



网络安全 Cisco 解决方案

Cisco Secure Internet Security Solutions

[美] Andrew G. Mason 著
Mark J. Newcomb

詹文军 等译

CISCO SYSTEMS
CISCO PRESS



电子工业出版社
Publishing House of Electronics Industry
www.phei.com.cn

网络安全 Cisco 解决方案

Cisco Secure Internet Security Solutions

[美] Andrew G. Mason 著
Mark J. Newcomb

詹文军 等译

电子工业出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

虽然 Cisco Systems 公司通过推出 Cisco Secure 产品系列来帮助客户建立安全的网络,但到目前为止,国内尚没有使用 Cisco Secure 产品系列来解决因特网安全性问题的出版物,本书的出版填补了这一空白。本书英文原版的作者都是具有高深资历的网络安全专家,其中主笔人 Andrew G. Mason 作为一位 Cisco 网络认证工程师,具有多年使用 Cisco Secure 产品来设计和实现网络安全解决方案的丰富经验,为本书内容的权威性提供了充分的保证。本书内容覆盖了因特网安全性基础,并对 Cisco Secure 产品系列中的每种产品进行了集中介绍,提供了因特网安全所需要的优选配置示例。

本书主要针对网络工程师和网络设计人员,其基本读者是负责企业网连接或 Cisco Secure 产品安装的网络工程师和设计人员,也适用于负责网络安全以及对 Cisco Secure 产品感兴趣的其他网络人员、参加 CCIE 和 CCDP/CCNP 认证考试的人员、业界专家等。

Authorized translation from the English language edition published by Cisco Press. Copyright © 2001.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Simplified Chinese language edition published by Publishing House of Electronics Industry. Copyright © 2002.

本书中文简体版专有翻译出版权由 Pearson 教育集团所属的 Cisco Press 授予电子工业出版社。其原文版权及中文翻译出版权受法律保护。未经许可,不得以任何形式或手段复制或抄袭本书内容。

图书在版编目(CIP)数据

网络安全 Cisco 解决方案 / (美)梅森(Mason, A. G.)著;詹文军等译. —北京:电子工业出版社, 2002.1

书名原文: Cisco Secure Internet Security Solutions

ISBN 7-5053-7292-0

I. 网... II. ①梅... ②詹... 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(2001)第 088110 号

书 名: 网络安全 Cisco 解决方案

原 书 名: Cisco Secure Internet Security Solutions

著 者: [美] Andrew G. Mason Mark J. Newcomb

译 者: 詹文军 等

责任编辑: 谭海平 窦 昊

排版制作: 今日电子公司制作部

印 刷 者: 北京东光印刷厂

出版发行: 电子工业出版社 www.phei.com.cn

北京市海淀区万寿路 173 信箱 邮编: 100036

经 销: 各地新华书店

开 本: 787 × 1092 1/16 印张: 23.5 字数: 601.6 千字

版 次: 2002 年 1 月第 1 版 2002 年 1 月第 1 次印刷

书 号: ISBN 7-5053-7292-0

TP · 4182

定 价: 35.00 元

著作权合同登记号 图字: 01-2001-1439

凡购买电子工业出版社的图书,如有缺页、倒页、脱页者,请向购买书店调换。若书店缺货,请与本社发行部联系调换。联系电话: 88211980 68279077

译者序

Cisco Systems公司通过推出Cisco Secure产品系列致力于帮助其客户来建立安全的网络,但到目前为止,国内尚没有使用Cisco Secure产品系列来解决因特网安全性问题的出版物,本书的出版填补了这一空白,本书英文版的作者都是具有高深资历的网络安全性专家,其中主笔人Andrew G. Mason作为一位CCIE,其多年来使用Cisco Secure产品来设计和实现网络安全性解决方案的丰富经验为本书内容的权威性提供了充分的保证。

作为译者,我们希望能够尽自己的最大努力将这一本好书忠实、完整、正确地译出,希望它既能够符合国人阅读习惯,又能保证其原汁原味,如果能够达到这一目的,我们就觉得很欣慰了。

