Official
Cert Guide

Learn, prepare, and practice for exam success

CCNP Security FIREWALL 642-618

- Master **CCNP Security FIREWALL 642-618** exam topics
- Assess your knowledge with **chapter-opening quizzes**
- Review key concepts with **exam preparation tasks**
- Practice with **realistic exam questions** on the CD-ROM

DAVID HUCABY, CCIE® No. 4594
DAVE GARNEAU
ANTHONY SEQUEIRA, CCIE No. 15626

ciscopress.com

CCNP Security FIREWALL 642-618 Official Cert Guide

David Hucaby
Dave Garneau
Anthony Sequeira

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCNP Security FIREWALL 642-618 Official Cert Guide

David Hucaby
Dave Garneau
Anthony Sequeira

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

Printed in the United States of America

Second Printing: June 2013 with corrections August 2014

The Library of Congress Cataloging-in-Publication Data is on file.

ISBN-13: 978-1-58714-271-0

ISBN-10: 1-58714-271-6

Warning and Disclaimer

This book is designed to provide information for the Cisco CCNP Security 642-618 FIREWALL exam. 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.

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 the United States, 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

Copy Editor: Sheri Cain

Editorial Assistant: Vanessa Evans

Composition: Mark Shirar

Proofreader: Apostrophe Editing Services

Cisco Press Program Manager: Anand Sundaram

Cisco Representative: Erik Ullanderson

Senior Development Editor: Christopher Cleveland

Project Editor: Mandie Frank

Technical Editors: Kenny Hackworth, Doug McKillip

Designer: Gary Adair

Indexer: Brad Herriman

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

David Hucaby, CCIE No. 4594, is a network architect for the University of Kentucky, where he works with healthcare networks based on the Cisco Catalyst, ASA, FWSM, and Unified Wireless product lines. David has a bachelor of science degree and master of science degree in electrical engineering from the University of Kentucky. He is the author of several Cisco Press titles, including *Cisco ASA, PIX, and FWSM Firewall Handbook*, Second Edition; *Cisco Firewall Video Mentor*; *Cisco LAN Switching Video Mentor*; and *CCNP SWITCH Exam Certification Guide.*

David lives in Kentucky with his wife, Marci, and two daughters.

Dave Garneau is a senior member of the Network Security team at Rackspace Hosting, Inc. Before that, he was the principal consultant and senior technical instructor at The Radix Group, Ltd. In that role, Dave trained more than 3,000 students in nine countries on Cisco technologies, mostly focusing on the Cisco security products line, and worked closely with Cisco in establishing the new Cisco Certified Network Professional Security (CCNP Security) curriculum. Dave has a bachelor of science degree in mathematics from Metropolitan State College of Denver. Dave lives in San Antonio, Texas, with his wife, Vicki, and their two brand new baby girls, Elise and Lauren.

Anthony Sequeira, CCIE No. 15626, is a Cisco Certified Systems Instructor (CCSI) and author regarding all levels and tracks of Cisco Certification. Anthony formally began his career in the information technology industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about Microsoft and Cisco technologies. Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company, KnowledgeNet, and Anthony trained there for many years. Anthony is currently pursuing his second CCIE in the area of Security and is a full-time instructor for the next-generation of KnowledgeNet, StormWind Live. Anthony is also a VMware Certified Professional.

About the Technical Reviewers

Doug McKillip, P.E., CCIE No. 1851, is an independent consultant specializing in Cisco Certified Training in association with Global Knowledge, a training partner of Cisco. He has more than 20 years of experience in computer networking and security. McKillip provided both instructional and technical assistance during the initial deployment of MCNS Version 1.0, the first Cisco Security training class, which debuted in early 1998, and has been a lead instructor for the security curriculum ever since. Doug has supplemented his instruction by authoring numerous security troubleshooting white papers and security blogs for Global Knowledge. He holds bachelors and master's degrees in chemical engineering from MIT and a master's degree in computer and information sciences from the University of Delaware. He resides in Wilmington, Delaware.

Kenny Hackworth is a senior network automation engineer at Rackspace Hosting, the service leader in cloud computing. His current expertise includes supporting content switching (Cisco CSS and F5 LTMs) and security appliances (Cisco and Juniper firewalls). His primary focus is currently on automation, particularly configuration changes as well as equipment deployments. Prior to Rackspace, Kenny supported the NSA while working for the Air Intelligence Agency, performing Digital Network Exploitation analysis and Cryptanalysis.

Dedications

From David Hucaby:

As always, this book is dedicated to the most important people in my life: my wife, Marci, and my two daughters, Lauren and Kara. Their love, encouragement, and support carry me along. I'm so grateful to God, who gives endurance and encouragement (Romans 15:5), and who has allowed me to work on projects like this.

From Dave Garneau:

I am also dedicating this book to the most important people in my life: my wife, Vicki, our daughters, Elise and Lauren, and my stepson, Ben. Without their love and support, I doubt I would succeed in any major endeavor, much less one of this magnitude. Additionally, I want to dedicate this book to my mother, Marian, who almost 40 years ago, believed a very young version of myself when he declared he would one day grow up and write a book. I am glad I was finally able to live up to that promise.

From Anthony Sequeira:

This book is dedicated to the many, many students I have had the privilege of teaching over the past several decades. I hope that my passion for technology and learning has conveyed itself and helped motivate—and perhaps even inspire.

Acknowledgments

It has been my great pleasure to work on another Cisco Press project. I enjoy the networking field very much—and technical writing even more. And more than that, I'm thankful for the joy and inner peace that Jesus Christ gives, making everything more abundant and worthwhile.

I've now been writing Cisco Press titles continuously for more than 10 years. I always find it to be quite fun, but other demands seem to be making writing more difficult and time-consuming. That's why I am so grateful that Dave Garneau and Anthony Sequeira came along to help tote the load. It's also been a great pleasure to work with Brett Bartow and Chris Cleveland. I'm glad they put up with me yet again, especially considering how much I let the schedule slip.

I am grateful for the insight, suggestions, and helpful comments that the technical editors contributed. Each one offered a different perspective, which helped make this a more well-rounded book—and me a more educated author.

—David Hucaby

The creation of this book has certainly been a maelstrom of activity. I was originally slated to be one of the technical reviewers, but became a coauthor at David Hucaby's request.

Right after accepting that challenge, I started a new job, moved to a new city, and built a new house. Throughout all the resulting chaos, Brett Bartow and Christopher Cleveland demonstrated the patience of Job, while somehow keeping this project on track. Hopefully, their patience was not exhausted, and I look forward to working with them again on future projects.

I am also thankful to our technical reviewers for their meticulous attention to detail. The input of Doug McKillip and Kenny Hackworth, both of whom I count as a close friends, was invaluable. The extremely thorough reviews provided by Doug and Kenny definitely improved the quality of the material for the end readers.

—Dave Garneau

Brett Bartow is a great friend, and I am so incredibly thankful to him for the awesome opportunities he has helped me to achieve with the most respected line of IT texts in the world, Cisco Press. I am also really thankful that he continues to permit me to participate in his fantasy baseball league.

It was such an honor to help on this text with the incredible David Hucaby and Dave Garneau. While they sought out a third author named David, it was so kind of them to make a concession for an Anthony.

I cannot thank David Hucaby enough for the assistance he provided me in accessing the latest and greatest Cisco ASAs for the lab work and experimentation that was required for my chapters of this text.

Finally, thanks to my family, Joette and Annabella and the dog Sweetie, for understanding all the hours I spent hunched over a keyboard. That reminds me, thanks also to my chiropractor, Dr. Paton.

—Anthony Sequeira

Contents at a Glance

Contents

Icons Used in This Book


Cisco ASA


IPS

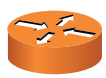

Content Services Module


AAA Server


CA


SSL VPN Gateway


IPsec VPN Gateway


Router


Layer 3 Switch


Layer 2 Switch


PC


IP Phone


Server


Network Cloud


Access Point


Wireless Connection

Ethernet Connection

Introduction

This book helps you prepare for the Cisco FIREWALL 642-618 certification exam. The FIREWALL exam is one in a series of exams required for the Cisco Certified Network Professional Security (CCNP Security) certification. This exam focuses on the application of security principles with regard to the Cisco Adaptive Security Appliance (ASA) device.

Who Should Read This Book

Network security is a complex business. It is important that you have extensive experience in and an in-depth understanding of computer networking before you can begin to apply security principles. The Cisco FIREWALL program was developed to introduce the ASA security products, explain how each product is applied, and explain how it can be leveraged to increase the security of your network. The FIREWALL program is for network administrators, network security administrators, network architects, and experienced networking professionals who are interested in applying security principles to their networks.

How to Use This Book

This book consists of 17 chapters. Each chapter tends to build upon the chapter that precedes it. Each chapter includes case studies or practice configurations that can be implemented using both the command-line interface (CLI) and Cisco Adaptive Security Device Manager (ASDM).

The chapters of this book cover the following topics:

- **Chapter 1, "Cisco ASA Adaptive Security Appliance Overview":** This chapter discusses basic network security and traffic filtering strategies. It also provides an overview of ASA operation, including the ASA feature set, product licensing, and how various ASA models should be matched with the environments they will protect.
- **Chapter 2, "Working with a Cisco ASA":** This chapter reviews the basic methods used to interact with an ASA and to control its basic operation. Both the CLI and ASDM are discussed.
- **Chapter 3, "Configuring ASA Interfaces":** This chapter explains how to configure ASA interfaces with the parameters they need to operate on a network.
- **Chapter 4, "Configuring IP Connectivity":** This chapter covers the ASA features related to providing IP addressing through DHCP and to exchanging IP routing information through several different dynamic routing protocols.
- **Chapter 5, "Managing a Cisco ASA":** This chapter reviews the configuration commands and tools that can be used to manage and control an ASA, both locally and remotely.

- **Chapter 6, "Recording ASA Activity":** This chapter describes how to configure an ASA to generate logging information that can be collected and analyzed. The logging information can be used to provide an audit trail of network and security activity.
- **Chapter 7, "Using Address Translation":** This chapter describes how IP addresses can be altered or translated as packets move through an ASA. The various types of Network Address Translation (NAT) and Port Address Translation (PAT) are covered. This chapter covers address translation methods for OS versions both before and after 8.3, where translation configuration was completely transformed.
- **Chapter 8, "Controlling Access Through the ASA":** This chapter reviews access control lists and host shunning, and how these features can be configured to control traffic movement through an ASA.
- **Chapter 9, "Inspecting Traffic":** This chapter covers the Modular Policy Framework, a method used to define and implement many types of traffic inspection policies. It also covers ICMP, UDP, TCP, and application protocol inspection engines, as well as more advanced inspection tools, such as Botnet Traffic Filtering and threat detection.
- **Chapter 10, "Using Proxy Services to Control Access":** This chapter discusses the features that can be leveraged to control the authentication, authorization, and accounting (AAA) of users as they pass through an ASA.
- **Chapter 11, "Handling Traffic":** This chapter covers the methods and features that can be used to handle fragmented traffic, to prioritize traffic for QoS, to police traffic rates, and to shape traffic bandwidth.
- **Chapter 12, "Using Transparent Firewall Mode":** This chapter reviews transparent firewall mode and how it can be used to make an ASA more stealthy when introduced into a network. The ASA can act as a transparent bridge, forwarding traffic at Layer 2.
- **Chapter 13, "Creating Virtual Firewalls on the ASA":** This chapter discusses the multiple context mode that can be used to allow a single physical ASA device to provide multiple virtual firewalls or security contexts.
- **Chapter 14, "Deploying High Availability Features":** This chapter covers two strategies that can be used to implement high availability between a pair of ASAs.
- **Chapter 15, "Integrating ASA Service Modules":** This chapter explains the basic steps needed to configure an ASA to work with the AIP and CSC Security Services Modules (SSM), which can be used to offload in-depth intrusion protection and content handling.
- **Chapter 16, "Traffic Analysis Tools":** This chapter discusses two troubleshooting tools that you can use to test and confirm packet movement through an ASA.
- **Chapter 17, "Final Preparation":** This short chapter lists the exam preparation tools useful at this point in the study process and provides a suggested study plan now that you have completed all the earlier chapters in this book.

- **Appendix A, "Answers to the 'Do I Know This Already?' Quizzes":** This appendix provides the answers to the "Do I Know This Already?" quizzes that you will find at the beginning of each chapter.
- **Appendix B, "CCNP Security 642-618 FIREWALL Exam Updates: Version 1.0":** This appendix provides you with updated information if Cisco makes minor modifications to the exam upon which this book is based. When Cisco releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you need to consult the new edition of the book for the updated content. This additional content about the exam will be posted as a PDF document on this book's companion website (www.ciscopress.com/title/9781587142796).
- **Glossary of Key Terms:** This glossary defines the key terms that appear at the end of each chapter, for which you should be able to provide definitions on your own in preparation for the exam.

Each chapter follows the same format and incorporates the following tools to assist you by assessing your current knowledge and emphasizing specific areas of interest within the chapter:

- **"Do I Know This Already?" Quiz:** Each chapter begins with a quiz to help you assess your current knowledge of the subject. The quiz is divided into specific areas of emphasis that enable you to best determine where to focus your efforts when working through the chapter.
- **Foundation Topics:** The foundation topics are the core sections of each chapter. They focus on the specific protocols, concepts, or skills that you must master to successfully prepare for the examination.
- **Exam Preparation:** Near the end of each chapter, the Exam Preparation section highlights the key topics from the chapter and the pages where you can find them for quick review. This section also provides a list of key terms that you should be able to define in preparation for the exam. It is unlikely that you will be able to successfully complete the certification exam by just studying the key topics and key terms, although they are a good tool for last-minute preparation just before taking the exam.
- **Command References:** Each chapter ends with a series of tables containing the commands that were covered. The tables provide a convenient place to review the commands, their syntax, and the sequence in which they should be used to configure a feature.
- **CD-ROM-based practice exam:** This book includes a CD-ROM containing several interactive practice exams. It is recommended that you continue to test your knowledge and test-taking skills by using these exams. You will find that your test-taking skills will improve by continued exposure to the test format. Remember that the potential range of exam questions is limitless. Therefore, your goal should not be to "know" every possible answer but to have a sufficient understanding of the subject matter so that you can figure out the correct answer with the information provided.

Certification Exam and This Preparation Guide

The questions for each certification exam are a closely guarded secret. The truth is that if you had the questions and could only pass the exam, you would be in for quite an embarrassment as soon as you arrived at your first job that required these skills. The point is to know the material, not just to successfully pass the exam.

We do know which topics you must know to successfully complete this exam because Cisco publishes them as "642-618 Deploying Cisco ASA Firewall Solutions Exam Topics (Blueprint)" on the Cisco Learning Network. Table I-1 lists each FIREWALL v2.0 exam topic listed in the blueprint along with a reference to the chapter that covers the topic. These are the same topics you should be proficient in when configuring the Cisco ASA in the real world.

