FIRST-STEP SERIES

Network Security first-step

Second Edition

Your first step into the world of network security

- No security experience required
- Includes clear and easily understood explanations
- Makes learning easy

Tom Thomas and Donald Stoddard

ciscopress.com

Network Security First-Step

Tom Thomas
Donald Stoddard

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Network Security First-Step

Tom Thomas
Donald Stoddard

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

First Printing December 2011

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58720-410-4

ISBN-10: 1-58720-410-X

Warning and Disclaimer

This book is designed to provide information about network security. 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 author 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.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests . For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S. please contact: **International Sales** international@pearsoned.com

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.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Senior Project Editor: Tonya Simpson

Editorial Assistant: Vanessa Evans

Cover Designer: Sandra Schroeder

Composition: Mark Shirar

Business Operation Manager, Cisco Press: Anand Sundaram

Manager Global Certification: Erik Ullanderson

Senior Development Editor: Christopher Cleveland

Copy Editor: Apostrophe Editing Services

Technical Editors: Phil Lerner, James Risler

Proofreader: Mike Henry

Indexer: Cheryl Lenser

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Authors

Tom Thomas, CCIE No. 9360, claims he never works because he loves what he does. When you meet him, you will agree!

Throughout his many years in the networking industry, Tom has taught thousands of people how networking works and the secrets of the life of a packet. Tom is the author or coauthor of 18 books on networking, including the acclaimed *OSPF Network Design Solutions*, published by Cisco Press and now in its second edition. Beyond his many books, Tom also has taught computer and networking skills through his roles as an instructor and training-course developer.

In addition to holding the Cisco Certified Internetwork Expert (CCIE) certification—the pinnacle of networking certifications—Tom holds Cisco CCNP Security, CCDA, and CCNA certifications and is a certified Cisco Systems instructor (CCSI). These certifications support his industry-proven, problem-solving skills through technical leadership with demonstrated persistence and the ability to positively assist businesses in leveraging IT resources in support of their core business. He has also completed his Master of Science degree in network architecture and is looking at a doctorate next.

Tom currently is the CIO of Qoncert, a Cisco Gold Partner in Southern Florida that has an affiliated arm known as CCPrep.com, a Cisco Learning Partner, where he provides strategic direction and a little hands-on for customers of all types.

Donald Stoddard began his career in information technology in 1998, designing networks and implementing security for schools in North Dakota and South Dakota. He then went on to design and implement Geographical Information Systems (GIS) for a firm in Denver, Colorado. While there, he earned his Bachelor of Science degree in computer information systems management from Colorado Christian University. From Colorado, he then moved south, learned the ins-and-outs of Cisco VoIP, and began working through designing and securing VoIP solutions throughout the southeast. Don holds Microsoft MCSA and Linux+ and Security+ certifications and is presently wading through the CISSP material.

Currently, Don works for the Department of the Navy as the Information Assurance Officer for one of the premier Navy research and development labs, where he provides certification and accreditation guidance for the various projects being developed for implementation and deployment.

About the Technical Reviewers

Phil Lerner, CISSP, GFSP, GAWN, CHS-IV, CGEIT, ECSA, C-EH is an industry veteran with 20 years of experience covering information security. Most recently, Phil was one of the few senior technical solutions architects at Cisco Systems focused on Data Center and Security. Phil's areas of expertise include sanctioned attack and penetration, digital and network forensics, wireless security, network security architecture, and policy work. Phil is also an adjunct professor at St. John's University in Queens, New York, teaching wireless security to all levels of undergraduate students. Phil earned his MS-CIS (Cyber Security) from Boston University in 2009 and is a frequent information security show speaker and trusted advisor to many large firms.

James Risler, CCIE No. 15412, is a systems engineer education specialist for Cisco. His focus is on security technology and training development. James has more than 18 years of experience in IP internetworking, including the design and implementation of enterprise networks. Prior to joining Cisco, James provided Cisco training and consulting for Fortune 500 companies and government agencies. He holds two bachelor's degrees from University of South Florida and is currently working on his MBA at the University of Tampa.

Dedications

Tom Thomas: How do you put into words the importance someone has in your life? Love and time strengthens the emotions until they are so powerful they make you want to express them in a meaningful way. I dedicate this book and this poem to my partner and soul mate, Kristi. During the course of this writing we found out together that we are having a child, twins in fact, and I welcome them into our life with open arms.

How do I begin to tell you how
lucky I am to have you in my life?
I'll start by saying what a gift you
gave me the day you became my wife.

In you I have truly found
An Angel who walks upon the ground.
You go beyond all limits for me
Just to show your love endlessly.
I could search my whole life through
And never find another "you."
You are so special that I wanted you to know
I truly, completely love you so.

You must be an angel without wings
To put up with all of my bothersome things
My anger, my love, my sometimes weary heart
What others hated about me you love
How could I not love you with all that I am
You are the steady I need for my trembling hand
You simply must be an angel without wings!

You're my best friend in the good times
and my rock in times of sorrow.
You're the reason for sweet yesterdays
and my promise for tomorrow.

I never thought I could feel this loved
until you became my wife.
You made this year and every year
the best one of my life.

Donald Stoddard: To AJ, my friend, my lover, my wife and queen. You have done the impossible…you've made me believe in myself again. From the moment I saw you across the room I knew you were the other half my soul longed for. Thank you for your love, support, and strength: ost min kis mik.

Acknowledgments

Tom Thomas: Special acknowledgments go to my good friend and the best editor, Chris Cleveland. His insight, abilities, and editorial comments take a rough manuscript and gave it life beyond what a simple nerd was able to envision. I have had the pleasure of working with Chris for many years, and I do not think I would ever want to write a book without his involvement.

As always, I would like to thank my technical editors for their friendship, insight, and awesome comments. Your knowledge helped to fine-tune my thoughts. I know that this book will help many people, and that was the goal. Thank you.

Don, we have been friends for years and you have always been a part of my life through the good and the bad; I am lucky to call you brother.

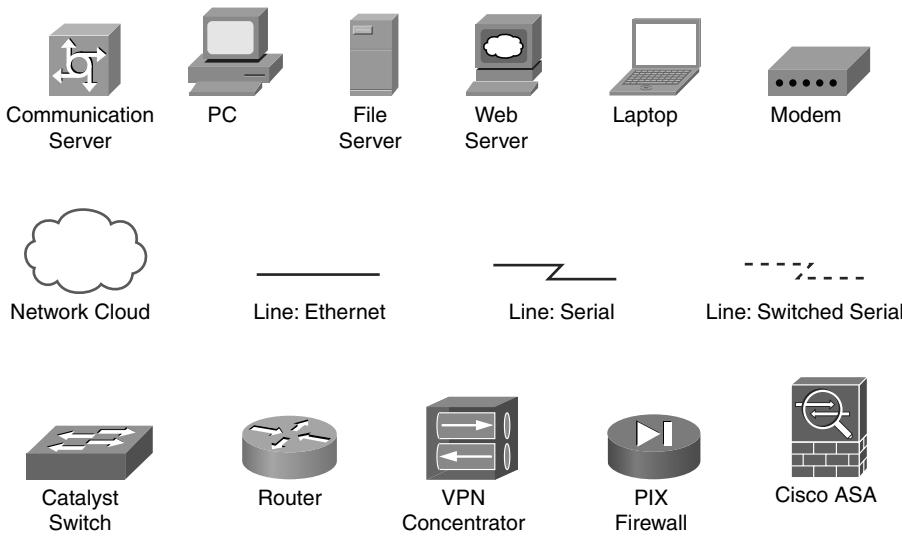
Donald Stoddard: I would like to extend a great thank-you for a great staff: Brett Bartow, Vanessa Evans, Chris Zahn, Chris Cleveland, and the technical reviewers (James Risler and Phil Lerner); without your patience and attention to detail this book would not be in the hands of readers today. Honestly, without you to guide, push, and correct, none of this is possible. Thank you all for your hard work and contributions throughout the long months from start to finish…truly this has been a marathon, not a sprint, and it has been a pleasure from the beginning.

