Cisco Secure Internet Security Solutions

By Andrew G. Mason, Mark J. Newcomb

Publisher : Cisco Press
Pub Date : May 30, 2001
ISBN : 1-58705-016-1
Pages : 528

Must-have security strategies using Cisco's complete solution to network security.

- The only book to cover interoperability among the Cisco Secure product family to provide the holistic approach to Internet security
- The first book to provide Cisco proactive solutions to common Internet threats
- A source of industry-ready pre-built configurations for the Cisco Secure product range

Cisco Systems strives to help customers build secure internetworks through network design featuring its Cisco Secure product family. Cisco Secure Internet Security Solutions covers the basics of Internet security, and then concentrates on each member of the Cisco Secure product family, providing a rich explanation with examples of the preferred configurations required for securing Internet connections. The Cisco Secure PIX Firewall is covered in depth from an architectural point of view, and a reference of the PIX commands explains their use in the real world. Although Cisco Secure Internet Security Solutions is primarily concerned with Internet security, the information inside is also applicable to many general network security scenarios.

Copyright

Published by:

Cisco Press

201 West 103rd Street

Indianapolis, IN 46290 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Library of Congress Cataloging-in-Publication Number: 00-105222

Warning and Disclaimer

This book is designed to provide information about Cisco Secure. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Credits

Publisher

John Wait

Editor-in-Chief

John Kane

Cisco Systems Program Manager

Bob Anstey

Managing Editor

Patrick Kanouse

Development Editor

Andrew Cupp

Project Editor

Marc Fowler

Copy Editor

Ginny Kaczmarek

Technical Editors

Sean Convery

Masamichi Kaneko

Duane Dicapite

Joel McFarland

Steve Gifkins

Brian Melzer

Per Hagen

Ruben Rios

Jeff Hillendahl

Joe Sirrianni

Tom Hua

John Tiso

Team Coordinator

Tammi Ross

Book Designer

Gina Rexrode

Cover Designer

Louisa Klucznik

Production Team

Argosy

Indexer

Larry D. Sweazy

Corporate Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

http://www.cisco.com

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 526-4100

European Headquarters

Cisco Systems Europe

11 Rue Camille Desmoulins

92782 Issy-les-Moulineaux

Cedex 9

France

http://www-europe.cisco.com

Tel: 33 1 58 04 60 00

Fax: 33 1 58 04 61 00

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

http://www.cisco.com

Tel: 408 526-7660

Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems Australia, Pty., Ltd

Level 17, 99 Walker Street

North Sydney

NSW 2059 Australia

http://www.cisco.com

Tel: +61 2 8448 7100

Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at
www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Dedications

I would like to dedicate this book to my beautiful wife, Helen. Once again she had to put up with me coming home from work during the summer months and disappearing straight into my study to research and write this book. I thank her for being so patient and understanding, and giving me the space to write this book. I would also like to thank my wonderful daughter, Rosie, as she keeps me smiling throughout the day.

—Andrew Mason

This work is dedicated to my lovely wife, Jacqueline, without whose help I could never have accomplished as much as I have.

—Mark Newcomb

About the Authors

Andrew G. Mason, CCIE #7144, CCNP Security, and CCDP, is the CEO of CCStudy.com Limited (www.ccstudy.com), a United Kingdom-based Cisco Premier Partner specializing in Cisco consulting for numerous United Kingdom-based companies. The CCStudy.com web site is a fast-growing online Cisco community for all of the Cisco Career Certifications.

Andrew has 10 years of experience in the network industry and currently is consulting for Energis-Squared, the largest ISP in the United Kingdom. He is involved daily in the design and implementation of complex secure hosted solutions, using products from the Cisco Secure product range.

Mark J. Newcomb, CCNP Security and CCDP, is a senior consulting network engineer for Aurora Consulting Group (www.auroracg.com), a Cisco Premier Partner located in Spokane, Washington, USA. Mark provides network design, security, and implementation services for clients throughout the Pacific Northwest.

Mark has more than 20 years of experience in the microcomputer industry. His current projects include designing secure communication systems for wireless devices and providing comprehensive security services to the banking industry.

About the Technical Reviewers

Sean Convery is a network architect in Cisco's VPN and Security business unit. He has been at Cisco for three years. Prior to that he held positions in both IT and security consulting during his six years in the network security industry.

Steve Gifkins is a CCIE and CCSI of four and five years, respectively. He is based in the United Kingdom, where he runs his own independent Cisco-only consulting and training business. He is married with no children, and his hobbies include anything to do with outdoor life. Having retired with a knee injury from playing active sports such as squash, rugby, and soccer, he has taken up new hobbies in horse eventing and show jumping. In addition, he enjoys skiing and hill scrambling.