Table I-1 *FIREWALL v2.0 Exam Topics and Chapter References*

Exam Topic	Chapter Where Topic Is Covered
ASA Basic Configurations	
Identify the ASA product family	Chapters 1, 15
Implement ASA licensing	Chapter 1
Manage the ASA boot process	Chapter 2
Implement ASA interface settings	Chapters 3, 8
Implement ASA management features	Chapters 2, 4, 5, 6, 16
Implement ASA access control features	Chapters 8, 10
Implement NAT on the ASA	Chapter 7
Implement ASDM public server feature	Chapter 2
Implement ASA QoS settings	Chapter 11
Implement ASA transparent firewall	Chapter 12
ASA Routing Features	
Implement ASA static routing	Chapter 4
Implement ASA dynamic routing	Chapter 4
ASA Inspection Policy	
Implement ASA inspections features	Chapter 9
ASA Advanced Network Protections	
Implement ASA botnet traffic filter	Chapter 9
ASA High Availability	
Implement ASA interface redundancy and load sharing features	Chapter 3
Implement ASA virtualization feature	Chapter 13
Implement ASA stateful failover	Chapter 14

Notice that not all the chapters map to a specific exam topic. Each version of the exam can have topics that emphasize different functions or features, while some topics can be rather broad and generalized. The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. In order to do this, all possible topics that have been addressed in different versions of this exam (past and present) are covered. Many of the chapters that do not specifically address exam topics provide a foundation that is necessary for a clear understanding of network security. Your short-term goal might be to pass this exam, but your long-term goal should be to become a qualified network security professional.

It is also important to understand that this book is a "static" reference, whereas the exam topics are dynamic. Cisco can and does change the topics covered on certification exams often.

This exam guide should not be your only reference when preparing for the certification exam. You can find a wealth of information available at Cisco.com that covers each topic in great detail. The goal of this book is to prepare you as well as possible for the FIREWALL exam. Some of this is completed by breaking a 600-page (average) implementation guide into a 30-page chapter that is easier to digest. If you think that you need more detailed information on a specific topic, you should read the Cisco documentation that focuses on that topic.

Note that because security vulnerabilities and preventive measures continue to develop, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics listed in Table I-1, always check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, hovering over Training & Events, and selecting from the Certifications list. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book at www.ciscopress.com/title/9781587142710. It's a good idea to check the website a few weeks before taking your exam to be sure that you have up-to-date content.

Overview of the Cisco Certification Process

The network security market is currently in a position where the demand for qualified engineers vastly surpasses the supply. For this reason, many engineers consider migrating from routing/networking over to network security. Remember that "network security" is just "security" applied to "networks." This sounds like an obvious concept, but it is actually an important one if you are pursuing your CCNP Security certification. You must be familiar with networking before you can begin to apply the security concepts. For example, the skills required to complete the CCNA or CCNP will give you a solid foundation that you can expand into the network security field.

Taking the FIREWALL Certification Exam

As with any Cisco certification exam, you should strive to be thoroughly prepared before taking the exam. There is no way to determine exactly what questions are on the exam, so the best way to prepare is to have a good working knowledge of all subjects covered on the exam. Schedule yourself for the exam and be sure to be rested and ready to focus when taking the exam.

The best place to find out the latest available Cisco training and certifications is under the Training & Events section at Cisco.com.

Tracking Cisco Certification Status

You can track your certification progress by checking www.cisco.com/go/certifications/login. You must create an account the first time you log in to the site.

How to Prepare for an Exam

The best way to prepare for any certification exam is to use a combination of the preparation resources, labs, and practice tests. This guide has integrated some practice questions and example scenarios to help you better prepare. If possible, you should get some hands-on experience with the Cisco ASA. There is no substitute for real-world experience; it is much easier to understand the commands and concepts when you can actually work with a live ASA device.

Cisco.com provides a wealth of information about the ASA and its software and features. No single source can adequately prepare you for the FIREWALL exam unless you already have extensive experience with Cisco products and a background in networking or network security. At a minimum, you will want to use this book combined with the Support and Downloads site resources (www.cisco.com/cisco/web/support/index.html) to prepare for the exam.

Assessing Exam Readiness

Exam candidates never know if they are adequately prepared for the exam until they have completed about 30 percent of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the "Do I Know This Already?" quizzes at the beginning of each chapter, review the foundation and key topics presented in each chapter, and review the command reference tables at the end of each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Cisco Security Specialist in the Real World

Cisco has one of the most recognized names on the Internet. Cisco Certified Security Specialists can bring quite a bit of knowledge to the table because of their deep understanding of the relationship between networking and network security. This is why the Cisco certification carries such high respect in the marketplace. Cisco certifications demonstrate to potential employers and contract holders a certain professionalism, expertise, and dedication required to complete a difficult goal. If Cisco certifications were easy to obtain, everyone would have them.

Exam Registration

The FIREWALL exam is a computer-based exam, with around 60 to 70 multiple choice, fill-in-the-blank, list-in-order, and simulation-based questions. You can take the exam at any Pearson VUE (www.pearsonvue.com) testing center. According to Cisco, the exam should last about 90 minutes. Be aware that when you register for the exam, you might be told to allow a certain amount of time to take the exam that is longer than the testing time indicated by the testing software when you begin. This discrepancy is because the testing center will want you to allow for some time to get settled and take the tutorial about the test engine.

Book Content Updates

Because Cisco occasionally updates exam topics without notice, Cisco Press might post additional preparatory content on the web page associated with this book at http://www.ciscopress.com/title/9781587142710. It is a good idea to check the website a few weeks before taking your exam to review any updated content that might be posted online. We also recommend that you periodically check back to this page on the Cisco Press website to view any errata or supporting book files that may be available.

Premium Edition eBook and Practice Test

This Cert Guide contains a special offer for a 70% discount off the companion CCNP Security FIREWALL 642-618 Official Cert Guide Premium Edition eBook and Practice Test. The Premium Edition combines an eBook version of the text with an enhanced Pearson IT Certification Practice Test. By purchasing the Premium Edition, you get access to two eBook versions of the text: a PDF version and an EPUB version for reading on your tablet, eReader, or mobile device. You also get an enhanced practice test that contains an additional two full practice tests of unique questions. In addition, all the practice test questions are linked to the PDF eBook, allowing you to get more detailed feedback on each question instantly. To take advantage of this offer, you will need the coupon code included on the paper in the CD sleeve. Just follow the purchasing instructions that accompany the code to download and start using your Premium Edition today!

This chapter covers the following topics:

- **Firewall Overview:** This section provides an overview of protecting networks by establishing security domains and positioning firewalls to protect them.
- **Firewall Techniques:** This section describes various firewall and network security methods.
- **Cisco ASA Features:** This section covers the long list of security features that a Cisco ASA can provide.
- **Selecting a Cisco ASA Model:** This section presents an overview and specifications of each ASA model so that the appropriate device can be selected.
- **Selecting ASA Licenses:** Once an ASA model is selected to secure a network, it must be licensed to perform everything that is required. This section explains the variety of feature licenses and how to select them, based on the ASA model.

CHAPTER 1

Cisco ASA Adaptive Security Appliance Overview

The Cisco Adaptive Security Appliance (ASA) is a versatile device that is used to secure a network. This chapter explains the concepts behind firewalls and other security tools, as they apply to the Cisco ASA. In addition, this chapter covers how to select an ASA model, the appropriate ASA features, and the correct ASA licenses based on high-level design requirements.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 1-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 1-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
Firewall Overview	1–2
Firewall Techniques	3–5
Cisco ASA Features	6–8
Selecting a Cisco ASA Model	9–11
Selecting ASA Licenses	12

Caution: The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following are recommended tasks for making a security domain secure? (Choose all that apply.)
   a. Place a router at the boundary of trusted and untrusted areas of the network, and then place a firewall inside the trusted area.
   b. Place a firewall at the boundary of trusted and untrusted areas of the network.
   c. Make the firewall the only path into and out of the security domain.
   d. Make the firewall the only path into and out of the untrusted domain.
   e. Harden the firewall against attacks.
   f. Force protected traffic through the firewall and bypass other traffic around it.
2. Which one of the following is considered to be the most secure?
   a. Logically separating a network with a firewall.
   b. Physically separating a network with a firewall.
   c. Putting the trusted and untrusted areas on different VLANs that are connected to a firewall over a trunk link.
   d. None of these answers are correct.
3. Consider the following list of rules, and then choose the answer that best describes it.

```
10      Permit all HTTP traffic
20      Permit all SMTP traffic to host 10.10.1.10
30      Permit all DNS queries
40      Deny everything
```

   a. Reactive access control
   b. Permissive access control
   c. Restrictive access control
   d. Protective access control
4. Which one of the following techniques would be the best choice for filtering HTTP (TCP port 80) sessions?
   a. Stateless packet filtering
   b. Stateful packet filtering
   c. Stateful packet filtering with application inspection and control
   d. Network intrusion protection system
   e. Network behavior analysis
5. Which of the following is not typically used for a restrictive approach to traffic filtering?
   a. Stateless packet filtering
   b. Stateful packet filtering
   c. Stateful packet filtering with AIC
   d. Network IPS
   e. Network behavior analysis

6. A company wants to join its network with another business partner, but wants to place a firewall between the two. Users within the company's home network should appear to use the business partner's IP address space when they access the partner's servers. Which of the following Cisco ASA features should be used to meet this requirement?

   a. Stateful packet filtering
   b. NAT
   c. IPS
   d. AIC
   e. NBA

7. A business has been the target of several attacks recently, where its network was scanned or probed to find unsuspecting victims. Which Cisco ASA feature should you leverage to detect and prevent further attacks?

   a. Remote Access VPNs
   b. Virtualization
   c. Traffic policing
   d. Botnet Traffic Filtering
   e. Threat detection

8. A company wants to begin using a firewall to protect its network, but it doesn't want to disrupt its operations with any IP address reconfiguration. In fact, it doesn't want to change the IP addresses on any of its existing network devices when the firewall is installed. Which Cisco ASA feature could you use to meet this requirement?

   a. NAT
   b. Virtualization
   c. IP routing
   d. Transparent firewall mode
   e. AIC

9. A medium-sized business would like to implement a firewall where it borders the public Internet. The business also plans to add intrusion prevention at the border. Assuming the business's Internet bandwidth will not exceed 350 Mbps, which of the following ASA models in combination with an integrated IPS module should you select?

   a. ASA 5505 with an AIP-SSC-5
   b. ASA 5510 with an AIP-SSM-10
   c. ASA 5520 with an AIP-SSM-20
   d. ASA 5550 with an AIP-SSM-40
   e. Any of the combinations in these answers will work.

10. Which one of the following represents a typical environment or application for an ASA 5550?

- **a.** A remote office
- **b.** A teleworker's home
- **c.** A data center requiring 10-Gbps throughput
- **d.** A large enterprise requiring 5-Gbps throughput
- **e.** A large enterprise requiring 1-Gbps throughput

11. Assuming the correct license has been purchased and activated, which of the following ASA models can support 50 virtual firewalls or security contexts? (Choose all that apply.)

- **a.** ASA 5510
- **b.** ASA 5520
- **c.** ASA 5540
- **d.** ASA 5550
- **e.** ASA 5580
- **f.** ASA 5585-X

12. Which one of the following functions requires the purchase of an additional feature license for a Cisco ASA 5520?

- **a.** Strong encryption
- **b.** Botnet Traffic Filtering
- **c.** DHCP server
- **d.** Threat protection
- **e.** Stateful packet filtering with AIC

Foundation Topics

To preserve the integrity and stability of resources on a network, they must be protected from things that can't always be trusted or controlled. Rather than begin with a list of possible network attacks, exploits, and vulnerabilities, this chapter presents an overview of a firewall, its features, and how it fits into various scenarios to protect a network. Individual security threats are described throughout this book as the appropriate firewall features to protect against those threats are introduced.

Firewall Overview

Network security engineers must protect valuable resources within a network. For example, corporate data might be confidential or critical to the operation of a business or to offering patient care, in which case it must be kept from prying eyes and protected from tampering. Similarly, the computers in a network might need to be protected from outside interference so that they are kept stable and in good working order.

To protect these resources, the network must somehow be divided into *trusted* and *untrusted* parts. The trusted portions of the network are known as *security domains*; everything inside the security domain is protected from everything outside the domain. As a simple example, a small company decides to protect itself from the public Internet. The security domain forms where the company's network meets the Internet, and everything inside the company network resides within a secure boundary. Figure 1-1 illustrates this scenario.

Key Topic

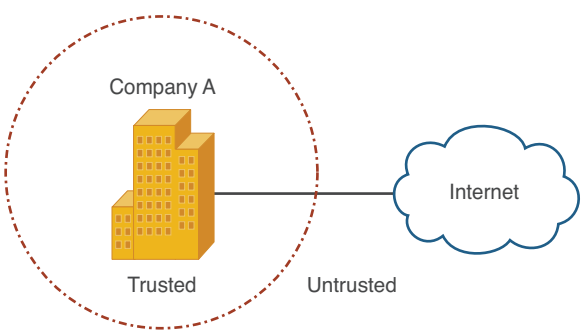


Figure 1-1 *A Simple Security Domain*

The most common and effective way to implement a security domain is to place a firewall at the boundary between the trusted and untrusted parts of a network. By definition, a *firewall* is a device that enforces an access control policy between two or more security domains. Firewalls have interfaces that connect into the network. In order for a firewall to do its job, all traffic that crosses a security domain boundary must pass through the firewall. In effect, a firewall becomes the only pathway or "chokepoint" to get in or out of the security domain.

For the simple network shown in Figure 1-1, a firewall would sit on the trust boundary and become the only path between Company A's internal trusted network and the untrusted public Internet, as shown in Figure 1-2. Although Figure 1-2 shows the addition of the firewall, several things must happen before the firewall can make the security domain truly secure:

- The firewall must be the only path into and out of the secured network. No other paths around the firewall or "backdoors" into the network behind the firewall can exist. The firewall can enforce security policies on only the traffic that passes *through* it, not around or behind it.
- The firewall itself must be hardened or made resistant to attack or compromise. Otherwise, malicious users on the untrusted side might take control of the firewall and alter its security policies.

Sometimes, a single security domain with a single firewall isn't enough. Suppose Company A wants to secure itself from the public Internet, but it also has a data center that needs to be even more secure. Company A trusts its employees to perform their job functions, but it can't risk letting anyone access its mission critical resources in an improper way or disrupt any services in its data center. Therefore, Company A decides to make a second security domain around the data center, as shown in Figure 1-3.

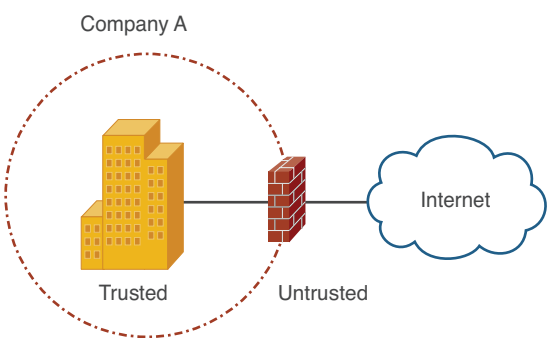


Figure 1-2 *Implementing a Security Domain with a Firewall*

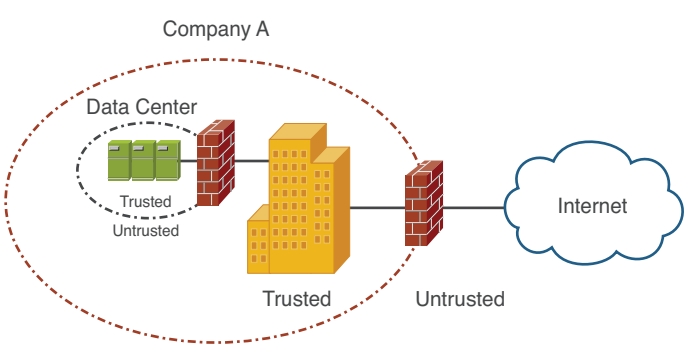


Figure 1-3 *Multiple Security Domains and Firewalls*

Each security domain is implemented with a firewall at its border. On the inside of the security domain or firewall, trusted resources exist; on the outside are untrusted things. This trust relationship is only locally significant, however. Consider the data center boundary firewall in Figure 1-3. The users just outside the data center are untrusted (at least from the perspective of that firewall), but they are still trusted from the perspective of the Internet boundary firewall. Each firewall has its own set of security policies and its own concept of a trust boundary.