And finally, I want to acknowledge a man who has guided my career and life for a long time. Tom, we've known each other for many years, and you have always been there to guide me when my career was derailed. You have been an inspiration. I will always remember you telling me to get focused. In fact, I think your words to me were, "…Don, you know what your problem is? You lack focus…." We've never been people who mince words, have we? I have focus now, I have a plan, and I have a career set before me all because of you. Thank you for your professional guidance and your friendship.

Contents at a Glance

Contents

Icons



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally, as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a show command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

This book was written to address the need for increased understanding of network security. Many texts are available on the subject, and they have value. However, many people and companies are now considering increasing their network security. Where do you start? Perhaps you want to deploy wireless and you need to ensure that it is secure. What single resource can provide you with a good overview of wireless security or firewalls, and so on? This book provides you with enough security information that you can leverage your newfound knowledge for your own benefit and for the benefit of your organization.

This book was written from the standpoint that every reader needs security but does not actually understand the risks and available techniques and possibilities. Each chapter addresses a specific aspect of an overall layered security model and enables you to see and understand why security for each area is needed, what you should consider, and how you should proceed.

Goals and Methods

The goal of this book is to provide a resource for every person concerned with security. Readers do not have to be networking professionals or CIOs to benefit from this book, although they can as well. It is our hope that all readers, from students to professionals, will benefit from this book.

You can explore each component of the network and verify how it can be securely deployed. When complex security technologies or concepts are encountered, they are explained with real-world examples and practical analogies. This book covers serious topics, but it should also be fun and easy to read. We have endeavored to meet this goal.

Who Should Read This Book?

This book was written with a broad audience in mind. Consider students who are hearing all about the importance of network security and want to focus on this area. This book helps them by providing an understanding of all the major components of securing a network. Perhaps you are a networking professional with in-depth expertise in routing and switching, and now you have been asked to deploy wireless (securely). This book provides a solid foundation upon which to explore the subject matter in more depth, while understanding the different components necessary for accomplishing your goals. You might even be a CIO who has been tasked with determining whether you should invest in an intrusion detection system (IDS). Perhaps you need to understand why this is needed, how it works, and when/where to use it.

Regardless of your expertise or role in the IT industry, this book has a place for you; it takes concepts and simplifies them to give you a solid foundation of understanding. What you do with that knowledge is up to you. This book might give you what you need, or it might be the first step in your journey.

How This Book Is Organized

Although you could read this book cover-to-cover, it is designed to be flexible and enable you to easily move between chapters and sections of chapters to cover only the material you need. If you do intend to read them all, the order in which they are presented is an excellent sequence.

Chapters 1 through 12 cover the following topics:

- **Chapter 1, "There Be Hackers Here":** Provides a glimpse into the mind and motivation of the individuals who attack your systems. This chapter covers tools, techniques, and attacks.

- **Chapter 2, "Security Policies":** Starts the defense-in-depth concept with the foundation of securing your network, which is the security policy. This chapter goes over roles and responsibilities within your organization, defines various corporate policies, and then goes over industry standards in use that you should be aware of. When you finish with the chapter, you will understand the role that polices play and one of the ways to prepare/respond to incidents.

- **Chapter 3, "Processes and Procedures":** Discusses common security operating processes and provides an overview of how to implement those processes and procedures from the ground up. This chapter also includes some industry best practices that are sure to help you and your organization.

- **Chapter 4, "Network Security Standards and Guidelines":** Goes into depth on the industry standards and guidelines for security implementation within your organization for Cisco, Microsoft, and Macintosh products. It then gives some best practices for implementing and configuring various security devices, such as your Cisco IOS, firewall/ASA, and intrusion prevention system (IPS).

- **Chapter 5, "Overview of Security Technologies":** Discusses the nuts and bolts of how to use security technologies from the most basic access control lists available in every router to global solutions such as PKI. Many of these technologies are used today without your needing to fully understand when or where they operate. After reading this chapter, you will understand the benefits of these technologies, where they operate, and some of the risks associated with them.

- **Chapter 6, "Security Protocols":** Looks at security from an encryption protocol implementation point of view. In addition, it considers the limitations of each covered security protocol because nothing is perfect.

- **Chapter 7, "Firewalls":** Covers firewalls and how they operate. It examines who needs a firewall and why they are an essential part of your network's defense.

- **Chapter 8, "Router Security":** If you have a network, you have a router; they have evolved over the years and are now effective security devices. This chapter discusses the expanded security capabilities of routers.

- **Chapter 9, "IPsec Virtual Private Networks (VPN)":** Discusses the role of VPNs and how they are reshaping the public Internet, encrypting all information that flows across the Internet. This includes the functional characteristics and operational parameters.

- **Chapter 10, "Wireless Security":** Discusses the hottest technology, wireless, and explains that all is not well in this IT nirvana. Hackers have also come here, and they bring a full complement of tools. Many think that wireless is safe and easy; this chapter ensures that those people become security conscious.

- **Chapter 11, "Intrusion Detection and Honeypots":** Discusses how you can detect a hacker's attempt to gain access into your network by implementing an intrusion detection system (IDS) or intrusion prevention system (IPS). It compares and contrasts the two so that you understand the role of each device. In addition, it discusses one of the ways to confuse a hacker—through the use of a honeypot.

- **Chapter 12, "Tools of the Trade":** Chapter 1 warns you that there be hackers . . . this chapter helps you understand what you are up against by discussing the various methods and tools used by hackers to infiltrate computer systems. This chapter then examines the available tools for identifying weaknesses in your network and the anatomy of a security audit, which is a crucial piece for ensuring that a network is secure and thus foiling the bad guy.

Chapter 7

Firewalls

"Courage is resistance to fear, mastery of fear—not absence of fear."—Mark Twain

By the end of this chapter, you should know and be able to explain the following:

- Who needs a firewall, and why firewalls are used to protect network resources
- How a firewall is a technological expression of your organization's written security policy
- When a DMZ is appropriate and the security benefits you gain by deploying a firewall with a DMZ

Answering these key questions enables you to understand the overall characteristics and importance of network security. By the time you finish this book, you will have a solid appreciation a firewall's role, its issues, how it works, and why it is so important to the security of your network.

The Internet is an exciting and wonderful place to browse and explore. It has been likened to the Wild West, The Great Frontier, and other grandiose achievements of mankind. In reality, the World Wide Web is merely a collection of routers and servers that make up the largest WAN in recorded history. This collection of networking gear provides mail servers, websites, and other information storage and retrieval systems and is all connected to the Internet and accessible to every person who is also connected. It has even been said that the Internet will contain the collective institutional knowledge of mankind, eventually. Entire books have been written on the Internet's potential and its impact on our lives—rest assured that this is not one of those books. But it does make you ponder just how much of your life is out there already that you might or might not be aware of.

We are concerned with a network's security, so we must ask what kinds of safeguards are in place to protect such an unbelievable amount of information. Is there some organization that polices the Internet much in the same way that law enforcement cruises the highways? How about a governmental agency that snoops around and double-checks every

possible device connected to the Internet? The answer to these questions is no; there is no unifying organization responsible for protecting the Internet.

