21 BEIJING HOPE

21世纪网络工程师设计宝典丛书 9

Cisco PIX Configuration Guide

网络核心技术内幕

Cisco PIX 防火墙配置指南

本书配套光盘内容包括：
与本书配套的电子书

21世纪网络工程师设计宝典丛书编委会 编

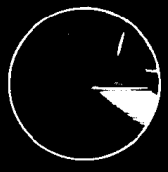
北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

21 BEIJING HOPE

21世纪网络工程师设计宝典丛书 9

Cisco PIX Configuration Guide

网络核心技术内幕



Cisco PIX 防火墙配置指南

本书配套光盘内容包括：
与本书配套的电子书

21世纪网络工程师设计宝典丛书编委会　编

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书是“21 世纪网络工程师设计宝典系列”网络核心技术内幕套书之一。网络安全是当今网络技术领域人们最为关注的焦点之一。美国网络通信巨头 Cisco 公司的 PIX 防火墙是全球著名的网络安全产品之一，该产品的安全系数达到美国国家安全等级 C_2 级（国防级）标准。本书详尽地介绍了在网络上配置和安装 PIX 防火墙、优化网络安全结构，是一本有关网络安全的权威指导书。

全书由 7 章构成，第 1 章总体介绍了 Cisco 防火墙基础知识，第 2~3 章具体介绍了防火墙的通用配置和安装规则，以及各种专用配置原则，第 4~5 章着重介绍了如何配置 IPSec 和相关配置实例，最后两章重点介绍相关命令参考，PIX 515 配置等。

本书是根据实际工程项目操作所需知识编写而成，内容新颖、丰富、实用性和可操作性强，并附有大量的实例。

本书不但是网络规划人员、网络开发人员、网络管理人员和网络维护人员重要的工作指导书，而且也是科研院所、国防部门单位、高等院校师生比较好的自学、教学参考用书。

本书配套光盘内容为与本书配套的电子书。

系　　列　　书：21 世纪网络工程师设计宝典（9）
书　　　　名：网络核心技术内幕——Cisco PIX 防火墙配置指南
文 本 著 作 者：21世纪网络工程师设计宝典丛书编委会　编
责 任 编 辑：王玉玲　陈河南
C D 制 作 者：希望多媒体开发中心
C D 测 试 者：希望多媒体测试部
出版、发行者：北京希望电子出版社
地　　　　址：北京海淀路 82 号，100080
网址: www.bhp.com.cn
E-mail: lwm@hope.com.cn
电话: 010-62562329,62541992,62637101,62637102,62633308,62633309
（发行和技术支持）
010-62613322-215（门市）　010-62531267（编辑部）

经　　　　销：各地新华书店、软件连锁店
排　　　　版：希望图书输出中心
CD 生　产　者：文录激光科技有限公司
文 本 印 刷 者：北京双青印刷厂
开本 / 规格：787×1092　1/16 开本　20.25 印张　460 千字
版次 / 印次：2000 年 4 月第 1 版　2000 年 4 月第 1 次印刷
印　　　　数：0001-5000 册
本　　版　　号：ISBN7-900031-53-7/TP・53
定　　　　价：50.00 元（1CD，含配套书）

21世纪计算机网络工程师设计宝典丛书

编 委 会 名 单

序

21 世纪是网络经济时代，网络与我们同呼吸，网络大潮波涛滚滚、汹涌澎湃，社会生活节奏加快，世界是在知识和经济实力的较量中不断发展，前进的步伐大大加快。据我国有关部门统计，21 世纪我国最缺的人才领域之一是计算机网络工程人员和计算机网络管理人员。为满足社会对计算机网络人才日益高涨的需求，我们特与美国 Cisco 公司、美国耶鲁大学的部分计算机和通信专家共同策划和开发了、为培养 21 世纪网络工程专业人才用的又一套热门书："21 世纪网络工程师宝典丛书"，共计 14 种，书名如下：

1.《网络核心技术内幕—专业 IP 网络规划与设计》

2.《网络核心技术内幕—Cisco 网络安全解决方案》

3.《网络核心技术内幕—组网技术解决方案》

4.《网络核心技术内幕—Cisco Debug 命令参考》

5.《网络核心技术内幕—网络设计教程》

6.《网络核心技术内幕—网络攻击秘笈》

7.《网络核心技术内幕—Cisco Works 使用手册》

8.《网络核心技术内幕—Cisco IP/TV 开发指南》

9.《网络核心技术内幕—Cisco PIX 防火墙配置指南》

10.《网络核心技术内幕—S/390 专用配置指南》

11.《网络核心技术内幕—Cisco IOS 新功能详解》

12.《网络核心技术内幕—网络协议解决方案》

13.《网络核心技术内幕—网络电话开发指南》

14. 《网络核心技术内幕—综合 IP 网络设计解决方案》

每种书由以下主要内容构成。

1.**《网络核心技术内幕—专业 IP 网络规划与设计》**：是美国 Cisco 公司全球网络专家资格认证书的权威培训教材。全书由四部分、九章和五个附录组成。第一部分介绍网络稳定性的基础——网络的分层，讨论了分层规划的原则、地址分配和聚和、各层的冗余和网络规划原则的应用。第二部分介绍了各种先进的内部网关协议，包括 OSPF，IS-IS，EIGRP 网络规划。第三部分介绍网络的扩展，讨论了 BGP 核心层和网络的可扩展性以及其它大规模核心层。第四部分作为本书的附录介绍了 OSPF，IS-IS，EIGRP，BGP 的基础。在介绍基础理论的同时，本书各章后都附有实例学习和复习题，并针对部分疑难问题提出相应的解决方案，附录 E 中有各章复习题的答案。