Now consider a different scenario. Company A is surrounded by a security domain at the Internet boundary. It wants to allow its internal, trusted users to connect to resources out on the public Internet through the Internet firewall. Company A also has some web servers that it wants to have face the public so that untrusted Internet users can interact with the business.

If the web servers are located somewhere inside the security domain, then untrusted users would be granted access into the trusted environment. That isn't necessarily bad, except that malicious users might be able to attack or compromise one of the web servers. Because the web server is already a trusted resource, the malicious users might then use that server to attack other trusted resources.

A better solution is to put the web servers into a security domain of their own, somewhere between the trusted internal network and the untrusted Internet. This is commonly called a *demilitarized zone (DMZ)*. Figure 1-4 shows one solution that leverages the Internet firewall. With the addition of a third interface, the firewall can act as the boundary between a trusted domain, an untrusted public network, and a new "somewhat trusted" domain full of web servers.

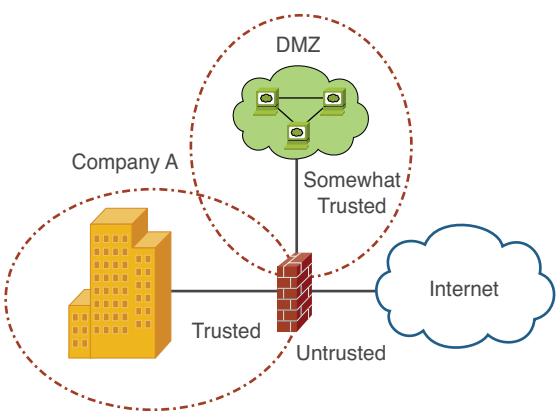


Figure 1-4 *Using a Single Firewall to Form Multiple Security Domains*

Whenever a firewall is used to form a security domain boundary, it must somehow separate the network into distinct parts. This can be done in one of two ways: physical separation or logical separation.

Physical separation requires that each physical firewall interface must be connected into a distinct network infrastructure. This usually requires additional hardware and additional

cost. For example, Figure 1-5 shows how a firewall physically separates a network into two distinct pieces, with each firewall interface connecting into a different switch. Physical separation provides the utmost security because traffic cannot pass between security domains without some sort of physical intervention—the firewall would have to be disconnected, cables rerouted, and so on.

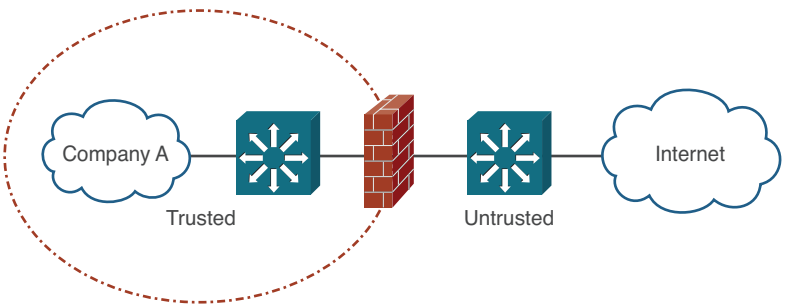


Figure 1-5 *Physical Separation of Security Domains*

A firewall can also be positioned to offer logical separation. In this case, the security domains exist on the same physical network infrastructure, but are separated logically into different *virtual local area networks (VLAN)*, *virtual storage area networks (VSAN)*, or *Multiprotocol Label Switching Virtual Private Networks (MPLS VPN)*. In Figure 1-6, a firewall forms a boundary between two security domains that are carried over two separate VLANs.

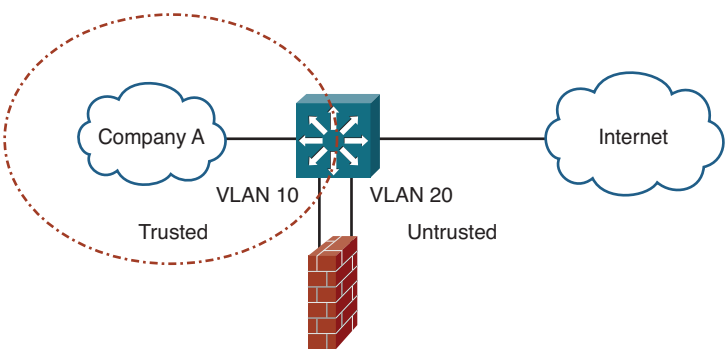


Figure 1-6 *Logical Separation of Security Domains*

While the firewall could use two physical interfaces to connect to the two VLANs, the VLANs could just as easily be carried over a single trunk link or one physical firewall interface. Logical networks are cost effective and can be flexible and complex. This makes logical separation less secure than physical separation, simply because a firewall might be bypassed or breached through a misconfiguration or failure of a logical network component or through an exploit of the logical separation itself.

Firewall Techniques

In its most basic form, a firewall strives to isolate its interfaces from each other and to carefully control how packets are forwarded from one interface to another. A firewall can enforce access control across a security boundary based on layers in the Open Systems Interconnection (OSI) model.

For example, a firewall performing *network layer access control* can make decisions based on Layers 2 through 4, or the data link, network, and transport layers. Such a firewall might control whether IP traffic can pass through, whether hosts on one side can open UDP or TCP connections to resources on the other side, and so on.

Firewalls that perform *application layer access control* enforce security policies at Layers 5 through 7, or the session, presentation, and application layers. Such a firewall can control what users do within applications that pass data from one side to another. For example, an application layer firewall might verify that a user's web browsing sessions are conforming to the industry standard protocols, or that a user's email or file transfers do not contain viruses or confidential material.

A firewall can take one of the following approaches to its access control:

- **Permissive access control:** All traffic is allowed to pass through unless it is explicitly blocked.
- **Restrictive access control:** No traffic is allowed to pass through unless it is explicitly allowed.

Permissive access control is also known as a *reactive* approach because it can react or block traffic only after potentially threatening things are identified and rules are put in place. Otherwise, everything else is allowed to pass through. Permissive rules are usually added to a firewall by intrusion prevention systems (IPS) and antivirus systems, which are tools that react to things that are detected on the network in real time.

Restrictive access control is also known as a *proactive* approach. Every acceptable type of traffic is identified ahead of time and entered into the firewall rules so that it may pass without further intervention. Any other traffic, whether it is malicious, undesirable, or just unidentified, is blocked by default. This is the same approach that is used by Cisco IOS access lists—traffic rules are processed in sequential order but always end with an implicit "deny all" rule.

A firewall can use its access control approach to evaluate and filter traffic based on the methods and techniques described in the following sections.

Stateless Packet Filtering

Some firewalls examine traffic based solely on values found in a packet's header at the network or transport layer. Decisions to forward or block a packet are made on each packet independently. Therefore, the firewall has no concept of a connection state; it knows only whether each packet conforms to the security policies.

Stateless packet filtering is performed by using a statically configured set of firewall rules. Even if a connection involves dynamic negotiation of further sessions and protocol port

numbers, the stateless firewall is unaware. Stateless packet filters can be characterized by the attributes listed in Table 1-2.

Table 1-2 *Characteristics of a Stateless Packet Filter*

Feature	Limitation
Statically configured rules, usually for a restrictive approach	Effective filtering is limited by human rule configuration
Effective for Layer 3 address, protocol, or Layer 4 port number filtering	No tracking of dynamically negotiated sessions or changing port numbers
Efficient and cost-effective	Relatively easy to exploit

Stateful Packet Filtering

Stateful packet filtering (SPF) requires that a firewall keep track of individual connections or sessions as packets are encountered. The firewall must maintain a state table for each active connection that is permitted, to verify that the pair of hosts is following an expected behavior as they communicate. As well, the firewall must inspect traffic at Layer 4 so that any new sessions that are negotiated as part of an existing connection can be validated and tracked. Tracking the negotiated sessions requires some limited inspection of the application layer protocol.

Stateful packet filters can be characterized by the attributes listed in Table 1-3.

Table 1-3 *Characteristics of a Stateful Packet Filter*

Feature	Limitation
Reliable filtering of traffic at Layers 3 and 4; typically used for a restrictive approach	No visibility into Layers 5 through 7
Simple configuration; less reliance on human knowledge of protocols	—
High performance	No protocol verification

Stateful Packet Filtering with Application Inspection and Control

To move beyond stateful packet filtering, firewalls must add additional analysis at the application layer. Inspection engines in the firewall reassemble UDP and TCP sessions and look inside the application layer protocols that are passing through. *Application inspection and control (AIC) filtering*, also known as *deep packet inspection (DPI)*, can be performed based on the application protocol header and its contents, allowing greater visibility into a user's activity.

AIC comes at a price, as a firewall needs more processing power and more memory to be able to inspect and validate application sessions and they unfold.

SPF with AIC can be characterized by the attributes listed in Table 1-4.

Table 1-4 *Characteristics of Stateful Packet Filtering with Application Inspection and Control*

Feature	Limitation
Reliable filtering of Layers 3 through 7; typically used for a restrictive approach	Limited buffering for thorough application analysis
Simple configuration; less reliance on human knowledge of protocols	—
Medium performance	AIC requires greater processing power

Network Intrusion Prevention System

A *network intrusion prevention system (NIPS)* examines and analyzes network traffic and compares it to a database of known malicious activity. The database contains a large number of signatures or patterns that describe specific known attacks or exploits. As new attacks are discovered, new signatures are added to the database.

In some cases, NIPS devices can detect malicious activity from single packets or atomic attacks. In other cases, groups or streams of packets must be collected, reassembled, and examined. A NIPS can also detect malicious activity based on packet and session rates, such as a denial-of-service TCP SYN flood, that differ significantly from normal activity on the network.

A network IPS usually operates with a permissive approach, where traffic is allowed to cross security domains unless something suspicious is detected. Once that occurs, the NIPS can generate firewall rules dynamically to block or reset malicious packets or connections.

A NIPS can be characterized by the attributes listed in Table 1-5.

Table 1-5 *Characteristics of a Network Intrusion Prevention System*

Feature	Limitation
A rich signature database of attack patterns, covering Layers 3 through 7	Limited buffering for thorough application analysis
Usually used in a permissive approach	Requires inline operation or partnership with a firewall to react to detected threats; cannot usually detect attacks that are new or not previously known
Medium performance	Requires periodic tuning to manage false positive and false negative threat detection

Network Behavior Analysis

Network behavior analysis (NBA) systems examine network traffic over time to build statistical models of normal, baseline activity. This isn't a simple bandwidth or utilization average; rather, the models consider things like traffic volume, traffic rates, connection rates, and types of application protocols that are normally used. An NBA system continually examines traffic and refines its models automatically, although human intervention is needed to tune the results.

Once the models are built, an NBA system can trigger on any activity that it considers to be an anomaly or that falls outside the normal conditions. In fact, NBA systems are often called anomaly-based network IPSs. Even when malicious activity involves a previously unknown scheme, an NBA system can often detect it if it involves traffic patterns or volumes that fall outside the norm. An NBA system can be characterized by the attributes listed in Table 1-6.

Table 1-6 *Characteristics of a Network Behavior Analysis System*

Feature	Limitation
Examines inline network traffic or offline traffic data to build profiles or models of normal network activity	Human intervention is required for model tuning.
Can detect previously unknown attacks	Generates false positives if legitimate traffic appears to be an anomaly.
Uses a restrictive approach, detecting or blocking everything that is not known good activity	—

Application Layer Gateway (Proxy)

An application layer gateway (ALG) or proxy is a device that acts as a gateway or intermediary between clients and servers. A client must send its application layer requests to the proxy, in place of any destination servers. The proxy masquerades as the client and relays the client's requests on to the actual servers. Once the servers answer the requests, the proxy evaluates the content and decides what to do with them.

Because a proxy operates on application requests, it can filter traffic based on the IP addresses involved, the type of application request, and the content of any data that is returned from the server.

Proxies can perform detailed and thorough analysis of client-server connections. Traffic can be validated against protocol standards at Layers 3 through 7, and the results can be normalized or made to conform to the standards, as needed. An ALG or proxy can be characterized by the attributes listed in Table 1-7.

Table 1-7 *Characteristics of an Application Layer Gateway (Proxy)*

Feature	Limitation
Protocol analysis and normalization	Not available for all protocols or applications.
Deep and thorough content analysis	Analysis might take too long for real-time traffic.
Access control over Layers 3 through 7	—
Can be permissive or restrictive	Can require configuration on the clients.

Cisco ASA Features

The Cisco ASA is the focus of the FIREWALL exam. Is the ASA a firewall? Yes. Is it more than a firewall? Yes! The Cisco ASA platform has the capability to perform any of the firewall techniques described in the previous sections.

Even further, the ASA has many features that go beyond the basic firewall techniques, giving it great versatility. A summary of the ASA features is presented in the following sections. You should become familiar with these features, as you will need to be able to select the appropriate ASA features and technologies on the exam, given some high-level design criteria:

- **Stateful packet filtering engine:** The SPF engine tracks connections and their states, performing TCP normalization and conformity checks, as well as dynamic session negotiation. Chapter 9, "Inspecting Traffic," covers the SPF engine in more detail.
- **Application inspection and control:** The AIC function analyzes application layer protocols to track their state and to make sure they conform to protocol standards. Chapter 9 covers the AIC functionality in more detail.
- **User-based access control:** The ASA can perform inline user authentication followed by Cut-through Proxy, which controls the access that specific users are allowed to have. Once a user is authenticated, Cut-through Proxy also accelerates inspection of a user's traffic flows. Chapter 10, "Using Proxy Services to Control Access," covers these functions in more detail.
- **Session auditing:** Accounting records can be generated for user-based sessions, as well as for application layer connections and sessions. Chapter 6, "Recording ASA Activity," covers session auditing in more detail. Session auditing can be used to generate audit trails, traffic accounting, and incident investigation.
- **Security Services Modules:** The ASA platform supports several Security Services Modules (SSM) that contain specialized hardware to offload processor-intensive security functions. An ASA can contain one SSM, offloading either IPS or content security services. Chapter 15, "Integrating ASA Service Modules," covers SSMs in more detail.
- **Reputation-based Botnet Traffic Filtering:** An ASA can detect and filter traffic involved with botnet activity on infected hosts. The Botnet Traffic Filter database

used to detect botnet threats is periodically updated by Cisco. Chapter 9 covers Botnet Traffic Filtering in more detail.