The job of securing and protecting the gateways of the Internet's knowledge is left up to the person or persons responsible for the Internet connection and network hardware/software, such as the router, firewall, switch, server operating systems, application, and so on. This person or persons are tasked with the job to ensure that hackers (the bad guys) do not make a mess of the carefully stored and catalogued information in question. And just how can you protect a website, mail server, FTP server, or other information sources accessible from the Web?

The answer is one word—firewall. The sole purpose of these dedicated hardware devices is to provide security for your network. A *firewall* is a security device that sits on the edge of your Internet connection and functions as an Internet border security officer. It constantly looks at all the traffic entering and exiting your connection, waiting for traffic it can block or reject in response to an established rule. The firewall is the law and protection in the lawless wild wild web. A firewall is ever vigilant in its mission to protect the network resources connected to it.

The Internet has made so much information available to individual users as, over the years, access to this information has evolved from an advantage to an essential component for both individuals and businesses. However, making your information available on the Internet can expose critical or confidential data to attack from everywhere and anywhere in the world—the Internet is literally a worldwide network. This means that, when you connect to the Internet in Madison, Mississippi, you can be subject to attacks from Europe, Asia, and Russia—literally any device connected to the Internet anywhere on the earth, which is kind of disturbing. Firewalls can help protect both individual computers and corporate networks from hostile attacks from the Internet, but you must understand your firewall to correctly use it.

This 24-hour/365-day-a-year "electronic Robocop" has an important job: to keep the bad guys out and let the good guys get to the resources they need to do their jobs. Sounds simple, right? On paper, it sounds like a walk in the park, but in reality, properly configuring a firewall is far from easy.

In some cases, a badly configured or feature-inadequate firewall can be worse than no firewall at all. This is difficult to believe, isn't it? Nonetheless, it is true. This chapter dissects a firewall's duties to understand what makes a firewall operate and how it does its job.

Firewall Frequently Asked Questions

Before looking at the overall operation of a firewall, the following sections examine and answer some of the fundamental questions about them.

Who Needs a Firewall?

This is perhaps the most frequently asked security question. If you plan to connect to the Internet, you need a firewall. It does not matter whether you connect from home or your company connects—**you need a firewall, period!** The increased penetration of broadband Internet services to the home and their always-on Internet connections make home security even more important.

Why Do I Need a Firewall?

You read about security threats in the papers or hear about them on the evening news almost every day: viruses, worms, denial-of-service (DoS) attacks, hacking, and new vulnerabilities to your computer. For example, Code Red, Slammer, and other threats/vulnerabilities. are changing with the prevalence of malware and botnets.

It is no secret that hackers are out there, and they are out to get you. Often, you do not know who they are, but you do know where they are and where you do not want them to be (in your network). Like pirates of old who roamed the seas, hackers freely roam the open expanses of the Internet. You do not want them to enter your network and roam among the computers that connect to it, and that is where a firewall becomes a requirement.

You know that you must protect your network from these attackers, and one of the most efficient methods of protecting your network is to install a firewall. By default, any good firewall prevents network traffic from passing between the Internet and your internal network. This does not mean that the firewall can stop all traffic—that defeats the purpose of being on the Internet. It does mean that the firewall is configured to allow only web browsing (HTTP/port 80) to access it from the Internet. Along the way, the firewall provides Stateful Packet Inspection (SPI) rules to every incoming packet (as discussed previously in Chapter 2, "Security Policies.")

The alternative to having a firewall is allowing every connection into your network from anyone, anywhere—there wouldn't be any sort of packet inspection to determine whether an attack is hidden within one of the incoming packets. Not having a firewall is ill-advised and will make your organization wide open to everyone on the Internet.

Do I Have Anything Worth Protecting?

I often hear people say, "I understand that if I had something worth protecting, I would definitely need a firewall. However, I do not have anything an attacker would want, so why should I worry about a firewall?"

Networks and their resources are important to the way our society conducts business and operates. In practical terms, this means that there is value to your network and having it effectively operate. This increased role of networks means that you definitely have something worth protecting to some degree, as documented in the following list:

- **Downstream liability:** This sounds like a confused Bassmasters fishing show title, but it is perhaps the next big step in the legal evolution of the Internet. Downstream lia-

bility involves allegations that an attacker has taken control of a target computer (yours) and used it to attack a third party. Assume that it is your company's computer that has been compromised by a hacker. Your company's failure to protect its own systems has resulted in the damaging of a third party; the attacker used your computer as a weapon against the third party. Your company is therefore negligent due to lack of due diligence because it failed to protect against reasonable risks—specifically, no firewall was in place, or it was improperly configured, which is just as bad.

The prudent person's responsibility for security here is to use reasonable care. You can find a more detailed definition in Prosser, Wade, and Schwartz's *Cases and Materials on Torts*: "...requiring the actor to conform to a certain standard of conduct, for the protection of others against unreasonable risks." Who says Hollywood liberalism doesn't contribute to society?

- **Lost data:** You have probably heard the stories of companies that lost all their business data in hurricanes such as Katrina or the September 11 attacks, and many companies did not recover. What if your company experienced the same loss of data because you did not have a firewall and an attacker deleted your data because he could? What would happen to your business? Would it cost money to re-create everything? Would you suffer lost sales? Would you still be employed the next day?
- **Compromise confidential data:** Every organization has data it considers confidential and, if lost, might cause financial problems, legal difficulties, or extreme embarrassment. These things might be caused by the loss of customer information such as credit card numbers, secret plans for the new weight loss formula, or secret product plans that end up in the hands of a competitor. The list goes on, and when you have been hacked, you must assume the worst. Perhaps this is why most cybercrimes go unreported—it is embarrassing, and admitting to being hacked is a sign of weakness that could affect the reputation and brand of a company.
- **Network downtime:** Have you ever gone to an ATM machine or a grocery store to get cash and paid with your cash card in the swipe card readers? The networks enabling these devices to operate usually work fine; however, if they were not protected, an attacker might cause them to go down. The loss of revenue from these networks can quickly grow if they are unavailable. Downtime is the bane of any network, and a cost is always associated with these types of events.

Ultimately, everyone has something worth protecting, and failure to do so is ill-advised; it is just a matter of time before something happens. The next question is, "*What does a firewall do to protect my network?*"

What Does a Firewall Do?

A firewall examines traffic as it enters one of its interfaces and applies *rules* to the traffic—in essence, permitting or denying the traffic based on these rules. Figure 7-1 shows a firewall filters both inbound and outbound traffic.

