

SYNGRESS®

1 YEAR UPGRADE
BUYER PROTECTION PLAN



MANAGING Cisco® Network Security

Second Edition

Everything You Need to Secure Your Cisco Network

- Complete Coverage of Cisco PIX Firewall, Secure Scanner, VPN Concentrator, and Secure Policy Manager
- Step-by-Step Instructions for Security Management, Including PIX Device Manager, and Secure Policy Manager
- Hundreds of Designing & Planning and Configuring & Implementing Sidebars, Security Alerts, and Cisco Security FAQs

Eric Knipp

Brian Browne

Woody Weaver

C. Tate Baumrucker

Larry Chaffin

Jamie Caesar

Vitaly Osipov

Edgar Danielyan Technical Editor

callisma

s o l u t i o n s @ s y n g r e s s . c o m

With more than 1,500,000 copies of our MCSE, MCSD, CompTIA, and Cisco study guides in print, we continue to look for ways we can better serve the information needs of our readers. One way we do that is by listening.

Readers like yourself have been telling us they want an Internet-based service that would extend and enhance the value of our books. Based on reader feedback and our own strategic plan, we have created a Web site that we hope will exceed your expectations.

Solutions@syngress.com is an interactive treasure trove of useful information focusing on our book topics and related technologies. The site offers the following features:

- One-year warranty against content obsolescence due to vendor product upgrades. You can access online updates for any affected chapters.
- “Ask the Author” customer query forms that enable you to post questions to our authors and editors.
- Exclusive monthly mailings in which our experts provide answers to reader queries and clear explanations of complex material.
- Regularly updated links to sites specially selected by our editors for readers desiring additional reliable information on key topics.

Best of all, the book you’re now holding is your key to this amazing site. Just go to **www.syngress.com/solutions**, and keep this book handy when you register to verify your purchase.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there’s anything else we can do to help you get the maximum value from your investment. We’re listening.

www.syngress.com/solutions

S Y N G R E S S[®]

SYNGRESS®

1 YEAR UPGRADE
BUYER PROTECTION PLAN



MANAGING

Cisco Network Security

Second Edition

Eric Knipp

Brian Browne

Woody Weaver

C. Tate Baumrucker

Larry Chaffin

Jamie Caesar

Vitaly Osipov

Edgar Danielyan Technical Editor

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, “Career Advancement Through Skill Enhancement®,” and “Ask the Author UPDATE®,” are registered trademarks of Syngress Publishing, Inc. “Mission Critical™,” “Hack Proofing™,” and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	42397FGT54
002	56468932HF
003	FT6Y78934N
004	2648K9244T
005	379KS4F772
006	V6762SD445
007	99468ZZ652
008	748B783B66
009	834BS4782Q
010	X7RF563WS9

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Managing Cisco® Network Security, Second Edition

Copyright © 2002 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN: 1-913836-56-6

Technical Editor: Edgar Danielyan
Technical Reviewer: Sean Thurston
Acquisitions Editor: Catherine B. Nolan
Developmental Editor: Jonathan Babcock

Cover Designer: Michael Kavish
Page Layout and Art by: Shannon Tozier
Copy Editor: Michael McGee
Indexer: Nara Wood

Distributed by Publishers Group West in the United States and Jaguar Book Group in Canada.



Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

Ralph Troupe, Rhonda St. John, Emlyn Rhodes, and the team at Callisma for their invaluable insight into the challenges of designing, deploying and supporting world-class enterprise networks.

Karen Cross, Lance Tilford, Meaghan Cunningham, Kim Wylie, Harry Kirchner, Kevin Votel, Kent Anderson, Frida Yara, Bill Getz, Jon Mayes, John Mesjak, Peg O'Donnell, Sandra Patterson, Betty Redmond, Roy Remer, Ron Shapiro, Patricia Kelly, Andrea Tetrick, Jennifer Pascal, Doug Reil, and David Dahl of Publishers Group West for sharing their incredible marketing experience and expertise.

Jacquie Shanahan, AnnHelen Lindeholm, David Burton, Febea Marinetti, and Rosie Moss of Elsevier Science for making certain that our vision remains worldwide in scope.

Annabel Dent and Paul Barry of Elsevier Science/Harcourt Australia for all their help.

David Buckland, Wendi Wong, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, and Joseph Chan of Transquest Publishers for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

Ethan Atkin at Cranbury International for his help in expanding the Syngress program.

Jackie Gross, Gayle Voycey, Alexia Penny, Anik Robitaille, Craig Siddall, Darlene Morrow, Iolanda Miller, Jane Mackay, and Marie Skelly at Jackie Gross & Associates for all their help and enthusiasm representing our product in Canada.

Lois Fraser, Connie McMenemy, Shannon Russell and the rest of the great folks at Jaguar Book Group for their help with distribution of Syngress books in Canada.

Thank you to our hard-working colleagues at New England Fulfillment & Distribution who manage to get all our books sent pretty much everywhere in the world. Thank you to Debbie "DJ" Ricardo, Sally Greene, Janet Honaker, and Peter Finch.