Brian Melzer, CCIE #3981, is an Internetwork Solutions Engineer for ThruPoint, Inc., out of their Raleigh, North Carolina, USA office. He has worked as a consultant for ThruPoint since September of 2000. ThruPoint is a global networking services firm and one of the few companies selected as a Cisco Systems Strategic Partner. Before working for ThruPoint, he spent five years working for AT&T Solutions on design and management of outsourcing deals

involving Fortune 500 clients. As a member of the Wolfpack, Brian received his undergraduate degree in electrical engineering and his master's degree in management at North Carolina State University.

John Tiso, CCIE #5162, is one of the chief technologists of NIS, a Cisco Systems Silver Partner. He has a bachelor's degree from Adelphi University, Garden City, New York. John also holds the CCDP certification, the Cisco Security specialization, the Cisco Voice Access specialization, and Sun Microsystems, Microsoft, and Novell certifications. John can be reached by e-mail at johnt@jtiso.com.

Acknowledgments

I would like to thank Mark Newcomb for working on this book with me. We live at different ends of the world and have only met once, but still have built a long-lasting friendship. My thanks also go out to John Kane, Andrew Cupp, and the rest of the Cisco Press team for pulling all of this together and providing an editorial service that is second to none. The technical reviewers, John Tiso, Brian Melzer, and Steve Gifkins, helped us both a lot with the technical direction of the text, thanks to you all. I would like to thank Sean Convery and Bernie Trudel for allowing us to include their excellent white paper as an invaluable reference in this book.

Finally, I would like to thank Sean Convery, Duane Dicapite, Per Hagen, Jeff Hillendahl, Tom Hua, Masamichi Kaneko, Joel McFarland, Ruben Rios, and Joe Sirrianni. This group of Cisco employees provided helpful feedback that immensely improved the quality of this book.

—Andrew Mason

As with all works of any consequence, this book was not simply the work of two authors. There were a great number of individuals behind the scenes that made this work a reality. I would like to list a few.

I want to acknowledge the technical reviewers, Steve Gifkins, Brian Melzer, and John Tiso, all superior engineers. These three individuals showed us where we did not cover enough material, showed us where we were unclear, and provided a large number of suggestions that added to the quality of this work. Their efforts are truly appreciated.

I thank Andrew Cupp and John Kane at Cisco Press for their ceaseless pursuit of the best possible work. They, along with many others at Cisco Press, have provided us with everything necessary to successfully complete this book.

I would also like to express my gratitude to Sean Convery and Bernie Trudel for letting us use their Cisco SAFE white paper as a reference in this book.

I want to thank Sean Convery, Duane Dicapite, Per Hagen, Jeff Hillendahl, Tom Hua, Masamichi Kaneko, Joel McFarland, Ruben Rios, and Joe Sirrianni, all from Cisco, for their time and very helpful suggestions.

Finally, I want to thank Andrew Mason for all of his work on this book. Even though we live on opposite sides of the world, I consider him one of my best friends.

—Mark Newcomb

Introduction

The Internet is a core business driver for many large corporations. Along with the expanded business, however, come security issues. Recent news headlines often feature articles about large e-commerce sites getting hacked, with potentially disastrous results.

Cisco Systems strives to help customers build secure internetworks through network design that features its Cisco Secure product family. At present, no available publication deals with Internet security from a Cisco perspective, using the Cisco Secure product family. This book covers the basics of Internet security and then concentrates on each member of the Cisco Secure product family, providing a rich explanation with examples of the preferred configurations required for securing Internet connections.

The book starts by explaining the threats posed by the Internet and progresses to a complete working explanation of the Cisco Secure product family. The individual components of the Cisco Secure product family are discussed in detail, with advice given about how to configure each individual component to meet the requirements of the situation. The Cisco Secure PIX Firewall is covered in-depth, from presenting an architectural point of view to providing a reference of the common PIX commands and their use in the real world. Although the book is concerned with Internet security, it is also viable for use in general network security scenarios.

Audience

Cisco Secure Internet Security Solutions is for network engineers and network designers. The primary audience is network engineers and network designers responsible for the corporate Internet connection or the installation of Cisco Secure products. The secondary audience is other networking staff members that have an interest in security or Cisco Secure products in relation to their specific corporate environment.

Also, CCIE and CCDP/CCNP candidates will take interest in the title to improve their Internet security skills.