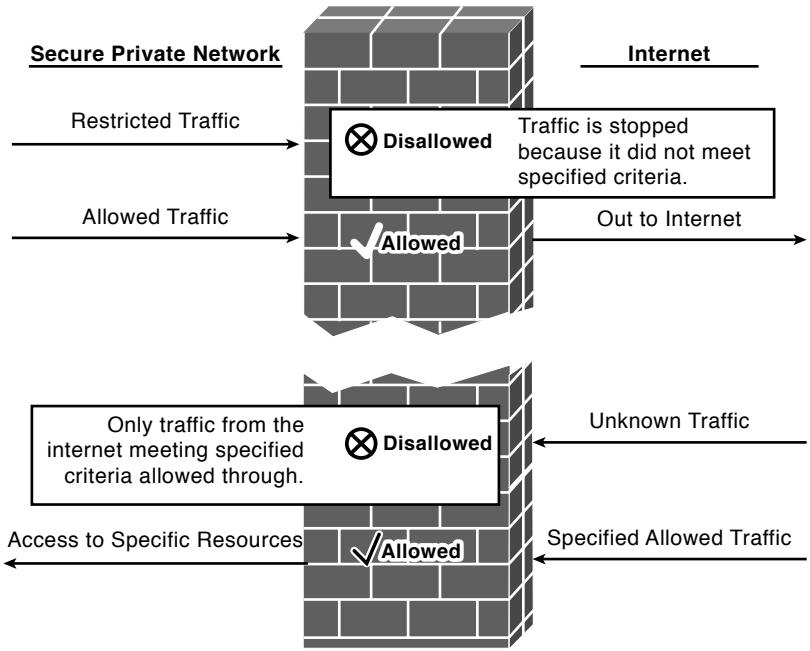


Figure 7-1 *Firewall in Operation*

Firewalls use access control lists (ACLs) to filter traffic based on source/destination IP addresses, protocol, and the *state* of a connection. In other words, normally you might not allow FTP/21 *into* your network (via the firewall), but if a user inside your network begins an FTP session out to the Internet, it is allowed because the session was *established* from inside the network. By default, firewalls trust all connections to the Internet (outside) from the trusted internal network (inside).

A firewall can also log connection attempts with certain rules that might also issue an alarm if they occur. Finally, firewalls enable you to perform Network Address Translation (NAT) from internal private IP addresses to public IP addresses. The section "Firewall Operational Overview" discusses the roles of a firewall; however, here you can tie the firewalls back to Chapter 2's security policy discussions by examining how a firewall enforces your security policy.

Firewalls Are "The Security Policy"

What kind of traffic is allowed into or out of your network? How do you secure your network against attacks? What is your security policy? What happens to the people who do not follow the security policy? Who is responsible for writing and updating the security policy?

All these questions are valid, and they all deserve answers. Having a network that connects to the Internet via a firewall is only the first step to security; because this book is

about first steps, this would be a perfect place to start. You should now know that the security policies form the basis of how firewall rules are determined and then implemented into a production network.

Do you remember the old saying, "No job is ever finished until the paperwork is done?" Well, no security solution is complete until you establish a written narrative of the rules and regulations that govern your organization's security posture. This written version of your security rules and regulations is known as a *security policy*. Now, this policy document is different in nature and scope than a security plan, so be sure that you understand what makes a policy unique from every other security document an organization maintains. And just what is it that makes a security policy different from a security plan? Drum-roll please....

PUNISHMENT! That is correct; a security policy includes what is permissible and what will happen to you if you do not live by the law of the land. If you do not follow the rules, you can be

- Fired or dismissed
- Demoted
- Demoted and fined
- Fired, dismissed, and demoted
- Demoted, dismissed, and even punked!
- All the above

All kidding aside, the security policy document spells out in clear language exactly what the regulations and expectations are, who enforces them, and what happens to you if you break them. A security policy is all about the consequences of user actions coupled with audit in the form of AAA usually.

Having said that, how can a firewall be the security policy? Simple—a firewall does what it does by following the rules configured by a network engineer or information security officer (ISO). These rules should perfectly align with a written narrative version found in the security policy document you have on your shelf, next to the box of CDs at the back of the server room or sitting useless in some manager's office. Grab that old dusty binder and check it out. You should see that the security policy document contains information and a listing of the network rules (refer to Chapter 2). The interesting thing is that all the rules in the policy document form the basis of what you must configure on the firewall.

Note Wait a minute! We have a hand in the front row. Yes...you with the confused look on your face. Your question is, "Why is the binder that contains the security policy so dusty and located in such an obscure place?" As strange as that might sound, go ahead and put your hand down. I will tell you the answer to that question is that most organizations either do not have a security policy set, or the set that they have is so old that it was written during a previous presidential administration.

The configuration rules entered on a firewall should perfectly align with the rules outlined in an organization's security policy. If you were to examine the firewall's configuration file, you might see something like Example 7-1, which is a portion of a Cisco Adaptive Security Appliance (ASA) configuration.

Example 7-1 *Sample Cisco ASA Firewall Rules*

```
access-list OUTSIDE extended permit tcp any object-group HTTPS-SERVERS eq https
access-list OUTSIDE extended permit tcp any object-group WEB-SERVERS eq www
access-list OUTSIDE extended deny ip host 90.84.x.x any
access-list OUTSIDE extended permit icmp any any time-exceeded
access-list OUTSIDE extended permit icmp any any unreachable
access-list OUTSIDE extended permit icmp any any echo-reply
access-list OUTSIDE extended permit tcp any host 12.238.x.x eq ftp
access-list OUTSIDE extended permit tcp any host 12.238.x.x eq ftp-data
```

The **access-list permit** statements in Example 7-1 are most likely in keeping with some security policy statement that dictates what services are allowed, by name, to enter the protected network and the destinations to which those services are allowed to access. Specifically, this example shows the customer having web servers (www-80), secure web servers (https-443), and an FTP-21 server. These permit entries in your firewall's configuration are your network's security plan, and the security policy defines what they are and why they are present.

To expand on the firewall to security policy analogy, examine some additional security policy bullet points and how a firewall aligns with them:

- A security policy outlines what action will be taken in response to circumstances that arise.
- A security policy document is constantly evolving and changing to meet new security needs.
- A security policy dictates both acceptable and unacceptable usage parameters.

If you perform a point-by-point comparison of a security policy with a firewall configuration, you see that firewalls act with a written security policy document, as shown in Table 7-1.

Table 7-1 *Comparing Security Policies and Firewall Configurations*

	Security Policy	Firewall Configuration
Ability to respond to circumstances	Yes	Yes
Constantly evolving	Yes	Yes
Dictates behavior	Yes	Yes

The intention of this section is not to convince you that a firewall is a replacement for a security policy document, but to get you thinking about security as an all-encompassing philosophy of plans, policies, and security devices. You must put a great deal of thought into a complete solution—not simply rely on a single aspect to protect your network. When you are ready to plan your firewall's configuration and develop the rules permitting or denying traffic, you should use your security policy as the starting point. Firewalls are the physical and logical manifestations of your security policy.

We Do Not Have a Security Policy

The reality is that not every company has a security policy set (yet), and although it is important, you can still secure your network without one. Presume that you have a firewall already in place and functional. The best advice is to slowly start the process of implementing security in your network. This means carefully reviewing the business needs (very important) of each rule that you currently have in your firewall and writing down each need. Documenting *why* something was done will be helpful later if there is a security incident or when the network changes, providing justification on removing the entry. Certainly this advice is also true for anything new that needs to be accessed; you can plan on new things given the ever-forward marching of technology. If this book helps you keep your business and family safer, you have done something to be proud of...now go write those security policies!

Firewall Operational Overview

Every long journey begins with the first step. Before delving too deeply into other areas of security appliance behavior, it is essential to understand how a firewall performs its magic.

Most firewalls (most, not all) rely on Stateful Packet Inspection (SPI) to keep track of all outbound packets and the responses these packets might generate. Keeping track of the hosts on the protected network that are generating outbound packets keeps rogue or unsolicited WAN packets from entering an external interface.

In other words, a firewall that uses SPI, as discussed in Chapter 5, "Overview of Security Technologies," watches all traffic that originates from an inside host, tracks the conversation from that host to the desired destination, and ensures that the inbound response to that request makes it back to the host that started the whole thing in the first place.