Contributors

F. William Lynch (SCSA, CCNA, LPI-I, MCSE, MCP, Linux+, A+) is co-author of *Hack Proofing Sun Solaris 8* (Syngress Publishing, ISBN: 1-928994-44-X), and *Hack Proofing Your Network, Second Edition* (Syngress Publishing, ISBN: 1-928994-70-9). He is an independent security and systems administration consultant and specializes in firewalls, virtual private networks, security auditing, documentation, and systems performance analysis. William has served as a consultant to multinational corporations and the federal government including the Centers for Disease Control and Prevention headquarters in Atlanta, GA as well as various airbases of the United States Air Force. He is also the Founder and Director of the MRTG-PME project, which uses the MRTG engine to track systems performance of various UNIX-like operating systems. William holds a bachelor's degree in Chemical Engineering from the University of Dayton in Dayton, OH and a master's of Business Administration from Regis University in Denver, CO.

Robert “Woody” Weaver (CISSP) is a Principal Architect and the Field Practice Leader for Security at Callisma. As an information systems security professional, Woody's responsibilities include field delivery and professional services product development. His background includes a decade as a tenured professor teaching mathematics and computer science, as the most senior network engineer for Williams Communications in the San Jose/San Francisco Bay area, providing client services for their network integration arm, and as Vice President of Technology for Fullspeed Network Services, a regional systems integrator. Woody received a bachelor's of Science from Caltech, and a Ph.D. from Ohio State. He currently works out of the Washington, DC metro area.

Larry Chaffin (CCNA, CCDA, CCNA-WAN, CCDP-WAN, CSS1, NNCDS, JNCIS) is a Consultant with Callisma. He currently provides strategic design and technical consulting to all Callisma clients. His specialties include Cisco WAN routers, Cisco PIX Firewall, Cisco VPN, ISP

design and implementation, strategic network planning, network architecture and design, and network troubleshooting and optimization. He also provides Technical Training for Callisma in all technology areas that include Cisco, Juniper, Microsoft, and others. Larry's background includes positions as a Senior LAN/WAN Engineer at WCOM-UUNET, and he also is a freelance sports writer for *USA Today* and ESPN.

Eric Knipp (CCNP, CCDP, CCNA, CCDA, MCSE, MCP+I) is a Consultant with Callisma. He is currently engaged in a broadband optimization project for a major US backbone service provider. He specializes in IP telephony and convergence, Cisco routers, LAN switches, as well as Microsoft NT, and network design and implementation. He has also passed both the CCIE Routing and Switching written exam as well as the CCIE Communications and Services Optical qualification exam. Eric is currently preparing to take the CCIE lab later this year. Eric's background includes positions as a project manager for a major international law firm and as a project manager for NORTEL. He is co-author on the previously published *Cisco AVVID and IP Telephony Design and Implementation* (Syngress Publishing, ISBN: 1-928994-83-0), and the forthcoming book *Configuring IPv6 for Cisco IOS* (Syngress Publishing, ISBN: 1-928994-84-9).

Jamie Caesar (CCNP) is the Senior Network Engineer for INFO1 Inc., located in Norcross, GA. INFO1 is a national provider of electronic services to the credit industry and a market leader in electronic credit solutions. INFO1 provides secure WAN connectivity to customers for e-business services. Jamie contributes his time with enterprise connectivity architecture, security, deployment, and project management for all WAN services. His contributions enable INFO1 to provide mission-critical, 24/7 services to customers across all of North America. Jamie holds a bachelor's degree in Electrical Engineering from Georgia Tech. He resides outside Atlanta, GA with his wife, Julie.

Vitaly Osipov (CISSP, CCSA, CCSE) is a Security Specialist with a technical profile. He has spent the last five years consulting various companies in Eastern, Central, and Western Europe on information security issues. Last year Vitaly was busy with the development of managed security service for a data center in Dublin, Ireland. He is a regular contributor to various infosec-related mailing lists and recently co-authored *Check Point NG Certified Security Administrator Study Guide*. Vitaly has a degree in mathematics. Currently he lives in the British Isles.

C. Tate Baumrucker (CISSP, CCNP, Sun Enterprise Engineer, MCSE) is a Senior Consultant with Callisma. He is responsible for leading engineering teams in the design and implementation of complex and highly available systems infrastructures and networks. Tate is industry recognized as a subject matter expert in security and LAN/WAN support systems such as HTTP, SMTP, DNS, and DHCP. He has spent eight years providing technical consulting services in enterprise and service provider industries for companies including American Home Products, Blue Cross and Blue Shield of Alabama, Amtrak, Iridium, National Geographic, Geico, GTSI, Adelphia Communications, Digex, Cambrian Communications, and BroadBand Office.

Brian Browne (CISSP) is a Senior Consultant with Callisma. He provides senior-level strategic and technical security consulting to Callisma clients, has 12 years of experience in the field of information systems security, and is skilled in all phases of the security lifecycle. A former independent consultant, Brian has provided security consulting for multiple Fortune 500 clients, and has been published in *Business Communications Review*. His security experience includes network security, firewall architectures, virtual private networks (VPNs), intrusion detection systems, UNIX security, Windows NT security, and public key infrastructure (PKI). Brian resides in Willow Grove, PA with his wife, Lisa and daughter, Marisa.