The book should be read and used by an intermediate to advanced reader. Because of the unique content, industry experts could reference this book.

Audience Prerequisites

The content in this book assumes that the reader is familiar with general networking concepts and terminology. This includes a thorough understanding of the network

protocol TCP/IP, and a familiarity of the topics covered in the Cisco Press books *Internetworking Technologies Handbook* and *IP Routing Fundamentals*.

What Is Covered

The book is organized into 11 chapters and one appendix:

- **Chapter 1 "Internet Security"—** This chapter provides a historical overview of the Internet and the growing number of risks that are associated with it.
- **Chapter 2 "Basic Cisco Router Security"—** This chapter looks at Cisco routers and the related security threats and vulnerabilities from an Internet point of view. Sample configurations and tips are provided for implementation on your corporate Internet routers.
- **Chapter 3 "Overview of the Cisco Security Solution and the Cisco Secure Product Family"—** This chapter provides an overview of the Cisco Security Solution and the Cisco Secure product range. The following six chapters look at each device in more detail.
- **Chapter 4 "Cisco Secure PIX Firewall"—** This chapter covers the Cisco Secure PIX Firewall. A technical overview of the PIX is provided, along with a configuration guide and sample configurations based against a case study.
- **Chapter 5 "Cisco IOS Firewall"—** This chapter looks at the Cisco IOS Firewall. Sample configurations are provided, and the major technologies are explained.
- **Chapter 6 "Intrusion Detection Systems"—** This chapter looks at one of the latest and most emergent security technologies, intrusion detection. It gives a brief explanation of the various types of intrusion detection systems, and then provides configurations for both a Cisco router and a Cisco Secure PIX Firewall based on perimeter intrusion detection.
- **Chapter 7 "Cisco Secure Scanner"—** This chapter covers the Cisco Secure Scanner. A brief explanation of network scanning and its uses, good and bad, is provided before looking in-depth at the offering from Cisco, the Cisco Secure Scanner.
- **Chapter 8 "Cisco Secure Policy Manager (CSPM)"—** This chapter covers the Cisco Secure Policy Manager. The CSPM provides a centralized management platform for an enterprise network that incorporates Cisco routers running the Cisco IOS Firewall and Cisco Secure PIX Firewalls. This chapter provides a sample installation and configuration of CSPM.
- **Chapter 9 "Cisco Secure Access Control Server (ACS)"—** This chapter looks at the Cisco Secure Access Control Server and its uses within an internetwork. Configuration guidelines are provided for both the network access server (NAS) and the Cisco Secure ACS server component.
- **Chapter 10 "Securing the Corporate Network"—** This chapter looks at a common corporate network and identifies the risks associated with external connections. Numerous tips and configuration solutions are provided to overcome the associated risks.

- **Chapter 11 "Providing Secure Access to Internet Services"—** This chapter focuses on Internet services and the protection that can be offered to them. The chapter is written with servers hosted either at an ISP or on the corporate DMZ in mind. Each Internet service is looked at individually, and potential vulnerabilities and remedies are proposed.
- **Appendix A "Cisco SAFE: A Security Blueprint for Enterprise Networks"—** The principle goal of SAFE, Cisco's secure blueprint for enterprise networks, is to provide best practice information to interested parties on designing and implementing secure networks. SAFE serves as a guide to network designers considering the security requirements of their networks. SAFE takes a defense-in-depth approach to network security design. This type of design focuses on the expected threats and their methods of mitigation, rather than on "put the firewall here, put the intrusion detection system there" instructions. This strategy results in a layered approach to security, where the failure of one security system is not likely to lead to the compromise of network resources. SAFE is based on Cisco products and those of its partners.

Command Syntax Conventions

Command syntax in this book conforms to the following conventions:

- Commands, keywords, and actual values for arguments are **bold.**
- Arguments (which need to be supplied with an actual value) are *italic.*
- Optional keywords or arguments (or a choice of optional keywords or arguments) are in brackets, [ ].
- Choice of mandatory keywords or arguments is in braces, { }.