Note A firewall that is not stateful in design and configuration is incomplete and should not be used to protect your network. The importance of the stateful tracking of connections is critical to the security of any network. This chapter focuses on firewalls that track the state of a connection. As a reference point, all Cisco ASA and PIX firewalls are considered stateful packet inspection firewalls.

The critical dual purposes of *packet inspection and filtering* (blocking) of packets is one of the most fundamental responsibilities of a firewall. The following list includes the most common rules and features of firewalls:

- **Filter *incoming* network traffic based on source or destination:** Blocking unwanted incoming traffic is the most common feature of a firewall and is the main reason for a firewall—stopping unwanted traffic from entering your network. This unwanted traffic is usually from attackers, thus the need to keep it out.
- **Filter *outgoing* network traffic based on source or destination:** Many firewalls can also screen network traffic from your internal network to the Internet. For example, you might want to prevent employees from accessing inappropriate websites. You might also place a firewall between your network and a business partner with rules to keep each of you safe.
- **Filter network traffic based on content:** More advanced firewalls can screen network traffic for unacceptable content. For example, a firewall integrated with a virus scanner can prevent files that contain viruses from entering your network. Other firewalls integrate with email services to screen out unacceptable email.
- **Detect and filter malware:** The rise and proliferation of botnets and malware have driven firewall manufacturers to implement features designed to detect infected hosts through packet inspections. This is a good example of how security is ever changing and the security of the network must continue to advance as well because what was secure yesterday might not be tomorrow.
- **Make internal resources available:** Although the primary purpose of a firewall is to prevent unwanted network traffic from passing through it, you can also configure many firewalls to enable selective access to internal resources, such as a public web server, while still preventing other access from the Internet to your internal network. In many cases, you can accomplish this by using a DMZ, which is where the public web server would be located. (DMZs are discussed later in the section "Essentials First: Life in the DMZ.")
- **Allow connections to internal network:** A common method for employees to connect to a network is using virtual private networks (VPN). VPNs enable secure connections from the Internet to a corporate network. For example, telecommuters and traveling employees can use a VPN to connect to the corporate network. VPNs can also connect branch offices to each other over the Internet, saving on WAN costs.
- **Report on network traffic and firewall activities:** When screening network traffic to and from the Internet, you need to know what your firewall is doing, who tried to break in to your network, and who tried to access inappropriate material on the Internet. Most firewalls include a reporting mechanism of some kind. A good firewall can also log activity to a syslog or other type of archival storage receptacle. Perusing firewall logs after an attack occurs is one of a number of forensic tools you have at your disposal.

Firewalls in Action

These might be new concepts for you, and hopefully you are not thoroughly confused at this point. Look at Figure 7-2 for a bit more clarity of this process. Please refer to the list, which explains the steps a bit more in depth.

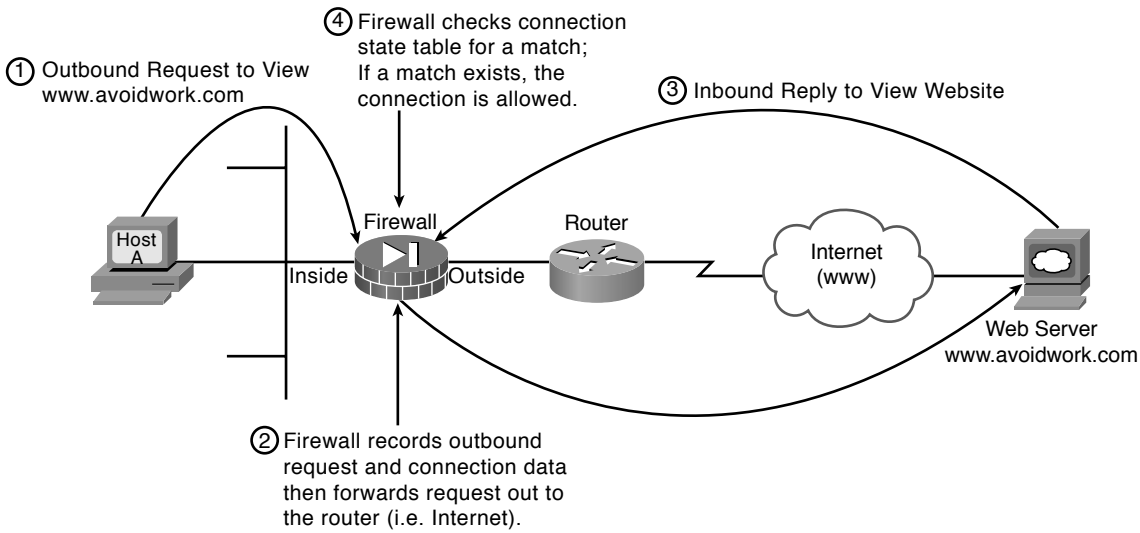


Figure 7-2 *Firewall in Operation*

Before looking at the list of steps, you need to know that many firewalls have only two physical interfaces, and 99 percent of them are based on Ethernet. These interfaces are called *inside* (protected) and *outside* (unprotected) and are deployed in relation to *your network*; some have DMZ interfaces as well. Thus, in practice, the outside interface connects to the Internet and the inside interface connects to your internal network:

Figure 7-2 shows a high-level view of the following:

1. Host A is an Apple Macbook Pro that opens a web browser and wants to view a web page from the www.avoidwork.com web server. This action causes Host A to send the request to view this web page out through the firewall across the Internet and to the web server.
2. The firewall sees the request originated with Host A and is destined for www.avoidwork.com.
   a. The firewall records (tracks) the outbound request and expects that the reply will come only from the www.avoidwork.com web server.
   b. A session marker is placed in the firewall's session state table that tracks the communication process from start to finish.

   c. Connection metrics, such as time opened and so forth, are also placed with the marker in the session state table record maintained by the firewall for this conversation.

3. The Avoidwork.com web server replies to the web page request from Host A, which is then transmitted back through the Internet and to the firewall.

4. The firewall checks its session state table to see whether the metrics being maintained for this session match the outbound connection. If all the stored connection details match exactly, the firewall enables the inbound traffic.

The information contained in the firewall's state table records and tracks information such as who needed www information from the avoidwork.com server, when they asked for it, how they asked for it, and so forth. This provides an added level of protection over and above the "can I enter or not" rules because if a certain traffic type is allowed in but the host did not ask for it (attack), it's denied. Because a firewall maintains connection state information about inbound and outbound connections, the possibility of a hacker "spoofing" or "forging" a packet with the intention of penetrating your network becomes more difficult. When attackers try to send packets to get through a firewall, incorrect or missing connection state information means that the session is terminated and most likely logged for later review.

Note Many firewalls examine the source IP addresses of packets to determine whether they are legitimate. An attacker would conduct an IP spoofing attack to try to gain entry by spoofing the source IP address of the packets sent to the firewall. If the firewall thinks the packets originated from a trusted host because they had the correct source IP address, the firewall might let the packets through unless other criteria fails to be met. This reinforces the principle that technology alone does not solve all security problems. In addition, you need the involvement of your company's management and, you guessed it, a security policy. Cisco firewalls use an adaptive security algorithm as a method of dynamically appending a random number to the translated session to make it even more difficult for a hacker to intercept.

Implementing a Firewall

The choice of firewalls is almost mind-boggling these days; they come in every shape, size, and capacity. When I am designing a firewall solution for a customer, the first thing I want to know is what will the firewall's responsibilities be?