Technical Reviewer

Sean Thurston (CCDP, CCNP, MCSE, MCP+I) is an employee of Western Wireless, a leading provider of communications services in the Western United States. His specialties include implementation of multi-vendor routing and switching equipment and XoIP (Everything over IP installations). Sean's background includes positions as a Technical Analyst for Sprint-Paranet and the Director of a brick-and-mortar advertising dot com. Sean is also a contributing author to *Building a Cisco Network for Windows 2000* (Syngress Publishing, ISBN: 1-928994-00-8) and *Cisco AVVID & IP Telephony Design and Implementation* (Syngress Publishing, ISBN: 1-928994-83-0). Sean lives in Renton, WA with his fiancée, Kerry. He is currently pursuing his CCIE.



Technical Editor

Edgar Danielyan (CCNP Security, CCDP, CSE, SCNA) is a self-employed consultant, author, and editor specializing in security, UNIX, and internetworking. He is the author of *Solaris 8 Security* available from New Riders, and has contributed his expertise as a Technical Editor of several books on security and networking including *Hack Proofing Linux* (Syngress Publishing, ISBN: 1-928994-34-2) and *Hack Proofing Your Web Applications* (Syngress Publishing, ISBN: 1-928994-31-8). Edgar is also a member of the ACM, IEEE, IEEE Computer Society, ISACA, SAGE, and the USENIX Association.

Contents

Remote Dial-in User System

Remote Dial-in User System (RADIUS) is an open standard and available from many vendors:

- RADIUS uses UDP, so it only offers best effort delivery at a lower overhead.
- RADIUS encrypts only the password sent between the Cisco access client and RADIUS server. RADIUS does not provide encryption between the workstation and the Cisco access client.
- RADIUS does not support multiple protocols, and only works on IP networks.
- RADIUS does not provide the ability to control the commands that can be executed on a router: It provides authentication, but not authorization to Cisco devices.

Foreword

xxxi

Chapter 1 Introduction to IP Network Security

1

Introduction	2
What Role Does Security Play in a Network?	2
Goals	2
Confidentiality	3
Integrity	4
Availability	4
Philosophy	6
What if I Don't Deploy Security?	7
The Fundamentals of Networking	8
Where Does Security Fit in?	9
Network Access Layer Security	10
Internetwork Layer Security	11
Access Control Lists	12
Host-to-Host Layer Security	14
IPSec	14
Process Application Layer Security	17
PGP	19
S-HTTP	19
Secure Sockets Layer and Transport Layer Security	19
The Secure Shell Protocol	20
Authentication	21
Terminal Access Controller Access System Plus	22

Answers to Your Frequently Asked Questions

Q: Is a vulnerability assessment program expensive?

A: Not necessarily. The Cisco product is not terribly expensive, and there exist open source solutions which are free to use. The actual assessment program is probably less expensive than the remediation efforts: Maintaining all your hosts on an ongoing basis is a steep maintenance requirement, and one that not all enterprises have accepted. But ever since the summer of 2001, there has been clear evidence that you have to manage your hosts and keep their patch levels up-to-date just to stay in business.

Remote Dial-in User System	23
Kerberos	23
OSI Model	25
Layer 1: The Physical Layer	26
Layer 2: The Data-link Layer	26
Layer 3: The Network Layer	28
Layer 4: The Transport Layer	29
Layer 5: The Session Layer	30
Layer 6: The Presentation Layer	31
Layer 7: The Application Layer	32
How the OSI Model Works	34
Transport Layer Protocols	34
The Internet Layer	40
The Network Layer	43
Composition of a Data Packet	44
Ethernet	44
Security in TCP/IP	45
Cisco IP Security Hardware and Software	46
The Cisco Secure PIX Firewall	46
Cisco Secure Integrated Software	49
Cisco Secure Integrated VPN Software	50
The Cisco Secure VPN Client	50
Cisco Secure Access Control Server	50
Cisco Secure Scanner	51
Cisco Secure Intrusion Detection System	51
Cisco Secure Policy Manager	52
Cisco Secure Consulting Services	53
Summary	54
Solutions Fast Track	56
Frequently Asked Questions	59

Chapter 2 What Are We Trying to Prevent? 61

Introduction	62
What Threats Face Your Network?	64
Loss of Confidentiality	65
Loss of Integrity	65
Loss of Availability	65

NOTE

Make sure the COM port properties in the terminal emulation program match the following values:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- Hardware flow control

Sources of Threats	66
Malicious Mobile Code	67
Trojan Horses	67
Viruses	67
Worms	68
Current Malicious Code Threats	70
Current Malicious Code Impacts	70
Denial of Service	71
The Smurf Attack	73
The SYN Flood Attack	74
Distributed Denial of Service (DDoS) Attacks	75
Detecting Breaches	76
Initial Detection	77
File System Integrity Software	77
Network Traffic Anomaly Tools	78
Are Forensics Important?	78
What Are the Key Steps after a Breach Is Detected?	79
Preventing Attacks	80
Reducing Vulnerabilities	81
Providing a Simple Security Network Architecture	82
Developing a Culture of Security	85
Developing a Security Policy	86
Summary	88
Solutions Fast Track	91
Frequently Asked Questions	94

