配置、验证并管理 PIX 防火墙产品系列以及 Cisco 路由器中的 Cisco IOS 防火墙特性集。CSPFA 教材和 Cisco Press 出版社的其他书籍都具有较高的质量标准，保证了高质量的知识传授。无论读者是为了准备 CSS-1 认证考试，还是对安装、配置并操作 Cisco PIX 防火墙感兴趣，这本书都将增强读者对防火墙的理解。

其他 CSS-1 认证教材包括《管理 Cisco 网络安全》、《Cisco 安全虚拟专用网络》和《Cisco 安全入侵检测系统》。

Rick Stiffler
Cisco Systems 公司
VPN 和安全培训部经理
2001 年 9 月

目　录

原书空白页