The type of firewall you install depends on your exact requirements for protection and management, and the size of your network, or what is to be protected by the firewall. Firewalls usually fall into one of the following categories:

- **Personal firewall:** A personal firewall is usually a piece of software installed on a single PC to protect only that PC. These types of firewalls are usually deployed on home PCs with broadband connections or remote employees. Of course, any time

someone wants to deploy a firewall, it is a good idea. You can find some of the more well-known personal firewalls at these websites:

www.zonealarm.com

www.firewallguide.com

Operating system manufacturers such as Apple and Microsoft have responded to this need by integrating personal firewalls within them. Apple's OS X comes with an IP firewall and Windows has a similar firewall, it is just not as secure as the one in OS X. Most antivirus companies have expanded their products to include all sorts of protection through the use of their product suites.

- **All-in-one firewall/routers:** These kinds of firewalls are widely used by broadband (cable or DSL) subscribers who have the benefit of a single device that offers the following features and functionality: router, Ethernet switch, wireless access point, and a firewall. If this type of firewall appeals to you, ensure that you take care to determine the firewall's capabilities, and be skeptical of the security you can gain from these devices, regardless of who makes them. WARNING: Do not be tricked into assuming that a home router has a good firewall built into it; do your research first. I especially advise people to check on how the manufacturer supports what it makes; for example, if it does not take phone calls, you might want to continue shopping.
- **Small-to-medium office firewalls:** These firewalls, such as the Cisco ASA 5505 and 5510 or the older PIX 501 and 506, are designed to provide security and protection for small office home office (SOHO) types of requirements. In most cases, they have expansion slots allowing for additional network connections or advanced feature cards to be installed.
- **Enterprise firewalls:** These firewalls, such as the Cisco ASA 5520 and up, are designed for larger organizations with thousands of users. These larger models are needed when there are demands for larger numbers of connections, capacity, and features. As a result, they have additional features and capacity, such as more memory and extra interfaces along with slots for advanced feature cards to be added. An example in some cases would be an IPS module.

Normally, a firewall is installed where your internal network connects to the Internet. Although larger organizations also place firewalls between different parts of their internal network that require different levels of security, most firewalls are placed to screen traffic passing between an internal network and the Internet. For example, if a large organization enables business partners to connect directly to its network, you typically find a firewall controlling what is allowed into its network from the partners. This placement of an internal firewall is definitely considered best practice.

Note No matter what type of firewall you choose, you must define the traffic filters that will support your security policy. Cisco firewalls all run the same version of an operating

system that has the same reporting and management capabilities, regardless of the model, which is helpful when administering them.

Determine the Inbound Access Policy

As network traffic passes through a firewall, the traffic is subject to the rules defined within the firewall. Because 99 percent of all networks use private IP addresses on the inside of their networks, you can expect almost every firewall to be using Network Address Translation (NAT)—as discussed in Chapter 5.

Note Packets coming in from the Internet in response to requests from local PCs (users) are addressed to the firewall's outside interface. The firewall is likely using NAT and tracking the state of each inside user request. The firewall is dynamically allocating port numbers on the outside interface using NAT. Thus, allowing multiple users to use a public IP address so their requests can be routed on the Internet is the essence of NAT. The use of a single IP address and port numbers to translate addresses is known as *port address translation (PAT)*. These port changes are also rapidly made, making it difficult for an attacker to make assumptions about which port numbers to use.

If all your LAN traffic were destined for the Internet, the inbound access policy would be straightforward in its design. The firewall permits only inbound traffic in response to requests from hosts on the internal LAN. The firewall tracks all outbound requests in its state table, as previously discussed.

However, there will come a time when specific requests from the outside must be allowed and controlled through the firewall. Notice that we did *not* say that this was a good idea or that you should do it, we are just acknowledging that it's a business function that a security professional must support.

Note The realities of the real world make companies want to have their own email or web servers without spending money on a new firewall that has a DMZ interface, which is where you place these servers whenever possible. The section "Essentials First: Life in the DMZ" discusses the purpose and role of a DMZ interface.

Allowing direct access from the Internet (outside) through your firewall is perilous but common practice. The key to security in these types of implementations is to strictly define the traffic types you will allow and the port number. For example, permitting IP to any location inside your network is inappropriate. For example, you should permit only inbound traffic from the Internet HTTP (port 80) traffic to your web server (IP address: 10.10.10.10). Allowing only HTTP (port 80) traffic to the web server from the Internet is much smarter than allowing every kind of TCP/IP protocol and port.

A strongly recommended best practice is to add layers of security in the form of a personal firewall, intrusion detection system (IDS), and antivirus software. Also, before you implement these devices as layers, make sure your security policies outline the best practices and what steps are needed to maintain security. A layered security model should be used to protect your network; the more layers, the harder it is for an attacker to penetrate your network. The use of layers is sort of like the joke told between hunters. When you see a hungry and angry bear in the woods start to charge you, as you begin to run remember you do not have to be faster than the bear, just faster than the other hunter! Layering network security definitely helps make your network less appealing than your competitors. Another layer would be to integrate an IPS in a firewall, making a layered defense.

Determine Outbound Access Policy

All firewalls screen traffic coming into a firewall from the Internet, but a well-implemented and designed firewall also screens outgoing user traffic. Spoiled employees are not going to like this, but the truth of the matter is that companies pay for Internet connections in support of their business, NOT to let employees surf, watch video, stream music, or look at pictures they are not supposed to.

You might also want to use your firewall to control what IP addresses are allowed to exit; specifically, you should allow only IP addresses that are found on your internal network out, thus preventing spoofing of IP addresses.

Perhaps there are also certain places on the Internet where you do not want users to go. Alternatively, you might want to specify the locations they are allowed to go because every other destination will be denied by default. Recall the earlier discussion of proxy servers and how they can be used to control and monitor traffic that leaves your network. They are a good example of a device that defines an outbound access policy. Remember, employees and contractors are bound to rules, whether they be policies or service-level agreements (SLA), and good behavior is not optional—it's mandatory—and so are accurate logging and event correlation.

In addition, recall the earlier discussion about placing a firewall between your network and connections to business partners. This type of firewall usage and placement is also where you would apply and control traffic bound from your network to theirs. The next section looks at the next aspect of firewall and network security: the Demilitarized Zone (DMZ).

Essentials First: Life in the DMZ

The *Demilitarized Zone (DMZ)* is a term used in the military to define a buffer area between two enemies. Perhaps the most commonly acknowledged DMZ in the world is the DMZ between North Korea and South Korea, which separates them because they have not yet signed a permanent peace treaty since the Korean War. Perhaps this is an interesting piece of military and political trivia that you did not know, but how does it relate to securing your network and firewalls?

If your company has a self-hosted public website complete with email servers, you might consider using a two-interface (inside and outside) firewall and have the firewall create translation rules that direct the inbound traffic to the correct servers on your private network. Although this might seem like a safe thing to do, it could be disastrous if a talented hacker sets his sights on you. Connecting web, mail, and FTP servers located on the inside of your network to the Internet can be dangerous and, in some cases, simply not recommended. Secure FTP is also an option but the same rules apply.

Well, some smart people got together a long time ago and said, "Hey—let's put a third interface on the firewall and call it a DMZ." Sending traffic from the Internet inbound directly to your private network is a *bad* idea. Adding the third interface to a standard firewall made things both easier and quite a bit safer when deploying Internet accessible servers and services (www, email, and so on). If you were going to sell computers out of your house, you would not want people coming inside your house to buy one, would you? Of course not; you would want to set up a little shop in the garage or on the front porch, thus preventing people that you do not know from wandering all over your house and tampering with your comic book collection or going into your fridge to make a sandwich.