Chapter 3 Cisco PIX Firewall 97

Introduction	98
Overview of the Security Features	100
Differences between PIX OS Version 4.x and Version 5.x	104
Differences between PIX OS Version 6.0 and Version 5.x	106
Cisco PIX Device Manager	107
VPN Client v3.x	107

CPU Utilization Statistics	107
Dynamic Shunning with Cisco	
Intrusion Detection System	107
Port Address Translations	108
Skinny Protocol Support	108
Session Initiation Protocol	108
Stateful Sharing of HTTP (port 80)	
Sessions	108
Ethernet Interfaces	109
Initial Configuration	109
Installing the PIX Software	109
Connecting to the PIX—Basic	
Configuration	110
Identify Each Interface	111
Installing the IOS over TFTP	113
The Command-Line Interface	115
IP Configuration	116
IP Addresses	117
Configuring NAT and PAT	119
Permit Traffic Through	120
Security Policy Configuration	123
Security Strategies	125
Deny Everything that Is Not	
Explicitly Permitted	126
Allow Everything that Is Not	
Explicitly Denied	126
Identify the Resources to Protect	127
Demilitarized Zone	127
Identify the Security Services to Implement	129
Authentication and Authorization	129
Access Control	130
Confidentiality	130
URL, ActiveX, and Java Filtering	130
Implementing the Network Security Policy	131
Authentication Configuration in PIX	131
Access Control Configuration in PIX	133
Securing Resources	135

Logging Commands

There are also eight different levels of messages, which will be listed from most severe (Emergency - Level 0) to least severe (Debugging - Level 7):

- Emergency – Level 0
- Alerts – Level 1
- Critical – Level 2
- Errors – Level 3
- Warning – Level 4
- Notification – Level 5
- Informational – Level 6
- Debugging – Level 7

Confidentiality Configuration in PIX	138
URL, ActiveX, and Java Filtering	138
PIX Configuration Examples	140
Protecting a Private Network	140
Protecting a Network Connected to the Internet	142
Protecting Server Access Using Authentication	145
Protecting Public Servers Connected to the Internet	146
Securing and Maintaining the PIX	152
System Journaling	152
Securing the PIX	154
Summary	157
Solutions Fast Track	157
Frequently Asked Questions	160

Chapter 4 Traffic Filtering in the Cisco Internetwork Operating System 163

Introduction	164
Access Lists	164
Access List Operation	166
Types of Access Lists	167
Standard IP Access Lists	169
Source Address and Wildcard Mask	170
Keywords <i>any</i> and <i>host</i>	171
Keyword Log	172
Applying an Access List	174
Extended IP Access Lists	176
Keywords <i>permit</i> or <i>deny</i>	181
Protocol	181
Source Address and Wildcard-mask	182
Destination Address and Wildcard-mask	183
Source and Destination Port Number	183
Established	184
Log and Log-input	189

**Configuration
Commands**

Before NAT can be implemented, the “inside” and “outside” networks must be defined. To define the “inside” and “outside” networks, use the *ip nat* command.

```
ip nat inside |
  outside
```

- **Inside** Indicates the interface is connected to the inside network (the network is subject to NAT translation).
- **Outside** Indicates the interface is connected to the outside network.

Named Access Lists	189
Editing Access Lists	190
Problems with Access Lists	192
Lock-and-key Access Lists	193
Reflexive Access Lists	199
Building Reflexive Access Lists	202
Applying Reflexive Access Lists	205
Context-based Access Control	205
The Context-based Access Control Process	208
Configuring Context-based Access Control	208
Inspection Rules	211
Applying the Inspection Rule	212
Configuring Port to Application Mapping	213
Configuring PAM	213
Protecting a Private Network	214
Protecting a Network Connected to the Internet	217
Protecting Server Access Using Lock-and-key	219
Protecting Public Servers Connected to the Internet	221
Summary	227
Solutions Fast Track	227
Frequently Asked Questions	230

Chapter 5 Network Address Translation/Port Address Translation	233
Introduction	234
NAT Overview	234
Address Realm	235
RFC 1918 Private Addressing	235
NAT	237
Transparent Address Assignment	237
Transparent Routing	238
Public, Global, and External Networks	240
Private and Local Networks	240
Application Level Gateways	240

Encryption Key Types

Cryptography uses two types of keys: *symmetric* and *asymmetric*. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the ciphertext. This type of key is called a *secret key*, because you must keep it secret. Otherwise, anyone in possession of the key can decrypt messages that have been encrypted with it. The algorithms used in symmetric key encryption have, for the most part, been around for many years and are well known, so the only thing that is secret is the key being used. Indeed, all of the really useful algorithms in use today are completely open to the public.