本书结构清晰，内容丰富，技术新、实用性强，不但是想获取 Cisco 网络专家资格认证的广大科技人员必读的教科书，同时也是从事网络应用设计和开发的广大工程人员、开发人员、网络管理人员的重要参考书，高等院校相关专业师生重要的自学、教学参考用书和社会相关领域培训班教材。

本书配套光盘内容包括：1. 与本书配套电子书；2. 送"计算机基础知识全面速成"多媒体学习软件。

2.**《网络核心技术内幕—网络安全解决方案》**：本书全面介绍了如何针对 Cisco 网络设备配置 Cisco IOS 安全特性。通过 Cisco IOS 安全特性的配置，使我们的网络能够避免有意和无意的攻击，避免由于合法用户的误操作造成的数据丢失或泄露，从而保护网络系统的安全。全书共分六部分：认证、授权及记帐（AAA）、安全服务器协议、流量过滤和防火墙、IP 安全和加密技术、其它安全特性和附录。认证提供了识别用户的方法，它在允许用户访问网络以及网络资源之前确认用户的身份；授权提供了远程访问控制的方法，它包括一次性授权和对每个服务进行授权；记帐提供了收集和发送帐单信息、审计信息以及报告信息的手段。

安全服务器协议部分介绍了配置 RADIUS、Kerberos、TACACS+、TACACS 和扩展 TACACS 的方法、命令和过程。流量过滤和防火墙部分介绍了如何配置网络设备进行流量过滤以及如何把网络设备配置成精细入微的防火墙。IP 安全与加密部分介绍配置 Cisco 加密技术、配置 IPSec、配置证书认证机构（CA）的互操作能力以及配置 Internet 密钥交换的方法。其它安全特性部分介绍了进一步加强网络安全的其它技术与措施。

3.**《网络核心技术内幕—组网技术解决方案》**：随着网络应用的不断深入，企业组网已经成为发展的必然趋势，如何设计企业组网的整套软、硬件解决方案已经成为许多 IT 人员密切关心的问题。本书提供了一套 Cisco 系统公司组网技术切实可行的解决方案。

全书由五部分，15 章构成。第一部分介绍了如何用隧道技术访问 VPN 方案；第二部分介绍了 Cisco 安全 VPN 客户方案指南，讨论了虚拟专用网、Cisco 路由器的相互操作性以及使用预共享密钥、使用数字证书和使用 Internet 密钥交换方式配置的业务案例；第三部分用 37 个例子介绍了侵入探测计划指南；第四部分介绍了如何使用 CiscoSecure 与 Oracle 的分布式数据库特性；第五部分介绍了 Cisco SS7/CCS7 拨号访问方案系统集成指南。

本书结构清晰，事例丰富，技术新，实用性强。本书是企业 IT 人员、专业网络公司技术人员和系统集成人员的宝贵资料，是解决组网方案的重要参考手册，也是大、中专院校介绍网络技术重要的教学、自学参考用书和社会相关领域培训班教材。

4.**《网络核心技术内幕—Cisco Debug 命令参考》**：随着网络应用的不断深入，企业组网已经成为发展的必然趋势。如何设计企业组网的整套软、硬件解决方案已成为许多 IT 人员密切关心的问题。当网络出现故障时，尽快解决问题尤为关键。通过使用 Debug 命令，就可以快速地查找出故障发生的原因和地方，为故障的解决提供依据。

本书详细介绍了 Debug 命令的使用方法，以及命令的使用对路由器将产生的影响。对每种方法都给出了其命令格式、语法说明、使用说明等，并给出了命令的输出实例。用典型范例教读者如何尽快学习和掌握 Cisco Debug 命令的使用是本书最大的特色。

5.**《网络核心技术内幕—网络设计教程》**：本书通过以网络设计概念、网络设计基本分析、设计要点、实际案例设计、巩固思考题的组成形式，使读者能够达到学习和掌握网络设计的效果，同时涵盖了全球著名网络设计师认证考试 CCDA 的所有课题。全书共分为七大部分。第一部分介绍了现代网络技术的发展和基本概念；第二部分提供了中小规模的商务解决方案框架；第三部分介绍了怎样准确地描述现有的网络，怎样确定客户的网络需求；第四部分详细介绍在特定的拓朴结构和互联网络约束条件下，如何设计网络来满足客户对性能、安全、容量和可伸缩性的需求；第五部分描述如何建立和测试网络原型或先导；第六部分提供了一个 CCDA 考试样题；第七部分是一些附录，在附录里提供了大量有用的附加信息，其中包括有四个案例分析，还有各章中问题的参考答案。最后给出了一个英汉对照的术语表。

6.**《网络核心技术内幕—网络攻击秘笈》**：随着 Internet 的飞速发展，尤其是近年来电子商务的快速发展，网络越来越与我们日常生活密不可分。但是，通过网络犯罪而对国家安全、企业安全和个人安全造成的损失日益严重。网络安全性已成为最为关心和棘手的问题。