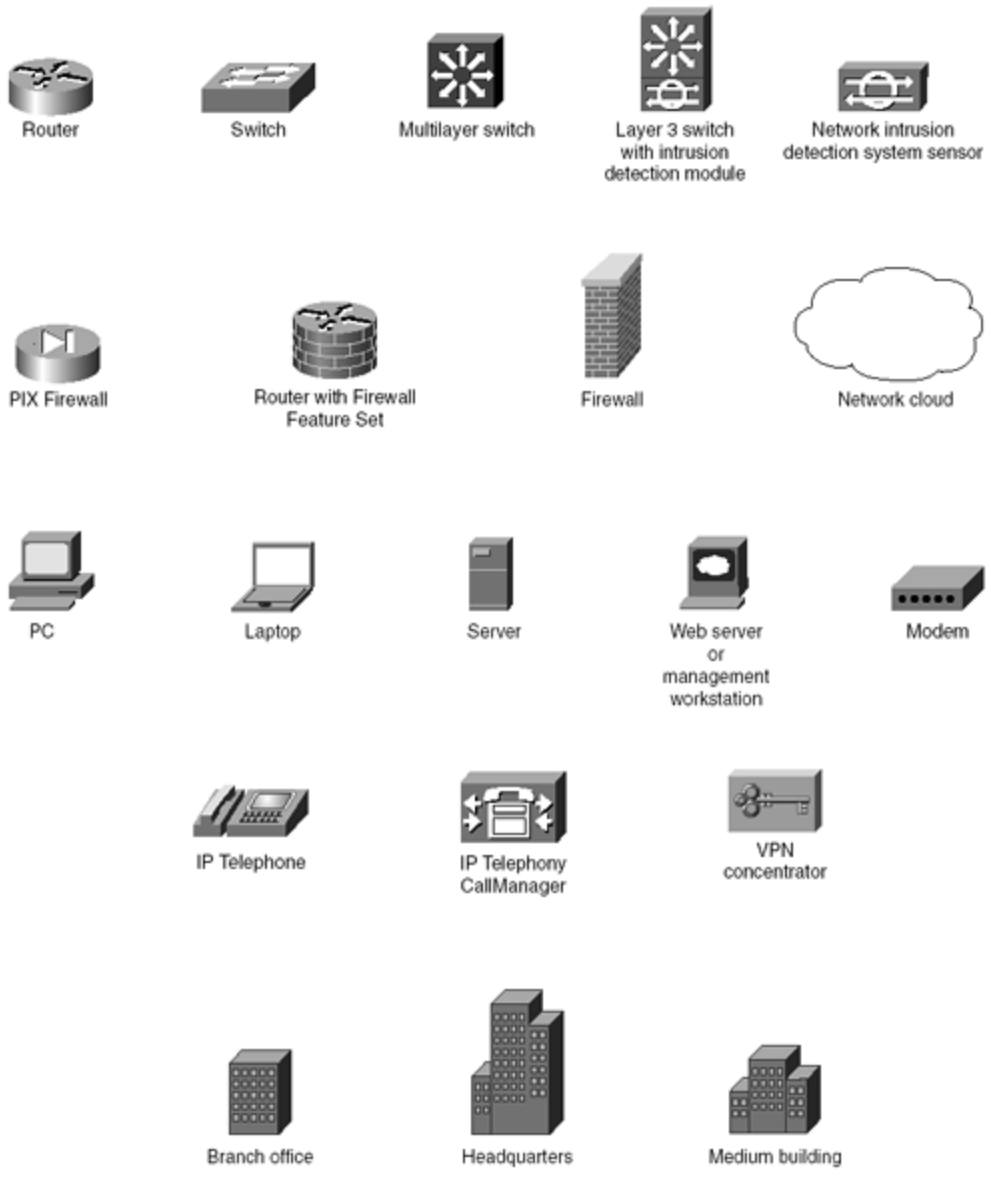
NOTE

Note that these conventions are for syntax only. Actual configurations and examples do not follow these conventions.

Device Icons Used in the Figures

Figure I-1 contains a key of the most important device icons used in the figures in this book.

Figure I-1. Device Icon Key



Part I: Internet Security Fundamentals

Chapter 1. Internet Security

This chapter contains the following sections:

- Internet Threats
- Network Services
- Security in the TCP/IP Suite
- Denial of Service (DoS) Attacks
- Creating a Corporate Security Policy
- Summary
- Frequently Asked Questions
- Glossary

This chapter introduces some of the basics of network security. It starts with a brief description of some of the most common forms of attacks. Next, the chapter describes the characteristics of several types of network devices.

The Cisco Secure IOS software is specifically designed to prevent attacks from affecting your network. Cisco Secure provides the highest levels of protection from unauthorized access, denial of service (DoS) attacks, man-in-the-middle attacks, and many other common methods used either to deny service or to obtain unauthorized information. The Cisco Secure IOS relies on a number of configuration techniques, hardware solutions, and technologies, including the Adaptive Security Algorithm (ASA). These provide the best security available to the network administrator today.