NAT Architectures	241
Traditional NAT or Outbound NAT	241
Port Address Translation	243
Static NAT	245
Twice NAT	246
Guidelines for Deploying NAT and PAT	248
IOS NAT Support for IP Telephony	251
H.323 v2 Support	251
CallManager Support	252
Session Initiation Protocol	252
Configuring NAT on Cisco IOS	252
Configuration Commands	253
Verification Commands	258
Configuring NAT between a Private	
Network and the Internet	259
Configuring NAT in a Network with DMZ	261
Considerations on NAT and PAT	263
IP Address Information in Data	263
Bundled Session Applications	264
Peer-to-Peer Applications	264
IP Fragmentation with PAT en Route	264
Applications Requiring Retention	
of Address Mapping	264
IPSec and IKE	265
Summary	266
Solutions Fast Track	268
Frequently Asked Questions	271
Chapter 6 Cryptography	273
Introduction	274
Understanding Cryptography Concepts	274
History	275
Encryption Key Types	275
Learning about Standard Cryptographic	
Algorithms	277

Understanding Symmetric Algorithms	278
DES	278
AES (Rijndael)	280
IDEA	281
Understanding Asymmetric Algorithms	282
Diffie-Hellman	282
RSA	284
Understanding Brute Force	285
Brute Force Basics	285
Using Brute Force to Obtain Passwords	286
L0phtcrack	288
Crack	289
John the Ripper	289
Knowing When Real Algorithms Are	
Being Used Improperly	291
Bad Key Exchanges	291
Hashing Pieces Separately	292
Using a Short Password to Generate	
a Long Key	293
Improperly Stored Private or Secret Keys	294
Understanding Amateur Cryptography Attempts	296
Classifying the Ciphertext	297
Frequency Analysis	297
Ciphertext Relative Length Analysis	298
Similar Plaintext Analysis	298
Monoalphabetic Ciphers	299
Other Ways to Hide Information	299
XOR	299
UUEncode	303
Base64	303
Compression	305
Summary	307
Solutions Fast Track	308
Frequently Asked Questions	310

LocalDirector Product Overview

The LocalDirector product is available in three different ranges:

- **LocalDirector 416**
This is both the entry-level product as well as the medium-size product. It supports up to 90 Mbps throughput and 7,000 connections per second.
- **LocalDirector 430**
This is the high-end product. It supports up to 400 Mbps throughput and 30,000 connections per second.
- **LocalDirector 417**
Newer platform with different mounting features. It is even more productive than 430 series and has more memory—two Fast Ethernet and one Gigabit Ethernet interfaces.

Chapter 7 Cisco LocalDirector and DistributedDirector	313
Introduction	314
Improving Security Using Cisco LocalDirector	314
LocalDirector Technology Overview	315
LocalDirector Product Overview	315
LocalDirector Security Features	316
Filtering of Access Traffic	316
Using synguard to Protect Against SYN Flood Attacks	318
Using NAT to Hide Real Addresses	320
Restricting Who Is Authorized to Have Telnet Access to LocalDirector	321
Password Protection	321
The <i>enable</i> Password	322
The <i>telnet</i> Password	322
Syslog Logging	322
Securing Geographically Dispersed Server Farms	
Using Cisco DistributedDirector	323
DistributedDirector Technology Overview	323
DistributedDirector Product Overview	326
DistributedDirector Security Features	326
Limiting the Source of DRP Queries	326
Authentication between DistributedDirector and DRP Agents	327
The <i>key chain</i> Command	327
The <i>key</i> Command	328
The <i>key-string</i> Command	328
Password Protection	329
The <i>enable secret</i> Password	329
The <i>enable</i> Password	330
The <i>telnet</i> Password	330
Syslog Logging	330
Summary	331
Solutions Fast Track	331
Frequently Asked Questions	333

Chapter 8 Virtual Private Networks and Remote Access 335

Overview of the Different VPN Technologies

- A *peer* VPN model is one in which the path determination at the network layer is done on a hop-by-hop basis.
- An *overlay* VPN model is one in which path determination at the network layer is done on a “cut-through” basis to another edge node (customer site).
- Link Layer VPNs are implemented at link layer (Layer 2) of the OSI Reference model.

Introduction	336
Overview of the Different VPN Technologies	336
The Peer Model	336
The Overlay Model	338
Link Layer VPNs	338
Network Layer VPNs	339
Tunneling VPNs	339
Virtual Private Dial Networks	340
Controlled Route Leaking	340
Transport and Application Layer VPNs	340
Intranet VPNs	340
Extranet VPNs	341
Access VPNs	341
Layer 2 Transport Protocol	342
Configuring Cisco L2TP	343
An LAC Configuration Example	344
A LNS Configuration Example	344
IPSec	345
IPSec Architecture	346
Security Associations	349
Anti-replay Feature	350
A Security Policy Database	351
Authentication Header	351
Encapsulating Security Payload	352
Manual IPSec	352
Internet Key Exchange	353
Authentication Methods	354
IKE and Certificate Authorities	355
IPSec limitations	356
Network Performance	356
Network Troubleshooting	356
IPSec and Cisco Encryption Technology	357
Configuring Cisco IPSec	358
IPSec Manual Keying Configuration	358
IPSec over GRE Tunnel Configuration	364

Connecting IPSec Clients to Cisco IPSec	373
Cisco Secure VPN Client	373
Windows 2000	374
Linux FreeS/WAN	374
Summary	376
Solutions Fast Track	376
Frequently Asked Questions	377

WARNING

The SRVTAB is the core of Kerberos security. Using TFTP to transfer this key is an IMPORTANT security risk! Be very careful about the networks in which this file crosses when transferred from the server to the router. To minimize the security risk, use a cross-over cable that is directly connected from a PC to the router's Ethernet interface. Configure both interfaces with IP addresses in the same subnet. By doing this, it is physically impossible for anyone to capture the packets as they are transferred from the Kerberos server to the router.