参加本书翻译的有:詹文军、廖铮、卢陈思、索为群、黄国平、孙大庆、白常青、张伟、张建伟、林依然、高博、吉明宇、黎建辉、姜楠、候捷、钱林海、李波等人,由詹文军负责统稿。

最后希望热心的读者对本书中的各种错误进行指正,谢谢。

前 言

因特网对于许多大企业来说已成为核心的业务驱动器，但是，随着业务的发展，安全性问题随之而来。最近的许多新闻头条常常出现关于大型电子商务站点被黑，造成潜在的灾难性后果的文章。

Cisco Systems 公司致力于帮助客户通过网络安全设计建立安全的网络连接，在这些网络安全设计中，Cisco Secure 产品系列扮演了重要的角色。目前还没有关于使用 Cisco Secure 产品系列来处理因特网安全性的公开出版物，出版本书的目的正是在于此。本书的内容覆盖了因特网安全性基础，并对 Cisco Secure 产品系列中的每种产品进行了集中介绍，提供了丰富的解释以及为因特网连接提供安全性所需要的优选配置示例。

本书首先开始介绍由因特网所带来的安全性威胁，然后对 Cisco Secure 产品系列进行了完整的解释，同时对该产品系列中的每种产品进行了详细的讨论，而且还对如何根据具体环境的需求来对每个单独的组件进行配置提出了建议。另外，本书对 Cisco Secure PIX 防火墙进行了深入的介绍，从提出一个体系结构化的观点，到提供一个有关常用 PIX 命令和它们实际应用的参考。虽然本书关注的是因特网安全性，但它对于一般的网络安全也是可用的。

读者对象

本书针对网络工程师和网络设计人员。其基本读者是负责企业网连接或 Cisco Secure 产品安装的网络工程师和设计人员。其他的一些读者则可以是和他们所在的特定企业网环境相关的网络安全性和 Cisco Secure 产品感兴趣的其他网络人员。

另外，有志于通过 CCIE 和 CCDP/CCNP 认证的那些人可以在本书中获得提高其因特网安全性水平的内容。

本书面向中级和高级读者，由于本书内容的惟一性，一些业界的专家也可将本书作为参考。

读者阅读本书应具备的条件

本书中的内容假定读者已经熟悉了一般的网络概念和术语，其中包括对 TCP/IP 网络协议的完整了解，或者是已经熟悉了由电子工业出版社出版的《网络互联技术手册（第三版）》和《IP 路由基础》中的内容。

覆盖的内容

本书分为 11 章和一个附录：

- 第 1 章提供了对因特网的一个历史回顾，以及和因特网有关的风险。
- 第 2 章介绍了 Cisco 路由器和相关的安全性威胁，以及从因特网的角度来看，这些路由器所具有的安全性弱点。另外还提供了示例配置来作为用户实现自己的企业因特网路由

器的参考。

- 第3章提供了Cisco安全性解决方案和Cisco Secure产品系列。下面的6章对每种产品进行了详细的介绍。
- 第4章介绍了Cisco Secure PIX防火墙,并提供了对PIX的一个技术性概述,以及根据一个案例研究来提供的一个配置指导和示例配置。
- 第5章介绍了Cisco IOS防火墙,并提供了示例配置,而且对其中的主要技术进行了解释说明。
- 第6章介绍了一种最新出现的安全性技术,入侵检测。本章对各种入侵检测系统的类型进行解释,然后针对网络边界入侵的情况,提供了分别针对Cisco路由器和Cisco Secure PIX防火墙的示例配置。
- 第7章内容覆盖了Cisco Secure Scanner,并对网络扫描和其正当和非法的使用进行了简短的说明,然后深入介绍了Cisco所提供的Cisco Secure Scanner产品。
- 第8章介绍了Cisco Secure Policy Manager (CSPM),CSPM提供了一个针对企业网的集中化管理平台,该企业网中包含了运行Cisco IOS防火墙软件的Cisco路由器和Cisco Secure PIX防火墙。另外,本章提供了一个CSPM的示例安装和配置过程。
- 第9章介绍了Cisco Secure访问控制服务器(ACS)和它在网络中的使用。另外本章还提供了分别针对网络访问服务器(NAS)和Cisco Secure ACS服务器部分的配置。
- 第10章介绍了一个常见的企业网络,并列举出和外部连接相关的安全性威胁。另外还提供了对付安全性风险的各种提示和配置解决方案。
- 第11章集中介绍了因特网服务和能够为它们提供的安全性保护。本章的内容以这些公共服务器位于ISP或企业网DMZ作为基础,对每种因特网服务进行了介绍,并说明了各自潜在的安全性风险和减轻这些威胁的方法。
- 附录A“Cisco SAFE:针对企业网的安全性蓝图”——SAFE作为Cisco针对企业网的一个安全性蓝图,它的基本目标是为那些感兴趣的团体或个人提供有关设计和实现一个安全的网络的最佳实践信息。SAFE可以作为网络设计人员在考虑网络中安全性需求时所参考的一个指导手册。另外,SAFE采用了一种defense-in-depth(深入防范)的方式进行网络安全设计,这种类型的设计将视点聚焦于所预期的威胁以及减轻这些威胁的方法,而不是“在此放置一个防火墙,在那放置一个入侵检测系统”这种浅泛的指导。这种策略使网络的安全性采用了分层设计设施的方式,使得某个安全性系统的失效不太可能导致网络资源遭到损害。另外,SAFE基于Cisco公司及其合作伙伴所生产的产品。