As technologies evolve, Cisco continuously refines its hardware and software solutions to remain on the cutting edge of network security. This book explores the methods of protecting the network that are available through use of the Cisco Secure solutions.

To set the foundations necessary for preventing attacks, the first chapter covers the format of several protocols, including Transmission Control Protocol (TCP), Internet Protocol (IP), Address Resolution Protocol (ARP), and User Datagram Protocol (UDP). The more common forms of DoS attacks are then examined. Specific techniques for dealing with DoS attacks are provided in later chapters.

This chapter concludes by examining the need for and use of a corporate security policy.

Internet Threats

The Internet is a collection of privately and publicly owned hosts. Virtually anyone owning a computer is able to get onto the Internet. There are hundreds of thousands of individuals on the Internet at any given time. Although most of these individuals have no ill intentions, there are a number who, for one reason or another, choose to try and penetrate or disrupt services on corporate networks. Sometimes networks are attacked by a technique where an innocent third party is used to launch the attack. For example, an individual whose system has been infected by a worm inadvertently passes along this worm to all known e-mail contacts. This

book is designed to show the administrator how to design networks that are resistant to attack.

There are a number of ways that the data on a corporate network can be compromised. Among them are the following:

- **Packet sniffing—** In this method, the attacker uses a packet sniffer to analyze the data for sensitive information traveling between two sites. One example is to use a packet sniffer to discover username and password combinations.
- **IP address spoofing—** In this method, an attacker changes the source IP address of packets to pretend to be a trusted user or trusted computer.
- **Port scans—** This method determines the ports on a network device where a firewall listens. After the attacker discovers the weaknesses, attacks are concentrated on applications that use those ports. Port scans can be launched against firewalls, routers, or individual computers.
- **DoS attack—** The attacker attempts to block valid users from accessing a resource or gateway. This blockage is achieved by sending traffic that causes an exhaustion of resources.
- **Application layer attack—** This method attempts to exploit weaknesses in server software to obtain the permission of the account that runs an application or to limit use of the system through a DoS attack.
- **Trojan horse—** In this method, the user is made to run a malicious piece of software. The Trojan horse attack uses an apparently safe application or data packet to transport destructive data to the recipient. After the destructive data has reached its destination, the program or script launches, causing damage. Trojan horse attacks can exploit technologies such as HTML, Web browser functionality, and the Hypertext Transfer Protocol (HTTP). These attacks include Java applets and ActiveX controls to transport programs across a network or load them on user Web browsers.

Network Services

At this point, it is important for you to understand some security services available on networks. Each of these services is fully discussed later in this book. The following services are discussed within this chapter in a general manner. There is overlap among these services; for example, basic authentication services are included on all Cisco routers. Therefore, this section should be referred to only for general guidelines.

Router Services

Routers have two general ways of providing security services on a network. The first is through routing. If, for example, the administrator does not want any user to be able to send or receive from a given network, the administrator can simply set a static route for that network to go to the *null interface.* The administrator can also set up route mappings to dump certain protocols or individual ports to the null interface or to a nonexistent network.

Although this is a rudimentary way to protect a network, it is still effective in limited circumstances. The problem with relying on this technique is that it does not scale well in large installations; it is static and can be overcome by a persistent attacker. Most network administrators need more granularity in their security settings than simply to allow or disallow traffic to a network.