A DMZ is an interface that sits between a trusted network segment (your company's network) and an untrusted network segment (the Internet), providing physical isolation between the two networks enforced by a series of connectivity rules within the firewall. The physical isolation aspect of a DMZ is important because it enables Internet access only to the servers isolated on the DMZ and not directly into your internal network, as shown in Figure 7-3.

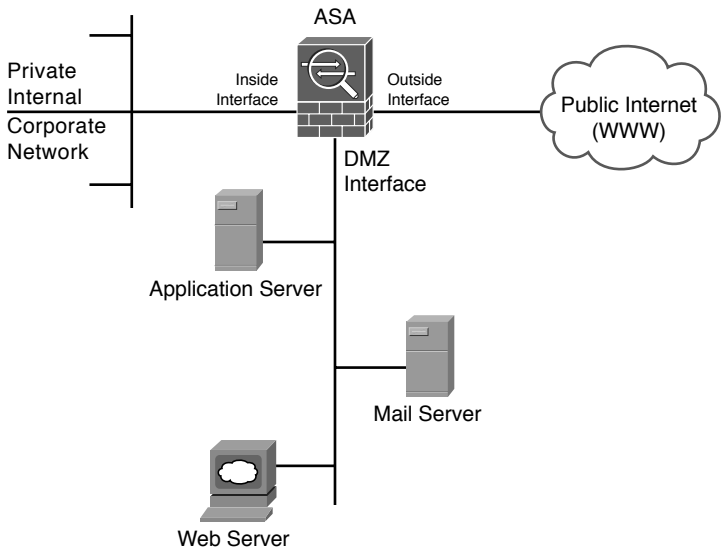


Figure 7-3 *DMZ Placement and Function*

In Figure 7-3, the segment connected to the DMZ interface contains the mail, web, and application servers. Rules applied to the DMZ interface prevent traffic from the Internet from going beyond the segment attached to it.

The biggest benefit to a DMZ is in isolating all unknown Internet requests to the servers on the DMZ and no longer allowing them into your internal network. However, some additional benefits to deploying a firewall with a DMZ can help you better understand what happens in your network and thereby increases security:

- Auditing DMZ traffic
- Locating an IDS on the DMZ
- Limiting routing updates between three interfaces
- Locating DNS on the DMZ

This section discussed what a DMZ is and provided a general example of how to use one. The following case studies examine a requirement for a DMZ and why you should use one in a network given a specific set of criteria.

Case Studies

This chapter presented several interesting aspects of how firewalls operate and how they can be deployed in networks. The introduction of this information needs to be reinforced with some real-world case studies that provide some answers to questions you might still have and clarify the important aspects of what has already been covered.

Case Study: To DMZ or Not to DMZ?

Carpathian Corporation has grown and is in need of increased security and additional capacity in the form of a new firewall; this time it wants to use a dedicated DMZ. If the Carpathian Corporation wants to continue with its proposed plan for self-hosting, it needs to consider the security-related issues relevant to the suggested DMZ solution. It is taking the right steps by asking what security ramifications should be addressed prior to making the purchase. The Carpathian IT staff needs to take a good look at the risk factors involved with providing for its own Internet services (web servers) and where the pitfalls might occur:

- **Question/Security Issue #1:** Can Internet traffic travel to servers on the private network, or is there another solution?

  Answer: The web and mail servers will be attached to the DMZ segment. They will not be dual homed or have conflicts of security in its implementation because they will be physically separated from inside hosts.

- **Question/Security Issue #2:** How can the IT staff ensure that inbound network traffic will stay confined to the segment containing the web and mail servers?

Answer: The DMZ interface rule set will not allow external traffic to reach the private network, by nature of configured connectivity rules. This will keep the inbound Internet traffic confined to the DMZ segment only.

- **Question/Security Issue #3:** What measures can be taken to hide the private network from the inbound network traffic?

  Answer: The DMZ interface will not have routes or dual-homed NIC cards that would normally enable this to occur.

The Carpathian IT staff is in the "If we self-host, we must use a DMZ" frame of mind. This frame of mind is correct, and that should be obvious at this point: Use a firewall with a DMZ interface—always!! A DMZ is another layer of security and defense for your network, as shown in Figure 7-4.

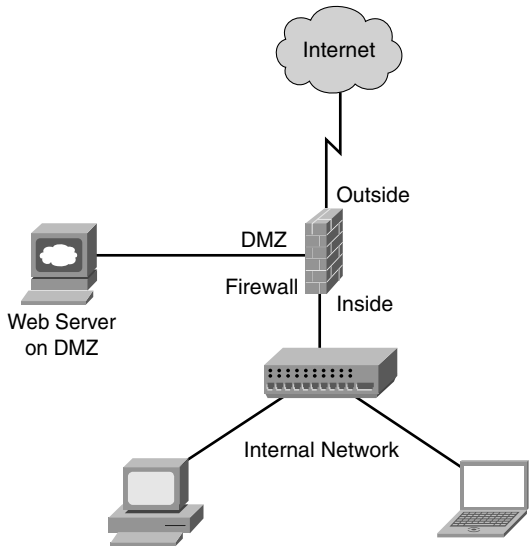


Figure 7-4 *Firewall Deployment with Web Server in a DMZ*

Cisco lists a variety of configuration settings when viewing their devices' configuration files. Example 7-2 shows several configuration files for clarity purposes. To illustrate the case study, comments are made surrounding key configuration entries; however, not every command is discussed because that is beyond the scope of this book. You can find additional information at Cisco.com.