语法规约与图标

在本书中的命令语法遵循以下约定:

- 命令、关键字和实际的参数值以粗体显示。
- 参数(需要提供实际的值)以斜体显示。
- 可选关键字或参数(或者是可选关键字或参数的选项)位于中括号[]中。
- 必须具有的关键字或参数位于大括号{}中。

注意：以上约定只针对命令语法，实际的配置和示例不遵循这些约定。

下图列举了本书中使用的大多数重要设备的图标。



目 录

第一部分 因特网安全性基础

第 1 章 因特网安全性	2
1.1 因特网上的威胁	2
1.2 网络服务	3
1.2.1 路由器服务	3
1.2.2 防火墙服务	4
1.2.3 认证和授权服务	5
1.2.4 网络地址转换服务	5
1.2.5 加密和解密服务	6
1.2.6 代理服务	7
1.3 TCP/IP 协议集的安全性	7
1.3.1 TCP/IP 概述	8
1.3.2 网际协议	9
1.3.3 地址解析协议	15
1.3.4 因特网控制报文协议	16
1.3.5 传输控制协议	18
1.3.6 用户数据报协议	19
1.4 拒绝服务攻击	20
1.4.1 SYN 洪泛攻击	20
1.4.2 Ping 攻击	21
1.5 创建企业安全性策略	22
1.6 小结	23
1.7 FAQ (常见问题)	23
1.8 词汇表	24
第 2 章 基本的 Cisco 路由器安全性	25
2.1 基本的管理安全性	26
2.1.1 访问列表	27
2.1.2 标准访问列表	28
2.1.3 扩展访问列表	33
2.1.4 命名访问列表	33
2.2 密码管理	34
2.2.1 enable password 命令	34

2.2.2 enable secret 命令	35
2.3 物理安全性	35
2.3.1 控制线路访问	36
2.4 带外管理安全性	37
2.5 Cisco 发现协议	38
2.6 超文本传输协议 (HTTP) 配置服务	38
2.7 简单网络管理协议	39
2.8 网络时间协议	41
2.9 警示标语	43
2.10 推荐的最小 IOS 安全性设置	43
2.10.1 拒绝 RFC 1918 路由	44
2.10.2 UDP 和 TCP 服务器	45
2.10.3 Finger 服务	45
2.10.4 IP Unreachable 报文	45
2.10.5 ICMP Redirect 报文	47
2.10.6 定向广播	48
2.10.7 Proxy ARP	48
2.10.8 IP Verify	48
2.10.9 IP 源路由	49
2.11 TCP 截获	50
2.12 小结	52
2.12.1 全局命令示例配置	53
2.12.2 接口命令示例配置	54
2.12.3 vty 命令示例配置	54