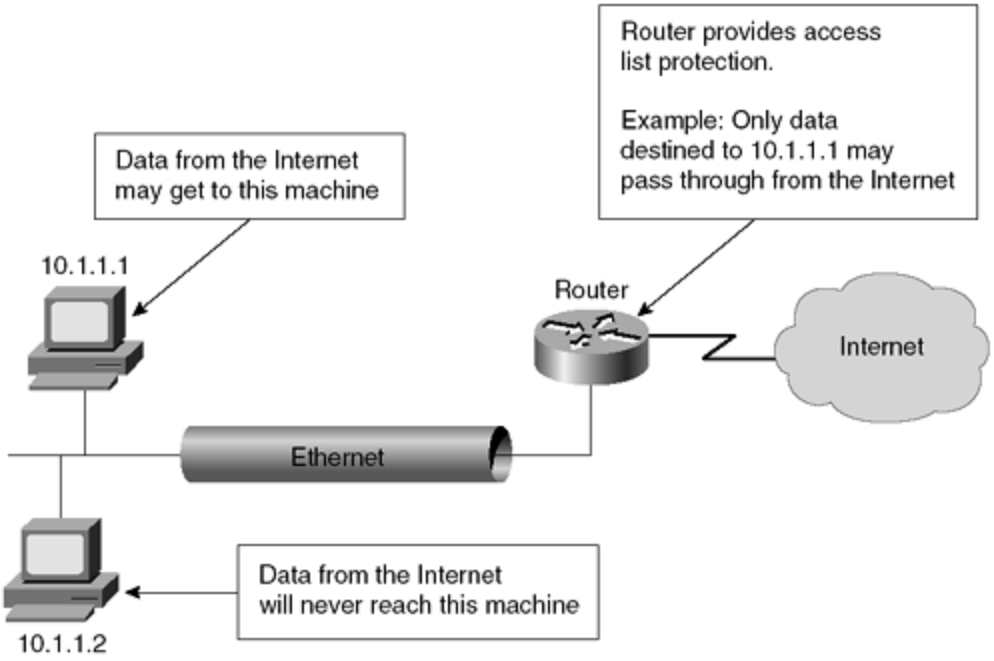
When more flexibility is needed, administrators rely on the second way that routers can provide security services on a network: access lists. Four main types of access lists are used on Cisco equipment:

- Standard
- Extended
- Reflexive
- Context-based Access Control (CBAC)

Standard access lists allow or deny packets based only on the source address of the packet. Extended access lists are more extensible, allowing filtering based on source or destination address, in addition to protocol, ports used, and whether the connection is already established.

Reflexive access lists dynamically change in response to outgoing requests for data. As a local host establishes a connection by requesting data, the access list attached to the inbound interface changes to allow returning packets through. Once the session is closed, returning packets are again denied access. Context-based Access Control (CBAC) is used with a limited number of programs to allow ports to open and close dynamically based on the needs of that particular application. Figure 1-1 gives an example of basic router services. Each of these types of access lists will be thoroughly explored throughout this book.

Figure 1-1. Basic Router Services



Firewall Services

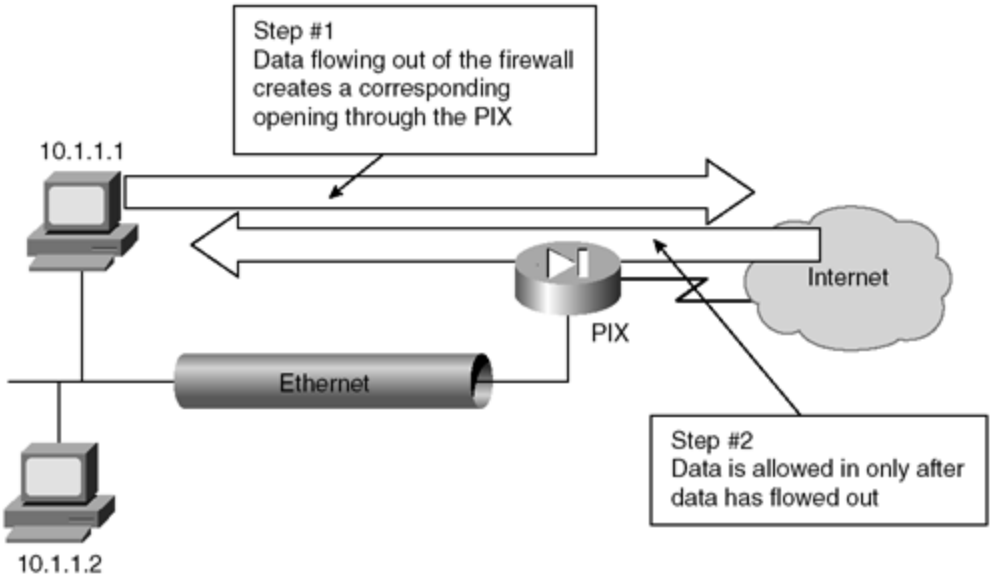
Firewall services tend to be more sophisticated than routing services. One example of this is the granularity of packet filtering on a firewall compared with a router without the firewall operating system.

On a router, it is not unusual to use the keyword **established** in extended access lists; this keyword is only useful while working with connection-oriented protocols. The keyword **established** does not allow for protocols such as UDP where there is no connection.

Additionally, the keyword **established** merely checks to ensure that the data packet is formatted to look like there has been a connection established. The Cisco Private Internet Exchange (PIX) Firewall, on the other hand, actually checks to make sure that data from a host has gone outbound before allowing data inbound.