本书汇聚了当今 400 余种典型网络攻击方法和手段，并对每种攻击手段和方法进行了全面的技术分析并提出了相应的解决措施，为从事网络安全开发和应用的广大科技人员提供了全面而权威的网络安全指南，对创建和维护网站有着十分重要的意义。

7.**《网络核心技术内幕—CiscoWorks 使用手册》**：本书详细地介绍 CiscoWorks 4.0 软件在多种软件平台下的运行和操作方法，全面地介绍利用 CiscoWorks 对 Cisco 网络设备的管理、状态监控和故障诊断技术，并系统地阐述网络安全和用户的管理方法。全书共分八章，主要内容包括：CiscoWorks 的功能和性能以及在多种平台下的应用程序； 利用 CiscoWorks 软件建立网络设备信息库并对其进行管理的方法； 利用

CiscoWorks 软件对网络设备和网络系统进行故障诊断的策略与技术和应用程序的操作方法；利用 CiscoWorks 软件对网络系统进行管理的方法，以便提高系统的运行效率和管理水平；利用 CiscoWorks 软件对 Cisco 网络设备进行配置的方法； CiscoWorks 软件对网络安全和用户帐户的管理方法； CiscoWorks 软件对网络及其设备维护信息库的管理技术和 CiscoWorks 软件如何对自身应用程序的管理与调度的方法。

本书图文并茂，内容丰富，技术新颖，实用性强。

8.**《网络核心技术内幕—IP/TV 开发指南》**：本书是专为从事网络开发和网络应用人员编写的。随着网络应用的不断深入，企业组网已经成为发展的必然趋势。而多媒体在网络上的应用更成为网络发展的一种时尚。Cisco 迎合这种发展的潮流，通过 IP / TV 使人们的梦想成为可能。

IP/TV 是一个客户/服务器体系结构的软件系统，为基于 IP 协议的局域网或广域网上的广大用户提供实时节目转播或预定节目数字视频和音频流的播放。

全书共分三部分：分别介绍 IP/TV 内容管理器，IP/TV 服务器，IP/TV Viewer。其中内容管理器部分主要介绍系统管理员或者广播管理员如何利用 IP/TV Content Manager 来建立和管理 IP/TV 实时节目转播或预定节目、频道、记录和在 IP/TV Server 之间的文件传输。IP/TV Server 则介绍了如何进行对内容管理器的控制，包括多点广播、单点传输点播节目、记录预定的节目，以及如何根据在内容管理器中定义的节目单点传输节目。而用户则需要通过 IP/TV Viewer 观看节目。IP/TV Viewer 从内容管理器取得节目信息，显示 IP/TV 服务器广播或单独播放的节目。也可以通过国际广播主干（Mbone）或从别的服务器传送的与 Mbone 兼容的广播节目获取所需的节目。

IP/TV 将一个完全动感的视频空间展现给终端用户，无需专用的视频电缆、显示器和会议室，并提供了对使用 ActiveMovie 结构的最新视频流格式的支持。可用于桌面电视会议、视频点播、网上培训、远程教学、团体通讯、制造过程监控，以及监视系统等。其前卫的设计思想展现了网络发展之必然，具有广阔的发展前景。

9.**《网络核心技术内幕—Cisco PIX 防火墙配置指南》**：本书是一本介绍 Cisco PIX 防火墙配置的指导书。全书共由 7 章组成，主要内容包括引言，配置 PIX 防火墙，高级配置，配置 IPSec，配置实例，命令参考，PIX 515 配置。

本书根据实际工程项目操作所需知识编写而成，可操作性强，内容新颖、丰富、实用性很强。同时，本书还附有大量的实例。

10.**《网络核心技术内幕—S/390 专用配置指南》**：本书是专为从事网络开发和应用人员编写的。

Cisco IOS for S/390 是 Cisco 公司专门为 IBM 主机系列的 S/390 开发的专用通信系统。本书包括了 Cisco IOS 用户指南、S/390 机 Cisco 配置指南、S/390 机规划指南和 S/390 机的 Cisco IOS 系统管理指南四部分内容。每部分内容都详细描述了 Cisco 实现的协议和技术、相关的配置任务，并包含综合配置的示例。每个命令索引都补充其相应配置内容并提供了完整的命令语法信息。

11.**《网络核心技术内幕—Cisco 新功能详解》**：本书是专为从事网络开发和应用的人员编写的。主要介绍 Cisco IOS 的新功能，涵盖了 Cisco IOS 版本增强特征的方方面面，主要包括防火墙功能集、各种设备互通、配置的各种增强特征、三级 DES 加密、动态数据包传输接口处理、PPP 等。本书对 Cisco IOS 版本的新特征进行了详尽、全面、透彻的介绍。本书结构清晰，内容丰富，技术新，实用性强。

12.**《网络核心技术内幕—网络协议解决方案》**：本书由 16 章组成，主要介绍 AppleTalk、Novell IPX、Apollo Domain、Banyan VINES、DECnet、ISO CLNS 和 XNS 等路由协议的网络解决方案，Cisco 实现的协议和技术、相关的配置任务，并包含综合配置的示例。每个命令索引都补充其相应配置内容并提供了完整的命令语法信息。