第二部分 Cisco Secure 产品系列

第 3 章 Cisco 安全性解决方案和产品系列概述	56
3.1 Cisco 安全性解决方案	56
3.1.1 标识	57
3.1.2 周边安全性	57
3.1.3 安全连接性	58
3.1.4 安全性监控	58
3.1.5 安全性管理	59
3.2 Cisco Secure 产品系列	59
3.2.1 Cisco Secure PIX 防火墙	59
3.2.2 Cisco IOS 防火墙	60
3.2.3 Cisco Secure IDS	61
3.2.4 Cisco Secure Scanner	63
3.2.5 Cisco Secure Policy Manager	65
3.2.6 Cisco Secure Access Control Server	66

3.3 小结	68
3.4 常见问题	68
3.5 词汇表	68
3.6 参考书目	69
3.7 网上资源	69
第4章 Cisco Secure PIX 防火墙	70
4.1 PIX 产品型号	71
4.1.1 PIX 506	71
4.1.2 PIX 515	72
4.1.3 PIX 520/525	73
4.1.4 PIX 535	73
4.2 PIX 防火墙功能	74
4.3 PIX 配置	76
4.3.1 基本配置	76
4.3.2 实际的配置	82
4.3.3 单个 DMZ 配置	87
4.3.4 带 AAA 认证的双重 DMZ	94
4.4 通过 PPTP 实现的 VPN	105
4.4.1 ip local pool 命令	106
4.4.2 vpdn 命令	106
4.4.3 sysopt 命令	108
4.5 使用 IPSec 和手工密钥的 VPN	108
4.5.1 crypto map 命令	110
4.5.2 crypto ipsec 命令	111
4.6 使用预共享密钥的 VPN	113
4.6.1 isakmp 命令	114
4.6.2 对使用预共享密钥的 VPN 的解释	114
4.7 获得证书授权机构证书	115
4.8 PIX 到 PIX 的配置	116
4.8.1 使用相同内部 IP 地址的 PIX 到 PIX 配置	118
4.9 小结	119
第5章 Cisco IOS 防火墙	120
5.1 访问列表	120
5.2 动态访问列表	120
5.3 基于时间的访问列表	123
5.4 反射访问列表	124
5.4.1 Null Route 命令	128
5.5 Cisco IOS 防火墙特性	129
5.5.1 端口应用程序映射 (PAM)	129

5.6 CBAC 如何工作	131
5.6.1 CBAC 工作方式	132
5.6.2 CBAC 事件发生顺序	134
5.6.3 CBAC 所支持的协议	134
5.6.4 与 Cisco 加密技术 (CET) 以及 IPSec 的兼容性	135
5.7 配置 CBAC	136
5.7.1 选择一个接口	136
5.7.2 在接口上配置 IP 访问列表	137
5.7.3 配置全局超时值和门限值	138
5.7.4 定义检查规则	139
5.7.5 配置记录和审核追踪	141
5.7.6 CBAC 配置示例	141
5.8 小结	143
第 6 章 入侵检测系统	144
6.1 入侵检测概述	144
6.1.1 基于主机的入侵检测系统	145
6.1.2 基于网络的入侵检测系统	146
6.2 入侵检测系统	147
6.3 Cisco Secure 入侵检测系统 (CSIDS)	147
6.3.1 CSIDS 部件概述	148
6.3.2 CSIDS 感应器	149
6.3.3 CSIDS 邮局协议	153
6.3.4 CSIDS 管理器	154
6.3.5 签名	156
6.3.6 对警报进行响应	159
6.3.7 截获日志	161
6.4 Cisco IOS 防火墙 IDS	162
6.5 Cisco Secure PIX 防火墙 IDS	163
6.6 Cisco IDS 配置	167
6.6.1 Cisco IOS 防火墙 IDS 配置	167
6.6.2 Cisco Secure PIX 防火墙 IDS 配置	169
6.7 小结	172
6.8 常见问题	173
6.9 词汇表	173
第 7 章 Cisco Secure Scanner	174
7.1 Cisco Secure Scanner 的功能	175
7.1.1 第 1 步: 网络映射	175
7.1.2 第 2 步: 数据收集	178
7.1.3 第 3 步: 数据分析	180