The Cisco PIX Firewall that will be discussed in Chapter 4, "Cisco Secure PIX Firewall," filters both connection-oriented and connectionless protocols based on whether a host inside has requested data. This is only one example of many where the granularity of a firewall exceeds that available on a router. Figure 1-2 gives an example of firewall services.

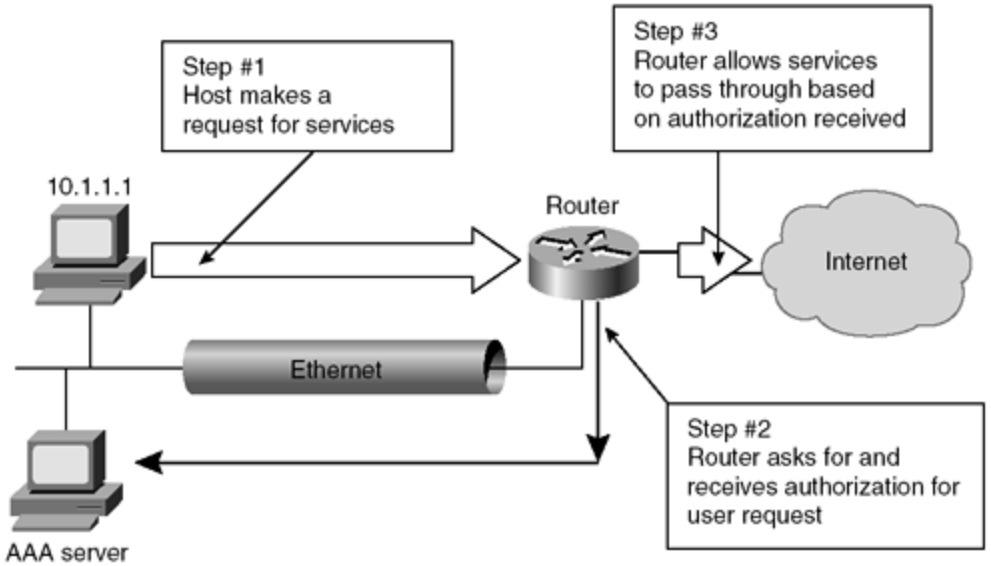
Figure 1-2. Firewall Services



Authentication and Authorization Services

Authentication refers to the process of ensuring that a claimed identity of a device or end user is valid. Authorization refers to the act of allowing or disallowing access to certain areas of the network based on the user, system, or program. Both services can be provided through either a Remote Access Dial-In User Service (RADIUS) or a Terminal Access Controller Access Control System (TACACS) server. Encryption is also available for authentication and can run on a firewall or a router. Figure 1-3 shows an example of authorization services implemented on a network.