13.**《网络核心技术内幕—网络电话开发指南》**：专为从事网络电话开发和应用的人员编写的，是一本介绍 Cisco 智能电话控制器的指导书。全书由 6 章和 3 个附录组成，主要内容包括：电话控制器软件概述、

准备电话控制器、电话控制器的操作、检索呼叫详细记录及网络测量、维护过程和系统故障诊断与调试。附录分别介绍了配置数据文件参考、MML 命令和 UNIX 系统操作及安装。

本书内容新颖、结构清晰、丰富、实用性强，并附有大量的图例。书中既有对 Cisco 智能电话控制器软件的详细介绍，又有对其调试及安装的全面描述。

14.**《网络核心技术内幕—综合 IP 网络设计解决方案》**：IP 网络是现代网络技术的一个重要发展方向。建设综合 IP 网络对提高现代企业的竞争力尤为关键。本书对建设综合 IP 网络进行了全面阐述。本书分为两大部分：Internet 概述、网络核心与分布，内容涉及网络设计的概述，WAN、LAN 和路由器技术，以及路由协议的配置，QoS 发布和网络管理。第一部分包括 5 章：数据网络的发展、IP 基础、网络技术、网络拓扑结构设计、路由器等。第二部分包括 11 章：路由选择信息协议、路由选择信息协议版本 2、增强内部网关选择协议、开放最短路径优先、中间系统到中间系统、边界网关协议、迁移技术、协议无关多播、服务特性的质量、网络操作和管理、设计和配置的案例研究等。

本丛书具有以下特点：

1. **技术新，具有前瞻性** 紧跟 90 年代末、21 世纪初国际网络最新技术的发展是本丛书第一大特色。套书中介绍的网络规划与建设、软件和硬件的配置、安全与维护技术、网络电话的开发等技术均是国际目前最具代表、最流行的网络产品和技术。

2. **技术全面、内容丰富** 本丛书从网络巨头 Cisco 公司全球网络工程师资格认证考试 CCDA 教材、网络安全解决方案、组网技术解决方案、网络配置、如何阻挡和对抗黑客的攻击、网络协议解决方案到网络电话的开发、典型网络应用范例 S/390 专用配置，高起点、高定位，技术新、全面、系统、内容丰富和与当前市场网络产品同步或超前则是本丛书第二大特色。

3. **范例经典，实用性强** 本丛书结构设计合理、概念清晰、范例经典、可操作性和实用性强，所针对的问题具有现实性和代表性，解决方法具有实际指导性是本丛书第三大特色。

通过书中范例的学习，读者在学习和工作中可达到事半功倍的目的。本丛书不但是从事网络开发、应用和管理的广大网络技术人员的指导性读物，而且也是高等院校相关专业师生自学、教学用书和社会相关领域培训班的教材。

在此特别感谢世界通信巨头 Cisco 公司的首席技术顾问、美国 ATD 国家实验室主任、耶鲁大学教授约瑟夫·帕利洛先生，本丛书就是在他的大力帮助和协调下才得以完成。感谢美国国家网络安全委员会成员、麻省理工学院教授琼斯·雷蒙女士，耶鲁大学教授米勒·汉克斯先生，Cisco 公司技术主任蒂姆·克拉克博士，由于他们的全力参与和辛勤劳动，本丛书能够及时完稿和及时面市。

特别要感谢的是本丛书的翻译人员：刘大伟、曾春平、刘道云、李志、程永敬、邱仲潘、杜德宁、夏红山、杨键、韩平；编辑人员：刘晓融、龙启铭、马宏华、王玉玲、周艳、周凤明、苏静、郭淑珍、赵玉芳、徐建华； 录排人员：全卫、杜海燕、李毅、刘桂英、董淑红、马君、周宇、邓娇龙；美工设计人员张洁、徐立平； 光盘制作人员尹飒爽等，是他们的加班、加点、忘我的工作，才使本丛书如期付印出版，在此表示深切的谢意！

尽管我们很努力，但相信书中会有不少需要修改之处，希望能得到各界读者的信息反馈，以期为大家提供更好的作品。

北京希望电子出版社

2000 年 3 月

第1章 引 言

本章提供配置 PIX 防火墙所需要的信息，具体包括以下五部分：

- 理解 PIX 防火墙
- PIX 防火墙的特性
- 创建一个安全策略
- 决定多路接口的使用
- 命令行指导

有关这一章出现的缩写请参考附录 B“首字母缩写词与简写”部分。

1.1 理解 PIX 防火墙

正确地配置 PIX 防火墙有助于防止在两个或多个网络之间非授权的连接。

本节包括以下 3 个主题：

- 简介
- 自适应安全算法
- 更多的信息

1.1.1 简介

PIX 防火墙可以保护一个或多个网络，以便防止外部无保护网络的入侵。PIX 防火墙可以有选择地支持多种外部或边界网络（有时也称为非军事区（DMZs））。网络之间的连接都可以通过 PIX 防火墙来控制。

为了有效地在你的组织中使用防火墙，你需要一个安全策略来保证所有来自受保护网络的流量只有通过防火墙才能传递给无保护的网络（更多的信息请参考“创建一个安全策略”这一节）。然后可以使用 PIX 防火墙提供的特征来控制访问网络的人员使用哪些服务，以及怎样实现你的安全策略。