7.1.4 第4步：安全性弱点确认	180
7.1.5 第5步：数据表达和导航	182
7.1.6 第6步：报告	186
7.2 Cisco Secure Scanner 安装	187
7.3 Cisco Secure Scanner 的配置	187
7.3.1 第1步：运行 Cisco Secure Scanner	187
7.3.2 第2步：创建一个会话来捕获数据	188
7.3.3 第3步：截获所收集的数据	191
7.3.4 第4步：对所收集的数据进行报告	192
7.4 小结	192
7.5 常见问题	193
7.6 词汇表	193
7.7 URL	193
第8章 Cisco Secure Policy Manager (CSPM)	194
8.1 CSPM 的功能	194
8.2 CSPM 的安装	196
8.2.1 硬件需求	196
8.2.2 软件需求	197
8.2.3 规划安装	197
8.2.4 安装过程	202
8.3 配置示例	206
8.3.1 配置网络拓扑	207
8.3.2 配置安全性策略	219
8.3.3 生成并发布和特定设备相关的命令集	221
8.4 小结	223
8.5 常见问题	223
8.6 词汇表	223
8.7 URL	224
第9章 Cisco Secure ACS	225
9.1 Cisco Secure ACS 的功能	225
9.2 认证、授权和记账 (AAA) 概述	226
9.2.1 认证	227
9.2.2 授权	227
9.2.3 记账	227
9.3 RADIUS 和 TACACS+	228
9.3.1 RADIUS	229
9.3.2 TACACS+	229
9.3.3 RADIUS 和 TACACS+ 之间的差异	230
9.4 Cisco Secure ACS 的安装	231

9.4.1	Windows NT 和 Windows 2000 版本的安装	231
9.4.2	UNIX 版本的安装	232
9.5	Cisco Secure ACS 的配置	233
9.5.1	基于 Web 的配置和 ACS Admin 站点	233
9.5.2	User Setup 和 Group Setup 配置选项	234
9.5.3	Network Configuration 配置选项	236
9.5.4	System Configuration 配置选项	238
9.5.5	Interface Configuration 配置选项	240
9.5.6	Administrtion Control 配置选项	241
9.5.7	External User Databases 配置选项	243
9.5.8	Reports and Activity 配置选项	245
9.5.9	Online Documentation 配置选项	247
9.6	网络访问服务器的配置	248
9.6.1	AAA 配置概述	248
9.7	配置示例	253
9.7.1	案例假设	253
9.7.2	技术方面	253
9.7.3	潜在的风险	254
9.7.4	配置	254
9.7.5	ACS 服务器的配置	254
9.7.6	NAS 配置	255
9.7.7	认证配置	256
9.7.8	授权配置	257
9.7.9	记账配置	258
9.8	小结	259
9.9	常见问题	259
9.10	词汇表	259
9.11	书目	260
9.12	URL	260

第三部分 因特网安全性环境

第 10 章	保护企业网的安全	262
10.1	拨号连接的安全性	262
10.2	拨号用户认证、授权和记账 (AAA)	264
10.3	使用 TACACS+ 和 RADIUS 的 AAA 认证设置	266
10.3.1	初始配置	267
10.3.2	创建一个方法列表	268
10.3.3	将列表应用到接口	270
10.3.4	调整配置	271
10.4	AAA 授权设置	272