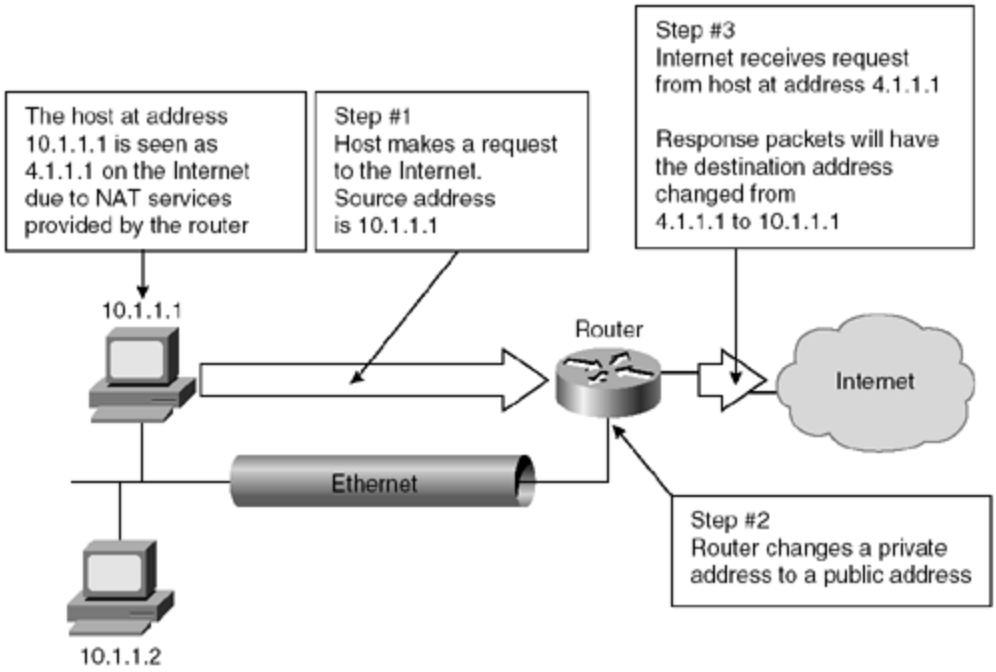
Figure 1-3. Authorization Services



Network Address Translation (NAT) Services

Many corporate networks choose to hide their local-area network addresses from all outside users. Network Address Translation (NAT) changes the local Layer 3 IP network addresses, generally called *private addresses,* to what are generally called *global* or *public addresses.* This translation can occur at a router or on a firewall. There are both security and practical advantages to using NAT. The security advantage is that attacks cannot be made directly to the end device, because the NAT device must translate each packet before forwarding that packet to or from the end device. The practical advantage is that NAT is easily done at both firewalls and routers, allowing the corporation to use a large number of public IP addresses without being forced to purchase more than a handful of private IP addresses. NAT is defined by RFC 1631. Figure 1-4 shows an example of a network employing NAT.

Figure 1-4. NAT Services

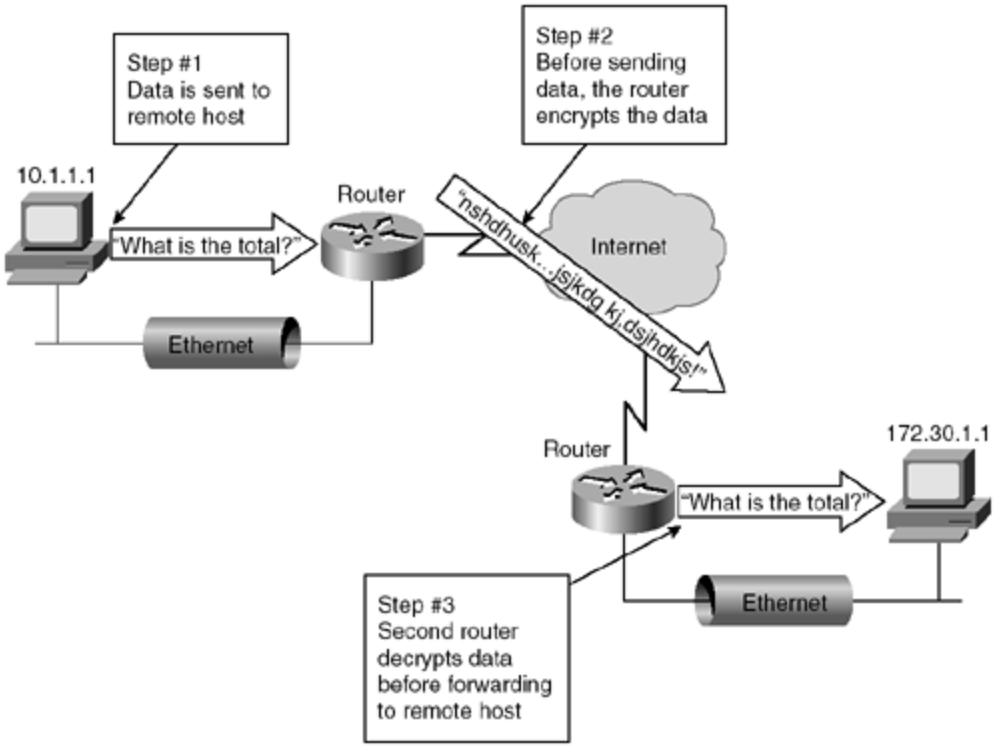


Encryption and Decryption Services

Encryption is the act of changing the content of data in a way that prevents recognition of that data without reversing the encryption process. The reversing of the encryption process is called decryption. Encryption and decryption services can be accomplished on end devices, routers, and firewalls.

A Virtual Private Network (VPN) is created when an encrypted connection is established through a public packet network. A VPN can be established between two hosts at different locations, between two networks of the same company, or between the networks of two different companies. Figure 1-5 shows how encryption services can secure data through the Internet.

Figure 1-5. Encryption Services



Proxy Services

A *proxy* is an intermediary. In networking, it is a device that sits between a local host and remote hosts. Acting as an intercept device, the proxy server accepts requests from the remote site as if the proxy server were in fact the local host. The proxy then sends its own request to the local host. The local host answers the proxy server, which then responds to the remote site's request. A proxy server isolates the local host from all requests made from remote sites. Unless the remote site is able to bypass the proxy server, the local hosts will never be subject to direct attack. Figure 1-6 shows proxy services in use on a network.