Chapter 9 Cisco Authentication, Authorization, and Accounting Mechanisms

379

Introduction	380
Cisco AAA Overview	381
AAA Authentication	382
AAA Authorization	385
AAA Accounting	385
AAA Benefits	385
Cisco AAA Mechanisms	386
Supported AAA Security Protocols	387
RADIUS	388
TACACS+	393
Kerberos	397
Choosing RADIUS, TACAS+, or Kerberos	405
Configuring AAA Authentication	407
Configuring Login Authentication	
Using AAA	409
Configuring PPP Authentication	
Using AAA	413
Enabling Password Protection for Privileged EXEC Mode	416
Authorization	417
Configure Authorization	419
TACACS+ Configuration Example	422
Accounting	424
Configuring Accounting	425
Suppress Generation of Accounting Records for Null Username Sessions	429

FlowWall Security

FlowWall provides intelligent flow inspection technology that screens for all common DoS attacks, such as SYN floods, ping floods, smurfs, and abnormal or malicious connection attempts. It does this by discarding packets that have the following characteristics:

- Frame length is too short.
- Frame is fragmented.
- Source IP address = IP destination (LAND attack).
- Source address = Cisco address, or the source is a subnet broadcast.
- Source address is not a unicast address.
- Source IP address is a loop-back address.
- Destination IP address is a loop-back address.
- Destination address is not a valid unicast or multicast address.

RADIUS Configuration Example	429
Typical RAS Configuration Using AAA	431
Typical Firewall Configuration Using AAA	435
Authentication Proxy	439
How the Authentication Proxy Works	439
Comparison with the Lock-and-key Feature	440
Benefits of Authentication Proxy	441
Restrictions of Authentication Proxy	442
Configuring Authentication Proxy	442
Configuring the HTTP Server	443
Configuring the Authentication Proxy	444
Authentication Proxy Configuration Example	446
Summary	448
Solutions Fast Track	449
Frequently Asked Questions	451

Chapter 10 Cisco Content Services Switch 455

Introduction	456
Overview of Cisco Content Services Switch	456
Cisco Content Services Switch Technology Overview	457
Cisco Content Services Switch Product Information	457
Security Features of Cisco Content Services Switch	459
FlowWall Security	459
Example of Nimda Virus Filtering without Access Control Lists	462
Using Network Address Translation to Hide Real Addresses	464
Firewall Load Balancing	465
Example of Firewall Load Balancing with Static Routes	466
Password Protection	468
The User Access Level	468
The SuperUser Access Level	469

Searching the Network for Vulnerabilities

There are three primary steps in creating a session to search your network for vulnerabilities:

1. Identifying the network addresses to scan
2. Identifying vulnerabilities to scan by specifying the TCP and UDP ports (and any active probe settings)
3. Scheduling the session

Disabling Telnet Access	470
Syslog Logging	471
Known Security Vulnerabilities	471
Cisco Bug ID CSCdt08730	472
Cisco Bug ID CSCdt12748	472
Cisco Bug ID CSCdu20931	472
Cisco Bug ID CSCdt32570	472
Cisco Bug ID CSCdt64682	472
Multiple SSH Vulnerabilities	473
Malformed SNMP Message Handling Vulnerabilities	473
CodeRed Impact	473
Summary	474
Solutions Fast Track	475
Frequently Asked Questions	476
Chapter 11 Cisco Secure Scanner	479
Introduction	480
Minimum System Specifications for Secure Scanner	481
Searching the Network for Vulnerabilities	483
Identifying Network Addresses	485
Identifying Vulnerabilities	487
Scheduling the Session	491
Viewing the Results	493
Changing Axis Views	495
Drilling into Data	497
Pivoting Data	498
Zooming In and Out	500
Creating Charts	501
Saving Grid Views and Charts	502
Reports and Wizards	503
Keeping the System Up-to-Date	504
Summary	508
Solutions Fast Track	508
Frequently Asked Questions	510

Frequently Asked Questions

Q: Which IDS platforms are supported in CSPM?

A: Only Cisco Secure IDS sensors (former NetRanger sensors) are supported, either in standalone configuration or as Catalyst 6000 blades. Embedded IDS features of Cisco PIX firewalls and Cisco IOS routers are not supported.