Example 7-2 *Firewall with Self-Hosted Internal Web Server (No DMZ)*

```
Cyberwall(config)# sh run
: Saved
ASA Version 8.5
```

```
!
hostname CyberWall
domain-name CarpathianCorp.com
enable password <ChangeMe> encrypted
passwd <ChangeMe>  encrypted
names
!
!
interface Vlan1
 description SECURE INSIDE LAN [do not change]
 nameif INSIDE
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface Vlan2
 description OUTSIDE UPLINK TO SERVICE PROVIDER [do not change]
nameif OUTSIDE
 security-level 0
 ip address 209.164.3.2 255.255.255.0
!
interface Vlan3
 description DMZ INTERFACE FOR INTERNET FACING SERVERS [alter with care]
nameif DMZ
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
!--- These commands name and set the security level for each vlan or interface, the
ASA 5505 uses vlans to assign inside and outside whereas all other models have
physical interfaces. Through these commands, the firewall knows which interface is
considered untrusted (outside), trusted (inside) and DMZ. Notice the numeric values in
this configuration example. Here we have the least secure interface outside assigned a
security value of 0, as it should be. The inside interface is considered secure, so it
has a value of 100, with the DMZ being somewhere in between at 50.
!
interface Ethernet0/0
 description OUTSIDE INTERFACE [do not change]
 switchport access vlan 2
!
interface Ethernet0/1
 description INTERFACE FOR THE DMZ WEB SERVER [do not change]
 switchport access vlan 3
!
interface Ethernet0/2
 description RESERVED FOR INTERNAL HOST [alter with care]
!
```

```
interface Ethernet0/3
 description RESERVED FOR INTERNAL HOST [alter with care]
!
interface Ethernet0/4
 description RESERVED FOR INTERNAL HOST [alter with care]
!
interface Ethernet0/5
 description RESERVED FOR INTERNAL HOST [alter with care]
!
interface Ethernet0/6
 description RESERVED FOR INTERNAL HOST [alter with care]
!
interface Ethernet0/7
 description RESERVED FOR INTERNAL HOST [alter with care]
!
!--- An access list is created called "OUTSIDE" allowing WWW (http) traffic from
anywhere on the Internet to the host at 10.10.10.212 (the web servers REAL IP address
on the DMZ). Add additional lines to this access list as required if there is a email
or DNS Server. This is the first step in creating a rule set that permits traffic into
our network if it is destined for a specific IP Address.
!
access-list OUTSIDE extended permit tcp any host 10.10.10.212 eq www
!
! --- For purposes of this example we are not going to add anything else. Any
additional entries needing to be placed in the access list must be specified here. If
the server in question is not WWW, replace the occurrences of WWW with SMTP, DNS,
POP3, or whatever else might be required, like the ability to ping the server from the
Internet.
!
logging enable
logging timestamp
!
<<<output omitted for brevity>>>
!
! --- The following NAT commands specify that any traffic originating inside from the
ASA on the 192.168.0.0 /24 network will be NAT'd (via PAT because of the dynamic
interface command) to the ASAs public IP address that is assigned to the OUTSIDE
interface.
!
! --- The ASA NAT rules changed completely the new way is to define the subnets you
wish to NAT using object groups, the next four lines we have defined them as needed
for the INSIDE corporate as well as the DMZ.
```

```
!
object network OBJ_NAT_CORP
 description inside "corporate" subnet that must have internet access
 subnet 192.168.0.0 255.255.255.0
!
object network OBJ_NAT_DMZ
 description DMZ subnet that must have internet access
 subnet 10.10.10.0 255.255.255.0
!
! --- Once the subnets are defined in an object group we assign the type of NAT we
wish to perform as well as the direction. In the following examples we are permitting
the INSIDE and DMZ subnets to access the Internet using PAT via the ASAs outside
interface IP Address for both. This is shown in the command NAT (source interface,
destination interface) dynamic interface. The dynamic keyword means PAT to the ASA.
One of my favorite ways to check if this is working after configuring it open a web
browser and go to www.ipchicken.com this website will tell you the public IP Address
you are coming which should be the ASAs outside IP Address. Yes I know it's a goofy
name but that's what makes it easy to remember plus it makes people smile when you
tell them it.
!
object network OBJ_NAT_CORP
 nat (INSIDE,OUTSIDE) dynamic interface
!
object network OBJ_NAT_DMZ
 nat (DMZ,OUTSIDE) dynamic interface
!
! --- The last remaining NAT we must perform is for the Internet accessible Web
server that is on our DMZ. Once again we create an object group but this time we
specify a single host, which is the real IP address of the web server.
!
object network OBJ_NAT_WEBSERVER
 description real ip address assigned on the web servers nic card
 host 10.10.10.212
!
! --- Now that the object group is created identifying the servers real IP Address
we assign a NAT in the same format as we previously did with the difference being
after the direction (inside,outside) we define this as a STATIC NAT and give the
public IP Address to use. In practice what will happen is as packets reach the ASA
if they pass the access-list the ASA will check what their destination IP Address
is. Should the destination address be 209.164.3.5 (web server public IP Address)
the ASA will NAT those packets to the real IP Address of the server of 10.10.10.212
and forward them to the server on the DMZ.
```

```
!
object network OBJ_NAT_WEBSERVER
 nat (INSIDE,OUTSIDE) static 209.164.3.5
!
!
access-group OUTSIDE in interface outside
!
! --- There is only one access list allowed per interface per direction (for example,
inbound from the Internet on the outside interface) as we have shown here.
!
route outside 0.0.0.0 0.0.0.0 209.164.3.1
!
!--- Set the default route to be via the WAN routers Ethernet interface
!
<<<output omitted for brevity>>>
!
dhcpd dns 192.168.0.10 192.168.0.11
dhcpd domain mydomain.com
dhcpd address 192.168.0.2-192.168.0.125 inside
dhcpd enable inside
!
<<<output omitted for brevity>>>
!
! --- The last major functionality of an ASA show in its configuration is that of the
"inspects". Generally an inspect statement in the following section represents a
protocol that the ASA will be taking extra steps on the packets the statement
represents. For example many attacks are based on altering DNS replies so the ASA has
been configured to inspect DNS packets to help protect your network. Two inspects that
might be of importance to you are "inspect esmtp" and "inspect sip", depending on your
email server configuration and version the presence of esmtp may cause user issues
with emails, try removing it if this occurs. Regarding SIP when NATing a SIP
connection to an internal voice gateway you will want this statement as it provides
functionality that enables NAT to be done correctly and SIP to work, gotcha is it
depends on the provider. Inspects are very helpful and can be adjusted to offer very
granular security, please see www.cisco.com for more information.
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
```

```
!
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:88251e3c18c7d99dfa33f70b90228b63
: end
Cyberwall(config)#
```

Firewall Limitations

A firewall is a crucial component of securing your network and is designed to address the issues of data integrity or traffic authentication (via stateful packet inspection) and confidentiality of your internal network (via NAT). Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. The importance of including a firewall in your security strategy is apparent; however, firewalls do have the following limitations:

- A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce your password policy or prevent misuse of passwords. Your password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.

- Firewalls are ineffective against nontechnical security risks such as social engineering, as discussed in Chapter 1, "There Be Hackers Here."
- Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.
- Firewalls cannot protect you from poor decisions.
- Firewalls cannot protect you when your security policy is too lax.

Note The FBI's arrest of the phone master's cracker ring brought several of these security issues to light. These hackers were accused of breaking into credit-reporting databases belonging to Equifax, Inc. and TRW, Inc. and the databases of Nexis/Lexis and Dun & Bradstreet. They also broke into many of the world's providers. In doing so, these hackers did not use any high-tech attack methods. The phone masters used a combination of social engineering and dumpster diving, both techniques used by attackers that have little technical skill (refer to Chapter 1).

Chapter Summary

This chapter covered the world of firewalls and their role in securing a network. Not everyone believes in the value of these devices, and the discussions answered these naysayers and showed them the folly of their ways. Further proof of the importance of firewalls was provided by expanding on their pure technical aspects, while expressing the fundamental truth that firewalls are the manifestation of a company's security policy.

One of the online resources that may assist you in determining the direction and policy of your network security is www.opengroup.org/jericho/about.htm. The Jericho Project was formed by a group of corporate security officers who saw the ever-decreasing security being driven by the concept of deperimeterization. In 2004, the Forum set out to drive and influence development of secure architectures, technology solutions, and implementation approaches, for the deperimeterizing IT world, to enable safe, secure collaborative interworking, globally between enterprises—business partners, customers, suppliers, and out-workers—and to encourage development of open standards that would underpin these solutions.

Operationally, this chapter covered how firewalls function, where and when to implement them, and how to design the access policies necessary to define access into your network. Furthermore, the chapter introduced the DMZ interface as an evolution in firewalls and how they provide special locations for various Internet servers. The chapter concluded with several brief case studies demonstrating firewalls in action, followed by some of their limitations.

Chapter Review Questions

The following questions assist in reinforcing the concepts covered in this chapter:

1. Who needs a firewall?
2. Why do I need a firewall?
3. Do I need a firewall?
4. How is a firewall an extension of a security policy?
5. What is the name of the table in a firewall that tracks connections?
6. What fundamental role does a DMZ fulfill in network security?
7. What are four benefits of a DMZ?
8. Can firewalls enforce password policies or prevent misuse of passwords by users?
9. Do firewalls guarantee that your network will be protected?
10. Are all firewalls created equal?

Index

A

B

C

D

E

F

G

H

I

J-K

L

M

N

O

P

Q-R

S

T

U

V

W

X

Z