- **Category-based URL filtering:** An ASA can leverage an external URL filtering server to enforce acceptable use policies and control user access to various types of web services.
- **Cryptographic Unified Communications (UC) proxy:** When Cisco Unified Communications traffic must pass through an ASA, the ASA can be configured as an authorized UC proxy. The ASA can then terminate and relay cryptographically protected UC sessions between clients and servers.
- **Denial-of-service prevention:** An ASA can leverage traffic-control features like protocol normalization, traffic policing, and connection rate controls to minimize the effects of denial-of-service (DoS) attacks. Chapter 9 covers DoS prevention in more detail.
- **Traffic correlation:** The threat detection feature examines and correlates traffic from many different connections and sessions to detect and block anomalies stemming from network attacks and reconnaissance activity. Chapter 9 covers threat detection in more detail.
- **Remote access VPNs:** An ASA can support secure VPN connections from trusted users located somewhere on an untrusted network. Clientless SSL VPNs can be used to offer a secure web portal for limited remote access to users, without requiring VPN client software. For complete secure network access, full tunneling of all user traffic is supported with either SSL VPNs or IPsec VPNs, which require VPN client software. Remote access VPNs are covered in the *CCNP Security VPN 642-648 Official Cert Guide*.
- **Site-to-site VPNs:** An ASA can support IPsec VPN connections between sites or enterprises. Site-to-site or LAN-to-LAN VPN connections are usually built between firewalls or routers at each location. Site-to-site VPNs are covered in the *CCNP Security VPN 642-648 Official Cert Guide*.
- **High availability failover clustering:** Two identical ASA devices can be configured to operate as a failover pair, making the ASA security functions redundant in case of a hardware failure. Chapter 14, "Deploying High Availability Features," covers failover clustering in more detail.
- **Redundant interfaces:** To increase availability within a single ASA, interfaces can be configured as redundant pairs so that one is always active, while the other takes over after an interface hardware failure. Redundant interfaces are covered in Chapter 3, "Configuring ASA Interfaces," and can be used in conjunction with failover clustering.
- **EtherChannel:** Multiple ASA interfaces can be aggregated or bundled together as a single logical interface. By connecting an EtherChannel between an ASA and a switch, you can scale the bandwidth and offer additional redundancy. EtherChannels are covered in Chapter 3.

- **Traffic and policy virtualization:** An ASA can be configured to operate multiple virtual instances or security contexts, each acting as an independent firewall. Each virtual context has its own set of logical interfaces, security policies, and administrative control. Chapter 13, "Creating Virtual Firewalls on the ASA," covers virtual security contexts in more detail.
- **Rich IP routing functionality:** An ASA can forward traffic onto the local networks connected to each of its interfaces without any additional IP routing information. It can also be configured to use static routes or a dynamic routing protocol such as RIPv1, RIPv2, EIGRP, and OSPF to make more complex routing decisions. Chapter 4, "Configuring IP Connectivity," covers IP routing in more detail.
- **Powerful Network Address Translation (NAT):** As an ASA inspects and forwards packets, it can apply a rich set of NAT functions to alter source and destination addresses. Chapter 7, "Using Address Translation," covers NAT in more detail.
- **Transparent (bridged) operation:** An ASA can be configured to operate as a transparent firewall, effectively becoming a secure bridge between its interfaces. Transparent firewall mode allows an ASA to be wedged into an existing network without requiring any readdressing of the network. Chapter 12, "Using Transparent Firewall Mode," covers transparent firewall mode in more detail.
- **Integrated DHCP, DDNS, and PPPoE:** An ASA can be configured to act as a DHCP client or a PPP over Ethernet (PPPoE) client to obtain a dynamic IP address for its interfaces from the network, and as a Dynamic DNS (DDNS) client to record information for hostname-to-address resolution. As well, an ASA can act as a DHCP server to offer IP addressing services to other hosts on the network. Chapter 4 covers most of these features.
- **IPv6 support:** An ASA can be configured to operate natively in an IPv6 network.
- **IP multicast support:** An ASA can leverage the Internet Group Management Protocol (IGMP) and the Protocol Independent Multicast (PIM) protocol to participate in handling IP multicast traffic.
- **Management control and protocols:** An ASA supports several different methods of management control, including a console port, Telnet, Secure Shell (SSH), Secure HTTP (HTTPS), and Simple Network Management Protocol (SNMP; Versions 1, 2c, and 3). A dedicated out-of-band management port is also available. An ASA can send event notifications using SNMP traps, NetFlow, and syslog. Chapter 5, "Managing a Cisco ASA," covers management control in more detail.
- **Simple software management:** An ASA supports a local file system and remote file transfers for software upgrades. Software upgrades can be performed manually, automatically, or in a zero-downtime fashion on a failover cluster of ASAs. Chapter 13 covers software management in more detail.
- **Configuration flexibility and scalability:** Security policies and rules can be configured using reusable objects. Through the Modular Policy Framework (MPF), security features can be configured and applied in a flexible and versatile manner.

Chapter 8, "Controlling Access Through the ASA," and Chapter 9 cover these features in more detail.

- **Cisco Security Management Suite:** Multiple ASAs can be managed from the Cisco Security Management Suite for ease of administration.

Selecting a Cisco ASA Model

The Cisco ASA family consists of seven different models. In the FIREWALL exam, you will probably have to select an appropriate ASA model based on some high-level design criteria. How can you learn all of the specifications about every model? Fortunately, the model numbers can be used as a crude guide because they increase as the firewall capabilities or capacities increase.

The following sections briefly describe each of the ASA models, presented in order of increasing performance. The ASA features are consistent across the entire platform range, with some models limited only by feature licensing. Therefore, when you need to select an ASA model for a given scenario, your decision will most often hinge on the type of environment and the performance that is required.

ASA 5505

The ASA 5505 is the smallest model in the ASA lineup, in both physical size and performance. It is designed for small offices and home offices (SOHO). For a larger enterprise, the ASA 5505 is frequently used to support teleworkers in remote locations. Figure 1-7 shows front and rear views of the ASA 5505.

Figure 1-7 *ASA 5505 Front and Rear Views*

There are eight FastEthernet ports on the ASA 5505, all connected to an internal switch. Two of the ports are capable of offering Power over Ethernet (PoE) to attached devices. (The ASA itself cannot be powered by PoE.) By default, all eight ports are connected to the same VLAN in the switch, allowing connected devices to communicate with each other at Layer 2 directly.

The switch ports can be broken up into multiple VLANs to support different areas or functions within a small office. The ASA connects to each VLAN through individual logical interfaces. Any traffic crossing between VLANs must pass through the ASA and its security policies.

The ASA 5505 has one Security Services Card (SSC) slot that can accept an optional AIP-SSC-5 IPS module. With the module installed, the ASA can augment its security features with network IPS functions.

ASA 5510, 5520, and 5540

The ASA 5510, 5520, and 5540 models all use a common chassis and have identical front panel indicators and hardware connections. Figure 1-8 shows front and rear views of the common platform.

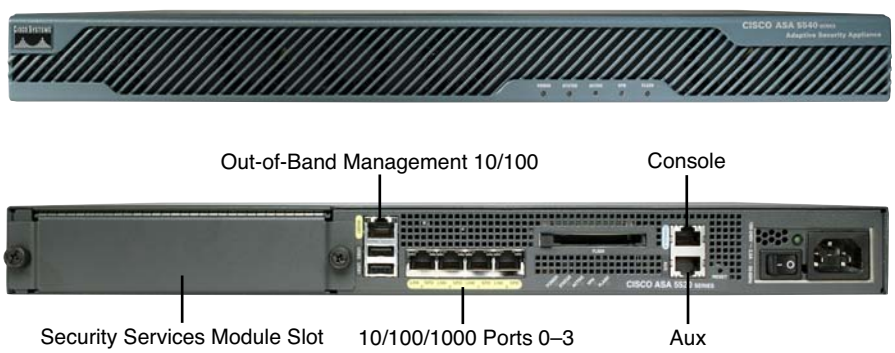


Figure 1-8 *ASA 5510, 5520, and 5540 Front and Rear Views*

The models differ in their security performance ratings, however. The ASA 5510 is designed for small to medium businesses (SMB) and remote offices for larger enterprises. The ASA 5520 is appropriate for medium-sized enterprises, while the ASA 5540 is more suited for medium- and large-sized enterprises and service provider networks.

The ASA 5520 and 5540 models has four 10/100/1000 Ethernet ports that can be used to connect into the network infrastructure. The four ports are dedicated firewall interfaces and are not connected to each other. An ASA 5510 can use all four Ethernet ports in FastEthernet (10/100) mode by default. If a Security Plus license is purchased and activated, two of the ports can operate as Gigabit Ethernet (10/100/1000) and two as FastEthernet. A fifth management Ethernet interface is also available.

The ASA 5510, 5520, and 5540 chassis have one SSM slot that can be populated with one of the following:

- **Four-port Gigabit Ethernet SSM:** This module adds four additional physical firewall interfaces, as either 10/100/1000 RJ45 or small form-factor pluggable (SFP)-based ports.
- **Advanced Inspection and Prevention (AIP) SSM:** This module adds inline network IPS capabilities to the ASA's security suite.
- **Content Security and Control (CSC) SSM:** This module adds comprehensive content control and antivirus services to the ASA's security suite.

Each of the SSMs is described in more detail in the section, "Security Services Modules."

The ASA 5510, 5520, and 5540 models have one AUX port that can be used for out-of-band management through an asynchronous serial connection or a modem. It also has one FastEthernet port that is designated for management traffic but can be reconfigured for normal data traffic if needed.

ASA 5550

The ASA 5550 is designed to support large enterprises and service provider networks. Figure 1-9 shows both front and rear views. Notice that the ASA 5550 looks identical to the ASA 5510, 5520, and 5540 models. The most noticeable difference is that the ASA 5550 has one fixed four-port Gigabit Ethernet (4GE-SSM) module in the SSM slot, which cannot be removed or changed.

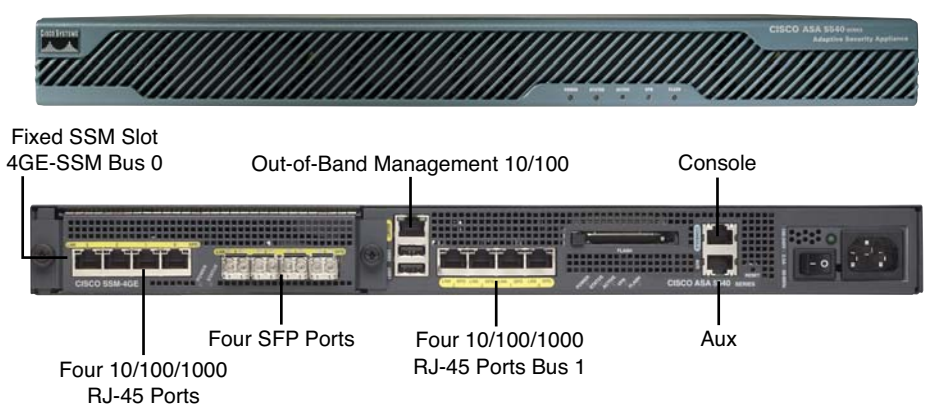


Figure 1-9 *ASA 5550 Front and Rear Views*

The ASA 5550 architecture features two groups of physical interfaces that connect to two separate internal buses. The interface groups are referred to as slot 0 and slot 1, corresponding to bus 0 and bus 1. Slot 0 consists of four built-in copper Gigabit Ethernet ports.

Slot 1 consists of four built-in copper and four built-in SFP Gigabit Ethernet ports, though only four of the eight ports can be used at any time.

The ASA 5550 offers high performance for demanding environments. To maximize the firewall throughput, the bulk of the traffic should go from the switch ports on bus 0 to the switch ports on bus 1. The ASA can forward traffic much more efficiently from bus to bus than it can if traffic stays within a single bus.

ASA 5580

The ASA 5580 is a high-performing model in the family and is designed for large enterprises, data centers, and large service providers. It can support up to 24 Gigabit Ethernet interfaces or up to 12 10Gigabit Ethernet interfaces. It is one of two models that has a chassis larger than one standard rack unit (RU).

Note: As of February 10, 2011, the ASA 5580 reached end-of-life status. In all likelihood, although it still exists as a product at press time, the FIREWALL course and exam will no longer cover the model.

The ASA 5580, shown in Figure 1-10, comes in two performance models: the ASA 5580-20 (5-Gbps throughput) and the ASA 5580-40 (10-Gbps throughput). The chassis includes two built-in 10/100/1000 Gigabit Ethernet ports, which are normally used for out-of-band management traffic. The system also uses dual redundant power supplies.

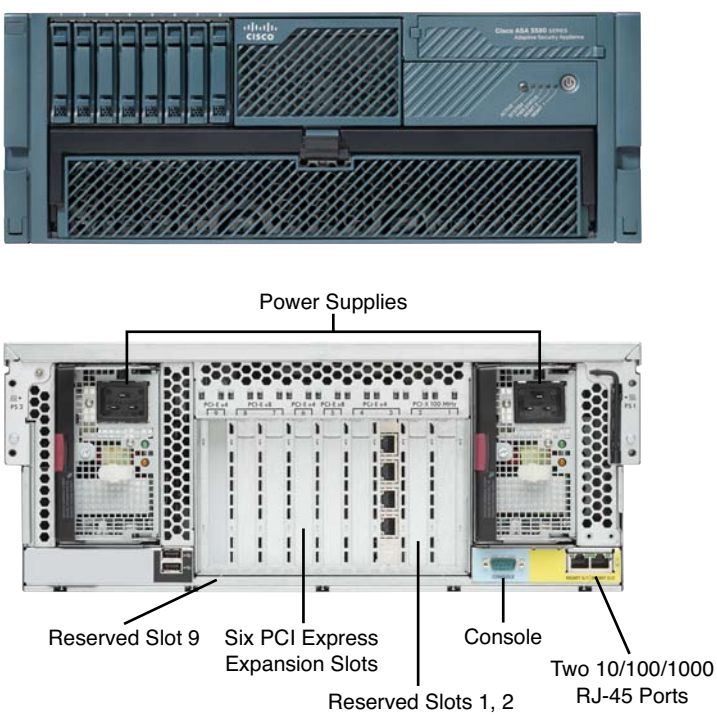


Figure 1-10 *ASA 5580 Front and Rear Views*

The ASA 5580 chassis has a total of nine PCI Express expansion slots. Slot 1 is reserved for a cryptographic accelerator module, to support high-performance VPN operations. Slots 2 and 9 are reserved for future use, leaving six slots available for the following network interface cards:

- 4-port 10/100/1000BASE-T copper Gigabit Ethernet interfaces
- 4-port 1000BASE-SX fiber-optic Gigabit Ethernet interfaces
- 2-port 10GBASE-SR 10Gigabit Ethernet fiber-optic interfaces

The ASA 5580 architecture has two I/O bridges that provide connectivity to the expansion slots, as shown in Figure 1-10. Unlike the ASA 5550, maximum throughput on the ASA 5580 is achieved when traffic flows stay *within* a single I/O bridge. The interfaces in slots 7 and 8 are all connected to I/O bridge 1, while the interfaces in slots 3, 4, 5, and 6 are connected to I/O bridge 2.

Any 10Gigabit Ethernet interfaces should be installed in slots 5, 7, or 8, which are high-capacity PCIe-x8 slots.

Security Services Modules

Many of the ASA models can accept one Security Services Module (SSM). The SSM contains dedicated hardware that can offload specialized or processor-intensive functions. Cisco offers the Advanced Inspection and Prevention (AIP) SSM, the Content Security and Control (CSC) SSM, and the 4-port Gigabit Ethernet (4GE) SSM, which are shown in Figure 1-11 and described in the following sections.