Chapter 12 Cisco Secure Policy Manager	513
Introduction	514
Overview of the Cisco Secure Policy Manager	514
The Benefits of Using Cisco Secure Policy Manager	515
Installation Requirements for the Cisco Secure Policy Manager	516
Features of the Cisco Secure Policy Manager	518
Cisco Firewall Management	519
VPN and IPSec Security Management	520
Security Policy Management	522
Security Policy Definition	522
Security Policy Enforcement	523
Security Policy Auditing	525
Network Security Deployment Options	526
Cisco Secure Policy Manager Device and Software Support	526
Using the Cisco Secure Policy Manager Configuration	528
CSPM Configuration Example	530
Summary	535
Solutions Fast Track	535
Frequently Asked Questions	538
Chapter 13 Intrusion Detection	541
Introduction	542
What Is Intrusion Detection?	542
Types of IDSs	543
IDS Architecture	543
Why Should You Have an IDS?	544
Benefits of an IDS in a Network	545
Reduce the Risk of a Systems Compromise	545
Identifying Errors of Configuration	546
Optimize Network Traffic	546
Documenting Existing Threat Levels for Planning or Resource Allocation	546

Distributed Denial of Service Attacks

Recently, distributed denial of service (DDoS) attacks have become more common. Typical tools used by attackers are Trinoo, TFN, TFN2K and Stacheldraht ("barbed wire" in German). How does a DDoS attack work? The attacker gains access to a Client PC. From there, the cracker can use tools to send commands to the nodes. These nodes then flood or send malformed packets to the victim. Coordinated traceroutes from several sources are used to probe the same target to construct a table of routes for the network. This information is then used as the basis for further attacks.

Changing User Behavior	547
Deploying an IDS in a Network	547
Sensor Placement	547
Difficulties in Deploying an IDS	548
IDS Tuning	549
Tuning	551
Turn It Up	551
Tone It Down	552
Network Attacks and Intrusions	552
Poor Network Perimeter/Device Security	553
Packet Decoders	553
Scanner Programs	554
Network Topology	554
Unattended Modems	555
Poor Physical Security	556
Application and Operating Software	
Weaknesses	556
Software Bugs	556
Getting Passwords—Easy Ways of Cracking Programs	557
Human Failure	557
Poorly Configured Systems	557
Information Leaks	558
Malicious Users	558
Weaknesses in the IP Suite of Protocols	558
Layer 7 Attacks	559
Layer 3 and Layer 4 Attacks	561
The Cisco Secure Network Intrusion Detection System	565
What Is the Cisco Secure Network Intrusion Detection System?	566
The Probe	566
The Director	566
The Cisco Secure Policy Manager	567
The Post Office	567
Before You Install	569

**Network Security
Management**

To overcome security management issues, Cisco has developed several security management applications including these:

- PIX Device Manager
- CiscoWorks2000 Access Control Lists Manager
- Cisco Secure Policy Manager
- Cisco Secure Access Control Server

Director and Probe Setup	570
Director Installation	570
Director Configuration	571
Probe Installation	571
Completing the Probe Installation	572
General Operation	573
nrConfigure	574
Configuring Logging from a Router to a Sensor	574
Configuring Intrusion Detection on Sensors	574
Customizing the NSDB	575
Upgrading the NSDB	576
The Data Management Package	576
An E-mail Notification Example	576
Cisco IOS Intrusion Detection Systems	577
Configuring Cisco IOS IDS Features	578
Associated Commands	582
Summary	583
Solutions Fast Track	587
Frequently Asked Questions	589

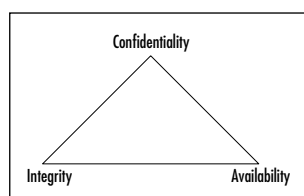
Chapter 14 Network Security Management 593

Introduction	594
PIX Device Manager	594
PIX Device Manager Overview	595
PIX Device Manager Benefits	595
Supported PIX Firewall Versions	596
PIX Device Requirements	596
Requirements for a Host Running the PIX Device Management Client	597
Using PIX Device Manager	598
Configuring the PIX Device Manager	598
Installing the PIX Device Manager	599
Configuration Examples	606
Connecting to the PIX with PDM	608

Configuring Basic Firewall Properties	609
Implementing Network Address Translation	612
Allowing Inbound Traffic from External Sources	615
CiscoWorks2000 Access Control List Manager	617
ACL Manager Overview	617
ACL Manager Device and Software Support	619
Installation Requirements for ACL Manager	619
ACL Manager Features	620
Using a Structured Access Control List Security Policy	621
Decreasing Deployment Time for Access Control Lists	621
Ensure Consistency of Access Control Lists	621
Keep Track of Changes Made on the Network	622
Troubleshooting and Error Recovery	622
The Basic Operation of ACL Manager	623
Using Templates and Defining Classes	623
Using DiffViewer	624
Using the Optimizer and the Hits Optimizer	625
Using ACL Manager	626
Configuring the ACL Manager	626
Installing the ACL Manager and Associated Software	627
Configuration Example: Creating ACLs with ACLM	628
Cisco Secure Policy Manager	632
Cisco Secure Access Control Server	633
Overview of the Cisco Secure Access Control Server	633

Understanding Security Fundamentals and Principles of Protection

Security protection starts with the preservation of the *confidentiality*, *integrity*, and *availability* (CIA) of data and computing resources. These three tenets of information security, often referred to as “The Big Three,” are sometimes represented by the CIA triad.



