# About This Guide

## Introduction

Welcome to *Securing Your Network with the Cisco Centri Firewall*. This guide describes the "theory of operation" for your new security system—the concepts that are key to understanding the system and the way it is meant to be used. These concepts include security perimeters, security policies, the system's architecture, and countermeasures for potential security threats and vulnerabilities. This guide's primary purpose is to provide a strong foundation for understanding and using your Cisco Centri Firewall effectively.

This guide introduces the major components of and concepts behind your new security system. It explores why we created Cisco Centri Firewall and how it prevents various threats from affecting your organization's network assets. It delineates the core network security concepts around which the product was designed and built, and it defines the terminology and concepts that you should be familiar with when using the Cisco Centri Firewall.

This guide also introduces the user interface for the Cisco Centri Firewall, focusing on its graphic portrayal and organization of network components and its intuitive design that facilitates the development, application, and maintenance of security policies. The last chapter of this guide provides an overview of the process that you should follow to get the most out of your new security system and to help you plan its deployment.

With the exceptions of Chapter 1, "Overview of the Cisco Centri Firewall Product" and Appendix A, "Understanding TCP/IP," you should read each chapter in order as many discussions in later chapters rely upon terminology and concepts presented in earlier chapters. If you are unfamiliar with the TCP/IP protocol suite and how it works, you should read Appendix A first.

# Who Should Read This Guide

The intended audience of this guide is network administrators who want to understand the basic concepts behind the design and deployment of Cisco Centri Firewall. In addition, this guide can assist those professionals who are evaluating network security solutions and want to understand how the Cisco Centri Firewall product family distinguishes itself from other solutions, how it works, and how it should be used.

# How This Guide is Organized

This guide presents information following a general to specific structure, and it comprises the following chapters:

Chapter 1, “Overview of the Cisco Centri Firewall Product.” This chapter provides a general overview of the features provide by the Cisco Centri Firewall product.

Chapter 2, “Why You Need a Firewall.” This chapter describes the problems that firewalls attempt to address from a network security perspective. It defines common attack scenarios that firewalls are typically designed to prevent or disarm.

Chapter 3, “Evolution of the Firewall Industry.” This chapter provides background information on the firewall industry and introduces the four architectural models used to implement most modern-day firewalls. It also briefly discusses ease-of-administration issues within the firewall industry.

Chapter 4, “Understanding Security Policies.” This chapter defines the concept of perimeter networks and identifies the differences among trusted, untrusted, and unknown networks. It also explains how network security policies are used within Cisco Centri Firewall.

Chapter 5, “Inside the Cisco Centri Firewall.” This chapter details the key components of the security system and explains the roles and relationships that each component maintains within the system to provide a complete network security solution. It also details how Cisco Centri Firewall addresses the security issues identified in earlier chapters.

Chapter 6, “Using Cisco Centri Firewall to Protect Your Network.” This chapter provides an overview of the seven-step process that you perform to deploy the Cisco Centri Firewall product correctly and securely. It also provides worksheets that we encourage you to use when recording the information that you will need to install and configure your network security solution.

Appendix A, “Understanding TCP/IP.” This appendix provides the requisite background information on the TCP/IP protocol suite, as well as the reference model used to describe how firewalls work. It introduces the concept of a network protocol stack and various terms and definitions that are required as background material for understanding firewall architectures. Readers who are familiar with the TCP/IP protocol suite and its operation may ignore this appendix with no loss of understanding concerning this guide.

Appendix B, “Recommended Readings.” This appendix provides a list of publications that support this guide. These publications provide information on TCP/IP and networking, Windows NT security, network security concepts, and security policy development.

Appendix C, “Glossary.” The glossary defines the technical and application-specific terms used throughout this guide.

# Conventions Used in This Guide

The typographical conventions used throughout this guide are defined in Table 1:

**Table 1 Document Conventions**

| Convention | Meaning |
|---|---|
| *Italics* | Introduces new or important terminology, as well as variable input for commands. |
| `Script` | Denotes pathnames, file names, and example screen output. Also denotes Secure Script translations of security policy decision trees. |
| **Bold** | Identifies special terminology and options that should be selected during procedures. |

**Note** Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in the manual.

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data. Cautions are also used to identify potential security breaches.

# Where to Find Additional Information

This section identifies the various documents and document types provided as part of the Cisco Centri Firewall documentation set. This documentation set comprises three types of documents:

- COPY: hard copy books;
- HTML: HTML reference help; and
- HELP: Windows-based online help

*Securing Your Network with the Cisco Centri Firewall.* (COPY) This guide introduces you to the Cisco Centri Firewall. It provides a high-level overview of the major pieces of and concepts surrounding Cisco Centri Firewall and explains how the security system is intended to be used to protect your networks. It defines the terminology and networking concepts that you should be familiar with when using Cisco Centri Firewall and walks you through the basic process required to set up and deploy the security system.

*Cisco Centri Firewall Installation Guide.* (COPY) This guide identifies the hardware and software requirements of Cisco Centri Firewall. It also walks you through the install process in detail to ensure that you have an "up-and-running" system using the default services you enable during the install process.

*Understanding and Writing Security Policies.* (HTML) This guide describes the role of security policies within an organization and presents procedures for building network security policies using the Policy Builder security policy development environment. In addition, it explains how to apply security policies to your network objects to reduce the complexity of managing security policies.

*Using Cisco Centri Firewall to Protect Your Network.* (HTML) This guide provides an overview of the seven-step process that you perform to deploy any member of the Cisco Centri Firewall product family correctly and securely. It also provides links to additional reference material and the procedures that support each of the seven steps.

*Understanding Network Services.* (HTML) This guide explains how network services are constructed within Cisco Centri Firewall, how to define network services, network applications, and bundled applications.

*Understanding the CentriServer Node.* (HTML) This guide explains the administrative features associated with the Security Knowledge Base, including long-term storage of audit records and check-pointing operations.

*Understanding the CentriFirewall Node.* (HTML) This guide explains the administrative features associated with the Centri Firewall server, including exposed services, network adapter cards, routing rules, HTTP filter rules, and network address translation.

*Understanding User Accounts.* (HTML) This guide explains the in-line user authentication methods provided by Cisco Centri Firewall and provides a link for creating new accounts.

*Dialog and Field Reference.* (HELP) The WinHelp-based online information provides context-sensitive help for fields in panels and dialog boxes presented in the user interface. You can access What's This? help using the right-mouse button and dialog descriptions by selecting the Help button found on dialogs and property panels.

Additional HTML-based documentation will be provided as it becomes available. To see the complete list of HTML documentation, see Contents.html in the Centri\wwwroot directory.

For the latest information on Cisco Centri Firewall, please refer to www.cisco.com/centri. The Cisco Centri Firewall website includes product reviews, press releases, and frequently asked questions (FAQs), as well as training information and product and documentation updates as they become available. In addition, information related to using Cisco Centri Firewall more effectively will be posted to this site on an ongoing basis.

# CD-ROM Documentation

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

# Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

---