图 1-1 显示了当网络提供向外连接时，PIX 防火墙如何保护网络使网络能安全地访问 Internet。

在这个结构中，PIX 防火墙在受保护网络和无保护网络之间形成一条边界。受保护网络和无保护网络之间的所有流量必须通过防火墙流动以保持安全。无保护网络对于 Internet 来讲是可以访问的。PIX 防火墙让你在受保护网络中定位服务器，例如用于 Web 访问、SNMP、电子邮件（SMTP）的服务器，并对外面的用户访问这些服务器进行控制。

作为选择，服务系统可以在边界网络上定位，如图 1-1 所示，对服务系统的访问能够在 PIX 防火墙的控制和监视下进行。PIX 防火墙允许在内部网络的向内和向外连接上执行安全策略。

有代表性的内部网络是由一个组织拥有的内部网，或者 Intranet，外部网络是 Internet。但在 Intranet 中，PIX 防火墙也可以用来对内部计算系统的组和用户之间提供隔离或保护。

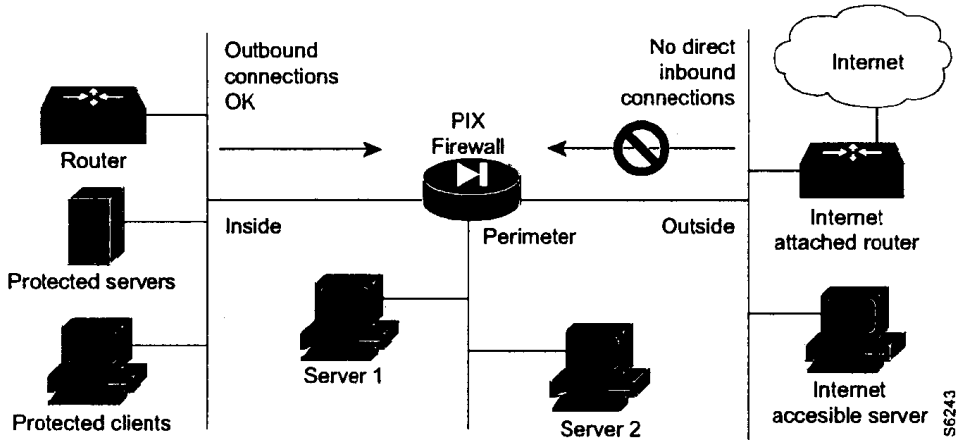


图 1-1 网络中的防火墙

边界网络可以配置成同内部网一样安全，也可以配置成从具有最高安全性的内部网到最低安全性的外部网之间可变的安全级别。内部网和边界网络都采用 PIX 防火墙的自适应安全算法来保护自己。自适应安全算法将在这章的后面描述。内部网、边界网络、外部网能监听 RIP 路由表的更新，并且如果需要的话，所有的接口会广播一个 RIP 缺省的路由表。

1.1.2 自适应安全算法

自适应安全算法（ASA）特性适用于动态转换槽（translation slots）和静态转换槽。你可以用 static 命令创建静态转换槽，用 global 命令创建动态转换槽。集中地讲，两种类型的转换槽都可以以“xlate”为参考。

这一节包括以下三个主题：

- 理解自适应安全算法
- 数据如何通过防火墙进行移动
- 内部地址的转换

理解自适应安全算法

自适应安全算法是同状态密切相关的安全性方法。每个进入的包要经过自适应安全算法和内存中的连接状态信息的检查。在工业界，这种同状态相关的安全性方法被认为比同状态无关的包筛选方法要安全得多。

自适应安全算法遵循下面的规则：

- 任何没有进行连接和无状态的包不可能穿过 PIX 防火墙。
- 除在访问控制表中专门被拒绝的以外，向外的连接或状态是允许的。一个向外连接的发起者或者客户端处在一个比接收方或者服务器更高的安全接口上。最高级别的安全接口通常为内部接口，最低级别的安全接口通常为外部接口。任何一个边界接口具有的安全级别可能在内部值和外部值之间。
- 除特别的被管道命令允许的外，向内的连接或状态被拒绝。一个向内连接的发起者或者客户端处在一个比接收方或者服务器更低的安全接口上。你可以对单个转

换应用多种例外。这允许你从 Internet 上的任何一台机器、网络、主机访问由 xlate 定义的主机。

- 所有的 ICMP 包都要被拒绝，但特别由 conduit permit icmp 命令允许的包除外。
- 所有要违反上述规则的企图都要被停止，并向系统日志发送一条消息。

PIX 防火墙以一种同 TCP 相似的方式处理 UDP 数据的传递。专门地处理使 DNS、archie，Stream Works，H.323 和 RealAudio 安全地工作。当一个 UDP 分组从内部网发送出来的时候，PIX 防火墙会创建 UDP 连接状态信息。该分组的应答包如果同连接状态信息匹配，那么将被接收。在短暂的停止之后，连接状态信息被删除。