Benefits of the Cisco Secure Access Control Server	634
Authentication	634
Authorization	635
Accounting	636
Installation Requirements for the Cisco Access Control Server	636
Features of Cisco Secure ACS	637
Placing Cisco Secure ACS in the Network	638
Cisco Secure ACS Device and Software Support	639
Using Cisco Secure ACS	641
Installing Cisco Secure ACS Configuration	642
Configuration Example: Adding and Configuring a AAA Client	643
Summary	646
Solutions Fast Track	646
Frequently Asked Questions	648

Chapter 15 Looking Ahead: Cisco Wireless Security 649

Introduction	650
Understanding Security Fundamentals and Principles of Protection	651
Ensuring Confidentiality	651
Ensuring Integrity	653
Ensuring Availability	654
Ensuring Privacy	655
Ensuring Authentication	655
Extensible Authentication Protocol (EAP)	659
An Introduction to the 802.1x Standard	663
Per-Packet Authentication	666
Cisco Light Extensible Authentication Protocol	667

Configuration and Deployment of LEAP	669
Ensuring Authorization	670
MAC Filtering	672
What Is a MAC Address?	672
Where in the Authentication/Association	
Process Does MAC Filtering Occur?	673
Determining MAC Filtering Is Enabled	674
MAC Spoofing	674
Ensuring Non-Repudiation	675
Accounting and Audit Trails	678
Using Encryption	679
Encrypting Voice Data	680
Encrypting Data Systems	681
Reviewing the Role of Policy	681
Identifying Resources	683
Understanding Classification Criteria	685
Implementing Policy	686
Addressing the Issues with Policy	689
Implementing WEP	691
Defining WEP	691
Creating Privacy with WEP	692
The WEP Authentication Process	693
WEP Benefits and Advantages	693
WEP Disadvantages	694
The Security Implications of	
Using WEP	694
Implementing WEP on the Cisco	
Aironet AP 340	694
Exploiting WEP	695
Security of 64-Bit versus 128-Bit Keys	696
Acquiring a WEP Key	696
Addressing Common Risks and Threats	697
Finding a Target	698
Finding Weaknesses in a Target	698
Exploiting Those Weaknesses	700
Sniffing, Interception, and Eavesdropping	701

Defining Sniffing	701
Sample Sniffing Tools	701
Sniffing Case Scenario	702
Protecting Against Sniffing and Eavesdropping	704
Spoofing and Unauthorized Access	704
Defining Spoofing	704
Sample Spoofing Tools	705
Protecting Against Spoofing and Unauthorized Attacks	706
Network Hijacking and Modification	706
Defining Hijacking	707
Sample Hijacking Tools	708
Hijacking Case Scenario	708
Protection against Network Hijacking and Modification	708
Denial of Service and Flooding Attacks	709
Defining DoS and Flooding	709
Sample DoS Tools	710
DoS and Flooding Case Scenario	710
Protecting Against DoS and Flooding Attacks	711
Summary	712
Solutions Fast Track	713
Frequently Asked Questions	718
Index	721



Foreword

Today's Security Environment

Information security has become an extremely important topic for everyone over the past few years. In today's environment the number of touch points between an organization's information assets and the outside world has drastically increased: millions of customers can interact via a Web site, thousands of employees and partners may connect using Virtual Private Networks (VPNs), and dozens of critical applications may be completely outsourced to application service providers (ASPs). The deployment of wireless LANs also means that users no longer even need a physical connection to the network to gain access.

In addition to an explosion of touch points, we are faced with an infinitively complex and rapidly changing web of networks, applications, systems, client software, and service providers. Under these circumstances, absolute security cannot be guaranteed since it's impossible to test the security implications of every configuration combination of hardware and software under every set of conditions.

A critical strategy for reducing security risk is to practice defense-in-depth. The essence of defense-in-depth is to create an architecture that incorporates multiple layers of security protection. Recognizing this requirement, Cisco Systems has placed a high priority on security and offers a wide range of stand-alone and integrated security products. *Managing Cisco Network Security, Second Edition* is important to anyone involved with Cisco networks, as it provides practical information on using a broad spectrum of Cisco's security products. Security is not just for "security geeks" anymore. It is an absolute requirement of all network engineers, system administrators, and other technical staff to understand how best to implement security.

About This Book

In addition to providing a general understanding of IP network security and the threat environment, this book offers detailed and practical information on how to use Cisco's suite of security products. Callisma's contributing authors are industry experts with real world implementation experience. Each chapter will guide you through a particular aspect of security, from the family of PIX firewalls, to the Cisco Secure Intrusion Detection System (IDS), to traffic filtering in IOS, to the Cisco Secure Policy Manager (CSPM). In reading this book, you will obtain a firm understanding of how to secure your Cisco network.

About Callisma

Callisma is setting a new standard for network consulting, helping today's enterprises and service providers design and deploy networks that deliver strategic business value. By providing its clients with a broad base of technical practices, a flexible, results-oriented engagement style, and the highest quality documentation and communication, Callisma delivers superior solutions—on time and on budget. Callisma practices include IP Telephony, Internetworking, Optical Networking, Operations Management, Project Management, and Security and Storage Networking. Callisma is headquartered in Silicon Valley, with offices located throughout the United States. For more information, visit the Callisma Web site at www.callisma.com or call 888-805-7075

—*Ralph Troupe*
President and CEO, Callisma