Introduction

This book focuses on the complete product line of Cisco firewall hardware: the PIX and ASA Security Appliance families and the Catalyst Firewall Services Module (FWSM). Of the many sources of information and documentation about Cisco firewalls, very few provide a quick and portable solution for networking professionals.

This book is designed to provide a quick and easy reference guide for all the features that can be configured on any Cisco firewall. In essence, an entire bookshelf of firewall documentation, along with other networking reference material, has been "squashed" into one handy volume.

This book covers only the features that can be used for stateful traffic inspection and overall network security. Although Cisco firewalls can also support VPN functions, those subjects are not covered here.

This book is based on the most current Cisco firewall software releases available at press time—ASA release 8.0(1) and FWSM release 3.2(1).

In the book, you will find ASA, PIX, and FWSM commands presented side-by-side for any specific task. The command syntax is shown with a label indicating the type of software that is running, according to the following convention:

- **ASA**—Refers to any platform that can run ASA release 7.0(1) or later. This can include the ASA 5500 family, as well as the PIX 500 family. For example, even though a PIX 535 can run a specific build of the ASA 8.0(1) code, the commands are still labeled "ASA" to follow the operating system being used.
- **PIX**—Refers to a PIX release 6.3.
- **FWSM**—Refers to FWSM release 3.1(1) or later.

If you are using an earlier version of software, you might find that the configuration commands differ slightly.

With the advent of the ASA platform, Cisco began using different terminology: firewalls became known as *security appliances* because of the rich security features within the software and because of the modular nature of the ASA chassis. This new terminology has been incorporated in this book where appropriate. However, the term *firewall* is still most applicable here because this book deals with both security appliances and firewalls embedded within Catalyst switch chassis. As you read this book, keep in mind that the terms *firewall* and *security appliance* are used interchangeably.

How This Book Is Organized

This book is meant to be used as a tool in your day-to-day tasks as a network or security administrator, engineer, consultant, or student. I have attempted to provide a thorough explanation of many of the more complex firewall features. When you better understand how a firewall works, you will find it much easier to configure and troubleshoot.

This book is divided into chapters that present quick facts, configuration steps, and explanations of configuration options for each Cisco firewall feature. The chapters and appendixes are as follows:

- **Chapter 1, "Firewall Overview"**—Describes how a Cisco firewall inspects traffic. It also offers concise information about the various firewall models and their performance.
- **Chapter 2, "Configuration Fundamentals"**—Discusses the Cisco firewall user interfaces, feature sets, and configuration methods.
- **Chapter 3, "Building Connectivity"**—Explains how to configure firewall interfaces, routing, IP addressing services, and IP multicast support.
- **Chapter 4, "Firewall Management"**—Explains how to configure and maintain security contexts, flash files, and configuration files; how to manage users; and how to monitor firewalls with SNMP.
- **Chapter 5, "Managing Firewall Users"**—Covers the methods you can use to authenticate, authorize, and maintain accounting records for a firewall's administrative and end users.
- **Chapter 6, "Controlling Access Through the Firewall"**—Describes the operation and configuration of the transparent and routed firewall modes, as well as address translation. Other topics include traffic shunning and threat detection.
- **Chapter 7, "Inspecting Traffic"**—Covers the Modular Policy Framework, which is used to define security policies that identify and act on various types of traffic. The chapter also discusses the application layer inspection engines that are used within security policies, as well as content filtering.
- **Chapter 8, "Increasing Firewall Availability with Failover"**—Explains firewall failover operation and configuration, offering high availability with a pair of firewalls operating in tandem.
- **Chapter 9, "Firewall Load Balancing"**—Discusses how firewall load balancing works and how it can be implemented in a production network to distribute traffic across many firewalls in a firewall farm.
- **Chapter 10, "Firewall Logging"**—Explains how to configure a firewall to generate an activity log, as well as how to analyze the log's contents.
- **Chapter 11, "Verifying Firewall Operation"**—Covers how to check a firewall's vital signs to determine its health, how to verify its connectivity, and how to observe data that is passing through it.
- **Chapter 12, "ASA Modules"**—Discusses the Security Services Modules (SSMs) that can be added into an ASA chassis, along with their basic configuration and use.

- **Appendix A, "Well-Known Protocol and Port Numbers"**—Presents lists of well-known IP protocol numbers, ICMP message types, and IP port numbers that are supported in firewall configuration commands.
- **Appendix B, "Security Appliance Logging Messages"**—Provides a quick reference to the many logging messages that can be generated from an ASA, PIX, or FWSM firewall.

How to Use This Book

The information in this book follows a quick-reference format. If you know what firewall feature or technology you want to use, you can turn right to the section that deals with it. The main sections are numbered with a quick-reference index that shows both the chapter and the section (for example, 3-3 is Chapter 3, section 3). You'll also find shaded index tabs on each page, listing the section number.

Feature Description

Each major section begins with a detailed explanation of or a bulleted list of quick facts about the feature. Refer to this information to quickly learn or review how the feature works.

Configuration Steps

Each feature that is covered in a section includes the required and optional commands used for common configuration. The difference is that the configuration steps are presented in an outline format. If you follow the outline, you can configure a complex feature or technology. If you find that you do not need a certain feature option, skip over that level in the outline.

In some sections, you will also find that each step in a configuration outline presents the commands from multiple firewall platforms side-by-side in a concise manner. You can stay in the same configuration section no matter what type or model of firewall you are dealing with.

Sample Configurations

Each section includes an example of how to implement the commands and their options. Examples occur within the configuration steps, as well as at the end of a main section. I have tried to present the examples with the commands listed in the order you would actually enter them to follow the outline.

Many times, it is more difficult to study and understand a configuration example from an actual firewall because the commands are displayed in a predefined order—not in the order you entered them. Where possible, the examples have also been trimmed to show only the commands presented in the section.

Displaying Information About a Feature

Each section includes plenty of information about the commands you can use to show information about that firewall feature. I have tried to provide examples of this output to help you interpret the same results on your firewall.