数据如何通过防火墙

当一个向外发送的包到达一个 PIX 防火墙较高级别的接口时（用 nameif 命令设置安全级别），不管前一个包是否来自哪个主机，PIX 防火墙用自适应安全算法检查该包是否有效。如果不是，该包属于一个新的连接，PIX 防火墙会为该连接在状态表中创建转换槽。PIX 防火墙存储在转换槽中信息包括内部的 IP 地址和全局唯一的 IP 地址，该地址由 NAT、端口地址转换（PAT），或者身份（使用内部地址作为外部地址）分配。PIX 防火墙接着改变包的源地址为全局唯一地址，按照要求修改校验和以及其他域的内容，并将包转发给较低的安全级别接口。

当一个向内传送的包到达无保护的接口时，它必须首先要通过 PIX 防火墙的自适应安全标准的检查。如果包通过了安全检查，PIX 防火墙移走目的 IP 地址，并在相应的位置上插入内部的 IP 地址。该包接着被转发给受保护的接口。

内部地址转换

动态转换槽对于 Internet 上不需要固定地址的桌面机器是有用的。拥有 IP 地址的内部网络主机，虽然该 IP 地址没有在 NIC(network Information Center)注册，但在 PIX 防火墙内部通过地址转换，也可以在桌面上用标准的 TCP/IP 软件直接地访问 Internet。不需要专门的客户端软件。

PIX 防火墙支持 NAT（网络地址转换）和端口地址转换，NAT 为每个内部网络主机提供了一个全局唯一地址，端口地址转换可以使同时访问多达 64K 个内部主机共享一个全局唯一地址，

PIX 防火墙另外一类地址转换是静态转换，静态转换有效地在 PIX 防火墙中将一个内部的、没有注册的主机移进虚拟网。这对于被外部 Internet 网关寻址的内部机器是有用的。例如，SMTP 服务器。

基本配置将在第 2 章“配置 PIX 防火墙”中描述，创建了基本配置之后， PIX 防火墙允许从受保护的网络到无保护网络的所有向外连接。拒绝任何来自无保护网络的向内连接。这个缺省的策略可以通过表 1-1 描述的特性来修改以符合你所在组织的策略要求。

1.1.3　更多的信息

要获得更多的防火墙信息，请参考：

Bernstein,T.,Bhimani,A.B.,Schultz,E.and Siegel,C.A.Internet Security for Business. Wiley. information about this book is available at:http://www.wiley.com

Chapman,D.B.&Zwicky,E.D.Building Internet Firewall.O'Reilly. Information about this

book is available at http://www.ora.com/

Cheswick,W.and Bellovin,S.Firewall&Internet Security.Addison-Wesley.Information about this book is available at:http://www.aw.com/cp/Ches.html

Garfinkel,S.and Spafford,G.Practical UNIX Security.O'Reilly.Information about this book is available at:http://www.ora.com/

Stevens,W.R.TCP/IP Illustrated,Volume 1 The Protocols.Addison-Wesley.Information about this book is available at:http://www.awl.com/cp/Vol1.html

注意：你可以通过万维网浏览 PIX 防火墙的信息和附加的文档，地址是 http://www.cisco.com/warp/public/778/security/pix/

1.2 PIX 防火墙的特性

PIX 防火墙提供了全面的保护，这种保护对于外界完全地隐藏了内部网络结构。PIX 防火墙允许从现有的私有网络内部安全地访问 Internet，并有能力在不考虑 IP 地址不足的情况下扩展和配置 TCP/IP 网络。

PIX 防火墙特性在表 1-1 中描述。

表 1-1 PIX 防火墙特性

特性	描述	优点	安全含义
AAA 服务器组	PIX 防火墙允许你为指定的不同类型流量定义独立的 TACACS+或者 RADIUS 服务器组；例如，一个 TACACS+服务器处理入网流量，另外一个处理出网流量	AAA 服务器组用标记名定义，标记名把不同类型的流量指示给认证服务器	如果帐号有效，则帐号信息转给活动服务器
访问表	控制哪一个内部系统能够同外部网络建立连接	以内部的源地址，外部的目的地址，或者协议为基础，通过对向外连接进行限制，则缺省的安全策略可以被修改以使它同站点的安全策略相一致，	如果你的安全策略要对向外连接进行了限制，则要认真地配置访问表
ActiveX 阻塞	ActiveX 控件，以前被称为 OLE 或者 OCX 控件，是你可以插入 Web 页面或者其他应用程序的组件	PIX 防火墙的 ActiveX 阻塞特性将 Web 页面中出现的 HTML<object> 命令过滤掉	作为一种技术，ActiveX 对网络客户产生了许多潜在的问题，包括导致工作站故障，引起的网络安全问题，或者被用于攻击服务器