10.5	AAA 记账设置	273
10.6	同时使用所有的 AAA 服务	274
10.7	虚拟专用网 (VPN)	275
10.7.1	L2F	275
10.7.2	L2TP	276
10.7.3	GRE 隧道	276
10.7.4	加密	276
10.7.5	IPSec 配置	276
10.8	小结	278
第 11 章	提供到因特网的安全访问	279
11.1	因特网服务	280
11.2	要常见的因特网安全性威胁	280
11.2.1	网络入侵	281
11.2.2	拒绝服务 (DoS) 攻击	282
11.3	因特网服务安全性示例	284
11.3.1	在因特网服务安全性示例中的最初问题和威胁	284
11.3.2	对因特网服务安全性示例的建议修改	286
11.3.3	在因特网服务安全性示例修改后的问题和威胁	289
11.4	Web 服务	290
11.4.1	针对 Web 服务器的威胁	290
11.4.2	针对 Web 服务器所受威胁的解决方案	290
11.4.3	针对 Web 服务器的配置建议	291
11.5	文件传输协议 (FTP) 服务	291
11.5.1	针对 FTP 服务器的威胁	291
11.5.2	针对 FTP 服务器所受威胁的解决方案	292
11.5.3	针对 FTP 服务器的配置建议	292
11.6	因特网电子邮件服务器 (SMTP/POP3/IMAP4)	292
11.6.1	针对因特网电子邮件服务器的威胁	293
11.6.2	针对因特网电子邮件服务器所受威胁的解决方案	294
11.6.3	针对因特网电子邮件服务器的配置推荐	294
11.7	域名系统 (DNS) 服务器	294
11.7.1	针对 DNS 服务器的威胁	295
11.7.2	针对 DNS 服务器所受威胁的解决方案	295
11.7.3	针对 DNS 服务器的配置建议	295
11.8	后端服务器	295
11.8.1	针对后端服务器的威胁	296
11.8.2	针对后端服务器所受威胁的解决方案	296
11.9	小结	296
11.10	常见问题	297
11.11	词汇表	297

第四部分 附录

附录 A Cisco SAFE：针对企业网的安全性蓝图	300
A.1 本附录的作者	300
A.2 概述	300
A.3 本附录的读者	301
A.4 忠告	301
A.5 体系结构概述	302
A.6 模块概念	302
A.7 企业模块	309
A.8 企业网园区模块	309
A.9 企业网边缘模块	320
A.10 移植策略	334
A.11 附件 A：确认实验室	335
A.12 附件 B：网络安全性入门	352
A.13 附件 C：体系结构分类学	359
A.14 RFC	360
A.15 其他参考	361
A.16 其他公司产品参考	361
A.17 致谢	362

第一部分

因特网安全性基础

第 1 章 因特网安全性

第 2 章 基本的 Cisco 路由器安全性

第1章 因特网安全性

本章包含以下内容：

- 因特网威胁
- 网络服务
- TCP/IP 协议集的安全性
- 拒绝服务攻击
- 创建企业安全性策略
- 小结
- 常见问题
- 词汇表

本章介绍网络安全的一些基础内容，首先对最常见的攻击形式进行一番简介，然后介绍一些网络设备类型的特性。

Cisco Secure IOS 软件专门设计为用于防止外界攻击对用户网络的影响，Cisco Secure 软件对未经授权访问、拒绝服务（Dos，Denial of Service）攻击、人在中间（man-in-the-middle）攻击和许多其他常见的攻击方法可提供最高级别的防护，这些攻击方法或者是用来拒绝服务，或者是用于获得未经授权信息。Cisco Secure IOS 的安全性特性依赖于一些配置、硬件解决方案和技术，包括自适应安全性算法（ASA，Adaptive Security Algorithm），这些为当今的网络管理员提供了最佳的网络安全。

随着技术的发展，Cisco 公司也一直不断地改进其硬件和软件安全性解决方案以维持其在网络安全领域的先进性。本书对一些通过 Cisco Secure 解决方案的使用可提供的网络安全防护方法进行了探讨。

为介绍防止网络攻击的基本内容，本章的内容覆盖了一些协议，包括传输控制协议（TCP）、网际协议（IP）、地址解析协议（ARP）和用户数据报协议（UDP）等协议的格式，同时还介绍了最常见的 DoS 攻击形式。在本章以后的章节中提供了一些用于对付 DoS 攻击的专门技术。

本章的结尾则总结了企业安全性策略的需求和使用。

1.1 因特网上的威胁

因特网是由专用主机和公共主机所组成的一个集合。事实上，任何拥有一台计算机的人都可以通过某种方式连接到因特网，在任何时候，因特网上都存在着成百上千个个体。虽然这些个体中的大多数都没有不良企图，但总是有一些人，因为各种原因，试图渗透或摧毁位于网络上的服务。有时候网络会被这样一种技术所攻击，在这种技术中，无辜的第三方被利用来发起攻击。例如，一个系统被某种蠕虫病毒所感染的个体会非有意地将这一蠕虫病毒传递给所有和