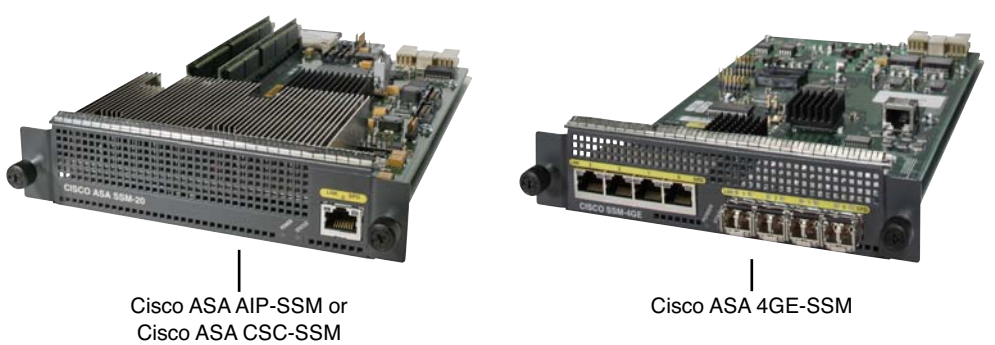


Figure 1-11 *Cisco ASA AIP-SSM, CSC-SSM, and 4GE-SSM*

Note: The AIP-SSM and the CSC-SSM use identical hardware form factors, but run entirely different software.

Advanced Inspection and Prevention (AIP) SSM

The AIP-SSM runs the Cisco IPS Software image and performs network intrusion prevention functions in conjunction with the ASA. The ASA can put the AIP-SSM inline, where traffic is internally redirected to the module for inspection and handling before it is

forwarded. Otherwise, the AIP-SSM can operate in promiscuous mode, where the ASA copies traffic to the module as it is being forwarded.

To be effective as a network IPS, the AIP-SSM must update its IPS signature database in a timely fashion. Signature updates are available only by subscribing to the Cisco Services for IPS service. The signature database is maintained and updated by Cisco Security Intelligence Operations (SIO) and contains well over 25,000 threat signatures. As new threats are discovered and identified, new signatures are added to the database, which must be downloaded into the AIP-SSM.

The AIP-SSM is available in several models, as listed in Table 1-8. The models are numbered sequentially, in order of increasing performance. Notice that not all models can work in every ASA platform. Higher-performing ASA models require higher-performing AIP-SSMs. Also notice that the ASA 5550 and 5580 models cannot accept an AIP-SSM at all.

Table 1-8 *AIP-SSM Models*

AIP SSM Model	ASA 5505	ASA 5510	ASA 5520	ASA 5540
AIP-SSC-5	75 Mbps			
AIP-SSM-10		150 Mbps	225 Mbps	
AIP-SSM-20		300 Mbps	375 Mbps	500 Mbps
AIP-SSM-40			450 Mbps	650 Mbps

Content Security and Control (CSC) SSM

The CSC-SSM performs comprehensive antivirus, antispyware, antispam, antiphishing, file blocking, URL blocking and filtering, and content filtering in conjunction with the ASA. The ASA internally redirects traffic through the CSC-SSM, which runs the Trend Micro InterScan for Cisco CSC-SSM software image. Because so many of the CSC-SSM's functions mitigate such a wide range of malware approaches, it is commonly referred to as the "Anti-X" module. HTTP, FTP, SMTP, and POP3 traffic are protected by the CSC-SSM.

For the CSC-SSM to be effective, it must stay updated with the latest content security information from Trend Micro. This is done automatically but requires a subscription service license from Cisco.

The CSC-SSM is available in two models, as listed in Table 1-9. The CSC-SSM-10 can support up to 50 users by default but can be expanded to 500 users through the purchase of additional licenses. The CSC-SSM-20 begins with 500 users and can be expanded to 1000 users with additional licenses.

Table 1-9 *CSC-SSM Models*

CSC-SSM Model	ASA 5505	ASA 5510	ASA 5520	ASA 5540
CSC-SSM-10		Up to 500 users	Up to 500 users	
CSC-SSM-20		Up to 1000 users	Up to 1000 users	Up to 1000 users

Both models come with a standard license that includes the antivirus, antispyware, and file-blocking features. If a Security Plus license is purchased, the CSC-SSM can also perform antispam, antiphishing, URL blocking/filtering, and content control.

4-port Gigabit Ethernet (4GE) SSM

The 4GE-SSM provides four additional Gigabit Ethernet ports to an ASA 5510, 5520, or 5540 model. Although the module has four copper 10/100/1000 RJ-45 ports and four SFP fiber-optic ports, only four ports of any type can be used at any time.

ASA 5585-X

The ASA 5585-X is the highest-performing model in the family and is designed for large enterprises and mission critical data centers. It has a 2-RU two-slot chassis and dual redundant power supplies, as shown in Figure 1-12. Each slot can accept a Security Services Processor (SSP).

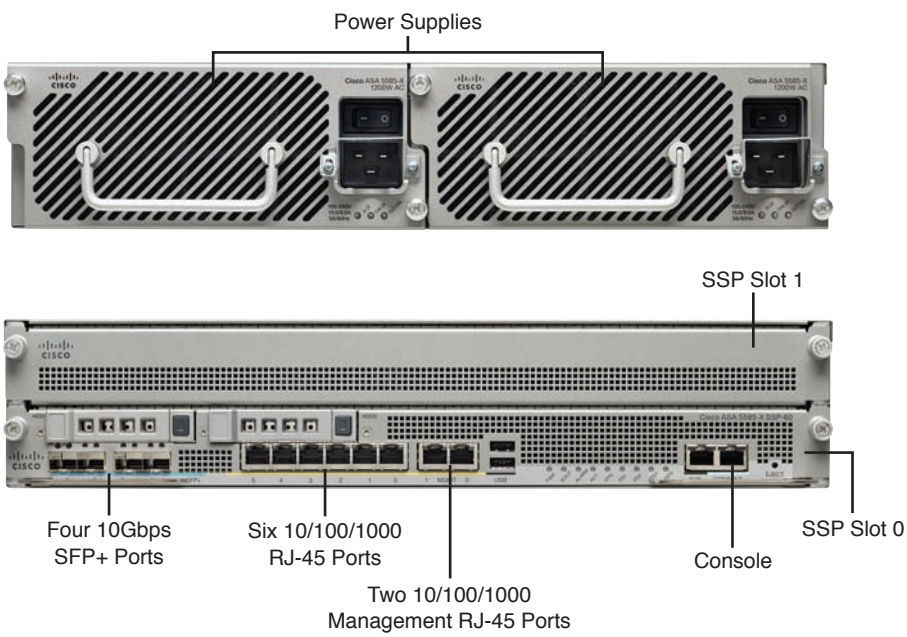


Figure 1-12 *ASA 5585-X Front and Rear Views*

The ASA 5585-X comes in four performance models, depending on which one of the following SSPs is installed with the firewall/VPN SSP: the SSP-10 (3-Gbps throughput), the SSP-20 (7-Gbps throughput), the SSP-40 (12-Gbps throughput), and the SSP-60 (20-Gbps throughput). Depending on the model, the firewall/VPN SSP can offer up to four 10-Gbps Ethernet, six 10/100/1000, and two 10/100/1000 management interfaces, as shown in Figure 1-12.

The ASA 5585-X can also provide high-performance IPS operation in four performance models, through the addition of one of the following IPS SSPs in the upper slot (slot 1):

- IPS SSP-10 (2-Gbps throughput)
- IPS SSP-20 (3-Gbps throughput)
- IPS SSP-40 (5-Gbps throughput)
- IPS SSP-60 (10-Gbps throughput)

Figure 1-13 shows an ASA 5585-X with a firewall/VPN SSP installed in slot 0 and an IPS SSP in slot 1. The firewall/VPN SSP is always in control of and passes traffic to and from the IPS SSP. Notice that the two SSPs look identical, although they perform totally different functions. When an IPS SSP is added to a chassis, it also brings up to four 10-Gbps Ethernet and six 10/100/1000 additional interfaces that are controlled by the firewall/VPN SSP.

Figure 1-13 *ASA5585-X Populated with a Firewall/VPN and IPS SSPs*

Note: The ASA 5585-X requires Cisco ASA software 8.2(3) or later. However, if an IPS SSP is installed, the ASA must run release 8.4(2) or later and Cisco IPS 7.1(1)E4 or later.

ASA Performance Breakdown

Sometimes, you will need to select an ASA model based on sheer performance ratings. For example, the exam might ask you to choose an appropriate ASA model based on the relative size of an organization or on the expected traffic or connection loads. You can use Table 1-10 and Table 1-11 to study how each ASA model relates to the type of environment or application it can typically support. The table also lists the throughput for bandwidth, connections, and packet handling.

Key Topic

Table 1-10 *Traffic Performance of ASA Models*

	5505	5510	5520	5540	5550	5580-20	5580-40
Typical application	Small office, home office, teleworker	Small to medium businesses, remote offices	Medium sized enterprise	Medium to large enterprises	Large enterprise, service provider	Large enterprise, data center, service provider	Large enterprise, data center, service provider
Firewall throughput	150 Mbps	300 Mbps	450 Mbps	500–650 Mbps	1–1.2 Gbps	5–10 Gbps	10–20 Gbps
Connections per second	4000	9000	12,000	25,000	36,000	90,000	150,000
Packets per second (64-byte)	85,000	190,000	320,000	500,000	600,000	2.5 M	4 M
Maximum connections	10,000/25,000[1]	50,000/130,000[1]	280,000	400,000	650,000	1 M	2 M

[1] ASA 5505, 5510: Base license/Security Plus license

Key Topic

Table 1-11 *Traffic Performance of ASA 5585-X Models*

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Typical application	Mission-critical data centers	Mission-critical data centers	Mission-critical data centers	Mission-critical data centers
Firewall throughput	3 Gbps	7 Gbps	12 Gbps	20 Gbps
Connections per second	65,000	140,000	240,000	350,000
Packets per second (64 byte)	1.5 M	3.2 M	6 M	10.5 M
Maximum connections	1 M	2 M	4 M	10 M

You should also be familiar with the number of interfaces that each ASA model can support. Table 1-12 and Table 1-13 list each ASA model along with the default number of physical interfaces that are installed, the maximum number of physical interfaces supported, and the number of VLANs or logical interfaces supported.

Table 1-12 *Interfaces Supported by ASA Models*

	5505	5510	5520	5540	5550	5580-20	5580-40
Default interfaces	8 FE switch (2 PoE)	5 FE or 2 GE + 3 FE	4 GE + 1 FE	4 GE + 1 FE	8 GE	2 GE	2 GE
Maximum interfaces	8 FE switch (2 PoE)	4 GE + 5 FE or 6 GE + 3 FE	8 GE + 1 FE	8 GE + 1 FE	8 GE + 1 FE	24 GE or 12 10 GE	24 GE or 12 10 GE
VLANs	3/20[1]	50/100[1]	150	200	250	250	250

[1] ASA 5505, 5510: Base license/Security Plus license

Table 1-13 *Interfaces Supported by ASA 5585-X Models*

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Default interfaces	8 GE + 2 10 GE	8 GE + 2 10 GE	6 GE + 4 10 GE	6 GE + 4 10 GE
Maximum interfaces	16 GE + 4 10 GE	16 GE + 4 10 GE	12 GE + 8 10 GE	12 GE + 8 10 GE
VLANs	1024	1024	1024	1024

Except for the ASA 5505, all other models can support virtual firewalls, also called security contexts. Each virtual firewall can operate independently, sharing processor, memory, and interface resources from the hardware platform. The number of supported virtual firewalls is listed in Table 1-14 and Table 1-15.

Table 1-14 *Virtual Firewalls and High Availability Supported by ASA Models*

	5505[1]	5510[1]	5520	5540	5550	5580-20	5580-40
Virtual firewalls (security contexts)[2]	0/0	0/5	20	50	50	50	50
High availability[3]	—/Stateless A/S	—/A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S

[1] ASA 5505, 5510: Base license/Security Plus license.

[2] All models include two security contexts by default, except the ASA 5505 and ASA 5510 Base, which include none.

[3] A/S = Active/Standby, A/A = Active/Active.

Key Topic

Table 1-15 *Virtual Firewalls and High Availability Supported by ASA 5585-X Models*

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Virtual firewalls (security contexts)[1]	100	250	250	250
High availability[2]	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S

[1] All models include two security contexts by default, except the ASA 5505 and ASA 5510 Base, which include none.

[2] A/S = Active/Standby, A/A = Active/Active.

ASA devices can also be configured to offer high availability by operating as clusters or failover pairs. The high availability mode varies depending upon the model and the installed license. In Table 1-14 and Table 1-15, the mode is shown to be Active/Standby (A/S), where one ASA actively protects a network while the other ASA sits idle in standby mode, or Active/Active (A/A), where both ASAs in a pair can actively participate in network protection.

Although the FIREWALL course and exam do not cover VPN topics in detail, you should still be familiar with the VPN capabilities of the ASA product family. Table 1-16 and Table 1-17 list the VPN throughput and maximum session ratings for each ASA model. VPN performance becomes important when an ASA must also support secure access for remote users and remote sites. By selecting the appropriate ASA model, you can make sure that the number of VPN users and the bandwidth they require are supported.

Table 1-16 *VPN Performance by ASA Model*

	5505	5510	5520	5540	5550	5580-20	5580-40
Max VPN throughput	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
Max IPsec VPN sessions	10/25[1]	250	750	5000	5000	10,000	10,000
Max SSL VPN sessions	25	250	750	5000	5000	10,000	10,000

[1] ASA 5505: Base license/Security Plus license.

Table 1-17 *VPN Performance by ASA 5585-X Model*

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Max VPN throughput	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Max IPsec VPN sessions	5000	10,000	10,000	10,000
Max SSL VPN sessions	5000	10,000	10,000	10,000

Selecting ASA Licenses

The Cisco ASA has a long list of security features (some common and some not so common) such that no one size fits all. To tailor an ASA to a specific environment or application, features and capabilities are unlocked through an aggregated licensing scheme based on the ASA's serial number. Each ASA model comes with a Base license that opens up a basic set of features. If additional capabilities are required, additional licenses must be purchased and their license activation keys must be entered into the ASA's permanent memory. These licenses are considered to be permanent licenses because they are applied to the ASA on a permanent basis.

Suppose you want to try out an ASA feature or capability without a commitment to purchase the license just yet. Cisco also offers temporary time-based licenses so that you can evaluate a feature or upgrade a capability until a permanent license can be purchased. Most of the time-based licensees are valid for a time limit from 1 to 52 weeks. Once they are requested from Cisco, time-based license activation keys can be entered into the ASA.

For ASAs running Cisco ASA Software Release 8.0(4) or later, time-based licenses can be aggregated or used in conjunction with permanent licenses. Until a time-based license expires, the permanent and time-based licenses are combined. With features like Unified Communications Proxy and Multiple Security Contexts, the permanent and time-based licenses are added together. With most other features, the higher value of the two licenses is used. In contrast, Releases 8.0(3) or earlier consider time-based licenses to override any permanent licenses for a given feature. Beginning with Release 8.3, you can install multiple time-based license keys so that you can evaluate several features.

When two ASAs are configured as a failover pair for high availability, the licenses between the two units must be compatible. Prior to Cisco ASA Software Release 8.3(1), both ASAs must have identical licenses installed. Beginning with Release 8.3(1), the two units can have disparate licensing. For feature licenses that involve a numerical limit, the sum of license on the two failover units is used. For feature licenses that are either enabled or disabled, the feature is enabled if the license is found on either ASA. If a time-based license is installed on either unit, the duration found on each unit is combined for a total license duration.

