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

solutions@syngress.com

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

SYNGRESS®

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

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

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.

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.

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

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

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.

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.

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.

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.

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.

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.

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

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.

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.

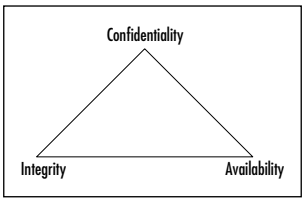
Network Security Management

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

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.



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 Network s (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