（续表）

特性	描述	优点	安全含义
自适应安全算法（ASA）	通过防火墙实现同状态相关的连接控制	如果没有为每个内部系统和程序进行显式地的配置，则防火墙允许单向连接（内部→外部）	通常情况下，监视返回包的操作是用来保证他们的有效性，主动地打乱TCP序号使TCP序号攻击的危险减少到最低
类 Cisco IOS 的配置方式	同Cisco IOS相似，PIX防火墙支持命令行接口	熟悉 Cisco IOS 路由器接口的管理员会很轻松地使用PIX防火墙	相似的接口会减少产生错误和引起安全漏洞的机会
管道（conduits）	管道允许从外部网络到内部网络的连接	对于某种应用或者商业需求，存在和内部或者边界网络建立连接的要求，这就可能允许某个远程系统对内部网进行访问，或者提供位于内部系统主机上的应用程序的访问	每个管道是穿过 PIX 防火墙的潜在的漏洞，所以，它们的使用应该以你的安全策略和商业需求为限，通过指定远程的源地址、本地目的地址和协议，使管道的说明尽可能的详细
快速穿越代理（cut throught Proxies）	基于用户的向内和向外连接的认证，不象代理服务器那样在 OSI 模型的七层上分析每个包，一个定时和集中处理的功能，PIX 防火墙首先查询认证服务器，一旦同意连接，则建立数据流。其后的流量在双方之间直接、快速地流动	安全策略在每个用户 ID 的基础上得到了加强，在连接能够建立之前，连接必须用用户 ID 和口令进行认证。支持认证和授权。用户 ID 和口令通过初始的 HTTP、Telnet、或者 FTP 连接填入	同检查源 IP 地址的方法比较来看，允许更好的连接管理控制，当提供向内认证时，需要对外部用户使用的用户 ID 和口令进行恰当地控制（这种情况下，推荐输入一次性口令）
PIX 防火墙 520 采用直流电源	PIX 防火墙 520 采用直流电源模式	能够工作在 48 伏的直流电环境中	在电话和环境中提供网络安全，在这些环境中先前未考虑到 PIX 防火墙
DNS 卫士	标识向外的 DNS 解析请求，并且只允许单个的 DNS 响应	一个主机为了得到应答可能检索几个服务器（例如第一个服务器响应速度慢），但只有对特定问题的第一个回答被允许，所有其他从服务器的回答都被丢弃	总是处于激活的状态下

（续表）

特性	描述	优点	安全含义
failover 特性	PIX 防火墙的 Failover 特性允许你以完全冗余的拓扑结构配置两个 PIX 防火墙单元	对容错网络需求日益增加。PIX 防火墙的 Failover 特性可以提供这样的网络	两个 PIX 防火墙单元必须是相同的配置，Failover 特性不提供状态冗余
FDDI 接口	PIX 防火墙支持两个 FDDI 网络接口	Cisco FDDI 卡符合 ANSI 规范 ASC X3T9.5，它同以太网的 IEEEE802.3 或者令牌环网的 IEEEE802.5 规范是同等的。FDDI 驱动器支持 Failover 特性	FDDI 接口不可能用作以太网或者令牌环接口
洪流防御	通过给 nat 和 static 命令设置最大的初始连接数，以保护内部网络免受 TCP SYN 洪流的攻击	允许内部网络服务器免受拒绝服务的攻击（DoS）（这并不是 floodguard 的特性）	保护内部系统免受 SYN 的攻击
Flood Guard	控制 AAA 服务对无回答登录企图的容忍度，特别要防止对 AAA 拒绝服务攻击	优化 AAA 系统的使用，用 floodguard1 命令	缺省处于激活状态
四端口的以太网接口	这部分提供了 4 个 10 / 100 兆的以太网连接，并且具有自动感知的能力	除了 PIX515 外，其他的可以和令牌环接口相互混合使用	四端口卡上的连接器由高到低编号，而实际的设备号依靠四端口卡所安装槽的位置而定
PIX 防火墙管理器采用图形用户界面	以 Windows NT，Windows 95，Solaris Web 浏览器为管理接口	可以通过 GUI 而不是命令行来配置 PIX 防火墙	限制用 HTML 接口对内部网络的特殊客户进行访问，并采用口令保护
同一性	允许地址转换失效	如果现有的内部系统有有效的全局唯一地址，那么对于这些系统同一性允许 NAT 和 PAT 有选择地失效	使内部网络地址对于外部网络是可见的
防止 IP 碎片	保护 PIX 防火墙免受 IP 碎片的攻击	保护 PIX 防火墙免受 IP 碎片的攻击	同样阻塞了正常的 IP 碎片，缺省设置为失效

（续表）

特性	描述	优点	安全含义
IPSec	通过数字签名或者预先共享的或者手工输入的关键字，提供虚拟专用网络（VPN）的访问	在对等实体之间进行加密	与 VPN 客户，路由器和另外一个 PIX 防火墙一同工作。采用 Iec，你可以远程地管理 PIX 防火墙
Java 过滤	让管理员阻止内部系统下载 Java applets	Java applets 是一种可执行程序，但在某中安全策略下会被禁止	Java 程序可以提供一种手段，通过它内部系统可能会被侵犯
邮件保护	为建立从外部到内部的邮件服务器的简单邮件传输协议（SMTP）连接提供一个安全的管道	允许在内部网络中配置一个专一的邮件服务器，不会暴露出某种 SMTP 服务器的执行所带来的安全问题。避免了需要外部邮件中继系统	执行一个 SMTP 命令的最小安全集来避免一个 SMTP 服务器系统被侵犯。同样记录所有的 SMTP 连接
内存升级	使 PIX 防火墙更有效的工作，最少需要 16MB 的 RAM，推荐使用 32MB	内存升级允许通过 PIX 防火墙同时建立更多的连接	需要 PIX 防火墙软件版本 4.2 和以后的版本
多种接口	给 PIX 防火墙增加附加的网络接口	在单一的底座中取代多个 PIX 单元	为边界接口提供自适应安全
多媒体支持	PIX 防火墙支持多媒体应用包括 ealAudio,Streamworks,CU-SeeMe,IP 电话，IRC，H.323，Vxtreme 和 VDO live	用户对各种各样的多媒体应用程序的使用日益增加，在防火墙环境下，许多应用需要专门地处理，PIX 不要求客户重新配置就可以处理这些应用，而且不会成为性能瓶颈	需要的话，使用访问表可以使对协议的支持无效
通过 IP 的 NEIBIOS	支持从内部网络到外部网络的通过 IP 的 NEIBIOS 连接	允许在内部网络的微软客户端系统，例如 Windows 95，使用 NAT 来对外部网络上的 Windows NT 服务器进行访问，这可以使安全策略能够覆盖 Internet 和内部的 Intranet 微软环境	允许访问控制本地的微软环境