Key Topic

ASA licenses are broken up into the following categories:

- **Base license:** The default set of features.
- **Platform-specific licenses:** The ASA 5505 and 5510 are unique because they offer a Base license that can be upgraded to a Security Plus license. On the ASA 5505, the Security Plus license increases the maximum number of connections, VPN sessions, and VLANs, and it unlocks stateless firewall high availability. On the ASA 5510, Security Plus increases the maximum number of connections, physical interfaces, VLANs, and virtual firewalls, and it unlocks VPN load balancing and full high availability support. The specific differences between the Base and Security Plus licenses are shown in Tables 1-10, 1-12, 1-14, and 1-16.

  The ASA 5505 also keeps track of the number of concurrent active hosts or IP addresses on its inside network interface. The ASA can be purchased with an initial license of 10, 50, or an unlimited number of internal users. The number of internal users can also be upgraded to a total of 10, 50, or an unlimited number at a later time.
- **Feature licenses:** The features listed in Table 1-18 can be licensed individually.

Table 1-18 *ASA Aggregated Feature Licenses*

Feature License	Description
Botnet Traffic Filter	Enables Botnet Traffic Filtering
Strong Encryption	Enables 3DES and AES encryption algorithms for VPN sessions (free license)
GTP/GPRS Inspection	Enables GPRS Tunneling Protocol inspection (ASA 5520 and higher)
Cisco IME	Enables the Intercompany Media Engine functionality
AnyConnect Essentials	Enables the maximum number of AnyConnect SSL VPN clients only
AnyConnect Premium	Enables the maximum number of AnyConnect SSL VPN clients, clientless SSL VPN, and Cisco Secure Desktop features
AnyConnect for Mobile	Enables AnyConnect client access for Windows Mobile touch screen devices (also requires AnyConnect Essentials or Premium license)
Advanced Endpoint Assessment	Enables enhanced host scanning with Cisco Secure Desktop and AnyConnect SSL VPN clients
VPN Shared Licensing	Enables a license with a large number of SSL VPN sessions to be shared among several ASAs
FIPS Validation License	Enables Cisco AnyConnect SSL VPN client version 2.4 users for federal agencies requiring Federal Information Processing Standard (FIPS) 140-2 compliance

- **Virtualization licenses:** By default, every ASA (except the 5505 and 5510 Base licenses) comes with two virtual firewalls or security contexts. The number of contexts can be increased by purchasing either an initial feature license of 5, 10, 20, 50, or 100 contexts or a feature upgrade license to go from 5 to 10, 10 to 20, 20 to 50, or 100 to 250 contexts. The maximum number of contexts is limited by the ASA model.

- **Per-user cryptographic UC proxy licenses:** An ASA can extend Unified Communications (UC) services to remote users on the outside of a network through the cryptographic UC proxy features. Each remote user can be supported by any or all of the following proxy functions: ASA Phone Proxy, ASA Mobility Proxy, ASA Presence Federation Proxy, and ASA TLS Proxy.

  By default, each ASA model comes with two user UC proxy licenses. UC proxy functions can be increased by purchasing an initial license of 24, 50, 100, 250, 500, 750, 1000, 2000, 5000, or 10,000 users, depending on the ASA model being used. As well, the number of users can be increased by purchasing an upgrade license to go from the initial number of users to the next increment of users.

- **Per-user Premium SSL VPN licenses:** An ASA can support remote access to users over SSL VPN connections. By default, every ASA comes with a license that allows two Cisco AnyConnect SSL VPN users to connect. Premium SSL VPN includes support for users who have the Cisco AnyConnect client software installed, clientless SSL VPN users, and the Cisco Secure Desktop protected environment.

The number of AnyConnect users can be increased by purchasing an initial license of 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10,000 users, depending on the ASA model being used. The number of VPN users can also be increased by purchasing an upgrade license to go from the initial number of users to the next increment of users.

ASA Memory Requirements

All ASA models ship with a default amount of DRAM installed, which is based on the feature set and the newest code image that are available at that time. As more features and functions are added into the code image, the ASA needs more memory resources at its disposal.

Cisco ASA Software Release 8.3 added many new features over previous releases. As a result, Cisco increased the minimum amount of DRAM required to run the image, as shown in Table 1-19. ASAs shipped with Release 8.3 or newer have the appropriate amount of memory installed; however, many ASA models that were put into service before Release 8.3 do not have the minimum memory to run 8.3 or newer. Cisco offers memory upgrades to bring such models into alignment with the newer code images.

Table 1-19 *ASA Memory Requirements*

ASA Model	Minimum DRAM Required Prior to 8.3	Minimum DRAM Required 8.3 and Later
5505	256 MB	256 MB
5505 Unlimited User and Security Plus	256 MB	512 MB
5510	256 MB	1 GB
5520	512 MB	2 GB
5540	1 GB	2 GB
5550	4 GB	4GB
5580-20	8 GB	8 GB
5580-40	12 GB	12 GB
5585-X SSP-10	N/A	6 GB
5585-X SSP-20	N/A	12 GB
5585-X SSP-40	N/A	12 GB
5585-X SSP-60	N/A	24 GB

Exam Preparation Tasks

As mentioned in the section, "How to Use This Book," in the "Introduction," you have a couple of choices for exam preparation: the exercises here, Chapter 17, "Final Preparation," and the exam simulation questions on the CD-ROM.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 1-20 lists a reference of these key topics and the page number on which each is found.

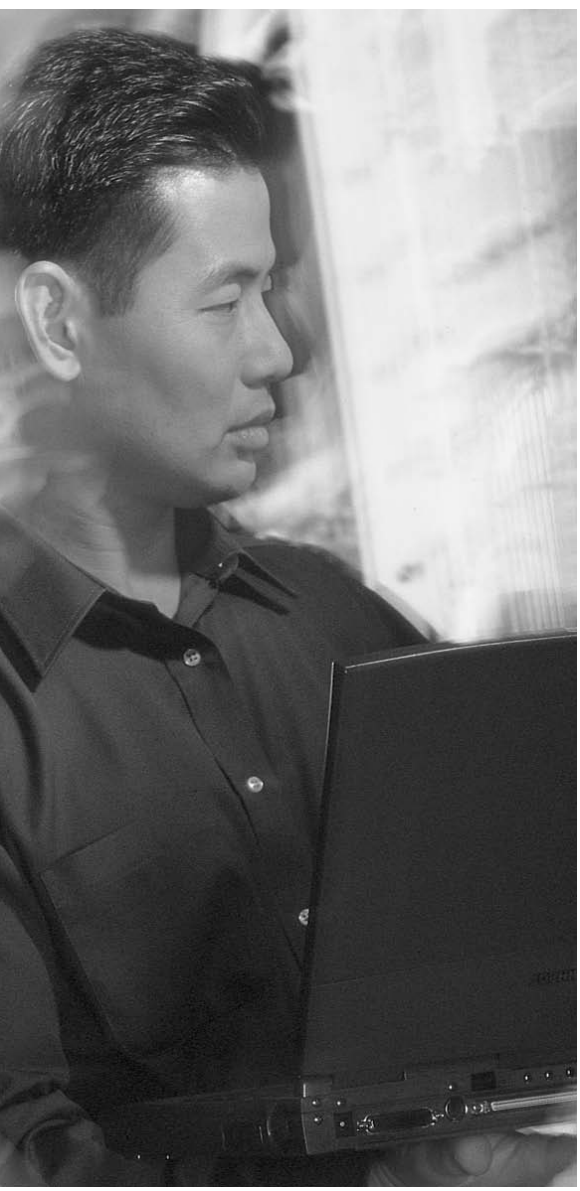
Table 1-20 *Key Topics for Chapter 1*

Key Topic Element	Description	Page Number
Paragraph	Explains security domains	7
List	Lists the two approaches to firewall access control	11
Paragraph	Explains stateful packet filtering with application inspection and control	12
List	List of the major Cisco ASA features and technologies	15
Tables 1-10 and 1-11	List of ASA models and their performance characteristics	26
Tables 1-12 and 1-13	List of ASA models and the number of supported interfaces	27
Tables 1-14 and 1-15	List of ASA models and their virtual firewall and high availability support	27–28
List	Explains the types of Cisco ASA licenses	30

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

firewall, security domain, demilitarized zone (DMZ), network layer access control, application layer access control, permissive access control, restrictive access control, stateless packet filtering, stateful packet filtering (SPF), application inspection and control (AIC) filtering, deep packet inspection (DPI), network intrusion prevention system (NIPS), network behavior analysis (NBA) system, application layer gateway (ALG), security context



This chapter covers the following topics:

- **Using the CLI:** This section describes the Cisco ASA command-line interface (CLI) and how you can use it to configure and display information about an ASA device.
- **Using Cisco ASDM:** This section describes the Adaptive Security Device Manager (ASDM) and how you can enter an initial ASA configuration to use it.
- **Understanding the Factory Default Configuration:** Every Cisco ASA comes with a factory default or preinstalled initial configuration. This section explains the initial configuration and how it bootstraps an ASA so that you can connect and make configuration changes.
- **Working with Configuration Files:** This section describes the startup and running configurations that an ASA uses as it boots and runs.
- **Working with the ASA File System:** This section covers the nonvolatile flash file system that an ASA uses to store configuration files, image files, and other types of files.
- **Reloading an ASA:** This section describes the ASA bootup sequence, how you can make an ASA reload, and how you can upgrade the operating system image during a reload.

CHAPTER 2

Working with a Cisco ASA

A Cisco Adaptive Security Appliance (ASA), like any other networking device, offers several ways for an administrative user to connect to and interact with it. The command-line interface (CLI) is an important part of that process. As you work with an ASA, you also need to understand its configuration files, file systems, and how to reboot or reload it when necessary.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 2-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 2-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
Using the CLI	1–3
Understanding the Factory Default Configuration	4–5
Working with Configuration Files	6–8
Working with the ASA File System	9–11
Reloading an ASA	12

Caution: The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following are modes that an ASA can offer through the CLI? (Choose all that apply.)
   a. Configuration mode
   b. Privileged EXEC mode
   c. Service mode
   d. User EXEC mode
   e. Specific configuration mode
   f. ROMMON mode
   g. Routed mode
2. Which keyboard key can be used to autocomplete a command in the ASA CLI?
   a. Space
   b. ESC
   c. ?
   d. Tab
   e. *
3. You want to display an ASA's running configuration to find any occurrence of the **deny** keyword, but the output is so large that it scrolls by too fast on your terminal emulator. Which one of the following commands can help you pinpoint the information?
   a. **show running-config deny**
   b. **show running-config | begin deny**
   c. **show running-config | include deny**
   d. **show running-config > grep deny**
   e. **show running-config all**
4. An ASA is booted up with its initial factory default configuration. You connect a PC to the appropriate Ethernet interface on the ASA so that you can use a web browser to open an ASDM session. Which IP address should you use for the ASA in your web browser?
   a. **10.0.0.1**
   b. **10.1.1.1**
   c. **192.168.0.1**
   d. **192.168.1.1**
   e. **1.1.1.1**
5. Which one of the following commands should you use to force an ASA to return to its initial factory default configuration?
   a. **write erase**
   b. **copy factory-config startup-config**
   c. **configure factory-default**
   d. **clear configure default**
   e. **reload /default**

6. After making some configuration changes to an ASA, you would like to save the changes permanently. Which one of the following commands should you use?

   a. **save all**
   b. **copy start run**
   c. **copy startup-config**
   d. **reload /save**
   e. **copy run start**

7. Suppose you decide to use a new startup configuration file called new-startup.cfg on an ASA. Based on the following commands and console output, which startup configuration will the ASA use after it is reloaded?

```
ciscoasa# copy run disk0:/new-startup.cfg
ciscoasa# config term
ciscoasa(config)# boot config disk0:/new-startup.cfg
ciscoasa(config)# exit
ciscoasa#
ciscoasa# show bootvar
BOOT variable = disk0:/asa823-k8.bin
Current BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable = disk0:/new-startup.cfg
ciscoasa# reload
```

   a. The initial factory default configuration.
   b. The original startup configuration.
   c. The new disk0:/new-startup.cfg file.
   d. The disk0:/asa823-k8.bin file.
   e. None; the ASA will boot into ROMMON mode.

   The original startup-configuration will be used because the running configuration has not yet been saved. If the running configuration had been saved, "CONFIG_FILE variable" would be shown as "disk0:/new-startup.cfg."

8. Suppose you enter the **write erase** command on a functioning ASA. What should you do before the next time the ASA is reloaded?

   a. Enter **copy startup-config running-config**.
   b. Enter **copy running-config startup-config**.
   c. Do nothing, because the ASA will be just fine.
   d. Panic because the ASA just lost its running configuration.

9. Entering the command **dir flash:** will actually show the contents of which one of the following file systems?

   a. Running configuration
   b. /
   c. disk0:/
   d. disk1:/
   e. All of the answers are correct.

10. A new startup configuration file has been saved on an ASA as disk0:/mystartup.cfg. The **boot config disk0:/mystartup.cfg** command has already been entered. Which of the following commands can be used to view the contents of the new file? (Choose all that apply.)

    a. **show disk0:/mystartup.cfg**
    b. **show startup-config**
    c. **show running-config**
    d. **more disk0:/mystartup.cfg**
    e. **view disk0:/mystartup.cfg**

11. An ASA is currently in production in your network. Suppose that you want it to be running operating system release 8.4(8) to leverage some new features and bug fixes. The 8.4(8) image file is located on a TFTP server. The following output is obtained from the **show version**, **show boot**, and **dir flash:** commands:

```
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Fri 10-Jan-11 07:51 by builders
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 2 days 6 hours

Hardware:   ASA5510-K8, 256 MB RAM, CPU Pentium 4 Celeron 1599 MHz
Internal ATA Compact Flash, 256MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                                Boot microcode   : CN1000-MC-BOOT-2.00
                                SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                                IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.04
```

```
 0: Ext: Ethernet0/0          : address is 001a.a22d.1ddc, irq 9
 1: Ext: Ethernet0/1          : address is 001a.a22d.1ddd, irq 9
[output truncated for brevity]

ciscoasa# show boot

BOOT variable =
Current BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
ciscoasa#
ciscoasa# dir flash:
Directory of disk0:/
93      -rwx  14503836     14:46:38 Sep 17 2010  asdm-645.bin
94      -rwx  15243264     14:44:02 Sep 17 2010  asa842-k8.bin
3       drwx  8192         14:04:34 Apr 27 2007  log
13      drwx  8192         14:05:02 Apr 27 2007  crypto_archive
255426560 bytes total (225050624 bytes free)
ciscoasa#
```

Which one of the following answers reflects the most logical next step you should take in the upgrade process?

a. Do nothing; the ASA is already running the upgraded image.

b. Enter the **reload** command.

c. Enter the **boot system disk0:/asa848-k8.bin** command.

d. Enter the **copy tftp: disk0:/asa848-k8.bin** command.

e. Enter the **copy running-config startup-config** command.

12. Which one of the following commands can be used to show the operating system version that is currently running on an ASA?

a. **show image**

b. **show version**

c. **dir disk0:/**

d. **show system**

e. **show running-config | include image**

Foundation Topics

To work with a Cisco ASA, you need to be able to interact with it and perform some basic maintenance procedures. This chapter covers the CLI, ASA configuration files, ASA file systems, and how to reload an ASA as part of the system maintenance or upgrade processes.

Using the CLI

Security professionals usually need to make changes to a firewall's security policies and its configuration. Other day-to-day tasks might include monitoring firewall activity and troubleshooting how a firewall is handling the traffic that is passing through it. An ASA offers the following ways for an administrative user to connect to and interact with it:

- CLI by an asynchronous console connection
- CLI by a Telnet session
- CLI by Secure Shell (SSH) version 1.x or 2
- Adaptive Security Device Manager (ASDM) through a web browser

In addition, before an ASA has fully booted up, it can provide a user interface to its ROM monitor bootstrap code when the normal operating system is not yet running.

Only the CLI itself is covered in this chapter. The mechanisms to reach it (Telnet, SSH, and ASDM) are covered in Chapter 5, "Managing a Cisco ASA."

The CLI-based user interface of a Cisco Firewall consists of several modes, each providing a different level of administrative capability and a different function:

- **User EXEC mode:** By default, the initial access to an ASA places a user in user EXEC mode and offers a limited set of commands. When you connect to the firewall, a user EXEC level password is required. When you are in user EXEC mode, the ASA always gives a prompt of this form:

```
ciscoasa>
```

- **Privileged EXEC mode:** The privileged EXEC level offers complete access to all firewall information, configuration editing, and debugging commands. Once you gain access to user EXEC mode, you can use the **enable** command to enter the privileged EXEC or "enable" mode. The ASA prompts for a password before granting access to the privileged EXEC mode. To leave privileged EXEC mode, use the **disable**, **quit**, or **exit** command. The syntax for entering privileged EXEC mode is as follows:

```
ciscoasa> enable
password: password
ciscoasa#
```

  Notice that the ASA changes the command prompt to differentiate the privileged EXEC and user EXEC modes. For privileged EXEC mode, a pound, or number, sign (#) is added at the end of the prompt.

- **Global configuration mode:** From privileged EXEC mode, you can enter global configuration mode. From this mode, you can issue firewall commands to configure any feature that is available in the operating system. To leave configuration mode and return to EXEC mode, enter **exit** or press **Ctrl-Z**. You can also use the **exit** command to exit a submode and return to global configuration mode.

  The syntax for entering global configuration mode is as follows:

  ```
  ciscoasa# configure terminal
  ciscoasa(config)#
  ```

  Notice how the ASA added (config) to the prompt to indicate global configuration mode.

- **Specific configuration mode:** The ASA offers many specific configuration submodes, much like Cisco IOS Software. More specific submodes are indicated by adding a suffix after config in the command prompt. For example, interface configuration mode is indicated by ciscoasa(config-if)#.

- **ROMMON mode:** As an ASA is booting, it runs an initial firmware from its read-only memory (ROM) that provides a limited interface that you can use to monitor the ASA hardware (hence, the name ROM monitor [ROMMON]).

From the CLI, you can enter commands and get helpful information about entering commands. As well, you can filter the information that an ASA displays in a CLI session as a result of a command. These mechanisms are discussed in the following sections.

Entering Commands

You can enable a feature or parameter by entering the command and its options into a CLI session. To disable a command that is in effect, begin the command with the **no** keyword, followed by the command. Be sure to include enough options to identify the command uniquely as it exists in the ASA session or configuration. For example, the following configuration commands enable and then disable the embedded HTTP server:

```
ciscoasa(config)# http server enable
ciscoasa(config)# no http server enable
```

You can see the configuration commands that are currently in effect by using one of the following commands:


```
ciscoasa# write terminal
```

or

```
ciscoasa# show running-config [command]
```

Notice that an ASA allows you to specify a *command* keyword in the **show running-config** command. If it is included, only the related configuration commands are shown, rather than the entire configuration.

Note: Some ASA configuration commands and their options are not shown if they use their default values. To see every configuration command that is enabled or active, even if it is a default, you can use the **show running-config all** [*command*] syntax.
The running configuration is covered in more detail in the section, "Working with Configuration Files."

Commands and their options can be abbreviated with as few letters as possible without becoming ambiguous. For example, to enter configuration mode, the command **configure terminal** would normally be used. In Example 2-1, the command **configure** is shortened to **co** and the keyword **terminal** is shortened to just its first letter, **t**. Because there are other possible commands that begin with the letters "co," the command is flagged as ambiguous. Adding one more letter, **con**, successfully identifies the right command, and configuration mode is entered.

Example 2-1 *Abbreviating an ASA Command*

```
ciscoasa# co t
ERROR: % Ambiguous command:  "co t"
ciscoasa#
ciscoasa# con t
ciscoasa(config)#
```

The ASA also offers a keyword-completion function. If you enter a shortened or truncated keyword, you can press the **Tab** key to make the firewall complete the keyword for you. Keyword completion can be useful when you are entering keywords that are long or are hyphenated. For example, pressing the Tab key after entering **show ru** produces the completed command **show running-config**:

```
Firewall# show ru<Tab>
Firewall# show running-config
```

This works only if the truncated keyword is unambiguous; otherwise, the firewall can't decide which one of several similar keywords you want. If you press Tab and the keyword stays the same, you know you haven't entered enough characters to make it unambiguous.

You can edit a command line as you enter it by using the left and right arrow keys to move within the line. If you enter additional characters, the remainder of the line to the right is spaced over. You can use the Backspace and Delete keys to make corrections.

Sometimes, the firewall might display an informational or error message while you are entering a command. To see what you've entered so far, you can press **Ctrl-l** (lowercase *L*) to redisplay the line and continue editing.

For example, suppose you are trying to enter the **hostname** configuration command to change the ASA's hostname. Before you can enter the command, the ASA displays a logging message that interrupts the command line, as shown in Example 2-2. Pressing **Ctrl-l** displays the line again without all the clutter.

Example 2-2 *Redisplaying an Interrupted Command Line*

```
ciscoasa# config t

ciscoasa(config)# hostnJan 10 2012 09:21:08  %ASA-5-502103: User priv level
  changed:
Uname: enable_15 From: 1 To: 15<Ctrl-l>
ciscoasa(config)# hostn
```

Command Help

An ASA offers context-based help within the command line, much like Cisco IOS Software. Entering a question mark after a command keyword causes the ASA to list all the possible keywords or options that can be used. If you enter a question mark alone on a command line, the ASA will display *all* the available commands.

Suppose that you are interested in displaying the ASA's ARP table, but you can't remember the command syntax to use after the **show** command. Example 2-3 shows how the context-based help can be used as an aid. Entering **show ?** displays all the possible keywords that can go along with the **show** command. The **show arp** command appears to be the one that you want in this case. From there, you might use another question mark to find out what other possible parameters you can enter at the end of the **show arp** command. As shown in the example, **show arp** can be followed by the **statistics** keyword, a pipe symbol (|), or the Enter key (<cr>).

Example 2-3 *Using Context-Based Help*

```
ciscoasa# show ?
  aaa                 Show information for AAA runtime data
  aaa-server          Show aaa-server configuration information
  access-list         Show hit counters for access policies
  activation-key      Show activation-key

  arp                 Show ARP table or ARP statistics
  asdm                Show Device Manager history, sessions or log
  asp                 Show the current contents of selected memory in the
                      Accelerated Security Path
  auto-update         Show Auto Update
  banner              Show login/session banners
  blocks              Show system buffer utilization
[output truncated for brevity]

ciscoasa# show arp ?
  statistics  Show ARP statistics
  |           Output modifiers
  <cr>
ciscoasa# show arp
```

You can also end a partially completed command keyword with a question mark if you don't know the exact spelling or form to use. The ASA will display all possible keywords that can be formed from the truncated word. For example, suppose you don't remember which commands can be used to configure access lists. In Example 2-4, entering **access?** in configuration mode reveals two possible commands: **access-group** and **access-list**. Notice that the truncated command keyword is displayed again, ready to be completed with more typing.

Example 2-4 *Using Context-Based Help to List Possible Commands*

```
ciscoasa(config)# access?
access-group  access-list
ciscoasa(config)# access
```

If you enter a command but use the wrong syntax, you see the following error:

```
Type help or '?' for a list of available commands
```

An ASA will also display a carat (^) symbol below the command-line location to point out the error. In Example 2-5, suppose you forget the correct command and enter the command **config type** rather than **config term**. The carat points to the keyword **type**, starting at the **y**, where the syntax error begins.

Example 2-5 *An ASA Pointing Out a Syntax Error*

```
Firewall# config type
                  ^
ERROR: % Invalid input detected at '^' marker.
Firewall#
```

You can also use the **help** [*command*] command to display some concise information about how to use a command, a description of the command, and the command syntax. Example 2-6 shows the help output generated from entering **help passwd** from within configuration mode.

Example 2-6 *Help Output Generated from the* **help passwd** *Command*

```
ciscoasa(config)# help passwd
USAGE:
        [no] password|passwd <password> encrypted
        clear configure passwd
DESCRIPTION:
passwd          Change Telnet console access password
SYNTAX:
<password>      A password of up to 16 alphanumeric characters
                Factory-default password is cisco
```

```
encrypted       Indicate the <password> entered is encrypted
see also:       telnet
ciscoasa(config)#
```

Command History

An ASA keeps a history of the last 19 commands that were entered in each CLI session. You can see the entire history list for your current session with the **show history** command.

You can use the command history to recall a previous command that you want to use again. This can save you time in entering repetitive commands while allowing you to make edits or changes after you recall them.

Each press of the up arrow key (c) or Ctrl-p recalls the next older or previous command. Each press of the down arrow key (T) or Ctrl-n recalls the next most recent command. When you reach either end of the history cache, the firewall displays a blank command line.

When commands are recalled from the history, they can be edited as if you just entered them. You can use the left arrow key (d) or right arrow key (S) to move within the command line and begin typing to insert new characters. You can also use the Backspace or Delete key to delete characters.

Note: The arrow keys require the use of an American National Standards Institute (ANSI)-compatible terminal emulator, such as PuTTY. You can find PuTTY at www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Searching and Filtering Command Output

A **show** command can generate a long output listing. If the listing contains more lines than the terminal session can display (24 lines by default), the listing is displayed one screenful at a time, with the following prompt at the bottom:

```
<---More --->
```

To see the next screen, press the spacebar. To advance one line, press the **Enter** key one time. To exit to the command line, press the **q** key.

Key Topic

Sometimes, you might need to sift through a long output listing for some specific information. You can use a regular expression to match against lines of output. Regular expressions are made up of patterns—either simple text strings (such as **permit** or **route**) or more complex matching patterns. Typically, regular expressions are regular text words that offer a hint to a location in the output of a show command. You can use the following command structure to perform a regular-expression search:

```
Firewall# show command ...|{begin|include|exclude|grep [-v]}
  reg-expression
```

To search for a specific regular expression and start the output listing there, use the **begin** keyword. This can be useful if your firewall has a large configuration. Rather than using the spacebar to eventually find a certain configuration line, you can use **begin** to jump right to the desired line.

To display only the lines that include a regular expression, use the **include** (or **grep**) keyword. To display all lines that don't include a regular expression, use the **exclude** (or **grep-v**) keyword.

A more complex regular expression can be made up of patterns and operators. Table 2-2 lists and defines the characters that can be used as operators.

Table 2-2 *Regular Expression Operators*

Character	Description
.	Matches a single character.
*	Matches zero or more sequences of the preceding pattern.
+	Matches one or more sequences of the preceding pattern.
?	Matches zero or one occurrences of the preceding pattern.
^	Matches at the beginning of the string.
$	Matches at the end of the string.
_	Matches a comma, braces, parentheses, the beginning or end of a string, or a space.
[ ]	Defines a range of characters as a pattern.
( )	Groups characters as a pattern. If used around a pattern, the pattern can be recalled later in the expression using the backslash (\) and the pattern occurrence number.

Example 2-7 shows how the command **show log | include 302013** can be used to display all the logging messages with message ID 302013 currently stored in the logging buffer. Because message 302013 records TCP connections that are built in either the inbound or outbound direction, you might decide to rework the regular expression to find more specific information. To display only the inbound TCP connections recorded, the regular expression could be changed to include 302013, any number of other characters (.*), and the string "inbound," as shown at the bottom of the example.

Example 2-7 *Searching Through Command Output*

```
ciscoasa# show logging | include 302013
302013: Built outbound TCP connection 1788652405 for outside:69.25.38.107/80
  (69.25.38.107/80) to inside:10.1.198.156/1667 (207.246.96.46/52531)
302013: Built outbound TCP connection 1788652406 for outside:218.5.80.219/21
  (218.5.80.219/21) to inside:10.1.100.61/3528 (207.246.96.46/52532)
[output truncated]

ciscoasa# show log | include 302013.*inbound
```

```
302013: Built inbound TCP connection 1788639636 for outside:216.117.177.135/54780
  (216.117.177.135/54780) to inside:10.1.3.16/25 (207.246.96.46/25)
ciscoasa#
```

You might also use a regular expression to display command output that contains IP addresses within a range. For example, the following command filters the output to contain only IP addresses that begin with 10.10.5, 10.10.6, and 10.10.7:

```
ciscoasa# show log | include 10.10.[5-7].*
```

Terminal Screen Format

By default, all output from an ASA is displayed for a terminal session screen that is 80 characters wide by 24 lines long. To change the terminal screen width, use the following configuration command:

```
ciscoasa(config)# terminal width characters
```

Here, *characters* is a value from 40 to 511. You can also specify 0, meaning the full 511-character width.

To change the screen length, or the number of lines displayed when paging through a large amount of output, use the following configuration command:

```
ciscoasa(config)# pager [lines] number
```

Here, *number* can be any positive value starting at 1. The **lines** keyword is optional, where the number of lines given is the same either with or without it.

You can also disable screen paging completely by using **pager 0** or **no pager**. This action might be useful if you are capturing a large configuration or logging message output with a terminal emulator. With paging disabled, all of the output could scroll by and be captured into the emulator's capture buffer. Otherwise, you would have to use the spacebar to page through the output and then later remove all the <-- More --> prompts that were captured.

Using Cisco ASDM

Cisco ASDM provides a GUI that you can use to administer, configure, and monitor an ASA. Although ASDM does not use a regular web browser, it does use the HTTPS protocol to communicate with the ASA.

To access ASDM, you need a PC-based launcher utility. The launcher allows you to select an ASA and enter administrator credentials. The launcher will then connect to the ASA, download the ASDM application (if it has not already been installed on the PC), and automatically launch it on the PC.

Before you can use ASDM, you need to enter an initial "bootstrap" configuration in the ASA using the following steps:

Step 1. Copy an ASDM image file into ASA flash memory.

Use a file transfer method such as TFTP to copy an ASDM image file from your PC to the ASA's flash memory. Be aware that a specific ASDM image release might work with only a specific release of the ASA operating system. You can verify that the ASDM image is ready to use by using the **dir disk0:/** command to display the flash file system contents, as shown here:

```
ciscoasa# dir disk0:/
Directory of disk0:/
132     -rwx  17232256      18:37:02 Nov 02 2011  asdm-645.bin
131     -rwx  25159680      18:36:08 Nov 02 2011  asa842-k8.bin
3       drwx  8192          14:04:34 Apr 27 2007  log
13      drwx  8192          14:05:02 Apr 27 2007  crypto_archive

255426560 bytes total (225050624 bytes free)
ciscoasa#
```

Step 2. Specify the ASDM image file to use.