（续表）

特性	描述	优点	安全含义
网络地址转换（NAT）	对于内部系统而言，依据 RFC 1631，转换向外传送的包的源地址。不但支持动态转换，而且支持静态转换	允许给内部系统分配地址（RFC1981 定义）或者保持现有的无效地址	对外部网络隐藏了内部系统的网络特性
PIX 515	PIX 515 在主板上包含两个 10/100 以太网接口，16MB 的闪存，32MB 的内存，两个 PCI 插槽是为了安装额外的接口或者 VPN 卡，基本的模型有 32MB 的 RAM 并且可同时接受 68000 个连接	PIX 515 为进入低价的防火墙市场提供了一条通路	PIX 515 对向内和向外的接口仅支持以太网接口
端口地址转换(PAT)	通过使用端口重映射，一个单一有效的 IP 地址可能为 64000 个活动的 xlate 对象支持源 IP 地址转换	PAT 减少了为支持专用或者无效的内部网络地址方案而要求的全局有效的地址数量	对外部网络隐藏了内部系统的网络特性
安装向导简化了安装过程	PIX 防火墙安装向导工作在 Windows 95 或者 Windows NT 系统上，用以简化初始的配置	通过一个既有屏幕上的描述又有关联详细信息的帮助文件的过程，会指导你加快初始的安装	消除了公共的配置问题
6 个接口	PIX 防火墙支持多达 6 个接口，其中的四个在可选的 4-端口以太网卡上	可以提供一个混合的令牌环和以太网环境	允许将网络分配给单独的接口，它可采用独立的安全策略被单独地保护
支持 SNMP MIB-II	通过简单网络管理协议支持对网络的监视	采用本身的 SNMP 接口，PIX 防火墙能与网络管理环境集成	仅支持 SNMP GET 访问（只读）
系统日志服务	利用 Windows NT 提供系统日志服务，在 NT 上接收从 PIX 防火墙发送过来的 TCP 和 UDP 系统日志信息	系统日志服务可以提供加上时间戳的系统日志消息，轮流地接收端口上的消息，如果收不到消息，则应配置为停止 PIX 防火墙的流量	如果 NT 系统日志服务登记磁盘满或者服务器停止工作。则可以停止 PIX 防火墙连接

（续表）

特性	描述	优点	安全含义
Telnet 接口	同 Cisco IOS 相似，它提供了一个命令行接口。Telnet 接口允许你通过控制台接口远程地管理 PIX 防火墙	使 PIX 防火墙控制台的远程配置和管理成为可能	在内部网络中，限制 Telnet 接口的访问到指定的客户系统并提供口令保护，如果内部网络不安全，局域网上的会话可能被侦听到，你应该限制 Telnet 接口的使用，如果配置了 IPSec 你也可以从外部接口访问 PIX 防火墙控制台
TFTP 配置服务器	提供通过 TFTP 配置 PIX 防火墙	允许中心源一次或多次访问防火墙配置	不安全。如果你的安全策略阻止明文来共享特权信息，你就不要使用该特性
TFTP 图片下载	从 CCO 下载的一个.bin 图片可以通过 TFTP 从位于内部网络接口的主机下载到 PIX 防火墙	允许你从远程的服务器上管理 PIX 防火墙上的.bin 文件并在需要的时候下载它们	当传递文件时 TFTP 不执行任何的认证过程，所以，不需要远程主机上的用户名和口令
URL 过滤	PIX 防火墙 URL 过滤功能与网络伙伴的 WebSENSE 产品是伙伴关系，PIX 依据定义在 WebSENSE 服务器上的策略检查向外的 URL 请求，WebSENSE 服务器可以运行在 Windows NT 或 UNIX 上	依据网络伙伴的 WebSENSE 服务器的响应，它根据判定为不适于商业用途的 17 个 Web 站点的特性列表来匹配请求，如果认为是不适合商业应用，则 PIX 防火墙或者同意或者拒绝连接	因为 URL 过滤是在独立的平台上处理的，不会给 PIX 防火墙增加额外的负担 访问 http:\\www.websense.com 获取更多的信息
VPN	利用 IPSec 技术，取代以前的专用的连接软件。可以同专用连接卡一起工作	在对等实体之间加密	与 VPN 客户，路由器和另外的 PIX 防火墙一同工作。采用 IPSec，你可以远程地管理 PIX 防火墙

1.3.1 创建一个安全策略

PIX 防火墙把执行安全策略的细节同提供网络服务（例如 Web，Telnet，FTP 和 SMTP）分开。

本节包括以下三个主题：

- 安全策略为我们提供了什么