Use the **asdm image** configuration command to specify which ASDM image file to use. For example, the following command tells the ASA to use ASDM release 6.4(5), contained in file disk0:/asdm-645.bin:

```
ciscoasa(config)# asdm image disk0:/asdm-645.bin
```

Once the ASDM image file has been specified, you can use the **show asdm image** command to display the file location and name.

Step 3. Enable the HTTP server process.

Use the following command to enable the HTTP server on the ASA. Both HTTP and HTTPS are supported, although ASDM uses only HTTPS.

```
ciscoasa(config)# http server enable
```

Step 4. Specify IP addresses that are permitted to access ASDM.

Because ASDM uses the HTTP server process, you can enter the following command to specify which IP addresses are permitted to access ASDM through a specified interface:

```
ciscoasa(config)# http ip-address subnet-mask interface
```

For example, you can use the following commands to permit clients in the 192.168.100.0/24 subnet on the outside interface and 192.168.2.0/24 on the inside interface to access ASDM:

```
ciscoasa(config)# http 192.168.100.0 255.255.255.0 outside
ciscoasa(config)# http 192.168.2.0 255.255.255.0 inside
```

You can also use the **http 0.0.0.0 0.0.0.0 outside** command to permit ASDM access to any host on the outside interface.

Next, you need to access ASDM for the first time. Open a web browser to the ASA interface that you have configured to permit HTTP connections. In Figure 2-1, the web browser has been opened to https://192.168.100.10—the outside interface of an ASA.

Figure 2-1 *Accessing ASDM*

The initial ASDM page gives you the following three options:

- **Install ASDM Launcher and Run ASDM:** The Launcher and ASDM will run as native applications on the PC, without the need for a web browser.
- **Run ASDM:** You can run ASDM from within the web browser as a Java application.
- **Run Startup Wizard:** ASDM will initiate a wizard to step you through the initial ASA configuration, if you have not already done so.

The first option is the most common choice and needs to be done only once. After the Launcher application is installed, you can run it directly to initiate an ASDM session. Click the **Install ASDM Launcher and Run ASDM** button. You will be prompted for an ASA username and password. The installer must authenticate with the ASA to download the Launcher file. ASDM always needs "enable" or the highest available user access in order to launch and run.

Next, the ASA prompts you to enter a location to store the downloaded Launcher installer, as shown in Figure 2-2. Click **Save File** and browse to the desired location. Once the installer file has been downloaded onto your PC, find the file and double-click it. The Launcher application will install and run automatically.

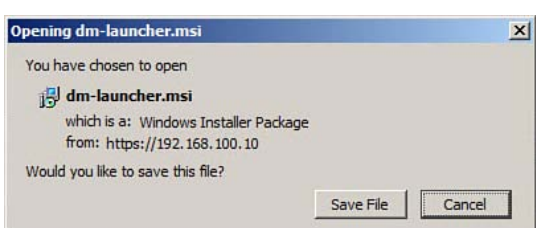


Figure 2-2 *Saving the ASDM Installer File*

Figure 2-3 shows the ASDM Launcher application. To connect to an ASA and begin an ASDM session, enter the ASA's IP address and administrator credentials. The IP address will be cached and added to a list of possible ASAs so that you can choose from a list the next time you run the Launcher.

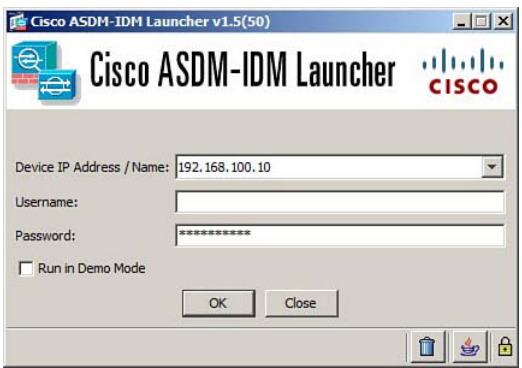


Figure 2-3 *ASDM Launcher Application*

Once the Launcher successfully connects to the ASA, the full-blown ASDM application window appears. Figure 2-4 shows the initial ASDM Home view. By clicking the buttons in the upper-left portion of the window, you can navigate through the following functions:

- **Home:** Displays information about the ASA platform, VPN sessions, CPU and memory resource usage, interface status, and traffic bandwidth.

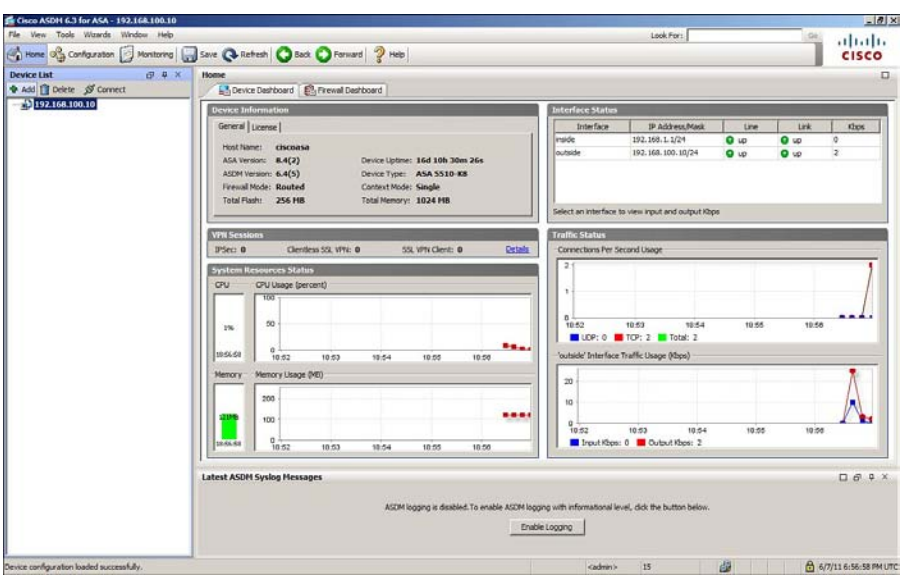


Figure 2-4 *ASDM Home View*

- **Configuration:** Provides a hierarchy of ASA features and parameters that you configure and verify.
- **Monitoring:** Offers categories and lists of specific ASA parameters that you can monitor or observe.

At any time, you can click the **Save** button to save the current running configuration to the startup configuration, or click the **Refresh** button to load the current running configuration into ASDM.

In Configuration view, which is shown in Figure 2-5, you can select any of the following different feature categories in the lower-left area of the window:

- **Device Setup:** Features such as interfaces, routing, device name, and system time that are necessary for the ASA to operate
- **Firewall:** Stateful inspection features needed to inspect traffic and secure a network
- **Remote Access VPN:** Virtual private networks (VPN) used for remote clients to securely connect to the ASA
- **Site-to-Site VPN:** VPNs used for remote sites to securely connect to the ASA
- **Device Management:** Features such as management access, feature licensing, high availability, logging, DNS, and DHCP services

After selecting a feature category, you can select a specific feature to configure from the list in the middle-left portion of the ASDM window. You can then configure individual parameters that are shown in the main part of the window.

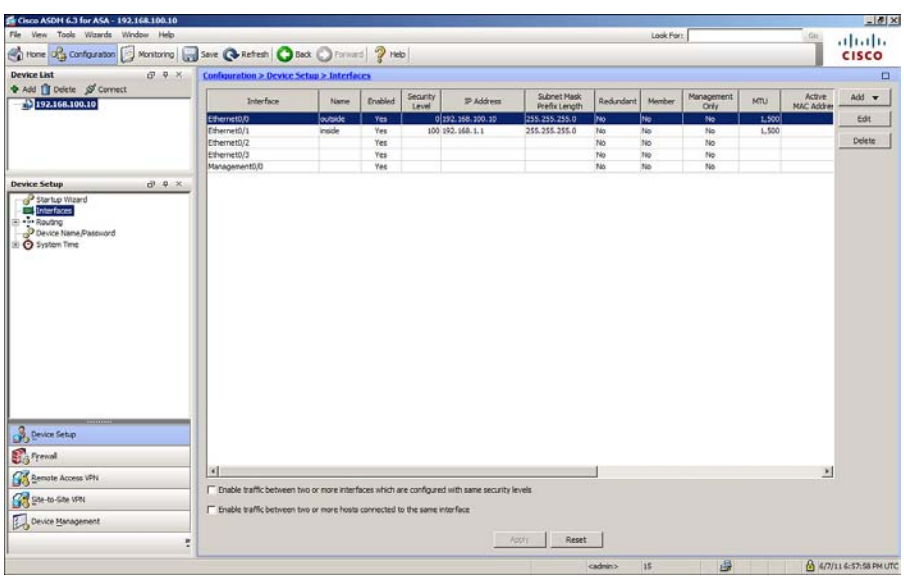


Figure 2-5 *ASDM Configuration View*

As you make configuration changes in ASDM, be aware that the changes are not made to the ASA dynamically. Instead, you must click the **Apply** button that is shown in Configuration view to actually apply the ASDM changes to the ASA's running configuration.

In Monitoring view, shown in Figure 2-6, you can select categories of ASA functions to monitor. For example, you can select interface operation, VPN status, routing activity, device properties, and logging.

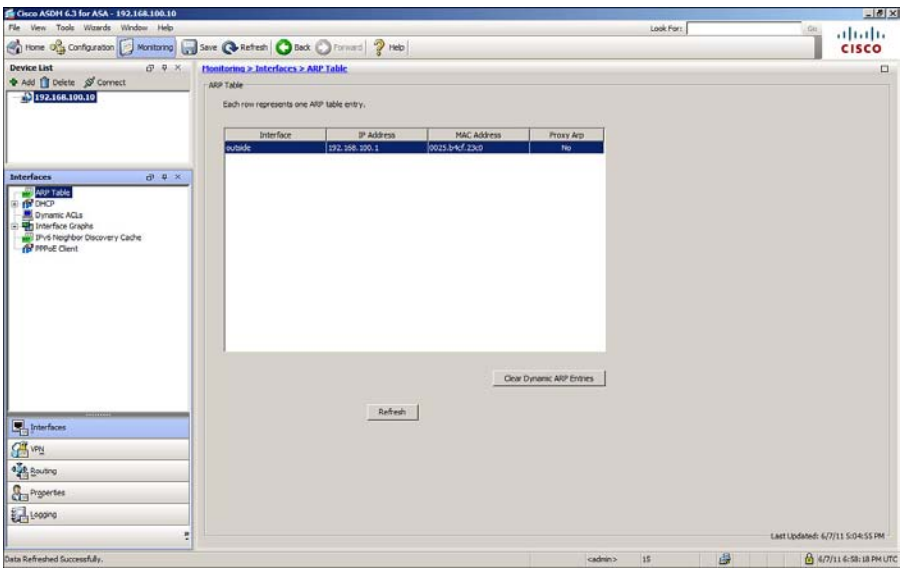


Figure 2-6 *ASDM Monitoring View*

Understanding the Factory Default Configuration

When an ASA boots for the first time, it comes up running a factory default or initial configuration. For the most part, the configuration is barebones, but provides enough functionality so that someone can connect a PC to the ASA and configure it further.

The initial configuration brings up the following basic functions:

- One interface is set aside as a protected "management" network, where a PC will be connected.
- A DHCP server is enabled on the management network, to automatically provide an IP address for the PC.
- An HTTP server is enabled on the management network, to allow the PC to access secure web-based ASDM sessions with the ASA via HTTPS over TCP port 443.

In the initial configuration, the management interface is always configured to use IP address 192.168.1.1 and subnet mask 255.255.255.0. The DHCP server is configured to

provide addresses from a range of 192.168.1.2 to 192.168.1.254. The HTTP server is configured to allow ASDM sessions from devices on the 192.168.1.0/24 management network.

On ASA 5510 and higher platforms, the initial configuration always uses the Management0/0 physical interface for the management network, as shown in the top portion of Figure 2-7. The ASA 5505, however, doesn't have a dedicated management interface. Instead, it uses VLAN 1 for the secure "inside" network, which is assigned to physical interfaces Ethernet0/1 through 0/7.

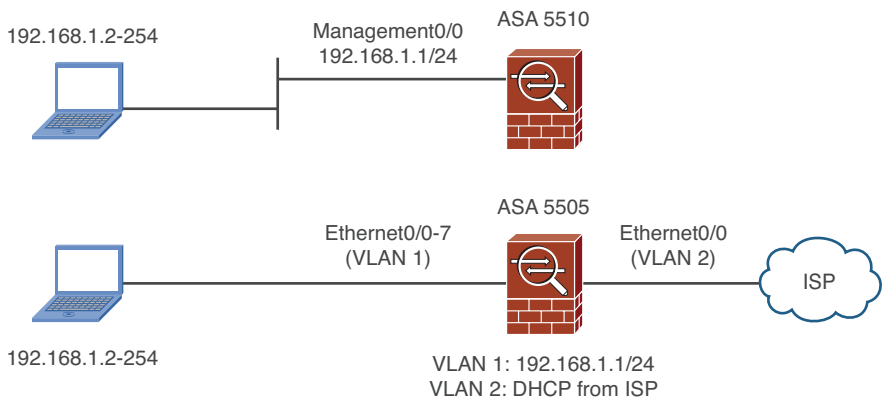


Figure 2-7 *Using the ASA Factory Default Configuration*

Because the ASA 5505 is usually installed in smaller environments, it often connects directly to an Internet service provider (ISP) through a broadband connection. The ASA 5505 default configuration provides basic connectivity from its inside network to the outside world, as shown in the bottom portion of Figure 2-7. The outside network must be connected to physical interface Ethernet0/0, which is mapped to VLAN 2. The ASA is configured to obtain an IP address for its outside interface automatically, through a DHCP request. Then, any device that is connected to the inside network will have its IP address translated as it passes through the ASA toward the outside world.

At any time in the future, you can force an ASA to return to its factory default configuration by entering the **configure factory-default** command in configuration mode. Be aware that this command immediately takes effect, with no further confirmation, as shown in Example 2-8. If you are connected to the ASA remotely, through Telnet, SSH, or ASDM, you will likely be cut off; instead, you should enter this command only while directly connected to the ASA console port.

Example 2-8 *Returning an ASA to the Factory Default Configuration*

```
ciscoasa(config)# configure factory-default
Based on the management IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 192.168.1.1 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 192.168.1.0 255.255.255.0 management
Executing command: dhcpd address 192.168.1.2-192.168.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Working with Configuration Files

An ASA keeps a "startup" configuration file in flash memory. The configuration commands in the startup configuration are not lost after a reload or power failure. As soon as an ASA boots, the startup configuration commands are copied to the "running" configuration file in RAM (volatile) memory. Any command that is entered or copied into the running configuration is also executed at that time.

Key Topic

You can see the contents of the startup configuration by entering the **show startup-config** command, as demonstrated in Example 2-9. The first line denotes that the startup configuration has been saved at least once in the ASA's lifetime. The next line records a timestamp that shows the last date and time that the running configuration has been saved to the startup configuration. In addition, a user called enable_15 (someone in privileged EXEC or enable mode) saved the configuration.

Example 2-9 *Displaying the Startup Configuration Contents*

```
ciscoasa# show startup-config
: Saved

: Written by enable_15 at 13:47:39.249 UTC Wed Nov 9 2011
!
ASA Version 8.4(2)
!
```